Business-Intelligence-Systeme im Spannungsfeld zwischen Usability und Sicherheit

Inaugural-Dissertation
zur Erlangung des Doktorgrades
der Wirtschafts- und Sozialwissenschaftliche Fakultät
der Eberhard Karls Universität Tübingen

vorgelegt von
Thorsten Hinck
aus Hechingen

2010

Dekan:	**Prof. Dr. rer. soc. Josef Schmid**
Erstberichterstatter:	**Prof. Dr. rer. pol. Bernd Jahnke**
Zweitberichterstatter:	**Prof. Dr. rer. pol. Ralph Berndt**
Tag der mündlichen Prüfung:	**27.10.2010**

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGG	Gesetz zur Gleichstellung behinderter Menschen
BI	Business Intelligence
BIS	Business-Intelligence-System
iBIS	integratives Business-Intelligence-System
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Errichtungsgesetz
BSS	Benutzungsschnittstelle
DIN	Deutsches Institut für Normung
DOS	Denial of Service
DSK	Datenschutzkonzept
DW	Data Warehouse
CC	Common Criteria
CUA	Common User Access
EIS	Executive Information System
ETL	Extraktion, Transformation und Laden
EVG	Evaluationsgegenstand
FTC	Federal Trade Commission
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoB	Grundsätze ordnungsgemäßer Buchführung
GoBS	Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik

IM	Informationsmanagement
ISO	International Standard Organisation
IT	Informationstechnik
IV	Informationsverarbeitung
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
SQL	Standard Query Language
OLAP	Online Analytical Processing
OLTP	Online-Transaction-Processing
PDA	Persönlicher Digitaler Assistent
RAID	Redundant Array of Inexpensive Disks
ROI	Return on Investment
RoSI	Return on Security Investment
SAA	System Application Architecture
StGB	Strafgesetzbuch
TCO	Total Cost of Ownership
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TSTS	Time-Salary-Time-Sales
UStG	Umsatzsteuergesetz
USV	Unterbrechungsfreie Stromversorgungen
WI	Wirtschaftsinformatik

1. Einleitung

Die Informationsverarbeitung (IV) hat seit ihren Anfängen eine große Entwicklung erfahren. Die im Zeitverlauf leistungsfähiger werdende Technologie hat die Informationsinfrastruktur von Unternehmen tiefgreifend verändert.[1] Entwicklungen wie die Globalisierung, der technologische Fortschritt, die Geschäftsprozessorientierung und die zunehmende Vernetzung, bieten Chancen, begünstigen aber auch Bedrohungen gegenüber Unternehmen, welche in der Informationsgesellschaft von ihrem Wissen und der Informationsverarbeitung abhängig sind.[2] Die Ressource Information hat sehr an Bedeutung gewonnen und ein Großteil der Unternehmen ist heute auf die Informationsverarbeitung angewiesen.[3] Der Leistungserstellungsprozess kann ohne ihren Einsatz gar nicht oder nur sehr eingeschränkt stattfinden. Ferner ist die Informationsverarbeitung von strategischer Relevanz, da ein Informationsvorsprung auf transparenter werdenden Märkten ein entscheidender Wettbewerbsfaktor ist.[4]

Die Unterstützung von Geschäftsprozessen durch Informationssysteme nimmt gegenwärtig weiter zu.[5] Lieferanten und Kunden werden an die unternehmenseigenen Informationssysteme angebunden (Vernetzung) und erhalten dadurch Zugang zur Infrastruktur der Unternehmung.[6] Informationstechnik und Kommunikationstechnik wachsen zur Informations- und Kommunikationstechnik (IKT) zusammen. Diese Vorgänge bieten Chancen für die Unternehmung, steigern jedoch die Unsicherheit des Umfeldes und ermöglichen Akteuren erfolgreiche Wirtschaftsdelikte durch Informationstechnologie.[7]

Vertrauliche Informationen können beispielsweise über elektronische Wege das eigene Unternehmen verlassen oder von Schädlingen des Informationszeitalters

---

[1] Vgl. Helmbrecht, Udo (2007), S. 3; vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 6.
[2] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 6; vgl. Thome, Rainer (2006), S. 27; vgl. Müller, Rainer (2005), S. 1.; vgl. Eckert, Claudia (2006), S. 12.
[3] Vgl. Jahnke in den Vorlesungen WI 1 und 4.
[4] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 6.
[5] Eckert, Claudia (2006), S. 3.
[6] Vgl. Müller, Klaus-Rainer (2003), S. 5.
[7] Vgl. [Pfitzmann, Andreas (a); http://dud.inf.tu-dresden.de]. Quellenangaben in [ ] beziehen sich auf das Internet. Aufgrund der Aktualität des Themas kann viellfach nur auf Internetquellen zurückgegriffen werden.

beeinträchtigt werden.[8] Ebenso kann es vorkommen, dass Daten unbewusst preisgegeben werden. Beispielsweise befanden sich auf der verkauften Festplatte der Brandenburger Polizei vertrauliche Einsatzpläne für Geiselnahmen oder Entführungen sowie Namenslisten für die Besetzung von Krisenstäben.[9] Die Folgen der Handlungen im Bereich der Informationsverarbeitung sind den Akteuren hierbei nicht immer transparent. PriceWaterhouseCoopers beziffert unter diesen Rahmenbedingungen 62 Prozent der deutschen Unternehmen mit über 5.000 Beschäftigten und 37 Prozent der Mittelständler mit weniger als 200 Beschäftigten als Opfer von Wirtschaftsdelikten im IT-Umfeld.[10]

Die Gesamtheit der heute anzutreffenden Informationssysteme in Unternehmen ist meist heterogen, sie beinhalten unterschiedliche Daten und haben unterschiedliche Reifegrade. Operative Systeme produzieren eine aus Transaktionsdaten bestehende „Datenflut". Daneben enthalten Business-Intelligence-Systeme (BIS) Wissensdatenbanken[11], Entscheidungsmodelle, ein mehr oder weniger entwickeltes Intranet und Zugriff auf externe Datenquellen wie das Internet. Diese Systeme vereinen qualitative und quantitative Daten, die teils in strukturierter, meist jedoch in unstrukturierter Form vorliegen. Sowohl die Heterogenität der Plattformen als auch der Daten selbst stellt für die Unternehmen und Entwickler eine große Herausforderung dar.[12] Somit ist Transparenz für den Bereich der Informationsinfrastrukur von Unternehmen, welche die Basis für sicheres Handeln darstellt aufgrund der Komplexität der Einzelkomponenten nur schwer herstellbar.

Durch die wachsende Abhängigkeit der Wirtschaft und Verwaltung von dem einwandfreien Funktionieren und der uneingeschränkten Verfügbarkeit informationstechnischer Systeme nimmt die Vertraulichkeit, Verfügbarkeit und Integrität der Daten (IT-Sicherheit) einen immer höheren Stellenwert ein.[13] Der Vertraulich-

---

[8] Vgl. Müller, Rainer (2005), S. 1.

[9] [Kästner, Sven (2005) in Spiegel Online; http://www.spiegel.de].

[10] Vgl. [Salvenmoser, Steffen; Kruse, Lars Heiko (2005); http://www.pwc.de], S. 1.

[11] Der Begriff Wissensdatenbanken wird verwendet, obwohl es derzeit keine Wissensdatenbanken gibt, welche den Anforderungen an solche genügen. Gemeint ist damit die Möglichkeit des Transfers von Informationen welche Beschreibungen von Vorgängen enthalten.

[12] Vgl. Knöll, Heinz-Dieter; Schulz-Sacharow; Zimpel, Michael (2006), S. 1f; vgl. Biethan, Jörg; Muksch, Harry; Ruf, Walter (2004), S. 10.

[13] Vgl. [BSI; http://www.bsi.bund.de]; vgl. Eckert, Claudia (2006), S. 10 ; vgl. Schmidt, Klaus (2006), S. 1ff.

keitsstatus dieser Informationen ist dabei abhängig von der Art des Inhaltes und den Nutzern, an die sich das System richtet.[14]

Erfolgreiches wirtschaftliches Handeln beruht auf richtigen Entscheidungen. Die sich dynamisch verändernden Gegebenheiten auf den Absatzmärkten aber auch im Bereich der Produktionstechnologie machen es schwierig, strategische Entscheidungen intuitiv zu treffen. Zunehmender Wettbewerbsdruck[15] und die zeitweise Talfahrt der Konjunktur machen es notwendig sich mit den sich ändernden und vorhandenen Rahmenbedingungen des wirtschaftlichen Umfeldes kritisch auseinanderzusetzen.[16] Es ist festzustellen, dass Entscheidungssituationen immer komplexer werden. Deshalb lohnt es sich für Entscheidungsträger über den Einsatz von Business-Intelligence-Systemen nachzudenken, welche sie bei ihren Entscheidungen unterstützen. Eine Vielzahl immer besserer aber auch komplexerer Technologien zur Steuerung von Unternehmen wird zur Unterstützung von verschiedenen Herstellern angeboten.

Informationssysteme, die den Entscheidungsprozess unterstützen, werden bereits rudimentär in vielen Unternehmen eingesetzt. Als Beispiel können Kundendatenbanken in Verbindung mit Produktionszahlen oder Marktdaten herangezogen werden. Die Anbieter SAP, SAS, Infor, MIS, Cognos, Oracle/Hyperion und Business Objects bieten Business Intelligence Software an, welche auf statistische Verfahren, Online Analytical Processing (OLAP), Data Mining bzw. Reporting-Verfahren zurückgreift, um den Unternehmensführern Entscheidungen zu erleichtern.[17] Die angebotenen Systeme sind sehr komplex und können von einem einzelnen Menschen kaum durchschaut werden.[18]

Strategische Entscheidungen sind von erheblicher Bedeutung für den Bestand des Unternehmens. Eine Sicherheitsbetrachtung der verwendeten Systeme und der Schutz der Wirtschaftsgeheimnisse als wesentlicher Teil des Betriebskapitals ist deshalb notwendig.[19] Probleme der IT-Sicherheit sind dabei hauptsächlich Zeit- und Ressourcenmangel, ständig neu auftretende und sich verändernde Gefahren,

---

[14] Vgl. Ertel, Wolfgang (2001), S. 160; Laudon, Kenneth, C.; Laudon, Jane, P. (2006); S. 351.
[15] Vgl. Wodtke, Carolina; Richters, Swantje (2004), S. 1.
[16] Vgl. Hamilton, Patrick (2007), S. 89ff.
[17] Vgl. Knöll, Heinz-Dieter; Schulz-Sacharow; Zimpel, Michael (2006), S. 2f.
[18] Meinung des Autors, nach einem direkten Vergleich der Angebot der der Firmen MIS, Cognos und BO; vgl. Dern, Gernot (2006); S. 13.
[19] Vgl. Wodtke, Carolina; Richters, Swantje (2004), S. 1.

hoher Aufwand, Komplexität und Heterogenität der Systeme, Budgetrestriktionen, Intransparenz, ungeeignete Standards für kleinere und mittlere Unternehmen sowie nicht zuletzt der Mensch als Unsicherheitsfaktor.[20] Ein junger Bereich des wissenschaftlichen Interesses gilt der Usability von Informationssystemen, welcher sich der Verbesserung der Gebraustauglichkeit widmet.[21]

1989 erschien in Deutschland das Buch Kuckucksei von Clifford Stoll. Es handelt sich um die authentische Geschichte eines Systemmanagers der über einen Abrechnungsfehler Sicherheitslücken in Systemen von Universitäten und militärischen Einrichtungen der USA sowie im weltweiten Datennetz aufdeckte. Die Sicherheit von Informationssystemen wird als Problem der nächsten Jahrzehnte erkannt.

Während meines Studiums arbeitete ich als Werkstudent im debis Systemhaus und konnte dabei Einblicke in die Gestaltung und Programmierung von Softwareprodukten im Bereich der BIS und Dokumentenmanagementsysteme für Industriekunden gewinnen. Diese Erfahrung sensibilisierte mich für die Teilaspekte Sicherheit und Usability von Informationssystemen. Die Gebrauchstauglichkeit der Systeme ist für mich von Interesse, da ich bei deren Nutzung oft an Grenzen gestoßen bin.

Deshalb sind moderne Informationssysteme in Verbindung mit dem Sicherheitsbedürfnis und der Entscheidungsrelevanz der ihnen anvertrauten Daten/Informationen Gegenstand dieser Arbeit.

1.1. Problemstellung

Der Ausgangspunkt der Überlegung ist die Annahme, dass Unternehmen integrative BIS zur Entscheidungsunterstützung der oberen Führungsebene einsetzen können. „Business Intelligence ist [dabei] der Prozess der Umwandlung von Daten in Informationen und weiter in Wissen. Entscheidungen und Prognosen stützen sich auf dieses Wissen und schaffen dadurch Mehrwert für ein Unternehmen.“[22] „Business Intelligence bezeichnet [ferner] den analytischen Prozess, der

---

[20] Vgl. Gründer, Torsten in Gründer, Torsten (2007), S. 18f.

[21] Vgl. Manhartsberger, Martina; Musil, Sabine (2001), S. 33ff; vgl. Herczeg, Michael (1994), S. 9; vgl. Harloff, Joachim (2005), S. 45; vgl. Bawa, Joanna; Dorazio, Pat; Trenner, Lesley (2001), S. xi.

[22] Humm, B.; Wietek, F. (2005), S. 3.

fragmentierte Unternehmens- und Wettbewerbsdaten in handlungsgerichtetes Wissen über die Fähigkeiten, Positionen und Ziele der betrachteten internen oder externen Handlungsfelder (Akteure und Prozesse) transformiert.“[23] Der Begriff selbst wurde mit großer Wahrscheinlichkeit zuerst von Hans Peter Luhn 1958 im IBM Journal in einem Artikel zu Business-Intelligence-Systemen verwendet und 1989 von Howard Dresner einem Analysten der Gartner Group übernommen. Des Weiteren sind viele Definitionen von Business Intelligence denkbar, dies zeigt sich insbesondere in der unterschiedlichen Verwendung des Begriffes für Systeme in unterschiedlichen Bereichen der Informationssystempyramide, welche von unterschiedlichen Gruppen auch zur Vermarktung von Informationssystemen eingeführt werden. Für diese Arbeit ist die oben genannte Definition am treffendsten, da die Unterstützung von Entscheidungen und Generierung von Prognosen dem Unterstützungspotential der Informationstechnik für Führungskräfte gerecht wird.[24]

BIS dienen der Entscheidungsunterstützung von Führungskräften der oberen Führungsebene. Ihre Aufgaben erfassen die Aufbereitung und Darstellung von entscheidungsunterstützenden Informationen für Führungskräfte. Architektonisch sind diese Systeme in die Unternehmensinfrastruktur vertikal und horizontal integriert, um diese Aufgabe erfüllen zu können. Sie sind im oberen Bereich der Informationssystempyramide einzuordnen.[25]

Es ist nicht ausreichend, wenn Daten und Informationen für die strategischen Entscheidungen im BIS enthalten sind. Sie müssen dem Nutzer (der Führungskraft) verfügbar und bewusst gemacht werden, indem eine berechtigte Interaktion zwischen Mensch und Computer stattfindet (Mensch-Computer-Interaktion). Die Interaktion zwischen Mensch und Maschine findet über Benutzungsschnittstellen statt.[26]

BIS bestehen aus einer Vielzahl von Technologien und Einzel-Systemen, die in Verbindung miteinander ein Entscheidungsunterstützungssystem darstellen. Diese Systeme beinhalten sensible Daten und Informationen, welche für den Bestand

---

[23] Grothe, M.; Gentsch, P.; (2000), S. 11.
[24] Luhn; Hans Peter (1958); vgl. Engels, Christoph (2008), S.4ff.
[25] Vgl. Leser, Ulf; Naumann, Felix (2007), S. 4f.
[26] Vgl. Schneier, Bruce (2000), S. 260ff.

und das Wachstum des Unternehmens unabdingbar sind. Dies ergibt sich aus dem Zweck dieser Systeme, welcher darin besteht, das Management mit entscheidungsrelevanten Informationen zu versorgen. Die Sicherheit dieser Systeme ist somit für das Unternehmen relevant und muss gemanagt werden. Management kann als Führungsaufgabe verstanden werden, welche eine Menge von Strukturierungs-, Koordinations- und Integrationsaufgaben umfasst, die für den Erhalt von arbeitsteilig organisierten Institutionen und Vorhaben notwendig sind.[27] Die Begriffe Führung und Management werden häufig synonym verwendet.[28] Sicherheitsmanagement bedeutet die systematische Planung, Umsetzung, Steuerung und Weiterentwicklung der Sicherheit im Unternehmen oder dessen Organisationseinheiten.[29]

Wegen der Bedeutung der in diesen Systemen verfügbaren Daten und Informationen für die Entscheidung von Führungskräften der oberen Führungsebene könnte es interessant sein, sich als bspw. Konkurrent, böswilliger Dritter, fremde Nation oder entlassender Mitarbeiter Zugang zu diesen Informationen zu verschaffen. Besteht Zugang zum Informationssystem, ist es möglich die enthaltenen Daten zu verändern um den Entscheidungsprozess zu beeinflussen oder die Informationen zu vernichten, um diesen zu behindern. Es ist nicht alleine das Interesse des Homo oeconomicus sich einen betriebswirtschaftlichen Vorteil zu verschaffen, sondern es sind eine Vielzahl von Motiven denkbar Schaden zufügen zu wollen.[30]

Fast täglich treffen Meldungen über Sicherheitslücken (Zugangsmöglichkeiten) in bestehenden Systemen ein. Betroffen ist nicht nur die Software der genutzten Systeme sondern auch die Kommunikationsprotokolle, das Betriebssystem und die Hardware.[31] Abhilfe bieten Sicherheitsmaßnahmen, diese erhöhen allerdings die bereits vorhandene Komplexität der Systeme und erschweren in der Regel auch berechtigten Nutzern den Umgang mit dem BIS. Des Weiteren sind die Wirkungsweisen von miteinander verwendeten und abhängigen Sicherheitsmaßnahmen sehr intransparent. Benutzer von Informationssystemen, insbesondere Führungskräfte, wünschen sich aber eine einfache und komfortable Bedienung der

---

[27] Vgl. Heinrich, Lutz, J. (1997), S. 9.
[28] Wild, Jürgen (1994) in Krüger (1994), S. 23; vgl. Küpper, Hans-Ulrich (2001), S. 14.
[29] Vgl. Müller, Rainer (2005), S. 445.
[30] Vgl. Eckert, Claudia (2006), S. 10.
[31] Vgl. E-Mailwarnungen des ZDV Tübingen.

Systeme. Damit ist ein Spannungsfeld zwischen Sicherheit und Usability (Gebrauchstauglichkeit) vorhanden. Es gilt ein Sicherheitskonzept zu entwerfen, welches größtmöglichen Nutzen und vertretbare Sicherheit für BIS ermöglicht.

1.2. Begründung für die Untersuchung

Für die Untersuchung sprechen zunächst ökonomische Gründe, da ein erhebliches Schadenspotenzial durch Unterlassen auftreten kann. Neben den bisher angesprochenen Teilbereichen gibt es eine weitere Aufgabe in Form des Risiko-Managements, das vor allem durch gesetzliche Regelungen in den Blickpunkt gerückt ist.

Auf deutscher Ebene gilt seit 1998 das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), welches das Management von Aktiengesellschaften zwingt, ein Überwachungssystem zur Früherkennung von Risiken einzuführen. Auf europäischer Ebene trat 2007 eine als „Basel II“ bekannte Regelung in Kraft, die der Risikominimierung bei der Kreditvergabe dienen soll.[32] Jedes Unternehmen, das einen Kredit beantragt, wird nach einem Rating-System bewertet. Ein Bestandteil des Ratings ist die Aufstellung aller Risiken und der Konzepte zur Kontrolle derselben.[33] In diesem Zusammenhang wird der Sarbanes-Oxley Act genannt, der in den USA seit Juli 2002 in Kraft ist. Nach dem Sarbanes-Oxley Act muss das Management innerhalb seines jährlichen Berichts zusätzlich über das interne Kontrollwesen Auskunft geben. Dies betrifft das Risiko-Management, weil dadurch angenommen wird, dass Risiken minimiert werden.

Das Risiko-Management ist im IV-Bereich besonders wichtig. Dort werden zum einen riskante Zukunftsinvestitionen in großer Höhe getätigt, die neue Möglichkeiten aber auch Gefahren beinhalten. Zum anderen ergeben sich durch die Abhängigkeit des Geschäftsbetriebs von der IV große Risiken für das Unternehmen in seiner Gesamtheit. Die Sicherheit und Zuverlässigkeit in diesem Bereich ist nicht immer gewährleistet, sodass Risiken hier einerseits eine hohe Eintrittswahrscheinlichkeit, andererseits aber auch eine starke Auswirkung besitzen. Folgender

---

[32] Vgl. Geiger, Gebhard (2007), S. 48¸ Vgl. Speichert, Horst (2007), S. 249f; vgl. Schrey, Joachim in Gründer, Torsten (2007), S. 275ff; vgl. Müller, Klaus-Rainer (2003), S. 6.
[33] Vgl. Haar, Tobias; Schädler, Sarah (2004), S. 99ff; vgl. Geiger, Gebhard (2007), S. 48.

Risikomanagementregelkreis kann aufgestellt werden[34]: Risikoidentifikation, Risikoanalyse durch Risikoanalyseverfahren[35], Risikosteuerung und Risikoüberwachung. Innerhalb dieser Risikosteuerung sind vier Grundstrategien denkbar. Die Risikoakzeptanz, Risikoverlagerung, Risikoverminderung und Risikovermeidung.[36]

Ziel der Arbeit ist es, die Wichtigkeit der „IT-Security“ aufzuzeigen. Des Weiteren sollen die Belange der Usability erörtert werden, um Fortschritte in der Gebrauchstauglichkeit von quasi-sicheren Informationssystemen zu erzielen. Schwerpunkt der Arbeit ist die Identifikation der Gefahren und deren Abwehr. Im Mittelpunkt der Betrachtung stehen Mensch (Führungskraft) und Benutzungsschnittstelle sowie eine sichere Architektur eines BIS. Sekundärziel der Arbeit ist es, die Leser dahin gehend zu sensibilisieren, dass die Wichtigkeit einer „Usabel Security“ erkannt wird und es operationalen Stellen zu ermöglichen geeignete Maßnahmen für dieses Ziel zu treffen.

1.3. Vorgehensweise

Nach den notwendigen Grundlagen des Themas, der Definition von integrativen BIS, Sicherheit und Usability werden, da die Risiken/Gefahren des Betriebs von integrativen BIS noch nicht ausreichend untersucht und dokumentiert sind, diese im Folgenden erarbeitet. Als nächster Schritt werden Sicherheitsmaßnahmen dargestellt, die für die Sicherung des ordnungsgemäßen Betriebs eines integrativen BIS verfügbar sind. Es zeigt sich, dass die Sicherheitsmaßnahmen bisher isoliert voneinander betrachtet werden.[37] Diese Untersuchung muss hinsichtlich der Wechselwirkungen von Sicherheitsmaßnahmen untereinander erweitert werden.

Im nächsten Schritt wird die Auswirkung von Sicherungsmaßnahmen auf die Usability von integrativen BIS untersucht. Da Führungskräfte der Adressat der Benutzerschnittstelle eines integrativen BIS sind, wird die Auswirkung der Sicherheitsmaßnahmen auf diese untersucht. Abschließend wird ein Sicherheitsprofil unter Beachtung des Spannungsfeldes von Sicherheit versus Usability erarbeitet.

---

[34] Vgl. Krcmar, H.; Reb, M. (Eds.), S. 445; vgl. Krcmar, Helmut (2005), S. 451; vgl. Ahrendts, Fabian; Marton, Anita (2008), S. 14.
[35] Vgl. Homeister, Matthias (2005), S. 180f.; vgl. Eckert, Claudia (2006), S. 171; vgl. Dridi, Fredj (2003), S. 54ff.
[36] Vgl. Ahrendts, Fabian; Marton, Anita (2008), S. 16.
[37] Vgl. exemplarisch Kollmann, Tobias (2007),S. 82. Hier wird Sicherheit auf SSL reduziert.

Ökonomisch betrachtet stellen Gefahren ein Verlustrisiko dar. Dieses ist gegenüber dem Nutzen abzuwägen. Nutzen und Verlust lassen sich unter den noch zu zeigenden Rahmenbedingungen mit herkömmlichen Methoden nicht einfach exakt quantifizieren. Es sind Methoden notwendig, die qualitative Aspekte mit einbeziehen.

2. Grundlagen

2.1. Untersuchungsgegenstand

Aufgabe der Wirtschaftsinformatik (WI) ist unter anderem die Erklärung und Gestaltung der Phänomene ihres Gegenstandsbereiches Informationssysteme und Informationsinfrastruktur.[38] Untersuchungsgegenstand dieser Arbeit sind „Informationssysteme" im Sinne von Mensch-Aufgabe-Technik-Systemen aus dem oberen Teil der Informationssystempyramide von Scheer im Hinblick auf das Verhältnis von Sicherheit zu Usability. Es handelt sich um integrative BIS zur Entscheidungsunterstützung innerhalb des Informationsmanagements. Sie haben eine lange historische Entwicklung bestritten und stehen gerade vor ihrem nächsten Entwicklungsschritt unterstützt von den Fortschritten im Enterprise Application Integration-Bereich, hin zu integrativen Business-Intelligence-Systemen.[39]

2.2. Objekte des Informationsmanagements

BIS werden im Rahmen des Informationsmanagements (IM) eingesetzt, deshalb werden im Folgenden die für diese Arbeit wichtigen Aspekte des IM vorgestellt.[40]

2.2.1. Informationsmanagement

Ziel des IM ist es, im Hinblick auf die Unternehmensziele den bestmöglichen Einsatz der Ressource Information zu gewährleisten.[41] IM ist sowohl Management wie Technikdisziplin und gehört zu den elementaren Bestandteilen der Unterneh-

---

[38] Vgl. Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2007), S. 15.

[39] Vgl. Dietrich von der Oelsnitz (Hrsg.); Weibler, Jürgen (Hrsg.); Gabriel, Roland; Beier, Dirk (2003), S. 43ff, vgl. Chamoni, Peter; Gluchowski, Peter (2006), S. 11.

[40] Vgl. Baschin, Anja; Steffen, Andreas (2001), S. 1,56; vgl. Horváth, Peter (2003), S. 720; vgl. Kaplan, R. S.; Norton, D. P. (1997); vgl. Töllner, Andrea (1995), S. 22ff., S. 32ff.; vgl. Eckert, Claudia (2006) S. 3.

[41] Vgl. Krcmar, Helmut (2005), S. 49; vgl. Dietrich von der Oelsnitz (Hrsg.); Weibler, Jürgen (Hrsg.); Gabriel, Roland; Beier, Dirk (2003), S. 59ff.

mensführung. Für den Bereich der Führungsaufgaben werden drei grundsätzlich zu treffende Entscheidungen identifiziert:[42]

1. Welche Leistungen sollen erbracht werden?

2. Von wem wird die Leistung erbracht?

3. Wird die Leistung „richtig“ erbracht?

Der Bedarf einer effizienten Organisationsstruktur zur Erledigung aller aus den drei Fragen resultierenden Aufgaben führt zum Begriff der IT-Governance[43], den Weill/Woodham wie folgt definieren: ”Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT“.[44] Um Aufgaben in Unternehmen zu lösen, werden demnach Informationen benötigt, die als Produktionsfaktor betrachtet werden können.[45]

Information

Der Begriff der Information wird kontrovers diskutiert. In der Wissenschaft gibt es verschiedene Definitionen des Begriffes Information, die hier dargestellt werden. Das Wort Information ist aus dem lateinischen informatio (= Bildung, Belehrung) abgeleitet. Allgemein versteht man darunter eine Nachricht, Mitteilung oder Auskunft über etwas oder jemanden. Außerdem sind als Definition noch Hinweis und Inkenntnissetzung angegeben.[46]

In der Betriebswirtschaftslehre herrscht die Definition von Wittmann, Information ist zweckbezogenes Wissen, vor.[47] Problematisch ist, dass sie mit dem Wort Wissen einen zu definierenden Begriff enthält. Zudem ist fraglich, ob Information erst durch eine Zweckbindung entsteht. Die DIN 44300 zur Informationsverarbeitung umgeht eine Erklärung des Informationsbegriffs und umschreibt ihn durch die Begriffe Zeichen, Signal und Daten[48]. Information wird durch ein Datum repräsentiert und ergibt sich aus der vorher festgelegten Interpretationsvorschrift. Datenobjekte sind dabei über Schnittstellen in Form von Operationen bzw. Methoden von anderen Objekten, zu denen auch seine Benutzer gehören erreichbar. Je-

---

[42] Vgl. Krcmar, Helmut (2005), S. 284.
[43] Vgl. Moormann, Jürgen; Schmidt, Günter (2007), S. 231ff.
[44] Weill, P.; Woodham, R. (2002), S. 1.
[45] Vgl. Meier, Andreas (2007), S. 1.
[46] Brockhaus - die Enzyklopädie: in 24 Bänden. F.A. Brockhaus GmbH, (1997), S. 524.
[47] Waldemar, Wittmann (1959), S. 14.
[48] Deutsches Institut für Normung. DIN 44300.

der Zugriff auf ein Datenobjekt ist deshalb als Zugriff auf die zugrunde liegende Information anzusehen.[49]

Die Semiotik unterscheidet zwischen vier Dimensionen der Information. In Bezug auf die Konventionen einer Sprache beschäftigt sich die Syntaktik mit der Beziehung einzelner Zeichen zueinander. Die zweite Dimension beinhaltet die semantische Analyse, welche die inhaltliche Bedeutung der Zeichen betrachtet. Die Sigmatik analysiert die Beziehung zwischen Zeichen und bezeichnetem Objekt. Als vierte Dimension untersucht die Pragmatik die Beziehung zwischen Zeichen und Verwender, also das, was Information kennzeichnet.[50] Aus Sicht der Wirtschaftsinformatik ist die semiotische Definition des Begriffs Information die treffendste, weil sie sowohl die Entstehung als auch die inhaltliche Bedeutung berücksichtigt.

Im Rahmen der Unternehmensführung treten unterschiedliche Aufgabenbereiche auf, deren Zeithorizonte divergieren, deshalb stellt die übergreifende Kommunikation von Informationen sowie deren Koordination einen Schlüsselfaktor für BIS dar.[51] Dass zur Entscheidungsunterstützung eine bloße Bereitstellung von großen und damit unüberschaubaren Datenmengen ungenügend ist, haben die Erfahrungen der letzten Jahrzehnte mit verschiedensten Arten von Informationssystemen gezeigt. [52] Ziel eines BIS, ist es, Informationen in Form von entscheidungsrelevanten Daten bereitzustellen.

Informationsbedarf

Die Anforderungen eines BIS bestehen grundsätzlich darin, den Informationsbedarf der Führungskraft abzudecken. Daher spielt dessen Ermittlung bei der Entwicklung eines BIS eine fundamentale Rolle.[53] Der Informationsbedarf ist dabei die Gesamtheit der Informationen, die zur Bewältigung einer bestimmten Aufgabe benötigt werden[54]. Darüber hinaus wird zusätzlich ausdrücklich auf den Mangel an den zur Problemlösung nötigen Informationen hingewiesen.[55] Besonders soll

---

[49] Vgl. Eckert, Claudia (2006) S. 3f.
[50] Krcmar, Helmut (2003), S. 16 .
[51] Vgl. Knöll, Heinz-Dieter; Schulz-Sacharow; Zimpel, Michael (2006), S. 9.
[52] Bernhard, Dorn (1994), S. 13; Groffmann, Hans-Dieter (1992), S. 1; vgl. Dietrich von der Oelsnitz (Hrsg.); Weibler, Jürgen (Hrsg.); Gabriel, Roland; Beier, Dirk (2003), S. 43ff.
[53] Vgl. Struckmeier, H. (1997), S. 28.
[54] Vgl. Wall, F. (1996), S. 13.
[55] Vgl. Hoffmann, H. (1993), S. 28; [Kluck, M. (2003); http://server02.is.uni-sb.de].

der Zweck der Information im Vordergrund stehen, da dieser die Grundlage für die Informationsbedarfsanalyse bildet.

Es gilt zwei Arten von Informationsbedarf zu unterscheiden. Zum einen den objektiven Informationsbedarf, welcher auf der Aufgabenstellung basiert und somit unabhängig vom Informationsempfänger ist und zum anderen der subjektive Informationsbedarf, der sich aus der Sicht des Aufgabenträgers und dessen Bedürfnissen ergibt. Trotz häufiger Unterschiede diesbezüglich, gehen einige Autoren davon aus, dass eine Unterscheidung im Bezug auf Führungskräfte eine eher unwichtige Rolle spielt. Ihre Begründung lautet, diese seien nur an möglichst guten Informationen interessiert.[56] Da möglichst gute Informationen aus der Sicht der Führungskraft durch den subjektiven Informationsbedarf gedeckt werden, folge ich dieser Auffassung nicht.

Die Informationsbedarfanalyse wird als die Bereitstellung derjenigen Informationen verstanden, welche das Lösen eines Problems und das innerbetriebliche Zurechtfinden durch einen Mitarbeiter erfordert.[57] Eine weniger formale Definition spricht von dem Vorgang der Ermittlung des Informationsbedarfs eines bestimmten Anwenders bei Entwicklung eines Informationssystems.[58] Es kann jedoch noch weiter im Verständnis der Informationsbedarfsanalyse gegangen werden. Hierbei wird zwar auch die Art der benötigten Informationen angesprochen, diese aber noch um den Ort, die Zeit, den Informationslieferanten und die Häufigkeit der erforderlichen Informationen ergänzt.[59]

Im Mensch-Aufgabe-Technik-System wird Information als handlungsbestimmendes Wissen über vergangene, gegenwärtige und zukünftige Zustände der Wirklichkeit und Vorgänge in der Wirklichkeit bezeichnet.[60] Der Mensch als Aufgabenträger nutzt Information zur Erfüllung seiner Aufgabe. Dieser anthropozentrische Ansatz berücksichtigt neben den notwendigen Informationen zur Erfüllung der Aufgabe auch das individuelle Informationsbedürfnis. Die technikorientierte Konzeption sieht im Gegensatz dazu den Mensch als Aufgabenerfüller, dem zur Bewältigung nur die objektiv und problemspezifisch ermittelten Informationen

---

[56] Vgl. Wall, F. (1996), S. 14; Hoffmann, H. (1993), S. 29.
[57] Vgl. Struckmeier, H. (1997), S. 28.
[58] Vgl. Kluck, M. (2003) in [Buder, M. (Hrsg.); http://server02.is.uni-sb.de].
[59] Vgl. Walpoth, G. (1993), S. 7.
[60] Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2007), S. 134.

zur Verfügung gestellt werden. Für die Arbeit wird der anthropozentrische Ansatz gewählt.

Um Informationen richtig bereitstellen zu können, wird eine Informationsbedarfsanalyse durchgeführt, welche es Führungskräften ermöglichen soll die richtigen Informationen zum richtigen Zeitpunkt zu erhalten, beziehungsweise um die richtigen Entscheidungen zu treffen. Die entstehende Informationsfunktion umfasst alle Aufgaben im Unternehmen, deren Zweck das Beschaffen und Verwenden von Information ist.[61]

2.2.2. Unternehmung

Als Unternehmen oder Unternehmung wird im Allgemeinen ein von Personen durchzuführendes Vorhaben bezeichnet, es handelt sich um eine dauerhafte organisatorische Einheit zur Produktion bzw. zur Erbringung von Dienstleistungen, die mehrere Betriebe umfassen kann. Je nach Träger werden private, öffentliche oder gemeinwirtschaftliche Unternehmen unterschieden. Je nach Rechtsform Einzel-, Personen- und Kapitalgesellschaften. Als Unternehmen wird der rechtliche Rahmen für die Betriebstätigkeit bezeichnet. Das Unternehmen nimmt Kredite auf, trägt das Risiko, erzielt Gewinne oder Verluste und schließt Geschäfte ab.[62]

Es handelt sich um eine Bezeichnung der Betriebswirtschaftslehre für eine wirtschaftlichrechtlich organisierte Wirtschaftseinheit, sie ist von dem Betrieb abzugrenzen, der den technischen Produktionsbereich kennzeichnet.[63] In Deutschland ist der Begriff des Unternehmers in § 14 BGB sowie §2 Abs. 1 UStG definiert. Unternehmer ist demnach, wer eine gewerbliche oder berufliche Tätigkeit selbstständig ausübt.

Betriebsmittel, Unternehmensinfrastruktur, Menschen und externe Schnittstellen stellen die Unternehmensgesamtheit dar. Die organisatorischen Rahmenbedingungen, in welche ein Unternehmen eingebettet ist, nennt man Unternehmensumwelt.

---

[61] Vgl. Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2007), S. 145.
[62] Vgl. Schweizer, M. in Bea, F.X.; Friedl, B.; Schweizer, M. (2004), S. 38ff; vgl. Schierenbeck, Henner (2003); S. 28.
[63] Vgl. Schweizer, M. in Bea, F.X.; Friedl, B.; Schweizer, M. (2004), S. 38ff; [Capital; http://www.capital-select.de].

2.2.3. Infrastruktur

Der Sammelbegriff Infrastruktur bezeichnet alle langlebigen Grundeinrichtungen personeller, materieller und institutioneller Art, die das Funktionieren einer arbeitsteiligen Volkswirtschaft garantieren.[64] Eine Infrastruktur ist weiter ein System von Einrichtungen, Ausrüstungen und Dienstleistungen, welche für den Betrieb einer Organisation erforderlich sind.[65] Jedes IT-System ist in eine Infrastruktur eingebettet.[66]

Unternehmensinfrastruktur

Komplexe Systeme bestehen in der Regel aus Recheneinheiten, Peripheriegeräten, Programmen, Netzwerken und Menschen, deren komplexes Zusammenspiel durch Hardware- und Softwarekomponenten geregelt wird. Der Mensch ist hier durch die Definition von Informationssystemen als Mensch-Aufgabe-Technik-Systeme im organisatorischen Kontext in die Systembetrachtung als wichtiger Teilaspekt mit einzubeziehen. Des Weiteren ist zu beachten, dass unter Informationssysteme nicht nur Computer, sondern auch Geräte wie Telefone, Faxgeräte und ähnliches fallen.

---

[64] Vgl. Olfert, Klaus; Rahn, Horst-J. (2005), S. 21; vgl. Paul, Joachim (2007), S. 1; S. 218; vgl. Thommen, Jean-Paul; Achleitner, Ann-Kristin (2003), S. 35; vgl. Wöhe, Günter; Döring, Ulrich (2005), S. 8; S. 71 ff.

[65] Vgl. Laudon, Kenneth, C.; Laudon, Jane, P. (2006); S. 199f; [Go-cert; http://www.go-cert.de].

[66] Vgl. Kersten, Heinrich; Klett Gerhard (2008), S. 34f.

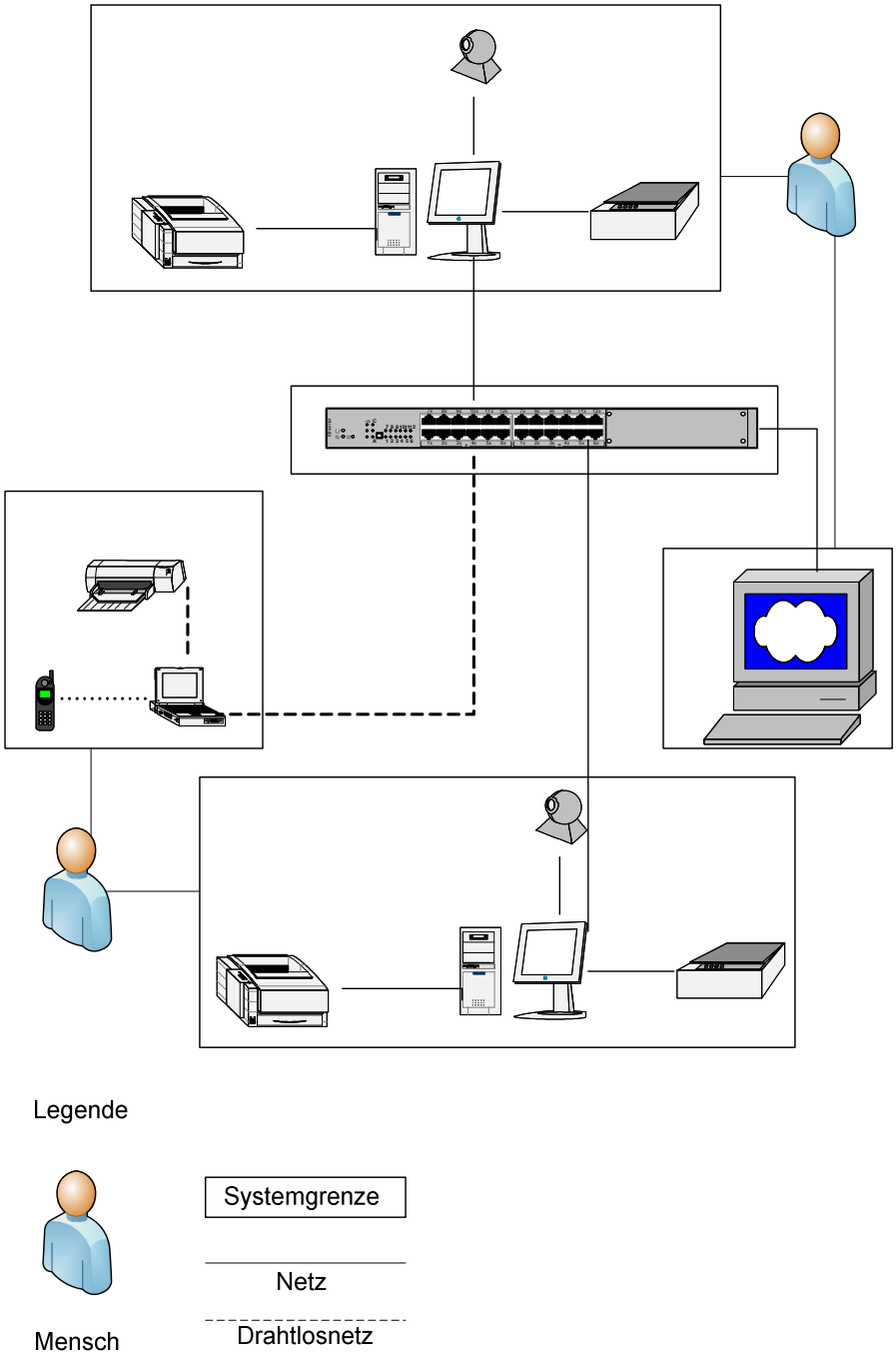

Abbildung 1: (Technischer) Ausschnitt einer Unternehmensinfrastruktur

Die Abbildung zeigt einen Ausschnitt aus einer technischen Unternehmensinfrastruktur. Es sind typische Computersysteme (oben und unten in der Abbildung) über einen Switch (Mitte der Abbildung) miteinander per Kabel (durchgezogene Linien) verbunden. Es besteht ein Zugang zum Internet (rechts in der Abbildung). Mobile Geräte sind links über Wireless-Verbindungen (gestrichelte Linien) einge-

bunden.[67] Infrastrukturelle Sicherheit[68] und Sicherheitsinfrastruktur[69] sind deshalb Teilziele dieser Arbeit.

Ein Fehler in der Infrastruktur macht das Gesamtsystem anfällig für Datenverlust, Missbrauch, Manipulation, etc.. Es ist deshalb notwendig eine Karte der Infrastruktur und speziell der IT-Infrastruktur des Unternehmens zu erstellen, in welcher die Informationsflüsse und Informationsaufbewahrungsorte verzeichnet sind, diese wird auch als Informationslandkarte bezeichnet.[70]

2.3. Objekte des Informationsprozesses

Die Objekte des Informations- bzw. Entscheidungsprozesses nehmen wesentlichen Einfluss auf die Entscheidungsunterstützung durch BIS.

2.3.1. Sicherheitsrelevante Objekte

Anforderungen an Sicherheit beziehen sich zum einen auf die Eigenschaften, die das betreffende System erfüllen soll, zum anderen auf die zu verwendenden Maßnahmen oder Mechanismen.[71] Als sicherheitsrelevante Objekte werden identifiziert: die Organisation, Kontinuitätsplanung, das Personal, die Notfallvorsorge, Wartung, Beschaffung, Infrastruktur, das Netzwerk, IT-System, externe Zugänge, Telekommunikation, Kryptografie, Virenschutz, Zugangsschutz/Authentisierung sowie Daten und Applikationen.[72]

Durch die Schutzbedarfsanalyse werden die Auswirkungen der Beeinträchtigung von Sicherheitskriterien ermittelt.[73] Schutzbedarf[74] ist der Schutz vor kriminellen Handlungen und höherer Gewalt sowie menschlichem Versagen, die Herstellung der Verfügbarkeit[75] und Vermeidung von Computerkriminalität[76].

---

[67] Vgl. Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2007), S. 159f.
[68] Vgl. Englbrecht, Michael (2004), S. 5.
[69] Vgl. Eckert, Claudia (2006), S. 30f.
[70] Vgl. Leser, Ulf; Naumann, Felix (2007), S. 7ff.
[71] Vgl. Weck, Gerhard; Horster, Patrick (Hrsg.) (1993), S. 225.
[72] Vgl. Pohlmann, Norbert (2004), S. 125.
[73] Vgl. Müller, Rainer (2005), S. 444.
[74] Vgl. Eckert, Claudia (2006), S. 162
[75] Vgl. Müller, Rainer (2005), S. 9.
[76] Vgl. Godschalk, David (2007), S. 51ff.

2.3.2. Führungskräfte

Der Terminus Führungskräfte bezeichnet Menschen in der mittleren bis obersten Management-Ebene von Unternehmen. Eine Führungskraft muss kein Unternehmer sein und besitzt nicht zwingend Anteile des von ihm geleiteten Unternehmens.[77] Angehörige der oberen Führungsebene weisen oft sehr spezielle, individuelle Eigenschaften bei der Aufgabenbewältigung auf, diese werden auch beim Einsatz von Informationstechnologie beibehalten. Sie zeichnen sich gegenüber Informationstechnologie durch eine positive Einstellungsbilanz, gleichermaßen aber überwiegend durch eine negative Verhaltensakzeptanz aus.[78]

Führungskräfte als Aufgabenträger müssen sich auf die dargebotenen Informationen verlassen können, um Entscheidungen zu treffen. Unter diesen Rahmenbedingungen wird ersichtlich, dass die Integrität und Authentizität von Informationen die über ein BIS dargestellt werden von entscheidender Bedeutung für den Erfolg oder Misserfolg von Unternehmen werden können. Sind die angebotenen Informationen falsch oder gelangen sie in unberechtigte Hände kann ein Schaden entstehen.[79]

Beispielsweise könnten die Produktionszahlen verfälscht werden, was falsche Bestellungen und strategische Ausrichtungen nach sich zieht. Übernahmepläne könnten vereitelt und Firmengeheimnisse weiterverbreitet werden.

Nach Henry Mintzberg lassen sich die Aktivitäten einer Führungskraft in drei Rollenbündel klassifizieren:

1. Repräsentative Rollen: Vorgesetzter, Vernetzer.

2. Informationale Rollen: Radarschirm, Sender, Sprecher.

3. Entscheidungsrollen: Innovator, Störungsregler, Ressourcenzuteiler, Verwalter.

Führungskräfte können zum Management des Unternehmens gezählt werden. Die Unternehmensführung bzw. das Management entspricht im betriebswirtschaftlichen Umfeld der Betriebsführung.[80]

---

[77] Vgl. Jahnke, B (1993a), S. 1.
[78] Vgl. Müller-Böling; Ramme (1990), Sp. 336ff; Vgl. Jahnke, B (1993a), S. 5.
[79] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[80] [Go-cert; http://www.go-cert.de].

Aufgabe eines Managers ist die Planung, Durchführung, Kontrolle und Anpassung von Maßnahmen zum Wohl der Organisation bzw. des Unternehmens und aller daran Beteiligten (Anspruchsgruppen = Stakeholder) unter Einsatz der ihm zur Verfügung stehenden betrieblichen Ressourcen. Eine Aufgabe ist die Verpflichtung eines Aufgabenträgers, eine vorgegebene Handlung durchzuführen. Da im engeren Sinn nur Menschen Aufgaben erfüllen können, spricht die DIN V ENV 26385 „… von einer aus dem Arbeitszweck abgeleiteten Aufforderung an die Arbeitsperson(en), eine Arbeit unter gegebenen Bedingungen nach einem vorgegebenen Verfahren auszuführen und ein bestimmtes Ergebnis anzustreben“. [81]

Es handelt sich bei einer Aufgabe in der betriebswirtschaftlichen Organisationslehre um ein zu erfüllendes Handlungsziel, eine durch physische oder geistige Aktivitäten zu verwirklichende Soll-Leistung.[82] Der Begriff der Aufgabe kann sich sowohl auf die Gesamtaufgabe wie auch auf Teilaufgaben einzelner Elemente oder Mitglieder beziehen.

Jede Aufgabe wird qualitativ bestimmt durch eine Verrichtung, ein Objekt in Raum und Zeit, quantitativ durch eine geforderte Mengenleistung je Zeitraum. Aufgaben werden unterschieden nach ihrem Wiederholungscharakter und ihrer Beherrschbarkeit. Ihr Wiederholungscharakter ist bestimmt durch ihre Häufigkeit und das Auftreten gemeinsamer Elemente. Die Beherrschbarkeit von Aufgaben hängt von deren Komplexität, Variabilität und Determiniertheit ab. Inhalt, Volumen und Erfüllungsanforderungen von Aufgaben ändern sich im Zeitablauf. Dies löst bei entsprechender Abweichung von Soll- und Ist-Anpassungen und Reorganisationen aus. Die unstrukturierten, komplexen Aufgaben betragen den Hauptteil der Arbeit eines Managers. Planung, Steuerung und Kontrolle sind bspw. klassische Aufgaben der Führungsebene.[83]

Da verschiedene Personengruppen auf das BIS eines Unternehmens zugreifen und dabei die unterschiedlichsten Prioritäten an das System stellen, ist es wichtig, diese Gruppen zu unterscheiden. Diese Arbeit beschränkt sich überwiegend auf die Sicht der Führungskraft auf das BIS und somit die Anforderungen, die eine Führungskraft an ein solches System stellt.

---

[81] Vgl. Frese (1980) , S. 207.
[82] Vgl. Hoffmann, H. (1993), S. 200).
[83] Vgl. Knöll, Heinz-Dieter; Schulz-Sacharow; Zimpel, Michael (2006), S. 16ff.

Derjenige Teil des Systems in dem die Informationen für die Führungsebene aufbereitet werden nennt sich Business-Intelligence-System (BIS) oder Executive Information System (EIS). Anhand der Abbildung werden die Unterteilungen deutlich, die innerhalb des BIS für die einzelnen Personengruppen bzw. Ebenen einer Unternehmung gemacht werden.

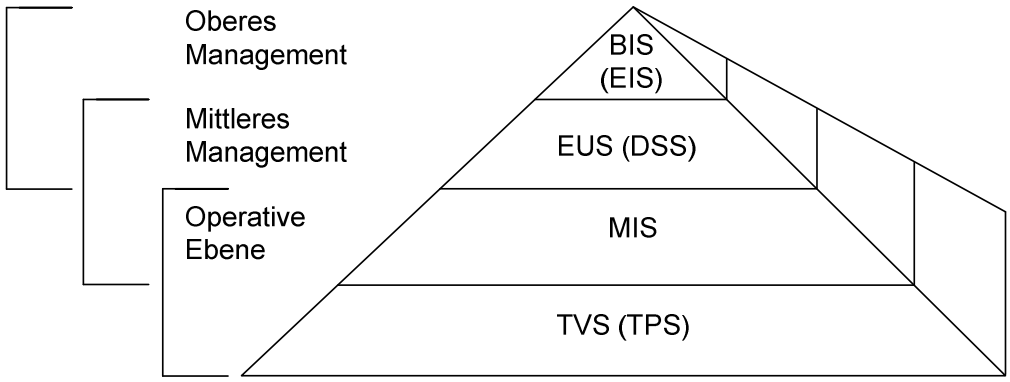

Abbildung 2: Informationssystempyramide[84]

Die Ansprüche, die eine Führungskraft an das BIS hat, divergieren von Fall zu Fall, da sich jedes Unternehmen in der Struktur unterscheidet. Die Führungskraft fordert dabei abhängig von ihrer Hierarchiestufe ein mehr gebrauchstaugliches BIS. Hoyer begründet diese Auffassung mit der Forderung von Grafiken gegenüber der einfachen Listendarstellung. Die Sinnhaftigkeit dieser Darstellungsform muss dabei objektiv die Gebrauchstauglichkeit nicht steigern, sondern hängt von der subjektiven Einstellung der Führungskraft ab.[85] Allerdings gibt es einige allgemein gültige Anforderungen, die ein Großteil der Führungskräfte stellt. Eine davon ist die Personalisierung von BIS.[86] Ein BIS sollte in der Lage sein, die Führungsebene bei ihren strategischen Planungsaufgaben zu unterstützen.[87]

Die Aufgaben der Führungskräfte sind überwiegend koordinierender und kommunizierender Art.[88] Daher ist es sehr wichtig, dass die Führungskräfte durch das Informationssystem die Möglichkeit haben mit den übrigen Mitarbeitern der Führungsebene zu kommunizieren und auch Informationen aus anderen Teilen des

---

[84] Vgl. Jahnke, B. (1993), S. 3.
[85] Vgl. Ertel, Wolfgang (2001), S. 160.
[86] Vgl. Herczeg, Michael (2006), S. 189ff.
[87] Vgl. Henning, M.; (2003), S. 78f.
[88] Vgl. Henning, M.; (2003), S. 77.

Betriebs einzuholen. Das gilt natürlich auch für die Zeit, in der sich der Manager außerhalb des Stammhauses befindet. Das BIS muss ihm die Möglichkeit bieten auch außerhalb seines Schreibtisches auf die für ihn wichtigen Informationen zugreifen und mit dem Unternehmen kommunizieren zu können.

Mithilfe des BIS muss es für Führungskräfte möglich sein, einen Überblick über die Unternehmenslage und die Lage der Umwelt (Konkurrenz) zu erhalten, um Entscheidungen treffen und Handlungen koordinieren zu können. Dazu werden sowohl Daten aus internen, als auch aus externen Quellen benötigt. Das

Eine weitere Anforderung an das System ist, die Daten nicht nur in Rohform darzustellen sondern auch als aufbereitete Präsentation in Form von Grafiken und Diagrammen.[89] Durch die Verwendung von Grafiken können Relationen leichter sicht- und merkbar gemacht und kreative Denkprozesse initiiert werden.[90] Wichtig ist auch, dass über das BIS sämtliche Medien (wie z. B. die Videopräsentation) genutzt werden können.[91] Vor allem, weil die Führungsebene die Daten nicht nur zur eigenen Information benötigt, sondern um sie vor anderen Personengruppen zu präsentieren.

Von großer Bedeutung ist ebenfalls, dass das System aktiv agieren und nicht nur auf die Benutzerinitiative reagieren kann.[92] Das BIS soll den Benutzer dazu animieren weitere Informationen zu erfragen, die für den von ihm bearbeiteten und angeforderten Sachverhalt von Bedeutung sind. So kann sichergestellt werden, dass der Manager für ihn relevanten Daten angezeigt bekommt.

Darüber hinaus gilt es den Anspruch an die Leistungsfähigkeit des Systems in Bezug auf Schnelligkeit, Ausfallsicherheit sowie Datensicherheit und –schutz zu berücksichtigen und zu gewährleisten.[93] Die Führungskräfte sollten schnell an die gewünschten Informationen gelangen und von möglichst wenigen Systemausfällen betroffen sein, da sonst die Bereitschaft zur Verwendung des Systems nachlas-

---

[89] Vgl. Behme, W.; Schimmelpfeng, K (1993), S. 6ff.
[90] Vgl. Jahnke, B. (1991), S. 33.
[91] Vgl. Jahnke, B. (1991), S. 33.
[92] Vgl. Jahnke, B.; Groffmann, H.-D. (1993a), S. 5.
[93] Vgl. Birkenbeul, A. (1995), S. 144.

sen kann. Die Sicherheit und der Schutz der Daten[94] spielen unter anderem deshalb eine so große Rolle, da die für die Führungsebene relevanten Daten selten für die Allgemeinheit bestimmt sind. Die Einführung eines speziell für das Top-Management zugeschnittenen Systems wäre sinnlos, wenn das ganze Unternehmen oder Dritte Zugriff auf die Daten haben. Ein IUK-System ist somit „ein Mensch-Aufgabe-Technik-System zur Information und Kommunikation."[95]

2.3.3. Entscheidungen

Eine Entscheidung beschreibt den Wahlakt aus einer Menge von mindestens zwei Handlungsalternativen, wobei die Unterlassungsalternative ebenfalls eine Handlungsalternative darstellt. Eine Entscheidung liegt nicht vor, wenn die Konsequenzen der Handlungsalternativen gleich sind und/oder die Handlungsalternativen nicht realisierbar sind. Entscheidungen müssen in Unternehmen getroffen werden. Die Entscheidungsfindung basiert dabei auf Informationen. Entscheidungsträger haben damit einen Informationsbedarf.[96]

Jedem bewussten Handeln des Menschen geht eine Entscheidung voraus. Dabei wird aus erkannten, real gegebenen Möglichkeiten eine Variante ausgewählt und somit die Verhaltensweise in einer mehrere Entwicklungsmöglichkeiten beinhaltenden Situation festgelegt. Die durch die Entscheidung ausgelösten Handlungen sollen die gegebene Situation verändern. Das gesetzte Ziel kann unter vorgegebenen Ressourcen im Ergebnis maximiert bzw. unter gesetztem Ziel mit minimierten Ressourcen zu erreichen versucht werden. Eine Maximierung des Ziels bei gleichzeitiger Minimierung der Ressourcen hat sich ökonomisch und logisch als nicht haltbar herausgestellt.[97]

Der Inhalt des Begriffs der Entscheidung wird abstrakt-mathematisch in der Spieltheorie erfasst. Jeder Zug eines Spielers oder die Wahl einer bestimmten Strategie für die Führung des Spiels stellen Entscheidungen dar. Mit dem Prozess der Ent-

---

[94] Daten (Lateinisch: dare, datum in der Bedeutung gegebenes) „Daten sind codierte Informationen, die in Computersystemen gespeichert sind" Vgl. Lehner, Franz; Wildner, Stephan; Scholz, Michael (2007), S. 29; vgl. Holzinger, Andreas (2000), S. 27.

[95] Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2004), S. 319.

[96] Vgl. Laux, Helmut (2005), S. 1; vg. Kirsch, Werner (1977), S. 71; vgl. Heinen, Edmund (1969), S. 207ff; vgl. Heinen, Edmund (1982), S. 22f. Das Wort selbst soll von entscheiden, das Schwert aus dessen Scheide ziehen stammen, da dann zwischen kämpfen und nicht kämpfen gewählt wurde.

[97] Vgl. Wittmann, Waldemar (1980), Sp. 897; Link, Jörg (1982). S. 262; vgl. Witte, Eberhard (1980), Sp. 634.

scheidung wird die Bedeutung des Handelns im Gegensatz zum einfachen Wissen betont.[98]

Der Unterschied zwischen einer Entscheidung und einer Berechnung liegt darin, dass für eine Entscheidung unter Umständen nicht alle Fakten erhoben werden können, die zu einer Berechnung erforderlich wären. Entweder weil die Erhebung unwirtschaftlich wäre oder weil die Faktoren sich nicht vergleichen lassen. Eine Entscheidung wird unter Unsicherheit getroffen. Daher sind Entscheidungen oft umstritten, da die verbleibende Unsicherheit mit subjektiven Annahmen belegt wurde. Theoretisch wird der Entscheidungsprozesses mithilfe der Entscheidungstheorie aufgearbeitet. Sie wird definiert als ein System von allgemeinen Regeln, Gesetzen und Erfahrungen, das dazu dient, eine Entscheidung vorzubereiten, zu treffen und zu realisieren. Ziel der Entscheidungstheorie ist es, im Entscheidungsprozess ein optimales Entscheidungsverhalten zu gewährleisten. Für Entscheidungsvorbereitung und Entscheidungsfindung sind operationale Modelle und Methoden Bedeutung, welche in einem BIS hinterlegt sein sollten.[99]

Der Entscheidungsprozess wird charakterisiert als Gesamtheit der notwendigen Schritte von der Erkenntnis der Problemsituation bis zur Entscheidungsfindung. Folgende Stufen sind zu unterscheiden:[100]

Erkenntnis der Problemsituation und Vorentscheidung über das (die) Ziel(e) der Handlung.

Analyse der Problemsituation in Form eines Vergleichs der sich bietenden Möglichkeiten zur Erreichung des (der) Ziels (Ziele).

Erkenntnis und Fixierung der wichtigen Faktoren als Aufgabenstellung unter Berücksichtigung von möglichen Störungen und Risikofaktoren, wobei auch mögliche Versagenssituationen durchgespielt werden können, um das Ziel selbst unter erschwerten Bedingungen zu erreichen.

---

[98] Vgl. Szyperski, Norbert; Windand, Udo (1974), S. 3f; Untersuchungen zur Entscheidung stammen zunächst von Psychologen bei der Analyse von Willenshandlungen der Persönlichkeit.
[99] Vgl. Schinzer, Heiko (1996), S. 9; vgl. Staehle, Wolfgang (1989), S. 484f; vgl. Wissensbach, Heinz (1967), S. 116ff; vgl. Pfohl, Hans-Christian; Braun, Günther, E. (1981), S. 22f; vgl. Pfohl, Hans-Christian (1977), S. 29ff.
[100] Vgl. Pfohl, Hans-Christian; Braun, Günther, E. (1981), S. 22f.

Verteilung der Aufgaben entsprechend zu beschreitender Wege, anzuwendender Mittel und Methoden.

Erarbeiten von Teilanalysen im Vergleich zwischen Ausgangssituationen und gegenwärtiger Situation zur Festlegung von Kriterien für die optimale Entscheidung unter Hervorhebung des Nutzeffekts.

Vorentscheidung über Prämissen zur Lösung der Problemsituation und Auswahl sowie Ausarbeitung günstiger Varianten nach festgelegten Optimalkriterien.

Bewertung der Varianten zur Ermittlung der optimalen Entscheidung sowie Realisierung der Entscheidung.

Entscheidungen können klassifiziert werden nach ihrer Bedeutung in strategische oder taktische Führungs-Entscheidungen, nach dem Gegenstand in Ziel-, Mittel-, Maßnahmeentscheidungen, nach dem Schwierigkeitsgrad der Entscheidungsfindung in routine-, programmierbare, nicht programmierbare und schöpferische Entscheidungen, nach dem Entscheidungssubjekt in Einzel- und Gruppenentscheidungen, nach dem Zeitraum ihrer Realisierung in operative, planende, perspektivische und prognostische Entscheidungen, wobei diese in kurz-, mittel- und/oder langfristige Zeitintervalle fallen. Deshalb sind Ziele (Schutzziele[101]) zu erkennen und zu gewichten.[102]

2.4. Definitionen

2.4.1. Risikobegriff/Gefahrbegriff

Die Wahrscheinlichkeit oder relative Häufigkeit einer Schädigung der Informationssicherheit wird Risiko genannt. Die Begriffe Risiko, Wagnis und Gefahr können synonym verwendet werden.[103] Formal ist Risiko = Eintrittswahrscheinlichkeit * Schaden.[104] Dieses Risiko ist zu beherrschen. Durchgeführt wird dies durch

---

[101] Vgl. Eckert, Claudia (2006), S. 6.
[102] Vgl. Pfohl, Hans-Christian; Braun, Günther, E. (1981), S. 22f.
[103] Vgl. Sandig, Curt in Crochla, Erwin; Wittmann, Waldemar; (1939), S. 45; vgl. Wack, Jessica (2007), S. 21; vgl. Eckert, Claudia (2006), S. 15.; [Insurance; http://www.infosurance.ch]; vgl. Ahrendts, Fabian; Marton, Anita (2008), S. 9.
[104] Vgl. Witt, Bernhard C. (2006), S. 92; vgl. Ahrendts, Fabian; Marton, Anita (2008), S. 9 u. 23.

den Prozess des Risikomanagements zur Identifizierung, Bewertung, Steuerung sowie Vermeidung, Verringerung, Verlagerung oder Vereinnahmung (Akzeptanz) von Risiken.[105]

Sicherheit ist für ein BIS von wichtiger Bedeutung, da strategische Entscheidungen von den zur Verfügung gestellten Informationen abhängen. Jedoch wirken sich Sicherheitsmaßnamen negativ auf die Usability von BIS aus. Umgekehrt trifft derselbe Zusammenhang zu. Je sicherer ein System wird desto schwieriger wird es in seiner Handhabung. Je usablilitykonformer ein System ist desto unsicherer wird es per se. Deshalb stehen Sicherheit und Usability in einem Spannungsfeld.

Sicherheit ist notwendig um das Vertrauen der Führungskräfte in Systeme zu erhalten und qualitativ hochwertige Entscheidungen zu treffen. Usability ist notwendig um Führungskräften zu ermöglichen intuitiv mit diesen Systemen zu arbeiten und keine Reaktanz zuzulassen. Des Weiteren werden Arbeitsabläufe durch Systeme die gebrauchstauglich (usable) sind beschleunigt und verbessert.[106] Es handelt sich teilweise um konkurrierende Ziele, welche aufeinander abgestimmt werden müssen. Der zweite Teil kann ein wenig abgeschwächt werden, indem die Definition von Usability den ersten Teil berücksichtigt. Dies ergibt das Sicherheitsbedürfnis von Business-Intelligence-Systemen.[107]

2.4.2. IT-Sicherheit

Ein Informationssystem ist verlässlich, wenn man sich auf seine Dienste verlassen kann. Diese umgangssprachliche Aussage wird konkretisiert, indem Teilaspekte, zum Beispiel im Sinne von Vermeidung von Unfällen oder gegenüber Schäden die durch Angreifer verursacht werden oder Funktionsfähigkeit genauer gefasst werden.[108]

Sicherheit bezeichnet einen Zustand, der weitgehend frei von Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.[109] Um den Zustand von Si-

---

[105] Vgl. Müller, Rainer (2005), S. 444.

[106] Vgl. Geis, Thomas (2005) Usability von der Stange? Von Normen und Standards, [http://www,fit-fuer-usability.de/1x1/standards/stange.html], Erstelldatum: 18.03.2005, Verfügbarkeitsdatum 04.01.2007; vgl. Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2004), S. 277; vgl. Sarodnick, Florian; Brau, Henning (2006), S. 15.

[107] Vgl. Leser, Ulf; Naumann, Felix (2007), S. 12f.

[108] Vgl. Weck, Gerhard; Horster, Patrick (Hrsg.) (1993), S. 9.

[109] Vgl. Drews, Hans-Ludwig; Leßenich, Heinz Rudolf (1993), S. 233; [IBI Tu-Berlin; http://www.ibi.tu-berlin.de/moses/glossar/glossarmain.htm].

cherheit zu erreichen, werden Sicherheitskonzepte erstellt und umgesetzt.[110] Sie stellen im Allgemeinen eine Analyse möglicher Angriffs- und Schadenszenarien mit dem Ziel ein definiertes Schutzniveau zu erreichen dar. Unterschieden werden muss dabei die Sicherheit gegenüber böswilligen Angriffen (*Security*) und die Sicherheit gegenüber menschlichem und technischem Versagen (*Safety*).[111] Allen Sicherheitskonzepten gemeinsam ist folgende strukturierte Vorgehensweise: Bestimmung des zu schützenden Objektes und der Schutzziele, Analyse der Bedrohungen/Schadenszenarien, Bewertung von Eintrittswahrscheinlichkeit und potenzieller Schadensschwere, Entwicklung von Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit, Planung von Maßnahmen und Bereitstellung von Mitteln zur Schadensbekämpfung und –eindämmung. Wenn das Risiko schlagend wird, Analyse der eigenen Risikotragbarkeit und Genehmigung des Restrisikos. Auch ein ausgefeiltes Sicherheitskonzept ist nicht in der Lage das Restrisiko komplett zu eliminieren.[112]

Sicherheitsmaßnahmen sind erfolgreich, wenn sie dazu führen, dass mit ihnen sowohl erwartete als auch nicht erwartete Gefahren abgewehrt werden. Allgemein wird Sicherheit nur als relativer Zustand der Gefahrenfreiheit angesehen, der stets nur für einen bestimmten Zeitraum, eine bestimmte Umgebung oder unter bestimmten Bedingungen gegeben ist. Sicherheitsvorkehrungen können durch Ereignisse, die sich nicht beeinflussen oder voraussehen lassen, zu Fall gebracht werden. Die Anforderungen der Sicherheit kommen aus der Gesellschaft, dem Staat, dem Markt und den Unternehmen selbst.[113] Im Zustand der Sicherheit liegen keine oder nur geringe Gefahren vor. Gefahren gehen von Bedrohungen aus und können durch Schutzmaßnahmen vermindert werden.

Das Risiko einer Gefahr ist im Zustand der Sicherheit minimal. Das verbleibende Restrisiko wird akzeptiert oder kann an Versicherungsgesellschaften übertragen

---

[110] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 641.
[111] Vgl. Eckert, Claudia (2006), S. 160.
[112] Vgl. Eckert, Claudia (2006), S. 6.
[113] Vgl. Brunnstein, Jochen (2006), S. 10.

werden.[114] In der Informationstheorie kann zwischen unbedingter Sicherheit und der rechentechnischen Sicherheit unterschieden werden.[115]

Weitere Definitionen umfassen Teilaspekte von Extranet- und E-Business-Applikationen sowie geschlossenen User-Gruppen, Mechanismen für die Zugangskontrolle und Autorisierung[116], die Freiheit von nicht akzeptablen Risiken[117], den Schutz von Informationsquellen vor unberechtigten Änderungen, die Zerstörungen oder Preisgabe von Daten, unabhängig davon, ob sie absichtlich oder unabsichtlich erfolgten.

IT-Sicherheit wird angestrebt durch die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen erhalten sollen. Sicherheit in der IT wird durch direkte Sicherheitsvorkehrung in informationstechnischen Systemen (oder Komponenten) und indirekt durch die Anwendung von Regelungen und informationstechnischen Systemen (oder Komponenten) erreicht.[118]

Ebenso sind Definitionen möglich welche Sicherheit als Prozess beschreiben. Diese Prozessdefinitionen sind am sinnvollsten anzuwenden, da sich das Umfeld der Sicherheitstechnologie und deren Herausforderungen ständig wandeln. Es lassen sich folgende Ziele der Sicherheit identifizieren: Vertraulichkeit, Identität, Authentifizierung, Verifizierung, Sicherheit und Informationsgenerierung.[119]

Vertraulichkeit[120] ist die Gewährleistung, dass Daten nur durch befugte Nutzer interpretiert werden.[121] Vertrauen ist die subjektive Überzeugung der Richtigkeit von Handlungen und Einsichten eines anderen oder von sich selbst. Zum Vertrauen gehört die Überzeugung der Möglichkeit von Handlungen und der Fähigkeit zu Handlungen. Das Gegenteil des Vertrauens ist das Misstrauen. In den Wirtschaftswissenschaften gibt es erst seit der Revidierung des Homo oeconomi-

---

[114] Vgl. Buchner, Frank (2007), 10ff; vgl. [FH-Heilbronn; http://sicherheit.i3g.fh-heilbronn.de]; vgl. Eckert, Claudia (2006), S. 15.
[115] Vgl. Erickson, Jon (2006), S. 212f.
[116] Vgl. Merz, Michael (1999), S. 120; [Achtg; http://www.achtg.de].
[117] [ISO-14971; http://www.iso-14971.de].
[118] Vgl. Leser, Ulf; Naumann, Felix (2007), S. 12f; [Uni Mannheim; http://ncc.uni-mannheim.de]; vgl. Eckert, Claudia (2006), S. 10; vgl. Poguntke, Werner (2007), S. 4.
[119] Vgl. Schulze, Tillmann (2006), S. 69f; vgl. Schmidt, Klaus (2006), S. 14ff.
[120] Vgl. Eckert, Claudia (2006), S. 8.
[121] Vgl. Witt, Bernhard C. (2006), S. 76.

cus-Axioms Platz für ein Konstrukt wie Vertrauen. Jedoch gibt es Uneinheitlichkeiten bei den Definitionen, den Begriffsverwendungen, den verwandten Konstrukten und den implizierten Mechanismen, was eine Vertrauenstheorie in den Wirtschaftswissenschaften bisher verhindert.

Zuverlässigkeit (auch Verlässlichkeit) ist der Umfang, in dem von einem System erwartet werden kann, dass es die beabsichtigte Funktion mit der erforderlichen Genauigkeit ausführt. Sie umfasst Korrektheit, Robustheit und Ausfallsicherheit. Zuverlässigkeit wird für allgemeine Beschreibungen in nichtquantitativem Sinn benutzt. Es handelt sich dabei um einen zeitbezogenen Aspekt der Qualität. Gegenbegriff ist die Unzuverlässigkeit.[122]

Verfügbarkeit[123] ist die Gewährleistung, dass ein IT-System für befugte Benutzer zugänglich und funktionsfähig ist.[124]

Integrität ist die Gewährleistung, dass die Daten des IT-Systems nur durch befugte Nutzer verändert werden.[125] Integrität = Unverfälschtheit ist die Eigenschaft eines Objektes nicht unzulässig oder unbefugt verändert oder gelöscht worden zu sein.[126]

Zurechenbarkeit ist die Gewährleistung, dass jederzeit festgestellt werden kann, welcher Nutzer einen Prozess ausgelöst hat.[127]

Authentifizierung ist der Vorgang der Überprüfung (Verifikation) einer behaupteten Identität, beispielsweise einer Person oder eines Objekts, z. B. eines Computersystems. Authentisierung ist der Vorgang des Nachweises der eigenen Identität. Das englische Wort authentication[128] steht für beide Vorgänge. Dementsprechend werden die beiden Ausdrücke im Deutschen oft (ungenau) synonym verwendet.[129]

---

[122] Vgl. Eckert, Claudia (2006), S. 10.
[123] Vgl. Eckert, Claudia (2006), S. 10.
[124] Vgl. Witt, Bernhard C. (2006), S. 69.
[125] Vgl. Witt, Bernhard C. (2006), S. 72.
[126] Vgl. Müller, Rainer (2005), S. 450.
[127] Vgl. Witt, Bernhard C. (2006), S. 80.
[128] Authentication = engl. Die Authentifikation bzw. Authentifizierung.
[129] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2; vgl. Eckert, Claudia (2006), S. 7; vgl. Dridi, Fredj (2003), S. 65.

Autorisierung bezeichnet in Informationstechnologischem Zusammenhang die Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Dienste an Systemnutzer. Die Autorisierung erfolgt nach einer erfolgreichen Authentifizierung. Die zwei häufigsten Spezialfälle sind der erlaubte Zugriff auf sogenannte Ressourcen in einem Computernetzwerk und die Erlaubnis zur Installation oder Benutzung von Computerprogrammen.[130] Rechtsverbindlichkeit gewährleistet, dass Daten und Vorgänge gegenüber Dritten jederzeit rechtskräftig nachgewiesen werden können.[131]

Als Anforderungen an sicherheitskritische Systeme wurden identifiziert: die Datensicherheit in den Ausprägungen Vertraulichkeit, Datenintegrität, Verbindlichkeit, Verfügbarkeit und Sicherstellung der Zustellung; die Zugriffssicherheit mit den Bestandteilen Autorisierung[132], Authentifikation, und Anonymität; die Systemsicherheit durch Monitoring, Traceability, Auditing und mehrstufige Sicherheit.[133] Die Authentifikation bedeutet in diesem Zusammenhang die Überprüfung der am Anfang festgelegten Sicherheitsanforderungen.[134] Häufig stehen jedoch kostenaufwendige Sicherheitsmaßnahmen den wirtschaftlichen Belangen zum Kapitalgewinn entgegen.

2.4.3. Rechtssicherheit

Die Begriffe Rechtssicherheit und juristische Sicherheit können synonym verwendet werden. Sie beinhalten die rechtliche Gestaltung des Unternehmensumfelds.[135] Die rechtlichen Anforderungen an die IT-Sicherheit sind umfangreich. Bisher existiert keine Systematik in welcher die einschlägigen Vorschriften nachgelesen werden könnten.[136] Für Unternehmen ist es deshalb wichtig die entsprechenden Vorschriften zu kennen.

Ausgangspunkt der Überlegung sind die gesetzlich bestimmten Sorgfaltspflichten.[137] Die Geschäftsführung eines Unternehmens hat die Sorgfalt eines ordentli-

---

[130] Vgl. Dridi, Fredj (2003), S. 66.
[131] Vgl. Witt, Bernhard C. (2006), S. 81.
[132] Vgl. Merz, Michael (1999), S. 120.
[133] Vgl. Englbrecht, Michael (2004), S. 6ff.
[134] Vgl. Müller, Rainer (2005), S. 451.
[135] Vgl. Speichert, Horst (2007), S. 270f.
[136] Vgl. Witt, Bernhard C. (2006), S. 3.
[137] Vgl. Witt, Bernhard C. (2006), S. 3.

chen Kaufmannes anzuwenden. Je nach Unternehmensform finden sich die Vorschriften in den gesellschaftsrechtlich einschlägigen Gesetzen und Normen. Beispielsweise im Aktiengesetz oder GmbH-Gesetz. Im Streitfall ist diese Sorgfalt von der Geschäftsführung nachzuweisen.[138] Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) konkretisiert diese Sorgfaltspflichten durch die Anweisung ein Überwachungssystem zur Erkennung fortbestandsgefährdender Entwicklungen einzurichten. Diese Gesetze verpflichten Unternehmen de facto ein funktionierendes Risikomanagement einzuführen.[139]

Handelsrechtlich müssen die Bücher der Unternehmung nach den Grundsätzen ordnungsgemäßer Buchführung (GoB) geführt werden. Wird dies durch IT-Unterstützung geleistet, ergänzen sich die Anforderungen zusätzlich um die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) des Bundesfinanzministeriums. Wirtschaftsprüfer kontrollieren diese Vorschriften auch im Hinblick auf die Risiken der IT-Infrastruktur, IT-Anwendungen und IT gestützte Geschäftsprozesse.[140]

Des Weiteren sind die Vorschriften des §17 UWG zur Wahrung des Betriebs- und Geschäftsgeheimnis einschlägig und die Aufbewahrungspflichten des § 257 HGB müssen erfüllt sein. Steuerrechtlich kommen die Vorschriften der §§ 145-147 AO, sowie die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) und § 14 IV UStG hinzu.[141] Im weiteren Sinne sind auch das Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz), das Gesetz über die Nutzung von Telediensten (Teledienstegesetz) sowie die Telekommunikations-Datenschutzverordnung, das Telekommunikationsgesetz maßgeblich. Eine weitere Rechtsquelle findet sich im Entwurf des Gesetzes zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts.[142]

Weitere rechtliche Anforderungen ergeben sich aus dem Bundesdatenschutzgesetz (BDSG), insbesondere die §§ 7 (Schadenersatz), 43 (Bußgeldvorschriften) und 44

---

[138] Vgl. §347 I HGB; §93 I AKTG; § 43 I GmbH; § 34 I GenG.
[139] Vgl. Witt, Bernhard C. (2006), S. 4; Kersten, Heinrich; Klett Gerhard (2008), S. 126ff.
[140] Vgl. Witt, Bernhard C. (2006), S. 4f.
[141] Vgl. Witt, Bernhard C. (2006), S. 5f.
[142] Vgl. Müller, Rainer (2005), S. 404f; vgl. Witt, Bernhard C. (2008), S. 2.

(Strafvorschriften) sowie dem TKG, TDG, und vielen mehr.[143] Der Datenschutz in der Privatwirtschaft ist im dritten Abschnitt des BDSG geregelt.[144] Grundlage des Datenschutzes ist Artikel 2 des Grundgesetzes.[145] Unter Datenschutz versteht man gesetzliche und vertragliche Regelungen, die zum Schutz von personenbezogenen Daten vor unbefugtem Zugriff oder Missbrauch dienen.[146]

Strafrechtlich sind die Gesetze zum Urheberrechtsschutz, die §§ 201, 202, 203, 206, 263, 267, 268, 269, 270, 271, 274, 303, 305, 317 StGB relevant. [147] Diese Straftatbestände können nicht nur durch positives Handeln, sondern auch durch das Unterlassen von Sicherheitsmaßnahmen begangen werden.[148] Garantenstellungen können neben den oben erwähnten gesetzlichen auch aus vertraglichen Bestimmungen entstehen.[149]

Diese Aufzählung kann im Hinblick auf BIS bei der derzeitigen Rechtsentwicklung nicht vollständig sein. Teile dieser Vorschriften sind wie in Deutschland üblich abstrakt formuliert und müssen von Gerichten noch ausgelegt werden. Dies birgt für das einzelne Unternehmen bis zur Klärung der Rechtslage das Risiko, den Anforderungen nicht zu genügen.

2.4.4. Sicherheitssystematik

Aus den oben angeführten Punkten lässt sich folgende Systematik der Sicherheitsziele, dargestellt in folgender Grafik, herleiten:

---

[143] Vgl. Witt, Bernhard C. (2006), S. 9ff; 15f; 16; vgl. Dietrich von der Oelsnitz (Hrsg.); Weibler, Jürgen (Hrsg.); Gabriel, Roland; Beier, Dirk (2003), S. 195f; vgl. Kaesler, Clemens (2007), S. 107ff.

[144] Vgl. Moos, Flemming (2006), S. 40.

[145] Vgl. Kütz, Martin (2005), S. 107.

[146] Vgl. Heilmann, Wolfgang, Reusch, Günter (1984), S. 85; vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 87ff; vgl. Eckert, Claudia (2006), S. 5.

[147] Vgl. Witt, Bernhard C. (2006), S. 14; vgl. Speichert, Horst (2007), S. 241f.

[148] Vgl. Speichert, Horst (2007), S. 243.

[149] Vgl. Speichert, Horst (2007), S. 243; Kersten, Heinrich; Klett Gerhard (2008), S. 126ff.

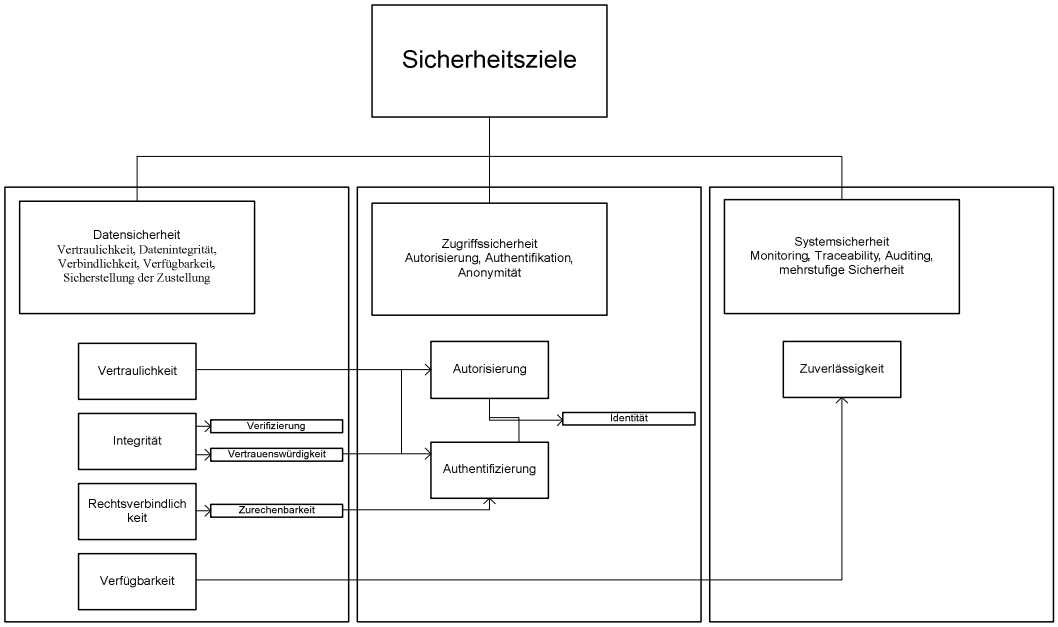

Abbildung 3: Sicherheitsziele

Unterschieden wird in Datensicherheit, Zugriffssicherheit und Systemsicherheit. Die Ausprägungen der einzelnen Ziele stehen miteinander in Verbindung, so beeinflusst die Forderung nach Vertraulichkeit die Möglichkeiten der Autorisierung ebenso wie die Rechtsverbindlichkeit über den Umweg der Authentifizierung. Die Integritätsforderung beeinträchtigt dagegen beide Bereiche der Autorisierung und Authentifizierung. Die Verfügbarkeitsforderung beeinflusst zuletzt die Zuverlässigkeit. Die jeweiligen Forderungen können wiederum wie in der Abbildung angegeben aufgespaltet werden.

2.5. Integrative Business-Intelligence-Systeme

2.5.1. Hierarchie der Informationssysteme

Nahezu alle Unternehmen nutzen für große Teilbereiche ihres Geschäftsbetriebs Informationssysteme. Im unteren Bereich der Informationssystemhierarchie sind die Administrations- und Dispositionssysteme angesiedelt. Administrationssysteme sind für Massendatenverarbeitung bei Routineaufgaben konzipiert. Sie kommen in Unternehmensbereichen wie Einkauf, Produktion oder Lager vor. Die Aufgabe von Dispositionssystemen ist es, entweder einfache und gut strukturierte Entscheidungen eigenständig zu treffen oder die Entscheidung des Aufgabenträgers vorzubereiten. Planungs- und Kontrollsysteme bilden die Spitze der Hierarchie. Sie fassen die im Unternehmen verwendeten Daten zusammen, um Informationen für Planungsentscheidungen zu generieren.

Die logische Zusammenführung der Daten der Systeme verläuft in zwei Richtungen. Bei der horizontalen Integration werden Daten einer Hierarchieebene allen Systemen zugänglich gemacht. Die zweite Dimension ist die vertikale Integration, bei der die Daten aller Ebenen zur Spitze der Hierarchie verdichtet werden. Das Ziel der Integration ist, Informationen über einzelne Geschäftsbereiche unternehmensweit verfügbar zu machen.[150] Die folgende Abbildung verdeutlicht den Zusammenhang.

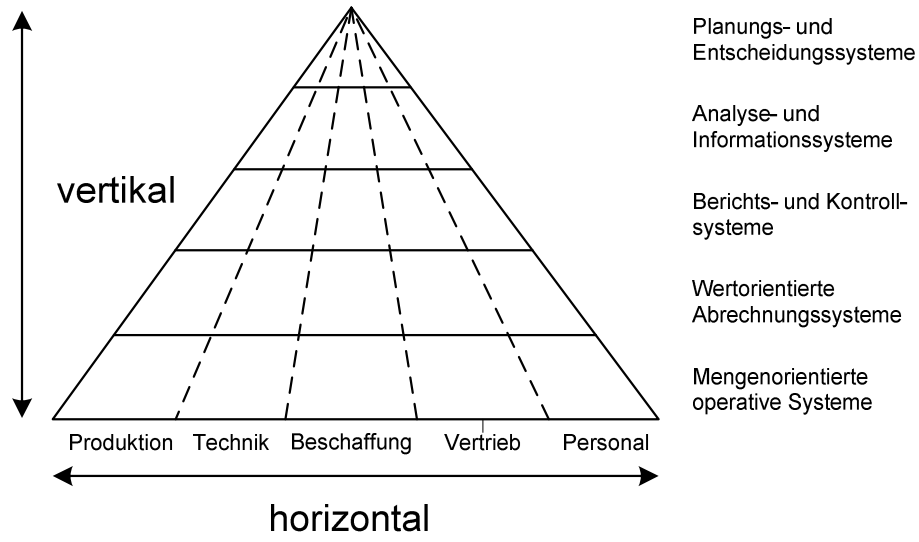

Abbildung 4: Funktionsorientierte Informationssystempyramide[151]

In der Abbildung kann der vertikale Doppelpfeil als der notwendige Informationsfluss über die verschiedenen Hierarchieebenen hinweg interpretiert werden. Der horizontale Doppelpfeil steht dabei für den Informationsfluss zwischen den einzelnen Abteilungen. Informationen können hier horizontal und vertikal ausgetauscht werden. In BIS werden diese Daten aggregiert, um Entscheidungsunterstützung zu bieten.

2.5.2. Informationssysteme

Informationssysteme können als Mensch-Aufgabe-Technik-Systeme im organisatorischen Kontext betrachtet werden. Aus Sicht der Tübinger Wirtschaftsinformatik ist der Mensch Aufgabenträger, der Aufgaben im organisatorischen Kontext

---

[150] Mertens, J.; Griese, P. (2004), S. 12; vgl. Leser, Ulf; Naumann, Felix (2007), S. 317ff.
[151] Vgl. Scheer, A.W. (1998).

der Unternehmung mithilfe der Technik löst. Um Unternehmen zu leiten, sind Entscheidungen zu treffen, welche auf Informationen beruhen. Diese können strategischer oder taktischer Art sein und sind für ein Unternehmen von großer Bedeutung. Diese Entscheidungsfindung bzw. die Aufgabenlösung zu unterstützen ist Bestandteil der Business Intelligence. Es ist dabei eine anthropozentrische Sichtweise anzunehmen, da insbesondere im Umfeld von Führungskräften der Ansatz den Menschen in den Mittelpunkt zu stellen und damit die Nutzereigenschaften mit in die Betrachtung einzubeziehen einen hohen Stellenwert besitzt. Der Gegensatz den Menschen als Aufgabenerfüller zu verwenden würde den besonderen Eigenschaften und Fähigkeiten von Führungskräften nicht gerecht werden. Die folgende Abbildung zeigt den Zusammenhang.

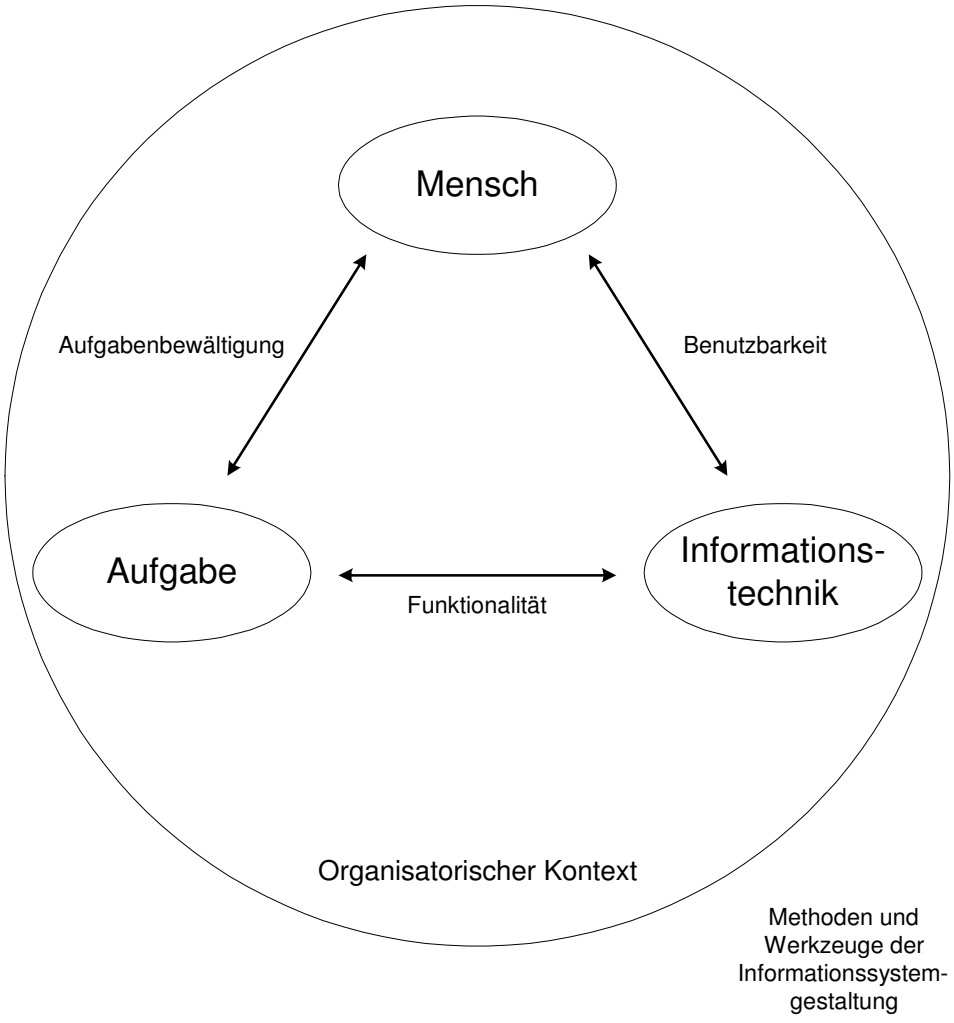

Abbildung 5: Mensch-Aufgabe-Technik im organisatorischen Kontext.[152]

[152] Jahnke, B. (WI1)

Aufgabenträger sind in diesem Modell Menschen, somit liegt die Verantwortung für die Erfüllung einer Aufgabe nur bei einer natürlichen Person. Menschen nutzen Informationssysteme zur Erfüllung von Aufgaben. Da BIS von der gesamten Informationsinfrastruktur einer Unternehmung abhängen und in diese integriert sein sollten, besteht eine Abhängigkeit zwischen Mitarbeitern und der Informationstechnologie. Beispielsweise müssen Mitarbeiter über geeignete Zugriffsberechtigungen in der Lage sein operative Daten, welche für die Aufgabe der BIS notwendig sind, im Rahmen ihrer Zuständigkeit zu bearbeiten.

In dieser Abbildung besteht zwischen Mensch und Aufgabe die Beziehung der Aufgabenbewältigung. Der Mensch soll die gestellte Aufgabe bewältigen können. Die Funktionalität ist mit der Aufgabe verbunden. Die Benutzbarkeit schließlich stellt die Verbindung des Menschen mit der Informationstechnik dar. Hier setzt die Arbeit an, da die Aufgabe nur dann bewältigt werden kann, wenn das System „benutzbar“ ist.[153]

2.5.3. Business-Intelligence-Systeme

BIS dienen der Informationsversorgung des oberen Managements. Umfassend informiert zu sein erleichtert die Entscheidungsfindung und bringt die Möglichkeit hervor, sich einen Vorteil gegenüber den Gesprächs- bzw. Verhandlungspartnern herauszuarbeiten.[154] Dies gilt allgemein und nicht nur speziell für die Führungsebene. Da aber Entscheidungen von gerade dieser Personengruppe meist von grundlegender Bedeutung für den Zustand des Unternehmens sind, wird klar, wie wichtig ein gutes, auf die Führungskraft zugeschnittenes BIS ist.

BIS „... dienen der *Informationstechnologie (Computer)gestützten*, bedarfsgerechten, individuellen und kooperativen Versorgung von Führungskräften der oberen Führungsebene mit entscheidungsrelevanten, vergangenheits-, gegenwarts- und zukunftsbezogenen Informationen. Es handelt sich um strategische Informationssysteme, die an der Spitze der Informationssystempyramide stehen.“[155] Sie stellen

---

[153] Vgl. Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2004), S. 679.
[154] Vgl. Bullinger H.-J.; Niemeier, J.; Kroll, P. (1993), S. 44f.
[155] Jahnke, B. (1993a), S. 1.

ein Zugangssystem zu anspruchsvollen Planungs- und Informationsunterstützungssystemen dar.[156]

Die entscheidungsunterstützungsrelevanten Informationen werden aus den unteren Ebenen der Informationssystempyramide und externen Quellen extrahiert. Dabei spielt die horizontale und vertikale Integration der Systeme der Informationssystempyramide die entscheidende Rolle.[157]

Vor nicht allzu langer Zeit war die Unterstützung durch BIS unbefriedigend.[158] Neue Technologien bewirken eine Rückkehr zu den damals gescheiterten Ansätzen der totalen Integration und verbessern die Möglichkeiten der Integration der einzelnen Teilsysteme erheblich. Die Anforderungen an ein BIS steigen dadurch beträchtlich. Eine Einbettung in das organisatorische Gesamtkonzept bleibt dabei hinsichtlich Wirtschaftlichkeit, Realisierbarkeit und Unterstützungspotenzial notwendig. Das Abstraktionsniveau von BIS ist zunächst sehr hoch. Es wird ein globales Modell der Entscheidungsunterstützung von Entscheidungen generiert welche wesentlich den Unternehmenserfolg beeinflussen.[159] Ganzheitliche Ansätze bieten Integrative Business-Intelligence-Systeme.[160]

2.5.4. Integrative Business-Intelligence-Systeme

Entscheidungsunterstützende Systeme haben eine lange Historie. Management Information Systems, Decision Support Systems, Executive Information Systems, Data Warehouse und Business Intelligence waren die Schlagwörter der jeweiligen vergangenen Perioden. BIS können durch die technologischen Fortschritte in der Zwischenzeit zu integrierten Informationssystemen[161]erweitert werden. Der Begriff integrative BIS steht als Ausdruck für die Möglichkeiten eines ganzheitlichen Informationssystems, innerhalb des ganzheitlichen Informationsmanagements.[162]

---

[156] Jahnke, B. (1993a). S. 9.
[157] Jahnke, B. (1993a). S.8.
[158] Jahnke, B. (1993a), S. 3; vgl. Biethan, Jörg; Muksch, Harry; Ruf, Walter (2007), S. 1f.
[159] Vgl. Hahn (1985) S. 25 f; vgl. Jahnke, B. (1993a), S. 3.
[160] Vgl. Biethan, Jörg; Muksch, Harry; Ruf, Walter (2007), S. 1.
[161] Vgl. Leser, Ulf; Naumann, Felix (2007), S. 3.
[162] Vgl. Biethan, Jörg; Muksch, Harry; Ruf, Walter (2004), S. 10.

Die folgende Abbildung zeigt die historische Entwicklung der BIS.

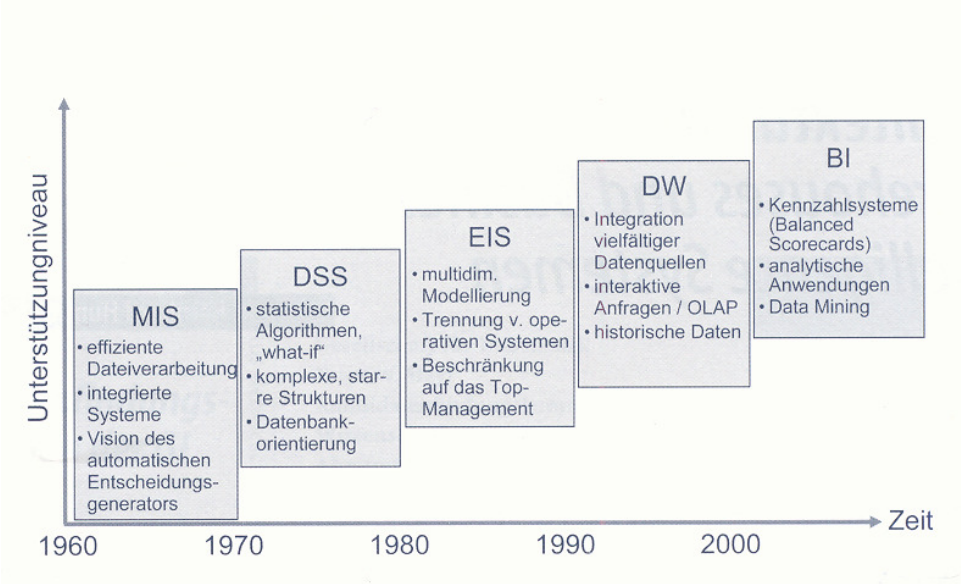

Abbildung 6: Historische Entwicklung von Business-Intelligence-Systemen.[163]

Der folgende Abschnitt erläutert, welche Technologie nötig ist, um die Anforderungen von integrativen BIS erfüllen zu können. Die Daten werden dabei entweder im Data Warehouse oder aber von dort ausgehend in einer eigenen Datenbank für OLAP optimiert abgelegt.[164] Für den Begriff Data Warehouse existieren unterschiedliche Definitionen. Ziel des Data Warehouse[165] ist es, eine zentrale, konsistente Datenbasis zu reinen Analysezwecken zu pflegen, die von den operativen Systemen und externen Quellen zwar gespeist wird, jedoch unabhängig von ihnen existiert.[166] Meist ist das Data Warehouse eine Datenbank, in der alle Daten aus den verschiedensten unternehmensinternen und -externen Bereichen eines Unternehmens liegen (dispositive Daten).[167]

OLAP hilft dem Benutzer online, d.h. interaktiv durch die gesamten Datenbestände des Unternehmens zu navigieren und dabei nahezu beliebig ins Detail zu gehen.[168] Der Benutzer kann auf Methoden der Statistik zurückgreifen und typische

---

[163] Humm, B.; Wietek, F. (2005), S. 4; vgl. Achatzi, Günter (1991), S. 84, vgl. Chamoni, Peter; Gluchowski, Peter (2006), S. 9.
[164] Vgl. Hahne, Michael (1999), S. 146; vgl. Reinke, Schuster (2000), S. 55f.
[165] Vgl. Chamoni, Peter; Gluchowski, Peter (1999), S. 13; Mucksch, Harry (2000), S. 13.
[166] Vgl. Kemper, Hans-Georg; Finger, Ralf (1999), S. 186.
[167] Vgl. Reinke, Schuster (2000), S. 28; Meyer, Markus; Winter, Robert (2000), S. 311.
[168] Vgl. Chamoni, Peter; Gluchowski, Peter (2000), S. 343.

Analysen, wie „Was-wäre-wenn-Fragestellungen“[169] durchführen und das, ohne eine Programmiersprache beherrschen zu müssen, wie das bei Abfragen gegen operative Datenbanken von Nöten wäre. Kennzahlen können erforscht werden indem bestimmte Dimensionen durch Drill-Down oder Roll-Up fein- oder grobgranularer dargestellt werden, um entweder die Details besser erkennen zu können oder den Überblick zu bewahren. So kann beim Analysieren von Verkaufszahlen durch das Verfeinern der Zeitachse von Monaten auf Tage unter Umständen festgestellt werden, dass ein bestimmtes Produkt zwar auf Monatsebene konstant verkauft wird, jedoch an bestimmten Wochentagen besonders gut oder schlecht abgesetzt wird.

Drill-Down und Roll-Up bedeuten die schrittweise Verfeinerung bzw. Verdichtung (Aggregation) von Analyseergebnissen.

Durch Slicing werden Scheiben aus einem Datenwürfel herausgeschnitten. So kann man bei Verkaufszahlen, die in Abhängigkeit von Verkaufsort, der Zeit und des verkauften Produkts gegeben sind, durch Slicing beispielsweise nur Verkäufe des letzten Quartals herausschneiden und die so entstandenen zweidimensionalen Kennzahlen in ein Tabellenkalkulationsprogramm importieren. Slice-and-Dice: Navigation in einem multidimensionalen Datenraum durch Fokussierung auf einzelne Aspekte.

Dicing nennt sich die Technik, aus einem Datenwürfel einen für den Betrachter relevanten Teilwürfel zur genaueren Betrachtung und um Ressourcen zu sparen herauszunehmen.[170] Pivoting erlaubt es, die Dimensionen einer zweidimensionalen Tabelle zu vertauschen.[171] Drill-Through: Direkter Zugriff aus analytischen Systemen auf operative Basisdaten. Definierte Standardberichte, Kennzahlenorientierung (Measures), Online Analytical Processing (OLAP), Data Mining, Collaboration, Business Performance, Forecasting/Simulation, Budgeting/Planning, Security sind weitere Anforderungen und Möglichkeiten des BIS.

Die genannten Möglichkeiten verbessern die Entscheidungsqualität der Aufgabenträger und tragen einen wesentlichen Teil zur Gewinnmaximierung bei. Ökono-

---

[169] Kurz (1999), S. 313.
[170] Vgl. Holthuis, Jan (2000), S157; vgl. Müller, Jochen (2000), S. 94.
[171] Vgl. Alpar, Paul (2000), S. 19.

misch sind diese Anforderungen an ein BIS damit relevant. Die Referenzarchitektur eines BIS sieht wie folgt aus:

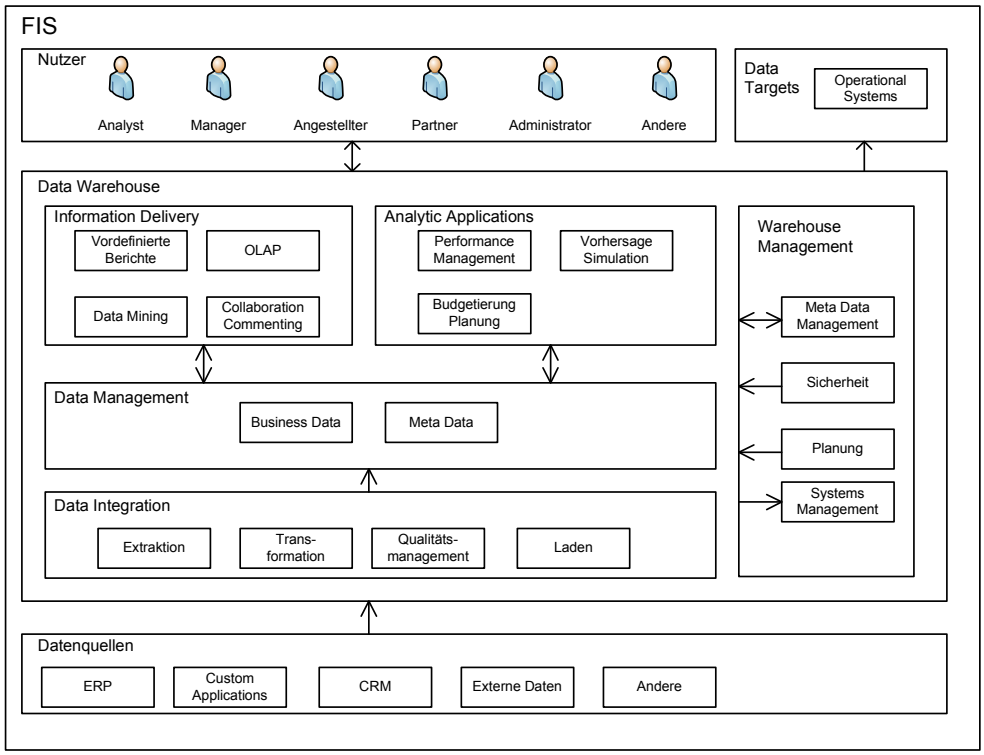

Abbildung 7: Referenzarchitektur BIS[172]

Die Abbildung unterteilt sich grob in Nutzer, Data Warehouse, Warehousemanagement und Datenquellen. Eine Sicherheitsarchitektur ist nicht ersichtlich.

Folgende kritische Erfolgsfaktoren für den Einsatz eines BIS konnten identifiziert werden:

Unterstützung der Planung, der Kommunikation, der Informationstätigkeit, Willensbildung und Willensdurchsetzung, Zielbildungsphase, Problemstellungsphase, Suchphase, Beurteilungsphase, Entscheidungsphase, Realisierungsphase, Kontrollphase, strategische Ausrichtung, Kooperation, Integration und Flexibilität.[173]

Sie dienen Führungskräften der oberen Führungsebene zur Entscheidungsunterstützung und im Idealfall zur selbstständigen Entscheidung von betriebswirtschaftlichen strategischen beziehungsweise operativen Entscheidungen. Sie aggregieren die Daten, Informationen und eventuell Wissen der an sie angebundenen

---

[172] Vgl. Cognos AG

[173] Vgl. Jahnke, B. (1993a), S. 6, S.12.

Informationssysteme. BIS müssen sich durch die genannten Punkte in die Informationsinfrastruktur des Unternehmens einfügen. Diese bezieht sich nicht nur auf die interne Sicht sondern auch auf die externen Schnittstellen.

Da von den unterstützten beziehungsweise getroffenen Entscheidungen des BIS der Unternehmenserfolg per Definition/Anspruch abhängt, ergibt sich eine besondere Problemstellung, die sich einerseits in der Person des Nutzers (Führungskraft) und andererseits in der „Security" der gesamten Infrastruktur manifestiert.

2.5.5. Business Intelligence

Der Begriff Business Intelligence (BI) hat sich in den letzten Jahren fest in der „IT-Branche" etabliert.[174] Unter diesem Label versuchen Anbieter von Softwareprodukten ihre BIS-Lösungen schneller zu vermarkten,[175] sodass die Gefahr einer Verwässerung dieses Begriffsverständnisses entstehen kann.[176]

Auf den ersten Blick scheint sich der BI-Begriff einer handfesten Definition entziehen zu wollen, weshalb eine Einordnung und Abgrenzung nicht trivial erscheint, zumal auch jede Definition angreifbar bleibt.[177] In der Literatur wird der BI-Begriff häufig als begriffliche Klammer bezeichnet, die eine Vielzahl unterschiedlicher Ansätze zur Analyse geschäftsrelevanter Daten zu bündeln versucht.[178] Primär soll BI Entscheidungsträger auf unterschiedlichen Ebenen mit präzisen Informationen versorgen, einen entscheidungsunterstützenden Charakter haben, die angeforderten Informationen schnell und gut aufbereiten und zum richtigen Zeitpunkt in der geeigneten (in einer gebrauchstauglichen)[179] Form zur Verfügung gestellt werden.

BI ist keine feste Bestandsgröße sondern vielmehr eine fortführende Prozessfolge,[180] die der Frühwarnung, der Unterstützung des Entscheidungsprozesses, der Konkurrenzbewertung und Beobachtung dient und dem Entscheidungsträger bei

---

[174] Vgl. Gluchowski, P. (2001), S. 5.
[175] Vgl. Gabriel, R. (2001), S. 23.
[176] Vgl. Gluchowski, P. (2001), S. 6.
[177] Vgl. Gluchowski, P. (2001), S. 5.
[178] Vgl. Gluchowski, P. (2001), S. 5.
[179] ISO-Norm 9241-11, International Standardisation Organisation 1996; vgl. Ertel, Wolfgang (2001), S. 159f.
[180] Vgl. Grothe, M.; Gentsch, P.; (2000), S. 19.

der Strategieplanung und Entwicklung helfen soll.[181] Begünstigt wird das prozessorientierte[182] oder prozessfokussierte[183] BI-Verständnis durch die Tatsache, dass in Unternehmungen häufig bestimmte Lösungen nach und nach erarbeitet werden und sich die ökonomischen und technischen Rahmenbedingungen im Zeitablauf ändern.[184]

Der Begriff Business Intelligence (BI) wurde Anfang der 1990er Jahre von der Gartner Group geprägt.[185] Ansatzpunkt für die Business Intelligence waren die Resultate, die aus dem statischen Berichtswesen von OLTP-Systemen generiert wurden und eher strukturlosen Datenbergen glichen als informativen Berichten.[186] In diesen Systemen wurden Daten „funktions- bzw. prozessorientiert mit dem Ziel einer effizienten Unterstützung bei der Abwicklung des Tagesgeschäfts gespeichert“[187].

Es entstand die Situation eines Informationsdefizits bei steigender Datenflut.[188] Daraus kam die Forderung nach einer funktionsübergreifenden themenorientierten Strukturierung der Unternehmensdaten auf, die eine Analyse erlaubte, um Beziehungen und Zusammenhänge zwischen den verschiedenen Daten verteilter Systeme zu erkennen. Dafür ist der Aufbau einer inhaltlich konsistenten und integrierten Datenbasis erforderlich.[189] Diesen Forderungen versucht die Business Intelligence durch die Selektion, Transformation und Speicherung von Daten, durch die Deutung und Herstellung von Beziehungen sowie Sinnzusammenhängen und letztlich durch die Diffusion der gewonnenen Informationen gerecht zu werden.

Intelligence kann dabei im Sinne von „Verständnis, Einsicht und Suche“[190] oder „Aufklärung“[191] verstanden werden. Je nach Verständnis wird ein anderer Ausgangspunkt gewählt und nach technischem Grad der Werkzeuge differenziert.

---

[181] Vgl. Henning M.; (2003), S. 57.
[182] Vgl. Weber, J.; Grothe, M.; Schäffer, U. (1999), S. 16-17.; Grothe, M.; Gentsch, P.; (2000), .S. 11; McLeod, R.; Schell, G. (2001), S. 45.
[183] Vgl. Gluchowski, P. (2001), S. 7.
[184] Vgl. Groffmann, Hans Dieter (1993), S. 41.
[185] Vgl. Knobloch, Bernd in Maur, E., & Winter, R. (Eds.) (2002), S. 11.
[186] Vgl. Preuschoff, Sarah (2002), S. 6.
[187] Dittmar, Carsten (2004), S. 315.
[188] Vgl. Behme, Wolfgang; Mucksch, Harry (2001), S. 9.
[189] Vgl. Dittmar, Carsten (2004), S. 315.
[190] Preuschoff, Sarah (2002), S. 7.
[191] Knobloch, Bernd in Maur, E., & Winter, R. (Eds.) (2002), S. 11.

Ziel der Business Intelligence ist es, mithilfe verschiedener Instrumente (Führungsinstrumente) und Werkzeuge das Zusammenspiel zwischen Mensch und Informationstechnologie zu ermöglichen, um aus der bestehenden Informationsfülle prägnante Relationen und Muster zu entdecken und zielgerichtet zu nutzen. Das Ergebnis soll Entscheidungsträgern relevante Informationen zur Verfügung stellen.[192] Für die Business Intelligence kommen im Folgenden also entscheidungsunterstützende Werkzeuge in Betracht, die der Datenhaltung und Datenaufbereitung dienen, analytische Werkzeuge der Muster und Zusammenhangsidentifikation sowie der Informationsaufbereitung und Darstellung.

Ein weiterer Definitionsansatz versteht unter Business Intelligence „den analytischen Prozess, der - fragmentierte - Unternehmens- und Wettbewerbsdaten in handlungsgerechtes Wissen über Fakten, Fähigkeiten, Positionen und Ziele der betrachteten internen und externen Handlungsfelder (Akteure und Prozesse) transformiert."[193] Daraus werden die drei Prozessphasen Bereitstellung, Analyse und Publikation abgeleitet:[194]

1. Bereitstellung quantitativer und qualitativer, strukturierter und unstrukturierter Rohdaten.

2. Entdeckung von relevanten Zusammenhängen und Mustern anhand vorbestimmter Hypothesen oder hypothesenfrei.

3. Kommunikation der gewonnenen Erkenntnisse im Unternehmen zur Unterstützung von Maßnahmen und Entscheidungen.

Es sollen durch die Prozessphasen „… allgemein verwendbare, effiziente Methoden gefunden werden, die autonom aus großen Rohdatenmengen die bedeutsamsten und aussagekräftigsten Muster identifizieren und sie dem Anwender als interessantes Wissen präsentieren"[195]. Betont wird der Integrationsbeitrag, den die BI durch das Zusammenführen fragmentierter Informationen zu leisten vermag.[196]

---

[192] Vgl. Grothe, M.; Gentsch, P. (2000), S. 17ff; vgl. Jäger-Goy, Heidi (2002); S. 24ff.
[193] Fank, Matthias (1985/2002); Fernholz, M.; Buresch, A. in Krcmar, H.; Buresch, A., & Reb, M. (Eds.), S. 9.
[194] Vgl. Fank, Matthias (1985/2002) Fernholz, M.; Buresch, A. in Krcmar, H.; Buresch, A., & Reb, M. (Eds.), S. 9.
[195] Bissanz, Nicolas; Hagedorn, Jürgen; Mertens, Peter (1998), S. 447f.
[196] Für eine Übersicht s. Knobloch, Bernd in Maur, E., & Winter, R. (Eds.) (2002), S. 11f.

Die Business Intelligence Lösung sollte im Unternehmen als Prozess gestaltet werden, um Kontinuität zu gewährleisten. Durch permanente aktive Informationsgenerierung soll die BI bei Wettbewerbsanalyse, Früherkennungssystem und Strategieformulierung unterstützen[197].

2.5.6. Technologie

In den verteilten operativen Systemen eines Unternehmens befinden sich zumeist strukturierte quantitative Daten, auf denen analytische Prozesse aus Performancegründen nicht gestartet werden können. Diese Systeme sind für die Bearbeitung großer Transaktionsmengen konzipiert, nicht aber für Analyseaufgaben. Darüber hinaus findet man in Unternehmen unstrukturierte, qualitative Daten. Diese befinden sich vornehmlich im Intranet, den unteren Systemen der Informationssystempyramide und diversen Dokumentenmanagementsystemen.

In der Prozessphase der Datenaufbereitung und Bereitstellung soll der Informationsarmut begegnet werden, indem eine inhaltlich konsistente Datenbasis, redundant neben den Beständen der operativen Systeme aufgebaut wird, um einer Vielzahl heterogener Benutzer performanten Zugriff mittels themenbezogener Analysewerkzeuge zu ermöglichen. Dazu sind Schnittstellen zu den operativen Systemen notwendig, welche durch Sicherheitsmaßnahmen abgesichert werden müssen.

Ziel ist es, nicht alle Daten zu übernehmen sondern nur die im Sinne der Thematisierung relevanten.[198] In dieser Prozessphase bietet sich der Aufbau eines Data Warehouse (DW) an, um die verteilten internen wie externen Datenquellen auszuwerten und gegebenenfalls im DW zu speichern.[199] Das DW ist ein vom BIS unabhängiger Baustein. Es kann als Datenquelle angesehen werden. Die Schnittstellen zwischen den operativen Systemen und den DWs sind dementsprechend abzusichern.

Abhängig von der Thematisierung wird die Relevanz der selektierten Daten durch Filter- und Hygieneprogramme sichergestellt und Redundanzen vermieden. Der komplexe Prozess der Extraktion, Transformation und des Ladens (ETL) beinhaltet auch die Aufbereitung durch Umordnung und Verdichtung der Daten. So ent-

---

[197] Vgl. Preuschoff, Sarah (2002), S. 10.
[198] Vgl. Dittmar, Carsten (2004), S. 315.
[199] Vgl. Lusti, Markus (2002), S. 129ff.

steht eine homogene, konsistente, von Fehlern bereinigte Datenbasis, die eine Informationsgenerierung durch BI-Werkzeuge erst möglich macht.

In dieser Prozessphase lässt sich vieles automatisieren. Ein DW ist ein sehr komplexes, schwer zu etablierendes System, weshalb man sich oft mit Data Marts begnügt. Diese beinhalten nur die Daten für eine bestimmte Aufgabe, z. B. das Controlling. Der Datenumfang ist somit geringer als beim gesamten DW. "In großen DW-Umgebungen stoßen einfache Abfrage-Werkzeuge für den Datenzugriff schnell an die Grenzen ihrer Leistungsfähigkeit"[200], insbesondere wenn es sich um komplexe analytische Abfragen handelt, die für die Gewinnung betriebswirtschaftlicher Kennzahlen erforderlich sind.[201]

Um diese ad hoc performant abrufen zu können, bietet sich eine multidimensionale Datenhaltungstechnologie wie beispielsweise OLAP an.[202] Der OLAP-Ansatz beinhaltet einerseits einen „anwendungsorientierten Gestaltungsrahmen zur multidimensionalen Modellierung von Daten"[203] als auch „ein analytisches Werkzeug, das dem Benutzer schnelle und interaktive Zugriffe auf einen multidimensionalen Datenbestand ermöglicht"[204]. Es wird zwischen der physischen mehrdimensionalen Datenhaltung (Multidimensionales-OLAP) und der virtuellen mehrdimensionalen Datenhaltung (Relationales-OLAP) unterschieden.[205]

In der Prozessphase der Datenanalyse unterscheidet man zwischen der hypothesengestützten und hypothesenfreien Entdeckung. Stellt der Anwender eine Hypothese auf, gilt es diese mittels geeigneter Analysewerkzeuge zu verifizieren oder zu falsifizieren. Hat der Anwender keine Vermutung über mögliche Zusammenhänge, ist eine Hypothese aufzustellen, welche durch geeignete Verfahren unterstützt werden kann. Mögliche Verfahren sind beispielsweise das Data Mining oder Text Mining.[206]

Strukturierte quantitative Daten (hard facts) werden mit Data Mining auf Dependenzen und Interdependenzen mit dem Ziel der Klassifikation oder Prognose bzw.

---

[200] [Konetzny, Michael; http://www.mkonetzny.de].
[201] Vgl. Jahnke, B. (1996), S. 4.
[202] Vgl. Kerner, Simone (2002), S. 132ff.
[203] Kerner, Simone (2002), S. 133f.
[204] Kerner, Simone (2002), S. 133f.
[205] Vgl. Jänig, Christian (2004), S. 210f.
[206] Vgl. Chamoni, Peter; Gluchowski, Peter (2006), S. 16ff.

des Clusterings oder der Assoziation untersucht.[207] Unstrukturierte Daten (soft facts) wie Textdokumente werden durch Text Mining auf relevante Zusammenhänge geprüft. Der Text soll nicht verstanden, sondern analysiert werden. Dieses Verfahren wird fast ausschließlich für externe Datenquellen, wie beispielsweise über das Internet zugängliche Datenbanken und Pressemitteilungen benutzt.

In der Prozessphase der Publikation sollen die neu generierten Informationen verbreitet werden. Die Diffusion von Informationen gehört ebenfalls zum Aufgabenbereich des Wissensmanagements. Die Definition des Wissensmanagements ist in der Literatur noch nicht vollständig abgeschlossen, jedoch können die zentralen Aufgaben wie folgt extrahiert werden, als Generierung von Wissen aus verfügbaren Quellen, die Strukturierung, Aufbereitung und Speicherung des generierten Wissens sowie die bedarfsgerechte Bereitstellung des Wissens.

Die BI liefert nach diesem Verständnis des Wissensmanagements technische Werkzeuge zur Datenauswertung, um relevantes Wissen zu generieren. Die Nutzung und Diffusion der gewonnenen Erkenntnisse stehen im Mittelpunkt der Konzepte des Wissensmanagements. BI wäre eine Konkretisierung von Methoden des Wissensmanagements.

Eine Abgrenzung der Aufgabenbereiche von Wissensmanagement und der Business Intelligence kann an dieser Stelle nicht erfolgen. Entscheidend ist, dass die Möglichkeit einer übersichtlichen, leicht zugänglichen Präsentation der neu entstandenen Informationen geschaffen wird, damit einem Aufgabenträger zu Wissen verholfen werden kann. Zur Interaktion und Visualisierung der Ergebnisse stehen leistungsfähige, grafische Front-end-Werkzeuge zur Verfügung, die den Anwender bei seiner Aufgabenbewältigung unterstützen. Beim Entwurf dieser Werkzeuge sind die Anforderungen an eine adäquate Benutzerschnittstelle zu beachten. Diese Aussage begründet eine Untersuchung der Auswirkungen von Sicherheitsmaßnahmen auf die Usability.

2.5.7. Datenquellen

Um Fach- und Führungskräfte bei der Entscheidungsfindung unterstützen zu können, wird eine Vielzahl verschiedenster, qualitativ hochwertiger Daten benötigt.[208]

---

[207] Für eine Übersicht vgl. Kerner, Simone (2002), S. 138ff., Bensberg, Frank (2001), S. 114ff.
[208] Vgl. Sprague, Ralph H. Jr.; Watson, Hugh J (1995), S. 54.

Da heutzutage in jedem Unternehmen große Datenmengen entstehen und gespeichert werden, herrscht kein Mangel an Datenquellen. [209]

Dafür ist es notwendig, dass die entscheidungsrelevanten Daten in quantifizierter Form vorliegen, da sie sonst kaum mit Hilfe von Informationstechnologie weiterverarbeitet werden können. Somit scheiden bisher Daten aus, die in Textform (Arbeitsberichte, Schadensmeldung oder Memo), grafisch (Diagramme oder Fotografien) oder audiell (Mitschnitt einer Besprechung, Musik) vorliegen. Die Bestrebung ist, alle Daten, die in den verschiedenen Systemen eines Unternehmens verwaltet werden zu verarbeiten. Es sollen quantifizierbare und qualitative Informationen zu Führungsinformationen verarbeitet werden.

In den letzten Jahren hat sich das Data Warehouse als Konzept der zentralen Datenspeicherung für Informationssysteme durchgesetzt. Hauptlieferanten an entscheidungsrelevanten Daten sind vor allem das interne und externe Rechnungswesen, aber auch Daten, die außerhalb des Unternehmens erhoben werden. Diese sind zum Teil Kennzahlen, welche als Zahlen definiert sind, die quantitativ erfassbare Sachverhalte in konzentrierter Form erfassen.[210] Mit diesen Werten soll der Unternehmensführung sowohl vergangenheits- und gegenwartsbezogene Auswertungen als auch verlässliche Prognosen ermöglicht werden.[211] Die genannten Datenquellen sind Teil der Infrastruktur eines Unternehmens. Sie sind somit in die Gesamtbetrachtung mit einzubeziehen.

Die entscheidungsrelevanten Daten für die Unternehmensführung können entweder im Unternehmen selbst anfallen, aus den Geschäftsbereichen von Mitbewerbern oder aus allgemein verfügbaren Daten von Forschungsinstituten stammen. Dabei wird zwischen unternehmensinternen und -externen Daten unterschieden.[212] Die wichtigsten internen Daten liefert wie oben angeführt das Rechnungswesen. Das interne Rechnungswesen erfasst alle Daten, die innerhalb des Unternehmens zwischen einzelnen Arbeitsbereichen anfallen. Zu ihnen zählen Größen der Kostenrechnung (Verrechnungspreise zwischen Abteilungen und Vor- und Endprodukten) und der Investitionsrechnung (z. B. Rentabilitätskennziffern).

---

[209] Vgl. Kurz (1999), S. 312f.
[210] Vgl. Reichmann, Laurenz; Lachnit, Thomas (1976), S. 706.
[211] Vgl. Jahnke, B. (1991), S. 42.
[212] Vgl. Reichmann, Thomas (2001), S. 11.

Das externe Rechnungswesen ermittelt gemäß geltendem Recht (HGB, StGB) den Jahresabschluss, der Anteilseignern Informationen über die finanzielle Situation geben soll und die Bemessungsgrundlage für Steuern bildet. Dieser beinhaltet Größen, die den Erfolg des Unternehmens erkennen lassen (Gewinn-und-Verlust-Rechnung) und stellt die finanzielle Situation dar (Struktur der Aktiva und Passiva, Schulden, Forderungen, etc.). Die genannten Positionen finden sich in der Unternehmensinfrastruktur wieder.

Daten aus externen Quellen werden nicht im Unternehmen selbst erhoben. Sie sind meist allgemein verfügbare Informationen, die für das Unternehmen als Referenzwert (Benchmark) dienen können. Allgemein verfügbar bedeutet, dass diese erworben werden können. Die Daten können aus Jahresabschlussinformationen von Mitbewerbern, Berichten des Statistischen Bundesamtes, Finanzberichten der Bundesbank oder Europäischen Zentralbank, Fachzeitschriften, kostenpflichtigen und freien Datenbanken oder dem Internet[213] sowie anderen Wegen gewonnen werden. Da sich diese Daten in einer externen Infrastruktur befinden müssen sie über eine geschützte Schnittstelle mit den intern erarbeiten Informationen verknüpft werden.

Ein weiteres Unterscheidungskriterium für Datenquellen ist der Grund der Entstehung der Daten. Sind Daten bereits vorhanden, weil sie zuvor für andere Zwecke erhoben wurden (z. B. Personaldaten der Mitarbeiter, Jahresabschlüsse anderer Unternehmen), spricht man von Sekundärquellen. Reichen diese Informationen allein für die Entscheidungsunterstützung in einem BIS jedoch nicht aus, müssen Daten speziell für den Zweck der Informationserstellung erhoben werden. Möglichkeiten der Datengewinnung sind Labor- und Feldexperimente, Befragungen und Beobachtungen. Diese werden dann als Primärquellen bezeichnet. Da eine solche Erhebung in der Regel mit sehr hohen Kosten verbunden ist, muss sehr genau abgewogen werden, in welchem Verhältnis der finanzielle Aufwand zu dem zu erwartenden informatorischen Nutzen steht. [214]

---

[213] Vgl. Hannig, Uwe (2002), S. 221.
[214] Vgl. Staudt, Erich (1985), S. 70f.; Groffmann, Hans-Dieter (1992), S. 7.

2.5.8. Datengewinnung/Informationsgewinnung

Um die Daten auswerten zu können, ist ein vielschichtiger Prozess notwendig, da sie im Unternehmen und außerhalb in vielfältiger Form vorliegen.[215] Der Veredelungsprozess von Rohdaten zu entscheidungsrelevanten Daten findet meist in zwei Stufen statt[216]. Zunächst werden die Daten aus den operativen Systemen transformiert, betriebswirtschaftlich aufbereitet und in ein Data Warehouse überführt. Dann werden sie von dort in applikationsspezifischen Datenbanken abgelegt und dienen den Auswertungsprogrammen als Datenbasis. Dieser Prozess kann auch innerhalb des BIS stattfinden. Der aufwendigste Teil bei der Erstellung eines Data Warehouse ist das Überführen der Daten aus der operativen in die dispositive Datenbasis. Hierfür wird oft ein Zeitaufwand von 80% der Aufbauphase genannt.[217]

Alternativ besteht die Möglichkeit ein virtuelles Data Warehouse zu nutzen, dass die für die Analyse benötigten Daten durch lesenden Zugriff auf die operativen Systeme bezieht.[218] Nachteilig an dieser Lösung sind die schlechten Abfragezeiten (Performance), die dem FASMI-Prinzip widersprechen und die Belastung der operativen Systeme, die bereits durch den regulären Betrieb stark ausgelastet sind.[219] Zudem sind die benötigten Daten oft auf mehrere Datenbanken verteilt[220] in denen nicht die Möglichkeit besteht aggregierte Daten zu speichern. Diese Nachteile treten bei einer zentralen, redundanten Datenhaltung nicht auf. [221]

Ein Data Mart kann als Data Warehouse für einen Teilbereich eines Unternehmens verstanden werden.[222] Es kann entweder zur Performanzsteigerung parallel zu einem zentralen Data Warehouse oder als Datenlager für eine Abteilung des Unternehmens betrieben werden und somit als kostengünstige Variante verstanden werden.[223]

---

[215] Vgl. Kemper, Hans-Georg; Finger, Ralf (1999), S. 79.
[216] Vgl. Kemper, Hans-Georg; Finger, Ralf (1999), S. 185; Behme, Wolfgang; Mucksch, Harry (2001), S. 19f.
[217] Vgl. Schinzer, Heiko; Bange, Carsten (1999), S. 52.
[218] Vgl. Schinzer, Heiko; Bange, Carsten (1999), S. 50f.
[219] Vgl. Mucksch, Harry; Behme, Wolfgang (2000), S. 55.
[220] Vgl. Jahnke, B. (1996), S. 1.
[221] Vgl. Schinzer, Heiko; Bange, Carsten (1999), S. 51.
[222] Vgl. Schinzer, Heiko; Bange, Carsten (1999), S. 52.
[223] Vgl. Müller, Jochen (2000), S. 114.

OLAP steht für On-Line Analytical Processing und wurde Anfang der Neunziger Jahre hauptsächlich von Edgar Frank Codd entwickelt. OLAP ist ein Datenanalysekonzept für historische, aggregierte Unternehmensdaten, das insbesondere auch der Entscheidungsunterstützung dient[224] und somit im Gegensatz zur Transaktionsverarbeitung der operativen Systeme (OLTP) steht. Wie auch für relationale Datenbanken stellte Codd zwölf Regeln für OLAP-Systeme auf.[225] Das Akronym FASMI bedeutet in diesem Zusammenhang Fast Analysis of Shared, Multidimensional Information und beschreibt die Anforderungen an ein OLAP-System ohne konkrete Implementierungsdetails vorzuschreiben.[226]

Die erste Forderung ist Schnelligkeit (Fast) und es wird ganz konkret verlangt, dass selbst eine komplexe Abfrage nicht länger als 20 Sekunden dauern darf. Durchschnittlich soll der Benutzer maximal fünf Sekunden auf sein Ergebnis warten müssen, damit sein Gedankenfluss nicht unterbrochen wird. Statistische Analysen und das Abfragen von Kennzahlenreihen werden dem zweiten Punkt nach verlangt (Analysis). Das soll auch Benutzern ohne Programmierkenntnisse möglich sein. [227]

Die Datenbank soll einen Mehrbenutzerbetrieb (Shared) ermöglichen und insbesondere mit konkurrierenden Schreibzugriffen umgehen können. Zudem wird gefordert, dass OLAP mit multidimensionalen Daten (Multidimensional) arbeitet. Da betriebliche Kennzahlen meist von vielen Parametern abhängen, eignet sich eine OLAP-Datenbank besser dafür, als andere Modelle. Auch soll der Benutzer all diejenigen Informationen zur Verfügung haben, die er für seine Analysen benötigt.

2.6. Usability

Unter dem Begriff Usability subsumiert man allgemein die Nutzbarkeit, Benutzerfreundlichkeit beziehungsweise die Gebrauchstauglichkeit eines Informationssystems.[228] Die Ermittlung der Gebrauchstauglichkeit erfolgt in Abhängigkeit von

---

[224] Vgl. Jahnke, B. (1996), S. 1.
[225] Vgl. Codd, Frank Edgar (1993), S. 5.
[226] Vgl. [Pendse, Nigel; Chreeth, Richard; (1995); http://www.busintel.com].
[227] Vgl. Chamoni, Peter; Gluchowski, Peter (1999), S. 267.
[228] Vgl. Beier, M.; von Gizycki, V. (2002), S. 1.

Nutzungskontext und verfolgten Zielen der Nutzer.[229] Die im Umfeld der BIS relevanten Nutzer sind Führungskräfte. Die Anforderungen an BIS betreffend die Usability ergeben sich aus den Anforderungen an Informationssysteme im Allgemeinen, den Spezifika der IT-Sicherheit sowie der Führungskräfte. Der Zweck einer Usabiltybetrachtung ist nicht die Einfachheit des Gebrauchs sondern die Verminderung des Aufwandes ein gegebenes Ziel zu erreichen.[230]

„Ein IT-Sicherheitssystem benötigt die Akzeptanz seiner Benutzer." (Ergonomiebetrachtung).[231] Eine wissenschaftliche Definition der Usability ist durch die zahlreichen Subsumtionen der Vergangenheit nicht einfach zu finden. Zeitweise wurde der Begriff im deutschen Sprachgebrauch mit Softwareergonomie gleichgesetzt.[232] Ein Versuch der Definition, welcher auf Effektivität und Effizienz sowie das Ausmaß der Zufriedenheit abzielt ist in der ISO 9241-11 zu finden.[233]

Die Usability ist eng verbunden mit der Ergonomie. Die Software-Ergonomie befasst sich mit der Anpassung an die kognitiven und physischen Fähigkeiten bzw. Eigenschaften des Menschen, also seine Möglichkeiten zur Verarbeitung von Informationen (z. B. Komplexität) aber auch softwaregesteuerten Merkmalen der Darstellung (z. B. Farben und Schriftgrößen). Ziel ist die Berücksichtigung des Menschen und seiner Aufgaben und Fähigkeiten sowie die Anpassung des Werkzeuges (sei es Software oder jedes andere Werkzeug) an diese.

Die Ermittlung der Usability erfolgt in Abhängigkeit von Nutzungskontext und verfolgten Zielen der Nutzer. Die Usability bezeichnet das Ausmaß, in dem ein Informationssystem durch bestimmte Benutzer (Führungskräfte) in einem bestimmten Anwendungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen. Sie bildet die standardisierte Grundlage für die Analyse und Interpretation der gesamten Nutzungserfahrung.[234]

Die Barrierefreiheit beschreibt die Nutzbarkeit für den Nutzungskontext, bei dem die Nutzer bestimmte Fähigkeiten nicht hat und deshalb bestimmte Interaktions-

---

[229] Vgl. Sarodnick, Florian; Brau, Henning (2006), S. 25; vgl. DIN EN ISO 9241-11 (1998); S. 5.
[230] Vgl. Stapelkamp, Torsten (2007), S. 514ff.
[231] Pohlmann, Norbert (2004), S. 84.
[232] Vgl. Manhartsberger, Martina; Musil, Sabine (2001), S. 40; vgl. DIN EN ISO 9241-11 (1998); S. 5
[233] Vgl. Manhartsberger, Martina; Musil, Sabine (2001), S. 38.
[234] Vgl. Sarodnick, Florian; Brau, Henning (2006), S. 25; vgl. DIN EN ISO 9241-11 (1998); S. 5.

formen nicht, oder nur sehr eingeschränkt nutzen kann, es handelt sich um eine spezielle Sicht auf die Usability. Die Mensch-Computer-Interaktion beschäftigt sich mit der benutzergerechten Gestaltung von interaktiven Systemen und ihren Mensch-Maschine-Schnittstellen.

2.7. Zwischenfazit

In dieser Arbeit wird die Vision eines Integrativen BIS vertreten, welches durch das Fortschreiten der Konzepte und Technologien bald umgesetzt werden kann. Die Besonderheit diese Ansatzes, der integrative Gedanke zielt auf die Verwendung unternehmensinterner wie auch unternehmensexterner Daten ab, um diese im System zu Führungsinformationen zu verdichten, welche den Führungskräften ermöglichen ihre Entscheidungen zu verbessern und strategische Vorteile gegenüber Mitbewerbern zu erarbeiten. Ein besonderes Augenmerk liegt dabei auf dem ETL-Prozess der die Daten in das BIS überträgt und dem OLAP-Konzept, welches die Daten so bereit hält, dass Führungsinformationen erstmalig konsequent und zeitnah erstellt werden können.

Des Weiteren wurde festgestellt, das der Personenkreis der Führungskräfte auf Grund ihrer Arbeit und ihres Status besondere Anforderungen an Informationssysteme stellen. Somit ist die Usability eines BIS ein wesentlicher Faktor für die Akzeptanz durch Führungskräfte. Diese Anforderungen stehen im Spannungsfeld mit der Sicherheit des Systems die nicht vernachlässigt werden darf.

Das BIS selbst wird in dieser Arbeit als Informationssystem an der Spitze der Informationssystempyramide gesehen dessen Inhalte von entscheidender Bedeutung für den Unternehmenserfolg sind. Die Grundlagen und Vorraussetzungen dieses Systems sowie die Bedeutung der Inhalte wurden im vorhergehenden Kapitel erarbeitet und bilden die Vorraussetzung für das nächste Kapitel die Gefahren von Informationssystemen.

3. Gefahren von Informationssystemen

3.1. Aktueller Stand der Forschung

Einen kompletten Überblick über die derzeit aktuellen Gefahren für Informationssysteme und Kommunikationssysteme zu erarbeiten ist nicht möglich. Die Gefahrenlage ändert sich momentan täglich. Sicherheitsupdates schließen vorhandene Lücken in Informationssystemen; generieren aber bedingt durch die Komplexität

des Gesamtsystems eventuell neue Sicherheitsrisiken. Diese werden wiederum nach geraumer Zeit durch Dritte oder die Entwickler selbst entdeckt. Der Kreislauf wiederholt sich.

2006 wurden durch die KES-Sicherheitsstudie folgende Vertrauensbrüche identifiziert:

Unbefugte Zugriffart	**Bekannt**	**Vermutet**
Verlust mobiler IT-Systeme	27%	9%
Einbruch in Gebäude	17%	1%
Missbrauch durch berechtigte	3%	15%
Verlust von Speichermedien	7%	5%
Abhören von Kommunikation	1%	8%
Online-Angriff	2%	4%
Sonstiger Weg	2%	1%

Tabelle 1: Vertrauensbrüche durch unbefugten Zugriff[235]

Dabei entstanden Schäden durch:

Schäden durch	**2002**	**2004**	**2006**
Unfälle (menschliches bzw. technisches Versagen	79%	73%	70%
Angriffe (ungezielt bzw. gezielt)	43%	60%	43%

Tabelle 2: Schäden durch Unfälle oder Angriffe[236]

Gefahren werden für sich behandelt, eine ganzheitliche Betrachtung im Sinne von „jede Kette ist nur so stark wie ihr schwächstes Glied“ findet nicht statt.[237] Beispielsweise erfordert die Windows Vista Reparaturkonsole auf an sonsten geschützten Systemen keine Authentifizierung.[238]

Die weitere Forschung in diesem Bereich wird nur vereinzelt in Bezug auf die Risikoarten verwirklicht. Ebenso werden die Gefahren nicht in Hinsicht auf das

---

[235] Vgl. <kes> Sicherheitsstudie 2006 in Witt, Bernhard C. (2006), S. 78.
[236] Vgl. <kes> Sicherheitsstudie 2006 in Witt, Bernhard C. (2006), S. 96.
[237] Sicherheitskette: Vgl. Eckert, Claudia (2006), S. 32f; vgl. Wilding, Edward (2006), S. 21.
[238] [Ziemann, Frank (2007); http://www.pcwelt.de].

Schadenspotenzial für Unternehmensinfrastrukturen untersucht. Hingegen werden Aussagen getroffen, welcher Schaden durch einen bestimmten Virus angerichtet wurde bzw. werden könnte. Eine Reduktion auf die später aufgegriffene Payload Problematik[239] findet nicht statt. Vorwiegend finden ex post-Untersuchungen statt.

Die Prävention wird von vielen Autoren auf Virenscanner, Adwarescanner und Firewalls reduziert. Einige wenige Autoren beziehen organisatorische Gefahren in ihre Betrachtung ein. Generell ist eine anthropozentrische Betrachtung nicht vorhanden.

3.2. Gefahrenidentifikation

Ein Ansatz des Risikomanagements besteht darin auftretende Risiken, hier Gefahren zu identifizieren, um sie zu operationalisieren und entsprechend auf diese reagieren zu können. Dieser Risikobegriff ist negativ und die durch Risiko implizierten Chancen werden nicht betrachtet. Wer die Risiken kennt, kann aktives Risikomanagement betreiben. In diesem Kapitel werden die Gefahren untersucht, welche speziell beim Betrieb bzw. der Anwendung von Informationssystemen auftreten. Der Fokus der Untersuchung liegt zum einen auf den grundlegenden Gefahren der Nutzung, zum anderen auf den konkreten Auswirkungen der Gefahren auf BIS. Somit wird ein Teil des Risikomanagements durch Identifizierung der auftretenden Gefahren in diesem Kapitel geleistet um in einem späteren Kapitel Wege aufzuzeigen, wie mit diesen Risiken verantwortungsvoll umzugehen ist.

Der Aufbau der Unterkapitel folgt soweit möglich folgender Vorgehensweise: Zunächst werden die auftretenden Risiken in technische, organisatorische, rechtliche und sonstige Risiken klassifiziert. Bei der Auswahl der Risiken wurde darauf geachtet, dass sie in Beziehung zu Business-Intelligence-Systemen stehen. Weitere Gefahren sind denkbar, beeinträchtigen das BIS aber nicht unmittelbar. Dazu wurden bereits die allgemeinen Aktivitäten, welche bei der Nutzung eines Informationssystems anfallen, beschrieben.

Das Vorgehen folgt folgender Schablone: Die Gefahren werden identifiziert und benannt. Danach erfolgt eine Definition und Beschreibung der Gefahren. Das Schadenspotenzial der Gefahren in Bezug auf die Nutzung eines BIS wird im An-

---

[239] Der Payload bezeichnet die Nutzdaten in der Kommunikationstechnik, im Rahmen von Sicherheitsbetrachtungen ist er mit dem Begriff Schadroutine gleichzusetzen.

schluss aufgezeigt. Abschließend werden die Interdependenzen der Gefahren untersucht, um darzulegen wie einzelne, vielleicht unproblematische Schwachstellen bei komplexen Systemen in Verbindung miteinander schwerwiegende Sicherheitslücken darstellen. Dies begründet die Notwendigkeit einer ganzheitlichen Betrachtung von IT-Sicherheitsrisiken.[240]

Einen weiteren Untersuchungsgegenstand innerhalb dieses Kapitels bilden die Rollen, in welche die Gegner der Systemsicherheit eingeordnet werden können. Die Fragestellung des Unterpunktes lautet, welche Personengruppen aus welcher Motivation zu den Verursachern von Schäden an Unternehmen zählen.[241] Diese Betrachtung ist insbesondere deshalb notwendig, weil sie Aufschluss darüber geben kann, welche Schutzmechanismen nötig sind, um BIS gegenüber menschlichen Bedrohungen abzusichern. Des Weiteren werden die Risiken auf die Nutzung von BIS und die Relevanz derselben für die Entscheidungsfindung bezogen.

3.3. Gefahrenkategorien

Gefahren für integrative BIS lassen sich in folgende Kategorien einteilen:

Ausfallbedrohung

Eine Unternehmensinfrastruktur oder ein Informationssystem kann in seinen Funktionen gestört sein und damit ausfallen. Ein Ausfall ist dann gegeben, wenn der Betrieb dauerhaft gestört ist und zur Wiederaufnahme der Funktionsfähigkeit ein Eingriff seitens eines Menschen notwendig wird. Dies bedingt nicht notwendigerweise die Veränderung oder Zerstörung von Daten. Die Behinderung des Informationsaustausches geht dagegen mit einem Ausfall einher.

Zerstörung von Daten

Daten die auf Medien zur dauerhaften oder kurzfristigen Speicherung abgelegt wurden werden vom Berechtigten unabsichtlich bzw. Unberechtigten unabsichtlich oder absichtlich vollständig gelöscht. Des Weiteren können die Daten durch Systemfehler der Hard- bzw. Software vernichtet werden. Die Verfügbarkeit eines Backups ist unerheblich. Es kommt auf die Zerstörung der vorhandenen Daten an.

---

[240] Vgl. Biethan, Jörg; Muksch, Harry; Ruf, Walter (2007), S. 1.
[241] Vgl. Eschweiler, Jörg (2006), S. 49ff.

Veränderung von Daten/Informationen

Digitale Daten können leicht verändert werden. Unterscheiden lassen sich eine sinnlose Veränderung und eine geplante Veränderung. Bei einer sinnlosen Veränderung können beliebige Zeichen durch andere ersetzt werden. Daten werden damit unbrauchbar. Geplante Veränderungen können gut- bzw. böswillig sein. Es kann beispielsweise ein Eintrag auf die richtige Adresse bzw. Umsatzzahl korrigiert werden. Handelt es sich um eine böswillige Veränderung, werden innerhalb eines bestimmten Speicherraums die gespeicherten Daten verändert. Es können beispielsweise Umsatzzahlen durch vordefinierte Werte oder durch Zufallszahlen ersetzt werden. Von Interesse ist im Rahmen der Arbeit die böswillige Veränderung. Für geplante Veränderungen gibt es Methoden Fehler zu minimieren.

Behinderung des Informationsaustausches

Wird der Austausch von Informationen zwischen Systemen oder Menschen oder beiden gestört, handelt es sich um eine Behinderung des Informationsaustausches. Die Information erreicht nicht den vorgesehenen Empfänger.

Unberechtigte Informationsweitergabe/-erlangung

Gespeicherte Daten, welche per Definition nur einem bestimmten Personenkreis zugänglich sein sollten (Autorisierung), werden einer Person außerhalb dieses Kreises zugänglich. Informationen können dabei unabsichtlich oder absichtlich Dritten bekannt werden. Unabsichtlich könnten Informationen beispielsweise durch eine fehlgeleitete E-Mail zugänglich gemacht werden. Absichtlich könnten Informationen bspw. kopiert und weitergegeben werden. Die Gefährdung kann sich auf die Applikationsebene oder die Netzwerkebene beziehen. Hiermit beschäftigen sich die Applikationssicherheits- und Netzwerksicherheitskonzepte.[242]

Die angeführten Kategorien verursachen der Unternehmung Kosten, welche für eine ökonomische Betrachtung ermittelt werden müssen. Da eine Ermittlung der genauen Werte nicht ohne Weiteres möglich ist, wird des öfteren mit Schätzungen gearbeitet. Gefährdungsfaktoren sind höhere Gewalt, Fahrlässigkeit, Vorsatz, technisches Versagen und organisatorische Mängel.[243]

---

[242] Vgl. Eckert, Claudia (2006), S. 4.
[243] Vgl. Eckert, Claudia (2006), S. 15.

Die Gefahren für Informationssysteme lassen sich in technische, organisatorische, rechtliche und sonstige Gefahren einteilen.[244] Allen ist gemein, dass nicht nur die Gefahren des BIS sondern diejenigen der gesamten Infrastruktur untersucht werden müssen. Auch die nachfolgende Einteilung wird vertreten:

Fahrlässigkeit beispielsweise durch: Irrtum, Fehlbedienung und unsachgemäße Behandlung.[245]

Vorsatz beispielsweise durch: Manipulation, Einbruch, Hacking, Vandalismus, Spionage und Sabotage.[246]

Technisches Versagen beispielsweise durch: Stromausfall, Hardware-Ausfall und Fehlfunktion.[247]

Organisatorische Mängel beispielsweise durch: unberechtigter Zugriff, „Raubkopie“ und ungeschultes Personal.[248]

Folgende Schadensformen können auftreten: Betrug, Verrat von Geschäftsgeheimnissen, missbräuchliche Nutzung von ITK-Diensten; Sabotage, Diebstahl von Hardware oder Software; Viren, nicht-autorisierter Zugriff auf Systeme, Imageschäden und Taxonomie.[249] Davon treten bei großen Unternehmen ca. 38 Missbrauchsfälle im Jahr auf.[250] Die Kosten und Häufigkeit von Schadensfällen[251] müssen im Unternehmen ermittelt und die Ausgaben für IT-Sicherheit danach begründet werden.[252]

Die geschätzten Folgen des Verlustes wichtiger Daten wurden in einer Sicherheitsstudie der Zeitschrift KES aus dem Jahr 2003 untersucht. 16% der Unternehmen befürchten existenzielle Auswirkungen in Form von Konkurs bei einem Totalverlust ihrer Daten. 46% rechnen mit einem Schaden in Höhe von über einer Million Euro.[253] Eine Studie der Firma Mummert Consulting spricht von einem

---

[244] Vgl. Wolfram, Gerd (1986/2005), S. 51ff. Eine Einteilung in vorsätzliches, humanes und technisches Risiko erscheint ebenfalls als möglich.
[245] Vgl. Eckert, Claudia (2006), S. 15.
[246] Vgl. Eckert, Claudia (2006), S. 15.
[247] Vgl. Eckert, Claudia (2006), S. 15.
[248] Vgl. Eckert, Claudia (2006), S. 15.
[249] Vgl. Godschalk, David (2007), S. 94ff.
[250] DTI (2004), Information Security Survey 2004.
[251] Vgl. Godschalk, David (2007), S. 119f.
[252] Vgl. Godschalk, David (2007), S. 114.
[253] Vgl. Geschonneck, Alexander (2004), S. 96.

Anstieg der Sicherheitsverletzungen bei 63% der teilnehmenden Firmen. Dabei verbuchte jedes zweite Unternehmen Schäden bis zu 100.000 Euro.[254]

Als Ergebnis kann bereits festgestellt werden, dass eine Sicherheitslücke das Vertrauen in das komplette System untergraben könnte. [255] Die Kategorisierung in technische, organisatorische, rechtliche und sonstige Gefahren ist bedingt durch den Aufbau und die Verwendungsweise eines BIS für diese Arbeit am sinnvollsten. Die Beschreibung der Kategorien findet sich in den entsprechenden Unterkapiteln.

3.4. Infektionsarten

Wird ein System kompromittiert, stellt sich die Frage, auf welchem Wege dies geschehen konnte. Hierbei kann nicht ausgeschlossen werden, dass sich mit Verbreitung neuer Technologien neue Wege eröffnen. Die Infektionsarten sind für viele in dieser Arbeit aufgeführte Schädlinge gültig.

Autostartfunktion/Dateien

Ein modernes Betriebssystem verfügt über Mechanismen, welche dem Nutzer die Arbeit erleichtern sollen. In Bezug auf einen Schädlingsbefall ist hier vor allem das automatische Anzeigen und Ausführen von Dateien zu nennen („Autostartfunktion“). Diese Aktion tritt vorwiegend beim Übertragen von Dateien auf das Computersystem auf. Wird eine infizierte Datei ausgeführt, ist der Schädling aktiv. Der Schaden, der angerichtet werden kann, hängt von der Schadroutine (Payload) und den Rechten der Datei ab, welche ausgeführt wurde. Die Dateiendung, Bezeichnung des Dateinamens nach dem „.“, bestimmt bei Windowssystemen die Behandlung der Datei durch das Betriebssystem. Dateiendungen die ausführbare Programme versprechen sind besonders gefährlich.

Medien

Zahlreiche mobile Speichermedien sind derzeit für Computersysteme in Gebrauch. Stationäre Speichermedien, wie mit dem System dauerhaft[256] verbundene Festplatten spielen für die Sicherheit eine untergeordnete Rolle. Es gibt Dis-

---

[254] Studie IT-Security 2004 der Firma Mummert Consulting zitiert in [Forthmann, Jörg (2005); http://www.presseportal.de].
[255] Vgl. Merz, Michael (1999), S. 119.
[256] Dauerhaft: Gemeint ist mit dem Computersystem verbunden. Es ist nicht gemeint, dass sie mit dem System verschmolzen sind, was der juristische Begriff implizieren würde.

ketten, mobile Festplatten, optische Speichermedien, USB-Sticks, Speicherkarten, etc.. Sie unterscheiden sich hinsichtlich ihres Speichervolumens. Die Daten liegen in Form von Dateien vor. Da mobile Datenträger zum Austausch oder der Sicherung von Dateien bestimmt sind, besteht eine große Gefahr der Übertragung von schädlingsverseuchten Dateien. Diese Datenträger werden normalerweise durch eine Autostartfunktion geöffnet (siehe oben).

E-Mail

Dateien können per E-Mail versandt werden, dies nennt man einen Dateianhang. Dabei tritt die Problematik auf, welche unter dem Punkt Dateien beschrieben wurde. Hinzu kommt, dass viele E-Mail-Programme eine automatische Vorschau oder Öffnungsfunktion besitzen. Ist eine Vorschaufunktion aktiviert, wird der Schädling sofort ausgeführt. Um das Kommunikationsmittel E-Mail so bequem wie möglich zu gestalten verwenden einige Programme Dateianhänge mit Adressdaten des Versenders der E-Mail. Diese können manipuliert werden und in eine Schädlingsdatei umgewandelt werden.

Web/Internet

Während die Ankunft einer E-Mail sichtbar ist, birgt das Internet weitere Gefahren, welche fast immer für den normalen Anwender unsichtbar sind. Ein Schädlingscode kann in den Quelltext von Internetseiten eingepflegt werden. Hat die verwendete Ansichts-Applikation, der sogenannte Internet-Browser, eine Lücke, dann wird das System infiziert. Dasselbe gilt, wenn Skriptsprachen oder andere Applikationen verwendet werden und in deren Anzeige-Programmen Fehler auftreten. Das Auftreten von Schwachstellen in Browsern, Skriptsprachen und anderen Applikationen ist ein häufiger Fall im Alltag der IT-Sicherheit.

Netzwerk

Netzwerke werden verwendet um Computer miteinander zu verknüpfen. Es kann sich um drahtgebundene oder drahtlose Verbindungen handeln. Vorteil der drahtgebundenen Netzwerke ist, dass sie materiell besser vor dem Zugriff durch Dritte geschützt sind. Diese Verbindungen bilden den Zugang zum jeweiligen Computersystem. Netzlaufwerke stellen einen Ort zur Verfügung, an dem Dateien gespeichert werden und auf den verschiedene Nutzer Zugriff haben können. Ebenso kann ein User von verschiedenen Computern Zugriff auf das Netzlaufwerk bekommen. Wird eine infizierte Datei auf ein Netzlaufwerk gespeichert, kann sie

von verschiedenen Nutzern ausgeführt werden und sich damit verbreiten. Es besteht die Möglichkeit der Infektion mehrerer Computersysteme. Des Weiteren ist es möglich Schadroutinen über schadhafte Netzwerkprotokolle zu verteilen (Wurm).

Programmierung

Softwareprogramme können mit einer Entwicklungsumgebung umgesetzt werden. Enthält diese einen versteckten Schädling, so kann er an eine mit der Entwicklungsumgebung programmierte Software weitergegeben werden. Des Weiteren ist der Vorgang der Programmierung selbst mit Unsicherheiten behaftet. Es kommt hierbei auf die Erfahrung und das Know-how des Programmierers an, Schaden zu vermeiden. Innerhalb der Programmiersprache Java gibt es beispielsweise einen Pseudozufallszahlengenerator, der die Ziffern auf Basis der aktuellen Zeit erzeugt. Wird diese Information nicht berücksichtigt erzeugt das Programm keine Pseudo-Zufallszahlen, sondern bei Verwendung einer Schleife bedingt durch die Geschwindigkeit moderner Rechner eine Reihe gleicher Zahlen, die sich erst nach Erreichen einer Zeitänderung mit anderen Zahlen fortsetzt.[257]

Betriebssystem

Betriebssysteme stellen dem Computernutzer zahlreiche Dienstprogramme zur Verfügung. Es gibt beispielsweise Dateidienste, Druckdienste, Serverdienste, E-Maildienste etc.. Dienste und Systemdateien des Betriebssystems bestehen aus Dateien, diese können durch einen Schädling infiziert werden. Werden Dienste oder Betriebssystemdateien infiziert, ist der gesamte Betrieb des Computers beeinträchtigt. Weiterhin werden Anwendungsprogramme immer stärker in Betriebssysteme integriert. Beispielsweise wird der Windows Internet Explorer oder der Windows MediaPlayer so stark mit dem Betriebssystem verwoben, dass die EU-Kommission ein Wettbewerbsverletzungsverfahren eingeleitet hat. Durch die Verknüpfung der Programme werden ebenso die Lücken verbunden. Das Informationssystem als Ganzes wird über eine Lücke angreifbar. Durch die herausragende Stellung des Betriebssystems beim Betrieb eines Computers sind die auftretenden Infektionswege hierüber besonders wichtig, da sie regelmäßig bei allen Anwendern welche dieses Betriebssystem benutzen auftreten und derzeit der Markt für

---

[257] Vgl. [Fox, Dirk (2002); http://www.secorvo.de]; Eigene Erfahrung mit Java; Schmeh, Klaus (2001), S. 147ff.

Betriebssysteme von wenigen Anbietern (beispw. Microsoft, Apple) beherrscht wird. Zusammenfassend kann ausgeführt werden, dass ein Betriebssystem durch schlecht programmierte Komponenten infizierbar wird.

Spezielle Übertragungswege

Durch den Fortschritt der Technik werden erneut Lücken in vorhandenen Programmen bzw. Filtern entdeckt. Lange Zeit galt es als unbedenklich digitale Bilder auf dem Computer anzuzeigen. Dies hat sich geändert. Eine Schwäche im Bilderformat ermöglicht es Schädlingscode auf ein Computersystem einzuschleusen. Besonders betroffen sind die Webbildformate. Dieser Infektionsweg ist sehr bedeutsam, da fast alle Benutzerschnittstellen, Web-Seiten, etc. in irgendeiner Form mit Bildformaten arbeiten. Bei der Anzeige eines manipulierten Bildes wird der Schädling ausgeführt. Anmerkung: Die Anzeige von Bildern ist standardmäßig eingeschaltet, kann in den gängigen Browsern aber manuell abgeschaltet werden.

Verschlüsselungsschwäche

Viele Passwörter oder Dateien sind unzureichend verschlüsselt. Entweder ist das Passwort, die verwendete Methode oder die Schlüssellänge zu schwach.[258] Es werden vom Nutzer bspw. die Standardpasswörter nicht geändert oder zu schwache Passwörter verwendet. Dadurch ist es möglich, dass Schädlinge Methoden verwenden um schwache Passwörter zu ermitteln (cracken) und damit Zugriff auf ein System bekommen.

Treiberschwachstelle

Die Kommunikation der Komponenten eines Systems funktioniert über Treiber bzw. Schnittstellen. Da alle Systeme ähnliche Treiber und Schnittstellen verwenden, kann ein schwacher Treiber Zugriff auf viele Systeme ermöglichen.

Ausführen einer exe-Datei mit böswilligem Code

Viele Nutzer führen Dateien aus, ohne darüber nachzudenken ob sie schädlichen Payload enthalten könnten. Der Payload erwirbt die Rechte des ausführenden Nutzers.

---

[258] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 5.

Buffer Overflow

Innerhalb der Softwareentwicklung werden Variablen eingesetzt um Speicherplatz für Werte zu reservieren. Ist der Speicherplatz einer Variablen für einen zugewiesenen Wert nicht groß genug und wird der Vorgang durch die verwendetet Programmiersprache oder den Programmierer selbst nicht abgefangen, schreibt das Programm den Wert über den vorgesehenen Speicherplatz hinaus. Bsp.: Zugewiesener Speicherraum 5 Stellen für eine Postleitzahl. Einfügewert „70000format c:". „format c:" entspricht dem Payload. In diesem Fall wird der Befehl „format c:" in den Speicherraum des Arbeitsspeichers geschrieben. Wenn nun dieser Speicherraum ausgelesen wird, führt der Computer den Payload aus.[259]

Benutzerschnittstelle

Alle Schnittstellen zwischen Mensch und Maschine aber auch zwischen Maschine und Maschine sowie zwischen unterschiedlichen Anwendungsprogrammen bergen prinzipiell die Gefahr eines Infektionsweges.

Die nächste Abbildung zeigt auf welchem Wege vertrauliche Daten ein Unternehmen ungewollt verlassen.

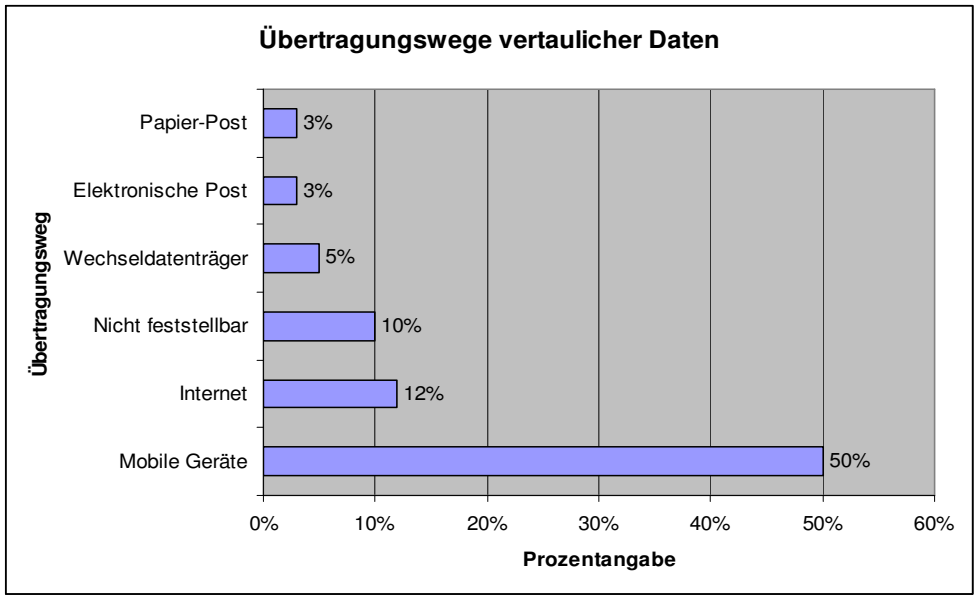

Abbildung 8: Übertragungswege für den Datenverlust[260]

[259] Vgl. Eckert, Claudia (2006), S. 37f; vgl. McClur, Stuart; Scrambray, Joel; Kurtz, George (2006), S. 686f; vgl. Erickson, Jon (2006), S. 35f.
[260] Vgl. [Wößner, Elke (2007); http://www.infowatch.com].

3.5. Technische Gefahren

Gefahren technischer Art ergeben sich aus den verwendeten Systemkomponenten der Hard- und Software. Sie können, müssen aber nicht durch die am Informationssystem beteiligten Menschen ausgelöst werden und können auch als Eintreten eines technischen Defektes verstanden werden.[261] Trotz dieser Definition ist eine scharfe Trennung in technische, organisatorische, rechtliche und sonstige Gefahren nicht immer einwandfrei möglich, da viele Gefahren simultan mehrere Aspekte tangieren.

3.5.1. Bloßstellende Abstrahlung

Diese Form des Risikos erscheint auf den ersten Blick etwas weit hergeholt oder aus Spionagefilmen entnommen, beruht aber auf einer ernst zu nehmenden technischen Begebenheit, die der holländische Elektroingenieur Wim van Eck 1985 offiziell entdeckte, daher der Beinname „Van Eck Phreaking“. Seit dieser Zeit ist die nachfolgend beschriebene Schwachstelle Gegenstand vieler Techno-Thriller. Inoffiziell ist diese Tatsache nach Schätzungen seit den 60iger Jahren bekannt. Es handelt sich um eine Methodik des Computerabhörens, welche sich folgende Einzelheiten zunutze macht.[262]

Definition, Erläuterung, Infektionsweg

Einzelne Computerkomponenten wie Monitor, Drucker, Maus, Tastatur, Grafikkarte, Prozessor, Random Access Memory, etc. tauschen Informationen über Hochfrequenzimpulsfolgen aus, welche elektromagnetische Wellen im Radiofrequenzbereich erzeugen. Diese Abstrahlungen sind durch geeignete technische Einrichtungen auf eine Entfernung von mehr als hundert Metern zu empfangen und durch entsprechende Software kann der Inhalt der Übertragung sichtbar gemacht werden.[263]

Angriffspunkt für das Auslesen von Informationen ist hier die Kommunikation der Rechnerkomponenten untereinander. Beispielsweise zwischen der Grafikkarte und dem Monitor. Alle Bildschirmdarstellungen und Ausdrucke können auf diese

---

[261] Vgl. Wolfram, Gerd (1986/2005), S. 51ff.
[262] Vgl. [Van Eck, Wim; http://jya.com]; [Pixelpark (1996); http://www.wildpark.com]; [Nadir; http://www.nadir.org]; [BSI; http://www.bsi.de].
[263] Vgl. [Van Eck, Wim; http://jya.com]; [Pixelpark (1996); http://www.wildpark.com]; [Nadir; http://www.nadir.org]; [BSI; http://www.bsi.de].

Weise mitgeschnitten werden. Daraus ergeben sich unmittelbare Gefahren für BIS, welche nicht nur durch die Architektur der Systeme sondern auch durch materielle Maßnahmen behoben werden müssen.

Schadenspotenzial Abstrahlung

Das Schadenspotenzial des „Van Eck Phreaking“ manifestiert sich darin, dass alle Informationen die auf dem Bildschirm der Führungskraft erscheinen oder ausgedruckt werden, solange keine Sicherungsmaßnahmen ergriffen werden, potenziell mitgeschnitten werden können. Das bedeutet, dass Geschäftsgeheimnisse wie beispielsweise Bilanzdaten, Strategiepapiere, neue Produktentwürfe aber auch persönliche Daten wie E-Mails etc. dem Abhörer bekannt werden (Unberechtigte Informationsweitergabe). Die so zugänglich gewordenen Informationen können aus ökonomischer Sicht einem Konkurrenten im Wettbewerb Vorteile verschaffen. Durch das Kopieren von Produkten ist eine frühere und kostengünstigere Markteinführung möglich, da die kostenintensiven Entwicklungskosten auf die Ausspäh- und Kopiermaßnahmen reduziert werden können. Aus Bilanzinformationen können Insiderinformationen werden, mit denen der Börsenkurs manipulierbar wird. Geplante Übernahmen könnten vereitelt bzw. illegale Gewinne erzielt werden, welche das übernehmende Unternehmen schädigen. Weiterhin können Schadensersatzansprüche durch unsachgemäßen Umgang mit Daten entstehen. Kompromittierende Informationen führen unter Umständen zur Erpressbarkeit von Führungskräften. Der Schaden entsteht durch die unberechtigte Informationsweitergabe.

3.5.2. Computerviren

Die Terminologie der Computerviren ist der ihrer biologischen Vorbilder sehr ähnlich. Die Begriffe Computervirus und Virus werden daher in Literatur, Fachzeitschriften, der Praxis und dieser Arbeit synonym verwendet.

Definition, Erläuterung, Infektionsweg

Viren sind Programme, die sich replizieren, indem sie andere Programme oder Dateien infizieren, damit diese eine Kopie des Virus enthalten. Die Kopie des Virusprogramms kann nach der Infektion Erweiterungen enthalten und ein verän-

dertes Verhalten an den Tag legen.[264] Technisch wird die einzige Voraussetzung für die Definition eines Virus auf die Eigenschaft der Reproduktion gelegt. Ein schadhaftes Verhalten oder ein Agieren im Hintergrund ohne Wissen des Computernutzers wird von vielen Autoren nicht verlangt.[265]

Diese Einschränkung ist für eine Arbeit über Computersicherheit und die Betrachtung von Usability Eigenschaften nicht geeignet. Interessant sind hier vor allem Programme, die Schadroutinen[266] enthalten, welche ohne Einwilligung des Computernutzers auf dem Rechner eingebracht und abgearbeitet werden.

Merkmale von Viren

Fast alle Viren sind verborgen, das heißt, ihre Anwesenheit auf einem System ist nicht wie bei normalen Dateien ersichtlich, sondern es müssen Maßnahmen ergriffen werden, um Viren aufzuspüren. In diesem Punkt ähneln Computerviren den biologischen Pendants, welche ebenfalls versuchen ihre Anwesenheit zu verbergen, um die Verbreitungswahrscheinlichkeit zu erhöhen. Durch diese Eigenschaft, des Wirken im Verborgenen, steigt die Zeitspanne, in welcher der Virus andere Systeme infizieren kann.

Eine Unterart sind Clusterviren, welche die eigentlichen Programmdateien nicht verändern, sondern die Systemzeiger[267] des Dateisystems auf Bereiche umlenken, die den Virus enthalten. Nicht polymorphe Viren infizieren ein Objekt, indem sie eine mehr oder weniger identische Kopie ihrer selbst in den Code des Objektes einfügen. Polymorphe Viren fügen eine weiter entwickelte Form ihrer selbst an. Dazu benötigten polymorphe Schädlinge Techniken, die beispielsweise die Ablaufreihenfolge des Programmcodes verändern, Scheinanweisungen einarbeiten, unsinnige Bytes hinzufügen oder eine Verschlüsselung verwenden, um ihre Signatur zu verändern und dadurch zu versuchen nicht mehr von Virenscannern erkannt zu werden.[268]

---

[264] Vgl. Cohen, F. (1994); Anonymous (2003), S. 382.
[265] Vgl. Anonymous (2003), S. 382; vgl. Eckert, Claudia (2006), S. 45.
[266] Programmcode, der negative Auswirkungen auf den gewünschten Betrieb des Rechners haben kann. Beispielsweise der Befehl „format“.
[267] Systemzeiger zeigen auf die Stelle an der Festplatte an der sich die Datei physisch befindet.
[268] Vgl. Anonymous (2003), S. 402; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 5.

Schadenspotenzial Viren

Computerviren werden oft als die meist gefürchtete sicherheitsrelevante Bedrohung von Informationssystemen betrachtet.[269] Sie zählen zu der Art von Bedrohung über die viele Märchen und Legenden im Umlauf sind.[270] Die tatsächlichen Schäden, die durch Viren an Informationssystemen und speziell der Informationsinfrastruktur einer Unternehmung auftraten waren meist kleiner als die Imageschäden, welche aus dem Befall bekannter Unternehmen mit Viren entstanden.[271] Das bedeutet aber nicht, dass die Schäden, welche durch Viren an einer Informationsinfrastruktur angerichtet werden nicht unternehmensbedrohlich werden können. Dies ist eine Frage der Verwendung der Programmroutine (Schadroutine, Payload) innerhalb der jeweiligen Bedrohung.[272]

Die Schäden betreffen die Applikations- und Netzwerksicherheit. Sie können abhängig vom Payload des Virus in Form des kompletten Spektrums der **Ausfallbedrohung, Zerstörung von Daten, Veränderung von Daten/Informationen, Behinderung des Informationsaustausches sowie der Unberechtigte Informationsweitergabe/-erlangung** bestehen. Sie führen meist zu einer Denial of Service (DOS) Bedrohung, indem sie Festplattenkapazität, Speicher und Prozesszeit für sich beanspruchen.[273] Denial of Service bezeichnet eine Attacke mit dem Ziel, Dienste und damit den Rechner durch Überlastung arbeitsunfähig zu machen. [274]

Befällt der Virus ein Teilsystem des Gesamtsystems, und handelt es sich bei diesem Teilsystem um einen wichtigen Knotenpunkt innerhalb der Unternehmensinfrastruktur, könnte das Gesamtsystem durch nicht zur Verfügung stehende Dienste, wie Paketweiterleitung, Dateispeicherung oder E-Mail-Weiterleitung erheblich beeinträchtigt oder unbenutzbar werden. Noch schwerwiegender ist der Vertrauensverlust in das Gesamtsystem, da man sich nie sicher sein kann den Virus komplett beseitigt zu haben. Einige Viren richten Schäden unabsichtlich an, andere

---

[269] Vgl. Anonymous (2003), S. 379; [Luckhardt, Norbert (2006); http://www.it-sa.de]; S. 5.
[270] Vgl. Anonymous (2003), S. 379.
[271] Vgl. Anonymous (2003), S. 379.
[272] Vgl. Schifreen, Robert (2006), S. 19ff.
[273] Vgl. Anonymous (2003), S. 379; vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 629.
[274] Vgl. Laudon, Kenneth, C.; Laudon, Jane, P. (2006); S. 347; vgl. Eckert, Claudia (2006), S. 15.

absichtlich.[275] Ökonomisch betrachtet ist die Unterscheidung irrelevant, da es bei der Bemessung des Schadens auf die Art und den Umfang desselben ankommt.

Die Zerstörung von Hardware durch Viren gehört in die Zeit als Programme noch direkt Hardwarekomponenten steuern konnten. Hier sind wenige Fälle bekannt, welche kaum nachweisbar sind. Es ist jedoch nur eine Frage der Schadroutine, welcher Schaden angerichtet wird. Geräte (Hardwarekomponenten) können außer Betrieb genommen werden, Dateien und Dateisysteme können beschädigt oder verändert werden. Es sind Routinen vorstellbar, die alle Ziffern um eine Stelle verschieben. Welche Auswirkungen dieses auf Bilanz- oder Produktionszahlen hätte ist ersichtlich.

Bei Mailviren wird das virenverseuchte Programm per E-Mail verschickt. Damit möglichst viele Empfänger erreicht werden, wird das Adressbuch des Nutzers verwendet. Dieser Effekt kann sich schneeballartig fortsetzen. Der aufkommende E-Mail-Verkehr belastet das Netzwerk, die Netzwerkverbindungen und die Mailserver durch den vielfachen Versand von E-Mails. Es handelt sich somit um eine DOS-Attacke.

Viren richten durch die Verwendung von Zeit und Ressourcen auf Prävention vor ihrer Infizierung, Beseitigung und Wiederherstellung verloren gegangener Daten den größten Schaden an. Mitarbeiter der Unternehmung müssen sich mit Viren beschäftigen und haben deshalb weniger Zeit für andere Aufgaben. Dies begründet Opportunitätskosten.

Schäden auf sozialer Ebene entstehen, indem besonders in angloamerikanischen Ländern der Ruf eines Menschen durch kompromittierende Dateien beeinträchtigt werden kann. Nicht bekannt, aber nicht auszuschließen sind Schadroutinen, welche Daten oder Informationen über das Unternehmen, den Computeruser sammeln und diese an unbefugte Dritte weiterleiten. Der Fantasie des Virenautors in Bezug auf die Schadroutine werden nur durch die zur Verfügung stehenden Programmiersprachen Grenzen gesetzt.

Computerwürmer

Wie bei Viren ist die Replikation eine Eigenschaft von Computerwürmern. Einige Spezialisten, wie Fred Cohen betrachten Würmer als Unterart der Gattung Vi-

---

[275] Vgl. Anonymous (2003), S. 379.

rus.[276] Auch bei diesem Schädling folgt die Terminologie den biologischen Vorbildern. Unterscheiden lassen sich Würmer und Viren an ihrer Fähigkeit sich an legitime Programme anzuhängen. Viren können sich anhängen und benötigen einen Wirt. Würmer kopieren sich selbstständig über Netzwerke oder Systeme ohne sich anzuhängen. Der Wurm infiziert nicht Objekte sondern seine Umgebung.[277]

Für die Infektion nutzt der Wurm deshalb Sicherheitslücken in der Soft- und Hardware der verwendeten Systeme. Weil Würmer ihre Umgebung infizieren führen Sicherheitslücken in Betriebssystemen vorwiegend zu einer exponentiellen Ausbreitung des Schädlings, da keine Benutzerinteraktion notwendig ist und die Lücken in allen Computersystemen, welche dieses Operating System verwenden so lange vorhanden ist, bis aktiv ein Patch eingespielt wird. Bei mangelnder Wartung und Pflege des Betriebssystems besteht somit eine erhöhte Gefahr eines Wurmbefalls.

Schadenspotenzial Computerwürmer

Da Computerwürmer die Umgebung eines Informationssystems infizieren ist ihr Schadenspotenzial im Vergleich zu Computerviren nicht unbedingt größer aber wahrscheinlicher. Die Wahrscheinlichkeit ist größer, da weniger aktive Beteiligung des Computernutzers für die Infektion eines Computers benötigt wird. Das Potenzial des Schadens ist von den verwendeten Schadroutinen abhängig. Insofern kann das Potenzial mit dem der Computerviren gleichgesetzt werden. Das Spektrum umfasst die **Ausfallbedrohung, Zerstörung von Daten, Veränderung von Daten/Informationen, Behinderung des Informationsaustausches sowie die Unberechtigte Informationsweitergabe/-erlangung**.

3.5.3. Trojanische Pferde

Unter einem „Trojanischen Pferd“ (umgangssprachlich: Trojaner) versteht man einen in böswilliger Absicht geschriebenen Computercode, der in Anwendungs-

---

[276] Vgl. Anonymous (2003), S. 383.
[277] Vgl. Anonymous (2003), S. 383; vgl. Eckert, Claudia (2006), S. 57.

programme, Dienst-Programme oder Spiele eingefügt wurde. Die Bezeichnung geht auf die Homer'sche Odyssee zurück.[278]

Definition, Erläuterung, Infektionsweg

„Trojanische Pferde“ sind Programme, die neben scheinbar nützlichen zusätzlich schädliche, nicht dokumentierte, Funktionen enthalten und diese unabhängig vom Computeranwender und ohne dessen Wissen ausführen. Im Gegensatz zu Computerviren können sich „Trojanische Pferde“ nicht selbstständig verbreiten.[279]

Nicht unter diese Definition fallen so genannte „Easter Eggs“. Dies sind Programmroutinen, die ebenfalls nicht offiziell vom Programmhersteller dokumentiert, also auch „versteckt“ sind, aber keine schädliche Funktion aufweisen. Dazu gehören beispielsweise Funktionen für die Fehlersuche, Protokollierung oder eine Liste der beteiligten Programmierer.

„Trojanische Pferde“ sind bereits seit den Anfängen der Computernutzung mit Großrechnern bekannt. Weil damals nicht jeder über einen eigenen Rechner verfügte, waren vor der weiten Verbreitung des PCs Arbeitsplätze an einen Großrechner angeschlossen. Unterschieden wurden die einzelnen Arbeitsplätze anhand von Benutzerdaten (Authentifizierung). Die entstandenen Kosten wurden entsprechend der Rechenzeit abgerechnet. Es kamen daher „Trojanische Pferde“ auf, mit deren Schadroutine es möglich war, die Rechner auf Kosten anderer Anwender zu benutzen. Hierzu ist die Kenntnis des Kennwortes sowie der Anmeldename für den Zugriff erforderlich. Diese wurden beispielsweise mittels heimlich installiertem „Password-Sniffer“ protokolliert. „Password-Sniffer“ haben das Erscheinungsbild des normalen Anmelde-Bildschirms[280], sodass der berechtigte Anwender von der Manipulation nichts bemerken kann, solange er nicht aktiv nachforscht.[281]

---

[278] [Meyer (2003); http://www.net-lexikon.de]:„…Als die Griechen wegen des Raubs Helenas die Stadt Troja zehn Jahre lang vergeblich belagert hatten, ersann Odysseus eine List. Er schlug vor, ein großes hölzernes Pferd zu bauen, in dessen Bauch sich Soldaten versteckten. Nach dem scheinbaren Abzug der griechischen Belagerungsarmee zogen die Trojaner das Pferd als vermeintliche Opfergabe in das Stadtinnere. Nachts entstiegen die versteckten griechischen Krieger dem Rumpf des Pferdes und öffneten ihren Mitstreitern die Stadttore Trojas. Wie die Soldaten in dem harmlos aussehenden Pferd wird der als ‚Trojanisches Pferd’ bezeichnete schädliche Computercode in einem harmlos aussehenden Programm versteckt.“.

[279] Vgl. Eckert, Claudia (2006), S. 63; vgl. [Meyer (2003); http://www.net-lexikon.de].

[280] Vergleiche Phishing.

[281] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

Mit der zunehmenden Zahl von Internet Service Providern, die ihren Kunden ihre Dienstleistungen ebenfalls in Rechnung stellen, verbreiteten sich „Trojanische Pferde“ auch auf dem PC. Weitere Anwendungsgebiete ergeben sich in der Remotesteuerung von fremden PCs sowie der Informationssammlung.

Schadenspotenzial „Trojanische Pferde“

Es sind hunderte von Programmen bekannt, die Zugangsdaten von Anwendern erfassen und über das Internet an den Cracker verschicken können. Wegen der starken Verbreitung und des niedrigen Sicherheitsstandards sind die Windows-Betriebssysteme der Firma Microsoft besonders stark durch „Trojanische Pferde“ bedroht. Dabei geht es in der letzten Zeit um den Versuch vertrauliche Daten zu erfassen. Zum Beispiel solche des Online-Bankings.

Außerhalb des privaten Bereiches gibt es darüber hinaus folgende Gefahren durch „Trojanische Pferde“: Der Schutz vertraulicher Daten auf vernetzten Computern (zum Beispiel Personendaten, Konstruktionsunterlagen, Kalkulationsdaten usw.) ist bei Befall mit „Trojanischen Pferden“ oder Computerviren nicht mehr gesichert. Die vorhandenen Daten können verändert, gelöscht oder ausgeforscht und über das Netz an den Angreifer verschickt werden. Das komplette Spektrum der **Ausfallbedrohung, Zerstörung von Daten, Veränderung von Daten/Informationen, Behinderung des Informationsaustausches sowie der Unberechtigte Informationsweitergabe/-erlangung** ist gegeben. Dieser „Datendiebstahl“ kann unbemerkt bleiben, weil im Gegensatz zum Diebstahl materieller Dinge nichts fehlt. Bei der Nutzung von Computern durch Unbefugte können hohe Kosten an anderer Stelle (bspw. bei der Haftung) entstehen.

3.5.4. Hardwaredefekt

Eine Unternehmensinfrastruktur besteht nicht nur aus einer einzelnen Komponente sondern aus vielen miteinander verbundenen Bestandteilen, welche zusammen ein komplexes System bilden. Jede einzelne Komponente kann dabei wiederum aus mehreren Bausteinen bestehen.

Betriebswirtschaftlich wird ein Unternehmensbestandteil über dessen gewöhnliche Lebensdauer/Nutzungsdauer abgeschrieben.[282] Diese Abschreibung trifft die Lebensdauer eines Objektes gewöhnlich gut. Dennoch kann es zu außergewöhnli-

[282] Vereinfacht dargestellter Sachverhalt.

chen Ausfällen kommen. Betrachtet man ein Computersystem, so kann der Defekt einer einzelnen Komponente, wie beispielsweise des Hauptspeicherriegels, den Ausfall oder gar die Zerstörung des gesamten Systems zur Folge haben. Computersysteme werden mit elektrischem Strom betrieben. Eine Schwankung der Stromstärke oder ein Ausfall der Stromversorgung führt bei diesen unter Umständen zu einem Totalausfall.

Schadenspotenzial

Durch defekte Bauteile können Kaskadeneffekte auftreten und weitere technische Geräte zerstört werden. Es sind nicht nur die Reparatur- oder Wiederbeschaffungskosten anzusetzen, sondern auch die dadurch entstehenden Opportunitätskosten und Datenverluste. Um den Schaden messen zu können, ist es notwendig ein Hardwareinventarverzeichnis zu erstellen, in dem die aktuellen Wiederbeschaffungskosten erfasst werden. Des Weiteren ist eine Informationslandkarte notwendig, in der die Speicherorte der Daten verzeichnet sind, um die Kosten der Datensicherung und Datenrettung zu berücksichtigen. Mögliche Schäden sind **Ausfallbedrohung, Zerstörung von Daten sowie die Behinderung des Informationsaustausches.**

3.5.5. Softwaredefekt

Software bezeichnet alle nicht physischen Funktionsbestandteile eines Computers bzw. technischen Gegenstandes, der mindestens einen Mikroprozessor enthält. Dies umfasst vor allem Computerprogramme sowie die zur Verwendung mit Computerprogrammen bestimmten Daten. Die Nutzung moderner Informationssysteme ist in der Regel nur durch Software möglich. Ebenso verbergen sich die für den Betrieb notwendigen Algorithmen, Modelle, Verfahren, etc. hinter dem Begriff Software.[283]

Schadenspotenzial

Bei komplexen Systemen wurde beobachtet, dass es sich um emergente Systeme handelt. Da Software zum Betrieb eines Informationssystems notwendig ist, kann ein Fehler dieser das komplette System beeinträchtigen. Eine gewohnte Aufgabenerfüllung ist nicht möglich. Es entstehen Reparatur- und Wartungskosten sowie Opportunitätskosten durch den Arbeitszeitausfall. Das Schadensspektrum

[283] Vgl. Shapiro, F. R. (2000), S. 69.

erstreckt sich über die **Ausfallbedrohung, Zerstörung von Daten, Veränderung von Daten/Informationen, Behinderung des Informationsaustausches sowie der unberechtigten Informationsweitergabe/-erlangung**.

3.5.6. Gefahren bei der Nutzung strombetriebener Anlagen

Computersysteme benötigen für den Betrieb ebenso wie viele andere Geräte der Informationsinfrastruktur elektrischen Strom. Der Betrieb solcher Systeme hängt von einer unterbrechungsfreien Stromversorgung ab, weil sie Strom für den normalen Betrieb aufgrund der Architektur der Systeme benötigen. Die Arbeit eines Rechnersystems findet in einem flüchtigen Speicher statt, dem Arbeitsspeicher. Wird die Stromversorgung unterbrochen, sind alle dort gerade noch vorhandenen Daten unwiederbringlich verloren.[284]

Des Weiteren sind Computersysteme bedingt durch ihre Architektur anfällig für Spannungsschwankungen. Mikrochips, bestehen aus sehr kleinen Vertiefungen auf einer Siliziumoberfläche, in denen entweder Strom fließt oder kein Strom fließt. Ein Spannungsüberschuss kann dazu führen das diese Vertiefungen in nicht gewünschter Weise miteinander verbunden werden. Der Chip wird unbrauchbar und dadurch die Computeranlage. Meist werden durch das entstehende magnetische Feld auch Teile der Festplatten gelöscht. Solch ein Überschuss kann sich kaskadierend durch die Infrastruktur fortsetzen.[285]

Durch den Elektromagnetischen Puls (EMP), der bei einem Blitzschlag ähnlich wie bei einem Nuklearwaffenabwurf entsteht, müssen Geräte nicht mit dem Stromnetz verbunden sein, um Chips zu zerstören (Fernwirkung). Daten und Informationen werden zerstört und können nur bedingt wiederhergestellt werden.[286]

3.5.7. Filesharing

Filesharingprogramme dienen zunächst dem Austausch von Dateien zwischen Rechnern. Der technische Fortschritt hat dazu geführt das Filesharingprogramme heute vor allem von der Jugend als Hilfsmittel zur Suche und dem Austausch von Mediendateien und Software gesehen werden. Die ursprüngliche Quelle der gesuchten Datei wird bei Filesharingprogrammen in der Regel nicht identifiziert.

---

[284] Vgl. Malz, Helmut (2004), S. 100ff.
[285] Vgl. Zipfel, Martin (2007), S. 29; Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2004), S. 679.
[286] Vgl. Schwab , Adolf J.; Kürner, Wolfgang (2007), S. 93ff.

Die Vertrauenswürdigkeit der Quelle ist nicht ersichtlich. Die Bezeichnung der Datei muss nicht mit dem Inhalt übereinstimmen. Ein User sucht in einem Filesharingprogramm die Nummer 1 der Deutschen Single Charts. Abgesehen von einer eventuellen Urheberrechtsverletzung kann der Suchende nicht sicher sein, welche Datei er sich lädt. Hinter dem Titel: Nummer 1 der deutschen Singlecharts.mp3 könnte sich jeder beliebige Inhalt verstecken.

Filesharingprogramme werden größtenteils kostenlos angeboten. Zwar ist der Quelltext oft vorhanden aber die Nutzer verwenden aus mangelnder Kenntnis bzw. Bequemlichkeit oft vorkompilierte Programme aus zweifelhaften Quellen. Diese Programme bergen die oben angeführten Risiken wie „Trojanische Pferde“ oder Backdoors. Ein weiteres Risiko besteht bei einem Teil dieser Anwendungen in ihrer Funktion als Server. Hierdurch können Lücken im internen Netzwerk entstehen.

Rechtliche Probleme und Schadensersatzforderungen können entstehen indem durch die Programme urheberrechtlich geschütztes Material verteilt wird bzw. illegale Inhalte beschafft und für Dritte zugänglich gemacht werden. Des Weiteren ist die Durchsetzung von Schadensersatzansprüchen schwierig, da der Verursacher ermittelt und die Tat zweifelsfrei nachgewiesen werden muss.[287]

3.5.8. Dialer

Als Dialer werden Programme bezeichnet die primär eine Verbindung zum Internet ohne Konfigurationsaufwand seitens des Anwenders herstellen oder auf dem Rechner einen neuen Internetzugang einrichten. Nach dem Download und der Installation wählt sich der Dialer über das Zugangsgerät wie bspw. ein Modem oder die ISDN-Karte ins Internet ein.[288]

Bei rechtskonformen Einwählprogrammen geschieht dies nach ausdrücklicher Bestätigung des Nutzers. Eine bereits bestehende Internetverbindung wird in der Regel zuvor getrennt. Die Zugangsnummer, die der Dialer bei der neuen Einwahl

---

[287] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 25.

[288] Vgl. [Informationsarchiv; http://www.informationsarchiv.net]; vgl. [Dialerschutz; http://www.dialerschutz.de].

benutzt, bestimmt die Höhe der anfallenden Kosten. Dialer funktionieren in aller Regel nur auf dem Betriebssystem Windows.[289]

Diese Definitionsansätze sind sehr eng gefasst und treffen nicht den wesentlichen Kern eines böswillig eingesetzten Programms. Es genügt einen Dialer als Einwählprogramm zu kennzeichnen, der nicht autorisiert installiert wird und eine durch einen Dritten festgelegt Telefonnummer wiederholt anwählt.

Schadenspotenzial

Der Schaden entsteht zunächst durch erhöhte Telefonmehrwertkosten. Des Weiteren ist es denkbar sich über den Dialer Zutritt zum Netzwerk zu verschaffen, in dem er als Remote-Werkzeug ausgestaltet wird.[290]

Sicherheitsmaßnahmen Dialer

Ob ein Schutz vor Dialern notwendig ist, hängt von der Unternehmensinfrastruktur ab. Maßnahmen werden über Softwareprodukte getroffen bzw. das Sperren von Nummerkreisen bei Telefonleitungen, an welche Zugangsgeräte angeschlossen werden.

3.5.9. Coockies

Browsern können Dateien (Coockies) auf dem lokalen PC des Nutzers ablegen. Diese Dateien werden in der Regel zur Authentifizierung des Nutzers bei wiederkehrendem Gebrauch einer Internetseite angelegt.[291] Coockies können auch genutzt werden, um das Surfverhalten von Internetnutzern auszuspähen. Eine Webseite legt den Coockie ab und andere versuchen diesen auszulesen. Aus den besuchten Webseiten ergibt sich das Profil des Nutzers. Da eine Datei auf dem lokalen PC des Nutzers hinterlassen wird, kann versucht werden per Coockies eine Schadroutine auf dem PC abzulegen. Nur die Schadroutine ist im Zusammenhang mit integrativen BIS relevant.

3.5.10. Internetzugang/Netzwerkzugang

Wird veraltete Zugangstechnik innerhalb einer Unternehmensinfrastruktur verwendet, treten folgende Sicherheitsprobleme auf: Ältere Zugänge werden in Si-

---

[289] Vgl. [Dialerschutz; http://www.dialerschutz.de].
[290] Vgl. [Dialerschutz; http://www.dialerschutz.de].
[291] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

cherheitskonzepten oft vergessen. Der Schutz wird als gegeben hingenommen, dabei handelt es sich meist um veraltete oder zu schwache Maßnahmen. Ein Beispiel sind Einwahlpunkte, sie können durch „Wardialing“ angegriffen werden.[292]

Wireless-Zugangspunkte haben den Nachteil, dass eine physische Verbindung nicht notwendig ist. Der Angreifer kann anonym versuchen sein Ziel zu erreichen, da die Zugangspunkte eventuell auch von außerhalb des Firmengeländes erreicht werden können. Ein Weg Zugangspunkte zu finden ist das „Wardriving“. Hier bewegt sich der Angreifer durch eine Stadt und versucht Wireless Accesspoints zu finden und zu kompromittieren. Nach Tests sind nur 7 GB mitgeschnittener Datenverkehr/Traffic notwendig um die oft verwendeten WEP-Schlüssel eines Wireless Routers zu errechnen. Bei einer derzeit aktuellen Datenübertragungsgeschwindigkeit von 54Mbits/s benötigt man ca. 18 Minuten unter Vollauslastung, um die benötigte Datenmenge zu sammeln. Erhöht sich die Übertragungsgeschwindigkeit auf 128Mbit/s werden nur noch ca. 9 Minuten benötigt. Für das errechnen der WEP-Schlüssel sind Standardtools verfügbar. [293] Der neue Standard für WLAN ist laut IEEE 802.11i/D9.0 der WPA2 (WPA2-Personal and WPA2-Enterprise), er bietet momentan besseren Schutz als WPA und WEP. Die benötigten Datenmengen sowie Standardtools sind noch nicht bekannt.[294]

Die Netzwerktopologie kann Fehler aufweisen, welche es ermöglichen leichteren Zugang zu geschützten Inhalten zu bekommen. Beispielsweise können Systeme falsch konfiguriert sein und einen Zugang zum gesamten Netzwerk ermöglichen.

3.5.11. Überwachungseinrichtungen

Kameras Kontrollprogramme etc. können bei schwachem Zugangsschutz missbraucht werden. Beispielsweise zeichnen Kameras die Eingabe von PIN-Nummern oder Passwörtern auf. Da diese Werkzeuge im Zuge des Pervasive Computing/Ubiquitous Computing kleiner, leistungsfähiger und allgegenwärtig werden, besteht die Gefahr einer unbeabsichtigten Weitergabe der Information. Kleidung und Funktion verschmelzen eng miteinander d.h., ein Dritter könnte eine kleine Kamera mit Mikrofon versteckt am Körper tragen und die Eingabe

---

[292] Anonymous (2003), S. 447ff.
[293] Anonymous (2003), S. 447ff.
[294] Vgl. IEEE 802.11i/D9.0.

von Passwörtern aufzeichnen. Mit ihnen können Eingaben und Ausgaben des integrativen BIS aufgezeichnet und an den Angreifer weitergeleitet werden.[295]

Als Keylogger wird Hard- oder Software bezeichnet, die dazu verwendet werden kann, die Eingaben per Tastatur oder Maus an einem System zu protokollieren. Dadurch ist es möglich das System zu überwachen indem die Eingaben rekonstruiert werden. Keylogger werden oft in Verbindung mit Trojanischen Pferden verwendet, um vertrauliche Daten zu ermitteln und zeichnen entweder alle Eingaben auf oder warten gezielt auf Schlüsselwörter vor der Aufzeichnung, um Speicherplatz zu sparen und ihre Anwesenheit dadurch zu verbergen.[296]

Es sind Software- und Hardware-Keylogger zu unterscheiden. Software-Keylogger befinden sich zwischen Betriebssystem und Eingabegerät, die Eingaben werden über den Keylogger an das Betriebssystem weitergegeben. Hardware-Keylogger erfordern einen physischen Zugang, sie werden zwischen Eingabegerät und Rechner eingebaut. Die erhobenen Daten werden entweder auf der Festplatte des überwachten Rechners gespeichert und danach versendet. Hardware-Geräte können die Daten in einem integrierten Speicher ablegen, der beim entfernen ausgelesen wird. Funkeingabegeräte können über die abgegebene Strahlung abgehört werden. Diese ist jedoch meist verschlüsselt, womit eine Kryptoanalyse notwendig wird.

3.5.12. Emergenz komplexer Systeme

Computersysteme verhalten sich ab einem gewissen Grade an Komplexität emergent. Das heißt sie entwickeln eine Eigendynamik, die vom Hersteller und dessen Programmierern nicht gewollt oder vorhersehbar ist. Betriebssysteme führen dann Funktionen aus, ohne dass ein gewollter Eingriff seitens eines Menschen stattgefunden hat. Ziel und Aktion differieren in diesem Fall.[297]

3.5.13. Zusammenfassung Schadenspotenzial technischer Gefahren

Es wurden zahlreiche Gefahren technischer Art identifiziert, welche für sich alleine genommen schon ein erhebliches Schadenspotenzial aufweisen. Die Schä-

---

[295] Vgl. Brands, Gilbert (2005), S. 666.
[296] Vgl. Anonymous (2003), S. 335.
[297] Vgl. Hellige, Hans Dieter (2003), S. 309ff.

den reichen von Unbequemlichkeiten bis zum Totalverlust der Unternehmung. Ursächlich müssen in diesem Falle nicht immer böswillige Dritte sein, sondern es kommt auch höhere Gewalt bzw. ein technischer Defekt als Ursache in Frage.

Interdependenzen der einzelnen Schadarten

Die technischen Gefahren lassen sich innerhalb der Infrastruktur miteinander verketten. So können beispielsweise durch ein zunächst aufgezeichnetes Passwort, danach Viren, Würmer, Trojaner in das System eingeschleust werden oder sonstige Aktionen ausgelöst werden. Umgekehrt ist es möglich durch Viren, Würmer oder Trojaner beispielsweise dieses Passwort erst zu ermitteln. Der Kombination der einzelnen Gefahren sind kaum Grenzen gesetzt. Deshalb ist es wichtig auch die vermeintlich geringeren Gefahren zu vermeiden.

3.6. Organisatorische Gefahren

Ein Informationssystem dient einer definierten Aufgabenerfüllung innerhalb von Unternehmen. Gefahren organisatorischer Art ergeben sich aus dem Aufbau der Organisationen in der das Informationssystem angewendet wird.

3.6.1. Menschliche Verhaltensweisen

Das wirtschaftliche Umfeld von Unternehmen ist von Lieferanten, Mitarbeitern und Kunden geprägt. Die Struktur der Einzelunternehmung wurde bereits angesprochen. Bei Lieferanten oder Kunden kann es sich dabei sowohl um Unternehmen als auch natürliche Personen handeln. Unternehmen bestehen neben ihrer nicht unumstrittenen Existenz als eigene Rechtspersönlichkeit aus natürlichen Personen in Form von Mitarbeitern, materiellen Gütern, wie Maschinen und immateriellen Gütern wie Informationen. BIS werden von Menschen genutzt. Es existiert ein komplexes Geflecht von Menschen, materiellen sowie immateriellen Gütern.[298]

Im Weiteren sind nicht nur Aufgaben zu erfüllen, sondern es müssen auch die Wartung und Pflege von Business-Intelligence-Systemen von Menschen vorgenommen werden. Es existieren Schnittstellen, zwischen Mensch und Maschine,

---

[298] Vgl. McIlwraith, Angus (2006), S25f.

welche einen Zugang zur Informationsinfrastruktur ermöglichen.[299] Menschen können Daten oder das System selbst verändern. Des Weiteren sind mutwillige Zerstörungen denkbar.[300]

Schadenspotenzial Menschen

Menschen in Form von Mitarbeitern oder Dritten verfolgen eigene Ziele, welche nicht mit den Zielen der Unternehmung, des Eigentümers übereinstimmen müssen. Der anzurichtende Schaden kann sehr weit gefasst werden. Die Schäden sind in absichtlich angerichtete Schäden und unabsichtlich begangene Schäden[301] zu klassifizieren. Die unabsichtlichen Schäden sind in Unkenntnis und Arbeitsvermeidung aufzuteilen. Absichtlich angerichtete Schäden lassen sich in Sorgfaltspflichtverletzungen und Sabotage unterteilen.

Das Schadenspotenzial ist abhängig von den Berechtigungen und Aufgaben sprich der Rolle des Menschen, welche durch IT-Sicherheitslücken erweitert werden können. Ein böswilliger Administrator kann größeren Schaden anrichten als ein Benutzer, der nur eingeschränkte Rechte auf dem Betriebsystem besitzt (Gastuser). In Bezug auf das Kriterium Gewalt ist der Zugang des Menschen erheblich.[302] Eine Studie von Gartner zeigt das in 37 Prozent der befragten europäischen sowie 32 Prozent der deutschen Unternehmen keine definierten Regeln für den Umgang ihrer Mitarbeiter mit vertraulichen Daten existieren. Sofern diese Regeln aufgestellt wurden, sind sie 24 Prozent der europäischen und 19 Prozent der deutschen Mitarbeiter unbekannt.[303] „Employees commit 82% of computer frauds, a third of whom are managers (Ernst & Young Fraud survey 2001).”[304] „Frauds committed by employees cause median losses of $60000, while frauds

---

[299] Vgl. [Fox, Dirk (2005); http://www.secorvo.de] in DUD Datenschutz und Datensicherheit 27 (2003).
[300] Vgl. McIlwraith, Angus (2006), Chapter I S. 25-44.
[301] Vgl. Schneier, Bruce (2000), S. 255; vgl. nach einer Studie von Gartner wird jedes fünfte Notebook durch den Eigentümer selbst verloren; vgl. [Lusk, Bill (2007); http://media.www.marshallparthenon.com]; vgl. Redmill, Felix; Anderson (Eds), Tom; (2004), S. 149ff.
[302] Vgl. [Fox, Dirk (2005); http://www.secorvo.de] in DUD Datenschutz und Datensicherheit 27 (2003).
[303] Vgl. [McAfee Inc (2007); http://www.mcafee.com]; [Lusk, Bill (2007); http://media.www.marshallparthenon.com].
[304] Wilding, Edward (2006), S. 16.

committed by managers or executives cause median losses of $250000. Managers and employees together $500000."[305]

3.6.2. Zugangssicherung

Die Zugangssicherung durch mechanische Sicherungen und Geheimnisse (bspw. in Form von elektronischen Schlössern welche durch eine Geheimnummer. ähnlich der PIN der EC Karte gesichert sind) können durch das Verhalten der Teilnehmer ausgehebelt werden. Häufig treten dabei der Kartentausch bzw. das Verlieren oder Überlassen solcher Karten auf, dies führt zu unbefugtem betreten und öffnen von Sicherheitsbereichen oder Informationen.

Die Erinnerung an viele verschiedene Passwörter ist für Menschen unbequem und schwierig. Deshalb werden Passwörter oft nicht nach dem Zufallsprinzip ausgewählt. Dies ist auf die Unwissenheit über die Wichtigkeit sicherer Passwörter zurückzuführen. Systemadministratoren ändern Standardpasswörter aus ähnlichen Gründen nicht. Teilweise liegt unter der Tastatur das Zugangspasswort zum System. Es existieren Listen von Standardpasswörtern der wichtigsten Applikationen und Dienste im Internet. Häufig gewählte Passwörter sind beispielsweise: Der eigene Name, der Vorname, der Namen von Kindern, Haustieren, Partnern, Geburtsdaten, Jahrestage, Anagramme etc.. Dies ist Angreifern bekannt und führt in Zusammenhang mit Social Engineering und Wörterbuchattacken leicht zu Zugang zum System.

3.6.3. Spam

Spam ist definiert als unverlangt zugestellte E-Mails. Der Name „Spam" ist dem Dosenfleisch SPAM[306] (**S**piced **P**orc and H**am**) der Firma Hormel Foods entliehen und spielt auf die Massenproduktion des Produktes an.[307]

Schadenspotenzial

Spam senkt die Produktivität der Mitarbeiter durch Arbeitszeitbelastungen in Form der Auswahl von wichtigen und unwichtigen Mails. Die Werbung trifft häufig auf Produkte zu, die gesellschaftlich nicht akzeptiert sind, aber gewisse Neugier erwecken. Das Hauptproblem ist die Unterscheidung zwischen Werbe-Mails

---

[305] Wilding, Edward (2006), S. 16.
[306] [Spam; http://www.spam.com].
[307] Vgl. [Kommission der Europ. Gemeinschaften; http://spam.trash.net].

und Angriffs-Mails. Schlecht eingerichtete E-Mail-Programme bilden über Nebeneffekte des Spams ein Einfallstor für den Payload von Schädlingen. In Bezug auf integrative BIS liegt die Gefahr in der Infektion mit einem Schädling.

3.6.4. Kreditrelevanz der IT-Sicherheit

Durch neu eingeführte Regeln in der Finanzwelt wie Basel II oder den Sarbanes-Oxley Act wird die IT-Sicherheit der Unternehmen zunehmend bei der Vergabe von Krediten berücksichtigt. Schadensfälle im Bereich der IT senken das Vertrauen der Banken in die IT-Sicherheit des Unternehmens und führen dadurch zu erhöhten Kreditkosten, in Form eines höheren Kreditzinses.[308]

Schadenspotenzial

Höhere Kreditzinsen mindern die Einnahmen des Unternehmens, damit sinkt die Attraktivität des Unternehmens für Investoren, was sich wiederum in höheren Kreditkosten niederschlägt. In Extremfällen können Sicherheitsverletzungen auch eine Zahlungsunfähigkeit seitens des Unternehmens auslösen.

3.6.5. Unberechtigte Installation

Menschen sind darauf ausgerichtet sich die Aufgaben zu erleichtern. Beispielweise installieren Mitarbeiter unberechtigt Programme und Hardwarebestandteile. Als nicht dokumentierte Teile der Unternehmensinfrastruktur stellen sie eine potenzielle Bedrohung dar, da die verwendete Software unter Standardkonfiguration sehr mitteilsam gegenüber Anfragen Dritter ist. Über eine geeignete Abfrage könnte beispielsweise das verwendete Betriebssystem und dessen Softwarekomponenten ermittelt werden, welche wiederum auf Schwachstellen schließen lassen. Dies kann durch geeignete Einstellungen und geplante Installationen verhindert werden.

3.6.6. Gefahren der Gestaltung des Informationssystems

Die Gestaltung der Informationssysteme unterliegt strengen Regeln. Sollten sich die äußeren Rahmenbedingungen ändern, so kann der Entwurf des integrativen BIS obsolet und somit der Zweck nicht mehr erfüllt werden. Es ist deshalb wich-

---

[308] Vgl. Schrey, Joachim in Gründer, Torsten (2007), S. 275ff; vgl. Fischer, Joerg K. (2008), S.237ff.

tig beim Entwurf auf die Anpassbarkeit, hinsichtlich gesetzlicher Rahmenbedingungen sowie Änderungen der Lehrmeinung und Forschung zu achten.

3.6.7. Fazit des Schadenspotenzials organisatorischer Gefahren

Organisatorische Gefahren entstehen aus dem Aufbau der Unternehmung und damit durch Aufgabenträger und Anwender welche die Unternehmensinfrastruktur des Betriebs nutzen. Auch die komplexesten Organisationen und Organisationsformen bestehen zum großen Teil aus Menschen (Aufgabenträgern) und besitzen Schnittstellen zu anderen Organisationen und Aufgabenträgern.

Schäden entstehen aus den Unzulänglichkeiten des Organisationsaufbaus und den menschlichen Schwächen. Die Methoden des Social Engineerings greifen gezielt menschliche Schwächen wie Vertrauensseligkeit, Eitelkeit, Unfähigkeit oder Schwachstellen im Aufbau von Organisationen an. Hierdurch wird es möglich technische Sicherheitssysteme zu überwinden, indem bereits vorhandene Zugänge genutzt oder eigens für den Angreifer pseudoautorisierte Zugänge geschaffen werden. Die entstehenden Schäden sind jenen der technischen Gefahren vergleichbar. Die Anzahl der Sicherheitsverstöße ist jedoch zu 63% auf menschliches Fehlverhalten zurückzuführen.[309]

3.7. Rechtliche Gefahren

Rechtliche Gefahren ergeben sich aus den von den Gesetzgebern vorgegebenen Rahmenbedingungen, innerhalb der die Unternehmung agiert.[310] Insbesondere im Bereich der Wirtschaft und Informationstechnik, spielt der Gestaltungsspielraum der Legislative eine erhebliche Rolle, da durch das rasche Fortschreiten der Technologie viele Regeln geschaffen beziehungsweise fortentwickelt werden müssen. Weitere Gefahren ergeben sich aus Veränderungen der gesellschaftlichen Rahmenbedingungen und des damit verbundenen Rechtswandels, woran Informationssysteme angepasst werden müssen. Bei Nichtbeachtung dieser Spielregeln drohen der Unternehmung oder deren Mitarbeiter erhebliche zivilrechtliche sowie strafrechtliche Konsequenzen.

---

[309] Vgl. [Handelsblatt (2005); http://www.handelsblatt.com].
[310] Vgl. Müller, Klaus-Rainer (2003), S. 6.

Des Weiteren spielt die Rechtsverbindlichkeit sowie die Kausalität zwischen Tat, Schadensverursachung und Haftung eine wesentliche Rolle.[311] Verstöße gegen materielle Datenschutzbestimmungen ziehen Bußgelder von bis zu 250.000 € nach sich. Verstöße gegen Verfahrensvorschriften können mit bis zu 25.000 € bestraft werden. Neben diesen Sanktionen ist auch eine strafrechtliche Verfolgung materieller Verstöße möglich.[312] Scheinen die Bußgelder gegenüber Großunternehmen und den Gewinnaussichten gering, ist die strafrechtliche Verfolgung ein besseres Sanktionsmittel um das Gesetz durchzusetzen.

Die Rahmenbedingungen ergeben sich aus dem Grundgesetz (Art 1,2), dem Volkszählungsurteil, den Landesverfassungen, dem Bundesdatenschutzgesetz, der europäischen Datenschutzrichtlinie, dem Signaturgesetz, der Signaturverordnung, dem TDDSG, MDStV, EG-EKRL, u.a.. Weitere Vorschriften ergeben sich aus der Gewerbeordnung. Aus diesen Regelungen wird in Deutschland das Recht auf informationelle Selbstbestimmung hergeleitet.[313] Zunächst gilt ein Verbot, das durch Einwilligung des Betroffenen bzw. Gesetz aufgehoben werden kann.[314]

Die rechtlichen Gefahren umfassen, insbesondere Schutz- und Sorgfaltspflichten gegenüber Kunden, Mitarbeitern und der Unternehmung. Das Gesetz zur Kontrolle und Transparenz (KonTraG) im Unternehmensbereich macht die Vorstände oder Geschäftsführer persönlich für die Risikovorsorge, auch der IT, verantwortlich und haftbar. Wird ein Verstoß festgestellt gilt das Prinzip der Beweislastumkehr, die Führungsspitze muss nachweisen ordnungsgemäß gehandelt zu haben. Eventuell entfällt bei fahrlässigen Verstößen der Versicherungsschutz.[315] Im Hinblick auf IT-Haftungsfragen und Vorgaben wie den Sarbanes-Oxley Act und Basel II ist es für Unternehmen mehr denn je erforderlich die Risiken in allen (elektronischen) Geschäftsprozessen für Wirtschaftsprüfer nachweisbar zu bemessen

---

[311] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 4ff; S. 41ff; S. 53; S. 25.
[312] Vgl. Moos, Flemming (2006), S. 178ff.
[313] Vgl. Eckert, Claudia (2006), S. 13.
[314] Vgl. Fischer, Joerg K. (2008), S. 12f., vgl. Prof. Dr. iur. Roßnagel Universität Kassel auf dem Symposium Der Computer im 21. Jahrhundert. Die Informatisierung des Alltags. 21-22.03.05 in Zürich. Vortrag Datenschutz in einem informatisierten Alltag.
[315] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 90ff; vgl. Speichert, Horst (2007), S. 253; vgl. [Handelsblatt (2005); http://www.handelsblatt.com]; vgl. Buchner, Frank (2007), S. 80.

und zu minimieren.[316] Dafür ist das Entdecken von Schwachstellen ein erster wichtiger Schritt.[317]

Aus Geschäftsbeziehungen können sich Schutzpflichten zur sicheren Verwahrung der Daten des Geschäftspartners ergeben. Sofern sie sich nicht aus den Rahmenbedingungen des Wirtschaftsumfeldes ergeben können vertragliche Vereinbarungen getroffen worden sein. Diese Vereinbarung kann erhebliche Vertragsstrafen und Konsequenzen entfalten. Dies spiegelt sich im integrativen BIS wider.

Durch Lizenzrechtsverletzungen beispielsweise durch unberechtigte Installation von Programmen oder Urheberrechtsverletzungen können hohe Kosten entstehen. Des Weiteren sind Schadensersatzansprüche aus der sogar unbeabsichtigten Verteilung von Schädlingen möglich. Der Download von Inhalten, deren Besitz allein schon strafbar ist kann Konsequenzen für das Unternehmen nach sich ziehen. Nicht richtig angewandter Datenschutz kann von Mitbewerbern als Wettbewerbsverstoß geahndet werden. Der Datenschutz in der Privatwirtschaft ist im dritten Abschnitt des BDSG enthalten.[318] Hierbei handelt es sich gegenüber dem integrativen BIS um sekundäre Gefahren.

3.8. Sonstige Gefahren

Gefahren, welche nicht in eine der oben genannten Kategorien fallen, werden unter sonstige Gefahren gefasst. Dazu gehören bspw. Tricks innerhalb der Wirtschaftsspionage wie Verwendung von technischen Geräten zum Abhören oder die Erpressung[319] und das Wardriving[320]. Diese Gefahren werden durch Wireless Risks ergänzt, die sich aus der physischen Ungebundenheit der Übertragungswege ergeben.

3.8.1. Höhere Gewalt

Elementarereignisse wie Blitzschlag, Feuer, Überschwemmung und Erdbeben können den Betrieb einer Anlage erheblich beeinträchtigen. Deshalb ist eine

---

[316] Vgl. Speichert, Horst (2007), S. 256f; S. 264f; vgl. Schrey, Joachim in Gründer, Torsten (2007), S. 275ff.
[317] Vgl. Schrey, Joachim in Gründer, Torsten (2007), S. 275ff.
[318] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 456ff; vgl. Moos, Flemming (2006), S. 40.
[319] Vgl. Wilding, Edward (2006), S. 103ff.
[320] Vgl. Wilding, Edward (2006), S. 100f.

räumliche Trennung der Systeme notwendig. Demonstrationen und Streiks können den Betriebsablauf stören. [321]

3.8.2. Angriffstechniken

Die Angriffstechniken können in passive und aktive Angriffe unterteilt werden.[322] Passive Angriffe beschränken sich auf das Abhören von Informationen. Es werden keine aktiven Spuren hinterlassen, wie bspw. das durchprobieren von Passwörtern, dass von Protokollierungswerkzeugen aufgezeichnet werden könnte.

Die Verwendung von Systemwerkzeugen (wie ping und traceroute/tracert) ermöglichen es neben ihrem eigentlichen Zweck auch einem Angreifer sich einen Überblick über die Architektur des Zieles zu erarbeiten. Portscans ermöglichen es Rückschlüsse auf die aktivierten Dienste zu ziehen. Interessant sind hierbei die sogenannten Stealth-Scan-Techniken, die nicht den vollen TCP-Handshake durchführen und damit besser vor der Entdeckung durch Firewalls und Intrusion Detection Systems geschützt sind. Die Entdeckung eines Scans korreliert mit der Aggressivität, mit der er durchgeführt wird.[323] Spoofing im Sinne von Manipulation, Verschleierung oder Vortäuschung werden in der Informationstechnik Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität genannt. [324]

3.8.2.1. Social Engineering

„Social Engineers“ nutzen nicht primär zum softwaretechnischen Informationssystem gehörende Schnittstellen (Menschen), um in technisch unüberwindbare Informationssysteme einzudringen. Gegen dieses Konzept des Angriffs sind technische Sicherungen weitgehend sinnlos, da auf menschliche Schwächen oder Eitelkeiten abgestellt wird. Menschliche Schwächen sind beispielsweise mangelndes Wissen oder Bequemlichkeit.[325] Es gibt zahlreiche Konzepte des „Social Engineering“, hier werden nur einige dargestellt, da der menschlichen Fantasie und dem Erfindungsreichtum des „Social Engineers“ keine Grenzen gesetzt sind. Eine sehr

---

[321] Vgl. Eckert, Claudia (2006), S. 15.
[322] Vgl. Dridi, Fredj (2003), S. 55ff; vgl. Erickson, Jon (2006), S. 26.
[323] Vgl. Rey, Enno; Thumann, Michael; Baier, Dominick (2005), S. 22ff; 25ff.
[324] Vgl. Laudon, Kenneth, C.; Laudon, Jane, P. (2006); S. 347; vgl. [Freiling, Felix (2006); http://pi1.informatik.uni-mannheim.de].
[325] Vgl. Schneier, Bruce (2000), S. 266ff; vgl. Eckert, Claudia (2006), S. 22; vgl. Mitnick, Kevin; Simon, William (2003), 2003 S. 20ff.

einfache Methode ist das Shoulder-surfing. Hierbei wird eine Person bei ihrer Arbeit beobachtet. Dies ist an öffentlichen Plätzen leicht zu bewerkstelligen.[326]

Für einen erfolgreichen Social Engineering-Angriff werden Informationen über das Ziel benötigt. Die Möglichkeiten der Informationsbeschaffung bestehen für den Social Engineer in folgenden Techniken.

Legale Techniken wie bspw. die Analyse des Quellcodes der Homepage des Angriffziels. Die verwendeten Skripte und Kommentare können Auskunft über die Qualifizierung des Personals geben. Eventuell im Quelltext versteckte Kommentare und E-Mailadressen runden den Eindruck ab und liefern erste Angriffsstellen. Eine Webrecherche auf die Geschäftspartner der Unternehmung beispielsweise durch eine Suche nach allen Webseiten, die auf die Domain des Angriffszieles verweisen. Dies ergibt Kontaktadressen und mögliche Rollen für den Social Engineer. Abfragen bei Weborganisationen ergeben weitere Informationen, um beispielsweise den Verantwortlichen für den Webauftritt des Unternehmens zu ermitteln. Organisatorisch könnte der Befehl whois oder eine Abfrage bei Denic verwendet werden. Des Weiteren kann über geeignete Abfragen der IP-Bereich des Unternehmens sowie die Adresse des Mail-DNS und weiterer Server ermittelt werden. Das Ziel dieser legalen Techniken ist es, sich Informationen über Geschäftspartner, Verantwortliche, deren Namen, Telefonnummern und E-Mailadressen zu verschaffen.[327]

Die Grauzone umfasst bspw. eine Manipulation der Telefonanlage, sie ermöglicht es beliebige Informationen über die Rufnummernübermittlung des Telefons zu übertragen und damit den Anschein einer Firmenzugehörigkeit zu erwecken.[328]

Illegale Techniken sind bspw. das Eindringen auf das Firmengelände durch Täuschungsversuche in Form der Anstellung als Praktikant, das Eindringen zusammen mit der Putzkolonne, die Rückkehr mit den Firmenmitarbeitern aus der Mittagspause, das Fälschen von Mitarbeiterausweisen usw..[329] Das Garbage Diving ist ebenso eine beliebte Technik des Social Engineers. Die oft unsachgemäße Entsorgung von digitalen und nichtdigitalen Informationen/Medien ermöglicht es

---

[326] Vgl. [Barrett, Neil; http://www.it-im-unternehmen.de].
[327] Vgl. Mitnick, Kevin; Simon, William (2003), S. 185.
[328] Vgl. Mitnick, Kevin; Simon, William (2003), S. 243ff.; S. 308.
[329] Vgl. Mitnick, Kevin; Simon, William (2003), S. 376f.

durch Untersuchung der Abfälle an Informationen wie Telefonlisten, Zugangspasswörtern, Konfigurationen, Backup-Medien, Festplatten und Quellcodestücken zu gelangen.[330]

Eine weitere Vorgehensweise stellt der Identitätsdiebstahl dar. Als Identitätsdiebstahl engl. Identity Theft wird die missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte bezeichnet.[331] Das Ziel eines Identitätsbetrugs ist es, einen unrechtmäßigen finanziellen Vorteil zu erlangen oder den rechtmäßigen Inhaber der Identitätsdaten in Misskredit zu bringen (Rufschädigung) beziehungsweise durch erlangte geheime Informationen zu erpressen.[332]

Für einen Identitätsdiebstahl werden persönliche Daten wie Geburtsdatum, Anschrift, Führerscheinnummern, Sozialversicherungsnummern, Bankverbindungsdaten oder Kreditkartennummern entwendet, um eine ordnungsgemäße Identitätsfeststellung zu umgehen. Die missbräuchliche Nutzung kann zu finanziellem Schaden oder Straftaten führen, die im Namen des Opfers durchgeführt werden.[333] Die am häufigsten auftretenden Formen von Identitätsdiebstahl sind Kreditkartenbetrug und Bankbetrug. Nach einer Studie der Federal Trade Commission (FTC) im Jahr 2002 entstand in den Vereinigten Staaten von Amerika ein gesamtwirtschaftlicher Schaden von ca. 36.7 Milliarden US-Dollar. Diese Summe teilt sich in 32,9 Milliarden US-Dollar für Geschäftskunden und 3,8 Milliarden US-Dollar bei Privathaushalten auf.[334] Diese Kriminalitätsform wächst, wie Zahlen der FTC aus dem Jahr 2002 mit insgesamt 168.000 Anzeigen sowie 380.000 Beschwerden wegen Identitätsdiebstahls verdeutlichen.[335] Dies zeigt, dass Identitätsdiebstähle tatsächlich auftreten und eine Gefahr für integrative BIS darstellen.

Ein Identitätsdiebstahl kann erhebliche Auswirkungen auf den elektronischen Geschäftsverkehr haben. Nach den Urteilen des OLG Köln vom 06.09.2002, Az.: 19 U 16/02 und des Amtsgerichts Erfurt vom 14.09.2001, Az.: 28 C 2354/01 muss

---

[330] Vgl. Mitnick, Kevin; Simon, William (2003), S. 371.
[331] Vgl. United States Code (1998), 18, U.S.C. §2028.
[332] Vgl. [Hoofnagle, Chris Jay (2007); S. 98ff.]
[333] Vgl. Vgl. [Pfitzmann, Andreas (2007); http://dud.inf.tu-dresden.de].
[334] Vgl. [Silicon (2004); http://www01.silicon.de].
[335] Vgl. [Hoofnagle, Chris Jay (2007); S. 98ff].

bei Vertragsabschlüssen im Internet der Verkäufer beweisen, dass der Käufer identisch mit dem Account-Inhaber ist.[336]

„Phishing“ ist eine besondere Art des Identitätsdiebstahls durch gefälschte E-Mails. Ein „Phisher“ versucht durch gefälschte E-Mails oder Briefe andere dazu zu bringen, gefälschte Websites zu besuchen und dort persönliche Informationen wie Bankzugangsdaten, Kreditkartennummern oder Ähnliches einzugeben. „Phishing“ ist demnach eine häufige Variante des Identitätsdiebstahls. Umgangssprachlich wurde das „F“ durch ein „Ph“ ersetzt. Übertragen bedeutet hierbei „Fishing“, dass jemand nach persönlichen Daten „fisht“. Eine andere Erklärung des Wortes: „P“asswort f „ishing“. Die beim Opfer ankommenden E-Mails erwecken den Eindruck, dass sie von einer vertrauenswürdigen Stelle stammen. Diese sind oft bis auf kleine Fehler branchenüblich verfasst. Der Empfänger erhält z. B. eine E-Mail, in der er aufgefordert wird, seine Bankzugangsdaten zu verifizieren.[337] Die Absenderdaten (E-Mailadresse) und die Ziel-Seiten haben bei gut gemachten „Phishing-Attacken“ gefälschte URL-Namen, die ähnlich klingen wie die offiziellen Seiten, auf die Bezug genommen wird.

3.8.2.2. Veränderung der IP-Adressenauflösung

Dies ist eine Mischform aus technischer und organisatorischer Gefahr. Eine weitere Steigerung des „Phishing“ und „Social Engineerings“ ist gegeben, wenn die URL-Auflösung bzw. IP-Adressenauflösung manipuliert wird. Internetauftritte sind über ihre IP-Adresse definiert. Eine URL kann über das Nameserver-System einer IP-Adresse zugeordnet werden. Dieses System ist streng hierarchisch aufgebaut und sollte weltweit eindeutig sein. In dieses System kann böswillig eingegriffen werden.

Die Denic verwaltet die Zuordnung von IP-Adressen zu URLs für Deutschland. Für internationale Domains ist die Organisation Internic zuständig. Weltweit existieren in vielen Ländern ähnliche Organisationen. Beantragt man einen Domainnamen, wird die zuständige Organisation tätig und prüft, ob er bereits vorhanden ist. Ist er bereits vorhanden, dies ist beim „Phishing“ der Fall, kann die Domain

---

[336] Vgl. [Hoofnagle, Chris Jay (2007); S. 98ff].

[337] Vgl. Graf; Jürgen-Peter (2007): Zur Strafbarkeit des „Phishing". In: Mathis Hoffmann, Stefan Leible, Olaf Sosnitza (Hrsg.): Geistiges Eigentum im virtuellen Raum. Richard Boorberg Verlag, Stuttgart, München, Berlin, Hannover, Dresden, Weimar 2007, S. 173–184.

nur übertragen werden. Die Übertragung ist durch den möglichen Providerwechsel ein häufiger Vorgang. Für die Übertragung selbst werden ein Antrag eines Providers und eine Bestätigung verlangt. Dieses Vorgehen ist nicht sicher, wie das Beispiel von eBay zeigt. Die Domain des Auktionsanbieters eBay wurde durch geschickte Manipulation der vorhandenen Sicherheitsmaßnahmen und Konzepte des „Social Engineerings“ kurzfristig auf einen unberechtigten übertragen. [338]

3.8.2.3. Nameserver-Angriffe

Bei Nameserver-Angriffen, eine Art des IP-Hijacking, werden die Zuordnungstabellen von DNS-Servern für kurze Zeit geändert. Die Änderung ist meistens nicht mehr nachzuvollziehen.[339] Dadurch kann der Angreifer Anfragen an fremde Webseiten auf seine Internetpräsenz umleiten und dadurch an Informationen wie eingegebene Passwörter gelangen.

Schadenpotenzial

Mit den Methoden des „Social Engineerings“ können an sich technisch sicher geschützte Informationen erlangt werden bzw. Aktionen mit oder auf diese Informationen veranlasst werden. Die Schäden, welche durch den Missbrauch von Informationen, welche in einem integrativen BIS verwahrt und verarbeitet werden, sind denen der anderen Bereiche ähnlich. Der anzurichtende Schaden hängt von der Qualität der erlangten Informationen ab. Vorstellbar sind die Kündigung von Mitarbeitern, Übernahme von Produktentwicklungen, Verfälschung von Bilanzdaten, Zugang zum System, etc.. [340]

3.8.2.4. Brute-Force-Methode

Für viele Probleme gibt es keine effizienten Algorithmen. Der natürlichste Ansatz zur algorithmischen Lösung eines Problems besteht dann darin, alle potenziellen Lösungen durchzuprobieren. Brute Force („rohe Gewalt“) ist eine Lösungsmethode für schwere Probleme aus dem Bereich der Informatik und der Spieltheorie, die auf dem Ausprobieren aller (oder eines erheblichen Teils der in Frage kommenden) Varianten beruht. Diese Methode kann durch bekannte Teile oder Annahmen verfeinert werden.

---

[338] [Ad/c´t; http://www.heise.de].
[339] Vgl. [Freiling, Felix (2006); http://pi1.informatik.uni-mannheim.de].
[340] Vgl. Mitnick, Kevin; Simon, William (2003), S. 376f.

Eine Annahme könnte sein, dass es sich beispielsweise bei einem Passwort um ein Wort aus einer Sprache handelt. Dadurch kann eine Wörterbuchattacke durchgeführt werden. Diese würde erheblich schneller zum Ergebnis führen. Mancher Brute-Force-Angriff bedient sich außerdem auch einer Wortliste, in welcher besonders häufig vorkommende Passwörter enthalten sind, um schneller Treffer erzielen zu können.[341] Der vielseitigen Anwendbarkeit steht der immense Zeitaufwand gegenüber.[342]

In der Spieltheorie bezeichnet man mit der Brute-Force-Methode eine Strategie, in der der Variantenbaum bis zu einer gewissen Tiefe vollständig analysiert wird. Eine Bewertungsfunktion für jede der dabei auftretenden Stellungen dient dabei zur Entscheidungsfindung für den besten Zug. Der Aufwand für die Brute-Force-Methode wächst exponentiell mit der verwendeten Maximaltiefe. Die Brute-Force-Methode kann mit den verschiedensten Methoden verfeinert werden, was durch das genannte exponentielle Wachstum zu erheblichen Verbesserungen führen kann. Eine übliche Verbesserung ist die Alpha-Beta-Suche. Wird ein Zug in einer bestimmten Tiefe durch einen Gegenzug widerlegt, dann ist es nutzlos, nach besseren Widerlegungen zu suchen. Eine andere übliche Methode ist, ab einer gewissen Tiefe nur noch „forcierende“ Züge zu betrachten. Brute-Force-Angriffe sind leicht automatisiert durchführbar, was beispielsweise bei schwachen Passwörtern zu einem erheblichen Sicherheitsrisiko führt.

3.8.2.5. Kryptoanalyse

„Kryptoanalyse und Kryptographie bilden die wesentlichen Teilgebiete der Kryptologie. Entgegen dieser eindeutigen Abgrenzung werden die Begrifflichkeiten Kryptologie und Kryptographie oft synonym verwendet.“[343] Bei der Kryptoanalyse handelt es sich um Verfahren zur Entschlüsselung von verschlüsselten Informationen. Werden alle möglichen Schlüssel nacheinander durchprobiert, handelt es sich um einen Brute-Force-Angriff. Die Reihenfolge wird gegebenenfalls nach der Wahrscheinlichkeit ausgewählt. Diese Methode ist auch bei modernen Verschlüsselungsverfahren sinnvoll, wenn von der Verwendung eines relativ schwachen

---

[341] Vgl. Schwenk, Jörg (2005), S. 11.
[342] Vgl. Schwenk, Jörg (2005), S. 11.
[343] [Jahnke, Bernd (2008); http://www.enzyklopaedie-der-wirtschaftsinformatik.de]

Passwortes ausgegangen werden kann.[344] Des Weiteren nutzen Kryptoanalytiker Schwachstellen der verwendeten Algorithmen und den Aufbau der verwendeten Sprache, um den Entschlüsselungsprozess abzukürzen. Theoretisch sichere Verfahren werden dadurch einfacher angreifbar. Über die Methoden der Kryptoanalyse könnte eine eigene Ausarbeitung angefertigt werden. Nachfolgend werden einige wichtige Angriffs- und Analysemethoden der Kryptoanalyse aufgeführt und so fern nicht aus anderen Teilen der Arbeit bekannt kurz beschrieben.

Wörterbuch-Angriff: Alle Schlüssel aus Passwortsammlungen werden durchprobiert. Bei einem Wortschatz von 50.000 Wörtern pro Sprache können auf handelsüblichen Rechnern viele Sprachen innerhalb weniger Sekunden getestet werden. Ein Wort als Schlüssel ist deshalb sehr unsicher.

Seitenkanalattacke: Der Angreifer versucht, außer dem Klartext, dem Chiffrat oder dem Schlüssel zunächst ebenso andere Daten zu erfassen und daraus Informationen über den verwendeten Algorithmus und Schlüssel zu gewinnen.

Lineare Kryptoanalyse: Das Verfahren basiert auf der linearen Annäherung an den wahrscheinlichsten Schlüssel zum cracken von Blockverschlüsselungsverfahren.

Differentielle Kryptoanalyse: Es werden zwei Klartexte gewählt, welche sich nur in bestimmten, vorher festgelegten Stellen unterscheiden. Auf diese wird das Verschlüsselungsverfahren angewendet. Da diese Verfahren in der Regel aus mehreren Runden bestehen, vergleicht man den Klartext in jeder Runde mit dem verschlüsselten Ergebnis. Dabei sollten Muster in der Differenz zu erkennen sein, um aus Ihnen den verwendeten Schlüssel herzuleiten oder zumindest die Eigenschaften des Schlüssels vorherzusagen.

SAT-Angriff: Der Algorithmus wird auf eine SAT-Instanz reduziert. Danach werden die 1-literalen Klauseln für den Klartext und den Ciphertext hinzugefügt. Anschließend wird die Instanz mit einem SAT-Solver gelöst und die Werte für die Key-Bits extrahiert.

Die Brute-Force-Methode wurde bereits, der Man-In-The-Middle-Angriff wird später beschrieben. Die Kryptoanalyse kann durch Rainbow-Tabellen verfeinert werden. Hierzu existieren Datenbanken, in denen bereits entschlüsselte Passwör-

---

[344] Vgl. [Fox, Dirk (2002); http://www.secorvo.de].

ter hinterlegt werden. Technisch wird zu einem Hashwert ein funktionierendes Passwort hinterlegt.

3.8.2.6. Hopping

Der Angreifer crackt zunächst unwichtige Systeme die sich an weltweit verteilten Orten befinden. Die Orte sollten sich in unterschiedliche Zeitzonen und unterschiedlichen Sprachgebieten befinden sowie verschiedene Gesetzeslagen aufweisen. Der Cracker springt durch den Einsatz von „Redirectors“ von Land zu Land, bevor er den eigentlichen Angriff startet. Nach diesem Schema besteht eine hohe Wahrscheinlichkeit anonym zu bleiben welches die Grundvoraussetzung ist, um sich einer Strafverfolgung zu entziehen, insofern überhaupt Gesetze übertreten wurden. Zivilrechtliche Ansprüche gegenüber Unbekannten durchzusetzen ist schwierig.[345]

3.8.2.7. Man-In-The-Middle-Angriff

Diese Angriffsform wird auch Janusangriff genannt. Der Angreifer befindet sich physikalisch oder logisch zwischen Kommunikationspartnern und hat dadurch Kontrolle über den Datenverkehr zwischen den Netzwerkteilnehmern. Er kann dadurch die Datenströme einsehen und manipulieren. Die Kommunikationspartner merken davon nichts. Sind die Datenströme unverschlüsselt, kann der Angreifer die Informationen unproblematisch mitlesen. Sind sie verschlüsselt, liest er den Schlüsseltext mit.[346]

Die Stellung des Man-In-The-Middle kann bspw. auf folgende Arten erreicht werden: Es besteht ein physikalischer Zugang zu den Netzwerken. Es besteht die Kontrolle über einen Router. Manipulierte ARP-Tabellen der Opfersysteme leiten den Datenverkehr durch ein vorherdefiniertes System. Die Netzwerktopologie ist die Busstruktur, damit kommen alle Pakete bei jedem Rechner im Bus an. Das Vorspiegeln eines falschen DHCP-Servers, durch eine falsche Gateway-Adresse zum Internet kann die Kommunikation durch einen Rechner des Angreifers leiten. Das Vortäuschen eines WLAN Access Points. Durch DNS-Täuschung kann eine falsche Zieladresse für die Internet-Kommunikation vorgegeben werden. Durch

---

[345] Diese Form des Hoppings unterscheidet sich vom „Island Hopping“ dadurch, das hier kein „Hopping“ über einen Host im internen Netz sondern über Länder verteilt vorgenommen wird. Vgl.

[346] Vgl. Eckert, Claudia (2007), S. 417ff.

Manipulation der host-Datei können Eingaben der echten URL in gefälschte IP-Adressen aufgelöst werden.[347]

3.8.2.8. Botnetz

Ein Bot, der Begriff stammt von robot ab, ist ein Computerprogramm, das möglichst autonom sich wiederholende Aufgaben erledigt. Verfügen Bots über die Fähigkeit untereinander zu kommunizieren, entsteht ein Botnetz. Illegal entsteht es durch die Infektion von sehr vielen Rechnern, welche dann Zombies genannt werden. Mit einem Botnetz kann ein Angreifer, der als Botmasters dem Netz Befehle erteilt, dieses für einen DDoS-Angriffs oder das Versenden von Spam verwenden. Werden diese DDoS-Attacken von vielen Bots im Netz gleichzeitig ausgeführt, so werden auf dem Ziel-Rechner Dienste gestört.[348]

3.9. Interdependenzen der einzelnen Gefahrenarten

Die aufgezeigten Sicherheitslücken sind für sich alleine bereits mehr oder weniger geeignet die Authentizität, Vertrauenswürdigkeit oder Sicherheit von Informationssystemen und der gesamten Unternehmensinfrastruktur zu beeinträchtigen. Wichtig ist hierbei die Erkenntnis, dass erfolgreiche Angriffe, die Unternehmen bedrohen, in der Form ausgeführt werden können, dass auch scheinbar unbedeutende Sicherheitslücken aus den verschiedenen Bereichen miteinander kombiniert Zugang zu wesentlichen Daten des Unternehmens ermöglichen. Nicht die einzelne Sicherheitslücke stellt das Problem dar, sondern die Kompromittierung der Gesamtstruktur. Durch die Kompromittierung wird der Zugang zum Gesamtsystem hergestellt und die Vertrauenswürdigkeit sinkt gegen Null. In der Praxis sinkt das Vertrauen bisher noch nicht so drastisch, jedoch wurden Sicherheitslücken bisher von Unternehmen lieber vertuscht als die Imageschäden in Kauf zu nehmen.[349]

Ob Entscheidungsträger sich darüber bewusst sind, ob sie Vertrauen in die Daten der Informationssysteme setzen können und wie dies ihre Entscheidung beeinflusst, kann ohne entsprechende Datenbasis nicht prognostiziert werden. Nach menschlichem Ermessen müsste ein Bekannt werden dieses Umstandes den Entscheidungsfindungsprozess der Führungskraft beeinflussen. Den Informationssys-

---

[347] Vgl. Eckert, Claudia (2007), S. 417ff.
[348] Vgl. Joos, Richard; Jorberg, Randolf; Gönnemann, Axel (2008), S. 9.
[349] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

temen kommt zugute, dass Entscheidungsträger sich nicht über die Risiken der Authentizität und Vertrauenswürdigkeit ihrer entscheidungsrelevanten Daten bewusst sind. Wenn sie bewusst werden, fehlt oft das Wissen über die Zusammenhänge zwischen Authentizität, Vertrauenswürdigkeit und Informationssystemlücken. Auch verschweigen IT-Verantwortliche gerne die Konsequenzen der Risiken.[350]

Angreifer verbinden geschickt einzelne unscheinbare Lücken, um zum gewünschten Ergebnis zu kommen. Insgesamt gibt es bei Systemen der Größenklasse integrativer BIS viele undokumentierte Wege um bestimmte Aktionen auszulösen, die in ihrer Gesamtheit einen Angreifer zum Ziel bringen.

3.10. Gegner von Systemsicherheit

Hacker, Cracker, Scriptkids[351], Einzeltäter, Vereinigungen, Mitarbeiter, Regierungsorganisationen, White Hats/Black Hats, politisch motivierte Täter und Wettbewerber/Wirtschaftsspione können Gegner von Systemsicherheit sein. Firmen und Hochschulen, sowie alle Einrichtungen welche über große Rechenleistung und Speicherkapazitäten sowie Breitband Netzwerkverbindungen (intern oder extern) verfügen oder von denen der Angreifer glaubt, dass sie über diese Mittel verfügen, sind für diese besonders interessante Ziele.[352]

IT-Sicherheit ist einfacher zu gewährleisten oder zu bewerten, wenn die Motive potenzieller Angreifer und deren Fähigkeiten dem für die Sicherheit Verantwortlichen bekannt sind. Erkannt wurden bisher Sucht oder Besessenheit, Neugierde, Anerkennung als soziale Motivation, Langeweile, Machtgefühl, technische Motivation, Robin-Hood-Syndrom, politische und ideologische Motivation, finanzielle Motivation, Rache sowie sexueller Missbrauch. Dabei gilt die finanzielle Motivation als einer der häufigsten Beweggründe für professionelles „Cracking“.[353]

Im IT-Bereich speziell der Aufgabenstellung IT-Sicherheit lassen sich den Akteuren bestimmte Rollen innerhalb des Gesamtsystems zuordnen. Zunächst kann

---

[350] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2

[351] Vgl. Eckert, Claudia (2006), S. 19f.; vgl. Godschalk, David (2007), S. 55ff.; vgl. Schumacher, Markus; Rödig, Utz; Moschgath, Marie-Luise (2003), S. 71ff; vgl. Görtz, Horst; Stolp, Jutta (1999), S. 33f.

[352] Vgl. [Briele, Marc (2004); http://idw-online.de]; Schifreen, Robert (2006); S. 7ff.

[353] Vgl. Schumacher, Markus; Rödig, Utz; Moschgath, Marie-Luise (2003), S. 95ff; vgl. Eschweiler, Jörg (2006), S. 49ff.

grob zwischen Verteidigern und Angreifern unterschieden werden. Da es sich bei dem Bereich IT-Sicherheit um ein sehr komplexes und weitläufiges Feld handelt benötigt man über die Standardsicherung hinaus Spezialisten sogenannte Verteidiger, welche von ihrer Institution beauftragt die Integrität, Authentizität und Vertrauenswürdigkeit der IT gewährleisten sollen. Diese Gruppe von Verteidigern wird im ursprünglichen Sinn als Hacker bezeichnet. Es handelt sich um eine Person mit Fähigkeiten im Umgang mit Computern und deren Programmierung. Das Wort Hacker wurde im Laufe der Zeit negativ besetzt und wird von Laien häufig als Synonym für den böswilligen Angreifer den sogenannten Cracker/Blackhat gebraucht. Spezialisten die sich der Bewahrung der Systemsicherheit widmen nennen sich konträr zu den Blackhats auch Whitehats.[354]

Die Einteilung der Angreifer kann in Gruppentäter oder Einzeltäter vorgenommen werden. In der Gruppe der Einzeltäter finden sich diejenigen, welche vollständig eigenständig agieren. Ihre Motive sind hauptsächlich Geldgier, Ruhmsucht und Anerkennungsstreben gegenüber Gleichgesinnten. Die Fähigkeiten der Gruppen können in einer Wissenspyramide aufgespannt werden. Hier können auch Insider der Betreffenden Organisation eingeordnet werden, welche aus Neugier, Enttäuschung oder Geldgier Zugang mit den Mitteln eines Crackers suchen. Die Gruppentäter sind weit komplexer organisiert als die Einzeltäter. Es kann sich um kleine Gruppen bis hin zu Regierungsorganisationen und Wettbewerber handeln. Ausstattung und Fähigkeiten dieser Gruppen variieren je nach verfolgtem Ziel und Mittelausstattung. Die unten beschriebene Wissenspyramide und die darauf folgende Mittelpyramide können auf Gruppentäter angewandt werden. Auch zu dieser Gruppe können Insider gehören die sich zur Erlangung eines Ziels zusammengeschlossen haben.

Eine weitere wichtige Gruppe bilden Vereine, wie der Chaos Computer Club (CCC). Diese Vereinigungen haben vordergründig das Ziel Systemsicherheit zu gewährleisten. Die Methoden umfassen auch fragwürdige Methoden wie das Beispiel des CCC in Bezug auf den Nedap-Hack oder die angebliche Veröffentlichung des Fingerabdrucks von Innenminister Wolfgang Schäuble zeigen.[355]

---

[354] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

[355] Vgl. [Wijvertrouwenstemcomputersniet (2007)]; [Zeit Online: „Schäubles Zeigefinger gehackt“ (2008)]

Unternehmen spielen in diesem Bereich ebenfalls eine Rolle. Sie beschäftigen eventuell interne und externe Abteilungen, die sich mit IT-Sicherheit auseinandersetzen, um einen Wettbewerbsvorteil gegenüber der Konkurrenz zu erarbeiten. Industriespionage bedeutet die Ausforschung eines Unternehmens durch mindestens ein anderes Unternehmen.[356] Ob das Kriterium konkurrierendes Unternehmen erfüllt sein muss ist umstritten, im Kern jedoch nicht notwendig. Durch Industriespionage können Konkurrenzunternehmen an wertvolle Informationen gelangen.

Das japanisch Ministery for international Trade and Industry schult deshalb Vertreter japanischer Firmen in Abwehrtaktiken.[357] Die Wirtschaftsspionage unterscheidet sich dadurch von der Industriespionage, dass der staatliche Nachrichtendienst eines Landes, dessen Unternehmen gezielt bei der Beschaffung von Informationen behilflich ist.[358] Das FBI schätzt den Verlust der USA durch Spionage auf 7,5 Milliarden Dollar jährlich.[359]

Wissenspyramide der Gegner von Systemsicherheit

Die Basis dieser Pyramide bilden die Skriptkids, welche noch recht unerfahren sind und die mit Standardtools meist automatisierte Angriffe durchführen. Die Standardtools sind regelrechte Baukästen für technische Gefahren. An der Spitze der Pyramide befinden sich Cracker, welche über tief greifende Kenntnisse in mehreren Betriebssystemen, Netzwerkprotokollen, Programmiersprachen und Erfahrung im Aufspüren und Ausnutzen auch neuer Sicherheitslücken verfügen.

Die Mitarbeiter entsprechender Regierungsorganisationen müssen ebenfalls an der Spitze der Pyramide eingeordnet werden. Dazwischen befinden sich viele Sonderfälle. Die meisten Mittel für die Kompromittierung von IT-Sicherheit liegen bei entsprechenden Regierungsorganisationen oder entsprechend aufgestellten Unternehmen. Skriptkids können über verhältnismäßig viel Geld verfügen, werden aber in der Regel nicht an oben genannte heranragen. Cracker arbeiten beispielsweise für Geld, spezielle Aufträge und aus Rache. Skriptkids verfolgen den wahllosen Easy Kill und Ruhm unter ihres Gleichen.

---

[356] Vgl. [Landesamt für Verfassungsschutz Baden-Württemberg (2006); http://www.Verfassungsschutz.bayern.de]; S. 9.
[357] Vgl. Hummelt, Roman (1997), S. 47.
[358] Vgl. [Winkels, Heinz-Michael (2004); http://www1.logistik.fh-dortmund.de]; S. 4.
[359] Vgl. Hummelt, Roman (1997), S. 47.

3.11. Schadenszenarien

Unter einem Schadenszenario ist der mögliche Ablauf von Schadensereignissen zu verstehen.[360] Um ein Schadenszenario zu entwerfen sind die Randbedingungen zu klären, unter denen sich Schäden entwickeln können. Szenarien erhalten dabei in Fällen, in denen es aus wirtschaftlichen, technischen oder ethischen Gründen nicht möglich ist reale Daten zu gewinnen, erhöhte Bedeutung.[361]

Folgende Tabelle ermöglicht die Darstellung von Schadenszenarien in tabellarischer Form. Die erste Spalte „Szenario" enthält die typischen Schadensfälle die bei der Verwendung von Informationssystemen anfallen. Die zweite Spalte „Folge" klassifiziert die Auswirkungen der Schadensfälle in die Kategorien Unversehrtheit von Menschen, Aufgabenerfüllung, Handlungsfähigkeit, Finanzen, Image, Strafen, Wettbewerbsfähigkeit, Unternehmensstrategie, sowie Nacharbeit und Restaurierbarkeit. Die dritte Spalte „Dauer in Arbeitstagen" gibt an wie lange sich der Schadensfall auswirkt. Die letzte Spalte kann mit einer „Bemerkung" ergänzt werden.

Szenario	**Folge**	**Dauer in Arbeitstagen**				**Bemerkung**
Ausfall des Systems		0,5	1	2	>3	
	M					
	A					
	H					
	F					
	I					
	S					
	W					
	U					
	N					
Fehlfunktion	M					
	A					
	H					
	F					
	I					
	S					
	W					
	U					
	N					

[360] Vgl. Leidinger, Bernhard J.G. (1998), S. 14ff.
[361] Vgl. Bauernfeind, Markus (2007), S. 12.

Fehlbedienung	M					
	A					
	H					
	F					
	I					
	S					
	W					
	U					
	N					
Datenverfälschung durch Manipulation	M					
	A					
	H					
	F					
	I					
	S					
	W					
	U					
	N					
Datenverfälschung durch technische Fehler	M					
	A					
	H					
	F					
	I					
	S					
	W					
	U					
	N					
Einsichtnahme Unberechtigter in vertrauliche Daten (Unternehmensstrategie, Forschungsergebnisse, neue Produkte)	M					
	A					
	H					
	F					
	I					
	S					
	W					
	U					
	N					
Einsichtnahme Unberechtigter in vertrauliche Daten (personenbezogene Daten)	M					
	A					
	H					

	F					
	I					
	S					
	W					
	U					
	N					
Veröffentlichung personenbezogenen Daten	M					
	A					
	H					
	F					
	I					
	S					
	W					
	U					
	N					
Unechte Daten (Identitätsdiebstahl)	M					
	A					
	H					
	F					
	I					
	S					
	W					
	U					
	N					
Legende: M = Unversehrtheit von Menschen A = Aufgabenerfüllung H = Handlungsfähigkeit F = Finanzen I = Image S = Strafen W = Wettbewerbsfähigkeit U = Unternehmensstrategie N = Nacharbeit und Restaurierbarkeit						

Tabelle 3: Schadenszenarien [362]

Aus dem Schadensmanagement des Versicherungsmanagement können weitere Methoden zur Ermittlung und Darstellung des Schadenszenarios verwendet wer-

[362] In Anlehnung an: Müller, Klaus-Rainer (2003), S. 47ff.

den. Beispielsweise können hier die Ausfalleffektanalyse, PAAG (Methode zur Nutzung des Wissens interdisziplinärer Expertenteams), Störfall- bzw. Ereignisablaufanalyse sowie die Fehlerbaumanalyse genannt werden.[363] Die Ermittlung von Schadensszenarien und Durchführung von Planspielen führt in der Praxis bereits zu risikomindernden Maßnahmen.[364]

4. Sicherheitsmaßnahmen

In diesem Kapitel werden Methoden der Gefahrenabwehr dargestellt. Die Klassifizierung der Schutzmaßnahmen (Risikomanagementmaßnahmen) folgt der Einteilung aus dem vorigen Kapitel. Es werden einzelne Vorgehensweisen vorgestellt, welche geeignet sind, Gefahren abzuschwächen.

4.1. Exkurs: Materielle Welt vs. digitale Welt

In der nicht elektronischen Welt gibt es bewährte Konzepte um Vertrauen, Vertrauenswürdigkeit, Identität, Authentifizierung und Sicherheit herzustellen.[365] Der Besitz und die persönliche Sicherheit des Einzelnen wird in der „realen Welt“ durch physische Sicherungsmaßnahmen zum Beispiel dem verschließen der Räumlichkeiten gewährleistet. Dies ermöglicht nur denjenigen Personen Zugriff, die entweder berechtigt sind oder die durch einen Berechtigten eingelassen werden. Die Nutzung materieller Güter kann somit auf eine bestimmte Personengruppe beschränkt werden.

Auch dieses Konzept hat Mängel, man denke an die entsprechenden Straftatbestände wie Einbruch (§ 242 StGB) oder Raub (§ 249 StGB). Überträgt man dieses Konzept auf eine Unternehmung, kann man es mit dem Schlagwort Zugangskontrolle umschreiben. Diese Kontrolle kann zum Beispiel durch einen Pförtner (Sicherheitsdienst) am Eingangstor gewährleistet werden. Tresore oder speziell gesicherte Räume dienen der sicheren Aufbewahrung von wertvollen Gütern oder Unterlagen. Transferiert man unter diesen Rahmenbedingungen Werte, wird dies vorwiegend durch einen Sicherheitstransport realisiert.[366]

---

[363] Vgl. Leidinger, Bernhard J.G. (1998), S. 23.
[364] Vgl. Leidinger, Bernhard J.G. (1998), S. 26.
[365] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[366] Vgl. Pohlmann, Norbert (2004), S. 28.

Die Identität einer Person wird in der „realen Welt“ durch die Merkmale Vorname, Nachname, Geburtsort, Geburtsdatum, Wohnort sowie die Merkmale deren Eltern eindeutig identifizierbar. Diese Daten sind in der Geburtsurkunde hinterlegt, Standesämter erfassen diese Informationen und leiten sie an Einwohnermeldeämter weiter, welche darauf basierend Ausweise herausgeben. Die Ausweisproblematik und deren Fälschungssicherheit kann an der aktuellen Diskussion der Einführung biometrischer Merkmale auf Ausweisen zur eindeutigen Identifikation der Person erahnt werden.

Informationen werden über verschlossene Briefumschläge ausgetauscht, diese können durch die Hände Dritter gehen und es ist gewährleistet, dass solange der Umschlag unversehrt ist, die Nachricht ihren Vertraulichkeitsstatus behält. Eigenhändige Unterschriften versichern nach §129 BGB die Verbindlichkeit eines signierten Schriftstücks oder dessen Urheber. Amtssiegel steigern das Vertrauen in diese Verbindlichkeit um ein Vielfaches.[367]

In der „digitalen bzw. elektronischen Welt“ versucht man die Konzepte der „realen Welt“ ebenso anzuwenden um Vertrauenswürdigkeit, Identität, Authentifizierung und Sicherheit herzustellen, dabei treten Probleme auf die in der „normalen Welt“ in dieser Form nicht zu finden sind.[368]

Die Sicherung des Besitzes und der persönlichen Sicherheit ist in der „digitalen Welt“ nicht mehr durch verschließen der Güter zu gewährleisten. In einer „elektronischen Welt“ sind Güter häufig immateriell. Immaterielle Güter können sehr leicht kopiert und vervielfältigt werden. Eine Kontrolle über den Zugang und die Weitergabe ist nur durch Digital-Rights-Management-Konzepte zu gewährleisten, die sich derzeit noch nicht bewährt haben. Transferiert man immaterielle Güter (Informationen, urheberrechtlich geschützte Werke etc.) so kann sobald der Transport über öffentliche Wege (Internet) führt der Inhalt solange sie ungeschützt sind eingesehen werden. Konzepte für den Transfer von Gütern und Informationen in der „elektronischen Welt“ müssen Verfahren bereitstellen, welche es erlauben diese vor dem Einblick Dritter zu bewahren.

---

[367] Vgl. Pohlmann, Norbert (2004), S. 28; vgl. Eckert, Claudia (2006), S. 11.

[368] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 22ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

Identität ist in der „realen Welt“ durch die Einzigartigkeit der Person und deren Ausweis zum großen Teil gewährleistet. In der digitalen Welt kann sich jeder eine Kopie des „Ausweises“ verschaffen, die „reale Person“ tritt nicht in Erscheinung. Es gilt somit Methoden zu verwenden, welche eine Identitätstäuschung vereiteln. Ein Ansatz könnten hierbei Hash-Funktionen aus dem Bereich Kryptografie bilden.[369]

Vertrauen ist in der „elektronischen Welt“ beispielsweise beim Abschluss von Verträgen genauso notwendig wie in der „realen Welt“. Das Problem liegt hierbei in der Flüchtigkeit und leichten Veränderbarkeit digitaler Dokumente. Ansätze dies zu gewährleisten werden durch Zertifizierungseinrichtungen vorgestellt. Ein Dritter bestätigt hierbei durch geeignete Unterschrift (Zertifikat) die Echtheit eines Dokuments. Technisch wird hierbei eine Form der Kryptografie angewandt. Insbesondere ist die vertrauliche Kommunikation zu gewährleisten. Hier muss eine Art Briefumschlag verwendet werden. E-Mails hingegen verhalten sich wie Postkarten. Der Briefumschlag ist in der „digitalen Welt“ viel komplexer, er besteht aus Verschlüsselungsalgorithmen, deren Wirksamkeit bisher nur von begrenzter Dauer ist.

Ähnlich einem Telefonat mit dem Telefon existiert auch in der digitalen Welt die Möglichkeit der IP-Telefonie. Auch hier ist die Verbindung analog zu E-Mails ungeschützt. Die Dauer der Vertraulichkeit einer Nachricht wird in der „digitalen Welt“ durch den Fortschritt der Leistungsfähigkeit von Rechnern und der Entwicklung neuer mathematischer Methoden zur Faktorzerlegung bestimmt. In diesem Umfeld arbeiten Business Intelligence Systeme.[370]

4.2. Technische Maßnahmen

Die Unterscheidung von technischen und organisatorischen Maßnahmen ist vom Blickwinkel des Betrachters abhängig. In diesem Kapitel werden Programme die selbstständig Bedrohungen[371] vermindern und in das System integriert (installiert) werden, den technischen Maßnahmen zugeordnet. Es wird hierbei nicht verlangt,

---

[369] Vgl. Schwenk, Jörg (2005), S. 11; vgl. [Fox, Dirk (2002); http://www.secorvo.de].
[370] Vgl. Pohlmann, Norbert; Blumberg Hartmut (2004), S. 30; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 5.
[371] Vgl. Eckert, Claudia (2006), S. 14.

dass es sich um Hardware handeln muss, Software kann in diesem Sinne ebenso Technik sein.

Computerprogramme welche dazu dienen nach Sicherheitslücken zu suchen und diese aufzuzeigen oder zu schließen werden als Sicherheitssoftware bezeichnet. Es handelt sich um Software, die auf dem betroffenen System selbst oder auf einem dritten System installiert ist und vorgegebene Ziele auf Bedrohungen überprüft und diese wenn möglich beseitigt. Im Folgenden werden die wichtigsten Werkzeuge vorgestellt.

4.2.1. Scanner

Als Scanner werden Programme bezeichnet, deren Bestimmung es ist Vorgänge nach definierten Regeln zu durchforsten. Im Idealfall kann zusätzlich zu den fest definierten Regeln eine Heuristik zur Bedrohungsanalyse integriert sein. Das englische Wort Scanner bedeutet, Abtaster, Beobachter, Leser oder Radarantenne. Die Übersetzung des Wortes weckt sehr gute Assoziationen zur Funktionsweise eines Scanners. Das bekannteste Werkzeug ist der Virenscanner der auch als Antivirenprogramm bezeichnet wird.

Ein Antivirenprogramm ist eine Software, die ihr bekannte Schädlinge wie bspw. Computerviren, -Würmer und Trojaner aufspüren, blockieren und gegebenenfalls beseitigen soll. Diese allgemeingültige Definition ist nicht vollständig, da moderne Virenscanner über Heuristiken verfügen, welche auch unbekannte Schädlinge aufgrund von Ähnlichkeiten zu bekannten Übeltätern oder bestimmten Regeln zu erkennen versuchen. Die Bezeichnung Antivirenprogramm oder Virenscanner ist insofern unvollständig, da auch andere Schädlinge erkannt werden können.[372]

Um schädliche Software zu erkennen, hat jeder Virenscanner eine Liste mit Beispielen aller ihm bekannten Viren und anderer schädlicher Software („Virensignaturen" oder „Virendefinitionen"), mit der er die zu überprüfenden Dateien vergleicht. Stimmt eine Datei oder ein Teil mit einem Beispiel aus der Liste überein, werden Schritte zur Neutralisierung und gegebenenfalls zur Reparatur der infizierten Datei und zur Beseitigung der schädlichen Software unternommen.

Da ständig neue Viren und Würmer programmiert und in Umlauf gebracht werden, müssen die entsprechenden Listen ständig aktualisiert werden. Viele Scanner

---

[372] Vgl. Munnelly, Brendan; Holden, Paul (2005), S. 117.

unterstützen deshalb automatische Aktualisierungsmethoden. Moderne Betriebssysteme warnen den Anwender bei nicht aktuellen Virendefinitionen.

Das Scannen von Dateien kann auf zwei Arten erfolgen: Einmal haben nahezu alle Antivirenprogramme die Möglichkeit, im Hintergrund aktiv zu sein und alle Dateien und Programme, auf die zugegriffen wird, hinsichtlich schädigendem Inhalt zu überprüfen. Hierbei tritt ein Performanceverlust des Systems auf, der jedoch für sich alleine nicht usability kritisch ist. Zum zweiten kann ein gezieltes Durchsuchen von Dateien oder Datenträgern durchgeführt werden. Findet ein Scanner schädliche Software, wird je nach Einstellung eine Warnung an den Benutzer ausgegeben oder eine vordefinierte Aktionsfolge ausgelöst. Die möglichen Optionen reichen von einem Löschen der infizierten Datei über einen Reparaturversuch bis hin zur Isolierung der Datei. Überlässt man dem Nutzer die Auswahl, so kann es vorkommen, dass der Anwender nichts unternimmt, da er die Datei benötigt und somit das System infiziert wird.

Virenscanner, die über ein Netzwerk gestartet werden haben die Besonderheit, dass sie helfen können, wenn das System selbst keinen Virenscanner installiert hat bzw. das System bereits infiziert ist oder eine bestimmte Datei mit verschiedenen Scannern zu testen ist.

Erfolgswahrscheinlichkeit

Ein Virenscanner kann nicht alle Schädlinge erkennen, da neue oder kaum verbreitete Schädlinge nicht in den Definitionen enthalten sind. Zwar verfügen einige Virenscanner über die Möglichkeit, auch nach allgemeinen Merkmalen zu suchen, jedoch sind diese Lösungen bisher unzureichend. Eine weitere Gefahr besteht darin, dass ein Angreifer für einen Computer maßgeschneiderte Schädlinge erstellt, die nur diesen bestimmten Rechner infizieren – von diesem Virus wird der Hersteller der Virenscanner kaum erfahren, weshalb ein Virenscanner diesen auch nicht erkennen kann. Ein Virenscanner kann als Ergänzung zu allgemeinen Vorsichtsmaßnahmen verwendet werden. Der Mensch als Aufgabenträger wird von seiner Verantwortung nicht entbunden sondern unterstützt.

Neue Schädlinge weisen die Fähigkeit (Payload) auf, Sicherheitssoftware auf infizierten Rechnern abzuschalten. Ist die schädliche Software gestartet worden wird der Scanner vom Schädling deaktiviert. Neue Virenscanner werden deshalb gegen Abschaltung durch Passwörter geschützt.

Auf vielen Projekt- oder Firmenseiten findet sich die Möglichkeit, online einen Scanner zu starten oder Dateien zur Untersuchung hoch zuladen. Viele der kommerziellen Angebote stellen ihre Scanner für Privatnutzer auch kostenlos zur Verfügung und konnten während der Bearbeitungszeit dieser Arbeit getestet werden.

Vulnerability Scanner[373] sind ein Werkzeug durch das Schwachstellen automatisiert überprüft werden. Manuell wäre eine Suche nach Schwachstellen für einen Systemadministrator zu aufwendig. Die Vorgehensweise dieser Scanner funktioniert analog zu einem Crackerangriff, technisch arbeiten sie nach dem Prinzip der Signaturerkennung, mit dem Unterschied, dass keine der entdeckten Schwachstellen bei legaler Verwendung destruktiv durch den Anwender ausgenutzt wird. Hier zeigt sich die Wichtigkeit der anthropozentrischen Ausrichtung der IT. Das Werkzeug ist weder gut noch schlecht, die Aufgabe, für die es verwandt wird, ist entscheidend. Die bekanntesten Vertreter sind: Nessus und ISS. Typische Unterarten sind Port- und Adwarescanner.[374]

Erfolgswahrscheinlichkeit

Die Erfolgswahrscheinlichkeit dieser Werkzeuge ist sehr hoch. Die vorhandenen und bekannten Sicherheitslücken werden aufgrund der Signaturen automatisiert erkannt und dem Anwender mitgeteilt. Dieser kann dann entsprechende Maßnahmen einleiten.

4.2.2. Firewall

Die nächste Gruppe der Sicherheitstools sind die Firewalls. Im Deutschen wird dieser englische Begriff oft unzureichend mit Brandmauer übersetzt. Die Assoziationen geben jedoch teilweise die Funktionalität einer Firewall wieder.[375] Zahlreiche Definitionen des Begriffes Firewall sind verbreitet: Als Firewall/Zugangsschutzsystem bezeichnet man ein organisatorisches und technisches Konzept zur Trennung von Netzbereichen und dessen korrekte Umsetzung und dauerhafte Pflege.[376]

---

[373] Vgl. Rey, Enno; Thumann, Michael; Baier, Dominick (2005), S. 22ff; 33ff.
[374] Vgl. Rey, Enno; Thumann, Michael; Baier, Dominick (2005), S. 22ff; [Nessus; http://www.nessus.org]; [ISS; http://www.iss.net]; [At-mix; http://www.at-mix.de]
[375] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 647ff.
[376] Vgl. Strobel, Stefan (1999), S. 81f.

Firewalls befinden sich an den Schnittstellen zwischen einzelnen Netzabschnitten und kontrollieren den Netzwerkverkehr zwischen den Teilen, um ungewünschten Verkehr zu verhindern und nur gewünschten Verkehr weiterzuleiten. Der häufige Einsatz einer Firewall besteht darin, den Verkehr zwischen einem lokalen Netzwerk und dem Internet zu kontrollieren und zu steuern. Umgangssprachlich ist mit einer Firewall sehr oft die Software gemeint, welche den Datenverkehr zwischen den getrennten Netzbereichen kontrolliert und regelt. Ein komplexes Szenario stellt die Demilitarized Zone (DMZ) dar. Als DMZ bezeichnet man ein Computernetzwerk mit sicherheitstechnisch kontrollierten Systemen. Die in der DMZ aufgestellten Systeme werden gegen andere interne Netze abgeschirmt. Durch diese Abschirmung kann der Zugriff auf öffentlich erreichbare Dienste gestattet und gleichzeitig das interne Netz geschützt werden.[377]

Erfolgswahrscheinlichkeit:

Es kann zwischen dem (Sicherheits-)Konzept Firewall, und den zwei Hauptbestandteilen der Firewall, der Hardware und Software, unterschieden werden. Die Hardware ist für das Empfangen und Senden der einzelnen Netzwerkpakete zuständig und die Software regelt den Verkehr.[378]

Die Hardwarekomponente (Hardware-Firewall) hat im Regelfall zwei Netzwerkschnittstellen, an denen jeweils die zu trennenden Netzwerke angeschlossen sind. Zwei Schnittstellen werden aus Sicherheitsgründen gewählt, damit gewährleistet ist, dass nur solche Pakete von einem Netz ins andere durchgelassen werden, die von der Software als gültig anerkannt werden. Eine Hardware-Firewall besteht tatsächlich aus einem materiellen Stück und die hinterlegten Regeln können nur durch physischen Eingriff verändert werden. Der Nachteil besteht im aufwendigen Ändern der Regeln.[379]

Software-Firewalls bestehen aus Programmcode. Hier besteht der Nachteil, dass Software einfach beeinflusst werden kann. Die Softwarekomponente der Firewall arbeitet auf den Schichten zwei bis sieben des ISO/OSI-Referenzmodells. Personal Firewalls oder auch Desktop Firewalls sind Programme, die lokal auf dem zu schützenden Rechner installiert sind. Sie beinhalten einen Paketfilter und

---

[377] Vgl. Kappes, Martin (2007), S. 158f.
[378] Vgl. Anonymous (2004), S.
[379] Vgl. Anonymous (2004), S.

einen Content-Filter. Darüber hinaus sind oft noch Virenscanner integriert. Die Wirkung von Personal Firewalls ist umstritten: Ist ein Rechner durch Schädlinge infiziert, welche unautorisiert auf das Netz zugreifen wollen, so kann der normale Weg des Versands verlassen werden und die Personal Firewall umgangen oder ausgeschaltet werden. Es sind bereits Viren entdeckt worden, welche die Regeln von gängiger Firewallsoftware modifizieren.[380]

4.2.3. Intrusion-Detection-Systeme

Scanner und Firewalls arbeiten nach vorher definierten Regeln, welche bekannte Angriffe abwehren sollen. Intrusion-Detection-Systeme bzw. Intrusion Prevention Systems versuchen über Muster Angriffe zu erkennen und diese zu protokollieren, zu melden, beziehungsweise abzuwehren.[381]

Protokollierungstools[382] zeichnen Vorgänge auf einem Computer auf. Sind diese Protokolle geschützt, lassen sich die protokollierten Handlungen, auch im Falle eines Angriffes nachvollziehen. Dem Schutz dieser Protokolle kommt hierbei eine Schlüsselrolle zu. Sie dürfen nicht deaktiviert werden und auch im Falle eines Versuchs des Löschens der Festplatte müssen sie erhalten bleiben. Dies kann durch einen separaten Speicherort gewährleistet werden. Auswertungskonzept von IDS ist die Erkennung von Anomalien.[383]

Erfolgswahrscheinlichkeit:

IDS erkennen Muster von Angriffen. Stimmt ein Angriff mit einem Muster überein, wird er erkannt. Die Problematik der Signatur der Angriffe ähnelt denen der Scanner.

4.2.4. Zugangssicherheit/Kennwortsicherheit

Passwörter werden zur Authentifizierung verwendet, dabei ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass es korrekt gebraucht wird. Es ist empfehlenswert, eine Regelung zum Passwortgebrauch einzuführen und die IT-Benutzer diesbezüglich zu sensibilisie-

---

[380] Vgl. Anonymous (2004)
[381] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 650f; vgl. Strobel, Stefan (1999), S. 177ff.
[382] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 651.
[383] Pohlmann, S. 439.

ren.[384] Die Vorgaben für die Passwortgestaltung müssen hinsichtlich der Usability einen praktikablen Kompromiss zwischen folgenden Sicherheitszielen darstellen[385]: Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass es nicht leicht zu erraten ist (Sicherheitsaspekt). Die Anzahl der möglichen Passwörter im vorgegebenen Schema muss so groß sein, dass es nicht in kurzer Zeit durch einfaches Ausprobieren (Brute Force Angriff) ermittelt werden kann (Sicherheitsaspekt). Das Passwort darf nicht zu kompliziert sein, damit der Besitzer mit vertretbarem Aufwand in der Lage ist, es auswendig zu lernen (Usability-Aspekt).

4.2.5. Sniffer

Ein Sniffer protokolliert den Netzwerkverkehr. Sie werden dazu verwendet übertragene Datenströme in Netzwerken mitzuschneiden. [386] Ein Netzwerkrouter kann jedes Datenpaket auslesen, welches über ihn geroutet wird. Folgende Informationen sind verfügbar: Ziel, zurückgelegter Weg und Inhalt des Pakets.[387]

Neben der Nutzung als Sicherheitswerkzeug zur Kontrolle des Netzverkehrs besteht die Möglichkeit dieses Werkzeug für böswillige Zwecke einzusetzen. Der mögliche Schaden erstreckt sich auf das Bekanntwerden des Inhaltes der übertragenen Daten sowie des Ziels und des Absenders.

4.2.6. Filter

Filter analysieren den Inhalt einer Übertragung auf Schlagwörter. Enthält eine E-Mail Schlagwörter, dann handelt es sich nach Ansicht der Filterprogrammierer häufig um Spam. Diese Filter sind durch Anpassen der Schreibweise (beispielsweise Viagra zu V1agra) einfach zu umgehen. Des Weiteren werden Open Relay Blacklist-Datenbanken eingesetzt, die eine Prüfung ermöglichen, ob der absendende Server als Open Relay bekannt ist. Es können Listen erwünschter (white) und unerwünschter (black) Absender angelegt werden. Blacklisting ist ineffizient, da es üblich geworden ist, die Absenderadressen zu fälschen.

---

[384] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[385] Vgl. Kersten, Heinrich (Hrsg.); Reuter, Jürgen; Schröder, Klaus-Werner (2008), S. VII; [BSI (a); http://www.bsi.bund.de].
[386] [IT-Security; http://www.itsecurity.com/ss.htm]; [Google; http://www.google.de].
[387] Vgl. Laudon, Kenneth, C.; Laudon, Jane, P. (2006); S. 347; [Alex; http://home.alexweb.net/glossary.htm]; [Google; http://www.google.de]; [TSS; http://tss.lcps.k12.nm.us].

Provider können Signaturen von allen eingehenden E-Mails erstellen. Erhalten zahlreiche Empfänger annähernd zeitgleich die gleiche E-Mail, wird vermutet, dass es sich um Spam handeln könnte. Erwünschte Massenmailings, die einen größeren Kundenkreis eines Providers erreichen, werden dabei ebenfalls ausgefiltert. Des Weiteren verändern Spammer die Signaturen der E-Mails, indem jeder Nachricht unterschiedliche zusätzliche Wörter angehängt werden.

Mailfilter verarbeiten eingehende E-Mails automatisiert nach bestimmten Kriterien. Ein klassisches Anwendungsgebiet ist das Einsortieren elektronischer Post in Postfächer. Dies kann z. B. anhand von Schlüsselwörtern der Mail, aufgrund der Größe oder des Absenders geschehen. Weitergehende Möglichkeiten von Mailfiltern sind das automatische Beantworten von Mails, das Entfernen oder Umwandeln von Dateianhängen, Viren- und UBE-Überprüfungen oder das Betreiben einfacher Mailinglisten. Viele Mailprogramme haben eingebaute Filterfunktionen, diese sind aber meist nicht so flexibel wie bei speziellen, eigenständigen Mailfilter-Programmen.

4.2.7. Physische Sicherungen/Backup

Als Backup werden Duplikate der Hardware und Daten bezeichnet. Es handelt sich beispielsweise um Sicherungen von Festplatten auf externen Festplatten. Physische Sicherungseinrichtungen sind beispielsweise Türen, Schlösser und Brandschutzmaßnahmen.

4.2.8. Netzwerkarchitektur

Unternehmensinfrastrukturen bestehen nicht nur aus Software sondern auch aus Hardwarekomponenten. Kommunizieren verschiedene Komponenten miteinander, so muss dies über Kommunikationseinrichtungen geschehen. Bei diesen handelt es sich bei Rechnern um Netzwerke, die verschiedene Topologien aufweisen können.

Die Topologie bezeichnet bei einem Computernetzwerk die Struktur der Verbindungen mehrerer Geräte zueinander, sie ist entscheidend für seine Ausfallsicherheit: Nur wenn alternative Wege existieren, bleibt bei Ausfällen einzelner Wege die Verbindungsmöglichkeit erhalten. Es wird zwischen physischer und logischer Topologie unterschieden. Die physische Topologie beschreibt den Aufbau der Netzwerkverkabelung; die logische Topologie den Datenfluss zwischen den End-

geräten. Welche Topologie gewählt wird, ist für die Sicherheit von Bedeutung, weil sie Folgen für den Schutz der Verbindungen zwischen den einzelnen Komponenten hat.

Verbindungen können kabelgebunden oder kabellos hergestellt werden. Kabellose Verbindungen bedingen ein höheres Sicherheitsrisiko wie Kabelverbindungen, da ein nicht physischer Zugriff nicht unbedingt festgestellt werden kann. Physische Kabelverbindungen können durch entsprechende Maßnahmen ebenfalls abgehört werden. Verlaufen Verbindungen über öffentliche Bereiche, kann die gesamte Kommunikation abgehört werden.

Problemlöser ist im Bereich der Kommunikation das Konzept der End-Point-Security.[388] Die Kommunikation zwischen zwei Endpunkten kann durch Maßnahmen wie Kryptografie oder Steganografie gesichert werden. Weiterhin wird darunter auch die Sicherstellung des Zugriffs durch Berechtigte verstanden.

4.2.9. Kryptografie/Steganografie

Kryptografie (griechisch *kryptós*, „verborgen“, und *gráphein*, „schreiben“) ist als die Wissenschaft der Verschlüsselung von Informationen ein Teilgebiet der Kryptologie. Im Gegensatz zu Steganografie befasst sie sich nicht damit, die Kommunikation an sich zu verschleiern, sondern damit, den Inhalt von Nachrichten für Dritte unzugänglich zu machen.[389] Sie gilt als Schlüsseltechnologie des Cyberspace.[390] Der heutige Einsatz von Kryptografie hat vier Hauptziele[391]:

Vertraulichkeit der Nachricht: Nur der gewünschte Empfänger sollte in der Lage sein, den Inhalt einer verschlüsselten Nachricht zu lesen. Weiterhin sollte es nicht möglich sein Informationen über den Nachrichteninhalt zu erlangen (beispielsweise eine statistische Verteilung bestimmter Zeichen).[392]

---

[388] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 34.
[389] Vgl. Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf (1998), S. 193ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 5.
[390] Schneier, Bruce (2000), S. 85.
[391] Vgl. Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf (1998), S. 52ff; vgl. Schwenk, Jörg (2005), S. 6.
[392] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 21; vgl. Schwenk, Jörg (2005), S. 6.

Datenintegrität der Nachricht: Der Empfänger sollte in der Lage sein festzustellen, ob die Nachricht seit ihrer Übertragung verändert wurde.[393]

Authentifizierung: Der Empfänger sollte den Absender eindeutig identifizieren können. Weiterhin sollte es überprüfbar sein, ob die Nachricht tatsächlich von diesem Absender stammt.[394]

Verbindlichkeit: Der Absender sollte nicht in der Lage sein zu bestreiten, dass er die Nachricht gesendet hat.[395]

Nicht alle kryptografischen Systeme und Algorithmen erreichen alle genannten Ziele. Die Hauptziele verwirklichen einen Großteil der Sicherheitsziele. Ein wichtiger Baustein vieler moderner Sicherheitssysteme sind Verschlüsselungsverfahren.[396] Die Verschlüsselung selbst dient dabei 3 Zielen. Zunächst soll Vertraulichkeit gewährleistet werden, indem die Daten von Dritten nicht gelesen werden können. Absender und Empfänger einer Nachricht müssen feststellbar sein. Eine Veränderung von Daten muss erkennbar sein.[397]

Die Verschlüsselung hat das Ziel, einen Klartext unter Verwendung eines Schlüssels in ein Chiffrat umzuwandeln, sodass es bei Kenntnis des passenden Schlüssels leicht ist, aus dem Chiffrat wieder den Klartext zu gewinnen, es aber nicht möglich (im Sinne von durchführbar) ist, dies ohne den Schlüssel zu tun. Bei den meisten Verfahren ist es darüber hinaus wichtig, dass es auch nicht möglich ist, aus der Kenntnis von Klartext und Chiffrat den Schlüssel zu berechnen. Die für Ent- und Verschlüsselung verwendeten Schlüssel können identisch sein, dann spricht man von einer symmetrischen Verschlüsselung, oder sie können verschieden sein, in diesem Fall liegt eins asymmetrische Verschlüsselung vor.[398]

Text, bedeutet in Bezug auf ein integratives BIS elektronisch gespeicherte Daten-, der/die in einer natürlichen Sprache verfasst ist und für deren inhaltliche Lesbar-

---

[393] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 22f.
[394] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 23f; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[395] Vgl Eckert, Claudia (2006), S. 11.
[396] Vgl. Strobel, Stefan (1999), S. 51; vgl. Merz, Michael (1999), S. 121.
[397] Vgl. Strobel, Stefan (1999), S. 51.
[398] Vgl. Schmeh, Klaus (2001), S. 93ff; vgl. Schwenk, Jörg (2005), S. 7ff, S. 13ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 5; vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 652f.

keit nicht unbedingt Verständnis und keine besonderen Vorkehrungen außer der Beherrschung der Sprache von Nöten sind. Es existiert für verschiedene Informationen eine Verschlüsselungshierarchie das heißt, manche Nachrichten müssen länger geheim sein als andere.

Moderne Verschlüsselungsverfahren wie die Verfahren nach Rivest, Shamir, Adleman RSA, Diffie-Hellman, oder der Data Encryption Standard DES beruhen auf der Schwierigkeit bestimmte mathematische Probleme zu lösen. In sofern besitzen sie Gemeinsamkeiten, mit älteren Verschlüsselungsmethoden. Die mathematische Grundlage für die oben genannten Verfahren bildet die Zahlentheorie und Erkenntnisse von Gauß, Euler, Fermat, Riemann, Miller-Rabin, den Erfindern des jeweiligen Verschlüsselungsverfahrens und vielen anderen. Wie wichtig die Zahlentheorie für diesen Bereich ist, verdeutlicht die Tatsache, dass bestimmte Veröffentlichungen zu diesem Thema in den Vereinigten Staaten erst dann gedruckt werden dürfen wenn eine staatliche Genehmigung seitens der NSA vorliegt.[399]

Basis der meisten Verfahren ist das Problem der Faktorisierung großer Zahlen. Laut Aussage der Literatur und vieler Mathematiker ist es relativ einfach das Produkt von zwei großen Zahlen zu bilden. Der umgekehrte Weg, die Faktorisierung ist dagegen nicht einfach. Das Problem wird durch die Eigenschaften von Primzahlen erschwert.[400] Bsp. für kleine Werte: Die Zahlen 5 und 7 sind Primzahlen. Ihr Produkt lautet: 5*7=35. Außer durch die Zahlen 5 und 7 kann diese Zahl nicht faktorisiert werden. Schon bei diesen relativ kleinen Zahlen sind 4 Schritte zur Faktorisierung notwendig. Die Anzahl der Schritte wird durch die kleinere der beiden Primzahlen -1 erzeugt. Vernachlässigt wurde die Tatsache, dass bei einem Verschlüsselungsverfahren beruhend auf Primzahlen auch nur durch Primzahlen geteilt werden müsste. Die folgende Abbildung verdeutlicht die Problematik.

Wert	Teiler	Ergebnis	Schritte
35	2	17,5	1
35	3	11,66667	2
35	5	7	3
35	7	5	

Tabelle 4: Faktorisierung

[399] Vgl. Du Sautoy, Marcus (2004), S. 14ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 5, S. 25.
[400] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 110.

Die Auswirkungen für die Multiplikation großer Zahlen lassen sich leicht ableiten. Die Anzahl der als Teiler zu verwendenden Zahlen steigt bis zur zweiten Wurzel der zu faktorisierenden Zahl -1.[401] Weitere Verschlüsselungsverfahren benutzen bspw. elliptische Kurven.[402]

Bei der Steganografie werden in eine Trägerdatei verschlüsselte Elemente integriert. Wer von der Verschlüsselung nichts weiß, kann die betreffende Trägerdatei bis auf die verschlüsselten Elemente ohne Einschränkungen nutzen. Der berechtigte Empfänger ist über die Verschlüsselung informiert und wenn er zudem Zugriff auf den Codierungs-Schlüssel hat, kann er die in der Trägerdatei enthaltenen Informationen entschlüsseln.[403] Die Steganografie existierte schon länger konnte aber erst mithilfe des Computers zu einer leistungsfähigen Technik für den Transport vertraulicher Informationen entwickelt werden.[404]

Erfolgswahrscheinlichkeit

Die Güte des Algorithmus und des Schlüssels tragen wesentlich zur Erfolgswahrscheinlichkeit bei. Derzeit existieren Verfahren welche durch eingehende Tests der Kryptologiegemeinschaft kaum Schwächen aufweisen und noch ungebrochen sind. Dies kann sich aber täglich ändern.

4.2.10. Biometrische Verfahren

Unter biometrischen Verfahren zur Zugangsicherung versteht man Zugangschutz durch überprüfen eineindeutiger körperlicher Merkmale. Lexikalisch wird die Biometrie als Lehre von der Anwendung mathematischer (statistischer) Methoden auf die Mess- und Zahlenverhältnisse der Lebewesen und ihrer Einzelteile definiert.[405]

Auf die IT-Welt bezogen ist dieser Begriff ein Synonym für den *Identitätsnachweis* von Personen unter Verwendung ihrer individuellen körperlichen Merkma-

---

[401] Vgl. Du Sautoy, Marcus (2004), S. 51.
[402] Vgl. Du Sautoy, Marcus (2004), S. 302, S. 311.
[403] Vgl. Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf (1998), S. 193ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 5ff.
[404] Vgl. [Heise; http://www.heise.de in c't 6/97, S. 330.] ; vgl. Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf (1998), S. 193ff; vgl. Eckert, Claudia (2006), S. 283
[405] Vgl. [Pfitzmann, Andreas; http://dud.inf.tu-dresden.de]; vgl. Roth, Richard (Hrsg.); Behrens Michael (2001), S. 10ff.

le.[406] Diese Merkmale müssen so einzigartig sein, dass sie möglichst einer einzigen Person eindeutig zugeordnet werden können. Auch eineiige Zwillinge sollten als Individuen erkannt werden. Zu einem solchen Verfahren gehören, wie in der Abbildung dargestellt, in der Regel drei Komponenten:

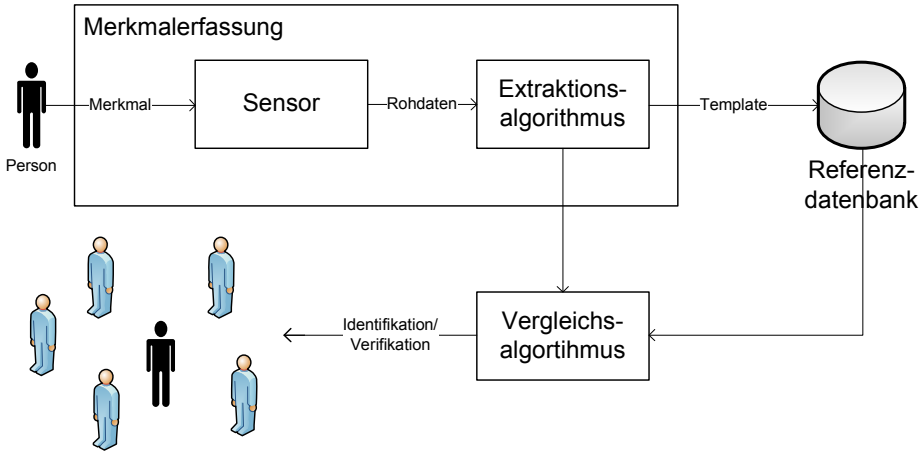

Abbildung 9: Erfassung von Biometriedaten[407]

Zur Erfassung individueller biologischer Merkmale dienen technische Einrichtungen wie Sensoren oder Scanner. Die erfassten Daten sind unter Einsatz mathematischer/statistischer Methoden so zu abstrahieren, dass von den wesentlichen Merkmalen Referenzmuster abgespeichert werden können. Die dritte wesentliche Komponente ist der programmtechnisch umzusetzende Vergleichsalgorithmus. Aus der Art der genutzten Merkmale kann man eine Zweiteilung der Verfahren ableiten:

Statische Verfahren, basierend auf physiologischen Merkmalen, die unveränderlich sind: Fingerabdruck, Hand- und Venengeometrie, Augenmerkmale (Netzhaut, Regenbogenhaut), Gesichtserkennung (visuell, thermisch) und der gesamte Körper.

Dynamische Verfahren, basierend auf verhaltenstypischen Merkmalen, die u.U. veränderlich sein können: Stimme und Motorik (Unterschrift, Tastenanschlag, Lippenbewegung).

---

[406] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 657f; vgl. Dridi, Fredj (2003), S. 85.

[407] In Anlehnung an Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 659.

Eine dritte Gruppe von Verfahren setzt Eingriffe in den Körper der Betroffenen voraus, wie z. B. die Blutbild- oder die DNA-Analyse. Diese Verfahren sind bisher zu Kontrollzwecken schlecht geeignet.

Einige Verfahren sind lange eingeführt, andere Techniken haben die experimentelle Phase verlassen, sind auf dem Markt verfügbar und werden bereits intensiv genutzt. Dabei erweisen sich solche Verfahren als besonders erfolgreich, die zum einen hohen Sicherheitsstandards genügen (insbesondere beeinflusst durch die Invarianz und die Einzigartigkeit der zugrunde liegenden biometrischen Merkmale), sowie ein günstiges Kosten-Nutzen-Verhältnis aufweisen (geringer Erfassungs- und Verifikationsaufwand) und bei den Betroffenen ohne psychologische Hemmungen akzeptiert werden.

Fingerabdruck-Verfahren sind weit verbreitet, kostengünstig und hinreichend sicher. Sie sind abgeleitet aus dem daktyloskopischen Verfahren im polizeilichen Erkennungsdienst. Handgeometrie-Verfahren werden kostengünstig angeboten, gewährleisten aber eingeschränkte Sicherheit, da es hier zu viele Ähnlichkeiten bei unterschiedlichen Individuen gibt. Es existieren kaum Akzeptanzprobleme bei beiden Verfahren.[408]

Verfahren, die auf der Auswertung von Augenmerkmalen (Irisscanner[409]) beruhen, befriedigen hohe Sicherheitsbedürfnisse, sind aber mit hohem Kostenaufwand verbunden und werden wegen des zur Merkmalserfassung benutzten Laserstrahls nicht vorbehaltlos akzeptiert.[410]

Gesichtserkennungs-Verfahren gewinnen aufgrund der geringen Akzeptanzprobleme größere Bedeutung. Die Probleme liegen in der Reduzierbarkeit der Merkmale auf Dateigrößen, die von preisgünstigen Geräten zu bewältigen sind.[411]

Sprach- oder Schrifterkennung ist ein aktives Verfahren das auf verhaltensbasierten Merkmalen beruht. Neben der Unterschrift selbst wird auch die Geschwindigkeit und die Druckverteilung des Schreibgerätes geprüft.[412]

---

[408] Vgl. Roth, Richard (Hrsg.); Behrens Michael (2001), S. 81ff; vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 658.
[409] Vgl. Roth, Richard (Hrsg.); Behrens Michael (2001), S. 129ff.
[410] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 659; vgl. Roth, Richard (Hrsg.); Behrens Michael (2001), S. 129.
[411] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 659; vgl. Roth, Richard (Hrsg.); Behrens Michael (2001), S. 105ff.

Dynamische Verfahren, die sich auf den Vergleich von Verhaltensmerkmalen stützen, haben ebenfalls Marktreife erlangt, sind allerdings wegen des meist damit verbundenen Zeitaufwands nicht universell einsetzbar (z. B. zur Zutrittskontrolle) im Gegensatz zu den statischen Verfahren.

Gesteigerten Sicherheitsbedürfnissen kommt man zunehmend durch sog. Hybridverfahren entgegen, d.h. solche Verfahren, bei denen eine Kombination verschiedener biometrischer Merkmale zum Vergleich herangezogen wird.

Bisher waren die Verfahren hinsichtlich der verwendeten Geräte (Hardware) und der damit verbundenen Verifikationsprozesse (Software) in hohem Maße herstellerabhängig (proprietär). Die derzeitige Entwicklung geht hin zu standardisierte Schnittstellen, die es ermöglichen, Hard- und Software unterschiedlicher Hersteller zu kombinieren. Dies dürfte einen zunehmenden Einsatz biometrischer Systeme zur Folge haben.

Erfolgswahrscheinlichkeit

Biometrische Verfahren erhalten zunehmende Bedeutung für Kontrollsysteme, mit deren Hilfe zwischen berechtigten und unberechtigten Personen unterschieden werden kann. Den bisher üblichen Kontrollsystemen liegen zumeist zwei Komponenten zugrunde. Das eine Element ist der Besitz des Sicherungsmechanismus, wie Schlüssel, Ausweise sowie Magnetstreifen- oder Chipkarten. Die zweite Komponente besteht im Wissen um ein individuell festgelegtes Geheimnis: In der Datenverarbeitung als Passwort bekannt. Neben dem möglicherweise unangenehmen Verlust dieses Wissens durch Vergessen weisen die Kontrollelemente eine wesentlich unangenehmere Eigenschaft auf: Sie sind - gewollt oder ungewollt - übertragbar. Das hat zur Folge, dass jede Person, die über Besitz oder Wissen verfügt, davon auch Gebrauch machen kann, mithin zur Benutzung eines zu schützenden Systems autorisiert wird.[413]

Erst durch die Kombination einer oder beider Komponenten mit einem nicht übertragbaren, eindeutig zuordenbaren persönlichen Kennzeichen erreichen Berechtigungsprüfungen eine neue Qualität: Aus der Autorisierung wird die *Authentifizie-*

---

[412] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 659; vgl. Roth, Richard (Hrsg.); Behrens Michael (2001), S. 159ff u. 179ff.

[413] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 24; vgl. Eckert, Claudia (2006), S. 1489f.

rung d.h., es kann geprüft werden, ob der „Berechtigte“ auch tatsächlich die Person ist, für die sie sich ausgibt. Das Missbrauchsrisiko wird erheblich gemindert.[414]

Durch den Einsatz biometrischer Verfahren entstehen neue datenschutzrechtliche *Gefahren*.[415] Die abgespeicherten Referenzdaten können zu Zwecken genutzt werden, die über die Authentifizierung hinaus gehen. Beispielsweise kann in einer zentralen Datenbank, in der die Referenzdaten abgelegt wurden, nicht nur überprüft werden, ob eine Person zu einer Gruppe von, dem System bekannten Berechtigten gehört („one-to-one“), sondern es besteht auch die Möglichkeit, eine zunächst unbekannte Person mithilfe der gleichen Datenbank zu identifizieren („one-to-many“).

Biometrische Verfahren sind daher datenschutzrechtlich sehr zwiespältig zu beurteilen. Einerseits verletzt ihr Einsatz die informationelle Selbstbestimmung der Betroffenen, wenn deren biometrische Merkmale ohne ihr Wissen mit denen gesuchter Personen verglichen oder für spätere Kontrollzwecke auf Vorrat registriert werden. Andererseits lassen sie wesentlich sicherere Authentifikationsverfahren erhoffen, damit die informationelle Selbstbestimmung durch die Verhinderung unbefugter Datenzugriffe geschützt wird.[416]

Im Sinne des Einsatzes datenschutzfreundlicher Technologien bei der Verarbeitung personenbezogener Daten sind in jüngster Zeit auch bei der Entwicklung von biometrischen Kontrollsystemen Tendenzen erkennbar, die diesem Anliegen Rechnung tragen. So werden mittlerweile solche Systeme auf dem Markt angeboten, die sich von zentral vorgehaltenen Datenbanken lösen und die Verfügungsgewalt über die persönlichen biometrischen Merkmale beim Betroffenen belassen.

Insbesondere die zuletzt beschriebene Entwicklung trägt dazu bei, die Akzeptanz biometrischer Kontrollsysteme bei Betroffenen zu erhöhen, da auf diese Weise die datenschutzrechtlichen Bedenken gegen deren Einsatz wesentlich reduziert wer-

---

[414] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 22ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

[415] Unter Datenschutz versteht man gesetzliche und vertragliche Regelungen, die zum Schutz von personenbezogenen Daten vor unbefugtem Zugriff oder Missbrauch dienen; vgl. Heilmann, Wolfgang; Reusch, Günter (1984), S. 85.

[416] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2; vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 87ff; vgl. Eckert, Claudia (2006), S. 493.

den können.[417] Derzeit erproben schon verschiedene Firmen weltweit und in Deutschland biometrische Identifikationssysteme.[418]

4.2.11. Isolierung

Systeme können durch eigene Leitungen vollständig vom öffentlichen Netz getrennt (isoliert) werden. Dies ist für Hochsicherheitssysteme notwendig. Es darf dann keine einzige Schnittstelle zu einem öffentlichen System bestehen. Die internen Schnittstellen zum System müssen ebenso gesichert werden.

4.2.12. Zertifikate

In einer Public-Key-Infrastruktur dient ein Zertifikat dem Nachweis, dass ein öffentlicher Schlüssel eines asymmetrischen Verschlüsselungsverfahrens zu einer angegebenen Person, Institution oder Maschine gehört.[419] Mithilfe des Zertifikates können weitere Daten verschlüsselt und signiert werden und somit zum einen die Echtheit (Authentizität) und die Vertraulichkeit (Integrität) der Daten Dritten gegenüber garantiert werden.[420]

Ein Zertifikat enthält Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle. Diese Daten sind in der Regel mit dem privaten Schlüssel der Zertifizierungsstelle signiert und können somit mit dem öffentlichen Schlüssel der Zertifizierungsstelle überprüft werden. Um die Echtheit des Zertifikates zu garantieren, wird dem Zertifikat eine digitale Signatur einer vertrauenswürdigen Organisation oder Instanz aufgeprägt. [421] Durch dessen Signatur kann die Integrität und Echtheit des Zertifikates nachgewiesen werden. Da auch der öffentliche Schlüssel einer Zertifizierungsstelle schließlich mittels eines Zertifikats überprüfbar sein muss, ergibt sich die Notwendigkeit einer obersten Zertifizierungsinstanz. Zertifikate für Schlüssel, die nicht mehr sicher sind, können über eine sogenannte Certificate Revocation List gesperrt werden.

---

[417] [Datenschutz-Berlin (1999); http://www.datenschutz-berlin.de].
[418] Vgl. Powell, C. (2006); in Biometric Technology Today; vgl. von Graevenitz, Gerik, Alexander (2006); vgl. [Heise Online (2006); http:// www.heise.de].
[419] Vgl. Merz, Michael (1999), S. 132ff.
[420] Vgl. Schwenk, Jörg (2005), S. 13ff; 22ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2; vgl. Schmeh, Klaus (2001), S. 279ff; vgl. Ertel, Wolfgang (2001), S. 110ff.
[421] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 655.

4.2.13. Wächterkarten

Es handelt sich um Hardware, welche Systemveränderungen erkennt.

4.2.14. Live CDs/Virtualisierung

Diese bieten ein System das von einem nicht veränderbaren Datenträger aus gestartet wird. Die Vorteile liegen in einer bekannten Systemumgebung, welche ohne Schnittstellen in öffentliche Bereiche unverändert bleibt.

4.3. Organisatorische Maßnahmen

Die technischen Maßnahmen sind nur dann wirkungsvoll, wenn diese in Unternehmen auch konsequent angewandt und umgesetzt werden. Untersuchungen der Praxis zeigen, dass dies nicht der Fall ist. Organisatorische Maßnahmen müssen gewährleisten das notwendige technische Maßnahmen getroffen und eingehalten werden. Zweitens müssen sie so gestaltet werden, dass Prozesse für das richtige Verhalten und den Umgang mit Computersystemen innerhalb und außerhalb des Unternehmens vorhanden sind und auf Einhaltung überprüft werden.

4.3.1. Schulungen

Schulungen von Mitarbeitern dienen dazu den Umgang mit Computersystemen zu erlernen. Fortbildungen müssen regelmäßig stattfinden damit die Bedeutung der IT-Sicherheit den Teilnehmern bewusst wird. Keinesfalls darf es sich um eine reine Anwesenheitsveranstaltung handeln.[422]

4.3.2. Sicherheitsrichtlinien

Sicherheitsrichtlinien geben dem Anwender einen Hinweis wie bei bestimmten Situationen verfahren werden kann. Eine Sicherheitsrichtlinie besagt beispielsweise: Das Passwort ist nur Ihnen bekannt. Niemals wird Sie jemand danach fragen. Fragt Sie jemand danach, handelt es sich mit Sicherheit um einen Unberechtigten. Ähnliche Sicherheitsrichtlinien sind für die technischen Maßnahmen, die organisatorischen Abläufe und sonstige Bereiche der Unternehmung individuell zu erstellen.[423]

---

[422] Vgl. Godschalk, David (2007), S. 205f.; vgl. McIlwraith, Angus (2006), S. 94.
[423] Vgl. Schneier, Bruce (2000), S. 307ff; vgl. Laudon, Kenneth, C.; Laudon, Jane, P. (2006); S. 357.

4.3.3. Trusted Computing

Eine Initiative um den Umgang mit dem PC sicherer zu gestalten, stellt das von einem Konsortium unter Führung der Firmen Microsoft und Intel getragene Trusted Computing dar. Kernpunkt dieser Entwicklung soll es sein, einen Hardwarechip in jede Computerarchitektur einzupflegen, der die Aktivitäten des Rechners überwacht. Würden größere Aktivitäten ohne Benutzereingabe registriert, könnte der Chip Alarm schlagen und vor einer Gefahr warnen. Der Fokus der Auswahl eines Chips liegt dabei in der möglichen Unveränderbarkeit der Überwachungsregeln.[424] Dieses Konzept lässt heftigen Widerstand von Seiten der Daten- und Wettbewerbsschützer erwarten. Durch den integrierten Chip könnten Computernutzer gezwungen werden nur bestimmte Software zu verwenden. Dies ist nicht erwünscht.[425]

4.3.4. Test (Penetrationstests)

Penetrationstests werden durchgeführt, um die bisherige Sicherheit des eigenen Systems zu testen. Es werden hierfür die Werkzeuge der Cracker benötigt. Diese werden auf die eigene Infrastruktur angewandt um die Sicherheitslücken zu identifizieren und anschließend zu beseitigen. Werden die von Vulnerability Scannern gefundenen bzw. andere vorhandene Schwachstellen durch den Systemadministrator auch ausgenutzt, spricht man von Penetrationstests.[426]

4.3.5. Listen/Filter

Es lassen sich die Konzepte des Whitelistings und des Blacklistings unterscheiden. Beim ersteren werden nur Aufrufe zugelassen, welche in einer Liste hinterlegt sind und im Gegensatz zum letzteren bei dem die hinterlegten Aufrufe nicht zugelassen werden. Beide Konzepte bedingen eine vorherige Untersuchung, welche Aufgaben zu erfüllen sind. Das Ausschlussprinzip des Blacklisting erfordert einen erhöhten Wartungsaufwand, da immer neue Gefahren für IT-Systeme entdeckt werden. Die Erstellung und Pflege der Listen muss in die Unternehmensstruktur implementiert werden.

---

[424] Vgl. Handschuh, Helena; Trichina, Elena, in Paulus, Sachar; Pohlmann, Norbert; Reimer Helmut, (2006), S. 38ff.
[425] Vgl. Pohlmann, Norbert; Reimer, Helmut (Hrsg.) (2008); S. 3ff u. 15ff; vgl. [Sendung Forschung aktuell am 31.01.2005 auf dem Sender Deutschlandfunk; http://www.dradio.de].
[426] Vgl. Rey, Enno; Thumann, Michael; Baier, Dominick (2005), S. 1ff; vgl. Eckert, Claudia (2006), S. 177f.

4.3.6. Schutzprofile/Berechtigungskonzept

Schutzprofile werden in Computersystemen mit verschiedenen Nutzern angelegt. Ein Benutzer kann dabei mit eingeschränkten Rechten angelegt werden. Eine weitere Bedeutung von Schutzprofilen lässt sich aus der Begriffsverwendung in den Common Criteria[427] herleiten. Hier bedeuten Schutzprofile die notwendigen Sicherheitsmaßnahmen und Richtlinien, die über eine Anforderungsanalyse für das Anwendungs-System festgelegt werden müssen.[428]

4.3.7. Common Criteria Schutzprofile

Die Common Criteria (CC) bieten die Möglichkeit, dass IT-Anwender ihre Bedürfnisse zur IT-Sicherheit in Schutzprofilen darstellen können. Das Konzept der Schutzprofile wurde in den Federal Criteria eingeführt, die Ende 1992 von NSA und NIST herausgegeben wurden. Im Rahmen der Entwicklung der CC wurde dieses Konzept überarbeitet und in das Modell der CC mit eingeflochten.

Schutzprofile sind eine Lösung für Standard-Sicherheitsprobleme einer Produktgruppe. Sie sind implementierungsunabhängig, können aber durch die daraus ableitbaren Sicherheitsvorgaben auf einen konkreten Evaluationsgegenstand (EVG) zugeschnitten werden. Schutzprofile beschreiben insofern ein Sicherheitskonzept.

Ein Merkmal des Schutzprofil-Konzepts der CC besteht darin, dass Schutzprofile nicht vom Antragsteller oder Hersteller, sondern von IT-Anwendern geschrieben werden können. Sie sind damit benutzerorientiert. Durch die Evaluierung eines Schutzprofils wird den IT-Herstellern die Sicherheit gegeben, dass das Schutzprofil ein sinnvolles Konzept für ein IT-Sicherheitsprodukt darstellt und es zweckmäßig erscheint, ein entsprechendes Produkt zu entwickeln und evaluieren zu lassen. Bedingt durch das allgemeine Sicherheitskonzept eines Schutzprofils ist für den IT-Anwender somit eine gute Vergleichbarkeit verschiedener Produkte gewährleistet, die auf Basis ein und desselben Schutzprofils entwickelt und evaluiert worden sind.[429]

---

[427] Vgl. Eckert, Claudia (2006), S. 224; vgl. Görtz, Horst; Stolp, Jutta (1999), S. 192ff.
[428] Vgl. Godschalk, David (2007), S. 216f.
[429] Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 641.

Die CC bieten im Teil 1, Anhang B eine ausführliche Beschreibung zur Spezifizierung von Schutzprofilen. Folgende Abbildung zeigt die empfohlene Struktur von Schutzprofilen:

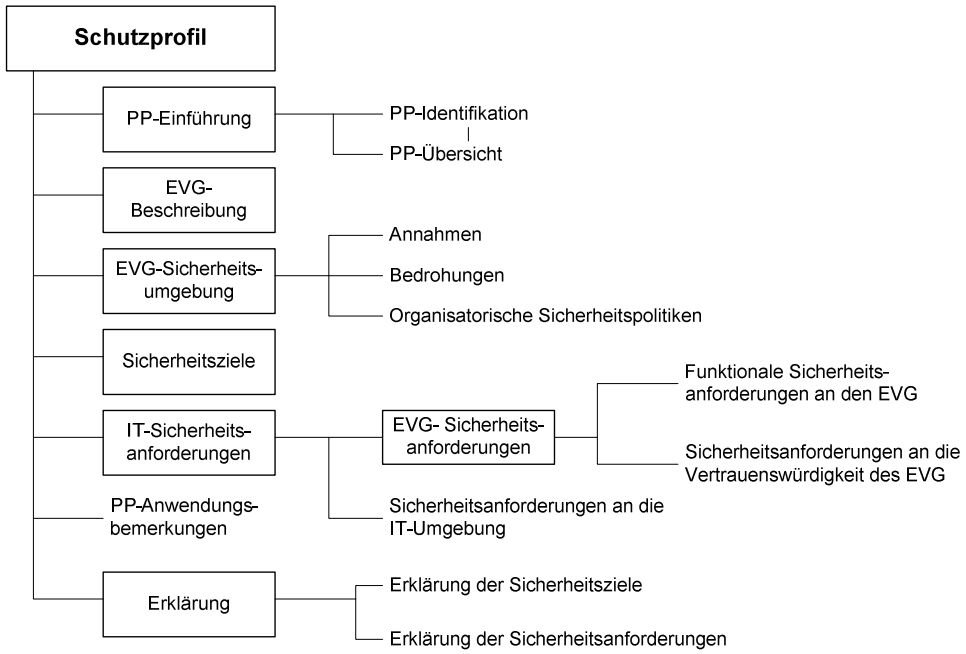

Abbildung 10: Schutzprofil[430]

Weitere Informationen zum Thema CC-Schutzprofil sind im Anhang zu finden.

4.3.8. Priorisierung

Die sicherheitsrelevanten Aufgaben können priorisiert werden. D. h. es ist eine Landkarte der Wichtigkeit verschiedener Anwendungen und Daten zu erstellen. Diese sind je nach Wichtigkeit zuerst zu pflegen.

4.3.9. Sicherheitsfunktion

Sicherheitsfunktionen werden zur Minimierung von Bedrohungen in Sicherheitsprodukten verwendet. Jede Sicherheitsfunktion beruht auf mindestens einer identifizierten Bedrohung.

4.3.10. Sicherheitsanalyse

Die Sicherheitsanalyse ist Teil der Tätigkeiten im Rahmen des Sicherheitsmanagements in einem Unternehmen. Ziel der Sicherheitsanalyse ist es, Bedrohungen

---

[430] CC-Schutzprofil

zu erkennen, deren Eintrittswahrscheinlichkeit und Schadenspotenzial einzuschätzen und daraus das Risiko für die Organisation abzuschätzen.[431] Dieses Vorgehen ist nur schwer zu formalisieren, es ist deshalb in Teilbereichen versucht worden, eine Standardisierung, beispielsweise im Rahmen des Standards ISO 17799, zu erreichen.[432] Mittel der Sicherheitsanalyse sind sowohl technischer Art, als auch prozessorientierter Art.[433] Das Ergebnis einer Sicherheitsanalyse ist eine Empfehlung und Umsetzung von Maßnahmen zur Steigerung der IT-Sicherheit.

In einem Datenschutzkonzept (DSK) werden die für eine datenschutzrechtliche Beurteilung notwendigen Informationen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschrieben. Es dokumentiert die Art und den Umfang der erhobenen, verarbeiteten oder genutzten personenbezogenen Daten. Die Beschreibung der Daten oder Datenfelder nennt man in der Regel Datenfeldkatalog. Aus der Festlegung datenschutzrechtliche Anforderungen ergibt sich die Rechtsgrundlage und Zweckbindung für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten.

Eine Beschreibung der Schnittstellen als Schnittstellenkatalog und aller vorgesehenen Auswertungen von Daten (Auswertekatalog) geben einen Überblick über die Nutzung bzw. Übermittlung von personenbezogenen Daten. Weiterhin werden die umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutz nach § 9 BDSG und dessen Anlage dokumentiert. Aus dieser Darstellung kann die Angemessenheit der getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz betrachtet werden.

Das Datenschutzkonzept gibt als umfassendes Dokument Auskunft über die Rechtmäßigkeit der Datenverarbeitung bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Es gehört neben Fachkonzept, Betriebskonzept und Sicherheitskonzept zur Dokumentation eines IV-Verfahrens (Prozess, Projekt, IV-Anwendung bzw. IV-System).[434]

In einem IT-Sicherheitskonzept werden im Unterschied zum Datenschutzkonzept nur die Sicherheitsmaßnahmen beschrieben. Grundlage für ein IT-Sicher-

---

[431] Vgl. Wack, Jessica (2007), S. 24.
[432] Vgl. Eschweiler, Jörg (2006), S. 97ff.
[433] Vgl. Rey, Enno; Thumann, Michael; Baier, Dominick (2005), S. 22ff; 33ff.
[434] Vgl. Krallmann, Hermann (1996), S. 219.

heitskonzept ist im Regelfall eine Sicherheitsbetrachtung mit Risikoanalyse auf der Basis einer Bedrohungsanalyse.[435]

4.3.11. Ermittlung der Wahrscheinlichkeit der Gefahren

Es müssen die relevanten Risiken, deren Eintrittswahrscheinlichkeiten und der jeweils zu erwartende Schaden festgestellt bzw. als Schätzung festgelegt werden. Möglich ist dies beispielsweise durch eine Monte-Carlo-Simulation.[436] Hierzu können die Inhalte des Kapitels Gefahren der Nutzung von Informationssystemen herangezogen werden. Ebenso kann dies beispielsweise über die Grundschutzkataloge des BSI angegangen werden.[437]

4.3.12. Ermittlung des Schadens der Gefahrenarten

Die Ermittlung des Schadens ist durch Rückzuführung auf die Grundproblematik der Bewertung der einzelnen Vorfälle der Ausfallbedrohung, Zerstörung von Daten, Veränderung von Daten/Informationen, Behinderung des Informationsaustauschs und der unberechtigten Informationsweitergabe zu leisten. Die Ermittlung der Schadenshöhe ist demnach für jedes Unternehmen einzeln durchzuführen, da der Nutzenwert des Informationssystems von Unternehmen zu Unternehmen differiert und dieser im Umkehrschluss als geeignet erscheint den Schaden der einzelnen Ereignisse zu ermitteln bzw. zu schätzen.

4.3.13. Ermittlung des Zugangs zum System

Bedrohungen erreichen Systeme über Schnittstellen, beispielsweise Kommunikationsschnittstellen, Benutzungsschnittstellen und physischen Zugang. Schnittstellen bergen somit die Gefahr der Kompromittierung des Systems. Im Folgenden ist deshalb der Schluss zu ziehen, dass die Schnittstellen der Systeme als Gatekeeper einem besonderen Schutz zu unterziehen sind.[438]

4.3.14. Anforderungsanalyse

Die Anforderungen an integrative BIS betreffend Sicherheit und Usability ergeben sich aus den Anforderungen an Informationssysteme im Allgemeinen, des

---

[435] Vgl. Eckert, Claudia (2006), S. 171f; 163f; vgl. Dridi, Fredj (2003), S. 54.
[436] Vgl. Wack, Jessica (2007), S. 24ff.
[437] Bundesamt für Sicherheit in der Informationstechnik (2005), S. 53ff.
[438] Vgl. [Handelsblatt (2005); http://www.handelsblatt.com].

Weiteren gibt es neben den aufgabenbezogenen Bedingungen auch rechtliche Voraussetzungen, welche erfüllt werden müssen.

Es muss im ersten Schritt die benötigte Sicherheitsstufe[439] des Systems festgelegt werden. Zu hundert Prozent sichere Systeme verfügen über keinerlei Schnittstellen nach Außen und sind deshalb nicht mehr handhabbar.[440] Anders verhält es sich, wenn die Anforderung lautet, alles Erdenkliche getan zu haben. Diese Anforderung wird oft durch Gesetzestexte impliziert und meint, dass der derzeitige Stand der Technik bzw. Wirtschaft eingehalten werden muss. Absolute Sicherheit[441] ist aus Sicht des Autors nur erreichbar wenn Systeme einen völligen Autarkheitsgrad erreichen. Hier stellt sich die Frage wie es dann noch möglich ist, Informationen in das System und aus dem System zu transferieren und wie sehr der Anspruch und Nutzen sowie die Zielsetzung dieser Systeme verloren geht.[442] Wichtige Aufgabe ist es deshalb das Sicherheitsbedürfnis individuell gegenüber der Gebrauchstauglichkeit abzuwägen. Das Sicherheitsniveau beschreibt hierbei das Maß an Sicherheit.[443]

Viele der Maßnahmen, welche das Sicherheitsniveau erhöhen betreffen die Führungskraft kaum, könnten also ohne Beeinträchtigung der Usability eingeführt werden. Eine ausführliche Untersuchung der Auswirkungen auf die Usability findet im Kapitel „Spannungsfeld Usability vs. Sicherheit“ statt und kann von dort übernommen werden.

Als erster Schritt ist eine Gefährdungsanalyse durchzuführen. Hierbei unterstützt das Kapitel Gefahren der Nutzung von Informationssystemen insbesondere bei der Identifikation der verschiedenen Interessengruppen. Die Gefährdungslage verändert sich dabei ständig. Sind die Gefahren identifiziert, kann das Sicherheitsniveau festgelegt werden. Ausgehend vom Sicherheitsniveau müssen Entscheidungen getroffen werden, in wie weit dieses für Belange der Usability eingeschränkt werden kann. Die Belange der Usability stehen den durch das Sicher-

---

[439] Vgl. Schmidt, Klaus (2006), S. 19ff.
[440] Ertel, Wolfgang (2001), S. 24.
[441] Im Sinne was menschenmöglich und vorhersehbar ist; vgl. Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf (1998), S. 106; vgl. Englbrecht, Michael (2004), S. 4.
[442] Sicherheit kann nie Absolut erreicht werden, sondern stellt einen Kompromiss aus Kosten und Nutzen dar; vgl. auch Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf (1998), S. 106.
[443] Vgl. Müller, Rainer (2005), S. 445.

heitsniveau vorgegebenen Anforderungen oft entgegen, umgekehrt gilt dies ebenso. Hierbei ist anzumerken, dass integrative BIS von Natur aus ein erhöhtes Sicherheitsbedürfnis wecken und es letztlich nur um die letzten Prozente an Sicherheit geht.

4.4. Rechtliche Maßnahmen

4.4.1. Verträge/Versicherungen

Mit Kunden, Lieferanten und sonstigen natürlichen oder rechtlichen Personen, können Verträge geschlossen werden, welche die Haftung im Falle eine Verletzung der Informationssicherheit auf das rechtlich zulässige Minimum beschränkt. Sollten keine Verträge geschlossen werden können, besteht die Möglichkeit Versicherungen für eintretende Schadensfälle abzuschließen. Dies gilt nur, wenn die Verletzung der Unternehmung zuzurechnen ist. Die Sorgfaltspflichten anderer, die in Verbindung mit der eigenen IT arbeiten, müssen ebenso in Verträgen festgelegt werden. Beispielsweise die Beachtung des Datenschutzes durch einen Dienstleister oder die Verwendung von sicheren Passwörtern durch Zulieferer.[444]

Versicherungen dienen der Risikoübertragung im Falle eines risikoaversen Verhaltens des Versicherungsnehmers. Für diesen besteht die Möglichkeit gegen eine Prämie das verbleibende Risiko an einen Dritten, Versicherer zu übertragen. Prinzipiell wird der Versicherer Sorgfaltspflichten von seinen Versicherungsnehmern verlangen. Diese Möglichkeit verschiebt die Gedanken über IT-Sicherheit vom Versicherungsnehmer zum Versicherungsgeber, der seinerseits wieder Vorgaben hinsichtlich einer sicheren IT machen wird, die sich an auftretenden Schadensfällen orientieren.

Eine weitere Möglichkeit ist die Nutzung der Rechtsordnung. Die Strafverfolgungsbehörden können innerhalb eines Strafverfahrens die Identität eines Straftäters ermitteln und die Taten strafrechtlich verfolgen. Einhergehend mit der strafrechtlichen Ermittlung des Täters kann nach dessen Ermittlung die zivilrechtliche Schadenersatzklage ein Weg sein, Teile des Schadens zu ersetzen.

---

[444] Buchner, Frank (2007), S. 60ff.

4.4.2. Zertifizierung

Die im Unternehmen eingesetzte Infrastruktur kann durch Dritte überprüft werden. Diese können Zertifikate ausstellen, welche diese Überprüfung anhand vorher festgelegter Kriterien dokumentieren. Dies kann in rechtlichen Belangen dann als Nachweis hinzugezogen werden, rechtliche Pflichten ordnungsgemäß erfüllt zu haben. In diesem Falle tritt dann eine Haftungsverschiebung in Kraft.

4.5. Sonstige Maßnahmen

4.5.1. Outsourcing

Eine weitere Möglichkeit des Risikoübertrags ist die Verwendung von IT-Dienstleistern (Outsourcing).[445] Die unterschiedlichen Stufen des Outsourcings können hier aus Platzmangel nicht aufgezählt werden, spielen aber bei den Überlegungen zur IT-Sicherheit keine wesentliche Rolle. Wichtig ist die Verpflichtung des Dienstleisters IT-Sicherheit im Rahmen der Vertragsgestaltung zu gewährleisten. Weiterhin liegt die Vermutung nahe, dass bei einer Spezialisierung des Dienstleisters das Sicherheitsniveau durch den Know-how-Vorsprung gegenüber der Unternehmung steigt. Im betriebswirtschaftlichen Sinne handelt es sich um eine Make oder Buy Entscheidung bzw. eine Entscheidung für eine Mischung aus beiden Varianten.[446]

4.5.2. Hardwareanpassung

Hardwareteile können verschiedene Ausprägungen annehmen, so können beispielsweise Monitore mit hohem bzw. niedrigem Abstrahlungswert angeschafft werden. Diese Entscheidungen sind sowohl unter dem Aspekt der Sicherheit als auch aus ökonomischen Gesichtspunkten zu treffen. Geringe Anpassungen der Hardware können zu einem erhöhten Sicherheitsniveau führen.

4.5.3. Digitale (Computer-) Forensik

Ziele von forensischen Ermittlungen sind unter anderem die Methode oder die Schwachstelle, welche einen Einbruch ermöglicht hat, die Ermittlung des entstandenen Schadens sowie die Identifikation des Täters. Dies dient ebenfalls der Si-

---

[445] Vgl. Laudon, Kenneth, C.; Laudon, Jane, P. (2006); S. 341.
[446] Vgl. Kleiner, Marco; Müller, Lucas; Köhler, Mario (2005), S. 7f; S. 15f.

cherung juristisch verwertbarer Beweise.[447] Tatbestände bei denen sich eine forensische Ermittlung lohnen könnte sind Fälle von Einbrüchen im Umfeld der Kinderpornografie, Urheberrechtsverletzungen, Geheimnisverrat und der Wirtschaftsspionage.[448]

Es handelt sich um Techniken, die eine Überprüfung der Authentizität digitaler Daten ermöglichen. Allgemein beschäftigen sich forensische Verfahren mit der Spurensuche und -analyse zur Rekonstruktion von (Straf-)Handlungen und zur Identifikation der daran Beteiligten.[449] Im Speziellen nutzen Verfahren der Multimediaforensik Modelle des Medieninhaltes oder der Digitalisierungstechnik, um auffällige Abweichungen vom modellierten Normalfall als forensische Indizien bei der Überprüfung der Authentizität zu verwenden. Durch statistische Analysen der digitalen oder digitalisierten Daten des Mediums an sich setzen sie dabei keinerlei Kenntnis der unverfälschten Daten voraus.[450]

4.5.4. Honigtopf

Das Konzept des Honigtopfs, englisch Honeypot umfasst die Aufgabe, Angriffe auf ein Netzwerk zu protokollieren und dient damit der Überwachung desselben. In einem Netzwerk werden ein oder mehrere Honeypots installiert, die von legitimen Anwendern nicht benutzt werden. Es handelt sich um eine Art Falle, da ein Angreifer nicht zwischen echten Zielen und Honeypots unterscheiden kann. Wenn versucht wird mit einem Honeypot zu kommunizieren, wird dies als potenzieller Angriff erkannt. Mithilfe eines Honeypot-Programmes werden deshalb Netzwerkdienste eines einzelnen Rechners oder ein vollständiges Netzwerk simuliert. Erfolgt ein unberechtigter Zugriff, werden alle ausgeführten Aktionen protokolliert und ein Alarm ausgelöst.

4.6. IT-Sicherheitskriterien, Normen und Standards

Als Maßstab zur Beurteilung der Sicherheit informationstechnischer Systeme dienen Kriterien für deren Bewertung. Ziel der Entwicklung von Sicherheitskriterien ist es eine Richtschnur für die Entwicklung sicherer und vertrauenswürdiger Systeme zu entwickeln sowie eine objektive Bewertung von einer neutralen und kom-

---

[447] Vgl. Geschonneck, Alexander (2004), S. 100.
[448] Vgl. Geschonneck, Alexander (2004), S. 100; Schmeh, Klaus (2001), S. 16f.
[449] Vgl. Dridi, Fredj (2003), S. 65.
[450] Vgl. Geschonneck, Alexander (2006) S. 55ff; [Tu-Dresden; http://www.inf.tu-dresden.de]

petenten Instanz zu ermöglichen, um dem Anwender die Möglichkeit einer Auswahl eines IT-Sicherheitsprodukts zu bieten.[451]

Folgenden Richtlinien sind bekannt: IT-Grundschutzhandbuch, ITSEC, ISO/IEC TR 13335-1, Part 1, ISO 15408 (Common Criteria), ISO/IEC 17799:2005 und Dr.-Ing. Müller sowie BS7799. Des Weiteren werden die Kriterien unter den Begriffen Common Criteria (ISO/IEC 15408), Common Evaluation Methodology, ITSEC, Deutsche IT-Sicherheitskriterien, Orange Book - TCSEC, Informationssicherheitsmanagement (ISO/IEC 27000ff), ITIL und ISO/IEC 20000 subsumiert. Nachfolgend werden die Richtlinien auf Ihren Gehalt an Überblicksmethoden und direkte Vorgaben, sprich Praktiken verglichen. [452]

Kategorisierung der Richtlinien zur Sicherheitspolitik		
Quelle	Überblicksartige Vorgaben	Praktiken
IT-Grundschutzhandbuch	Enthalten	Enthalten
ITSEC	Enthalten	Enthalten
ISO/IEC TR 13335-1, Part 1	Enthalten	Nein
ISO 15408 (Common Criteria)	Nein	Enthalten
ISO/IEC 17799:2000	Enthalten	Nein
Dr.-Ing. Müller	Enthalten	Nein
BS799		
Common Criteria		

Tabelle 5: Umfang der Richtlinien zur Sicherheitspolitik[453]

4.6.1. Protokolle

Technisch werden Sicherheitsmaßnahmen durch Protokolle umgesetzt. Diese sind derzeit zur Sicherung der Netzwerkebene: SSL, IPSEC, SKIP, GSS[454] sowie zur

---

[451] [BSI; http://www.bsi.bund.de].

[452] Vgl. [Völkner, Jörg (2005); http://www.secorvo.de]; vgl. Müller, Klaus-Rainer (2003), S. 15, S. 16, S. 17; S. 18; vgl. Görtz, Horst; Stolp, Jutta (1999), S. 191f; vgl. Kersten, Heinrich (Hrsg.); Reuter, Jürgen; Schröder, Klaus-Werner (2008), S. VII; vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 637; vgl. Witt, Bernhard C. (2006), S. 25ff; vgl. Brunnstein, Jochen (2006).

[453] In Anlehnung an: Müller, Klaus-Rainer (2003), S. 19.

[454] Vgl. Görtz, Horst; Stolp, Jutta (1999), S. 204-208.

Sicherung der Anwendungsebene: SHTTP; SET, S/MIME, MailTrust, I-SAKMP[455].

4.6.2. Sicherheitseinrichtungen

Die Auswahl zeigt die wichtigste Institution auf deutscher sowie auf internationaler Ebene.

4.6.2.1. BSI

Das Bundesamt für Sicherheit in der Informationstechnik ist in der Bundesrepublik Deutschland Ansprechpartner für alle Sicherheitsbelange. Es leistet in Form vom Broschüren, Beratungen sowie Artikeln Beiträge zur Computersicherheit. Gemäß des BSI-Errichtungsgesetzes (BSIG vom 17.12.1990) ist es eine der übertragenen Aufgaben des „Bundesamts für Sicherheit in der Informationstechnik – BSI“ IT-Sicherheitskriterien zu erstellen. Daher arbeitet das BSI seit Jahren auf internationaler Ebene bei der Erstellung von Sicherheitskriterien mit.

4.6.2.2. CERT

Das Computer Emergency Response Team ist ein Verband, der einen 24-Stunden-Beratungsservice für Internet-Benutzer anbietet. CERT beschäftigt sich mit Aspekten, welche die Datensicherheit betreffen, und gibt Benutzern Hilfestellung, wenn Viren oder andere Sicherheitslücken entdeckt werden.

4.7. Zusammenfassung

Es sind viele Sicherheitsmaßnahmen für unterschiedliche Gefahren bereits vorhanden. Diese können so gebraucht werden, dass sie im Zusammenspiel miteinander den Großteil der Risiken beim Betrieb von integrativen BIS abdecken. Die Maßnahmen müssen dabei aufeinander abgestimmt werden. In diesem Kapitel wurde des Weiteren deutlich, dass Sicherheitsmaßnahmen in Produktklassen eingeteilt werden können, welche jeweils auf eine bestimmte Bedrohung ausgerichtet sind.

---

[455] Vgl. Görtz, Horst; Stolp, Jutta (1999), S. 209-214.

5. Usability

Führungskräfte repräsentieren in Mensch-Aufgabe-Technik-Systemen Aufgabenträger, deren Aufgaben häufig unstrukturiert sind. Informationssysteme nehmen den Platz der Technik ein und die Unternehmung stellt die Rahmenbedingungen, den organisatorischen Kontext dar. Im anthropozentrischen Ansatz sind die Bedürfnisse der Führungskräfte in den Mittelpunkt zu stellen, damit Sie die ihnen zugeordneten Aufgaben bestmöglich erfüllen können. Damit Informationssysteme benutzt werden, müssen die Aufgaben durch diese besser unterstützt werden als durch andere oder keine Hilfsmittel. Empirisch ist oftmals eine Reaktanz gegenüber schwierig zu gebrauchenden und mit erheblichem Aufwand erlernbarer Software zu beobachten.[456] Die Informationssysteme werden durch die integrativen BIS repräsentiert.

Eine Möglichkeit dies zu erreichen ist die Benutzbarkeit/Usability zu verbessern. Unter dem Begriff Usability subsumiert man allgemein die Nutzbarkeit oder Benutzerfreundlichkeit eines Systems.[457] Ein Interface ist gebrauchstauglich (useable), wenn der Anwender dieses in einem bestimmten Kontext effektiv und effizient benutzen kann. „Benutzbarkeit und Inhalt müssen gleichermaßen sinnvoll präsentiert werden, sodass beide vom Anwender schnell erfasst und für seine individuellen Bedürfnisse wahrgenommen und Daten zu Informationen transformiert werden können.“[458] Dies bedeutet, dass ein integratives BIS für die Führungskraft das Unterstützungspotential zugänglich macht, sinnvoll visualisiert und effektiv sowie effizient darstellt.

Nicht alleine die Einfachheit des Gebrauchs, sondern der Aufwand das beabsichtigte Ziel zu erreichen, ist Fragestellung des Begriffes der sich in seiner Übersetzung nach der Trennung in use, gebrauchen und utility, der Nutzen als Benutzerfreundlichkeit definieren lässt.[459] Der Aufwand der Führungskraft zur Zielerreichung bei der Nutzung eines integrativen Business-Intelligence-Systems im Gegensatz zu anderen Herangehensweisen ist für diese wesentlich. In der Regel wählt die Führungskraft den Weg des geringsten Aufwandes bei gleicher Zieler-

---

456 Vgl. [Geis, Thomas (2005); http://www.fit-fuer-usability.de]; vgl. Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2004), S. 277; vgl. Sarodnick, Florian; Brau, Henning (2006), S. 15.
457 Vgl. Beier, M.; von Gizycki, V. (2002), S. 1.
458 Stapelkamp, Torsten (2007), S. 514.
459 Vgl. Stapelkamp, Torsten (2007), S. 514ff.

reichung. Beispielsweise könnte an Stelle der Nutzung eines Informationssystems eine Abfrage an das Assistenzpersonal gestellt werden, welche die erforderlichen Informationen zur Verfügung stellen.

Der Begriff Barrierefreiheit kann nach dem entsprechenden Gesetzestext (Gesetz zur Gleichstellung behinderter Menschen BGG §4, I) als eine Erweiterung der Usability angesehen werden.[460] Gesetzliche Anforderungen des Bundesgesetzes zur Gleichstellung behinderter Menschen von 2002 sind die Verwendung von Text-Äquivalenten, Farbneutralität, Standardkonformität, Sprachwechsel, Tabelle, Abwärtskompatibilität, Kontrolle, Zugänglichkeit, Geräteunabhängigkeit, Verwendung offener Standards, Kontext und Orientierung, Übersichtlichkeit und Verständlichkeit.[461] Die Barrierefreiheit zielt darauf ab, Inhalte und Interaktionen für möglichst alle Nutzergruppen und Endgeräte zugänglich zu gestalten.[462] Diese Maßgabe kann Usabilityanforderungen unterstützen.

Usability bedeutet Bequemlichkeit, die auf der Existenz von bestimmten Geräten, Gegenständen oder Einrichtungen beruht. Eine Einrichtung ist aufgrund ihrer Möglichkeiten und ihrer Ausstattung mit Gegenständen useable, wenn sie für den Menschen Arbeit verringert und ihm Behaglichkeit bietet. Usablility lässt sich allgemein auch als Abwesenheit von Diskomfort, also als Abwesenheit von auffälligen unangenehmen Empfindungen definieren. Hierbei wird davon ausgegangen, dass der Mensch ständig aktuelle mit bisher erlebten Situationen vergleicht. Solange keine Diskrepanzen zwischen dem Erlebten und den an die Situation gestellten Erwartungen bestehen, wird diese Situation nicht bewusst wahrgenommen. Erst wenn Unterschiede auftreten, werden diese konkret festgestellt.[463]

Demnach ist die Usability abhängig von den Erwartungen der Usability Beurteilenden. In Sinne dieser Untersuchung ist die Usability abhängig von den Erwartungen der Führungskräfte. Usability und Diskomfort sind nicht auf der Achse eines Kontinuums angeordnet. Usability ist mit dem Aspekt des Gefallens,

---

[460] Vgl. Stapelkamp, Torsten (2007), S. 518ff.
[461] Vgl. Radtke, Angie; Charlier, Michael (2006), S. 37ff.
[462] Vgl. Radtke, Angie; Charlier, Michael (2006), S. 1.
[463] Vgl. Zhang, L.; Helander, M. G.; Drury, C. G.(1996), S. 377ff.

Diskomfort mit dem Aspekt des Erleidens verbunden. Es ist somit möglich Komfort und Diskomfort zur gleichen Zeit zu erfahren.[464]

Menschen entwickeln eine Usability-Hierarchie. Je mehr Usabilitybedürfnisse bereits erfüllt sind, desto höhere Bedürfnisse werden entwickelt. Die bereits erfüllten Bedürfnisse werden als selbstverständlich angesehen und nicht mehr bewusst wahrgenommen. Führungskräfte haben dabei aufgrund ihrer sozialen und arbeitsrechtlichen Stellung bereits eine sehr hohe Stufe der Usability-Hierarchie erreicht.

Für den Bereich der Informationssysteme bietet die ISO-Norm 9241.11 eine allgemeingültige Definition, in der die Usability als Gebrauchstauglichkeit bezeichnet wird.[465] Diese Norm kann ebenfalls für integrative BIS verwendet werden. Die ISO 9241 ist ein internationaler Standard, der Richtlinien der die Interaktion zwischen Mensch und Computer beschreibt. Sie trägt den Titel „Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten“ und besteht aus insgesamt 17 Teilen, die unter anderem Anforderungen an visuelle Anzeigen, Eingabegeräte und Arbeitsplatzgestaltung betreffen. Die Teile 10-17 behandeln Aspekte der Software-Ergonomie, darunter Grundsätze der Dialoggestaltung und Informationsdarstellung. Der Aspekt Informationsdarstellung trifft im Wesentlichen den Zweck der integrativen BIS.

Gebrauchstauglichkeit bezeichnet die Eignung einer Sache oder eines Gutes in Bezug auf seinen Verwendungszweck. Diese Eignung beruht auf objektiv und nicht objektiv feststellbaren Gebrauchseigenschaften. Da die Beurteilung der Gebrauchstauglichkeit sich aus den Bedürfnissen ableitet, gibt es neben einer objektiven Beurteilung auch eine subjektive Beurteilung, die von Individuum zu Individuum sehr unterschiedlich ausfallen kann.[466] Die Definition der Gebrauchstauglichkeit ist in DIN 55350-11, 1995-08, Nr. 4 geregelt. Sie ist die Eignung eines Gutes im Hinblick auf seinen bestimmungsgemäßen Verwendungszweck und beruht auf subjektiv und nicht objektiv feststellbaren Gebrauchseigenschaften.[467] Geläufiger ist die englische Übersetzung Usability und die Definition der ISO

---

[464] Vgl. Zhang, L.; Helander, M. G.; Drury, C. G.(1996), S. 377ff.
[465] Vgl. International Standardisation Organisation, ISO-Norm 9241-11, (1996).
[466] Vgl. Deutsches Institut für Normung, DIN EN ISO 9241-11 (1999), S. 4.
[467] Vgl. Deutsches Institut für Normung, DIN EN ISO 9241-11 (1999), S. 4.

9241, wonach die Gebrauchstauglichkeit sich aus Effektivität, Effizienz und Zufriedenstellung zusammensetzt.[468]

Die Benutzerfreundlichkeit ist eine Ausprägung der Gebrauchstauglichkeit. Diese wiederum ist definiert als das Produkt der Effektivität, Effizienz und Zufriedenheit. Unter Zufriedenheit fällt die Akzeptanz und Erwartungserfüllung des Nutzers.[469] Weitere Anforderungen ergeben sich aus den ISO-Normen: 9126 (Bewertung von Softwareprodukten), 13407 (Benutzerorientierte Gestaltung), 14915 (Software-Ergonomie für Multimedia-Benutzerschnittstellen) sowie der ISO/IEC 12119 (Software-Erzeugnisse). Die Normen und Richtlinien ergeben Anforderungen, welche den Kanon bilden, um Informationssysteme hinsichtlich der Usablitiy zu untersuchen. Die Anforderungen sind sehr allgemein gehalten und können auf integrative BIS heruntergebrochen werden.

5.1. Gestaltung von Benutzerschnittstellen

Einer der wichtigsten Teilbereiche der Usability ist die Benutzerschnittstelle, mit dieser kommt die Führungskraft bzw. der Nutzer in Kontakt. Sie muss anwendungsgerecht und ergonomisch sein sowie ästhetischen Gestaltungskriterien genügen und ist deshalb Gegenstand der Betrachtung in diesem Kapitel.[470] Beschrieben werden kann eine Benutzerschnittstelle (englisch: user interface) als diejenigen Bestandteile des Mensch-Computer-Systems, mit denen der Mensch über seine Sinne und Motorik mit dem Computer interagiert. Entscheidend sind in diesem Zusammenhang die Modelle der Mensch-Computer-Interaktion.[471]

Menschen unterscheiden sich in ihrer Wahrnehmung und bewerten die Wichtigkeit von Informationen individuell verschieden.[472] Daher ist es von Bedeutung schon die Gestaltung der Benutzerschnittstelle auf den Anwender oder zumindest die Anwendergruppe anzupassen.

Folgende Gestaltungsrichtlinien lassen sich nennen: Nur die für den jeweiligen Benutzer relevanten Informationen dürfen dargestellt werden. Die Informationen müssen so aufbereitet werden, dass sie vom jeweiligen Anwender auch wahrge-

---

[468] Vgl. Deutsches Institut für Normung, DIN EN ISO 9241-11 (1999), S. 4.
[469] Vgl. International Standardisation Organisation, ISO-Norm 9241-11, (1996).
[470] Vgl. Herczeg, Michael (2006), S. 4ff.
[471] Vgl. Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2004), S. 110f; vgl. Herczeg, Michael (2006), S. 35f.
[472] Vgl. Henning, M.; (2003), S. 84.

nommen werden. Zur Sicherstellung der gewünschten Funktionalität ist es von großer Bedeutung, dass die Informationen verständlich dargestellt werden. Liegt eine irreführende bzw. verwirrende Darstellung der Informationen vor, so kann es passieren, dass die Benutzer diese falsch versteht und eine Handlungskette in Gang setzt, die entweder Daten verfälscht oder Systemausfälle bewirkt.[473] Im Extremfall basiert die Entscheidung auf falschen Annahmen und führt zu vermeidbaren Schäden. Des Weiteren entstehen Probleme bei der Funktionalitätssicherung, im Falle von Nicht-Routine-Aufgaben oder auch bei Überladung, wenn dem Benutzer zu viel Funktionalität geboten wird.[474] In Bezug auf integrative BIS liegt der Schwerpunkt auf der Visualisierung der Informationen zur Unterstützung der Aufgaben von Führungskräften. Sollten diese Informationen falsch dargestellt werden bzw. nicht korrekt sein können Entscheidungen getroffen werden, welche für das Unternehmen schwerwiegende Folgen haben.

Falls die Benutzerschnittstelle nicht einfach zu bedienen, sondern überwiegend mit Schwierigkeiten für den Benutzer verbunden ist, führt dies zu einer hohen Fehlerrate bis hin zur Verweigerung der Systemverwendung.[475] Daher ist es notwendig, dass die Bedienbarkeit den Kenntnissen und Fähigkeiten des jeweiligen Benutzers angepasst ist. In der Führungsebene gilt dies insbesondere, da hier selten die Akzeptanz für die Verschwendung von Ressourcen vorhanden ist.

Der Mensch muss bei der Gestaltung der Benutzerschnittstelle schon zu Beginn des Gestaltungsprozesses miteinbezogen werden, um die Bedienbarkeit sicherstellen zu können. Dazu müssen sowohl Anthropometrie, Umgebungseinflüsse wie Beleuchtung, Akustik und Klima, als auch das soziale Umfeld des Benutzers berücksichtigt werden.[476] Entscheidend bei der Berücksichtigung des sozialen Umfelds ist die Tatsache, dass die Benutzerschnittstelle es dem Anwender erlaubt mit anderen zu kommunizieren und nicht isoliert zu arbeiten, aber dennoch nicht zu viele Benutzer gleichzeitig zulässt. Dies gilt insbesondere für integrative BIS.

Menschliche Reaktionen, Gewohnheiten und Verhaltensweisen in die Gestaltung mit einzubeziehen ist eine weitere Forderung, diese wird allerdings kaum ganz

---

[473] Vgl. Sommerville, I. (2001), S. 337.
[474] Vgl. Jahnke, B. (2005).
[475] Vgl. Sommerville, I. (2001), S. 337.
[476] Vgl. Geiser, G. (1990), S. 12f.

gelingen, da der Mensch sehr komplex ist und sein Verhalten schwer vorherzusagen ist. Um sich der Ideallösung anzunähern bedarf es Verhaltensexperimenten. Diese sind im Umfeld von Führungskräften nur schwierig durchzuführen. [477]

Die ökonomischen Nebenbedingungen müssen ebenso bei der Gestaltung der Benutzerschnittstelle berücksichtigt werden. Hierzu zählen Budget- und Zeitrestriktionen sowie Standards, die in den Unternehmen vorgegeben sind.[478] Dies spielt im Hinblick auf die Vorbildfunktion von Führungskräften eine Rolle.

5.2. Mensch-Computer-Interaktion

Um eine Benutzerschnittstelle gestalten zu können ist es wichtig, sich einen Überblick darüber zu verschaffen wie Mensch und Computer miteinander interagieren können. Ausgangspunkt bei der Mensch-Computer-Interaktion ist das Zusammenwirken des Menschen mit einer Maschine zur Bewältigung einer Aufgabe.[479] In diesem Falle das Zusammenwirken der Führungskraft mit dem integrativen BIS mit dem Ziel Unternehmensentscheidungen zu treffen.

Entscheidend für die Interaktion zwischen Mensch und Computer sind die völlig unterschiedlichen Eigenschaften der Komponenten. Der Mensch ist durch seine Sinne, sein Gedächtnis und seine Gewohnheiten gekennzeichnet. Die Sinne stehen dem Menschen zur Aufnahme von Informationen zur Verfügung und das Gedächtnis dient zu deren Speicherung, wobei die Kapazitäten des Kurzzeitgedächtnisses sehr beschränkt und die des Langzeitgedächtnisses sehr groß, dafür aber unzuverlässig sind. Die Intelligentheorie teilt die Fähigkeiten des Menschen in zwei Ebenen, die Ebene I enthält die neutrale Registrierung und Konsolidierung der Reizeingänge und die Bildung von Assoziationen (Assoziative Fähigkeiten), die Ebene II umfasst die Evaluation der Stimuli (kognitive Fähigkeiten)[480].

Die Aufgabenbewältigung des Menschen ist durch seine Gewohnheiten gekennzeichnet. Die Qualität der Aufgabenbewältigung ist abhängig von der jeweiligen Tagesform des Benutzers sowie von den individuellen Gewohnheiten. Bezeich-

---

[477] Vgl. Geiser, G. (1990), S. 17.
[478] Vgl. Jahnke, B. (2005).
[479] Vgl. Geiser, G. (1990), S. 9.
[480] Vgl. Eysenck, Hans Jürgen (1984), S. 244.

nend für den Menschen ist auch, dass er, um seine Leistungsfähigkeit aufrechtzuerhalten, in gewissen Zeitabständen Regenerationsphasen benötigt.[481]

Computer können ihre Leistungsfähigkeit aufrechterhalten, ohne dass Regenerationszeiten essenziell sind. Die Qualität der Aufgabenbewältigung ist bei einem Computer nicht von Gewohnheiten, sondern von der Systemleistung abhängig. Bei Anforderungen, welche die Systemleistung überfordern kann es zwar zu Ausfällen kommen, bleibt aber die Aufgabe der Systemleistung angemessen, kann diese auf konstantem Niveau durchgeführt werden.

Die zur Beschreibung der Interaktion zwischen Mensch und Computer verfügbaren Ansätze gehören zur Kategorie der Beschreibungsmodelle. Exemplarisch wird hier das IFIP-Modell für interaktive Systeme erläutert. Das IFIP-Modell wurde von einer Arbeitsgruppe der International Federation for Information Processing entwickelt und ist gekennzeichnet durch, die Organisationsumgebung (organizational environment), die Ein- und Ausgabeumgebung (terminal environment), die Dialogumgebung (session environment) und die Funktionsumgebung (functional environment). Grafisch wird das IFIP-Modell in folgender Abbildung dargestellt.

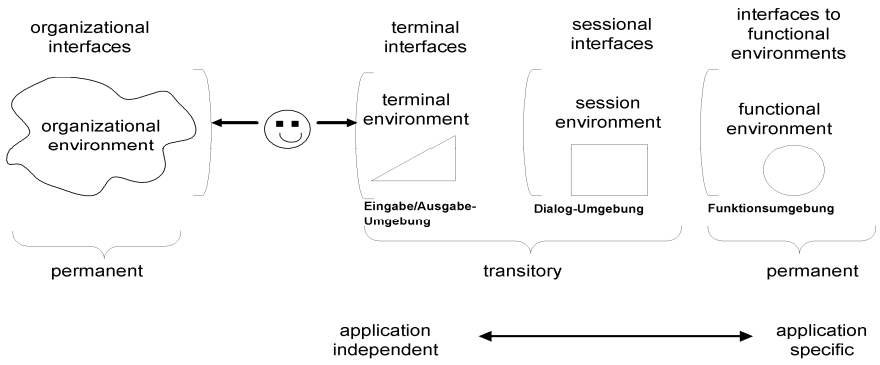

Abbildung 11: IFIP-Modell nach Williamson[482]

---

[481] Vgl. Oberquelle, H. in Eberleh, E.; Oberquelle, H.; Oppermann, R. (1994), S. 96.
[482] Vgl. Groffmann, Hans Dieter (1993), S. 101.

Die Organisationsumgebung bezeichnet die organisatorischen Umweltbedingungen, wie z. B. Verbindungen zu anderen Mitarbeitern oder Interdependenzen der Informationssysteme. Durch die Ein- und Ausgabeumgebung wird die Sicht des Anwenders auf das System beschrieben. In der Dialogumgebung werden die Interaktionsformen des Benutzers mit dem System festgelegt. Die Funktionen zur Manipulation der verfügbaren Informationen befinden sich in der Funktionsumgebung. Eine weitere Unterscheidung kommt bei den einzelnen Schnittstellen noch bezüglich der Unabhängigkeit vom System zum Tragen (Applikationsunabhängigkeit). Während die Ein- und Ausgabeumgebung unabhängig vom System ist, wird die Spezifizierung in Richtung Funktionsumgebung stärker. Das Modell kann zwar nicht die Komplexität der Mensch-Computer-Interaktion darstellen, ist aber gut geeignet die Realität abzubilden. [483]

5.3. Bedienbarkeit von Benutzerschnittstellen

Die Benutzbarkeit der Benutzerschnittstelle definiert sich über die Benutzerreaktionen und deren Abhängigkeit vom Computersystem, den Benutzermerkmalen (Merkmalen der Führungskräfte) und den Aufgabenmerkmalen (Treffen von Entscheidungen).[484] Die funktionalen Aspekte eines interaktiven Programms sind deshalb kein Selbstzweck.[485]

Die Bedienbarkeit wird oft daran gemessen, ob die Benutzung der Schnittstelle leicht zu erlernen ist und ob sie auch leicht zu benutzen ist („easy to learn, easy to use“), dieser Umstand ist besonders im Umfeld der Führungskräfte wichtig.[486] Je schneller der Benutzer sein Ziel erreicht und je weniger Schwierigkeiten dabei auftreten, desto benutzerfreundlicher wird die Schnittstelle eingestuft. Eine BSS sollte so gestaltet sein, dass sie den Schritt von der Intention des Anwenders bis zur Ausführung nicht verzögert oder unnötig aufwendig gestaltet. Sonst kann das Nutzenpotenzial des Systems nicht vollständig ausgeschöpft werden.[487] Hier findet sich der Grund für das Spannungsfeld zu den Sicherheitsmaßnahmen, diese verzögern die Ausführung der Intention des Nutzers durch Barrieren, welche aufgebaut werden, um unberechtigte Nutzer auszusperren.

---

[483] Vgl. Groffmann, Hans Dieter (1993), S. 100f; vgl. Rau, Karl-Heinz (2007), S. 138ff.
[484] Vgl. Eason, K. D. (1984), S. 133f.
[485] Vgl. Stapelkamp, Torsten (2007), S. 471ff.
[486] Vgl. Reitmann-Olson, J. (1985), S. 142ff.
[487] Vgl. Picot, A. (2003), 2003, S. 156.

Ein weiterer Maßstab zur Messung der Bedienbarkeit der Benutzerschnittstelle ist der Aufwand, den der Benutzer freiwillig aufbringt, um Kenntnisse über das System zu erlangen. Ist der Benutzer bereit Zeit zu investieren, um das System genauer kennenzulernen und sich mit den Funktionalitäten vertraut zu machen, spricht das für die Bedienbarkeit der Benutzerschnittstelle. Die leichte Erlernbarkeit spielt für den Zeitaufwand, den der Benutzer bereit ist zu investieren um das System kennenzulernen eine Rolle.[488]

BSS können nach Erlernbarkeit und Benutzbarkeit sowie Aufwand bewertet werden. Der Zeitaufwand sollte gering sein, sowohl beim erlernen als auch beim benutzen, da die spezifischen Umstände von Führungskräften dies erfordern.

5.4. Standardisierung der Mensch-Computer-Interaktion

Bei der Gestaltung von allgemeinen BSS, im Sinne der Mensch-Computer-Interaktion, ist besonders auf die Vereinheitlichung bzw. Standardisierung von BSS zu achten. Unter Standardisierung versteht man eine zu treffende Entscheidung über den Einsatz eines Standards oder einer Auswahlentscheidung zwischen mehreren Standards. Als Standards werden in diesem Fall die DIN 66234 Teil 8 und die darauf aufbauende internationale Norm, die ISO 9241 Part 10, betrachtet. Fraglich bleibt, ob bei BIS eine Standardisierung erwünscht ist, da die Systeme für die wichtigsten Entscheidungen eingesetzt werden sollen und deshalb eine Adaption an den Benutzer fragwürdig sein kann. Gewünscht ist Standardisierung der Benutzerschnittstelle in Hinblick auf die Usability. Eine Standardisierung der hinterlegten Methoden im integrativen BIS ist dagegen als sehr bedenklich anzusehen, da dadurch der Vorteil eines individuell für das Unternehmen angepassten Systems beeinträchtigt wird. Die Fragestellung ist der Entscheidung zwischen der Bereitstellung des objektiven bzw. subjektiven Informationsbedürfnisses ähnlich.[489]

5.5. DIN-ISO-Norm

Die DIN-Norm 66234 Teil 8 „Grundsätze der ergonomischen Dialoggestaltung“, enthält allgemein formulierte Leitlinien, die primär „normierte“ Qualitätseigen-

---

[488] Vgl. Wandmacher, J. (1993), S. 5.
[489] Vgl. Buxmann, P. (1996), S. 10.

schaften für BSS festlegen. Des Weiteren ist die DIN EN ISO 9241-10 einschlägig.[490] Sie ist keine rein technische Norm, sondern in ihr werden Ziele und Anforderungen definiert, die die bisherige Unschärfe der Gestaltungsregeln von BSS ausgleichen sollen. Dabei diente die Darstellung des IFIP-Modells[491] für BSS[492] als Grundlage der Definition.

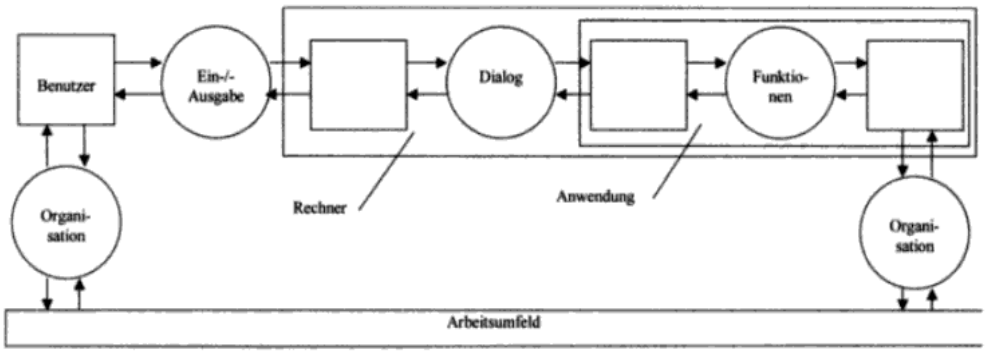

Abbildung 12: Erweitertes IFIP-Modell nach Dizida[493]

Es gibt fünf Grundsätze der Dialoggestaltung, die aus der DIN-Norm 66234 Teil 8 stammen und im Weiteren näher beschrieben werden. Diese sind, Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität und Fehlerrobustheit. Hierbei handelt es sich um Standards nach der Klassifikation von Smith.[494] In ihr werden folgende fünf allgemeine Anforderungen an die Dialoggestaltung von BSS formuliert, welche offizielle Verbindlichkeitscharakteristika besitzen sollen.[495] Diese Grundsätze sind ebenso für integrative BIS gültig. Eine Erweiterung der Prinzipien ist auf Grund ihrer Allgemeingültigkeit nicht notwendig.[496]

Bei der Aufgabenangemessenheit soll die Dialogschnittstelle den Benutzer bei der Erledigung seiner Arbeitsaufgabe unterstützen, ohne ihn zusätzlich durch techni-

---

[490] Vgl. Rau, Karl-Heinz (2007), S. 140.

[491] Dzida erweiterte das IFIP-Modell, indem er drei verschiedene Stufen anwendungsunabhängiger BSS explizit darstellt. Bei dieser Darstellung des IFIP-Modells wurde eine Reihe von Gestaltungsgrundsätzen aufgeführt und in einem analytischen Modell für BSS verankert.

[492] Vgl. Dzida, W. (1983), S. 6-8.; Dzida, W. (1988), S. 13-28.

[493] Herczeg, Michael (2005), S. 116.

[494] Vgl. Smith, S. L. in Helander, M. (Ed.) (1997) ;, S. 45-65.

[495] Vgl. Eckert, Claudia (2006), S. 11.

[496] Die Mensch-Computer-Interaktion wird über die Benutzerschnittstelle abgewickelt, die hinterlegten Methoden welche individuell für das Unternehmen angefertigt sein können werden durch dessen Standardisierung nicht beeinträchtigt.

sche Eigenarten des Systems unnötig zu belasten.[497] Eine unnötige Belastung entsteht z. B. durch Verlassen der Sprachebene auf eine maschinennahe, dem Benutzer fremde Sprachebene. Daraus folgt, dass „Tätigkeiten, die sich aus der technischen Eigenart des Dialogsystems ergeben, im Allgemeinen durch das Dialogsystem selbst ausgeführt werden sollen."[498] Systeminitiiert werden interne Aufgaben selbstständig erledigt. [499] Übrig bleiben die externen Aufgaben, welche vom Benutzer bearbeitet werden müssen.[500] Diese Forderungen können für integrative BIS übernommen werden. Die Benutzerschnittstelle kann hier als Schicht zwischen dem Computersystem und dem Menschen dienen indem sie die Möglichkeiten des Systems dem Benutzer anschaulich darstellt.

Die Komplexität, sowie Art und Umfang der zu verarbeitenden Informationen, wird durch das System reduziert und es kann eine ideale und transparente Arbeitsgestaltung stattfinden. Bei regelmäßig wiederkehrenden Aufgabenteilen oder Werten, die standardmäßig vorgegeben sind, wird eine Vereinfachung vom System empfohlen, indem Standardwerte oder häufig wiederholende Teilaufgaben nicht immer von Neuem eingegeben werden müssen, sondern mit Hilfe von Makros systeminitiiert, automatisch durchgeführt werden können.[501]

Für ein integratives BIS bedeutet dies das vorhalten bereits generierter Abfragen und deren Veränderbarkeit. Wenn es für Vergleichszwecke erforderlich ist, sollen laut DIN 66234 Teil 8 bei Datenänderung die ursprünglichen Daten erhalten bleiben und wieder aufrufbar sein. In Bezug auf integrative BIS sind die Nicht-routine Aufgaben zu beachten. Für diese ist eine Komplexitätsreduktion durch das System kritisch zu betrachten. Die Erhaltung der ursprünglichen Datenbasis über einen

---

[497] Vgl. Deutsches Institut für Normung, DIN 66234, Teil 8: Bildschirmarbeitsplätze, Grundsätze der Dialoggestaltung, S. 2.
[498] Zitat aus DIN 66234, Teil 8: Bildschirmarbeitsplätze, Grundsätze der Dialoggestaltung.
[499] Aufgaben, die durch die Bearbeitung externer Aufgaben mittels Werkzeuge, wie dem Computersystem, anfallen. Sie ergeben sich aus den mit dem Werkzeug auszuführenden Aktivitäten zur Bearbeitung der externen Aufgaben. Als Beispiel für interne Aufgaben können das Inbetriebnehmen des Computersystems, der Start des Textsystems, die Auswahl des Briefmusters, die Festlegung der Schriftform, die Formatierung des Textes, die Benutzung der Funktionen zum Aufbereiten und Ausdrucken eines Briefes genannt werden.
[500] Aufgaben, die im Rahmen der Arbeitsorganisation anfallen. Sie umfassen die eigentliche Problemstellung und sind unabhängig von den Werkzeugen, mit denen die Aufgabe bearbeitet wird, zu sehen. Als Beispiel für eine externe Aufgabe kann das Schreiben eines Geschäftsbriefes genannt werden. Die Aufgabe besteht in erster Linie aus dem Versehen des Briefes mit Anschrift, Absender und Datum sowie aus dem Verfassen und Schreiben des eigentlichen Brieftextes.
[501] Vgl. Herczeg, M. (1994), S. 107.

definierten Zeitraum hin weg ist dagegen eine Kernforderung an Informationssysteme.

Dadurch wird Führungskräften die Möglichkeit gegeben im Fall der Datenänderung eine gleichzeitige Darstellung des aktuellen und des alten Bearbeitungszustandes abzubilden. Eines der wichtigsten Argumente der Aufgabenangemessenheit ist, eine angemessene Funktionalität des Systems, bezogen auf die zu bearbeitende Aufgabe des Benutzers, zu geben. In diesen Zusammenhang gehört auch die Möglichkeit, effektivere Methoden bei der Bearbeitung einer Aufgabe bereitzustellen.[502] Ziel ist es, eine größere Direktheit[503] der BSS herzustellen und kleinere semantische und artikulatorische Distanzen bei der Aufgabenbearbeitung zu überbrücken.[504] Hierbei ist in einem integrativen BIS die Sprache der Führungskräfte zu verwenden. Die Sicherheitsmechanismen sind dagegen so zu gestalten, dass sie in den Hintergrund treten und die Aufgabenerfüllung nicht behindern.

Unter Selbstbeschreibungsfähigkeit versteht man eine Unterstützung des Dialogsystems, indem System- und Funktionszusammenhänge transparent dargestellt werden. Jeder einzelne Dialogschritt ist unmittelbar verständlich. Zusätzlich kann der Benutzer, auf Wunsch, entsprechende Erläuterungen im jeweiligen Dialogschritt erhalten. Prinzipiell ist zu fordern, dass die Erläuterungen des Systems den Kenntnissen des Benutzers und seiner verwendeten Fachsprache angepasst wird. Die Erklärungen sollen kontextabhängig, d.h. am jeweils aktuellen Dialog- und Anwendungszustand orientiert sein.[505] Bei Führungskräften darf die Arbeit mit dem System nicht durch häufiges Nachschlagen erschwert werden. Eine mögliche Alternative zu Handbüchern ist z. B. eine Online-Erklärung, die gezielt auf die Anfragen des Benutzers eingeht. Soweit dies möglich ist, soll ein Verzicht auf systemspezifische Bezeichnungen stattfinden und stattdessen aufgabenbezogene Begriffe oder Ausdrücke aus den jeweiligen Tätigkeitsbereichen der Führungskräfte verwendet werden.

Die Steuerbarkeit ist erfüllt, wenn „der Benutzer die Geschwindigkeit des Ablaufs, sowie die Auswahl und Reihenfolge von Arbeitsmitteln oder Art und Um-

---

[502] Roberts, T. L.; Moran, T. P. (1982), S. 136-141.
[503] Direktheit ist ein subjektives Maß der Übereinstimmung von Zielen und Interaktionsmöglichkeiten und ist umgekehrt proportional zur Distanz.
[504] Hutchins, E. L.; Hollan, J. D.; Norman, D. A. (1986), S. 87-124.
[505] Vgl. Herczeg, M. (1994), S. 108.

fang von Ein- und Ausgaben beeinflussen kann".[506] Dem Benutzer soll die Möglichkeit gegeben werden, die Steuerung des Dialoges selbst vorzunehmen (benutzerinitiiert) oder die Dialogkontrolle dem System zu überlassen (systeminitiiert).[507] In der Praxis liegen jedoch häufig wechselseitige (hybride) Aktivitäten zwischen Benutzer und System vor. In diesem Fall wechselt die Dialogkontrolle während der Arbeit mit dem System. Bei gemischten Dialogen kommt häufig die direkte Manipulation zum Einsatz. Sie geht auf Shneiderman[508] zurück und wird von ihm als Sammelbegriff für BSS mit folgenden Eigenschaften verwendet: Permanente Sichtbarkeit aller relevanten Objekte, ersetzen komplexer Kommandos durch physische Aktionen und schnelle, umkehrbare, einstufige Benutzeraktionen mit unmittelbarer Rückmeldung.[509] Die direkte Manipulation soll zur Reduzierung der Beanspruchung des Benutzers durch leichte Verständlichkeit, vorhersehbare Systemaktionen und Möglichkeit zum Rückgängigmachen von Operationen führen.[510] Diese Forderung gilt allgemein für Informationssysteme zur Verbesserung der Usability.

Dadurch soll Führungskräften ein schnelleres Erlernen der grundlegenden Funktionalitäten ermöglicht werden. Die Ergebnisse ihrer Aktionen sind sofort sichtbar und können bei einem nicht erwünschten Ergebnis jederzeit variiert werden. Besonders bei grafischen Darstellungen von Modellvariablen in Form von Säulen-, Treppen- oder Liniendiagrammen dominiert die direkte Manipulation. Die Elemente dieser Grafiken lassen sich als Objekte interpretieren, mit deren Hilfe über festgelegte Operationen bestimmte Funktionen aktiviert werden können.[511] Des Weiteren soll der Benutzer die Möglichkeit haben, jederzeit bereits ausgeführte Aktionen rückgängig machen zu können (UNDO). Somit sind Fehler durch eine Rücknahmeoption ohne negative Konsequenzen für den weiteren Ablauf. Bei Dialogen ist es wünschenswert, dass sie beliebig zu unterbrechen und wieder auf zu nehmen sind (keine erzwungene Sequenzialität).

---

[506] Vgl. Deutsches Institut für Normung, DIN 66234, Teil 8: Bildschirmarbeitsplätze, Grundsätze der Dialoggestaltung, S. 3.
[507] Vgl. Herczeg, M. (1994), S. 109.
[508] Vgl. Shneiderman, B. (1992), S. 221.
[509] Vgl. Hoffmann, H. (1993), S. 138.
[510] Vgl. Ziegler, J.; Ilg, R. (1991), S. 49.; vgl. Herczeg, Michael (2006), S. 29ff.
[511] Vgl. Hoffmann, H. (1993), S. 143.

Dadurch kann ein Dialog in Etappen erfolgen, wobei der Benutzer über die Geschwindigkeit des Systems selbst entscheiden und diese an seine individuelle Arbeitsgeschwindigkeit anpassen kann. Gerade bei Führungskräften ist es wichtig, BSS derart zu gestalten, dass diese sich auch nach längeren Pausen oder sonstigen Unterbrechungen (z. B. Störungen durch Telefonanrufe) schnell wieder im System zurechtfinden, um den Prozess von der Unterbrechungsstelle an wieder aufnehmen zu können.[512]

Erwartungskonformität bedeutet, dass der Benutzer Erwartungen an das System stellt, die er aus Erfahrungen mit bisherigen Arbeitsabläufen, sowie durch den Umgang mit dem Benutzerhandbuch und der Benutzerschulung bildet.[513] Um den unterschiedlichen Erwartungen entsprechen zu können, soll das Dialogverhalten innerhalb des Dialogsystems einheitlich sein. Das bedeutet, dass ähnliche Arbeitsaufgaben auch ähnliche Dialoge nach sich ziehen.[514] Mit dem Begriff der Einheitlichkeit wird die Konsistenz von Dialogen angesprochen. Ein konsistentes Dialogverhalten bedeutet, dass ähnliche Arbeitsabläufe zu ähnlichen Dialogverläufen führen und der Führungskraft das Gefühl der Durchschaubarkeit oder Transparenz des Systems gegeben wird. Konsistenz ist eine komplexe Forderung und wird in der Praxis, mangels fehlenden Überblicks, häufig verletzt, da zum Beispiel der Wunsch nach verbessertem Design und neuer Funktionalität mit den Vorteilen der Konsistenz in Wettstreit tritt.[515]

Als letzten Punkt der DIN-Norm wird die Fehlerrobustheit angeführt. „Ein Dialog ist fehlerrobust, wenn trotz erkennbarer fehlerhafter Eingabe das beabsichtigte Arbeitsergebnis mit minimalem oder ohne Korrekturaufwand erreicht wird. Dazu müssen dem Benutzer die Fehler zum Zwecke der Behebung verständlich gemacht werden.“[516] Aus psychologischer Sicht sind Fehler, die gemacht werden nicht unbedingt negativ zu bewerten. Vielmehr kann sich bei einer Fehlersituation

---

[512] Vgl. Wandmacher, J. (1993), S. 196; Hoffmann, H. (1993), S. 64.
[513] Vgl. Deutsches Institut für Normung, DIN 66234, Teil 8: Bildschirmarbeitsplätze, Grundsätze der Dialoggestaltung, S. 4; vgl. McIlwraith, Angus (2006), S 94.
[514] Vgl. Wandmacher, J. (1993), S. 197.
[515] Vgl. Manhartsberger, Martina; Musil, Sabine (2001), S. 147; vgl. Herczeg, M. (1994), S. 111-112.
[516] Vgl. Deutsches Institut für Normung, DIN 66234, Teil 8: Bildschirmarbeitsplätze, Grundsätze der Dialoggestaltung, S. 5.

ein Lerneffekt einstellen.[517] Fehler sollen erlaubt sein. Der Benutzer muss trotz fehlerhafter Eingabe, ohne oder nur mit minimalem Korrekturaufwand, zum gewünschten Ziel gelangen können. Fehlermeldungen sollen zur Selbstbeschreibungsfähigkeit beitragen, verständlich, sachlich und konstruktiv formuliert sein. Inhalt und Format von Fehlermeldungen sind möglichst einheitlich und konsistent zu gestalten.[518] Fehler führen insbesondere bei integrativen Business-Intelligence-Systemen zu einem Vertrauensverlust, dieser kann durch Fehlerrobustheit verringert werden.

Ziel der DIN-Norm 66234 Teil 8 ist es, einen ersten Ansatz zur Konkretisierung der Unschärfe von Usabilityanforderungen zu geben und dem Anspruch nach „Benutzerfreundlichkeit“ nachzukommen. Hierbei handelt es sich um allgemein formulierte Leitlinien für die Gestaltung von Dialogen, wobei der Gestaltungsspielraum möglichst groß gehalten wurde. In ihr werden Mindestanforderungen festgelegt, die man mit exemplarischen Beispielen veranschaulicht. Die DIN-Norm liefert einen ersten Beitrag zur Standardisierung von BSS. Diese Standards fordern einen hohen Umsetzungsaufwand und enthalten keine spezifischen Hilfen bei ihrer Umsetzung.[519] Eine vollständige Operationalisierung der genannten Grundsätze ist nicht gegeben. Es können Zielkonflikte zwischen einzelnen Anforderungen entstehen. So kann z. B. bei Maßnahmen, die zu einer Erhöhung der Steuerbarkeit führen sollen, ein Konflikt mit der Selbstbeschreibungsfähigkeit auftreten, da eine Forderung nach größtmöglicher Flexibilität auch damit verbunden ist, dass die Systeme komplexer werden und damit schwer bedienbar.[520]

Der neuere ISO-Standard 9241 Part 10 enthält wesentliche Teile der DIN und ergänzt diese um zwei weitere Gestaltungsgrundsätze für BSS:[521] die Individualisierbarkeit (Adaptierbarkeit) und die Erlernbarkeit. Dialogsysteme sollen die Individualisierbarkeit unterstützen, indem sie so konstruiert sind, dass eine Anpassung an die individuellen Bedürfnisse und Fähigkeiten des Benutzers ermöglicht wird. In diesem Gestaltungsgrundsatz wird eine Flexibilität hinsichtlich individueller Wünsche betont. Dem Benutzer soll die Möglichkeit gegeben werden, be-

---

[517] Vgl. Dzida, W. (1985), S. 430-444.
[518] Vgl. Wandmacher, J. (1993), S. 198.
[519] Vgl. Smith, S. L. in Helander, M. (Ed.) (1997), S. 45-65.
[520] Vgl. Thome, Rainer (2006), S. 149.
[521] Vgl. [Deutsches Institut für Normung (1995); http://wwwvis.informatik.uni-stuttgart.de].

stimmte individuelle Einstellungen vornehmen zu können. Dies sind z. B. Makros, die individuell zusammengestellt werden oder selbst definierte Kurzbefehle. Erkennbar ist, dass das Kriterium der Steuerbarkeit aus der DIN 66234 Teil 8 erweitert wurde und die individuellen Bedürfnisse des Benutzers in den Vordergrund gestellt werden.

Dialogsysteme sollen die Erlernbarkeit unterstützen, indem sie den Benutzer durch den Lernprozess führen und die dabei aufzuwendende Lernzeit minimieren. Die Voraussetzungen hierfür sind die Reduzierung der Komplexität und die Erhaltung der Konsistenz. Die Erlernbarkeit, auch Lernförderlichkeit genannt, hängt von vielen wichtigen, zum Teil schon erwähnten Kriterien (u. a. Steuerbarkeit, Erwartungen und Fehlerrobustheit) ab. Die Problematik hierbei äußert sich in der Qualität möglicher Befehle und in der Komplexität der Anwendung. Es soll darauf geachtet werden, dass in sich abgeschlossene, für den Benutzer verständliche Module gebildet werden, die zur Reduzierung oder einer Verbergung der Komplexität im System führen. Dadurch ist der Benutzer in der Lage, gebildete Module in aufeinanderfolgenden Phasen zu erlernen. Auch in diesem Fall spielt eine Individualisierbarkeit eine wichtige Rolle. Als Beispiel hierfür sei die Unterteilung der gebildeten Module in Laien- oder Expertenmodi genannt. Die Kritikpunkte sind mit denen der DIN-Norm 66234 Teil 8 weitestgehend äquivalent und werden deshalb nicht näher ausgeführt.

Die Normen sind für den Zweck dieser Arbeit nicht konkret genug. Es gilt das spezifische Umfeld der Führungskräfte zu beachten. Viele Bereiche der Usability spielen sich außerhalb der eigentlichen Benutzerschnittstelle ab. Sie ist nur die Schnittstelle nach Extern. Denkbar ist beispielsweise die Performance. Sie ist nicht Ausdruck der eigentlichen Benutzerschnittstelle sondern der gesamten Systemarchitektur.

5.6. Unternehmensstandards und Richtlinien

Viele Softwarehäuser, Hersteller oder industriell orientiere Interessengruppen haben Richtlinien zur Gestaltung von BSS erstellt, die mitunter auch der Öffentlichkeit zugänglich gemacht wurden. Das Ziel der Richtlinien (auch „Styleguides“ genannt) ist es, ein konsistentes Erscheinungsbild und ein „effizientes“ Interakti-

onsverhalten (look and feel) festzulegen.[522] Dabei wird auf eine einheitliche BSS Wert gelegt, um das Problem der Inkonsistenz und Inkompatibilität in den Griff zu bekommen.[523] Ein effizientes Interaktionsverhalten ist, da dadurch Inkonsistenzen vermieden werden können.

Die bekanntesten, unternehmensspezifischen Richtlinien[524] sind: CUA – Common User Access (IBM), Human Interface Guidelines (Apple), Open Look (UNIX), OSF/Motif (Open Software Foundation) und Windows Interface Guidelines (Microsoft). Alle Richtlinien, die oben angeführt werden, enthalten allgemein formulierte Empfehlungen für die Dialoggestaltung mit Beispielen, Erläuterungen und Referenzen.[525] Dabei soll der Verbindlichkeitscharakter, an den sich bestimmte Institutionen und Personengruppen halten müssen, um einen geringen Grad der Allgemeingültigkeit zu erreichen, betont werden. Hieran können sich Entwickler halten, um die Usability des Systems insgesamt zu verbessern und Sicherheitsmechanismen zu integrieren.

Jede Richtlinie hat ein spezifisches Erscheinungsbild (Corporate Image). Dadurch können Hersteller ihre Produkte auch äußerlich, z. B. durch Aufnehmen ästhetischer Stilelemente, von anderen Herstellern differenzieren. Besonders hervorzuheben ist der von IBM entwickelte „Common User Access“ (CUA),[526] der im Rahmen der „System Application Architecture“ (SAA)[527] entwickelt wurde. Die Differenzierung des Herstellers ist für die Verbesserung der Usability von integrativen Business-Intelligence-Systemen nicht von belang, sie wirkt eher nachteilig bei der Verwendung unterschiedlicher Systeme. Von Vorteil ist sie wenn die Aktionen (bspw. Kopieren und Einfügen) durch diese Standardisierung über verschiedene Systeme hinweg gleich bleiben.

---

[522] Vgl. Herczeg, M. (1994), S. 103.
[523] Vgl. Shneiderman, B. (1992), S. 55-58.
[524] Vgl. Wandmacher, J. (1993), S. 211.
[525] Vgl. Wandmacher, J. (1993), S. 211.
[526] Vgl. IBM (1987), S. 2.
[527] SAA ist ein IBM Standard zu Vereinheitlichung der Software. Hierbei handelt es sich um Verein-barungen die Benutzerführung vieler Softwareprogramme, vom PC bis zum Großrechner, einheitlich zu gestalten.

5.7. Individualisierung

Hinter der Aussage „Know The User“[528] steht eine vermeintlich simple Idee. In der Praxis handelt es sich dabei jedoch oft um ein schwer umsetzbares und unterbewertetes Ziel. Benutzer, die mit einem System arbeiten, haben unterschiedliche Fähigkeiten, Präferenzen und Erfahrungen. Um eine Differenzierung vornehmen zu können, muss aus verschiedenen Blickwinkeln heraus eine Anpassung von BSS erfolgen. Dabei wird zwischen adaptierbaren BSS (Adaptierbarkeit) und adaptiven BSS (Adaptivität) unterschieden.[529] Bei adaptierbaren BSS erfolgt eine Anpassung durch den Benutzer selbst. Nimmt das System eine Anpassung der BSS vor, so spricht man von einer adaptiven BSS. Beide Möglichkeiten sind für integrative Business-Intelligence-Systeme gangbare Wege, die Fähigkeiten und Präferenzen der Führungskraft anzunehmen.

Benutzerprofile geben dem Anwender die Möglichkeit, BSS selbst anzupassen. Bei der hier vorliegenden, häufig genutzten Form von Individualisierung, spricht man von adaptierbaren BSS.[530] Der Benutzer ist in der Lage, das System entsprechend seinen jeweiligen Anforderungen, Kenntnissen oder Präferenzen anzupassen. Im Fall von Führungskräften ist eine Differenzierung bei der Erstellung von Benutzerprofilen zwingend notwendig, um die Effizienz des Systems zu erhöhen und eine hinreichende Akzeptanz des Systems zu gewährleisten. In Anlehnung an Shneiderman[531] gibt es verschiedene Benutzertypen, die generisch unterschieden werden, in Anfänger (oder erstmalige Anwender), Erfahrene (periodische Anwender) und Experten (Power-User). Denkbar ist diese Unterteilung bei integrativen Business-Intelligence-Systemen in der Einführungsphase bis die Führungskraft das volle Potential des Systems nutzen kann.

Weitere interessante Typologisierungen liefern Müller-Böling, der eine Einteilung in überzeugte und verhinderte Benutzer vornimmt und Zanger et. al., die verschiedene Altersstrukturen betrachten und diese in drei Benutzertypen (junge Manager, Manager mittleren Alters und ältere Manager) einteilen. Auf eine nähere

---

[528] Vgl. Hansen, W. J. (1971), S. 523-532.
[529] Vgl. Herczeg, M. (1994), S. 175.
[530] Vgl. Herczeg, M. (1994), S. 175.
[531] Vgl. Shneiderman, B. (1987), S. 93.

Betrachtung dieser Ansätze wird jedoch nicht weiter eingegangen, da diese eher einen allgemeingültigen Charakter haben und vorsichtig zu bewerten sind.[532]

Eine andere Möglichkeit der Individualisierung ist die Anpassung der BSS durch das System. In diesem Fall spricht man von adaptiven BSS oder der Adaptivität.[533] Der Benutzer wird vom System beobachtet und daraufhin wird eine systeminitiierte, selbstständige Anpassung des Systems an die Bedürfnisse des Benutzers eingeleitet. Damit möchte man der Gefahr vorbeugen, dass durch das aktive Eingreifen in das System die Qualität einer BSS beeinträchtigt wird.[534] Das System muss Wissen über die Gestaltungsdimension und die Wirkung besitzen, d.h. es muss Wissen über sich selbst haben. Als einfaches Beispiel sei hier die Autokorrektur bei Tippfehlern genannt, oder die Anpassung der Menühierarchie durch eine Sortierung von Menüs nach der Häufigkeit ihrer Auswahl.[535] Jedoch kann hierbei eine mögliche Verletzung der Grundsätze für die Dialoggestaltung bei Erwartungskonformität und Konsistenz eintreten. Eine Entschärfung ist nur möglich, wenn der Benutzer über etwaige Änderungen des Systems informiert und um seine Zustimmung dafür gebeten wird.[536]

Adaptiven BSS wird in Unternehmen und Forschung eine immer größere Bedeutung zugemessen. Bei den beiden, häufig äquivalent gebrauchten, Begriffen „Pervasive Computing“ und „Ubiquitous Computing“[537] (der allgegenwärtigen Informationstechnik) wird davon ausgegangen, dass viele Alltagsgegenstände, in gewisser Weise „smart“ (intelligent) werden.[538] Die dann so genannten transformierten „Smart Objects“ sind mit kleinsten und quasi unsichtbaren Prozessoren und Sensoren versehen und können miteinander kooperieren. Sie sind in der Lage, neben ihrem eigenen Zustand, auch den ihrer Umgebung zu erfassen und mit ihm zu kommunizieren.[539]

---

[532] Vgl. Schinzer, H. (1996), S. 112f.
[533] Vgl. Herczeg, M. (1994), S. 175.
[534] Vgl. Herczeg, M. (1994), S. 181.
[535] Vgl. Mitchell, J.; Shneiderman, B. (1998), S. 33-34.
[536] Vgl. Herczeg, M. (1994), S. 182-183.
[537] Der Begriff wurde erstmals von Mark Weiser 1988 in einer Studie geprägt und wie folgt beschrieben: “Ubiquitous Computing is the method of enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user“
[538] Vgl. Ferguson, G. T. (2002), S. 138-144.
[539] Vgl. Fleisch, E.; Mattern, F.; Billinger, S. (2003), S. 5-14.

Erste Vorboten des Ubiquitous Computing sind internetfähige (datenfähige) Handys, Spielkonsolen, sowie PDA (Persönliche Digitale Assistenten), die drahtlos mit anderen Geräten ihrer Umgebung kommunizieren und es erlauben, über z. B. webbasierten Zugriff, unternehmensinterne Informationen zu portieren. Aus Sicht der Führungskraft kann bei ubiquitären Systemen eine dezentrale Datensammlung, -speicherung und -verarbeitung ermöglicht werden.[540]

Ein mobiler Zugriff auf unternehmensinterne Informationen kann außerhalb der Unternehmung erleichtert werden und somit Effizienz steigernd wirken. Zu beachten ist, dass Techniken nicht isoliert angewendet werden.[541] Eventuell können auch noch neuere Techniken, wie zum Beispiel Sprach- oder Gedankenerkennung im Bereich der Abfragemöglichkeiten oder Audiotextausgabetools für Blinde beziehungsweise sonstige Hilfen zur Unterstützung behinderter in Bezug auf die Darstellungstechniken eingesetzt werden. Auf dies wird im Rahmen dieser Arbeit nicht eingegangen.

5.8. Zusammenfassung

Die Wichtigkeit der Usability von BIS wurde verdeutlicht. Dabei spielt die Anwendersicht auf das System eine entscheidende Rolle, da sich die einzelnen Präferenzen der jeweiligen Benutzer unterscheiden.

Es ist wichtig die Gruppe der Führungskräfte in ihren Entscheidungen unterstützen zu können, da diese für den Unternehmenserfolg signifikant sind. Hierbei muss aufgrund der Zeitrestriktionen der Entscheidungsträger nicht die Quantität, sondern die Qualität der Informationen im Vordergrund stehen. Es ist deshalb eine exakte Bestimmung und Bereitstellung des von der Führungsebene benötigten Informationsbedarfs notwendig.

Da sich die Übermittlung der Informationen über ein Computersystem vollzieht, kommt der Gestaltung und Entwicklung von anwenderfreundlichen Benutzerschnittstellen als Hauptbereich der Usability eine entscheidende Bedeutung zu. Dazu wurden die Eigenschaften und Wünsche des typischen Benutzers ermittelt und diesbezügliche Prinzipien, Normen und Richtlinien vorgestellt, um durch allgemeingültige Grundlagen auf diese Anforderungen des Anwenders einzugehen.

---

[540] Vgl. Hübsch, G.; Springer, T.; Schill, A.; Spriestersbach, A.; Ziegert (2003), S. 42-43.
[541] Vgl. Struckmeier, H. (1997a), S. 154; vgl. Shneiderman, B. (1992), S. 235.

Die angesprochenen Gestaltungsgrundlagen der Benutzerschnittstelle wurden herausgearbeitet. Es gilt zu berücksichtigen, dass es sich um unverbindliche Leitlinien handelt, die situationsabhängig interpretiert werden müssen, also keineswegs in allen Fällen gleich zum Tragen kommen.

Zusammenfassend lässt sich hierzu festhalten, dass sich nicht der Nutzer an das System anpassen sollte, sondern durch die Gestaltung der Benutzerschnittstelle erreicht werden muss, dem User einen möglichst einfachen Zugang zum System zur Verfügung zu stellen. Dieses Ziel ist zu den Sicherheitszielen konkurrierend. Zusammenfassend kann festgestellt werden, dass es keine allgemeingültigen Regeln und kein allgemeines Verständnis von Usability geben kann.

Wichtige Teilaspekte der Sicherheitsmaßnahmen sind: Zugangssicherung und Autorisierung durch Einführung bspw. einer Anmeldefunktionalität durch Benutzername und Passwort oder biometrische Zugangsverfahren sowie die Anwendung von Verschlüsselung und die Bereitstellung durch Firewalls.

Wichtige Usabilityanforderungen sind: Erwartungen von Führungskräften an Informationssysteme; OLAP-Erwartungen (FASMI); Visualisierung einfach und strukturiert; einfache Bedienung; Übersichtlichkeit; wenig Aufwand; individuelle Anpassung; vordefinierte Abfragen; Voreinrichtung; Speicherbarkeit von Abfragen; Geschwindigkeit des Systems sowie die Authentifizierungsgeschwindigkeit.

Es ergibt sich die Fragestellung: Vermindern Sicherheitsmaßnahmen die Bedienbarkeit und beeinträchtigt die Sicherheitsmaßnahme die Führungskraft direkt? Bemerkt die Führungskraft die Sicherheitsmaßnahmen in negativer Weise?

5.9. Zwischenfazit

In diesem Kapitel wurde deutlich, wie wichtig die Gebrauchstauglichkeit bzw. Usability für den verfolgten Zweck eines integrativen BIS ist. Nur wenn die Benutzer hinreichend berücksichtigt werden, verwenden diese das angebotene Unterstützungspotential. Eine negative Wahrnehmung von Sicherheitsmaßnahmen führt zu Reaktanz gegenüber dem angebotenen Unterstützungspotential, dies trifft auch auf Führungskräfte zu.

6. Ökonomische Betrachtung der Risiken und Maßnahmen

6.1. Grundlagen ökonomische Betrachtung

Die Begründung für Investitionen in die IT-Sicherheit wird in Deutschland hauptsächlich mit Forderungen von Behörden und Gesetzen angegeben, da die Geschäftsleitung als Organ der Gesellschaft persönlich für Verfehlungen in diesem Bereich haftet.[542] Entscheidungen werden deshalb oft aus Haftungsängsten anstatt aus ökonomischen Erwägungen getroffen. „Unter dem alleinigen Kostengesichtspunkt ist es unsinnig, eine IT-Schutzmaßnahme zu etablieren, deren Aufwand den Ertrag aus Risikoverringerung und Kosteneinsparung übertrifft."[543] Die Haftungsangst ist jedoch nicht monetär sondern strafrechtlich begründet.[544]

Die Einführung von IT-Sicherheitsmaßnahmen und Verbesserung der Usability von Sicherheitsoperationen ist als Investition im betriebswirtschaftlichen Sinne zu betrachten. Die Betrachtung der Kosten und Nutzen des Investitionsvorhabens bildet die Grundlage für die Entscheidung des Einsatzes einer Sicherheitsmaßnahme.[545] Die Bewertung einer Investition kann durch die Gegenüberstellung von Kosten und Nutzen erfolgen. Ist der Erwartungswert des Nutzens im betrachteten Zeitraum größer als die verursachten Kosten ist die Investition rentabel. Sie muss dann mit der Unterlassungsalternative verglichen werden. Für eine Investition in Sicherheit bedeutet dies den Vergleich aller alternativen Sicherheitssysteme. Ist sie auch in diesem Vergleich besser, sollte die Investition durchgeführt werden. Aufgrund der Anzahl kombinierbarer Größen ergibt sich eine große Menge von Wirtschaftlichkeitsmerkmalen, wobei Produktivität und Rentabilität als die wichtigsten Indikatoren zu nennen sind.[546]

Die folgende Abbildung zeigt die Struktur des Kosten-Nutzen-Vergleiches. Die Wirtschaftlichkeit wird zunächst in einer Gegenüberstellung der Kosten und Nutzen dargestellt. Eine Ebene tiefer werden die Kosten in ihre Bestandteile der direkten und indirekten Kosten unterteilt. Der Nutzen wird in quantifizierbaren und

---

[542] Vgl. Schrey, Joachim in Gründer, Torsten (2007), S. 263f.
[543] Pohlmann, Norbert (2004), S. 85.
[544] Vgl. Pohlmann, Norbert (2004), S. 407.
[545] Vgl. Diedrich, Georg (2006), S. 41.
[546] Vgl. Schumm, Andreas (1996), S. 46; vgl. Jung (2004), S. 29-30.

nicht quantifizierbaren Nutzen klassifiziert. Des Weiteren muss danach der quantifizierbare Nutzen in monetäre und nicht monetäre Bewertbarkeit unterteilt werden. Die Kosten werden nur bis zur Ebene „Direkte und Indirekte“ Kosten dargestellt. Es wird angenommen, dass Kosten meist monetär bewertbar sind.

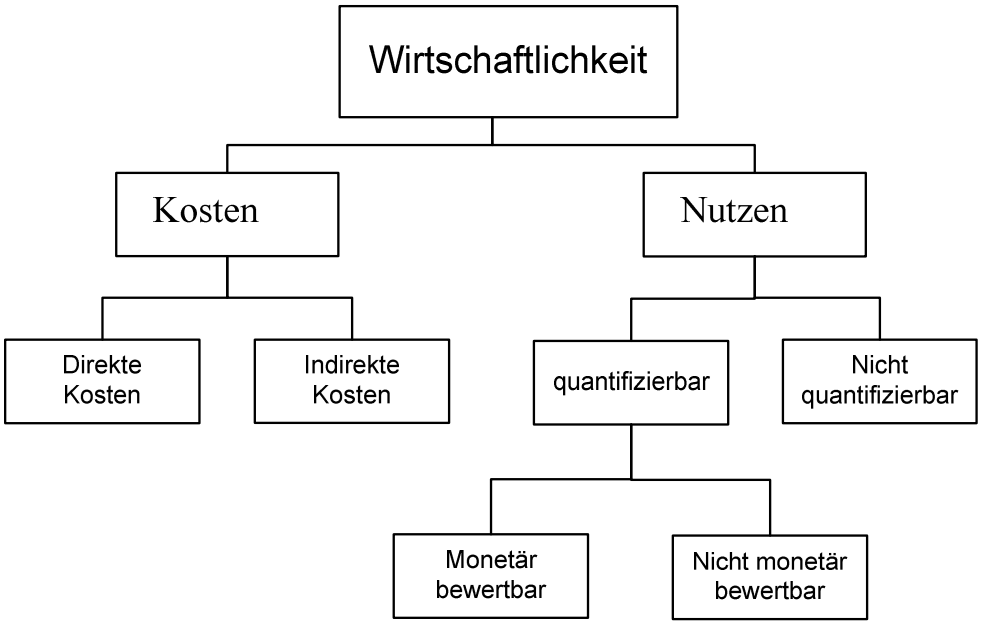

Abbildung 13: Struktur des Kosten-Nutzen-Vergleichs[547]

Vor diesem Hintergrund sind Wirtschaftlichkeitsanalysen ein unverzichtbarer Bestandteil bei der Planung des Einsatzes von Sicherheitssystemen und Usability Maßnahmen.[548] Ein Unternehmen sollte überlegen, was welche Informationen an welchem Punkt ihres Lebenszyklus wert sind und wer auf diese Zugriff haben soll.[549] Deshalb muss die Umsetzung den Anforderungen an die Vertrauenswürdigkeit und Zuverlässigkeit der realen Welt genügen. Dies bedingt ein angemessenes Sicherheitsniveau.[550]

„Die Erhöhung des Sicherheitsniveaus eines IT-Systems senkt den Erwartungswert der Schadenshöhe und somit die Kosten. Diese Senkung des Erwartungswertes ist das Resultat der Verringerung der Eintrittswahrscheinlichkeit der betrachteten Schäden und/oder der jeweiligen Schadenshöhe.“[551] Im unteren Sicherheitsni-

---

[547] In Anlehnung an Stickel, Eberhard (2001), S. 64.
[548] Vgl. Stickel, Eberhard (2001), S. 63.
[549] Vgl. Medosch, Armin (2007), Seite 18.
[550] Vgl. Pohlmann, Norbert; Blumberg Hartmut (2004), S. 31.
[551] Pohlmann, Norbert; Blumberg Hartmut (2004), S. 32.

veaubereich entsteht eine höhere Einsparung als im oberen Punkt. Somit kann ein optimaler Punkt bestimmt werden. Der Aufwand steigt nicht linear sondern überproportional.[552]

6.2. Messung der IT-Sicherheit

Man kann einen Prozess nur dann verbessern, wenn er auch gemessen werden kann, dieses Prinzip kann eingeschränkt auf die Messung der IT-Sicherheit übertragen werden. Das Ausbleiben von Schäden wird in diesem Zusammenhang oft als unzureichende Rechtfertigung für IT-Sicherheitsinvestitionen angesehen und begründet das Misstrauen der IT-Verantwortlichen gegenüber Kosten für die IT-Sicherheit.[553] Durch IT-Sicherheit werden im Allgemeinen keine Erlöse generiert, sie wird deshalb oft als reiner Kostenfaktor betrachtet. Dasselbe Problem stellt sich der IT an sich. „IT-Sicherheitsfunktionen sind immer dann nützlich gewesen, wenn nichts passiert ist“[554]. Es wird deutlich, dass der Nutzen von IT-Sicherheit somit nur schwer monetär quantifizierbar ist.[555]

Für die Messung von Sicherheit wurden der konservative und der progressive Ansatz entwickelt. Innerhalb des konservativen Ansatzes werden Sicherheitsmaßnahmen entweder zur Verringerung der Eintrittswahrscheinlichkeit eines Sicherheitsvorfalles oder zur Minimierung der Auswirkungen nach dem Schadenseintritt eingeführt (Kostenreduktion). Im progressiven Ansatz wird IT-Sicherheit als Wettbewerbsvorteil betrachtet (Nutzen). Im ersten Fall ist es schwierig, die Einsparungen richtig zu ermitteln, weil der Schaden bevor er entstand, verhindert wurde. Je wirksamer die Sicherheitsmaßnahme ist, desto schwieriger wird es, ihren objektiven Nutzen zu messen. Beim progressiven Ansatz sind die durch die Sicherheit zusätzlich generierten Erlöse schwierig in Relation zu den getätigten Sicherheitsinvestitionen zu setzen. [556] Diese Gründe können im Extremum zur Existenzbedrohung der IT-Sicherheitsverantwortlichen führen, da sie ihre Auf-

---

[552] Vgl. Pohlmann, Norbert; Blumberg Hartmut (2004), S. 32.
[553] Vgl. Windemann, P.; Schlienger,T.; Teufel, S. (2006), S. 55; vgl. Lubich, H. P. (2006), S. 8.
[554] Federrath, H. (2006), S. 4.
[555] Vgl. Heitmann, M. (2007), S. 27-28.
[556] Vgl. Müßig, S. (2006), S. 37.

wendungen für die Sicherheit aufgrund statistisch weniger Schäden unzureichend begründen können.[557]

Erfahrungsgemäß werden bisher Sicherheitsmaßnahmen nur dann eingeführt, wenn der Angriff bereits stattgefunden hat und ein Schaden eingetreten ist.[558] Das FUD-Prinzip (Fear, Uncertainty and Doubt) dominierte dadurch die Entscheidungen zur IT-Sicherheit. Die Folge waren subjektiv geprägte, schwer nachvollziehbare Entscheidungen. [559] Zwei Ansätze folgten daraus. Im Rahmen der ex-ante-Analyse soll durch den Kosten-Nutzen-Vergleich die Objektivität bezüglich der Entscheidung für eine Sicherheitsmaßnahme erreicht werden. Die ex-post-Analyse soll getroffene Entscheidungen bestätigen und zukünftige Entscheidungen verbessern.[560]

Es herrscht ein Zielkonflikt, bei dem ein ideales Maß an Sicherheit mit möglichst geringen Kosten anzustreben ist.[561] Ein kostenoptimales Sicherheitsniveau erfordert die Wahl eines ausgewogenen Verhältnisses zwischen Aufwand und Nutzen. Das verbleibende Restrisiko ist durch den Einsatz entsprechender Maßnahmen auf ein akzeptables Maß zu vermindern.[562]

6.3. Kosten mangelnder IT-Sicherheit

Ökonomisch betrachtet existieren beim Betrieb von Informationssystemen zwei Arten von Sicherheitsaufwand. Die Kosten, welche durch Gefahren für die Einrichtungen entstehen und die Kosten für die Schutzmaßnahmen. „Die Kosten aus der Gefährdung, die erwartete Schadenshöhe, bemessen sich aus der Summe der quantifizierbaren Einzelschäden jeweils multipliziert mit der zugehörigen Eintrittswahrscheinlichkeit. Die Kosten der Schutzmaßnahmen summieren sich aus den Aufwänden der einzelnen organisatorischen, administrativen und technischen Schutzmaßnahmen.“[563]

---

[557] Vgl. Lubich, H. P. (2006), S. 8
[558] Vgl. Schadt, D. (2006), S. 17.
[559] Vgl. Cavusoglu, H.; Mishra, B.; Raghunathan, S. (2004.), S. 87 f.
[560] Vgl. Nowey, T.; Federrath, H.; Klein, C.; Plößl, K. (2005), S. 15-26.
[561] Vgl. Werners, B.; Klempt, P. (2005), S. 7.
[562] Vgl. Hoppe, G.; Prieß, A. (), S. 280.
[563] Pohlmann, Norbert; Blumberg Hartmut (2004), S. 32.

Unter Kosten ist auch im Sicherheitsbereich der bewertete Verzehr von Gütern und Dienstleistungen (inklusive öffentlicher Abgaben), die zur Erstellung und zum Absatz der betrieblichen Leistungen sowie zur Aufrechterhaltung der Betriebsbereitschaft notwendig sind, zu verstehen.[564]

Die erwartete Schadenshöhe sinkt mit ansteigen des Sicherheitsniveaus. „Meist kosten die letzen 20 Prozent mehr als die ersten 80 Prozent eines Sicherheitsziels.“[565] Hier müsste aus ökonomischen Gesichtspunkten der Optimalpunkt zwischen Aufwand und Schadenshöhe für das Unternehmen gesucht werden.

Die Kosten selbst entstehen in der Beschaffungsphase, Installationsphase sowie in der Wartungsphase. Zusätzlich zu den Kosten in diesen Phasen müssen die Erwartungswerte der Risiken quantifiziert werden: Es können dafür unterschiedliche Einzelrisiken bestimmt werden. Zur Berechnung des Erwartungswertes des Risikoschadens für das Einzelrisiko gilt die Formel: Schadensbetrag für das Einzelrisiko multipliziert mit der Eintrittswahrscheinlichkeit des Einzelrisikos. Das Gesamtrisiko ergibt sich aus der Summation der Einzelrisiken.[566] Die nachfolgenden Tabellen verdeutlichen die Schäden welche bei der Vernachlässigung von Sicherheitsmaßnahmen 2002 bis 2006 in der <kes> Sicherheitsstudie erfasst wurden.

Durchschnittliche Ausfallzeit:

Sicherheitsvorfall/ Ausfallzeit/Kosten	**2002**	**2004**	**2006**
Virus-/Wurm-Infektion	94h/26228€	55h/25954€	48h/18324€
Hoax	13h/9621€	10h/1270€	36h/2223€
Fehlalarm	10h/8173€	6h/1817€	25h/3367€
Spyware-Befall	-	-	16h/3372€
(erfolgreicher) Online-Angriff	-	-	3h/5600€
Phishing	-	-	2h/980€

Tabelle 6: Ausfallzeiten und Kosten durch informationstechnische Angriffe[567]

Die Tabelle beschreibt die durchschnittlich aufgetretene Ausfallszeit und deren Kosten zur Beseitigung bei eintretenden Sicherheitsvorfällen. Es wurden die Jahre 2002 bis 2006 untersucht. Die Sicherheitsvorfälle Spyware-Befall, erfolgreicher Online-Angriff und Phising wurden in den Jahren 2002-2004 nicht untersucht. Dies zeigt eine Wandlung der Sicherheitsrisiken im Betrachtungszeitraum.

---

564 Vgl. Jung (2004), S. 993; vgl. Corsten, Reiß (1999), S. 315.
565 Pohlmann, Norbert (2004), S. 85.
566 Vgl. Wack, Jessica (2007), S. 24f; vgl. Aebi, Daniel (2004), S. 4.
567 <kes> Sicherheitsstudien 2002, 2004, 2006 in Witt, Bernhard C. (2006), S. 70.

Sicherheitsvorfall	Auftreten	Gefahr	Risiko
Viren	94%	4,8	4,51
Spam	80%	3,3	2,64
Trojanische Pferde	42%	4,5	1,89
Datenverlust	29%	4,6	1,33
DOS	15%	3,7	0,56
Verlust der Systemintegrität	10%	4,3	0,43
Unberechtigter Telekommunikationszugang	9%	4,1	0,37
Diebstahl	7%	4,1	0,29
Verbreitung illegaler Inhalte	9%	3,2	0,29
Betrug	5%	4,0	0,20
Manipulation von Systemprogrammen	5%	4,0	0,20
Manipulation von Anwendungen.	4%	4,1	0,16

Tabelle 7: Auftreten, Gefahr und Risiko von Sicherheitsvorfällen[568]

Die Tabelle setzt das Auftreten die Gefahr und das Risiko von Sicherheitsvorfällen zueinander in Beziehung. Die Spalte Auftreten wurde prozentual bewertet. Gefahr und Risiko wurden anhand einer Skala von 6 für sehr gefährlich bis 1 für nicht gefährlich eingestuft. Es ist ersichtlich, das der Sicherheitsvorfall mit einer Wahrscheinlichkeit eintritt. Die Gefahr des Vorfalls sowie das eintretende daraus folgende Risiko werden ebenfalls bewertet.

Der bedeutendste Sicherheitsvorfall ist damit der Befall von Viren. Die entstehenden Kosten (siehe vorherige Tabelle) wie auch die Eintrittswahrscheinlichkeit und die aus dem Sicherheitsvorfall resultierende Gefahr für das Unternehmen sind sehr hoch.

---

[568] IT-Security (2004); http://silicon.de in Witt, Bernhard, C. 2006, S. 93.

Gefahrenbereich/ Rangbezogene Bedeutung/ Rangbezogene Erwartung	**1998**	**2000**	**2002**	**2004**	**2006**
Fehler eigener Mitarbeiter	½	½	1/2	1/2	1/2
Malware (Viren, Würmer, trojanische Pferde, …)	2/1	2/1	2/1	2/1	2/1
Softwarebedingte Defekte	3/3	3/3	3/3	4/5	3/5
Hardwarebedingte Defekte	4/7	4/10	6/10	6/8	4/6
Unbefugte Kenntnisnahme	6/4	5/4	4/5	¾	5/3
Fehler durch Externe	7/8	8/7	10/4	7/9	6/7
Hacking (richtig Cracking)	-	-	5/6/	5/3	7/4
Dokumentationsbedingte Defekte	8/6	7/5	9/8/	10/10	8/9
Manipulation zur Bereicherung	8/5	9/6	8/9	9/7	9/8
Höhere Gewalt	4/8	6/8	7/11	8/11	10/11
Sabotage (inkl. DOS)	10/10	10/9	11/7	11/6	11/10

Tabelle 8: Gefahrenbereiche[569]

6.3.1. Kostenarten der IT-Sicherheit

In Bezug auf Sicherheitsmaßnahmen entstehen Kosten in folgenden Phasen: Analysephase, hier wird untersucht ob Sicherheitsmaßnahmen notwendig sind bzw. ob auf Sicherheitsmaßnahmen verzichtet werden kann. Auswahl der Sicherheitsmaßnahmen. In dieser Phase werden verschiedene Sicherheitsmaßnahmen gegeneinander abgeglichen. Einführung der Sicherheitsmaßnahmen, es handelt sich um die organisatorische Einbettung sowie um die Inbetriebsetzung der Sicherheitsmaßnahmen. Betrieb der Sicherheitsmaßnahmen, hier werden Kosten für den Betrieb erfasst. Wartung der Sicherheitsmaßnahmen, da Sicherheitsmaßnahem veralten ist es notwendig die entsprechenden Updates und Sicherheitskontrollen mit zu betrachten. Zu den finanziellen Schäden kommen Folgeschäden wie Image- und

[569] <kes Sicherheitsstudien 1998-2006 in Witt, Bernhard C. (2006), S. 95f.

Vertrauensverlust bei den Kunden sowie Schwächung der Mitarbeitermotivation.[570] Der Verlust von Daten kann ebenso wie ein Produktivitätsverlust für Unternehmen eine ernst zu nehmende Gefahr darstellen.[571] Hardwaredefekte können dieser Klassifizierung folgen: Reparaturkosten, Datenverlust und Ausfallzeit.[572]

6.3.2. Direkte Kosten

Direkte Kosten schließen alle Aufwendungen ein, die bei der jeweiligen IT-Abteilung durch das Anbieten ihrer Leistungen gegenüber ihrem Unternehmen aufkommen. In diese Kategorie fallen Kosten für Hard- und Software sowie der damit unmittelbar hervorgerufene Personalaufwand.[573]

Integrative Business Intelligence Systeme erfordern eine leistungsfähige Hardware, diese kann gekauft oder geleast werden. Es fallen also entweder Anschaffungskosten an, die dann über die geplante Nutzungsdauer abgeschrieben werden müssen, oder es müssen die Leasing- bzw. Mietraten aufgebracht werden. Mit dem/der Kauf/Miete von Hardware sind noch nicht alle von der Hardware verursachten direkten Kosten erfasst. Weiterhin sind vor allem die Kosten für Hardwarewartung und -reparatur, sowie Versicherungen zu berücksichtigen.[574] In diesem Zusammenhang stehen die Kosten für eine eventuelle Neuanschaffung und die Kosten für die erforderlichen Speichermedien im Vordergrund.

Falls noch nicht vorhanden, sind häufig zusätzliche Investitionen in ein Netzwerk erforderlich, um den in- und externen Informationsaustausch zu gewährleisten. Des Weiteren sind häufig Investitionen in die Arbeitsplatzsysteme des vorgesehenen Anwenderkreises erforderlich.

Ein weiterer großer Komplex direkter Kosten bei der Einführung eines integrativen BIS entsteht durch die Beschaffung der erforderlichen Software. Dabei sind nicht nur die Kosten der originären Anwendungsprogramme wie Datenbank, OLAP, Data Mining, Reportfunktionen und Analyse zu berücksichtigen sondern

---

[570] [PriceWaterhouseCoopers (2005); http://www.pwc.de].
[571] Vgl. Kersten, Heinrich (1991), S. 51.
[572] Vgl.[Sager, Michael (2005); http://www.wwsinternational.net], S. 9.
[573] Vgl. [Schwickert (2000); http://wi.uni-giessen.de], S. 10.
[574] Vgl. Schumm, Andreas (1996), S. 59.

auch Programme für die Überführung und Pflege bestehender/zukünftiger interner und gewünschter externer Daten.[575]

Installation und Konfiguration der Software stellen einen weiteren wesentlichen Kostenfaktor dar. Obwohl Software häufig zentral auf Netzservern zur Verfügung gestellt wird und über das Local Area Network bezogen werden kann, ist bei unterschiedlicher Konfiguration der Arbeitsplatzrechner häufig eine spezielle Installation bzw. Konfigurationsanpassung erforderlich. [576] Dieser Aspekt leitet zu den Personalkosten über. Zur ordnungsgemäßen Einführung und Erklärung der Systeme muss entsprechendes Fachpersonal zur Verfügung gestellt werden. Außerdem ist Fachpersonal zur Unterstützung der Endbenutzer bei der Behebung von Problemen bei der PC- und Softwarenutzung erforderlich.[577] Auch hier ist es notwendig, sorgfältig zu prüfen, ob dieser zusätzliche Personalbedarf kostengünstiger durch eigenes Personal oder durch die Vergabe externer Aufträge befriedigt werden kann.

6.3.3. Indirekte Kosten

Unter den indirekten Kosten eines IT-Systems versteht man diejenigen Aufwendungen, die aus den effizienzhemmenden Vorgängen während der Nutzung einer IT-Infrastruktur entstehen.[578] Indirekte Kosten sind ein nicht zu unterschätzender, wesentlicher Bestandteil der Gesamtkosten bei der Einführung und Nutzung eines integrativen BIS.

Normalerweise fallen sie nach der Installation und Inbetriebnahme des Systems an. Typischerweise werden sie z. B. durch nachträgliche Aufrüstung der Client-Systeme, notwendiger Verbesserung von Netzwerkstruktur und –durchsatz, erforderlichem Upgrade assoziierter Software und einem über das ursprünglich vorhergesehene Ausmaß an Ausbildung hinausgehenden Bedarf an Schulung hervorgerufen. Ein wesentlicher Teil der indirekten Kosten entsteht aber auch durch den anfänglichen Verlust an produktiver Arbeitszeit einzelner Mitarbeiter. Zuerst müssen die Benutzer an einer Schulung teilnehmen und/oder sich autodidaktisch in die Anwendung einarbeiten, wodurch ein Arbeitsausfall entsteht. Außerdem ist

---

[575] Vgl. Potthof, Ingo (1998), S. 93; vgl. Voß, Stefan; Gutenschwager, Kai (2001), S. 224-225.
[576] Vgl. Schumm, Andreas (1996), S. 59-60.
[577] Vgl. Schumm, Andreas (1996), S. 59-64.
[578] Vgl. Krcmar, Helmut (2005), S. 161; [Schwickert (2000); http://wi.uni-giessen.de], S. 1.

zu berücksichtigen, dass trotz Schulungen und Verfügbarkeit von Benutzerhandbüchern, es immer eine gewisse Zeit braucht, bis der Benutzer routiniert mit dem jeweiligen System umgehen kann.[579]

Nach erfolgreicher Einführung und andauernder Nutzung eines integrativen BIS stellt sich eine immer stärker werdende Abhängigkeit der innerbetrieblichen Prozessabläufe von der Verfügbarkeit dieser Funktion ein. Als Folge müssen daher oft die Standards für die Verfügbarkeit der Hardware den erhöhten Ansprüchen angepasst werden, was zu erheblichen Folgekosten führen kann. In diesem Zusammenhang spielen Technologien, die je nach der Abhängigkeit eines Unternehmens von der Verfügbarkeit bestimmter Geschäftsprozesse, wirtschaftlich sinnvoll eingesetzt werden können, wie „fault tolerant", „high availability", „continous availability" und RAID (Redundant Array of Inexpensive Disks) für Festspeicher eine Rolle.

Seit einigen Jahren wird auch das sog. „fuzzing" als bedeutende Quelle indirekter Kosten genannt. Unter „fuzzing" versteht man die Zweckentfremdung eines Systems für eigene Vorhaben wie z. B. privates surfen im Internet und Nutzung von Geschäftscomputern für andere private Zwecke. Durch diesen Missbrauch entsteht häufig ein nicht unerheblicher Arbeitszeitverlust.[580]

Eine genaue Abschätzung der Kosten, die auf ein Unternehmen im Zuge der Einführung und des Betriebes eines integrativen BIS zukommen, ist nur schwer durchführbar. In diesem Zusammenhang wird oft der 1987 von der Gartner Group geprägte Begriff „Total Cost of Ownership"(TCO) erwähnt.[581] Grundlage der Kostenermittlung nach dem TCO-Verfahren, ist der gesamte Lebenszyklus einer Installation; d.h. sie umfasst alle Kosten, die während der Entwicklung, dessen Einsatz/Gebrauch, einschl. der notwendigen Unterstützung, eines IT-Projekts anfallen.[582] Damit sind sowohl direkte als auch die indirekte Kosten erfasst. Dieses Erfassungsverfahren zeigt sehr deutlich, das die reinen Anschaffungskosten oft nur einen Bruchteil der Gesamtkosten ausmachen.[583]

---

[579] Vgl. Schumm, Andreas (1996), S. 62; vgl. Godschalk, David (2007), S. 205.
[580] Vgl. [Schwickert (2000); http://wi.uni-giessen.de], S. 14.
[581] Vgl. [Amberg (2004); http://www.wi3.uni-erlangen.de], S. 13.
[582] Vgl. Kyrer, Alfred (2001), S. 564.
[583] Vgl. [Quality (2005); http://www.quality.de]

Das „Total Cost of Ownership“ Modell betrachtet nur die Kosten eines Projektes und nicht seinen Nutzen. Grundsätzlich liefert die TCO-Methode jedoch einen besseren Ansatz zur Kostenschätzung als viele andere Verfahren. Allerdings muss, speziell bei der Bewertung der indirekten Kosten, kritisch vorgegangen werden, da sie sich oft nicht exakt quantifizieren lassen (z. B. Kosten der Verminderung der Arbeitsproduktivität während der Systemeinführung, Kosten des „fuzzing“ usw.). Da für eine wirtschaftlich sinnvolle Entscheidung über die Durchführung eines Projektes nicht nur von der Kostenseite her entschieden werden kann, ist eine alleinige Betrachtung der TCO nicht sehr aussagekräftig. Generell ist für eine betriebswirtschaftliche Entscheidung das Verhältnis von Kosten und Nutzen entscheidend. Da die TCO-Methode nur die Kostenseite abdeckt, bedarf es zur Entscheidungsfindung noch weiterer ergänzender Verfahren, wie z. B. einer „RoI“-Analyse.[584]

6.3.4. Erfassbarkeit des Nutzens

Nachdem die Kosten ermittelt wurden, muss der Nutzen operationalisierbar gemacht werden. Die Bewertung eines Gesamtnutzens von komplexen Projekten ist nahezu unmöglich.[585]

Der Nutzen durch die Einführung und Nutzung eines integrativen BIS ist nur sehr schwer monetäre zu bewerten,[586] da hier viele Faktoren eine Rolle spielen, welche auf die unterschiedlichen Teile eines Unternehmens Einfluss nehmen. So sind beispielsweise Erwartungen wie höhere Qualität oder Wettbewerbsvorteile gegenüber Mitkonkurrenten schlecht messbar.[587] Dementsprechend schwierig ist die Wirtschaftlichkeitsanalyse, da den Kosten der Nutzen entgegengestellt werden muss. Bei einer Investition in ein integratives BIS muss der Erfolg sichtbar werden.[588]

Problematisch sind hierbei die sehr unterschiedlichen Anforderungen, welche an ein integratives BIS gestellt werden. Genannt werden Kosteneinsparungen, bessere Aufbereitungsmöglichkeiten, Eindämmung der Informationsflut sowie Verbes-

---

[584] Vgl. [Amberg (2004); http://www.wi3.uni-erlangen.de] S.13.
[585] Vgl. Wieczorrek, Hans, W.; Mertens, Peter (2007), S. 233.
[586] Vgl. Vetschera, Rudolf (1996), S. 217; vgl. Franke, G. in Hichert, Rolf (1995), S. 213f.
[587] Vgl. Stickel, Eberhard (2001), S. 63.
[588] Vgl. Stickel, Eberhard (2001), S. 65; vgl. Vetschera, Rudolf (1996), S. 217; vgl. Stahlknecht, Peter; Hasenkamp, Ulrich (2004), S. 249.

serung der Informations- und Entscheidungsqualität. Bei solchen Zielvorstellungen ist der erwartete Nutzen schwierig zu beziffern.[589]

Es kann zwischen qualitativen und quantitativen Nutzen unterschieden werden. Der Nutzen einer Sicherheitsmaßnahme resultiert in der Regel in einer Erhöhung der Verfügbarkeit, Integrität und Vertraulichkeit.[590] Weiterer Nutzen ist die Verbesserung der Marktstellung und das positive Image einer Unternehmung. Hier wird eine Vertrauensbasis gegenüber Kunden und Lieferanten durch IT-Sicherheit geschaffen und in Arbeitsbereichen mit sensiblen Daten wird erhöhte Sicherheit für die Gewinnung neuer Kunden verantwortlich gemacht.[591] Des Weiteren wird die Reduzierung von Schäden, die Erhöhung der Ausfallsicherheit, die Begrenzung des Know-how-Verlustes, verbesserte Wirtschaftlichkeit durch die Aufrechterhaltung der Verfügbarkeit und Erschließung neuer Geschäftsfelder angeführt. Diese Nutzenarten bereiten die meisten Probleme bei der Wirtschaftlichkeitsbetrachtung, da sie schwierig monetär zu bewerten sind.[592]

Quantitativer Nutzen ist durch Einsparungspotenziale durch den Einsatz von IT-Sicherheit gekennzeichnet und somit leichter quantifizierbar. Der Nutzen der IT-Sicherheit stellt die Reduzierung der Risiken und Verluste durch Sicherheitsereignisse, potenzielle Schadenshöhe sowie Eintrittswahrscheinlichkeit eines Schadensereignisses dar, diese sind ungewiss.[593]

6.3.5. Nutzeneffekte

Ein integratives BIS kann verschiedene Arten des Nutzens hervorrufen. Diese Effekte lassen sich in drei Kategorien einteilen.[594] Direkt realisierbare Kostensenkungspotenziale: Durch die Einführung eines Systems treten unmittelbare Kostensenkungen auf. Ein gleiches Ergebnis kann durch den Einsatz des Systems mit weniger Aufwand erzielt werden, wenn es beispielsweise vorher manuell errechnet werden musste. Rationalisierungseffekte werden erzielt. Die Produktivität

---

[589] Vgl. Fritz, Burkhard (1999), S. 100.
[590] Vgl. BSI (2000), S. 118.
[591] Vgl. Saleck, T. (2005), S. 123.
[592] Vgl. Heitmann, M. (2007), S. 28-29; vgl. BSI (2000), S. 118.
[593] Vgl. Nowey, T.; Federrath, H.; Klein, C. ;Plößl, K. (2005), S. 16.
[594] Vgl. Stickel, Eberhard (2001), S. 75.

kann durch den Einsatz von integrativen Business-Intelligence-Systemen gesteigert werden, indem gewohnte Arbeiten durch das System unterstützt werden.[595]

Vom Einsatz eines BIS verspricht man sich qualitative Effekte, beispielsweise verbessertes Datenmaterial und dadurch geringere Fehlerhäufigkeit.[596] Führungskräfte werden von Routinearbeiten, wie zum Beispiel der Informationssuche, entlastet, und können sich so wichtigeren Tätigkeiten widmen.[597] Eine Entlastung findet ebenso dadurch statt, dass untere Ebenen im Unternehmen zusätzlich Teile der Aufgaben der Führung übernehmen, da leistungsfähige Systeme auch Expertenwissen vermitteln können.[598]

Strategische Nutzeffekte bringen einem Unternehmen mittel- bis langfristige Wettbewerbsvorteile gegenüber Konkurrenten. Mehrere Ziele werden mit solchen Effekten verbunden. Bspw. sollen durch die Nutzung von Informationen, die den Mitbewerbern nicht zur Verfügung stehen, Wettbewerbsvorteile erlangt werden. Weitere Ziele in diesem Bereich sind die Schaffung neuer Produkte und Produktvarianten, höhere Produktqualität und schnellere Reaktionszeiten.[599] Ein weiterer Effekt könnten erhöhte Markteintrittsbarrieren für neue Konkurrenten sein, da diese ebenfalls in neue Informationssysteme investieren müssten.[600]

Die genannten Vorteile müssen mittel- oder langfristig zu verteidigen sein. Ist das System einfach zu imitieren, treten Nachahmer auf, wodurch die Vorteile gegenüber Mitbewerbern verschwinden. Dann bleibt es beim Status quo, bei steigenden Kosten.[601]

6.3.6. Kriterien der Nutzenbewertung

Der größere Teil des Nutzens liegt nicht bei direkten Kosteneinsparungen, sondern in einem verbesserten Entscheidungsprozess. In der folgenden Abbildung wird gezeigt, dass die Eigenschaften des Systems auf den Entscheidungsprozess

---

[595] Vgl. Geier, Christoph (1999), S. 125f.
[596] Vgl. Stickel, Eberhard (2001), S. 75f.
[597] Vgl. Hichert, Rolf; Moritz, Michael (Hrsg.) (1995), S. 125f.
[598] Vgl. Stickel, Eberhard (2001), S. 76.
[599] Vgl. Stickel, Eberhard (2001), S. 92ff.
[600] Vgl. Geier, Christoph (1999), S. 126.
[601] Vgl. Stickel, Eberhard (2001), S. 93.

einwirken. Die Umsetzung der Entscheidung ergibt die Konsequenzen, welche für die Bewertung von Informationssystemen das entscheidende Kriterium sind.[602]

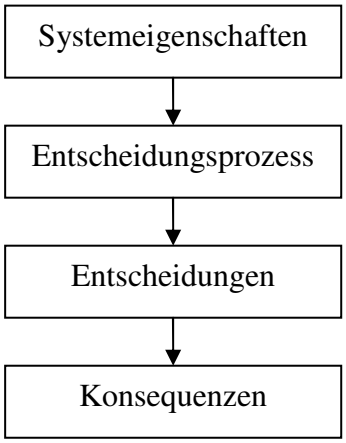

Abbildung 14: Gesamtzusammenhang der Wirkungen von BI-Systemen[603]

Die Kenntnisse des Nutzens eines integrativen BIS ermöglichen eine einfachere Bestimmung des Wertes der vermiedenen Schäden. IT-Sicherheit stellt ebenfalls einen Nutzen dar.

6.4. Methoden zur Wirtschaftlichkeitsbeurteilung

Finanzwirtschaftliche Kennzahlen, wie Return on Investment (ROI), total Cost of Ownership (TCO) Playback und Produktivität werden angeführt, wenn der Nutzen einer Investition quantifiziert werden soll. Auch wenn die Kennzahlen einfach definiert sind, ist es schwierig sie korrekt zu berechnen und den qualitativen schlecht quantifizierbaren Nutzen zu beachten. [604]

Nutzeneffekte können mit Verfahren der Investitionsrechnung ermittelt werden. Dabei ist zwischen einperiodischen und mehrperiodischen Verfahren zu unterscheiden.[605] Einperiodische Verfahren, wie Kostenvergleichs-, Gewinnvergleichs-, Rentabilitäts- und Amortisationsrechnung (Amortisation = Investition/(Schadensrisiko-Restrisiko) [in Jahren][606]), berücksichtigen nicht oder nur un-

---

602 Vgl. Vetschera, Rudolf (1996), S. 218.
603 Vgl. Vetschera, Rudolf (1996), S. 218.
604 Gartner Group (1987).
605 Vgl. Kargl, Herbert (2000), S. 41ff.
606 Vgl. Witt, Bernhard C. (2006), S. 94.

wesentlich den Faktor Zeit. [607] Für die Beurteilung eines Investitionsprojektes ist es jedoch notwendig den Zeitpunkt einer Zahlung einzubeziehen.[608] Deshalb werden sie hier nicht näher betrachtet. Die mehrperiodischen Verfahren Kapitalwertmethode und interner Zinsfuß, welche im Folgenden vorgestellt werden, berücksichtigen zeitliche Aspekte.[609]

Zur Bewertung und Ermittlung des Nutzens, welcher sich nicht monetär quantifizieren lässt, sind so genannte mehrdimensionale Verfahren notwendig. Ziel dieser Verfahren ist es, auch den nicht monetären Nutzen von integrativen Business-Intelligence-Systemen darzustellen. Dabei werden das Zufriedenheitsniveau mit den Nutzenwirkungen sowie subjektive Wertschätzungen analysiert.

Kapitalwertmethode: Der Kapitalwert resultiert aus den Rückflüssen, welche sich aus den Einzahlungen (Nutzen) minus den Auszahlungen (Kosten) einer Investition ergeben, abzüglich des Kapitaleinsatzes im Bezugszeitpunkt.[610] Dabei wird von einem festen Kalkulationszinssatz i ausgegangen.[611] Ergebnis der Kapitalwertmethode ist eine Mindestverzinsung, die ein Investitionsvorhaben, in diesem Fall ein integratives BIS, haben muss, um rentabel zu sein.[612] Ein Projekt ist vorteilhaft, falls der Kapitalwert positiv ist. Gibt es mehrere Alternativen für eine Investitionsentscheidung, wird jene mit dem höchsten Kapitalwert gewählt.[613]

Interne Zinsfußmethode: Bei dieser Methode wird ein Zinssatz ermittelt, bei dem eine Investition eine Verzinsung erreicht, sodass der Kapitalwert KW = 0 beträgt. Dadurch wird die effektive Verzinsung des Projektes errechnet, welche dann mit der Soll-Verzinsung verglichen wird. Liegt der effektive Zins gleichauf oder über der Sollverzinsung, ist eine Investition vorteilhaft.[614]

Im Folgenden werden die Verfahren Nutzenwirkungsnetz und Nutzwertanalyse dargestellt. Diese Verfahren sollten als Ergänzung zu den monetären Verfahren

---

[607] Vgl. Pohlmann, Norbert (2004), S. 406.
[608] Vgl. Stickel, Eberhard (2001), S. 77.
[609] Vgl. Kargl, Herbert (2000), S. 45.
[610] Vgl. Kargl, Herbert (2000), S. 46.
[611] Vgl. Stickel, Eberhard (2001), S. 78.
[612] Vgl. Kargl, Herbert (2000), S. 46f.
[613] Vgl. Stickel, Eberhard (2001), S. 78.
[614] Vgl. Kargl, Herbert (2000), S. 46f.

angewandt werden, da die monetäre Bewertung eines Investitionsvorhabens häufig den wichtigsten aber nicht einzigen Faktor darstellt.[615]

Nutzenwirkungsnetz: Dabei werden zu erwartende Nutzeneffekte aufgeschlüsselt und dargestellt. Gemeinsam haben die Nutzenwirkungen die Faktoren Zeit und Kosten. Dadurch lässt sich das Netz letztlich auf monetäre Kriterien aufschlüsseln.[616]

Nutzwertanalyse: Die Nutzwertanalyse wird bei Entscheidungen mit mehreren Zielsetzungen bei verschiedenen Handlungsalternativen eingesetzt. Das Ziel ist eine Anordnung der Alternativen nach ihren Gesamtnutzenwerten.[617] Zuerst wird eine Liste mit entscheidungsrelevanten Kriterien (durch die Entscheidungsträger) aufgestellt. Anschließend werden die Kriterien nach ihrer Bedeutung gewichtet. Dabei bietet sich eine Zahlenskala von null bis zehn an, mit der die Wichtigkeit des Kriteriums dargestellt werden kann.[618] Die Vorgabekriterien drücken die Erwartungshaltungen (der Entscheidungsträger) an das geplante Informationssystems aus.[619]

Als nächster Schritt werden diese Kriterien über die Alternativen hinweg verglichen. Dabei wird der Zielerreichungsgrad für jedes Kriterium ermittelt. Mit den ermittelten Zahlenwerten lässt sich nun die Gewichtung des Zieles mit dem Zielerreichungsgrad des zu bewertenden Systems multiplizieren, wodurch der Teilnutzenwert jedes einzelnen Kriteriums ermittelt wird. Der Gesamtnutzenwert berechnet sich durch die Addition der Teilnutzenwerte. Bei einem Vergleich verschiedener Investitionsalternativen oder zwischen einem IST-Zustand und einer Investition ist die Alternative vorteilhaft, welche den höheren Gesamtnutzenwert aufweist.[620] Problematisch bei der Nutzwertanalyse sind subjektive Einschätzungen, welche sowohl bei der Kriteriengewichtung als auch bei der Bewertung der Zielerreichungsgrade eine große Rolle spielen. Schwierig ist es auch, die Ziele

---

[615] Vgl. Kargl, Herbert (2000), S. 47f.
[616] Vgl. Kargl, Herbert (2000), S. 48f.
[617] Vgl. Geier, Christoph (1999), S. 142.
[618] Vgl. Stickel, Eberhard (2001), S. 79.
[619] Vgl. Kargl, Herbert (2000), S. 49.
[620] Vgl. Stickel, Eberhard (2001), S. 79.

unabhängig voneinander zu halten, da Ziele in der Praxis häufig voneinander abhängen oder konkurrieren.[621]

Um den Gesamtnutzen interpretieren zu können, werden daher zusätzlich Sensitivitätsanalysen durchgeführt, in denen Zielerreichungsgrade und Gewichtung der Kriterien variieren.[622] Eine Möglichkeit zur Verminderung der Gefahr, dass subjektive Einschätzungen das Ergebnis unbrauchbar machen, ist es, die Kriteriengewichtungen und Bewertungen des Zielerreichungsgrades von verschiedenen Personen unabhängig durchführen zu lassen. Stimmen dabei die Ergebnisse tendenziell überein, ist von einer höheren Qualität auszugehen.[623]

Das Time-Salary-Time-Sales(TSTS)-Verfahren ist eine Tätigkeitsprofilanalyse.[624] Es sollen Zeiteinsparungen monetär bewertet werden. Dabei werden zunächst die Zeiteinsparungsmöglichkeiten ermittelt, anschließend diese in eingesparte Personalkosten umgerechnet. Es gibt verschiedene Annahmen, die in diesem Modell getroffen werden. So sind alle Mitarbeiter optimal eingesetzt, außerdem arbeiten die Mitarbeiter effizient für das Unternehmen, es gibt keinen Opportunismus. Mitarbeiter lassen sich darüber hinaus in Klassen einteilen und ihre Tätigkeit in Tätigkeitsklassen. Die Beschäftigten können somit durch ihr Tätigkeitsprofil beschrieben werden. Berechnet wird die Zeit, die der Mitarbeiter durch die Einführung eines neuen Informationssystems spart.[625] Im Gegenzug sind die Personalkosten einer Sicherheitsmaßnahme zu errechnen. Problematisch bei diesem Verfahren ist, dass die unproduktive Zeit nicht errechnet wird. Außerdem bleiben Tätigkeitsverschiebungen von Routineaufgaben hin zu höherwertigen Aufgaben unberücksichtigt.[626]

Im Hedonic Wage Model, welches das TSTS-Verfahren erweitert, werden neben der Monetarisierung der Zeitersparnisse auch Effektivitätssteigerungen einbezogen. Der Einsatz eines Informationssystems verschiebt demnach die Tätigkeitsstruktur zu höherwertigen Tätigkeiten und erhöht damit den Nutzen für das Un-

---

[621] Vgl. Stickel, Eberhard (2001), S. 80.
[622] Vgl. Bea, Franz Xaver; Haas, Jürgen (2001), S. 435.
[623] Vgl. Stickel, Eberhard (2001), S. 80.
[624] Vgl. Potthof, Ingo (1998), S. 19.
[625] Vgl. Stickel, Eberhard (2001), S. 83ff.
[626] Vgl. Stickel, Eberhard (2001), S. 85.

ternehmen.[627] Die Nutzensteigerung können den Kosten gegenübergestellt werden.[628]

Bei der Value Analysis wird davon ausgegangen, dass bei der Einführung eines integrativen BIS das Konzept des Prototyping angewandt wird.[629] Die Entwicklung des Systems ist eher mit einer Investition im Bereich Forschung und Entwicklung vergleichbar, als mit einer Sachinvestition.[630] Es werden zunächst Überlegungen über die zu erwartenden und erwünschten Vorteile eines neuen Systems angestellt. Um diese besser abschätzen zu können, wird ein erster Prototyp des Systems erstellt, da die Vorteile ex-ante zu bestimmen zu schwierig erscheint. In der zweiten Phase werden den zu erwartenden Vorteilen die erwarteten Kosten gegenübergestellt. Ist man der Ansicht, dass die Kosten den Vorteilen angemessen sind, und diese erreicht werden können, wird der nächste Prototyp entwickelt. Kommt man zu einer gegenteiligen Ansicht, wird das Projekt beendet. Dieser Prozess wird wiederholt, bis ein einsatzfähiges System entwickelt wird, oder man das Projekt einstellt.[631]

Das Konzept der Value Analysis strukturiert zwar den Ablauf der Entwicklung eines Informationssystems, gibt dabei jedoch keine Methode zur Nutzenbewertung vor. Problematisch ist die Bindung an ein konkretes System, diese Methode ist daher für eine ex-ante Bestimmung der Auswahl von Systemalternativen nicht geeignet.[632]

Eine weitere Möglichkeit den Nutzen zu quantifizieren ist die Durchführung einer Expertenschätzung, die Messung von vermiedenen Kosten[633], das Minimax-Prinzip, das Maximin-Prinzip oder Optimax-Prinzip.[634]

---

[627] Vgl. Potthof, Ingo (1998), S. 19.
[628] Vgl. Stickel, Eberhard (2001), S. 86.
[629] Vgl. Walterscheid, Heinz (1994), S. 10.
[630] Vgl. Vetschera, Rudolf (1996), S. 236.
[631] Vgl. Vetschera, Rudolf (1996), S. 237f.
[632] Vgl. Vetschera, Rudolf (1996), S. 238.
[633] Vgl. Saleck, Theo (2005), S. 118.
[634] Vgl. Pohlmann, Norbert (2004), S. 406.

In der folgenden Tabelle werden die Verfahren der Wirtschaftlichkeitsanalyse hinsichtlich der quantitativen und qualitativen sowie der Verwendbarkeit zur Überführung in monetäre Werte beschrieben.

Verfahren		Bewertbarkeit			
		Quantitativ, monetär	Quantitativ, nicht monetär	Qualitativ, quantifizier-bar	Rein qualitativ
Semiotik	Syntaktik	Nein	Geeignet	Nein	Nein
	Semantik	Nein	Geeignet	Nein	Geeignet
	Pragmatik	Nein	Gut	Nein	Geeignet
Ein- & wenig-dimensionale Bewertungs-verfahren	Kardinale Nutzentheorie	Geeignet	Nein	Nein	Nein
	Ordinale Nutzentheorie	Nein	Nein	Nein	Gut
	Kostenvergleichs-rechnung	Gut	Nein	Nein	Nein
	Gewinnvergleichs-rechnung	Gut	Nein	Nein	Nein
	Renditever-gleichsrechnung	Gut	Nein	Nein	Nein
	Amortisations-rechnung	Gut	Nein	Nein	Nein
	Kapitalwert-Methode	Gut	Nein	Nein	Nein
	Annuitäten-Methode	Gut	Nein	Nein	Nein
	Interne Zinsfuss Methode	Gut	Nein	Nein	Nein
	Total Cost of Ownership	Gut	Nein	Nein	Nein
	Modell von Porter/Miller	Geeignet	Gut	Nein	Gut
	4-Ebenen-Modell	Geeignet	Gut	Nein	Geeignet
	Verf. v. Sassone/Schwarz	Geeignet	Gut	Nein	Geeignet
	Kennzahlen-methoden	Gut	Gut	Nein	Geeignet
Mehr-dimensionale Bewertungs-verfahren	Nutzwertanalyse	Geeignet	Gut	Gut	Geeignet
	Balanced Scorecard	Gut	Gut	Gut	Gut
	Nutzenanalyse	Gut	Gut	Gut	Geeignet
	Nutzenanalyse nach Nagel	Gut	Gut	Gut	Gut

Tabelle 9: Bewertung ausgewählter Verfahren der Nutzenbewertung[635]

Die Tabelle müsste noch hinsichtlich der Unsicherheit erweitert werden. Ebenso fehlen für eine umfassende Betrachtung bspw. Simulationsmodelle. Des Weiteren ist kritisch die Bewertung (mit durchgehend gut) der Verfahren Balanced Score-card sowie der Nutzenanalyse zu hinterfragen.

---

[635] Diedrich, Georg (2006), S. 97.

6.5. Entscheidungstheorie

Die Entscheidungstheorie beschäftigt sich mit der Erklärung von Entscheidungen (deskriptive Entscheidungstheorie) und mit Normen für Entscheidungen (normative Entscheidungstheorie). Erkenntnisgegenstand der deskriptiven Entscheidungstheorie ist es die Frage zu beantworten, warum Entscheidungen so und nicht anders getroffen werden. Es werden soziologische und psychologische Erkenntnisse verwendet. Die normative Entscheidungstheorie basiert auf der Annahme eines in jeder Situation ökonomisch rational handelnden Menschen (Homo oeconomicus), systematisiert Entscheidungssituationen und leitet Regeln für eine optimale Entscheidung ab. Die normative Entscheidungstheorie nutzt statistische Modelle.[636]

Im Mittelpunkt stehen Entscheidungen über die Auswahl einer Handlungsalternative, die aus einer Vielzahl von Alternativen bei Erfüllung einer Zielsetzung oder auch mehrerer Zielsetzungen ausgewählt werden soll. Voraussetzung ist dabei, dass die gefundene Alternative unter den möglichen Alternativen in Bezug auf die Entscheidungssituation das beste Ergebnis aufweist. Mit Hilfe der mathematischen Entscheidungsmodelle wird die Bestimmung einer optimalen Handlungsalternativen erleichtert. Bei hohem Komplexitätsgrad, geringer Determinierbarkeit und unvollkommenem Informationsgrad der Größen, die in das Modell eingehen, ist die Aussagefähigkeit der mathematischen Modelle begrenzt.[637]

Im Folgenden wird auf die normative Entscheidungstheorie eingegangen. In einer Entscheidungssituation hat der Entscheidungsträger unter Berücksichtigung seiner Zielsetzungen die Wahl zwischen verschiedenen Alternativen. Die Menge aller Aktionen bildet den Entscheidungsraum. Bei der Wahl sind die möglichen Umweltzustände zu beachten. Die Menge der Zustände wird als Zustandsraum be-

---

[636] Vgl. Schinzer, Heiko (1996), S. 9; vgl. Staehle, Wolfgang (1989), S. 484f; vgl. Wissensbach, Heinz (1967), S. 116ff; vgl. Pfohl, Hans-Christian; Braun, Günther, E. (1981), S. 22f; vgl. Pfohl, Hans-Christian (1977), S. 29ff.

[637] Vgl. Schinzer, Heiko (1996), S. 9; vgl. Staehle, Wolfgang (1989), S. 484f; vgl. Wissensbach, Heinz (1967), S. 116ff; vgl. Pfohl, Hans-Christian; Braun, Günther, E. (1981), S. 22f; vgl. Pfohl, Hans-Christian (1977), S. 29ff.

zeichnet. Hinsichtlich der Informationen, die über den Zustandsraum vorliegen, werden verschiedene Entscheidungssituationen unterschieden.[638]

In einer Sicherheitssituation gibt es einen möglichen Umweltzustand, dieser ist dem Entscheidungsträger bekannt. Es steht für jede Alternative ein Ergebnis fest, zu dem die Wahl führt. In der Risikosituation kennt der Entscheidungsträger alle zukünftigen Umweltzustände und kann ihnen eine Eintrittswahrscheinlichkeit zuordnen. Bei einer Entscheidungssituation unter Unsicherheit sind ebenfalls alle möglichen zukünftigen Zustände bekannt, es kann diesen aber keine Eintrittswahrscheinlichkeiten zugeordnet werden. Daneben gibt es die spieltheoretische Situation, in der das Ergebnis der Handlungsalternativen eines Entscheidungsträgers von den Handlungen eines Gegenspielers abhängt. Jede Handlungsalternative führt in Abhängigkeit von den möglichen Umweltzuständen zu einem Ergebnis. Für die Entscheidung zwischen den Alternativen muss jeder Umweltzustand entsprechend den Zielsetzungen des Entscheidungsträgers bewertet werden.

Formal wird dieser Vorgang durch eine Nutzenfunktion (Nutzen) des Entscheidungsträgers beschrieben, mit der jedem Ereignis ein sog. Nutzenwert zugeordnet wird. Eine Entscheidungssituation kann durch eine Entscheidungsmatrix abgebildet werden. Bei einer Entscheidungssituation unter Sicherheit hat die Tabelle nur eine Spalte. Es ist von einem Entscheidungsträger, der lediglich ein Ziel verfolgt, dann die Aktion auszuwählen, die in der Zeile mit dem höchsten Nutzenwert steht. In einer Risikosituation kann die Entscheidungsmatrix um die Eintrittswahrscheinlichkeiten p, der Umweltzustände z, erweitert werden. Eine Entscheidungsregel für die Risikosituation ist das Bayes Prinzip oder auch Erwartungswertprinzip. Bei diesem ist zunächst für jede Handlungsalternative der Erwartungswert der Nutzenwerte zu berechnen. Es sind die Nutzenwerte mit der Wahrscheinlichkeit der zugehörigen Zustände zu multiplizieren und die sich so ergebenden Produkte zu addieren.

Nach dem Bayes Prinzip ist dann diejenige Alternative zu wählen, die den höchsten Erwartungswert hat. Kritisch an dieser Entscheidungsregel ist, dass sie sich nur an dem Erwartungswert orientiert und nicht berücksichtigt, dass die Nutzen-

---

[638] Vgl. Schinzer, Heiko (1996), S. 9; vgl. Staehle, Wolfgang (1989), S. 484f; vgl. Wissensbach, Heinz (1967), S. 116ff; vgl. Pfohl, Hans-Christian; Braun, Günther, E. (1981), S. 22f; vgl. Pfohl, Hans-Christian (1977), S. 29ff.

werte möglicherweise sehr stark um den Erwartungswert streuen können. Ein Maß hierfür ist die Standardabweichung.

Dem Mangel des Bayes Prinzips wird durch den Ansatz begegnet eine Funktion zu bilden, in der sich die Risikoeinstellung des Entscheidungsträgers (Risikoaversion, Risikoneutralität, Risikosympathie (Risikofreude)) ausdrückt. Zu wählen ist die Alternative mit dem höchsten Funktionswert.

Dem Entscheidungskriterium Bernoulli Prinzip liegt folgende Vorgehensweise zugrunde. Hier werden, wie bei der Erstellung der Entscheidungsmatrix, die Ereignisse mit Hilfe einer Nutzenfunktion bewertet. In dieser spiegelt sich neben anderen Präferenzen eines Entscheidungsträgers auch seine subjektive Risikoneigung wider. Bernoulli zeigte, dass unter bestimmten Verhaltensannahmen für jeden Entscheidungsträger eine solche Funktion existiert. Eine Anleitung für die Konstruktion einer solchen Nutzenfunktion gibt es nicht. Nachdem jedem Ereigniswert ein Bernoulli Nutzen zugeordnet wurde, ist der Nutzenerwartungswert zu bestimmen und die Alternative mit dem höchsten Nutzenerwartungswert zu wählen.

Bei Entscheidungen unter Unsicherheit können den möglichen Umweltzuständen keine Eintrittswahrscheinlichkeiten zugeordnet werden. Die Laplaceregel nimmt deshalb alle Umweltzustände als gleich wahrscheinlich an und agiert im Folgenden wie bei der Bayesregel. Eine optimistische Haltung des Entscheidungsträgers unterstellt die Maximax-regel, indem sie diejenige Alternative empfiehlt, die den höchsten Nutzenwert über alle Umweltzustände aufweist. Eine entgegengesetzte Vorgehensweise schlägt die Maximin-regel vor. Nach ihr ist zunächst für jede Alternative der kleinste Nutzenwert über alle Zustände zu bestimmen. Es ist dann diejenige Alternative mit dem größten Zeilenminimum zu wählen. Mit dieser Entscheidung wird also von allen ungünstigsten Fällen der beste ausgesucht.

Einen Ausgleich zwischen den beiden Extrempositionen versucht die Hurwiczregel durch die Einführung eines Optimismus Parameters, der mindestens den Wert 0 und maximal den Wert 1 annehmen darf. Für jede Alternative wird nun über alle Umweltzustände der höchste Nutzenwert Max und der kleinste Nutzenwert Min bestimmt. Anschließend wird (für jede Alternative) der Wert Max, X, + Min, (1 X) bestimmt. Die Alternative mit dem höchsten Wert ist zu wählen. Die Wahl des Parameters X spiegelt die Risikoeinstellung des Entscheidungsträgers

wider. Je größer der Parameter ist, desto optimistischer ist der Entscheidungsträger; je kleiner er ist, desto pessimistischer ist der Entscheidungsträger.

Ebenfalls eine pessimistische Grundeinstellung des Entscheidungsträgers liegt der Savage Niehaus-regel zugrunde. Zunächst wird in jeder Spalte, also für jeden Umweltzustand, über alle Alternativen das Maximum Max(zi) bestimmt. Dann wird für jeden Nutzenwert einer Spalte die Differenz zum Spaltenmaximum Max(zi) uii berechnet. Inhaltlich gibt diese Differenz an, wie groß der Nachteil für den Entscheidungsträger ist, wenn der entsprechende Zustand i eingetreten ist und er sich für eine andere als die zu Max(zi) gehörende Alternative entschieden hat. Anschließend wird für jede Alternative die maximale Differenz notiert. Es ist dann die Alternative zu wählen, bei der dieser Wert am geringsten ist. Diese Alternative weist gegenüber allen anderen Alternativen die Eigenschaft auf, dass bei ihr die Abweichung vom maximal möglichen Nutzenwert durch den Eintritt eines anderen Umweltzustands am geringsten ist.

Von den bisher betrachteten Entscheidungssituationen unterscheidet sich die Spielsituation dadurch, dass die möglichen Umweltzustände durch die Handlung eines rational handelnden Gegenspielers definiert werden. Dabei wird unterstellt, dass der Gegenspieler in einem eigenen, dem Entscheidungsträger entgegengestellten Interesse handelt. Neben diesen sog. Zweipersonenspielen werden in der Spieltheorie auch Mehrpersonenspiele untersucht. Ziel spieltheoretischer Entscheidungsmodelle ist die Ermittlung sog. optimaler Strategien, die dem Entscheidungsträger einen maximalen Gewinn sichern.

In den bisher vorgestellten Entscheidungssituationen war jeweils eine Entscheidung durch den Entscheidungsträger zu treffen. Eine Verallgemeinerung sind mehrperiodige Entscheidungsmodelle. Durch sie sollen Entscheidungssituationen abgebildet werden, in denen ein Entscheidungsträger in mehreren aufeinander folgenden Zeitpunkten Entscheidungen zu treffen hat. Zur Veranschaulichung solcher Situationen wird häufig die Darstellung in Form eines Entscheidungsbaums gewählt. Grundsätzlich ist bei der Untersuchung von Entscheidungsmodellen zu beachten, dass in ihnen nur solche Aspekte einer Entscheidungssituation abgebildet werden können, die bewertbar sind.

Der Wert von Entscheidungsmodellen wird in der wirtschaftspolitischen Praxis durch eine Reihe von Faktoren eingeschränkt: Ökonometrische Modelle sind nur

bei quantifizierbaren Größen einsetzbar. Im Rahmen der Ordnungspolitik, aber auch bei längerfristig wirkenden Reformen sind sie ungeeignet. Sie setzen eine Quantifizierung der Zielfunktionen und der möglichen Mittelkombinationen voraus, über welche die Entscheidungsträger nur in Ausnahmefällen verfügen. Aufgrund falscher oder unvollständiger Spezifikationen, einer ungenauen Schätzung von Parametern sowie nicht immer ausgereifter mathematischer Verfahren liefern die Modelle nur bedingt verwendbare Ergebnisse.

6.6. RoSI als Konzept der Bewertung der IT-Sicherheit

Die Kennzahl Return on Security Investment (RoSI)[639] soll zeigen, ob und wann eine Sicherheitsinvestition einen Return on Investment liefert. Damit könnte ein Nutzen der Sicherheitsmaßnahmen begründet werden. Die Kennzahl selbst wurde an der Universität von Idaho entwickelt und ist im Jahr 2002 auf großes Interesse bei IT-Managern gestoßen.[640] Ob die Kennzahl einen absoluten oder relativen Wert darstellt und welche Einflussgrößen in dieses Modell einfließen, ist noch ungeklärt.[641] Trotz ihrer Mängel bietet die Kennzahl einen Ansatz zur Bewertung der IT-Sicherheit.

Die RoSI-Kennzahl ist wie folgt definiert:[642]

R-S+T = ALE oder R-ALE = RoSI oder RoSI = S-T

R = Kosten der wahrscheinlichen Schäden (Recovery Cost), S = Reduzierung der Kosten der wahrscheinlichen Schäden (Savings), T = Kosten für IT-Sicherheitsmaßnahmen (Tool Cost), ALE = verbleibende Kosten (Annual Loss Expenditure), RoSI = gesparte Kosten, erzielter Profit (Return on Security Investment), somit ist RoSI = Schadensrisiko-Restrisiko-Investition[643] Es wird eine Sicherheitsinvestition getätigt, solange T kleiner als S ist.[644]

Kritisch diskutiert wird hierbei die Tatsache, dass die RoSI-Kennzahl einer Investition von dem Wert der Daten abhängt und solche Werte so bemessen werden

---

639 [Forthmann, Jörg (2005); http://www.presseportal.de]; vgl. Pohlmann, Norbert (2004), S. 418ff.
640 Vgl. Pohlmann, N. (2006h), S. 29; vgl. Berinato, S., (2002.)
641 Vgl. Nowey, T.; Federrath, H.; Klein, C.; Plößl, K. (2005), S. 20.
642 Vgl. Sonnenreich, W.; Albanese, J.; Stout, B., (2006), S.1f.
643 Vgl. Witt, Bernhard C. (2006), S. 94.
644 Vgl. Heitmann, M. (2007), S.36.

können, dass die Investition eine gewünschte RoSI aufweist. Der Hauptkritikpunkt dieses Ansatzes ist, dass anscheinend exakte Werte auf Basis von unsicheren Werten berechnet werden.[645] Das Konzept basiert auf Annahmen und benötigt eine Datenbasis. Trotzdem wird argumentiert, dass in der Praxis unsichere Daten schon genutzt werden, um RoIs zu ermitteln.[646]

6.7. Fazit Nutzen und Sicherheit

Die Güte der Verfahren hängt unter anderem von den Möglichkeiten der Quantifizierung und Monetarisierung ab.

Die Bewertung des Nutzens der Sicherheit von integrativen BIS hängt wesentlich von ihrem Zweck ab. Auf die Bewertung des Schadens wirkt sich die Tatsache negativ aus, dass die unterstützten Entscheidungen strategischer Art sind und dadurch möglicherweise erst in Zukunft erfolgswirksam werden. Dies an sich könnte noch mit dynamischen Erfolgsrechnungsverfahren in Angriff genommen werden. Oft liegt aber der Zeitpunkt außerhalb der in diesen Verfahren angepeilten Zeithorizonte. Die Auswirkungen schlechter Informationen welche durch mangelnde Sicherheitsmaßnahmen entstehen sind nur schwer zuzurechnen.

Das Schadenspotenzial umfasst: Arbeitszeitverlust, Softwareschaden, Reparaturkosten, Produktivitätsverlust, Sachschaden, Hardwareersatz, Verlust durch Diebstahl, existenzielle Unternehmensbedrohung durch entgangene Gewinne, Vertragsstrafe, Verlust von Wettbewerbsvorteilen, Verlust von neuen Produkten, Entscheidungsverzögerung oder Entscheidungsdaten fehlen; diese müssen bewertet werden.

Die ökonomische Betrachtung kann des Weiteren nur sinnvoll auf Produktebene, nicht aber auf Produktklassenebenen vorgenommen werden. Dies liegt zum einen an den gesellschaftlichen Rahmenbedingungen und zum anderen am Schutzbedürfnis der BIS.

---

[645] Vgl. Lubich, H. P. (2006), S. 12.
[646] Vgl. Sonnenreich, W.; Albanese, J.; Stout, B., (2006), S. 1.

7. Spannungsfeld Usability vs. Sicherheit

7.1. Untersuchungsgegenstand

Kernpunkt dieses Kapitels ist die Frage, wie sich die Sicherheitsmechanismen auf die Usability von Informationssystemen auswirken. Aus den vorigen Kapiteln geht hervor, das integrative BIS sich an Führungskräfte wenden. Als Untersuchungsgegenstand ist deshalb die Auswirkung der Sicherheitsmechanismen auf die Usability in Bezug auf Führungskräfte zu wählen. Die Auswirkungen auf andere Mitarbeiter sind nur sekundär einzubeziehen.

Sicherheitsmechanismen herkömmlicher Lesart sind meist von der Art, dass ein Zugang zu einer bestimmten Information oder eine Berechtigung für eine hinterlegte Handlung überprüft wird (Authentifizierung). Diese Überprüfung findet in Form von erschwertem Zugang beispielsweise durch Passwörter statt. Ebenso wichtig ist der Punkt der Verifizierung, die Feststellung der Richtigkeit der Informationen.[647] Sicherheitsmechanismen kosten meist Zeit durch beispielsweise Auswendiglernen oder Eingabe der Authentifizierung und konterkarieren damit die erwünschte Produktivitätsförderung oder Effizienzsteigerung.

7.2. Auswirkungen

Um die Auswirkungen von Sicherheitsmechanismen würdigen zu können müssen zunächst Klassen gebildet werden, die Auskunft über die Beeinträchtigung geben. Folgende Klassen sind zu nennen: Nach der Beeinträchtigung der Funktionalität: Wird die Funktionsweise bzw. Unterstützungsfähigkeit des Informationssystems beeinträchtigt. Starke, mittlere, schwache und keine Beeinträchtigung der Funktionalität.

Nach der Beeinträchtigung der Usability. Wie wird die Benutzerfreundlichkeit des Programms im Vergleich mit dem jetzigen Zustand verändert. Bzw.: Wie benutzerfreundlich ist das Programm gemessen an absoluten Standards. Starke, mittlere, schwache und keine Beeinträchtigung der Usability

Zunächst müssen die allgemeinen Auswirkungen der Sicherheitsmaßnahmen auf die Usability erarbeitet und erfasst werden. Die Auswirkungen ergeben sich aus der Beschreibung der einzelnen Sicherheitsmaßnahmen und deren Aufbau. Fol-

---

[647] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

gende Auswirkungen konnten identifiziert werden: Ressourcenverlust (in der Form von Zeitverlust, Performanceeinbruch, Auswertungszeit); Arbeitszeitverbrauch (Zeitverlust); Lernaufwand (Zeitverlust); Organisationsaufwand (Zeitverlust); Werkzeugblockierung; Transparenzverlust und Komplexitätssteigerung.

Die Aufzählung der Beeinträchtigungen zeigt, dass sich viele Sicherheitsmaßnahmen in ihrer Wirkung auf die Usability-Eigenschaften auf den Faktor Zeit reduzieren lassen. Es wird von der Annahme ausgegangen, dass der Zeitaufwand bei der kombinierten Anwendung von Sicherheitsmaßnahmen messbar steigt. Diese Annahme wurde durch einen Test überprüft und als gültig befunden.

Weiterhin wichtig sind die Auswirkungen auf die Führungskraft als im Fokus stehender Faktor des Mensch-Aufgabe-Technik-Systems im Unternehmen. Die Auswirkungen auf andere Unternehmensmitglieder ist im Sinne von zusätzlichen Kosten zu bewerten, die gesondert in einer Kosten-Nutzen-Rechnung des Informationssystems aufzuführen sind.[648]

7.3. Versuchsaufbau

Die getroffenen Aussagen waren zunächst theoretischer Natur konnten aber empirisch nachgewiesen werden. Dazu wurde eine Performance-Messung durchgeführt. Überprüft wurde die Veränderung eines Prozesses durch Einführung von Sicherheitsmechanismen. Ein PC-Start wurde mit und ohne Anmeldung durchgeführt, Dateiübertragungen sowie Dateiöffnungen wurden mit und ohne Verschlüsselung gemessen, die Passworteingabe und Verschlüsselungsverarbeitung wird getestet. Bei einem Fingerabdruckscanner wurde die Anzahl der Versuche gezählt. Die Versuche zeigten, dass die Einführung aber auch die Kombination von Sicherheitsmaßnahmen zu Zeitverlusten führt. Die aufgeführte Software wurde anhand der aufgestellten Kriterien getestet. Die Beeinträchtigung wurde aufgeteilt in Beeinträchtigungen im engeren Sinn, das heißt das integrative BIS als System wird direkt beeinflusst und Beeinträchtigungen im weiteren Sinn, hier wird die Infrastruktur des integrativen BIS beeinträchtigt. Nachfolgende Tabelle stellt die Untersuchungsergebnisse dar.

---

[648] Vgl. Siebertz, Jens (2004), S 71ff.

7.4. Untersuchungsergebnisse

In der ersten Spalte wird die identifizierte Sicherheitsmaßnahme benannt, in der zweiten Zeile werden die Beeinträchtigungen des integrativen BIS durch die Sicherheitsmaßnahme hinsichtlich der Usability benannt. Die dritte Spalte Benutzbarkeit operationalisiert die Beeinträchtigung in dem diese auf die Forderungen der DIN hin geprüft wurden. Eine Nennung des Begriffes bedeutet eine Beeinträchtigung desselben.

Sicherheits-maßnahme	**Beeinträchtigung des iBIS**	**Benutzbarkeit**	**Kommentar**
Sicherheits-software	Beeinträchtigung durch Zeitverlust, Organisationsaufwand, Werkzeugblockade.	Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Beeinträchtigen die Arbeit mit dem iBIS und die Führungskraft nicht im engeren Sinne.	Sicherheitssoftware kann in Ihrer Gesamtheit die Usabilityanforderungen verletzen.
Scanner			Oberbegriff für eine Gruppe Sicherheitstools, diese sind normalerweise ständig auf einem Rechner aktiv und verbrauchen dadurch Ressourcen.
Virenscanner	Beeinträchtigung durch Zeitverlust, Arbeitszeitverbrauch, Lernaufwand, Organisationsaufwand, Werkzeugblockade, Transparenzverlust, Komplexitätssteigerung, Reaktanz.	Starke Beeinträchtigung der Aufgabenangemessenheit. Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Beeinträchtigen die Arbeit mit dem iBIS nicht im engeren Sinne.	Virenscanner können so eingestellt werden, dass Sie vor jeder Dateioperation diese auf Bedrohungen prüfen, dadurch kommt ein Zwischenschritt zustande der die Beeinträchtigungen je nach Aktion des Scanners auslösen kann.

Sicherheits-maßnahme	Beeinträchtigung des iBIS	Benutzbarkeit	Kommentar
Vulnerability Scanner	Beeinträchtigung kann durch Ressourcenverlust, Arbeitszeitverbrauch, Organisationsaufwand, Werkzeugblockierung, stattfinden. Es handelt sich aber um eine von Experten zusätzlich durchzuführenden Maßnahme. iBIS Benutzer sollten nicht mit dieser Maßnahme in Kontakt treten.	Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Beeinträchtigen die Arbeit mit dem iBIS nicht im engeren Sinne.	Die Zielgruppe des iBIS wird von dieser Maßnahme vernachlässigbar beeinträchtigt.
Adwaretools	Beeinträchtigung durch Zeitverlust, Arbeitszeitverbrauch, Lernaufwand, Organisationsaufwand, Werkzeugblockade, Reaktanz. Es handelt sich aber um eine von Experten zusätzlich durchzuführenden Maßnahme. IBIS Benutzer sollten nicht mit dieser Maßnahme in Kontakt treten.	Starke Beeinträchtigung der Aufgabenangemessenheit. Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Beeinträchtigen die Arbeit mit dem iBIS nicht im engeren Sinne.	Die Zielgruppe des iBIS wird von dieser Maßnahme vernachlässigbar beeinträchtigt.
Firewall	Beeinträchtigung durch Zeitverlust, Arbeitszeitverbrauch, Lernaufwand, Organisationsaufwand, Werkzeugblockade, Transparenzverlust, Komplexitätssteigerung, Reaktanz.	Starke Beeinträchtigung der Aufgabenangemessenheit. Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Beeinträchtigen die Arbeit mit dem iBIS nicht im engeren Sinne.	Die Firewall überprüft jede Verbindung auf dem Rechner selbst und kann Aktionen blockieren, dadurch kommt es zu den genannten Beeinträchtigungen.

Sicherheits-maßnahme	Beeinträchtigung des iBIS	Benutzbarkeit	Kommentar
Intrusion-Detection-Systeme	Beeinträchtigung durch Zeitverlust und Reaktanz	Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Beeinträchtigen die Arbeit mit dem iBIS nicht im engeren Sinne.	
Protokollierungstools	Beeinträchtigung durch Zeitverlust, Organisationsaufwand und Reaktanz.	Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Beeinträchtigen die Arbeit mit dem iBIS nicht im engeren Sinne.	
Authentifizierung			Oberbegriff zur Sicherstellung der Identität eines Nutzers
Kennwortsicherheit	Beeinträchtigung durch Zeitverlust, Lernaufwand, Organisationsaufwand. Mögliche Beeinträchtigung durch Werkzeugblockierung, Komplexitätssteigerung und Reaktanz	**Starke Beeinträchtigung der Aufgabenangemessenheit**	
Biometrie	Beeinträchtigung durch Zeitverlust, Lernaufwand, Organisationsaufwand und Transparenzverlust. Mögliche Beeinträchtigung durch Werkzeugblockierung, Komplexitätssteigerung und Reaktanz	**Starke Beeinträchtigung der Aufgabenangemessenheit**	Diese Sicherheitsmaßnahme ist meist verknüpft mit der Kennwortsicherheit.

Sicherheits-maßnahme	Beeinträchtigung des iBIS	Benutzbarkeit	Kommentar
Physische Sicherungen (Schlösser)	Beeinträchtigung durch Zeitaufwand, Organisationsaufwand. Mögliche Beeinträchtigung durch Werkzeugblockierung	**Geringe Beeinträchtigung der Aufgabenangemessenheit**	
Kryptografie	Beeinträchtigung durch Zeitverlust, Arbeitszeitverbrauch, Lernaufwand, Organisationsaufwand, Transparenzverlust, Komplexitätssteigerung mögliche Beeinträchtigung durch Werkzeugblockierung und Reaktanz.	**Starke Beeinträchtigung der Aufgabenangemessenheit**	Diese Sicherheitsmaßnahme ist meist verknüpft mit der Kennwortsicherheit.
Tarnkappen/ Steganografie	Beeinträchtigung durch Zeitverlust, Arbeitszeitverbrauch, Lernaufwand, Organisationsaufwand, Transparenzverlust, Komplexitätssteigerung mögliche Beeinträchtigung durch Werkzeugblockierung und Reaktanz.	**Starke Beeinträchtigung der Aufgabenangemessenheit**	Diese Sicherheitsmaßnahme ist meist verknüpft mit der Kennwortsicherheit. Hier werden Informationen versteckt abgelegt und müssen zunächst transformiert werden.

Sicherheits-maßnahme	**Beeinträchtigung des iBIS**	**Benutzbarkeit**	**Kommentar**
Sniffer	Beeinträchtigung durch Organisationsaufwand und Reaktanz	Keine Beeinträchtigung von Führungskräften im engeren Sinne, da nur von Spezialisten bedient.	Die Zielgruppe des iBIS wird von dieser Maßnahme vernachlässigbar beeinträchtigt. Die Reaktanz ist möglich, da der Sniffer alle Verbindungen eines Rechners zur anschließenden Analyse protokolliert und Dritte somit Einblick bekommen.
Filter	Beeinträchtigung durch Zeitverlust, Organisationsaufwand, Werkzeugblockade, Transparenzverlust, Komplexitätssteigerung und Reaktanz	**Starke Beeinträchtigung der Aufgabenangemessenheit**, Wartung erfolgt durch Spezialisten	
Netzwerkarchitektur	Beeinträchtigung je nach Aufbau der Architektur eventuell minimaler Zeitverlust	Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Beeinträchtigen die Arbeit mit dem iBIS nicht im engeren Sinne.	Die Zielgruppe des iBIS wird von dieser Maßnahme vernachlässigbar beeinträchtigt.
Isolierung	Beeinträchtigung durch Organisationsaufwand.	Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Beeinträchtigen die Arbeit mit dem iBIS nicht im engeren Sinne.	Bedrohungen werden isoliert, diese sind jedoch meist mit produktiven Mitteln verknüpft welche dann ebenfalls isoliert werden.

Sicherheits-maßnahme	Beeinträchtigung des iBIS	Benutzbarkeit	Kommentar
Zertifikate	Beeinträchtigung durch Zeitverlust, Arbeitszeit-verbrauch, Lern-aufwand, Organi-sationsaufwand, Werkzeugblockie-rung, Transpa-renzverlust, Kom-plexitätssteige-rung, Reaktanz	**Beeinträchtigung der Aufgabenangemessen-heit**	Zertifikate benö-tigen zur Prüfung einen Zwischen-schritt vor der eigentlichen Auf-gabenerfüllung
Schulungen	Beeinträchtigung durch Zeitverlust, Arbeitsaufwand, Lernaufwand, Or-ganisationsauf-wand, Reaktanz	Aufgabenangemessen-heit, Selbstbeschrei-bungsfähigkeit, Steuer-barkeit, Erwartungskon-formität, Fehlertoleranz, Individualisierbarkeit, Lernförderlichkeit. Be-einträchtigen die Arbeit mit dem iBIS nicht im engeren Sinne.	Die Zielgruppe des iBIS wird von dieser Maßnahme vernachlässigbar beeinträchtigt.
Sicherheits-richtlinien	Beeinträchtigung durch Lernauf-wand, Organisati-onsaufwand, Werkzeugblockie-rung, Komplexi-tätssteigerung, Reaktanz	**Starke Beeinträchti-gung der Aufgabenan-gemessenheit**	
Trusted Com-puting	Beeinträchtigun-gen können noch nicht abgesehen werden, da das Konzept noch nicht vollständig verwirklicht ist. Es werden Beein-trächtigungen durch Zeitverlust, Werkzeugblockie-rung, mangelnde Updatefähigkeit und Reaktanz er-wartet.	Beeinträchtigungen hin-sichtlich der Aufgaben-angemessenheit werden erwartet.	

Sicherheits-maßnahme	**Beeinträchtigung des iBIS**	**Benutzbarkeit**	**Kommentar**
Test (Penetrationstests)	Eventuelle Beeinträchtigung durch Zeitverlust und Organisationsaufwand sowie Reaktanz.	Keine Beeinträchtigung von Führungskräften im engeren Sinne, da nur von Spezialisten bedient.	Die Zielgruppe des iBIS wird von dieser Maßnahme vernachlässigbar beeinträchtigt.
Listen (Black/White)	Geringe Beeinträchtigung durch Zeitverlust. Beeinträchtigung durch Lernaufwand, Organisationsaufwand, Werkzeugblockierung, Reaktanz.	**Starke Beeinträchtigung der Aufgabenangemessenheit**, Wartung erfolgt durch Spezialisten	Listen werden oft in Verbindung mit Firewalls und Scannern eingesetzt.
Schutzprofile	Beeinträchtigung durch Zeitverlust, Lernaufwand, Organisationsaufwand, Werkzeugblockierung, Komplexitätssteigerung, Reaktanz	Beeinträchtigungen sind je nach Art und Ausprägung des Schutzprofil stark bis gering zu erwarten.	
Priorisierung			
Open Source	Beeinträchtigung durch Lernaufwand. Der Organisationsaufwand unterscheidet sich nicht von anderer SW		
Ad hoc OS	Beeinträchtigung durch Lernaufwand, Organisationsaufwand, Transparenzverlust, Komplexitätssteigerung, Reaktanz	**Beeinträchtigungen sind je nach Art und Ausprägung des ad hoc OS stark bis gering zu erwarten.**	Die Einstellungen des OS müssen vorab definiert werden, da bei jedem Start in den Grundzustand zurückgekehrt wird.

Sicherheits-maßnahme	Beeinträchtigung des iBIS	Benutzbarkeit	Kommentar
Thin clients	Beeinträchtigung durch Zeitverlust, Arbeitszeitverlust, Organisationsaufwand, Werkzeugblockierung, Transparenzverlust, Reaktanz	**Starke Beeinträchtigung der Aufgabenangemessenheit**	
Pen-Tests[649]	Geringe Beeinträchtigung durch Zeitverlust, Organisationsaufwand, Reaktanz	Keine Beeinträchtigung von Führungskräften im engeren Sinne, da nur von Spezialisten bedient.	Die Zielgruppe des iBIS wird von dieser Maßnahme vernachlässigbar beeinträchtigt.
Zentrale E-Mail-Verschlüsselung	Beeinträchtigung durch Zeitverlust, Arbeitszeitverbrauch, Lernaufwand, Organisationsaufwand, Transparenzverlust, Komplexitätssteigerung. Eventuell Reaktanz	Keine Beeinträchtigung von Führungskräften im engeren Sinne, da nur von Spezialisten bedient.	Die zeitliche Verzögerung durch die zentrale Verschlüsselung ist für den Anwender nicht spürbar.
Sicherheitsfunktion (Administratoren, Benutzer)		Keine Beeinträchtigung von Führungskräften im engeren Sinne, da nur von Spezialisten bedient.	Die Zielgruppe des iBIS wird von dieser Maßnahme vernachlässigbar beeinträchtigt.
Identity Management	Beeinträchtigung durch Zeitverlust, Arbeitszeitverbrauch, Lernaufwand, Organisationsaufwand, Transparenzverlust, Komplexitätssteigerung mögliche Beeinträchtigung durch Werkzeugblockierung und Reaktanz.	**Geringe Beeinträchtigung der Aufgabenangemessenheit**	

[649] Vgl. Rey, Enno; Thumann, Michael; Baier, Dominick (2005), S. 1ff.

Sicherheits-maßnahme	Beeinträchtigung des iBIS	Benutzbarkeit	Kommentar
Verträge	Beeinträchtigung durch Zeitverlust, Arbeitsaufwand, Lernaufwand, Organisationsaufwand, Komplexitätssteigerung, Reaktanz	**Geringe Beeinträchtigung der Aufgabenangemessenheit**	
Versicherungen	Beeinträchtigung durch Zeitverlust, Arbeitsaufwand, Lernaufwand, Organisationsaufwand, Komplexitätssteigerung, Reaktanz		Der Abschluss von Versicherungen ist mit dem Einführen von Sicherheitsmaßnahmen auf Grund der Forderung der Versicherung oft gekoppelt.
Outsourcing	Beeinträchtigung durch Lernaufwand, Organisationsaufwand, Transparenzverlust, Komplexitätssteigerung, Reaktanz	**Eventuelle Beeinträchtigung der Aufgabenangemessenheit**	
Hardwareanpassung:	Keine Beeinträchtigung	**Eventuelle Beeinträchtigung der Aufgabenangemessenheit**	
BSI	Je nach Ausbaustufe der Maßnahmen des Bundesamtes		
Notfallpläne	Keine Beeinträchtigung		

Tabelle 10: Untersuchungsergebnisse: Beeinträchtigung der Usability des iBIS durch Sicherheitsmaßnahmen.

8. Sicherheitsprofil eines useable und sicheren integrativen Business-Intelligence-Systems

In den vorangegangenen Kapiteln wurden die Bedeutung und der Zweck von integrativen Business-Intelligence-Systemen ausführlich dargestellt. Die angestrebte Zielsetzung ist derzeit noch nicht vollständig erreicht, wird aber bereits in Pilotprojekten erprobt. Anbieter wie BO, MIS und Cognos arbeiten bereits mit Systemen welche diese mit dem Schlagwort Business Intelligence benennen und die der angestrebten Vision des im ersten Kapitel dargestellten integrativen BIS nahe kommen.

Die notwendigen Basistechnologien in Form von Datenbanken, Data-Mining, Online Analytical Processing (OLAP), neuronale Netze sowie Web-Technologien sind bereits vorhanden. Des Weiteren drängt der Gesetzgeber in Form der Neuregelung von Haftungsregelungen im Management sowie die Wirtschaft selbst durch nicht gesetzliche Vorgaben wie beispielsweise die Corporate Governance bzw., Security Governance Richtlinien auf die zukünftige Einführung von Risikomanagement-systemen.[650] Manager haben nicht nur aus diesem Grund ein Interesse ihre Entscheidungen durch integrative BIS zu untermauern. Dieses Interesse geht so weit die Verantwortung an diese Systeme zu übertragen, was gesetzlich derzeit noch nicht zulässig ist sowie ethische Probleme mit sich bringt.[651]

Um einen sicheren Umgang mit Daten und informationsverarbeitenden Systemen zu gewährleisten, ist es erforderlich, der jeweiligen Gefährdungslage entsprechende Sicherheitsstandards zu entwickeln und einzuhalten.[652] Derzeit findet ein Paradigmenwechsel in der IT-Sicherheit statt. Die Sichtweise sich innerhalb des durch Firewalls geschützten Firmennetzwerkes sicher zu fühlen und alles extern als feindselig einzustufen greift unter dem Aspekt der neuen Entwicklungen nicht mehr.[653] Auch die Entwicklungen des RoSI steckt noch in den Anfängen und die ökonomische Betrachtung der IT-Sicherheit kommt zu kurz.

---

[650] Vgl. Le Roux, Yves; in Pohlmann, Norbert; Reimer, Helmut; Schneider, Wolfgang (2007), S. 136f.
[651] Vgl. Schrey, Joachim in Gründer, Torsten (2007) S. 265ff.
[652] Vgl. [BSI; http://www.bsi.bund.de].
[653] Vgl. Medosch, Armin (2007), S. 18; Bedrohungen existieren nicht nur extern, viele Zugänge zum Rechner sind nicht an die Firewall angebunden.

Die zu treffenden Maßnahmen können auf die Konzepte Authentifizierung, Autorisierung, Verifizierung und Validierung zurückgeführt werden.[654] Die Sicherheitskriterien können in die primäre Ausprägungen Vertraulichkeit, Integrität, Verbindlichkeit und Authentizität und die sekundären Werte Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs-, und Abwehrfähigkeit eingeteilt werden.[655] Die Anforderungen an sicherheitskritische Systeme sind dabei Datensicherheit (Vertraulichkeit, Datenintegrität, Verbindlichkeit, Verfügbarkeit, Sicherstellung der Zustellung), Zugriffssicherheit (Autorisierung, Authentifikation, Anonymität) und Systemsicherheit (Monitoring, Traceability Auditing, mehrstufige Sicherheit)[656].

Die Gefahren von Informationssystemen greifen dieses Konzept an, welches wiederum durch die Sicherheitsmaßnahmen aufrechterhalten werden soll. Es geht also im Kern darum die Vertrauenswürdigkeit des Systems in Vollständigkeit, Richtigkeit auf der einen Seite und Zugangsbeschränktheit an den definierten Personenkreis andererseits durch geeignete Maßnahmen unter Beachtung der Usabilityaspekte zu gewährleisten.[657] Es muss sichergestellt werden, dass die richtige Person, die richtigen Informationen, zum richtigen Zeitpunkt zur Verfügung gestellt bekommt. Diese Informationen müssen integer also wahrhaftig und unverfälscht sein. Die Abhängigkeit von der Richtigkeit der Information korreliert mit der Informationsbedarfsanalyse.[658]

Als Ergebnis der Arbeit können folgende Richtlinien aufgestellt werden, welche eingehalten werden müssen: Durch das IM als für das Unternehmen wichtig festgelegte Bereiche sind auch unter Missachtung der Usability Kriterien zu schützen. Die durch das IM als unwichtig definierten Bereiche sind unter stärkerer Beachtung der Usability Kriterien zu schützen. In Bereichen mit denen die Führungskraft nicht in Kontakt kommt ist Sicherheit der Usability vorzuziehen. Im Zweifel ist Sicherheit vorzuziehen.

---

[654] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 22ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[655] Vgl. Müller, Rainer (2005), S. 445.
[656] Vgl. Englbrecht, Michael (2004), S. 6ff.
[657] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[658] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

Sicherheitsmaßnahmen stehen in Konkurrenz zu deren Umgehung. Dies bedeutet, dass alle Maßnahmen in bestimmten Abständen ob ihrer Gültigkeit und Zweckmäßigkeit überprüft werden müssen. Von einem einmal festgestellten Sicherheitsniveau kann in diesem Zusammenhang nicht ausgegangen werden. Die Sicherheit von Informationssystemen stellt sich vielmehr als ein sich fortentwickelnder Prozess dar. Diese Tatsache lässt sich mit der Weiterentwicklung von Software und der Theorie der Emergenz von komplexen Systemen begründen.

Ferner kann festgestellt werden, dass durch Sicherheitsmaßnahmen ein bestimmtes Sicherheitsniveau erreicht werden kann. Je höher das Sicherheitsniveau steigt, desto höher werden die Usability-Beeinträchtigungen der Aufgabenträger, welche mithilfe des Informationssystems Aufgaben lösen. Dies lässt sich bereits durch die große Anzahl unterschiedlicher Sicherheitsmaßnahmen erklären, wobei es sich nicht um einzelne Maßnahmen handeln sollte, sondern um ein Gesamtkonzept. Ist im Gesamtkonzept eine Lücke vorhanden, wirkt sich dies so aus, dass die Anforderungen der Sicherheit nicht mehr gegeben sind.[659]

Es stellt sich die Frage in wie weit solche Maßnahmen überhaupt getroffen werden sollen. Es kann ökonomisch sinnvoller sein, ein Restrisiko zu akzeptieren, da sich ein Nutzen nicht nur durch Vermeidung von Schaden sondern auch durch die Verringerung von Kosten einstellen kann. Da die Kosten der Sicherung von Systemen mit zunehmendem Sicherheitsniveau exponentiell ansteigen ist diese Überlegung sinnvoll.

8.1. Schwachstellenanalyse eines integrativen Business-Intelligence-Systems

Eine Schwachstellenanalyse untersucht einen Prozess hinsichtlich Verfahrensfehlern und Schwachstellen mit dem Ziel den Prozess zu optimieren. Im Folgenden wird die das durch den Autor angepasste Vorgehen für eine Schwachstellenanalyse vorgestellt. Die Schwachstellenanalyse basiert auf den vorangehenden Kapiteln.

Es muss die Unternehmensinfrastruktur erfasst werden. Insbesondere sind die Schnittstellen der einzelnen Systeme welche an die integrativen BIS im weitesten

---

[659] Vgl. Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf (1998), S. 106; vgl. Englbrecht, Michael (2004), S. 4.

Sinne gekoppelt sind zu erheben. Jede Schnittstelle stellt per se eine Schwachstelle dar, die im Sicherheitskonzept beachtet werden muss. Dabei sind keinesfalls nur technische Schnittstellen mit einzubeziehen. Besonders wichtig sind Mensch-Maschine-Schnittstellen. Viele Schwachstellen betreffen den Benutzer des integrativen BIS kaum direkt. Diese können also durch geeignete Maßnahmen unter Beachtung ökonomische Nebenbedingungen geschlossen werden.

8.2. Integrative Business-Intelligence-Systeme und Schnittstellen

Zunächst müssen die Zielsetzungen der einzusetzenden Systeme bestimmt werden. Diese wurden in den vorangegangenen Kapiteln in Form der Entscheidungsunterstützung ausführlich diskutiert. Aus den Zielsetzungen und deren Anforderungen an die Sicherheit lässt sich folgendes ableiten: Authentifizierung, Verifizierung, Validierung, Autorisierung[660], Vertrauenswürdigkeit und Zuverlässigkeit.

Des Weiteren sind die relevanten Schutzziele zu definieren.[661] Diese Grundkonzepte müssen erstens für die Führungskraft „Usabel“ und zweitens für die Unternehmung ökonomisch sinnvoll umgesetzt werden. Die Usabel-Anforderungen ergeben sich aus dem Kapitel Usability und die ökonomischen Anforderungen aus dem Kapitel ökonomische Betrachtung der Risiken und Maßnahmen.

Da die Konzepte übertragen auf die Gesamtheit der Unternehmung sehr komplex werden muss versucht werden diese auf ein intelligibles Maß zu reduzieren. Dazu kann die Architektur herkömmlicher BIS und anderer IT-Systeme als Ausgangspunkt benutzt werden. Eine Analyse des Aufbaus ergibt, dass die wesentlichen zu schützenden Bereiche über Schnittstellen miteinander verbunden sind. Die Sicherheit der Systeme kann dadurch auf die Grundkonzepte innerhalb der gekapselten Systeme und die Schnittstellensicherheit reduziert werden.

Die Vision eines integrativen BIS lässt sich derzeit als Informationssystem charakterisieren in dem viele für das Unternehmen relevante Informationen zusammengefasst und nach Notwendigkeit aggregiert werden, um die Entscheidungen der Führungskräfte zu unterstützen. Das integrative BIS ist dabei die zentrale Stel-

---

[660] Vgl. Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007), S. 22ff; vgl. Eckert, Claudia (2006), S. 4.
[661] Vgl. Eckert, Claudia (2006), S. 6.

le innerhalb einer Unternehmensinfrastruktur, welche Zugriff auf alle internen und externen Daten und Informationen benötigt.

Es sind verschiedene Ebenen zu schützen. Zum einen das Informationssystem selbst, es kann durch Authentifizierungs-, Validierungs- und Verifizierungsmechanismen vor dem Zugriff Unberechtigter und durch Prüfalgorithmen vor Datenmanipulationen geschützt werden. Hierbei sind die Usability-Aspekte, insbesondere in Bezug auf Führungskräfte als Anwender nicht zu vernachlässigen.[662]

Die zweite Ebene umfasst den Schutz der übrigen Unternehmensinfrastruktur. Diese Ebene ist beim Schutz des integrativen BIS ebenfalls von Bedeutung, da dieses sich im Idealfall aus den Systemen der Informationsinfrastruktur und Unternehmensinfrastruktur bedient, um die benötigte Entscheidungsunterstützung zu generieren und darzustellen. Die Führungskräfte selbst nehmen im bestenfalls nur die Benutzungsschnittstelle des integrativen BIS wahr. Die Ausgestaltung der Unternehmensinfrastruktur ist für Führungskräfte zweitrangig. Des Weiteren existiert zusätzlich eine dritte Schnittstellenebene. Durch sie kommt das System beziehungsweise die Unternehmensinfrastruktur mit der Umwelt in Kontakt, das heißt, es werden externe Informationen eingepflegt oder an die Umwelt abgegeben.

8.3. Sicherheitsvorgehensmodell

Das Vorgehen zur Herstellung der Sicherheit sollte einem Sicherheitsregelkreis unter Beachtung der Usability entsprechen.[663] Der Sicherheitsregelkreis kann wie folgt dargestellt werden. Ausgehend vom Startpunkt der ökonomischen Betrachtung folgen die Schritte: Prävention (Erkennen und schließen bekannter Sicherheitslücken); Reaktion (Anpassend des Gesamtsystems); Kontrolle und Fortschreibung des Konzepts; Rücksprung zum Startpunkt. Dies kann in folgender Abbildung dargestellt werden.

---

[662] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[663] Vgl. Müller, Rainer (2005), S. 369ff.

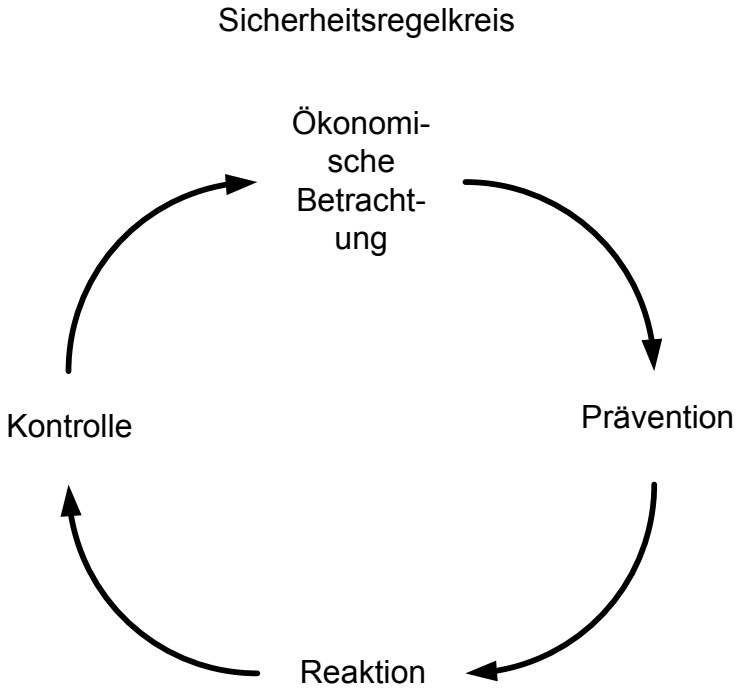

Abbildung 15: Sicherheitsregelkreis

Folgende Konzepte müssen verwirklicht werden: Einführen des Sicherheitsmodells[664] und dessen Überwachung durch den IT-Sicherheitsverantwortlichen[665] bspw. Sicherheitsmetriken wie Kennzahlensysteme oder die Messung der IT-Sicherheit selbst.[666].

8.3.1. Ökonomische Betrachtung

Aufgabe des Informationsmanagement ist es, festzulegen welche Art Information in den Informationssystemen der Unternehmung hinterlegt wird. Dadurch ist es dessen Aufgabe den Wert einer Information zu bestimmen.[667] Über den Wert der Information lässt sich der Schaden bestimmen, der beim Verlust einer Information oder deren nicht mehr exklusivem Wissen entsteht. Des Weiteren ist noch festzu-

---

[664] Vgl. Eckert, Claudia (2006), S. 241ff.

[665] Vgl. Godschalk, David (2007), S. 154.

[666] Vgl. [Freiling, Felix (2006); http://pi1.informatik.uni-mannheim.de]; vgl. Lotz, Volkmar (2007) S. 9.

[667] Informationen haben einen Wert, der sich teilweise aus der Handelbarkeit der Information bestimmen lässt. Der Wert selbst ergibt sich aus dem Nutzen der Information und den Kosten zur Produktion, Bereitstellung und Weiterleitung derselben. Die konkrete Bewertung des objektiven Wertes einer Information ist schwierig; Hilfestellung bieten Untersuchungen zum Informations-Paradoxon. Der subjektive Wert der Information wird dagegen vom Nutzer selbst festgelegt.

legen welcher Schaden entsteht, wenn falsche Informationen als Grundlage von Entscheidungen verwendet werden.

8.3.2. Prävention

Es empfiehlt sich ein schrittweises Vorgehen anhand eines Sicherheitsprozesses[668]. Dieser wird in der folgenden Abbildung dargestellt. Der Beginn des Sicherheitsprozesses ist es Ziele zu setzen.

Abbildung 16: Sicherheitsprozess

Es erfolgt eine Trennung in Maßnahmen, welche starke Usability Auswirkungen, mittlere und solche welche kaum Usability Auswirkungen auf Führungskräfte haben. Es kann folgendes Vorgehensmodell durch Einführen eines strategischen IT-Sicherheits- und Katastrophenmanagements abgeleitet werden[669]: Analyse des Sicherheitsbedarfs mit dem Ergebnis einer Beschreibung des Systems und dessen Anforderungen, in dem die Festlegung der Regeln für Authentifizierung, Verifizierung, Validierung und Backup stattfindet und vor allem die Zielvorstellung des integrativen BIS festgelegt wird.[670] In dieser Phase wird der Informationsfluss sowie das Sicherheitsniveau geregelt und die Schadenspotenziale, durch eine

---

[668] Vgl. Pohlmann, Norbert; Blumberg Hartmut (2004), S. 33; vgl. Leser, Ulf; Naumann, Felix (2007), S. 23f.
[669] Vgl. Biethan, Jörg; Muksch, Harry; Ruf, Walter (2004), S. 85f.
[670] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

Schadensanalyse ermittelt.[671] Aus diesem Ergebnis lassen sich zwingende und optionale Sicherheitsmaßnahmen ableiten. Ziel ist der Unternehmensinfrastrukturplan sowie der Sollzustand des Sicherheitsniveaus. Es können bspw. Checklisten entworfen werden, welche den Soll-Zustand dokumentieren.

Entwurf: Nach der Ermittlung des IST-Zustandes wird dieser mit dem SOLL-Zustand verglichen. Der IST-Zustand kann auf Basis der Analysephase bspw. Über die erstellten Checklisten ermittelt werden. Typische Fragestellung wäre: Ist eine Firewall vorhanden. Einleiten von Maßnahmen um den IST-Zustand in den SOLL-Zustand zu überführen. Dies ist nicht unproblematisch, da hier die Usability-Aspekte beachtet werden sollten. Umsetzen der Sicherheitsmaßnahmen unter Beachtung der Usability-Aspekte des Anwenders. Abstufung der Usability nach Sicherheitsniveau und Anwendergruppe. Maßnahmenauswahl: Zunächst werden die Risiken klassifiziert und danach wird dem Risiko mit der höchsten Klasse ein Maßnahmensatz zugeordnet.[672] Beispielsweise die Verwendung von nur verschlüsselter Übertragung und Speicherung durch Verwendung geeigneter Protokolle wie bspw. SSL, IPSEC, Link Layer, DNS, XML-Security[673] sowie Festplattenverschlüsselung bzw. Datenverschlüsselung.

Freigabe und Betrieb des Systems sowie der Schutzmaßnahmen und infolge dessen die Anwenderschulung.[674] Ständige Überwachung und Fortschreibung der Maßnahmen durch bspw. Penetrationstests. Festlegen von Überprüfungsmechanismen und Zyklen für Updates, Patches und Sicherheitsniveauprüfungen.

Die folgende Abbildung integriert die Sicherheitsmaßnahmen in ein Vorgehensmodell zur Softwareentwicklung. Als Ausgangsbasis wurde das Grundmodell der Softwareentwicklung gewählt. Es beinhaltet die Grundbausteine welche in weiterführenden Modellen wie bspw. dem Prototyping abgewandelt bzw. erweitert werden. Dieses Modell ist besonders geeignet, um weiterführende Bausteine zu integrieren, da es auf die grundlegenden Punkte der Softwareentwicklung konzentriert ist und dadurch Erweiterungen besonders gut sichtbar sind.

---

[671] Vgl. Eckert, Claudia (2006), S. 9.
[672] Vgl. Kersten, Heinrich (Hrsg.); Reuter, Jürgen; Schröder, Klaus-Werner (2008), S. 28.
[673] Vgl. Schwenk, Jörg (2005).
[674] Vgl. Godschalk, David (2007), S. 205; vgl. McIlwraith, Angus (2006), S. 94.

Das Grundmodell wurde um die Bereiche Sicherheits-/Usabilityanalyse, Informationssystemlandkarte/Schnittstellenkarte, Entwurf der Sicherheitsmaßnahmen, Dokumentation der Sicherheitsmaßnahmen sowie Sicherheitstests erweitert.

Die Kästen zeigen dabei die zu erfüllenden Aufgaben an und die Ellipsen die Ergebnisse. Die gestrichelten Kästen zeigen an, wo die Sicherheit explizit in das Modell bei bereits vorhandenen Aufgaben eingefügt wurde. Start des Vorgehens ist der Projektbeginn. Die Punkte Sicherheits-/Usabilityanalyse, Entwurf der Sicherheitsmaßnahmen als Modul, Dokumentation der Sicherheitsmaßnahmen, Sicherheitstests (Penetrationstest) und Organisatorische Sicherheitseinbindung wurden als Aufgaben hinzugefügt. Das Ergebnis Informationssystemlandkarte/ Schnittstellenlandkarte wurde ebenso aufgenommen. Ziel ist des die Aufgaben welche sich durch die Erfordernisse der Sicherheit ergeben herauszustellen.

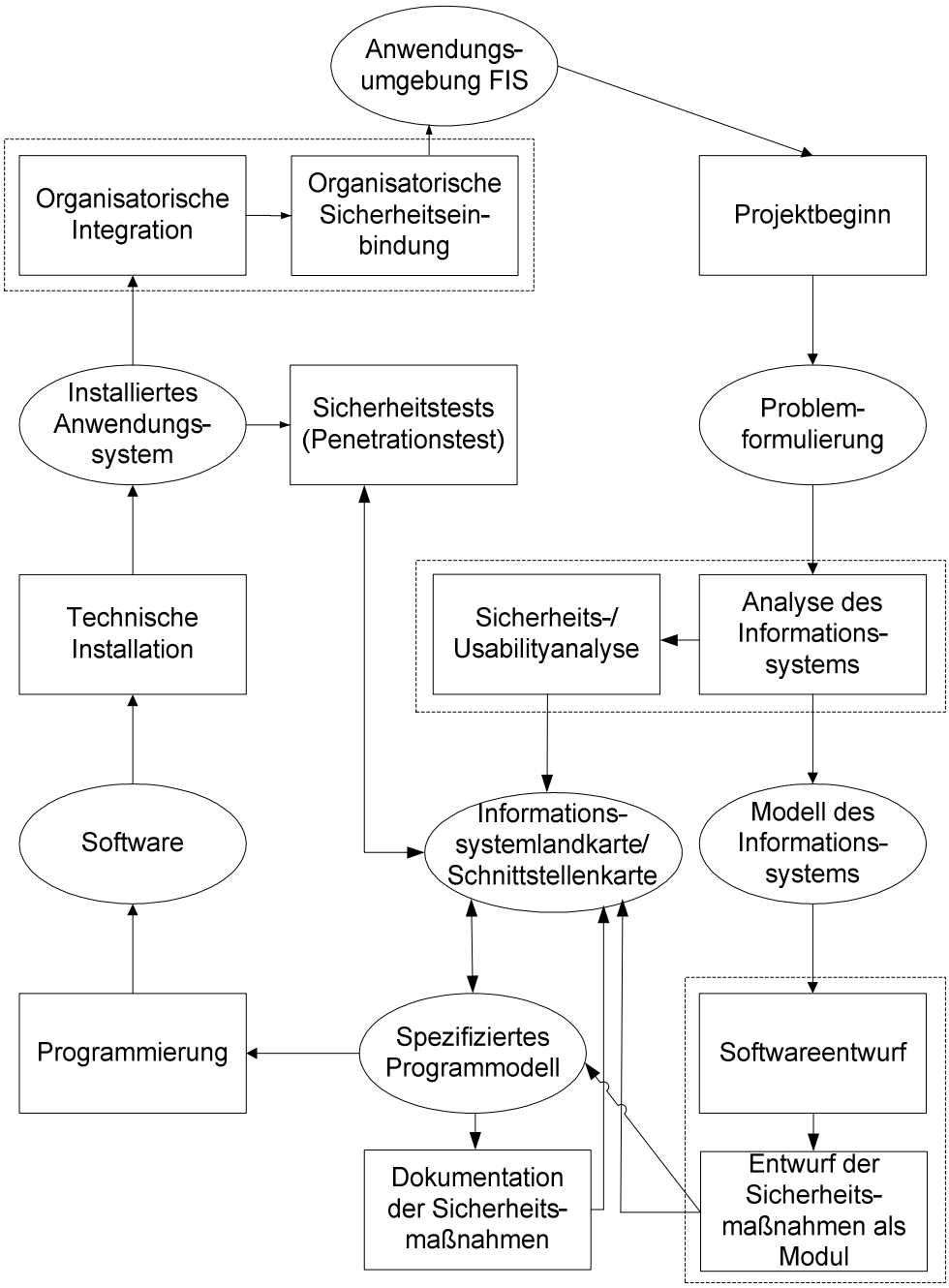

Abbildung 17: Vorgehensmodell Sicherheit

Diese Prozesse werden über einen Sollzustand definiert, wogegen der IST-Zustand geprüft werden kann. Folge ist meist das Aufstellen von sicheren Umgebungen durch Sandboxing und DMZ sowie die Trennung von externer und interner Umgebung. Inhalt dieser Konzepte ist ebenfalls eine rollenbasierte Zugriffskontrolle, die bei der Planung und Analyse festgelegt wird. Weiteres Ziel ist die physische Sicherheit des Gesamtsystems, das Prinzip des Information-Hidings

und der Kapselung[675], Security Audits, Penetrationstests[676] Anwenderschulung und die Transaktionssicherheit[677]. Die Folgende Tabelle zeigt mögliche Sicherheitsmechanismen.

Ziel	Maßnahme
Zugangsschutz	Manuelle und automatische materielle Sicherheitsmaßnahmen
Kommunikationsschutz	Verschlüsselung, physisch sichere Übertragungswege und Medien, Einwegfunktionen
Zugriffsschutz	Zugangsschutz durch Geheimnisschutz
Datenschutz	Zugangsberechtigungsverteilung, Pseudonymisierung
Datensicherheit	Schutz der Daten gegen System- und Programmfehler, Hardware-Ausfälle, Backup-Systeme

Tabelle 11: Sicherheitsmechanismen

8.3.3. Reaktion

Nachdem eine Kompromittierung stattgefunden hat, ist das Gesamtsystem nicht mehr vertrauenswürdig. Alle Daten und Programme könnten manipuliert sein und Informationen, die auf dem System gespeichert waren, können an Dritte weitergegeben worden sein. Folgende Maßnahmen müssen dann zwingend durchgeführt werden.

---

675 Vgl. Biethan, Jörg; Muksch, Harry; Ruf, Walter (2007), S. 329.
676 Vgl. Eckert, Claudia (2006), S. 177.
677 Vgl. Göbel, Siegbert (2005), S. 12f.

Abschalten	Abschalten, Netzwerktrennung
Bekanntmachung	Benutzerinformation, Daten sind als bekannt anzusehen
Systemimage	Ein Systemimage ist zur späteren Analyse zu erstellen
Ablauffeststellung	Rekonstruktion des Bedrohungsablaufs
Neuaufsetzen des Systems	Neuinstallation
	Benutzerkonten, Passwörter erneuern
	Anwendungen erneut installieren
	Daten prüfen, zurückspielen, wenn sie nicht kompromittiert sind
Schließen der Lücken	Einspielen von Patches, Veränderung der Sicherheitsmaßnahmen

Tabelle 12: Maßnahmen bei Kompromittierung.

Alarmierung des Sicherheitsverantwortlichen und des betroffenen Benutzerkreises bei Verletzungen der Sicherheit. Dies wird durch die Festschreibung der Sicherheitsstrategie verwirklicht[678] welche die Sicherheitsinfrastruktur betrifft[679] und einen Security Management Prozess implementiert in dem die Anforderungen, Plan, Do, Check und Act in einem Report festgelegt werden[680] bzw. die Maßnahmen "Protektion, Detection, Reaction" beschrieben werden.[681]

Die Einführung ist Top-Down bzw. Bottom-Up möglich.[682] Der BSI-Sicherheitsprozess ist ein guter Ausgangspunkt hierfür.[683] Einen ähnlichen Ausgangspunkt bietet der Aufbau eines zertifizierten Information Security Management Systems nach dem Secorvo White Paper, Case Study Aufbau und Zertifizierung eines ISMS nach BS7799-2:2002/ISO 27001, Version 1.3 Stand 24. September 2006. Es handelt sich auch um den BS799-Vorgang.[684]

---

[678] Vgl. Eckert, Claudia (2006), S. 27; 179.
[679] Vgl. Eckert, Claudia (2006), S. 30ff.
[680] Vgl. Brunnstein, Jochen (2006), S. 17.
[681] Vgl. Schneier, Bruce (2000), S. 279.
[682] Vgl. Biethan, Jörg; Muksch, Harry; Ruf, Walter (2007), S. 1. Die Ansätze Top-Down und Bottom Up unterscheiden sich grundlegend. Die Auswahl des Ansatzes der Einführung ist keine Besonderheit der Sicherheitsproblematik. Dennoch ist im Rahmen der BIS eine Einführung Top-Down in die engere Wahl zu ziehen, da es sich hauptsächlich um Systeme für Führungskräfte handelt.
[683] Vgl. Eckert, Claudia (2006), S. 153.
[684] Vgl. [Kühner, Klaus; Völkner, Jörg (2006); http://www.secorvo.de].

8.3.4. Kontrolle und Fortschreibung des Konzepts

Das Schadensmanagement durch Einführung von Computer Forensik, der Beweissicherung der Handlungen von Benutzern und Tätern[685] schließt den Regelkreis. Es ist eine ständige Überwachung und Fortschreibung der Maßnahmen notwendig.[686] Als Zielvorgabe muss die Wiederherstellung der Daten nach Störfällen in den korrekten Zustand möglich sein.[687]

8.3.5. Rücksprung zum Startpunkt

Der Regelkreis schliesst sich. Zusammenfassend ist zu sagen: Ziel des Vorschlags ist es ein Modell zu schaffen welches die Sicherheit von integrativen Business-Intelligence-Systemen und in diesem Zusammenhang die Unternehmensinfrastruktur verbessert ohne die Usability durch Sicherheitsmaßnahmen zu sehr einzuschränken. Beide Ziele sind konkurrierend und wirken in unterschiedliche Richtungen.

8.4. Architekturvorschlag integratives Business-Intelligence-System

8.4.1. Sicherheitshierarchie

An der Spitze der Informationssystempyramide nach Scheer stehen BIS.[688] Sie sind nach der Vision dieser Arbeit im Idealfall mit den restlichen Systemen dieser Pyramide verknüpft, die wiederum untereinander weitgehend integriert sind. Die Verknüpfung der einzelnen Systeme führt über den Austausch von Informationen zu einer Vereinheitlichung der Gesamthierarchie. Fehlerhafte Informationen würden sich von nachgeordneten Systemen bis an die Spitze der Pyramide durchziehen. Es gilt hier das Prinzip des schwächsten Gliedes. Des Weiteren besteht oft zwischen diesen Systemen eine Vertrauensstellung, welch die Weiterverbreitung von Bedrohungen begünstigt. Diese Systeme stehen an der Spitze der Gesamthie-

---

685 Vgl. Eckert, Claudia (2006), S. 25ff; Geschonneck, Alexander (2006) S. 65.
686 Vgl. Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005), S. 641.
687 Vgl. Pohlmann, Norbert (2004), S. 124; vgl. Stahlknecht, Peter; Hasenkamp, Ulrich, (1999) S. 208; vgl. Eckert, Claudia (2006), S. 5.
688 Vgl. Abbildung 2: Informationssystempyramide.

rarchie, da sie alle wichtigen Informationen, sammeln, generieren, aufbereiten und weitergeben.[689]

8.4.2. Sicherheitsprofil integratives Business-Intelligence-System

Bei einem integrativen BIS wird ein erhöhter Anspruch an das Sicherheitsniveau gestellt, da für das Unternehmen sicherheitskritische Informationen in diesem gebündelt werden. Diese Informationen werden aus unternehmensinternen Quellen also innerhalb der Unternehmensinfrastruktur aber auch aus externen Quellen von außerhalb der engeren Definition der Unternehmensinfrastruktur generiert oder gesammelt. Die Sicherheitsarchitektur muss gewährleisten, dass nur Berechtigte (Authentifizierung) Zugriff auf die enthaltenen Informationen bekommen und nur die Berechtigten diese verändern dürfen (Autorisierung).[690]

Die 10 Gebote des Datenschutzes sowie das Grundschutzhandbuch des BSI sind zu beachten. Dieses Sicherheitsprofil bewegt sich auf der Anwendungsebene des Programms selbst. Der Usabilityaspekt des Systems ist besonders zu beachten, da hier die untersuchte Schnittstelle zwischen Maschine und Führungskraft angesiedelt ist. Es ist also ein Berechtigungskonzept zu implementieren das nach der Analyse von Arbeitsaufgaben bestimmte Rollen einführt, welche definierte Operationen durchführen können. Zu bedenken ist, dass der Programmcode auf weiteren Systemen ausgeführt wird. Diese sind separat zu untersuchen.

Die implementierten Sicherheitskonzepte müssen modular und leicht austauschbar sein, da sie durch neue Erkenntnisse schnell obsolet werden können. Die Entwicklerfirma des Programms arbeitet selbst mit Menschen, diese könnten Hintertüren in das Programm einbauen, es ist also eine unabhängige Überprüfung oder zumindest Überwachung einzubauen.

Da die unabhängige Sichtung des Quellcodes meist nicht möglich ist, können beispielsweise die Anbieter der externen Sicherungsmaßnahmen für die Kommunikation mit dem integrativen BIS von außen „Sperren“ bzw. Authentifizierungsmaßnahmen über Netzzugriffsschutzmaßnahmen einarbeiten (bspw. ein Rollenkonzept unter Zuhilfenahme von Biometrie und starker Verschlüsselung als Zugriffs-

---

[689] Hoyer, Rudolfin; Krallmann, Hermann; Klotz, Michael; Wenzel, Hermann (Hrsg.) (1994), S. 159.

[690] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

und Authentifikationskonzept). Dies unterstreicht die Wichtigkeit eines Sicherheitsgesamtkonzeptes.[691]

8.4.3. Sicherheitsprofil für externe und interne Schnittstellen

Es sind zwei externe Schnittstellenarten zu unterscheiden. Die Schnittstellen des integrativen BIS zur restlichen Infrastruktur (Interne Unternehmensinfrastruktur) und die Schnittstellen der Unternehmensinfrastruktur zu Unternehmensumwelt.

Das Sicherheitsniveau beider externer Schnittstellen muss Mindeststandards entsprechen. Das Sicherheitsprofil interner Schnittstellen ist eine Frage des Standards der externen Schnittstellen und des Vertrauensmanagements innerhalb der Organisation. Authentifizierungsverfahren und Verschlüsselung, Verifizierung der Quelle und die Validierung der Daten sind notwendige Standardmaßnahmen.

8.4.4. Sicherheitsprofil auf Betriebssystemebene

Im Unternehmensalltag kommen verschiedene Betriebssysteme zum Einsatz. Vorherrschend als Betriebssysteme sind im Endanwender- sowie Unternehmensbereich Microsoft-Windows-Produkte sowie Linux und Unix Derivate. Die Server Betriebssysteme sind differenzierter. Dies bedeutet, dass die verschiedenen Vor- und Nachteile der Betriebssystemarchitektur in eine Betrachtung über IT-Sicherheit mit einbezogen werden müssen. Je heterogener eine Betriebssystemlandschaft in einem Unternehmen gestaltet ist, desto weniger anfällig ist sie für überspringende Sicherheitsattacken. Ein Schädling, der für ein bestimmtes Betriebssystem erstellt wurde, ist auf einem anderen System nicht ohne Weiteres ausführbar und kann somit weniger infektiös sein.

Dennoch sind die verschiedenen Betriebssysteme miteinander verknüpft, je nach Integrationsgrad können gemeinsame Ressourcen beispielsweise Speicherkapazitäten genutzt werden. Die populäreren Betriebssysteme haben unter Sicherheitsaspekten des Weiteren den Nachteil, dass ihre Schwachstellen aufgrund ihrer größeren Anzahl und damit der größeren Menge der möglichen Schadopfer, für potenzielle Angreifer interessanter erscheinen.[692]

---

[691] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[692]

8.4.5. Sicherheitsprofil auf Netzwerkebene

Die unterschiedlichen Systeme der Unternehmensinfrastruktur müssen miteinander kommunizieren, damit sie ihren definierten Zweck erfüllen können. Hier ist festzulegen welches System, mit wem kommunizieren darf. Es wird also ein Berechtigungskonzept benötigt, dass wiederum hier auf Systemebene Authentifizierung, Verifizierung und Validierung ermöglicht. Die Kommunikation ist zu verschlüsseln.

8.4.6. Sicherheitsprofil auf Infrastrukturebene

Wer darf, unter welchen Umständen, Zugang zum System erlangen ist die Fragestellung des Sicherheitsprofils auf Infrastrukturebene. Bisher konzentrierte sich die Fragestellung meist auf die Benutzerschnittstelle zwischen Mensch und Anwendungsprogramm. Hier weitet sich die Fragestellung zusätzlich auf alle Kontakte zwischen Mensch und Infrastruktur aus. Im Speziellen geht es um physische Kontakte und Zugänglichkeit. Dieses Sicherheitsprofil wird durch die Definition der Mensch-Maschine-Interaktion abgedeckt.

8.4.7. Integratives Sicherheitsprofil

Die verschiedenen Sicherheitsprofile sind in einem letzten Schritt zu integrieren. Ziele sind ein Schnittstellenplan, Infrastrukturplan sowie zur Umsetzung der Sicherheitsmaßnahmen ein modularer Aufbau, welcher die Austauschbarkeit der Maßnahmen erleichtert.

Analyse und Entwurf sollten unter Einbezug der aktuellen Sicherheitsrichtlinien des BSI-Grundschutzhandbuches sowie der Common Criteria erfolgen. Das Profil enthält zwei Komponenten, die Prävention und das Schadensmanagement. Das Gesamtsystem kann dabei als Schalenmodell in Form des IS-System selbst und der restlichen Informationsinfrastruktur angesehen werden.

Man benötigt eine Unternehmenslandkarte in der die Schnittstellen der Unternehmung gekennzeichnet sind. Sie könnte aus Unternehmensdatenmodell und Organigramm bestehen, die um die Komponente des Berechtigungskonzepts erweitert wird.

8.5. Architekturvorschlag integratives Business-Intelligence-System

Der Architekturvorschlag beruht auf den bisher gewonnenen Erkenntnissen dieser Arbeit. Zunächst wird das Modell des BIS um die Bestandteile Datensicherheit und Zugriffssicherheit modular erweitert. Dies ergibt folgende Abbildung.

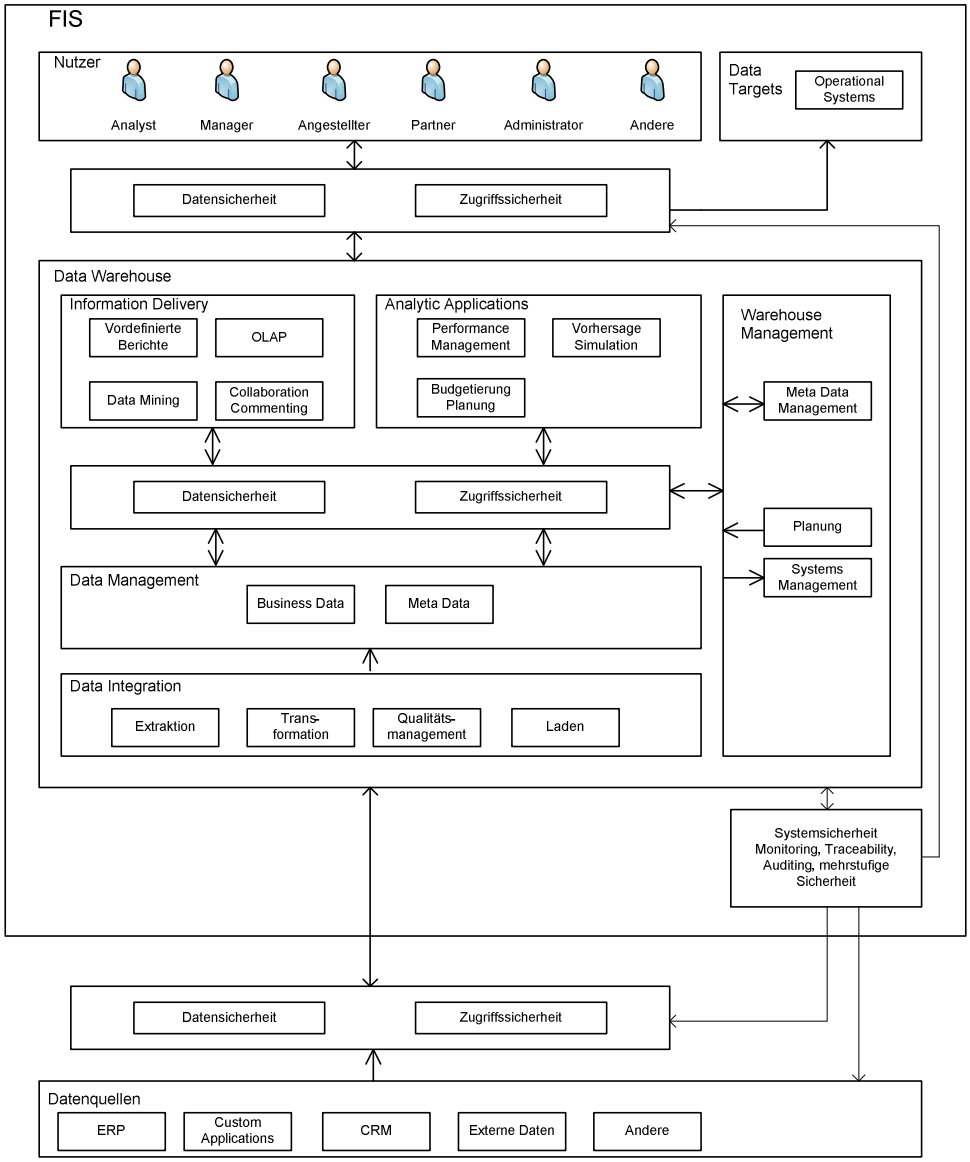

Abbildung 18: Sicherheitsarchitektur integratives BIS I (vereinfachte Abb.)

Insgesamt ist zu sehen, dass die Bestandteile an verschiedenen Übergängen des Systems eingeführt werden und die Schnittstellenproblematik beachtet wird. Die Abbildung ist insgesamt auf sehr abstraktem Niveau, sie wird im Folgenden konkretisiert. Im nächsten Schritt werden die behandelten und auf Usability getesteten Schutzmaßnamen eingebaut. Ein Hauptaspekt ist die Verschlüsselung der Infor-

mationsströme. Die Abbildung wird vorweggenommen, die Beschreibung folgt. Die folgende Abbildung ist des Weiteren im Anhang in größerer Form zu finden.

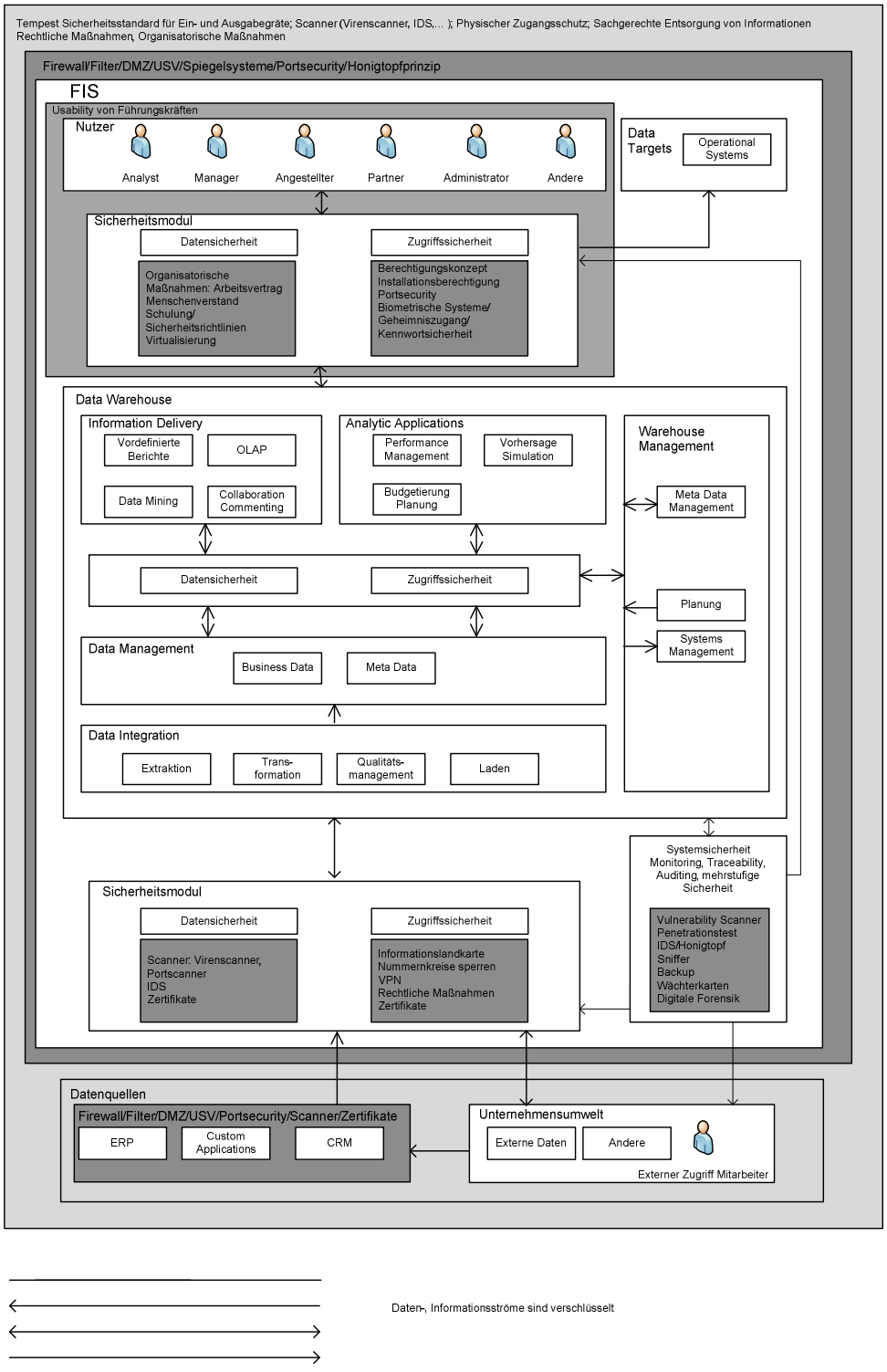

Abbildung 19: Sicherheitsarchitektur integratives BIS II[693]

[693] Eine vergrößerte Abbildung findet sich im Anhang.

Die Ziele lassen sich wie folgt konkretisieren: Das Modell muss die Authentifizierung und Integrität der im integrativen BIS enthaltenen Informationen gewährleisten. Es darf gleichzeitig nicht durch überzogene Sicherheitsmaßnahmen zu einer Einschränkung der Erfüllung der Aufgabe im Mensch-Aufgabe-Technik Kontext führen. Dies führt zu der Forderung den Benutzer zu kennen und ihn in die Gestaltung und Architektur von Systemen einzubinden.[694] Authentifizierung, Verifizierung, Datensicherheit, Datenschutz und Vertrauen sind damit die Grundpfeiler auf denen betriebswirtschaftliche Systeme und insbesondere integrative BIS aufgebaut sind. Diese sind durch geeignete Sicherheitsmaßnahmen im Kompromiss mit Usability Anforderungen und der benötigten Sicherheitsstufe herzustellen, hierzu kann das Kapitel Ökonomische Betrachtung verwendet werden. Basieren sollte das Modell auf einer leicht austauschbaren Sicherheitstechnologie, welche die betriebswirtschaftlichen Rahmenbedingungen beachtet.

Der zweite Pol besteht aus den Usability-Anforderungen von Führungskräften an die Systeme. Hier ist vor allem den in den vorigen Kapiteln aufgezeigten Punkten zu folgen. D.h. da Sicherheitsmaßnahmen nicht ursächlich/originär mit der Aufgabe zu tun haben, sollten Sie für den Anwender möglichst in den Hintergrund treten und nur dort sichtbar werden, wo es für die Förderung des Vertrauens in das System notwendig ist. Müssen solche Sicherheitsmaßnahmen sichtbar sein, ist auf Einfachheit und Akzeptanz der Benutzung durch den Anwender zu achten.

Vereinfacht können Informationssysteme als Geflecht von Kommunikationsströmen betrachtet werden. Es bestehen Dateninseln von denen aus Daten in Form von Bits und Bytes verarbeitet werden und nach der Verarbeitung über Ausgabegeräte angezeigt werden. Betrachtet werden muss die Mikroebene des einzelnen integrativen BIS aber auch die Makroebene der gesamten Unternehmung bis hin zu Umwelteinflüssen.

Die Kryptografie, die Verschlüsselung von Informationen ist ein wichtiger Baustein zum Schutz von Systemen. Eine ihrer Möglichkeiten ist es alle Kommunikation zu verifizieren und zu authentifizieren. Als Technologie kommt ein Public Key Verfahren in Betracht, da die kryptografischen Ansätze dieses Verfahrens gut von unabhängiger Stelle überprüft sind. Auf keinen Fall ist ein selbst entworfenes

---

[694] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2ff.

Verschlüsselungssystem einer IT-Firma zu verwenden, da IT-Fachleute oft keine guten Kryptografen darstellen. [695] Der Zuzug eines bekannten Kryptonanalytikers ist wünschenswert.[696] Nachteilig wirkt sich der Zeitaufwand aus, welcher durch den Einsatz von Kryptografietechnolgie entsteht sowie die nicht vorhersagbare Bestandsdauer der Technologie. Deshalb ist der leichte Austausch der Verschlüsselungstechnik zu ermöglichen. Zur Authentifizierung könnte ein biometrisches Verfahren in Kombination mit einem Geheimnis verwendet werden.

Die Sicherheitsmaßnahmen sind in ihrer Gesamtheit zu modularisieren sowie der Notfallplan zu erstellen: Die notwendige Dokumente, der Unternehmensinfrastrukturplan sowie der Notfallverantwortlichkeitsplan sind zu erstellen. Tritt ein Ereignis ein, ist der Fehler zu Beschreiben, eine Schulung der Beteiligten vorzunehmen[697]und Sofortmaßnahme zu ergreifen. Die Fragestellung lauten: Wer ist zu informieren, hier ist eine Kontaktliste bspw. in Form einer Telefonliste, Pagerliste, Adressliste oder E-Mailliste notwendig. Es sollte eine Informationslandkarte erstellt werden, auf der verzeichnet ist, welche Informationen an welcher Stelle vorliegen. Von diesen Informationen können Backups durchgeführt werden, diese müssen auf räumlich getrennten Systemen ausgelagert werden. Im Idealfall sollte eine Spiegelinfrastruktur verwendet werden. Spiegelinfrastrukturen sind im Unterhalt und der Anschaffung sehr teuer und nur bei sehr wichtigen Einrichtungen und Datenhaltungen anzutreffen. Dies wird sich eventuell mit dem weiteren Verfall der Hardwarekosten ändern. Folgende Maßnahmen sollten gegenüber konkreten Bedrohungen eingeführt werden, ihre Einwirkung auf die Usability kann den vorhergehenden Kapiteln entnommen werden.

Sicherheitsmaßnahmen Bloßstellende Abstrahlung

Als Abhilfe kann der in den USA seit den 60er Jahren geltende Tempest-Sicherheitsstandard[698] oder die Ratschläge des BSI eingeführt werden. Für alle Geräte, die im militärischen und polizeilichen Bereich benutzt werden, müssen diese Sicherheitsmaßnahmen standardmäßig eingehalten werden. Diese entspre-

---

[695] Vgl. Schwenk, Jörg (2005), S. 13ff; 22ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[696] Vgl. Schwenk, Jörg (2005), S. 13ff; 22ff; vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.
[697] Vgl. Godschalk, David (2007), S. 205.
[698] Vgl. [Eskimo; http://www.eskimo.com]; [BSI; http://www.bsi.de].

chen in der Regel dem Sicherheitsniveau von integrativen Business-Intelligence-Systemen womit der Standard auch für diese gelten muss. Eine Verschlechterung der Usability ist hier nicht zu erwarten.[699]

Sicherheitsmaßnahme Computerviren

Die Verwendung von Virenscannern bringt erhebliche Vorteile im Gegensatz zu ungeschützten Systemen. Es werden zumindest die bekannten Schädlinge eingedämmt sowie über eine Heuristik typische Schadroutinen erkannt.

Sicherheitsmaßnahme Computerwürmer

Die Verwendung einer Firewall kann die Ausbreitung eines Wurmes über Betriebssystemlücken vermeiden. Hierfür ist die richtige Konfiguration der Firewall nötig, da durch die Konfiguration Ausnahmen der Kontrolle zugelassen werden.

Sicherheitsmaßnahme Trojanische Pferde

Die Verwendung von Scannern bringt erhebliche Vorteile im Gegensatz zu ungeschützten Systemen.

Sicherheitsmaßnahmen Softwareausfall

Software kann nach Vorgehensmodellen entwickelt werden. Zahlreiche Ansätze sind in der Literatur vorhanden. Zum Beispiel ist eine Erweiterung des Vorgehensmodells Prototyping um Sicherheitskonstrukte bei der Analyse, Entwurf und Test möglich. Dabei ist ein modularer Aufbau der Sicherheitskomponente aber auch einzelne Bausteine der Sicherheit zu beachten.

Sicherheitsmaßnahmen strombetriebene Anlagen

Unterbrechungsfreie Stromversorgungen (USV) können Computersysteme vor Datenverlust und Zerstörung durch Spannungsüberschüsse oder Spannungsabfälle bedingt schützen. Bei Stromausfällen liefern die Geräte genügend Energie für das ordnungsgemäße speichern und beenden aller Programme. Übersteigt der Überschuss den Schutzwert der Anlage, hat diese Maßnahme keinen Erfolg. Für längere Stromausfälle sind für einen dauerhaften Betrieb Notstromaggregate notwendig. Eine erhöhte Anzahl von Speichervorgängen sowie automatische Speichervorgänge können ebenso vor größeren Datenverlusten bei Stromausfällen schüt-

---

[699] Vgl. [Nadir; http://www.nadir.org]; Crytonomium; [BSI; http://www.bsi.de].

zen, jedoch nicht gegen Spannungsschwankungen und Verluste durch Maschinenausfall. Wird ein Gewitter erwartet, kann die Netzversorgung nach ordnungsgemäßem Beenden der Maschinen getrennt werden. Bauliche Maßnahmen wie Blitzableiter etc. schützen vor Überspannungen.

Sicherheitsmaßnahmen Filesharing

Da Filesharingprogramme nicht zum üblichen Umfang einer Computerinstallation gehören, müssen diese durch den Anwender explizit installiert werden. Dem ist vorzubeugen, indem normalen Usern das Recht zur Installation von Programmen per Berechtigungsmanagement des Betriebssystems verweigert werden kann. Sollten User die Berechtigung zur Installation benötigen, müssen auf die Risiken extra hingewiesen und ein Verbot ausgesprochen und kontrolliert werden. Überwachungsprogramme bzw. Firewalls können als weiche Maßnahmen die benötigten Ports des Filesharings sperren. Diese Ports könnten aber ebenso von gewünschten Anwendungen benötigt werden. In diesem Fall greift diese Schutzmaßnahme nicht.

Sicherheitsmaßnahmen Netzwerkarchitektur

Ob ein Schutz vor Dialern notwendig ist, hängt von der Unternehmensinfrastruktur ab. Der Schutz wird über Softwareprodukte gewährleistet bzw. das Sperren von Nummerkreisen bei Telefonleitungen, an welche Modems angeschlossen werden. Die Überprüfung der Infrastruktur auf veraltete Zugangstechnik muss in regelmäßigen Abständen durchgeführt werden. Nichtphysischer Zugriff, außerhalb des Firmengeländes ist durch entsprechende Ausrichtung der Zugangspunkte zu unterbinden. So weit ökonomisch sinnvoll und möglich sind aktuelle Verschlüsselungsstandards zu verwenden. Der Netzwerkschlüssel sollte nach einer bestimmten Datenmenge geändert werden.[700]

Sicherheitsmaßnahmen Überwachungseinrichtungen

Schutz wird hier die Nutzung von biometrischen Systemen gewährleisten können, welche festen Körperkontakt benötigen.

---

[700] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 5.

Sicherheitsmaßnahmen Zugangsschutz durch ein Berechtigungskonzept

Folgenden Anforderungen werden an sichere Passwörter gestellt: Mindestzeichenlänge, Sonderzeichen, keine Verbindung zu persönlichen Informationen, Zufälligkeit und Wechsel des Passwortes in regelmäßigen Abständen. Eine Methode zur Auswahl eines guten Passwortes ist es einen Satz, beispielsweise „Ich hatte heute sehr viel Glück!“ durch Verwendung der Anfangsbuchstaben in „IhhsvG!“ zu verwandeln und zusätzlich Buchstaben in Zahlen zu transformieren. Bsp. I = 1. Dies erleichtert den Umgang mit Passwörtern.

Sicherheitsmaßnahmen Spam

Blacklist/Whitelist filtern den eingehenden Content nach Kriterien und löschen unerwünschte E-Mails. Blacklists löschen die E-Mails bestimmter vorher definierter Absender. Whitelists lassen nur die E-Mail vorher definierter Absender passieren. In der Diskussion befindet sich auch ein Porto von ca. einem Cent pro E-Mail.

Sicherheitsmaßnahmen Rechtliche Gefahren

Die Ausgestaltung des Arbeitsvertrages kann ein Schutzmittel darstellen. Ebenso die Berechtigungsvergabe und die Schulung der Mitarbeiter. Des Weiteren können Verträge mit anderen Beteiligten geschlossen werden.

Sicherheitsmaßnahmen Social Engineering

Ein Schreddern der Papiere oder sachgerechtes Entsorgen des Elektroschrotts wäre hier eine effektive Maßnahme. Ziele eines Social Enginner-Maßname sind hauptsächlich Softwarehäuser, Banken, militärische Einrichtungen, Universitätsnetze, Telekommunikations-, Internetprovider sowie sonstige Unternehmen. Schulungen ergänzen diese Maßnahme.

Sicherheitsmaßnahmen Phishing

Banken versenden wichtige Informationen grundsätzlich nicht per E-Mail, sondern mit der Post. Diese Regel ist in Zukunft wohl eher unglaubwürdig, sieht man sich die neusten Entwicklungen des Online-Banking an. Die ing Diba (Deutsche Direktbank) bietet wenn auch nur innerhalb ihres Online-Banking ein elektronisches Postfach mit Briefverkehr an. URLs und E-Mail-Absenderadressen können gefälscht werden und sind nicht vertrauenswürdig. Auskunft erteilt die Statuszeile des Browsers und im Extremfall nur der Quelltext der Internetseite. Diese Regel

setzt die Verwendung einer Skriptsprache (php, jscript) außer Kraft. Im Zweifelsfall müssen Aufforderungen seitens der Bank immer persönlich abgeklärt werden. Bankgeschäften sollte nur unter persönlicher Eingabe der Original-URL getätigt werden. Diese Prinzipien sind auf ein integratives BIS zu übertragen.

Sicherheitsmaßnahmen Hopping

Eine spezialisierte Rechtsabteilung und das hinwirken auf internationale Abkommen sowie Lobbyarbeit für Gesetzesinitiativen können Einwirkungen auf den Angriff des Hoppings vornehmen. Die reale Chance ist jedoch durch unterschiedliche Interessen gering. Intrusion-Detection-Systeme ermöglichen es Angriffe aufzuzeichnen und Honey-Pots führen den Angreifer auf eine falsche Fährte.

Sicherheitsmaßnahmen Man-In-The-Middle

Die Verschlüsselung des Datenverkehrs sowie die Authentifizierung des Gegenübers durch Zertifikate lässt viele dieser Angriffe mit verschlüsselten Datenströmen zurück. Dies müssen dann zunächst entschlüsselt werden. Die Entschlüsselung hängt dann wiederum von der Qualität der Verschlüsselung ab.

Auswahl einer Sicherheitsmaßnahme

Entscheidung für oder gegen eine Sicherheitsmaßnahme: Es gilt die Sicherheitsmaßnahme einführen, wenn der Erwartungswert des Schadens bei Nichteinführung > Erwartungswert des Schadens bei Einführung der Maßnahme + Usabilityverluste.

Weitere Maßnahmen

Die Trennung von Sicherheitsmaßnahmen in aktive Sicherheitsmaßnahmen mit denen der Benutzer in Berührung kommt und passive Sicherheitsmaßnahmen mit denen der Nutzer nicht in Berührung kommt sowie Mischformen, die im Allgemeinen von Spezialisten verwaltet werden, helfen dabei die Usability Beeinträchtigung von Sicherheitsmaßnahmen zu bewerten.[701]

---

[701] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

9. Fazit

In dieser Arbeit werden die Gefahren/Sicherheitsrisiken beim Betrieb von integrativen Business-Intelligence-Systemen aufgezeigt, die Gegenmaßnahmen erarbeitet um damit die Sicherheit der Systeme, unter den Rahmenbedingungen der Usability, zu erhöhen. Die Untersuchung ergab, dass eine Vielzahl sich ständig im Fluss befindlicher Bedrohungen den Betrieb von IT-Systemen im Allgemeinen und integrativen Business-Intelligence-Systemen im Speziellen beeinträchtigen. Als Fazit dieser Ausarbeitung steht fest, dass nur eine systematische gesamtheitliche Herangehensweise an diese Herausforderungen Erfolg versprechend sein kann. Der erste Teil der Arbeit schloss mit einem Katalog an Sicherheitsmaßnahmen, welche die Systeme sicherer machen können. Die Sicherheitsmaßnahmen ergeben sich aus den aktuellen Bedrohungen, den rechtlichen Anforderungen, der am Markt verfügbaren Sicherheitstechnologie sowie organisatorischen Anforderungen. Als Ergebnis kann festgestellt werden, dass sich Sicherheit auf Sicherheitsziele reduzieren lässt, welche sich im Architekturvorschlag und der Schnittstellenbetrachtung der integrativen BIS niederschlagen.

Ein Hauptproblem ist der zuverlässige Schutz vor Unbefugten. Dieser wird derzeit durch Verschlüsselungstechnologie innerhalb von Berechtigungskonzepten gewährleistet. Diese Verschlüsselungstechniken beruhen auf mathematischen Verfahren für die es noch keine einfachen Lösungsalgorithmen gibt. Sollte jemand in der Lage sein eine einfache Lösungs-Methode zu entwickeln, werden die bisher verwendeten Verfahren wertlos. Die verwendete Schutztechnologie muss deshalb modular eingebaut werden, sodass auf Veränderungen schnell reagiert werden kann. Die Modularität sowie verschlüsselte Kommunikation auch von Systemen untereinander ist für alle Sicherheitsmaßnahmen zu empfehlen.[702] Fortschritte im Bereich der Verschlüsselung werden durch die Quantenkryptografie und das Quantencomputing erwartet. Eine erste Geldüberweisung per Quantenkryptografie wurde bereits 2004 durchgeführt.[703] Der Vorteil hierbei ist, dass ein Angriff auf die verschlüsselten Daten durch Ausnutzung der Veränderung der Quanten

---

[702] Vgl. Homeister, Matthias (2005), S. 181f.
[703] Vgl. Homeister, Matthias (2005), S. 167ff.

durch Beobachtung ermittelt werden kann. Nachteilig wirkt sich die derzeit zu kurze Reichweite der Übertragungsmöglichkeit von Quantenschlüsseln aus.[704]

Der Maßnahmenkatalog wurde im Folgenden hinsichtlich der Auswirkungen auf die Nutzer von Business-Intelligence-Systemen, den Führungskräften untersucht. Als erstaunliches Ergebnis stellte sich heraus, dass viele Sicherheitsmaßnahmen sich zwar auf die Usability der Systeme in der Gesamtheit auswirken, aber kaum die Zielgruppe der Führungskräfte tangieren. Die angestrebten Sicherheitsmaßnahmen können an Fachkräfte übertragen werden, sodass diese Maßnahmen gegenüber Aufgabenträgern in den Hintergrund treten. Zeit und Ressourcenverlust halten sich in Bezug auf die Vertraulichkeit der Informationen nach Meinung des Autors in einem vertretbaren Rahmen. Die Usability des Gesamtsystems hingegen verschlechtert sich durch die Einführung von Sicherheitsmaßnahmen. Diese Betrachtung ist jedoch sehr eindimensional, da Sicherheit als Aufgabe im Unternehmensprozess definiert sein sollte.

Dennoch bleiben Usability-Beeinträchtigungen in der Mensch-Computer-Interaktion, im direkten Kontakt zwischen Führungskraft und integrativem BIS, insbesondere in Form der Authentifizierung und Arbeitsverlangsamung bestehen. Das Problem der Interaktion von Sicherheitsmaßnahmen untereinander und die damit sich vergrößernde Intransparenz konnte durch die Einteilung der Sicherheitsmaßnahmen in Klassen verringert werden.

Im Rahmen der ökonomischen Betrachtung der Sicherheitsmaßnahmen unter Berücksichtigung der Usability ergab sich folgendes Bild: Die Wahlalternative zwischen dem Einsatz und der Unterlassung von Sicherheitsmaßnahmen wird in Deutschland hauptsächlich durch gesetzliche Vorschriften und Richtlinien bestimmt. Der Spielraum Sicherheitsmaßnahmen einzuführen oder dies zu unterlassen wird dadurch seitens des Gesetzgebers reduziert. Der Entscheidungsraum verringert sich häufig auf die Art und Weise wie Sicherheitsmaßnahmen eingeführt werden sollen und ob das Risiko akzeptiert werden soll, gesetzliche Vorgaben bzw. Richtlinien der Wirtschaft zu missachten. Dennoch ist es sinnvoll und notwendig Wirtschaftlichkeitsanalysen durchzuführen. Für den verbleibenden Spielraum wurden deshalb Vorschläge zur Wirtschaftlichkeitsanalyse unterbreitet. Hier

---

[704] Vgl. Hiskett, P. A.; Rosenberg, D.; Peterson, C. G.; Hughes, R. J.; Nam, S; Lita, A. E.; Miller, A. J.; Nordholt J. E. (2006; S. 193.

zeigte sich die Komplexität des Themas. Vereinfachungen in Form von Annahmen bzw. Iterationsverfahren mussten in Betracht gezogen werden.

Die Sicherheit von integrativen Business-Intelligence-Systemen kann somit nur sekundär auf ökonomische Betrachtungen gestützt werden. Die Auswahl reduziert sich damit auf die Wahl des Produktes aus einer Produktklasse. Es werden dann nicht alle Sicherheitsmaßnahmen miteinander verglichen sondern die Sicherheitsmaßnahmen welche einen bestimmten Zweck erfüllen werden gegeneinander abgeglichen. Dies bestätigt auch die Antwort der Unternehmen auf die Frage, warum IT-Sicherheit wichtig ist. Es werden Haftungsprobleme genannt, wenn nicht der aktuelle Stand der Technik eingehalten wird. Diese Haftungsrisiken sind für die einzelne natürliche Person nicht akzeptabel. Im Rahmen der Gesamtabwägung kann unter Außerachtlassung ethischer Überlegungen das Risiko der Nichteinführung von IT-Systemen abgewogen werden. Des Weiteren sind die möglichen Verluste durch IT-Risiken inzwischen in unternehmensbedrohende Dimensionen gewachsen.

Usability-Verbesserungen können durch den Einsatz neuerer Zugangskontrolltechniken zum Beispiel im Bereich der Biometrie, des Pervasive Computings, RFID-Chips, welche allerdings eventuell Reaktanzprobleme hervorrufen, erreicht werden.[705] Die Zugangskontrollsysteme können bei geeigneter Implementierung teilweise in den Hintergrund treten. Biometrische Systeme schreiten in ihrer Entwicklung derzeit schnell voran und können durch ihre Verknüpfung mit Körpermerkmalen, welche nicht vergessen oder verloren werden können, Fortschritte hinsichtlich der Usability erzielen.

Digitale Wasserzeichen[706] können weiterhin Fortschritte in der Identifikationsmöglichkeit von Dateien, Systemen, Benutzern und Eigentumsnachweisen erbringen. Zu den neueren Entwicklungen im Bereich der Benutzerschnittstellen gehören die haptischen Benutzerschnittstellen, welche auf Bewegungen des Benutzers reagieren, zum Beispiel mit Hilfe von Kamerabeobachtung und somit einen intuitiveren Umgang mit Informationssystemen erwarten lassen.[707]

---

[705] Bundesamt für Sicherheit in der Informationstechnik (2004), S. 66.
[706] Vgl. Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf (1998), S. 195ff.
[707] Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006), S. 2.

Die Strafbarkeit beim Umgang mit IT-Sicherheitstools nach dem 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität, wird bei zukünftigen Untersuchungen zur IT-Sicherheit eine wesentliche Rolle spielen.[708] Ebenso ist die Absicht des Staates Online-Durchsuchungen (Bundestrojaner) durchzuführen ein Forschungsfeld, welches zukünftige Untersuchungen zur IT-Sicherheit beachten sollten. Die Usability von integrativen Business-Intelligence-Systemen ist neben der Sicherheit ein Thema, das zukünftige Forschungsarbeiten beeinflussen wird.

Integrative BIS verfügen über Daten und Verarbeitungsmethoden welche die Systeme aus Unternehmenssicht zu den schützenswertesten Systemen im Unternehmen machen. In ihnen befinden sich strategische Unternehmenspläne bis hin zu Informationen über Produktionsprozesse. Sie stehen somit annähernd auf derselben Stufe wie militärische Hochsicherheitssysteme. Die Sicherheit von Business-Intelligence-Systemen ist nicht nur durch die Sicherheit des Systems selbst zu gewährleisten. Die Integration des Systems zwingt den Betreiber die verbundene Infrastruktur mit zu betrachten. Dies wurde im Architekturvorschlag berücksichtigt.

Das komplexe Problem der Sicherheit von integrativen Business-Intelligence-Systemen kann dadurch vereinfacht werden, dass der Fokus der Betrachtung auf Vertraulichkeit, Integrität, Verbindlichkeit und Zugriffskontrolle. [709] Dies führt zu einer Betrachtung der Schnittstellenproblematik. Eine Empfehlung ist es die Verschlüsselungstechnik durchgängig zu verwenden sowie im Zweifel der Sicherheit gegenüber der Usability den Vorrang einzuräumen.

Der Schritt Analyse bei der Systementwicklung und die damit verbundene Aufnahme der Bedrohungs- und Schadzenarien bis hin zur Ermittlung des Wertes der im System enthaltenen Informationen gewinnt im Rahmen von Sicherheitsbetrachtungen noch mehr an Bedeutung und ist Aufgabe des IM.

Die Einführung einer Informationslandkarte zur Überwachung und Fortschreibung der IT-Sicherheitsmaßnahmen (Sicherheitsregelkreis) sowie die Einführung der Rolle des IT-Sicherheitsverantwortlichen, welcher die Einhaltung der gesetzlichen Vorschriften überwacht, ist notwendig. IT-Sicherheit ist Aufgabe der Unter-

---

[708] [Jlussi, Dennis (2007); http://www.jlussi.eu].
[709] Vgl. Dridi, Fredj (2003), S. 66.

nehmensorgane. Sollte die Einführung und Überwachung dieser Maßnahmen nicht nach Maßgabe der Regeln für ordentliche Kaufleute geschehen, kann eine persönliche Haftung entstehen.

Normalerweise finden sich geeignete Quellen zur Erarbeitung wissenschaftlicher Arbeiten in der wissenschaftlichen Literatur. Der Bereich Sicherheit in der Informationstechnik verändert sich jedoch in sehr kurzer Zeit. Eine Auswertung der einschlägigen Sicherheitsorganisationen und Anbieter war deshalb ebenso notwendig.

Derzeit werden Viren und Würmer, deren Bedeutung für die Sicherheit in dieser Arbeit bereits dargelegt wurde, durch menschliche Einwirkung verändert, allenfalls können sie selbst geringe Veränderungen vornehmen. Es wird nur eine Frage der Zeit sein, bis quasi-intelligente Programme existieren, welche sich dynamisch an die gegebenen Rahmenbedingungen anpassen. Es ist deshalb nötig, die einschlägigen Sicherheitsportale (wie bspw. www.Heise.de/security) zu überwachen, um auf neue Entwicklungen reagieren zu können. Dies wird in Zukunft wichtiger, da bedeutende Fortschritte in Rechengeschwindigkeit (Quantencomputer) und Programmentwicklung (Neuronale intelligente Netze) zu erwarten sind.[710]

Eine wichtige Entwicklung könnten abschliessend die Intrusion Detection Systems spielen, welche einen Angriff automatisch erkennen und geeignete Gegenmaßnahmen ergreifen sollen. Es ist deshalb zu überdenken, ob aktive Abwehrmaßnahmen nicht legalisiert werden sollten. Denkbar wäre das präventive entfernen von Schädlingen auch auf Computer von Dritten. Möglich wäre dies durch Sicherheitsprogramme die sich an der Verhaltensweise von Viren orientieren, jedoch mit dem Unterschied das der Payload eine Nutzroutine zur Erkennung und Beseitigung von Schadroutinen enthält.

---

[710] Vgl. Homeister, Matthias (2005).

10. Anhang

10.1. CC-Schutzprofil Erläuterung

Einführung: Die Einführung soll das Schutzprofil eindeutig identifizieren und einen allgemeinen Überblick über das Schutzprofil geben, sodass der Leser entscheiden kann, ob dieses Schutzprofil für ihn von Interesse ist.

Beschreibung: Dieser Teil soll den EVG bzw. die Produktgruppe beschreiben, auf die sich das Schutzprofil bezieht. Es sollen die Einsatzmöglichkeiten, die allgemeinen IT-Sicherheitseigenschaften aber auch Grenzen der Benutzung aufgezeigt werden.

Sicherheitsumgebung: In diesem Teil des Schutzprofils sollen die Sicherheitsaspekte der beabsichtigten Einsatzumgebung und die erwartete Art der Nutzung des EVG beschrieben werden. Hierbei wird eine Risikoanalyse durchgeführt, wobei die Bedrohungen zu den zu schützenden Werten in Bezug gebracht werden sollen.[711] Sowohl die möglichen Angriffsmethoden und die Schutzmethoden als auch die Bedrohungen, denen nicht durch den EVG entgegengewirkt wird, sollen genannt werden. Ziel ist, den Anwender darin zu unterstützen, den Bedrohungen durch andere (nicht IT-) Maßnahmen entgegenzuwirken. Die Sicherheitspolitiken beschreiben Annahmen über den sicheren Betrieb des EVG, die sicherstellen, dass die Sicherheitsziele effektiv befriedigt werden (materieller Schutz des EVG, verbindende Aspekte z. B. in Netzen, administrative Aspekte). Falls die Sicherheitsziele nur von den Bedrohungen abgeleitet werden, kann auf die Verwendung einer speziellen Sicherheitspolitik verzichtet werden.

Sicherheitsziele: Hier sollen die Sicherheitsziele des EVG in seiner Einsatzumgebung definiert werden. Die Sicherheitsziele müssen detaillierte Angaben darüber machen, wie den Bedrohungen entgegengewirkt werden soll bzw. die Sicherheitspolitiken erfüllt werden sollen. Es wird dabei zwischen IT-Sicherheitszielen und Nicht-IT-Sicherheitszielen unterschieden, wobei die Letzteren durch Anforderungen an die Einsatzumgebung erreicht werden sollen. Dabei soll jeder relevanten Bedrohung bzw. jeder Sicherheitspolitik durch mindestens ein Sicherheitsziel entgegengewirkt werden.

---

[711] Vgl. Eckert, Claudia (2006), S. 171; vgl. Dridi, Fredj (2003), S. 54.

IT-Sicherheitsanforderungen: Hier werden die Anforderungen an die Funktionalität und an die Vertrauenswürdigkeit definiert, denen der EVG genügen muss, damit die Sicherheitsziele erfüllt werden. Dabei ist zunächst auf die Anforderungen der Teile 2 und 3 der CC zurückzugreifen. Lassen sich jedoch keine passenden Anforderungen in den CC finden, so hat der Verfasser die Möglichkeit, seine Anforderungen frei zu formulieren.

PP-Anwendungsbemerkungen: Dieser optionale Abschnitt enthält zusätzliche Anwenderinformationen, die für die Erstellung, die Evaluierung oder den Gebrauch des EVG nützlich sein können.

10.2. Sicherheitsarchitektur BIS III (groß)

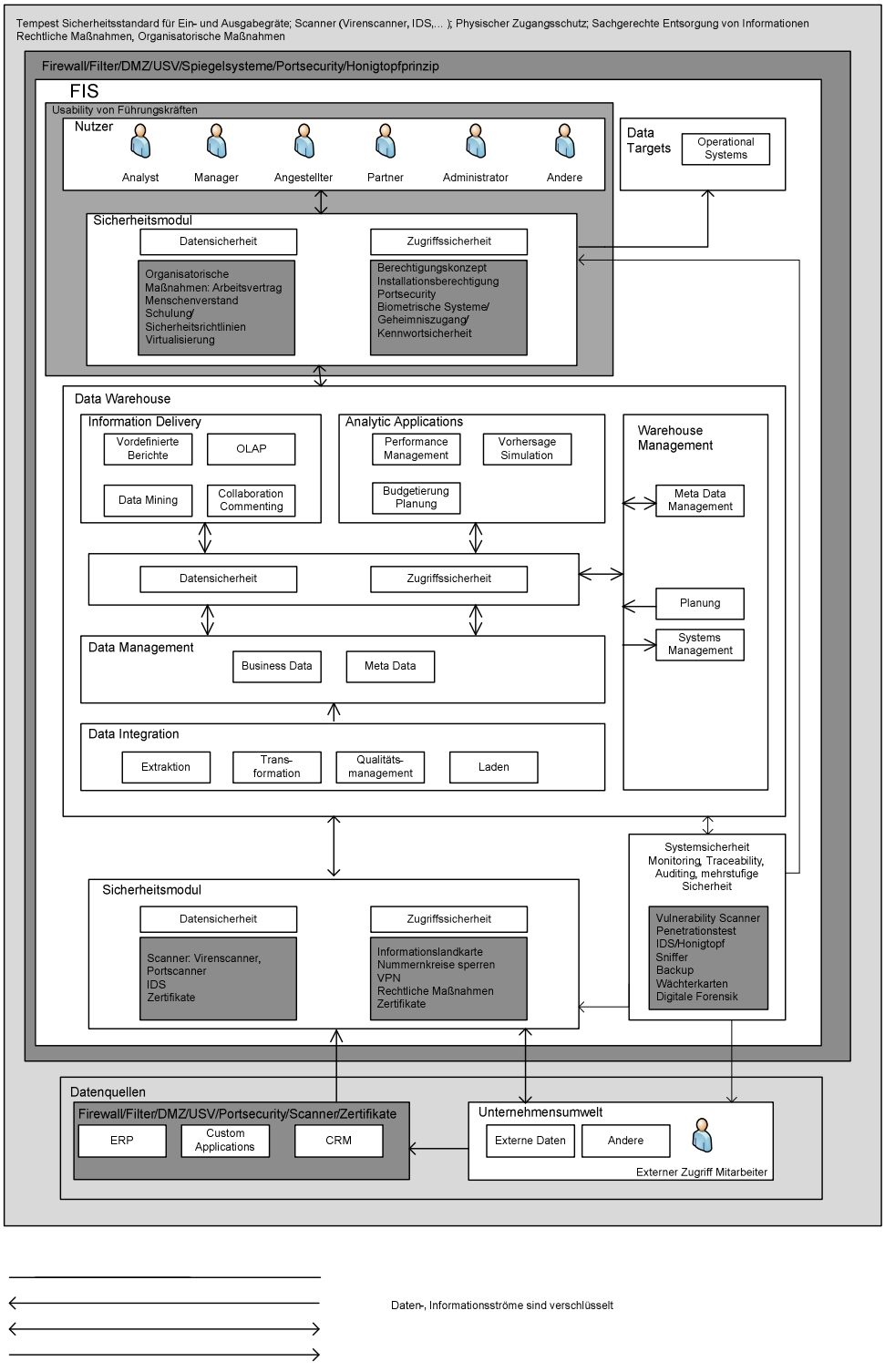

Abbildung 20: Sicherheitsarchitektur BIS III (groß)

10.3. Alternative Klassifizierung

Es folgt eine alternative Klassifizierung in der Gefahren in Bezug auf Objekte klassifiziert werden.

Objekte	Gefahren
Software	Fehlerhafte Erstellung
	unberechtigte Nutzung
	unnötige Zugriffsrechte
	Probleme der Versionsverwaltung
	IT-Sicherheitslücken
Input-/Outputdaten	Fehlerhafte Eingaben
	fehlerhafte Funktionen
	Missbrauch von Systemen
	Manipulation von Ergebnissen
	Falschinterpretation von Ergebnissen
	Computerviren
Hardware	Technisches Versagen
	Überlastung
	Stromausfall
	Auswertung der Abstrahlung
	Diebstahl
Rechnernetze	unberechtigter Zugang
	Ausfall der Versorgung
	Technische Störung
	Fehler in Systemkonzepten
	Hackerangriffe
Sicherungsmedien	falsche Lagerung
	fehlerhafte Erstellung
	Diebstahl
	unkontrollierte Weitergabe
Personal	organisatorische Mängel
	Ausfall der Versorgung
	Überforderung/Irrtum
	vorsätzliche Systembeeinträchtigung
	Sabotage/Spionage
	fehlende Regelung/Kontrollen
Umwelteinflüsse/ externe Effekte	Erbeben, Hochwasser, Sturm, Energieschwankungen, Schadstoffe
	Terroranschläge
	Rechtsfragen
	Verträge und Vertragserfüllung

Abbildung 21: Bedrohungspotenziale und Gefahren[712]

[712] In Anlehnung an Biethan, Jörg; Muksch, Harry; Ruf, Walter; (2004), S. 87

11. Literaturverzeichnis

<kes> Sicherheitsstudien (1998-2006) / <kes> Sicherheitsstudien 1998-2006.

Achatzi, Günter (1991) / Achatzi, Günter; Praxis der strukturierten Analyse, Eine objektorientierte Vorgehensweise, Carl Hanser Verlag München Wien 1991.

Aebi, Daniel (2004) / Aebi, Daniel; Praxishandbuch, Sicherer IT-Betrieb, Risiken erkennen, Schwachstellen beseitigen, IT-Infrastrukturen schützen, Gabler 1. Auflage Juni 2004.

Ahrendts, Fabian; Marton, Anita (2008) / Ahrendts, Fabian; Marton, Anita; IT-Risikomanagement leben!, Wirkungsvolle Umsetzung für Projekte in der Softwareentwicklung; Springer-Verlag Berlin Heidelberg 2008.

Aktiengesetz, GmbH-Gesetz (2007) / Aktiengesetz, GmbH-Gesetz; DTV-Beck; Auflage: 40., überarb. Auflage 2007.

Alpar, Paul (2000) / Alpar, Paul; Data Mining im praktischen Einsatz; Vieweg Gabler 2000.

Anonymous (2003) / Anonymous; Hacker's Guide, Sicherheit im lokalen Netz; Markt und Technik 2003.

Anonymous (2004) / Anonymous; Hacker's Guide, Sicherheit im lokalen Netz; Markt und Technik 2004.

Bartmann, D. (1991) / Bartmann, D. (Hrsg.); Lösungsansätze der Wirtschaftsinformatik im Lichte der praktischen Bewährung; Springer 1991.

Baschin, Anja; Steffen, Andreas (2001) / Baschin, Anja; Steffen, Andreas, IT-Controlling mit der Balanced Scorecard. krp – Kostenrechnungspraxis, 16. Auflage 2001.

Bauernfeind, Markus (2007) / Bauernfeind, Markus; Integriertes Risiko- und Qualitätsmanagement: Einführung zum Risikomanagement und Integrationsmöglichkeiten im Qualitätsmanagement; GRIN Verlag, 2007.

Bawa, Joanna; Dorazio, Pat; Trenner, Lesley (2001) / Bawa, Joanna; Dorazio, Pat; Trenner, Lesley; The Usability Business; Making the Web Work; Springer London 2001.

Bea, F.X.; Friedl, B.; Schweizer, M. (2004) / Bea, F.X.; Friedl, B.; Schweizer, M.; Allgemeine Betriebswirtschaftslehre Bd. 1: Grundfragen 9. Auflage Lucius und Lucius Verlagsgesellschaft Stuttgart 2004.

Bea, Franz Xaver; Haas, Jürgen (2001) / Bea, Franz Xaver; Haas, Jürgen, Strategisches Management, 3., neu bearbeitete Auflage, Stuttgart 2001.

Behme, W.; Schimmelpfeng, K (1993) / Behme, W.; Schimmelpfeng, K.: Führungsinformationssysteme: Geschichtliche Entwicklung, Aufgaben und Leistungsmerkmale in Führungsinformationssysteme, in Behme, W.; Schimmelpfeng, K. (Hrsg.) Führungsinformationssysteme, Gabler 1993.

Behme, Wolfgang; Mucksch, Harry (2001) / Behme, Wolfgang; Mucksch, Harry; Data Warehouse-gestützte Anwendungen. Gabler 2001.

Beier, M.; von Gizycki, V. (2002) / Beier, M.; von Gizycki, V.; Usability: benutzerfreundliches Webdesign; Springer-Verlag Berlin 2002.

Bensberg, Frank (2001) / Bensberg, Frank; Web log mining als Instrument der Marketingforschung: ein systemgestaltender Ansatz für internetbasierte Märkte (1. edition). Gabler Wiesbaden 2001.

Berinato, S., (2002.) / Berinato, S.; Finally, a Real Return on Security Spending. In CIO 4/2002.

Bernhard, Dorn (1994) / Bernhard Dorn; Das informierte Management: Fakten und Signale für schnelle Entscheidungen. Bernhard Dorn (Hrsg.) Berlin, Heidelberg Springer 1994.

Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter (2006) / Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus Dieter: Moderne Verfahren der Kryptographie, Von RSA zu Zero-Knowledge, 6., verbesserte Auflage 2006.

Biethan, Jörg; Muksch, Harry; Ruf, Walter (2007) / Biethan, Jörg; Muksch, Harry; Ruf, Walter; Ganzheitliches Informationsmanagement Band II: Entwicklungsmanagement; Oldenbourg Verlag München Wien 2007.

Biethan, Jörg; Muksch, Harry; Ruf, Walter; (2004) / Biethan, Jörg; Muksch, Harry; Ruf, Walter; Ganzheitliches Informationsmanagement Band I:

Grundlagen; Oldenbourg Verlag München Wien; 6. vollständig überarbeitete und neu gefasste Auflage 2004.

Biometric Technology Today M. Kockie, Ed. March (2006) / Biometric Technology Today M. Kockie, Ed. March 2006.

Birkenbeul, A. (1995) / Birkenbeul ,A.; Realisierung eines Führungsinformationssystems für eine Holding auf Basis von Standardsoftware in Grimm; Sokolwsky, (Hrsg.) Strategische Führungsinformationssysteme; Grimm 1995.

Borman, L. (1985) / Borman, L., Curtis, B. (Hrsg.); Proceedings of the ACM CHI 85 Human Factors in Computing Systems Conference. April 14-18, 1985.

Borman, L.; Curtis, B. (Hrsg.) (1985) / Borman, L.; Curtis, B. (Hrsg.; Proceedings of the CHI'85 Conference on Human Factors in Computing Systems; April 1985.

Brands, Gilbert (2005) / Brands, Gilbert; IT-sicherheitsmanagement: Protokolle, Netzwerksicherheit, Prozessorganisation; Springer 2005.

Brockhaus - die Enzyklopädie: in 24 Bänden. F.A. Brockhaus GmbH, (1997) / Brockhaus - die Enzyklopädie: in 24 Bänden. F.A. Brockhaus GmbH, 1997.

Brunnstein, Jochen (2006) / Brunnstein, Jochen; ITIL Security Management realisieren; Vieweg 1.Auflage 2006.

BSI (2000) / BSI; Kosten und Nutzen der IT-Sicherheit; SecuMedia Verlag Ingelheim 2000.

Buchner, Frank (2007) / Buchner, Frank; Die IT-Versicherung; Eine rechtliche Untersuchung der Versicherung von Risiken der Informationstechnologie unter Berücksichtigung bisher angebotener Versicherungskonzepte und deren versicherungsrechtlichen Problemen; Peter Lang Frankfurt am Main, Berlin, Bern, Bruxelles, New York, Oxford, Wien Univ., Diss 2007.

Bundesamt für Sicherheit in der Informationstechnik (2005) / Bundesamt für Sicherheit in der Informationstechnik; IT-Sicherheitsmanagement und

IT-Grundschutz; BSI-Standards zur IT-Sicherheit; Bundesanzeiger Verlag Köln 2005.

Bundesamt für Sicherheit in der Informationstechnik (2004) / Bundesamt für Sicherheit in der Informationstechnik; Risiken und Chancen des Einsatzes von RFID-Systemen SecuMedia Verlags-GmbH 2004.

Bullinger H.-J.; Niemeier, J. ; Kroll, P. (1993) / Bullinger H.-J.; Niemeier, J. ; Kroll, P.; Führungsinformationssysteme: Einführungskonzepte und Entwicklungspotentiale in Behme; Schimmelpfeng (Hrsg.) Führungsinformationssysteme, Gabler 1993.

Bullinger, H. J. (Hrsg.) (1985) / Bullinger, H. J. (Hrsg.); Software-Ergonomie 85. Mensch-Computer-Interaktion; Stuttgart 1985.

Buxmann, P. (1996) / Buxmann, P.; Standardisierung betrieblicher Informationssysteme, Gabler 1996.

Cavusoglu, H.; Mishra, B.; Raghunathan, S. (2004.) / Cavusoglu, H.; Mishra, B.; Raghunathan, S.; A Model for Evaluating IT Security Investments. In Communication of the ACM, 47(7) 2004.

Chamoni, Peter; Gluchowski, Peter (2006) / Chamoni, Peter; Gluchowski, Peter; Analytische Informationssysteme; Business Intelligence Technologien und Anwendungen; 3. Auflage Springer Berlin Heidelberg 2006.

Chamoni, Peter; Gluchowski, Peter (1999) / Chamoni, Peter; Gluchowski, Peter; Analytische Informationssysteme, Data-Warehouse, OLAP, Data-Mining, chapter Einordnung und Überblick. Springer 1999.

Chamoni, Peter; Gluchowski, Peter (2000) / Chamoni, Peter; Gluchowski, Peter; Das Data Warehouse-Konzept. Architektur - Datenmodelle Anwendungen. Mit Erfahrungsberichten, volume 4. vollständig überarbeitete Auflage; Gabler, 2000.

Codd, Frank Edgar (1993) / Codd, Frank Edgar; Providing OLAP to User-Analysts; Hyperion Solutions Corporation 1993.

Cohen, F. (1994) / Cohen, F.; A Short Course on Computer Viruses; John Wiley & Sons Inc 1994.

Crochla, Erwin (1939) / Crochla, Erwin; Wittmann, Waldemar; Handwörterbuch der Betriebswirtschaft, 3. Auflage, Stuttgart 1939.

Data-Warehouse, OLAP, Data-Mining, chapter Entwicklung und Architekturkonzepte des On-Line Analytical Processing. Springer, 1999. / Data-Warehouse, OLAP, Data-Mining, chapter Entwicklung und Architekturkonzepte des On-Line Analytical Processing. Springer, 1999.

Dern, Gernot (2006) / Dern, Gernot; Management von IT-Architekturen, Leitlinien für die Ausrichtung , Planung und Gestaltung von Informationssystemen; 2. Auflage Vieweg-Verlag Wiesbaden 2006.

Deutsches Institut für Normung. DIN 44300. / Deutsches Institut für Normung. DIN 44300.

Deutsches Institut für Normung. DIN 66234, Teil 8: Bildschirmarbeitsplätze, Grundsätze der Dialoggestaltung, / Deutsches Institut für Normung. DIN 66234, Teil 8: Bildschirmarbeitsplätze, Grundsätze der Dialoggestaltung.

Deutsches Institut für Normung. DIN EN ISO 9241 Part 10 (1995): Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten Teil 10: Grundsätze der Dialoggestaltung, http://wwwvis.informatik.uni-stuttgart.de/eng/teaching/lecture/ws01/sw-ergonomie/iso9241.pdf / Deutsches Institut für Normung. DIN EN ISO 9241 Part 10 (1995): Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten Teil 10: Grundsätze der Dialoggestaltung, http://wwwvis.informatik.uni-stuttgart.de/eng/teaching/lecture/ws01/sw-ergonomie/iso9241.pdf

Deutsches Institut für Normung. DIN EN ISO 9241-11 (1999) / Deutsches Institut für Normung. DIN EN ISO 9241-11 (1999); Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten, Teil 11 Anforderungen an die Gebrauchstauglichkeit - Leitsätze.

Deutsches Institut für Normung. DIN EN ISO 9241-110 (2006) Ergonomie der Mensch-System-Interaktion Teil 110: Grundsätze der Dialoggestaltung (ISO 9241-110:2006) / Deutsches Institut für Normung. DIN EN ISO 9241-110 (2006) Ergonomie der Mensch-System-Interaktion Teil 110: Grundsätze der Dialoggestaltung (ISO 9241-110:2006); Deutsche Fassung EN ISO 9241-110:2006.

Diedrich, Georg (2006) / Diedrich, Georg; Integrierte Nutzenanalyse zur Gestaltung computergetützter Informationssysteme, Eine differenzierte Auswahl von Realisierungsalternativen zur prozessualen Neuausrichtung im Rechnungswesen, Dissertation, Peter Lang Europäischer Verlag der Wissenschaften 2006.

Dietrich von der Oelsnitz (Hrsg.); Weibler, Jürgen (Hrsg.); Gabriel, Roland; Beier, Dirk (2003) / Dietrich von der Oelsnitz (Hrsg.); Weibler, Jürgen (Hrsg.); Gabriel, Roland; Beier, Dirk, Informationsmanagement in Organisationen, Kohlhammer 2003.

Dittmar, Carsten (2004) / Dittmar, Carsten; Knowledge Warehouse: ein integrativer Ansatz des Organisationsgedächtnisses und die computergestützte Umsetzung auf Basis des Data Warehouse Konzepts (1. edition). Gabler Verlag Wiesbaden 2004.

Drews, Hans-Ludwig; Leßenich, Heinz Rudolf (1993) / Drews, Hans-Ludwig; Kassel, Hans; Leßenich, Heinz Rudolf; Lexikon Datenschutz und Informationssicherheit: Juristische, organisatorische und technische Begriffe, 4. wesentlich überarbeitete und erweiterte Auflage Berlin München 1993.

Dridi, Fredj (2003) / Dridi, Fredj; Sicherheitsarchitektur für Internetbasierte Informationssysteme, Entwurf und Implementierung im Rahmen des E-Government-Projektes Webnocracy, Dissertation, Eul-Verlag 1. Auflage 2003.

DTI (2004) Information Security Survey Erstelldatum 2004; Verfügbarkeitsdatum 18.01.2005. / DTI 2004 Departement of Trade and Industry (Hrsg): Information Security Survey Erstelldatum 2004 Verfügbarkeitsdatum 18.01.2005.

Du Sautoy, Marcus (2004) / Du Sautoy, Marcus; Musik der Primzahlen, Auf den Spuren des größten Rätsels der Mathematik; C.H. Beck München 2004.

DUD Datenschutz und Datensicherheit 27 (2003) / DUD Datenschutz und Datensicherheit 27 (2003).

Dzida, W. (1983) / Dzida, W.; Das IFIP-Modell für Benutzerschnittstellen, Office Management, Band 31 (Sonderheft); Apr. 1983.

Dzida, W. (1985) / Dzida, W.; Ergonomische Normen für die Dialoggestaltung. Wem nützen die Gestaltungsgrundsätze im Entwurf DIN 66 234 Teil 8 in: Bullinger, H. J. (Hrsg.); Software-Ergonomie 85. Mensch-Computer-Interaktion; Stuttgart 1985.

Dzida, W. (1988) / Dzida, W.; Modellierung und Bewertung von Benutzerschnittstellen; Software Kurier 1988.

Eason, K. D. (1984) / Eason, K. D.; Towards the experimental study of usability. Behaviour and Information Technology 3 1984.

Eberleh, E.; Oppermann, R. (1994) / Eberleh, E.; Oberquelle, H.; Oppermann, R.; Mensch-Computer-Kommunikation- Grundwissen 1/2: Einführung in die Softwareergonomie, de Gruyter 1994.

Eckert, Claudia (2006) / Eckert, Claudia, IT-Sicherheit, Konzepte – Verfahren- Protokolle, 4., überarbeitet Auflage Oldenbourg Verlag München Wien 2006.

Eckert, Claudia (2007) / Eckert, Claudia, IT-Sicherheit, Konzepte – Verfahren- Protokolle, Oldenborurg Verlag 2007.

Engels, Christoph (2008) / Engels, Christoph (2008); Basiswissen Business Intelligence; W3l GmbH, 2008.

Englbrecht, Michael (2004) / Englbrecht, Michael; Entwicklung sicherer Software, Modellierung und Implementierung mit Java; Spektrum Akademischer Verlag 1. Auflage 2004.

Erickson, Jon (2006) / Erickson, Jon; Forbidden Code, mitp 2. überarbeitete Auflage 2006.

Ertel, Wolfgang (2001) / Ertel, Wolfgang; Angewandte Kryptographie; Fachbuchverlag Leipzig 2001.

Eschweiler, Jörg (2006) / Eschweiler, Jörg; Security @ Work; Pragmatische Konzeption und Implementierung von IT-Sicherheit mit Lösungsbeispielen auf Open-Source-Basis; Springer Heidelberg 2006.

Eysenck, Hans Jürgen (1984) / Eysenck, Hans Jürgen; Die Ungleichheit der Menschen; Orion-Heimreiter-Verlag Kiel 1984.

Fank, Matthias (1985/2002) / Fank, Matthias; Business Intelligence - Das Ringen um Trendthemen in wirtschaftlich turbulenten Zeiten. In für Management e.V., I. (Ed.), White Paper Köln Schmidt, E.; 1985.

Federrath, H. (2006) / Federrath, H.; Kosten und Nutzen der IT-Sicherheit. In HMD; Heft 248; April 2006.

Ferguson, G. T. (2002) / Ferguson, G. T.; Have your objects call my objects. In: Havard Business Review, 80(6) June 2002.

Fernholz, M.; Buresch, A. in Krcmar, H.; Buresch, A., & Reb, M. (Eds.) / Fernholz, M.; Kielwein, L.; Buresch, A.; IV-Produkt-Controlling in Krcmar, H., Buresch, A., & Reb, M. (Eds.), IV-Controlling auf dem Prüfstand.

Fischer, Joerg K. (2008) / Fischer, Joerg K.; Medienrecht und Medienmärkte; Springer Berlin Heidelberg 2009.

Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf (1998) / Fischer, Stephan; Steinacker, Achim; Bertram, Reinhard; Steinmetz, Ralf; Open Security, Von den Grundlagen zu den Anwendungen; Springer Berlin, Heidelberg 1998.

Fleisch, E.; Mattern, F.; Billinger, S. (2003) / Fleisch, E.; Mattern, F.; Billinger, S.; Betriebswirtschaftliche Applikationen des Ubiquitous Computing. In: Praxis der Wirtschaftsinformatik; Februar 2003.

Franke, G. in Hichert, Rolf (1995) / Franke, G. in Hichert, Rolf; Moritz, Michael (Hrsg.); Management- Informationssysteme; 2., völlig neubearbeitete und erweiterte Auflage Berlin 1995.

Fritz, Burkhard (1999) / Fritz, Burkhard; DV-unterstützte Führungsinformationssysteme; Frankfurt am Main 1999.

Gabriel, R. (2001) / Gabriel, R.; Dittmar, C.; Der Ansatz des Knowledge Management im Rahmen des Business Intelligence, HMD 222, Dez. 2001.

Gartner Group (1987) / Gartner Group 1987.

Geier, Christoph (1999) / Geier, Christoph; Optimierung der Informationstechnologie bei BPRProjekten, Hohenheim 1999.

Geiger, Gebhard (2007) / Geiger, Gebhard; Managementhandbuch IT-Sicherheit. Risiken, Basel II, Recht; Berlin 2007.

Geiser, G. (1990) / Geiser, G.; Mensch-Maschine-Kommunikation; Oldenburg 1990.

Genossenschaftsrecht (2007) / Genossenschaftsrecht; DTV-Beck 4. Aufl. 2007.

Geschonneck, Alexander (2006) / Geschonneck, Alexander; Computer Forensik, Systemeinbrüche erkennen, ermitteln, aufklären; 2., aktualisierte Auflage dpunkt.verlag Heidelberg 2006.

Geschonneck, Alexander (2004) / Geschonneck, Alexander; Datenrettung und digitale Spurensammlung Notaufnahme in IX 1/2004.

Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.) (2007) / Gitter, Rotraud; Lotz, Volkmar; Pinsdorf, Ulrich; Roßnagel, Alexander (Hrsg.); Sicherheit und Rechtsverbindlichkeit mobiler Agenten. Deutscher Universitäts-Verlag 1. Auflage 2007.

Gluchowski P. (2001) / Gluchowski P.; Business Intelligence, Konzepte, Technologien und Einsatzbereiche in Business Intelligence, HMD 222, Dez. 2001.

Göbel, Siegbert (2005) / Göbel, Siegbert; Elektronisches Geld zwischen Zahlungsmittel und Verrechnungssystem, Eine ökonomische Analyse; Logos Berlin 2005.

Godschalk, David (2007) / Godschalk, David; Computer Related Occupational Deviance; Ein Mehr-Ebenen-Modell zur Erklärung und Prävention; Deutscher Universitätsverlag Januar 2007.

Görtz, Horst; Stolp, Jutta (1999) / Görtz, Horst; Stolp, Jutta; Informationssicherheit in Unternehmen, Sicherheitskonzepte und –lösungen in der Praxis, Addison-Wesley, 1. Auflage 1999.

Governance Working Paper 236 / Governance Working Paper 236; Cambridge; Sloan School of Management.

Graf; Jürgen-Peter (2007) / Graf; Jürgen-Peter (2007); Zur Strafbarkeit des „Phishing". In: Hoffmann, Mathis; Leible, Stefan; Sosnitza, Olaf (Hrsg.): Geistiges Eigentum im virtuellen Raum. Richard Boorberg Verlag, Stuttgart, München, Berlin, Hannover, Dresden, Weimar 2007, S. 173–184.

Groffmann, Hans-Dieter (1993) / Groffmann, Hans Dieter ; Kooperatives Führungsinformationssystemen, Grundlagen-Konzept-Prototyp; Gabler 1993.

Groffmann, Hans-Dieter (1992) / Groffmann, Hans-Dieter; Kennzahlendatenmodell (KDM) als Grundlage aktiver Führungsinformationssysteme; Lehrstuhl für Wirtschaftsinformatik der Universität Tübingen (Hrsg.) Arbeitsberichte zur Wirtschaftsinformatik 1992.

Grothe, M.; Gentsch, P. (2000) / Grothe, M.; Gentsch, P.; Business Intelligence – Aus Informationen Wettbewerbsvorteile gewinnen; Addison Wesley München 2000.

Gründer, Torsten (2007) / Gründer, Torsten in Gründer, Torsten; Schrey, Joachim; Managementhandbuch IT-Sicherheit, Risiken, Basel II, Recht, Erich Schmidt Verlag; Berlin 2007.

Gründer, Torsten in Gründer, Torsten (2007) / Gründer, Torsten; Schrey, Joachim (Herausgeber); Managementhandbuch IT-Sicherheit, Risiken, Basel II, Recht; Erich Schmid Verlag 2007.

Haar, Tobias; Schädler, Sarah (2004) / Haar, Tobias; Schädler, Sarah iX 2004.

Hahn (1985) / Hahn 1985 S. 25 f Band 8 Arbeitsbericht.

Hahne, Michael (1999) / Hahne, Michael ; Analytische Informationssysteme, Data-Warehouse, OLAP, Data-Mining, chapter Logische Datenmodellierung für das DataWarehouse; Springer 1999.

Hamilton, Patrick (2007) / Hamilton, Patrick; Dynaxity, Management von Dynamik und Komplexität im Softwarebau; Springer 2007.

Handelsgesetzbuch (2007) / Handelsgesetzbuch; DTV-Beck 46., überarb. Auflage 2007.

Handschuh, Helena; Trichina, Elena; (2006) / Handschuh, Helena; Trichina, Elena; Hardware Security Features for Secure Embedded Devices in Paulus, Sachar; Pohlmann, Norbert; Reimer Helmut; ISSE 2006 Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe 2006 Conference, Vieweg 2006.

Hannig, Uwe (2002) / Hannig, Uwe; Knowledge Management and Business Intelligence; Springer 2002.

Hansen, W. J. (1971) / Hansen, W. J.; User engineering principles for interactive systems, Proc. Fall Joint Computer Conference, 39, AFIPS Press Montvale, NY 1971.

Harloff, Joachim (2005) / Harloff, Joachim (2005), Gebrauchstauglichkeit (Usability) – Idee und Rahmenbedingungen, in; Information Management & Consulting, 20. Jahrgang, Heft 3, 2005 S. 45.

Heilmann, Wolfgang, Reusch, Günter (1984) / Heilmann, Wolfgang, Reusch, Günter (1984) Datensicherheit und Datenschutz: Hilfe zur Bestimmung eines eigenen Standpunktes.

Heinen, Edmund (1969) / Heinen, Edmund; Zum wissenschaftsprogramm der entscheidungsorientierten Betriebswirtschaftslehre in Zeitschrift für Betriebswirtschaftslehre 39 1969 S. 207-220.

Heinen, Edmund (1982) / Heinen, Edmund; Einführung in die Betriebswirtschaftslehre, 8. durchgesehene Auflage, Wiesbaden 1982.

Heinrich, Lutz, J. (1997) / Heinrich, Lutz, J. ; Management von Informatik-Projekten, Wirtschaftsinformatik, München: Oldenbourg 1997.

Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2004) / Heinrich, Lutz; Heinzl, Armin; Roithmayr Friedrich; Wirtschaftsinformatik Lexikon, 7. vollständig überarbeitete und erweiterte Auflage München, Wien: R. Oldenbourg-Verlag 2004.

Heinrich, Lutz; Heinzl, Armin; Roithmayr, Friedrich (2007) / Heinrich, Lutz; J, Heinzl, Armin; Roithmayr, Friedrich; Wirtschaftsinformatik, Einführung und Grundlegung, Oldenbourg Verlag München Wien, 2., vollständig überarbeitete und ergänzte Auflage 2007.

Heitmann, M. (2007) / Heitmann, M.; IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie; 2007.

Helander, M. / Helander, M.; Handbook of human-computer interaction, Amsterdam: North-Holland Publishing Company.

Hellige, Hans Dieter (2003)/ Hellige, Hans Dieter; Geschichten der Informatik: Visionen, Paradigmen, Leitmotive; Springer, 2003.

Helmbrecht, Udo (2007) / Helmbrecht, Udo; Mobile Sicherheit gestalten, in: <kes> Special Mobile Security 2007, Sonderausgabe Juli 2007, Ingelheim.

Henning M.; (2003) / Henning M.: Konzeption und Implementierung eines computergestützten Management- Informations- und Steuerungssystems (MISS) im Projektmanagement, Kovac 2003.

Herczeg, Michael (2005)/ Herczeg, Michael; Software-Ergonomie: Grundlagen der Mensch-computer-kommunikation; Oldenbourg Wissenschaftsverlag, 2005.

Herczeg, M. (1994) / Herczeg, M.: Software-Ergonomie, Addison-Wesley 1994.

Herczeg, Michael (2006) / Herczeg, Michael; Interaktionsdesign, Gestaltung interaktiver und multimedialer Systeme; Oldenbourg Verlag München Wien 2006.

Hichert, Rolf (1995) / Hichert, Rolf; Moritz, Michael (Hrsg.); Management-Informationssysteme; 2., völlig neubearbeitete und erweiterte Auflage Berlin 1995.

Hichert, Rolf; Moritz, Michael (Hrsg.) (1995) / Hichert, Rolf; Moritz, Michael in Hichert, Rolf; Moritz, Michael (Hrsg.); Management- Informationssysteme, 2., völlig neubearbeitete und erweiterte Auflage Berlin u.a. 1995.

Hiskett, P. A.; Rosenberg, D.; Peterson, C. G.; Hughes, R. J.; Nam, S; Lita, A. E.; Miller, A. J.; Nordholt J. E. (2006): Long-distance quantum key distribution in optical fibre. In: New Journal of Physics. 8, Nr. 9, 2006, S. 193.

Hoffmann, H. (1993) / Hoffmann, H.; Computergestützte Planung als Führungsinstrument; Grundlagen, Konzept, Prototyp; Gabler 1993.

Holthuis, Jan (2000) / Holthuis, Jan; Das Data Warehouse-Konzept. Architektur Datenmodelle Anwendungen. Mit Erfahrungsberichten; 4. vollständig überarbeitete Auflage Gabler 2000.

Holzinger, Andreas (2000) / Holzinger, Andreas; Basiswissen Multimedia Band 1, Technik, Würzburg 2000.

Homeister, Matthias (2005) / Homeister, Matthias; Quantum Computing verstehen, Grundlagen, Anwendungen, Perspektiven; Vieweg-Verlag 2005.

Hoppe, G.; Prieß, A. () / Hoppe, G.; Prieß, A.; Sicherheit von Informationssystemen; NWB-Studienbücher; Herne/Berlin.

Horváth, Peter (2003) / Horváth, Peter Controlling (9. edition). Vahlen, München 2003.

Hoyer, Rudolfin; Krallmann, Hermann; Klotz, Michael; Wenzel, Hermann (Hrsg.) (1994) / Hoyer, Rudolfin; Krallmann, Hermann; Klotz, Michael; Wenzel, Hermann (Hrsg.); Führungsinformationssysteme in Unternehmen, Erfolgsfaktoren, Vorgehensweisen und Perspektiven, Erich Schmidt Verlag Berlin 1994.

Hübsch, G.; Springer, T.; Schill, A.; Spriestersbach, A.; Ziegert (2003) / Hübsch, G.; Springer, T.; Schill, A.; Spriestersbach, A.; Ziegert, T.; Systemlösungen für die Entwicklung adaptiver Anwendungen für mobile und ubiquitäre Infrastrukturen, In: Praxis der Wirtschaftsinformatik, Februar 2003.

Humm, B.; Wietek, F. (2005) / Humm, B ; Wietek, F. in Informatik Spektrum 2005 Heft 1 Band 28; Architektur von Data Warehouses und Business IntelligenceSystemen.

Hummelt, Roman (1997) / Hummelt, Roman; Wirtschaftsspionage auf dem Datenhighway. Strategische Risiken und Spionageabwehr; München Wien 1997.

Hutchins, E. L.; Hollan, J. D.; Norman, D. A. (1986) / Hutchins, E. L.; Hollan, J. D.; Norman, D. A.; Direct manipulation interfaces. In Norman D. A.; Droper S. W. (Eds.); User centered system design, Hillsdale, NJ Lawrence Erlaum Associates 1986.

IBM (1987) / IBM; Systems Application Architecture. Common User Access. Panel Design and User Interaction, o.O. 1987.

Informatik Spektrum 2005 Heft 1 Band 28. / Informatik Spektrum 2005 Heft 1 Band 28.

International Standardisation Organisation ISO-Norm 9241-11, (1996) / International Standardisation Organisation ISO-Norm 9241-11, 1996.

Jäger-Goy, Heidi (2002) / Jäger-Goy, Heidi (2002); Führungsinstrumente für das IV-Management; Peter Lang GmbH Europäischer Verlag der Wissenschaften Frankfurt am Main 2002.

Jahnke, B. (1993a) / Jahnke, Bernd; Entscheidungsunterstützung der oberen Führungsebene durch Führungsinformationssysteme. Lehrstuhl für Wirtschaftsinformatik der Universität Tübingen (Hrsg.), Arbeitsbericht zur Wirtschaftsinformatik; Tübingen 1993.

Jahnke, B. / Jahnke, B.; Vorlesung Wirtschaftsinformatik 1 und 4 an der Universität Tübingen.

Jahnke, B. (1991) / Jahnke, B.; Konzeption und Entwicklung eines Führungsinformationssystems in Bartmann, D. (Hrsg.); Lösungsansätze der Wirtschaftsinformatik im Lichte der praktischen Bewährung; S. 39-65; Springer 1991.

Jahnke, B. (1993) / Jahnke, B.; Einsatzkriterien, kritische Erfolgsfaktoren und Einführungsstrategien für Führungsinformationssysteme in Brehme; Schimmelpfeng (Hrsg.): Führungsinformationssysteme, S. 29-43; Gabler 1993.

Jahnke, B. (1996) / Jahnke, B.; Groffmann, Hans-Dieter; Kruppa, Stephan; On-Line Analytical Processing (OLAP). S. 321-324; Wirtschaftsinformatik, 1996.

Jahnke, B. (2005) / Jahnke, B.; Vorlesung Wirtschaftsinformatik 3 im Wintersemester 2004/2005 an der Universität Tübingen.

Jahnke, B.; Groffmann, H.-D. (1993a) / Jahnke, B.; Groffmann, H.-D.; Führungsinformationssysteme zwischen Anspruch und Realisierbarkeit in Arbeitsberichte zur Wirtschaftsinformatik 9, 1993.

Joos, Richard; Jorberg, Randolf; Gönnemann, Axel (2008) / Joos, Richard; Jorberg, Randolf; Gönnemann, Axel; gulli wars; Books on Demand Gmbh; Auflage: 1 August 2008.

Jung, V. (1998) / Jung, V.; Integrierte Benutzerunterstützung für die Visualisierung in Geo- Informationssystemen Dissertation am Fachbereich Informatik, Fachgebiet GRIS, TU Darmstadt, Fraunhofer IRB Verlag 1998.

Kaesler, Clemens (2007) / Kaesler, Clemens; Recht für Medienberufe; Kompaktes Wissen zu allen rechtstypischen Fragen Vieweg Wiesbaden 2007.

Kaplan, R. S.; Norton, D. P. (1997) / Kaplan, R. S.; Norton, D. P.; The Balanced Scorecard - Strategien erfolgreich umsetzen; Schäer-Poeschel 1997 .

Kappes, Martin (2007) / Kappes, Martin; Netzwerk- und Datensicherheit: Eine praktische Einführung; Vieweg+Teubner Verlag 2007.

Kargl, Herbert (2000) / Kargl, Herbert; Management und Controlling von IV-Projekten, München, Wien 2000.

Kästner, Sven / Kästner, Sven; Polizeidaten bei Ebay, Geheimes Schnäppchen.

Kemper, Hans-Georg; Finger, Ralf (1999) / Kemper, Hans-Georg; Finger, Ralf; Analytische Informationssysteme, Data-Warehouse, OLAP, Data-Mining, Chapter Datentransformation im Data Warehouse; Springer 1999.

Kerner, Simone (2002) / Kerner, Simone; Analytisches Customer Relationship Management in Kreditinstituten: Data Warehouse und Data Mining als Instrumente zur Kundenbindung im Privatkundengeschäft (1. edition). Wiesbaden 2002.

Kersten, Heinrich (1991) / Kersten, Heinrich; Einführung in die Computersicherheit, München, Wien 1991.

Kersten, Heinrich; Klett Gerhard (2008) / Kersten, Heinrich; Klett Gerhard; Der IT-Security Manager; Expertenwissen für jeden IT-Security Manager – Von namhaften Autoren praxisnah vermittelt; 2. Auflage <kes> vieweg teubner Wiesbaden 2008.

Kersten, Heinrich (Hrsg.); Reuter, Jürgen; Schröder, Klaus-Werner (2008) / Kersten, Heinrich (Hrsg.); Reuter, Jürgen; Schröder, Klaus-Werner; IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Der Weg zur Zertifizierung; vieweg 1. Auflage 2008.

Kirsch, Werner (1977) / Kirsch, Werner; Einführung in die Theorie der Entscheidungsprozesse; 2. durchgesehene und ergänzte Auflage der Bände I bis III als Gesamtausgabe, Wiesbaden 1977.

Kleiner, Marco; Müller, Lucas; Köhler, Mario (2005) / Kleiner, Marco; Müller, Lucas; Köhler, Mario; IT-Sicherheit – Make or Buy, Was Sie selbst machen müssen und was sich outsourcen lässt; Vieweg Verlag 1. Auflage 2005.

Knobloch, Bernd in Maur, E., & Winter, R. (Eds.) (2002) / Knobloch, Bernd; Ein Bezugsrahmen für integrierte Managementunterstützungssysteme; Einordnung und funktionale Anforderungen an Business-Intelligence-Systeme aus managementtheoretischer Sicht. In Maur, E., & Winter, R. (Eds.), Vom Data Warehouse zum Corporate Knowledge Center Heidelberg. Physica 2002.

Knöll, Heinz-Dieter; Schulz-Sacharow; Zimpel, Michael (2006) / Knöll, Heinz-Dieter; Schulz-Sacharow, Christoph; Zimpel, Michael; Unternehmensführung mit SAP® BI; Vieweg 2006.

Kollmann, Tobias (2007) / Kollmann, Tobias; E-Business, Grundlagen elektronischer Geschäftsprozesse in der Net Economy; Gabler 1. Auflage 2007.

Krallmann, Hermann (1996) / Krallmann, Hermann; Systemanalyse im Unternehmen: Geschäftsprozessoptimierung, partizipative Vorgehensmodelle, objektorientierte Analyse; Oldenbourg 2., durchges. Auflage 1996.

Krcmar, H. / Krcmar, H.; Buresch, A.; Reb, M. (Eds.); IV-Controlling auf dem Prüfstand.

Krcmar, Helmut (2003) / Krcmar, Helmut; Informationsmanagement. Springer 2003.

Krcmar, Helmut (2005) / Krcmar, Helmut; Informationsmanagement, 4. überarbeitete und erweiterte Auflage Berlin, Heidelberg 2005.

Krüger (1994) / Krüger; Organisation der Unternehmung, Kohlhammer-Lehrbuchreihe Betriebswirtschaft, Kohlhammer, 3. verb. Auflage Stuttgart 1994.

Küpper, Hans-Ulrich (2001) / Küpper, Hans-Ulrich; Controlling, Controlling-Konzepte. Konzeption, Aufgaben und Instrumente; Schäffer-Poeschel, 3. überarbeitete und erweiterte Auflage Stuttgart 2001.

Kurz (1999) / Kurz; Data Warehousing. Enabeling Technology; mitp 1999.

Kütz, Martin (2005) / Kütz, Martin; IT-Controlling für die Praxis, Konzeption und Methoden; dpunkt.verlag 1. Auflage 2005.

Kyrer, Alfred (2001) / Kyrer, Alfred; Wirtschaftslexikon; 4. vollständig neu bearbeitete und stark erweiterte Auflage, München, Wien 2001.

Laudon, Kenneth, C.; Laudon, Jane, P. (2006) / Laudon, Kenneth, C.; Laudon, Jane, P. Management information systems: managing the digital firm; Ninth Edition Pearson 2006.

Laux, Helmut (2005) / Laux, Helmut; Entscheidungstheorie; 6. durchgesehene Auflage, Berlin 2005.

Le Roux, Yves; in Pohlmann, Norbert; Reimer, Helmut; Schneider, Wolfgang (2007) / Le Roux, Yves; Information Security Governance for Executive Management in Pohlmann, Norbert; Reimer, Helmut; Schneider, Wolfgang; ISSE/SECURE 2007 Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe / SECURE 2007 Conference, vieweg, 1st editon 2007.

Lehner, Franz; Wildner, Stephan; Scholz, Michael (2007) / Lehner, Franz; Wildner, Stephan; Scholz, Michael; Wirtschaftsinformatik eine Einführung; München, Wien 2007.

Leidinger, Bernhard J.G. (1998) / Leidinger, Bernhard J.G., Schadensmanagement; Erich Schmidt Verlag GmbH &, 1998.

Leser, Ulf; Naumann, Felix (2007) / Leser, Ulf; Naumann, Felix; Informationsintegration, Architekturen und Methoden zur Integration verteilter und heterogener Datenquellen, dpunkt.verlag 1. Auflage 2007.

Link, Jörg (1982) / Link, Jörg; Die methodologischen, informationswissenschafltichen und führungspolitischen Aspekte des Controlling, in Zeitschrift für Betriebswirtschaftslehre 52, 1982 S. 264-280.

Lotz, Volkmar (2007) / Lotz, Volkmar; SOA-Sicherheit für moderne Unternehmen in DUD Datenschutz und Datensicherheit 31, 2007.

Lubich, H. P. (2006) / Lubich, H. P.; IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtungen. In HMD; Heft 248; April 2006.

Luhn; Hans Peter (1958) / Luhn; Hans Peter (1958); A Business Intelligence System; IBM Research Journal, 1958.

Lusti, Markus (2002) / Lusti, Markus; Data warehousing und data mining: eine Einführung in entscheidungsunterstützende Systeme (2. edition). Springer, Heidelberg 2002.

MacKinlay, J. (1986) / MacKinlay, J.; Automating the Desing of Graphical Presentations of Relational Information ACM Transactions on Graphics; Vol.5, Nr.2 1986.

Malz, Helmut (2004) / Malz, Helmut; Rechnerarchitektur; Vieweg + Teubner Verlag 2004.

Manhartsberger, Martina; Musil, Sabine; (2001) / Manhartsberger, Martina; Musil, Sabine; Web Usability, Das Prinzip des Vertrauens; Galileo Press 1. Auflage 2001.

McClur, Stuart; Scrambray, Joel; Kurtz, George (2006) / McClur, Stuart; Scrambray, Joel; Kurtz, George; Das Anti-Hacker-Buch; bhv Hamburg, 5. Auflage 2006.

McIlwraith, Angus (2006) / McIlwraith, Angus; Information Security and Employee Behaviour, How to Reduce Risk Throug Employee Education, Training and Awareness, Gower Publishing Company USA 2006.

McLeod, R.; Schell, G. (2001) / McLeod, R.; Schell, G.; Management Information Systems, 8th ed., Upper Saddle River NJ: Prentice-Hall 2001.

Medosch, Armin (2007) / Medosch, Armin; Modulares Verbrechen in IX 6/2007.

Meier, Andreas (2007) / Meier, Andreas; Relationale und postrelationale Datenbanken; 6. Auflage Springer Berlin Heidelberg 2007.

Mertens, J.; Griese, P. (2004) / Mertens, J. ;Griese, P.; Integrierte Informationsverarbeitung 1. Gabler, 2004.

Merz, Michael (1999) / Merz, Michael; Electronic Commerce, Marktmodelle, Anwendungen und Technologien, dpunkt.verlag Heidelberg 1. Auflage 1999.

Meyer, J. A. (1999) / Meyer, J. A.; Visualisierung von Informationen: verhaltenswissenschaftliche Grundregeln für das Management; Gabler 1999.

Meyer, Markus; Winter, Robert (2000) / Meyer, Markus; Winter, Robert; Data Warehousing 2000, Methoden, Anwendungen, Strategien, chapter Organisation des unternehmensweiten Data Warehousing; Physica-Verlag 2000.

Mitchell, J.; Shneiderman, B. (1998) / Mitchell, J.; Shneiderman, B.; Dynamic Versus Static Menus: An Exploratory Comparison. ACM SIGCHI Bulletin, Band 20(4), April 1998.

Mitnick, Kevin; Simon, William (2003) / Mitnick, Kevin; Simon, William; Risikofaktor Mensch, Die Kunst der Täuschung; mitp-Verlag/Bonn 2003.

Moormann, Jürgen; Schmidt, Günter (2007) / Moormann, Jürgen; Schmidt, Günter; IT in der Finanzbranche, Management und Methoden; Springer-Verlag Berlin Heidelberg 2007.

Moos, Flemming (2006) / Moos, Flemming; Datenschutz, Recht, Schnell Erfasst, Springer Berlin, Heidelberg 2006.

Mucksch, Harry; Behme, Wolfgang (2000) / Mucksch, Harry; Behme, Wolfgang; Analytische Informationssysteme, Das Data Warehouse-Konzept. Architektur Datenmodelle Anwendungen. Mit Erfahrungsberichten; 4. vollständig überarbeitete Auflage Gabler 2000.

Müller, Jochen (2000) / Müller, Jochen; Transformation operativer Daten zur Nutzung im Data Warehouse. DUV 2000.

Müller, Klaus-Rainer (2003) / Müller, Klaus-Rainer; IT-Sicherheit mit System, Strategie – Vorgehensmodell – Prozessorientierung – Sicherheitspyramide, vieweg Wiesbaden, 1. Auflage 2003.

Müller, Rainer (2005) / Müller, Rainer; Handbuch Unternehmenssicherheit, Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System, Vieweg 1. Auflage 2005.

Müller-Böling; Ramme (1990) / Müller-Böling; Ramme 1990. Arbeitsbericht 8.

Munnelly, Brendan; Holden, Paul (2005) / Munnelly, Brendan; Holden, Paul; ECDL: Der europäische Computer-führerschein; das komplette Kursbuch für Microsoft Office 2003 nach Syllabus 4.0;[anerkannte Schulungsunterlagen]; Pearson Education Deutschland 2005.

Müßig, S. (2006) / Müßig, S.; Haben Sicherheitsinvestitionen eine Rendite? In HMD; Heft 248; April 2006.

Norman, D. A. (1986) / Norman, D. A.; Droper, S. W. (Eds.); User centered system design, Hillsdale, NJ Lawrence Erlaum Associates 1986.

Nowey, T.; Federrath, H.; Klein, C. ;Plößl, K. (2005) / Nowey, T. ; Federrath, H.; Klein, C. ;Plößl, K.; Ansätze zur Evaluierung von Sicherheitsinvestitionen. In Sicherheit 2005; Beiträge der 2 Jahrestagung des GL-Fachbereichs Sicherheit; Köllen-Verlag Bonn 2005.

Oberquelle, H. in Eberleh, E.; Oberquelle, H.; Oppermann, R. (1994) / Oberquelle, H.; Formen der MCI in Eberleh, E.; Oberquelle, H.; Oppermann, R.; Mensch-Computer-Kommunikation- Grundwissen 1/2: Einführung in die Softwareergonomie, de Gruyter 1994.

Olfert, Klaus; Rahn, Horst-J. (2005) / Olfert, Klaus; Rahn, Horst-J.; Einführung in die Betriebswirtschaftslehre; 8. Aufl., Ludwigshafen/Rhein 2005.

Paul, Joachim (2007) / Paul; Joachim; Einführung in die Allgemeine Betriebswirtschaftslehre; Wiesbaden 2007.

Pfohl, Hans-Christian (1977) / Pfohl, Hans-Christian; Problemorientierte Entscheidungsfindung in Organisationen in Mensch und Organisation hrsg. von Staehle, Wolfgan, H. Band 5 Berlin, New York 1977.

Pfohl, Hans-Christian; Braun, Günther, E. (1981) / Pfohl, Hans-Christian; Braun, Günther, E.; Entscheidungstheorie. Normative und deskriptive Grundlagen des Entscheidens; Landsberg am Lech 1981.

Picot, A. (2003) / Picot, A.; Die grenzenlose Unternehmung, 5. Auflage, Gabler, 2003.

Poguntke, Werner (2007) / Poguntke, Werner; Basiswissen IT-sicherheit; Das Wichtigste für den Schutz von Systemen und Daten; W3I 2007.

Pohlmann, N. (2006h) / Pohlmann, N.; Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen? In HMD Heft 248; Praxis der Wirtschaftsinformatik 2/2006.

Pohlmann, Norbert; Blumberg Hartmut (2004) / Pohlmann, Norbert; Blumberg Hartmut; Der IT-Sicherheitsleitfaden Das Pflichtenheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen mitp-Verlag/Bonn 2004.

Pohlmann, Norbert; Reimer, Helmut (Hrsg.) (2008) / Pohlmann, Norbert; Reimer, Helmut (Hrsg.); Trusted Computing, Ein Weg zu neuen IT-Sicherheitsarchitekturen; 1. Auflage Vieweg Wiesbaden 2008.

Potthof, Ingo (1998) / Potthof, Ingo; Kosten und Nutzen der Informationsverarbeitung, Wiesbaden 1998.

Powell, C. (2006) / Powell, C.; „UK Co-op offers biometric payment“ in Biometric Technology Today M. Kockie, Ed. March 2006.

Powell, C. (2006); in Biometric Technology Today. / Powell, C.; „UK Co-op offers biometric payment“ in Biometric Technology Today M. Kockie, Ed. March 2006.

Praxis der Wirtschaftsinformatik (2003) / Praxis der Wirtschaftsinformatik, Februar 2003.

Preuschoff, Sarah (2002) / Preuschoff, Sarah; Business Intelligence – Gegenstand, Ansätze und Technologien. In Nohr, H. (Ed.), Arbeitspapiere Wissensmanagement Stuttgart 2002.

Paulus, Sachar; Reimer Helmut (2006) / Paulus, Sachar; Pohlmann, Norbert; Reimer Helmut; ISSE 2006 Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe 2006 Conference, Vieweg 2006.

Radtke, Angie; Charlier, Michael (2006) / Radtke, Angie; Charlier, Michael; Barrierefreies Webdesign, Attraktive Websites zugänglich gestalten, Addison-Wesley 2006.

Rau, Karl-Heinz (2007) / Rau, Karl-Heinz; Objektorientierte Systementwicklung, Vom Geschäftsprozess zum Java-Programm,Vieweg Wiesbaden, 1. Auflage 2007.

Redmill, Felix; Anderson (Eds), Tom; (2004) / Redmill, Felix; Anderson (Eds), Tom; Practical Elements of Safety, Proceedings of the Welth Safety-critical Systems Symposium, Birmingham, UK 17-19 February 2004, Springer-Verlag London 2004.

Reichmann, Laurenz; Lachnit, Thomas (1976) / Reichmann, Laurenz; Lachnit, Thomas; Planung, Steuerung und Kontrolle mit Hilfe von Kennzahlen; 1976.

Reichmann, Thomas (2001) / Reichmann, Thomas; Controlling mit Kennzahlen und Managementberichten; Vahlen 2001.

Reinke, Schuster (2000) / Reinke; Schuster. OLAP verstehen. Microsoft Press Deutschland, 2000.

Reiterer H.; Mann, T. M.; Mußler, G.; Bleimann, U. (2000) / Reiterer H.; Mann, T. M.; Mußler, G.; Bleimann, U.; Visualisierung von entscheidungsrelevanten Daten für das Management in HMD Praxis der Wirtschaftsinformatik, Heft 212 04/2000.

Reitmann-Olson, J. (1985) / Reitmann-Olson, J.; Expanded design procedures for learnable, usable interfaces, in Borman, L., Curtis, B. (Hrsg.); Proceedings of the ACM CHI 85 Human Factors in Computing Systems Conference. April 14-18, 1985.

Rey, Enno; Thumann, Michael; Baier, Dominick (2005) / Rey, Enno; Thumann, Michael; Baier, Dominick; Mehr IT-Sicherheit durch Pen-Tests, Optimierung der IT-Sicherheit durch gelenktes “Hacking“ – Von der Planung über die Vertragsgestalötung zur Realisierung, Vieweg 2005.

Roberts, T. L.; Moran, T. P. (1982) / Roberts, T. L.; Moran, T. P.; Evaluation of text editors. In: Proceedings of Human Factors in computing systems, Gaithersburg, Maryland, March 15-17, 1982, Washington, D.C.:ACM.

Roßnagel (2005) / Roßnagel; Universität Kassel auf dem Symposium Der Computer im 21. Jahrhundert. Die Informatisierung des Alltags. 21-22.03.05 in Zürich. Vortrag Datenschutz in einem informatisierten Alltag.

Roth, Richard (Hrsg.); Behrens Michael (2001) / Roth, Richard (Hrsg.); Behrens Michael; Biometrische Identifikation, Grundlagen, Verfahren, Perspektiven, Vieweg a. Auflage 2001.

Saleck, T. (2005) / Saleck, T.; Chefsache IT-Kosten; Vieweg Verlag 2. Auflage Wiesbaden 2005.

Saleck, Theo (2005) / Saleck, Theo; Chefsache IT-Kosten, Bezahlbare IT, Die Leistung sichern, Implementierungshilfen; Vieweg 2. verbesserte und erweiterte Auflage 2005.

Sandig, Curt in Crochla, Erwin; Wittmann, Waldemar; (1939) / Sandig, Curt; Risiko; in Crochla, Erwin; Wittmann, Waldemar; Handwörterbuch der Betriebswirtschaft, 3. Auflage, Stuttgart 1939.

Sarodnick, Florian; Brau, Henning (2006) / Sarodnick, Florian; Brau, Henning; Methoden der Usability Evaluation, Wissenschaftliche Grundlagen und praktische Anwendung, Huber Verlag Bern 2006.

Schadt, D. (2006). / Schadt, D.; Über die Ökonomie der IT-Sicherheit; in HMD; Heft 248; April 2006.

Scheer, A.-W. (1998) / Scheer, A.-W.; Wirtschaftsinformatik – Studienausgabe, 2. Aufl. Berlin/Heidelberg/New York 1998.

Schierenbeck, Henner (2003) / Schierenbeck, Henner (2003): Grundzüge der Betriebswirtschaftslehre, Oldenbourg Wissenschafts-Verlag, München, Seite 28.

Schifreen, Robert (2006) / Schifreen, Robert; Defeating the Hacker; A non-technical guide to computer security; John Wiley & Sons, LtdWest Sussex 2006.

Schinzer, H. (1996) / Schinzer, H.; Entscheidungsorientiertes Informationssystem, Verlag Vahlen 1996.

Schinzer, Heiko (1996) / Schinzer, Heiko; Entscheidungsorientierte Informationssysteme. Grundlagen, Anforderungen, Konzept, Umsetzung; München 1996.

Schinzer, Heiko; Bange, Carsten (1999) / Schinzer; Heiko; Bange; Carsten; Analytische Informationssysteme, Data-Warehouse, OLAP, Data-Mining, chapter Werkzeuge zum Aufbau analytischer Informationssysteme. Springer, 1999.

Schmeh, Klaus (2001) / Schmeh, Klaus; Kryptografie und Public-Key-Infrastrukturen im Internet; dpunkt.verlag 2. Auflage 2001.

Schmidt, Klaus (2006) / Schmidt, Klaus; Der IT-Security Manager; Carl Hanser Verlag München Wien 2006.

Schneider, Bruce (2000) / Schneier, Bruce; Secrets and Lies. Digital Security in a networked world; Wiley Computer Publishing 2000.

Schrey, Joachim in Gründer, Torsten (2007) / Schrey, Joachim in Gründer, Torsten; Schrey, Joachim (Herausgeber); Managementhandbuch IT-Sicherheit, Risiken, Basel II, Recht, Erich Schmid Verlag 2007.

Schulze, Tillmann (2006) / Schulze, Tillmann; Bedingt abwehrbereit; Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA; Verlag für Sozialwissenschaften 2006.

Schumacher, Markus; Rödig, Utz; Moschgath, Marie-Luise (2003) / Schumacher, Markus; Rödig, Utz; Moschgath, Marie-Luise; Hacker Contest, Sicherheitsprobleme, Lösungen, Beispiele; Springer Berlin, Heidelberg, New York 2003.

Schumann, H. (2000) / Schumann H.; Müller, W.; Visualisierung, Springer 2000.

Schumm, Andreas (1996) / Schumm, Andreas; Wirtschaftlichkeitsanalysen von PC-Infrastrukturen als Aufgabe des IS-Controlling; Frankfurt am Main, Berlin 1996.

Schwab , Adolf J.; Kürner, Wolfgang (2007) / Schwab , Adolf J.; Kürner, Wolfgang; Elektromagnetische Verträglichkeit: Aktualisierte und Ergänzte Auflage; Springer 2007.

Schwenk, Jörg (2005) / Schwenk, Jörg; Sicherheit und Krytographie im Internet, Von sicherer E-Mail bis zu IP-Verschlüsselung; 2. erweiterte und verbesserte Auflage 2005.

Shapiro, F. R. (2000) / Shapiro, F. R.; Origin of the term software: Evidence from the JSTOR electronic journal archive. IEEE Annals of the History of Computing 22 (April-June 2000).

Shneiderman, B. (1987) / Shneiderman, B.; User Interface Design (Deutsche Ausgabe). IBM System Application Architecture: Common User Acces, Panel Design and User Interaction, IBM Document SC26-4351-o, Boca Raton, FL Dezember 1987.

Shneiderman, B. (1992) / Shneiderman, B.; Designing the User Interface, Addison-Wesley, Reading, Ma., 1992, 2nd Edition.

Siebertz, Jens (2004) / Siebertz, Jens; IT-Kostencontrolling, Nutzenpotenziale von Controlling-Tools, VDM Verlag Dr. Müller 2004.

Smith, S. L. in Helander, M. (Ed.) (1997); / Smith, S. L.; Standards versus guidelines for designing user interface software. In Helander, M. (Ed.); Handbook of human-computer interaction, Amsterdam: North-Holland Publishing Com-pany 1997.

Sommerville, I. (2001) / Sommerville, I.; Software Engineering, 6. Auflage, Pearson Studium 2001.

Sonnenreich, W.; Albanese, J.; Stout, B., (2006) / Sonnenreich, W.; Albanese, J.; Stout, B.; Return on Security Investment (ROSI) - A Practical Quantitative Model. In Journal of Research and Practice in Information Technology; Vol. 38 No.1 February 2006.

Speichert, Horst (2007) / Speichert, Horst; Praxis des IT-Rechts, Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung; Vieweg-Verlag, 2., Auflage 2007.

Sprague, Ralph H. Jr.; Watson, Hugh J (1995) / Sprague, Ralph H. Jr.; Watson, Hugh J.; Decision Support for Management. Prentice Hall, 1995.

Staehle, Wolfgang (1989) / Staehle, Wolfgang; Management, Eine verhaltenswissenschaftliche Perspektive; 4. neu bearbeitete und erweiterte Auflage München 1989.

Stahlknecht, Peter; Hasenkamp, Ulrich (2004) / Stahlknecht, Peter; Hasenkamp, Ulrich; Einführung in die Wirtschaftsinformatik; 11., vollständig überarbeitete Auflage, Berlin, Heidelberg 2004.

Stahlknecht, Peter; Hasenkamp, Ulrich, (1999) / Stahlknecht, Peter; Hasenkamp, Ulrich; Einführung in die Wirtschaftsinformatik; 9. vollst. Überarbeitete Auflage 1999, Berlin, Heidelberg, New York.

Stapelkamp, Torsten (2007) / Stapelkamp, Torsten; Screen- und Interfacedesign, Gestaltung und Usability für Hard- und Software, Springer-Verlag, Berlin, Heidelberg 2007.

Staudt, Erich (1985) / Staudt, Erich; Kennzahlen und Kennzahlensysteme; Grundlagen zur Entwicklung und Anwendung E. Schmidt 1985.

Stickel, Eberhard (2001) / Stickel, Eberhard; Informationsmanagement; München, Wien 2001.

Strobel, Stefan (1999) / Strobel, Stefan; Firewalls, Einführung, Praxis, Produkte; dpunkt.verlag 2 aktualisierte und erweiterte Auflage 1999.

Struckmeier, H. (1997) / Struckmeier, H.; Führungsinformationssysteme: betriebswirtschaftliche Konzeption und Softwareanforderungen; Gabler 1997.

Struckmeier, H. (1997a) / Struckmeier, H.; Gestaltung von Führungsinformationssystemen: betriebswirtschaftliche Konzeption und Softwareanforderungen, Gabler 1997.

Szyperski, Norbert; Windand, Udo (1974) / Szyperski, Norbert; Windand, Udo; Entscheidungstheorie. Eine Einführung unter besonderer Berücksichtigung spieltheoretischer Konzepte Stuttgart 1974.

Thome, Rainer (2006) / Thome, Rainer; Grundzüge der Wirtschaftsinformatik; Integration der Informationsverarbeitung in die Organisation von Unternehmen; Pearson-Studium 2006.

Thommen, Jean-Paul; Achleitner, Ann-Kristin (2003) / Thommen, Jean-Paul; Achleitner, Ann-Kristin; Allgemeine Betriebswirtschaftslehre. Wiesbaden, 4. Auflage 2003.

Tiemeyer, Ernst (2005) / Tiemeyer, Ernst; IT-Controlling kompakt; 1. Auflage Spektrum-Verlag München 2005.

Tinnefeld, Marie-Theres; Gerling, Rainer, W. (2005) / Tinnefeld, Marie-Theres; Ehmann, Eugen; Gerling, Rainer, W.; Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht, 4., völlig neu bearbeitete und erweiterte Auflage, Oldenbourg Verlag München Wien 2005.

Töllner, Andrea (1995) / Töllner, Andrea 1995.

United States Code (1998), 18, U.S.C. §2028 / United States Code (1998), 18, U.S.C. §2028.

Vetschera, Rudolf (1996) / Vetschera, Rudolf; Informationssysteme der Unternehmensführung; Springer 1996.

Von Graevenitz, Gerik, Alexander (2006) / Von Graevenitz, Gerik, Alexander; Erfolgskriterien und absatzchancen biometrischer Identifikationsverfahren, 1.st ed. Ser. Management Wissen aktuell G.-M. Hellstern, Ed. Berlin: Lit Verlag 2006.

Voß, Stefan; Gutenschwager, Kai (2001) / Voß, Stefan; Gutenschwager, Kai; Informationsmanagement, Berlin, Heidelberg 2001.

Wack, Jessica (2007) / Wack, Jessica; Risikomanagment für IT-Projekte; Deutscher Universitätsverlag Dissertation Universität Hamburg 2006 1. Auflage 2007.

Waldemar, Wittmann (1959) / Waldemar, Wittmann; Unternehmung und unvollkommene Information: Unternehmerische Voraussicht - Ungewissheit und Planung; Westdeutscher Verlag, 1959.

Wall, F. (1996) / Wall, F.; Organisation und betriebliche Informationssysteme: Elemente einer Konstruktionstheorie; Gabler 1996.

Wall, Friederike (2001) / Wall, Friederike; Jahnke, Bernd; IT-gestützte betriebswirtschaftliche Entscheidungsprozesse; Gabler 1. Auflage 2001.

Walpoth, G. (1993) / Walpoth, G.; Computergestützte Informationsbedarfsanalyse: strategische Planung und Durchführung von Informationsprojekten; Physica-Verlag 1993.

Wandmacher, J. (1993) / Wandmacher, J.; Softwareergonomie; de Gruyter 1993.

Weber, J.; Grothe, M.; Schäffer, U. (1999) / Weber, J.; Grothe, M.; Schäffer, U.;Business Intelligence; Advanced Controlling, Schriftreihe der WHU Koblenz, Lehrstuhl Controlling & Logistik, Band 13, Vallendar 1999.

Weck, Gerhard; Horster, Patrick (Hrsg.) (1993) / Weck, Gerhard; Horster, Patrick (Hrsg.); Verläßliche Informationssysteme, Proceedings der GI-Fachtagung VIS´93, Friedrich Vieweg & Sohn Braunschweig/Wiesbaden 1993.

Weill, P.; Woodham, R. (2002) / Weill, P.; Woodham, R.; Don't just lead, govern: Implementing Effective 2002.

Werners, B.; Klempt, P. (2005) / Werners, B.; Klempt, P.; Standards und Kriterienwerke zur Zertifizierung von IT-Sicherheit; Arbeitsbericht Nr. 9; Ruhr-Universität Bochum 2005.

Wieczorrek, Hans, W.; Mertens, Peter (2007) / Wieczorrek, Hans, W.; Mertens, Peter; Management von IT-Projekten, Von der Planung zur Realisierung; Springer-Verlag Heidelberg, 2. überarbeitete und erweiterte Auflage 2007.

Wild, Jürgen (1994) / Wild, Jürgen; Unternehmensführung, in: Festschrift für Kosiol, Erich zu seinem 75. Geburtstag, Berlin, Duncker & Humblot 1974 zitiert in Krüger; Organisation der Unternehmung, Kohlhammer-Lehrbuchreihe Betriebswirtschaft, Stuttgart: Kohlhammer, 3. verb. Auflage. 1994.

Wilding, Edward (2006) / Wilding, Edward; Information Risk and Security; Preventing and Investigating Workplace Computer Crime; Gower Publishing Company 2006.

Windemann, P.; Schlienger,T.; Teufel, S. (2006) / Windemann, P.; Schlienger,T.; Teufel, S.; Messung der Informationssicherheit auf der Ebene der Sicherheitspolitik. In HMD, Heft 248; April 2006.

Wissensbach, Heinz (1967) / Wissenbach, Heinz; Betriebliche Kennzahlen und ihre Bedeutung im Rahmen der Unternehmensentscheidung. Bildung , Auswertung und Verwendungsmöglichkeiten von Betriebskennzahlen in der unternehmerischen Praxis; Berlin 1967.

Witt, Bernhard C. (2008) / Witt, Bernhard C.; Datenschutz kompakt und verständlich; Eine praxisorientierte Einführung; 1. Auflage vieweg Wiesbaden 2008.

Witt, Bernhard C. (2006) / Witt, Bernhard C.; IT-Sicherheit kompakt und verständlich. Eine praxisorientierte Einführung, 1. Auflage vieweg Wiesbaden 2006.

Witte, Eberhard (1980) / Witte, Eberhard; Entscheidungsprozesse, in Handwörterbuch der Organisation; hrsg. Von Grochla, Erwin unter Mitarbeit von zahlreichen Fachgelehrten und Experten aus Wissenschaft und Praxis, 2. völlig neu gestaltete Auflage Stuttgart 1980, Sp. 894-904.

Wittmann, Waldemar (1980) / Wittmann, Waldemar; Inormation, in Handwörterbuch der Organisation, hrsg. Von Grochla, Erwin unter Mitarbeit von zahlreichen Fachgelehrten und Experten aus Wissenschaft und Praxis; 2. völlig neu gestaltete Auflage, Stuttgart 1980, Sp. 894-904.

Wodtke, Carolina; Richters, Swantje (2004) / Wodtke, Carolina; Richters, Swantje; Schutz von Betriebs- und Geschäftsgeheimnissen, Leitfaden für die Praxis; Erich Schmidt Verlag Berlin 2004.

Wöhe, Günter; Döring, Ulrich (2005) / Wöhe, Günter; Döring, Ulrich; Einführung in die Allgemeine Betriebswirtschaftslehre; 22. Aufl., Wiesbaden 2005.

Wolfram, Gerd (1986/2005) / Wolfram, Gerd; Bürokommunikation und Informationssicherheit: Die Gestaltung eines Informationssicherheitssystems als Herausforderung für die Unternehmung in der Bürokommunikation, Braunschweig 1986/2006.

Zhang, Helander (1996) / Zhang, Helander; Drury; Clusteranalyse der Begrifflichkeiten von 1996.

Zhang, L.; Helander, M.G.; Drury, C.G.(1996) / Zhang, L.; Helander, M.G.; Drury, C.G.; Identifying factors of comfort and discomfort in sitting, Human Factors, 38 (3), 1996, Seite 377-389.

Ziegler, J.; Ilg, R. (1991) / Ziegler, J.; Ilg, R.; Techniken der direkten Manipulation für die Benutzerschnittstellengestaltung In: HMD (1991).

Zipfel, Martin (2007) / Zipfel, Martin; Sicherheit von Systemen- Ausfallsicherheit, redundante Systeme, Notfallmaßnahmen, Technik, Kosten; GRIN Verlag, 2007.

12. Internetquellen

Achtg; http://www.achtg.de / Achtg;
http://www.achtg.de/dialog/glossar.html; Erstelldatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Ad/c´t; http://www.heise.de /
Ad/c´t; http://www.heise.de/newsticker/meldung/50479;
Erstelldatum [29.08.2004]; Verfügbarkeitsdatum [22.09.2008].

Alex; http://home.alexweb.net/glossary.htm /
Alex; http://home.alexweb.net/glossary.htm;
Erstelldatum [unbekannt]; Verfügbarkeitsdatum [22.01.2007].

Amberg (2004); http://www.wi3.uni-erlangen.de / Amberg
http://www.wi3.uni-erlangen.de/lehre/lv/ws2002/BE/BE-ws02-11.ppt. Erstellungsdatum [2004], Verfügbarkeitsdatum [22.09.2008].

At-mix; http://www.at-mix.de / At-mix;
http://www.at-mix.de/vulnerability_scanner.htm;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Barrett, Neil; http://www.it-im-unternehmen.de / Barrett, Neil; Uralte Hackertricks noch immer eine Gefahr, in: IT im Unternehmen
[http://www.it-im-unternehmen.de/strategie/article2006070014.aspx],
Erstellungsdatum [7/2006]; Verfügbarkeitsdatum [16.08.2006].

Briele, Marc (2004); http://idw-online.de / Briele, Marc;
http://idw-online.de/public/zeige_einrichtung.html
Erstellungsdatum [25.03.2004]; Verfügbarkeitsdatum [30.03.2004].

BSI (a); http://www.bsi.bund.de / BSI http://www.bsi.bund.de/gshb/deutsch/m/m02011.html; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

BSI; http://www.bsi.bund.de / BSI http://www.bsi.bund.de/zertifiz/itkrit/itkrit.htm; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

BSI; http://www.bsi.de / BSI http://www.bsi.de/literat/faltbl/012_blab.htm; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [01.09.2007].

Buder, M. (Hrsg.); http://server02.is.uni-sb.de / Buder, M. (Hrsg.); Grundlagen der praktischen Information und Dokumentation. München et al.: K.G. Saur, S. 795-821, http://server02.is.uni-sb.de/trex/index.php?id=1.8.2. Erstellungsdatum [2003], Verfügbarkeitsdatum [01.01.2005]

Capital; http://www.capital-select.de / Capital; http://www.capital-select.de/capital/glossar/u; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Däßler, R. (1999); http://fabdp.fh-potsdam.de / Däßler, R.; Informationsvisualisierung, Stand, Kritik und Perspektiven, Projektgruppe Info Viz, FH Potsdam; http://fabdp.fh-potsdam.de/daessler/pdf/bericht99.pdf; Erstellungsdatum [10.05.2000]; Verfügbarkeitsdatum [22.09.2008].

Datenschutz-Berlin (1999); http://www.datenschutz-berlin.de / Datenschutz-Berlin; http://www.datenschutz-berlin.de/jahresbe/98/teil3-5.htm; Erstellungsdatum [22.11.99]; Verfügbarkeitsdatum [05.05.05].

Dialerschutz; http://www.dialerschutz.de / Dialerschutz; http://www.dialerschutz.de/grundlagen-was-sind-dialer.php; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Eskimo; http://www.eskimo.com / Eskimo http://www.eskimo.com/~joelm/tempestintro.html; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

FH-Heilbronn; http://sicherheit.i3g.fh-heilbronn.de / FH-Heilbronn ; http://sicherheit.i3g.fh-heilbronn.de/dv_glossar.html; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.01.2007].

Forthmann, Jörg (2005); http://www.presseportal.de / Forthmann Jörg; IT-Sicherheit: Unternehmen beachten ROSI zu wenig;
http://www.presseportal.de;
Erstellungsdatum [15.02.2005]; Verfügbarkeitsdatum [16.02.2005].

Fox, Dirk (2002); http://www.secorvo.de / Fox, Dirk; Kelm Stefan; Knobloch, Hans Joachim; Michels, Markus; Petersen, Holger; „Empfehlung geeignete Kryptoalgorithmen“ gemäß §17 (1) SigG
http://www.secorvo.de/publikationen/stellungnahme-algorithmen empfehlung-021024.pdf;
Erstellungsdatum [24.10.2002]; Verfügbarkeitsdatum [22.09.2008].

Fox, Dirk (2005); http://www.secorvo.de / Fox, Dirk; Security Awareness Oder: Die Wiederentdeckung des Menschen in der IT-Sicherheit;
http://www.secorvo.de/publikationen/security-awareness-fox-2003.pdf;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [12.10.2007] in DUD Datenschutz und Datensicherheit 27 (2003).

Freiling, Felix (2006); http://pi1.informatik.uni-mannheim.de / Freiling, Felix, Angewandte IT-Sicherheit,
http://pi1.informatik.uni-mannheim.de/filepool/teaching/sicherheit-2006/ITS_20061128.pdf;
Erstellungsdatum [Herbst 2006]; Verfügbarkeitsdatum [22.09.2008].

Geis, Thomas (2005); http://www.fit-fuer-usability.de / Geis, Thomas; Usability von der Stange? Von Normen und Standards,
http://www.fit-fuer-usability.de/1x1/standards/stange.html;
Erstellungsdatum [18.03.2005]; Verfügbarkeitsdatum [04.01.2007].

Go-cert; http://www.go-cert.de / Go-cert; http://www.go-cert.de/htm/glossar.htm;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Google; http://www.google.de / Google;
http://www.google.de/search?hl=de&lr=lang_de&oi=defmore&q=define:Sniffer; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Pixelpark / Pixelpark;
http://www.wildpark.com/konserve/netzzeug/abhoer/c_abhoer_nz.html;
Erstellungsdatum [1996]; Verfügbarkeitsdatum [22.09.2008].

Handelsblatt (2005); http://www.handelsblatt.com / Handelsblatt
http://www.handelsblatt.com: Rechtliche Aspekte werden bei IT-Sicherheit oft vernachlässigt.
Erstellungsdatum [18.02.05]; Verfügbarkeitsdatum [21.02.05].

Heise Online (2006); http:// www.heise.de / Heise Online: Citibank Singapur führt biometrisches Bezahlsystem ein;
http:// www.heise.de/newsticker/meldung/81378;
Erstellungsdatum [21.11.2006]; Verfügbarkeitsdatum [22.09.2008].

Heise; http://www.heise.de in c't 6/97, S. 330 / Heise
http://www.heise.de/security/dienste/pgp/stego.shtml; Überblick in Jürgen Rinks Artikel "Hinters Licht geführt" in c't 6/97, Seite 330.“

Hoofnagle, Chris Jay (2007), Hoofnagle, Chris Jay (2007): Harvard Journal of Law & Technology; Volume 21, Number 1 Fall 2007; IDENTITY THEFT: MAKING THE KNOWN UNKNOWNS KNOWN;
http://ssrn.com/abstract=969441;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [18.04.2009].

IBI Tu-Berlin; http://www.ibi.tu-berlin.de/moses/glossar/glossarmain.htm / IBI Tu-Berlin; http://www.ibi.tu-berlin.de/moses/glossar/glossarmain.htm;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2007].

Informationsarchiv; http://www.informationsarchiv.net / Informationsarchiv; http://www.informationsarchiv.net/clexid_700.shtml;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Insurance; http://www.infosurance.ch / Insurance;
http://www.infosurance.ch/de/glossar_p_t.htm;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.01.2006].

ISO-14971; http://www.iso-14971.de / ISO-14971; http://www.iso-14971.de/risikomanagementprozess-definitionen.htm;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

ISS; http://www.iss.net / ISS; http://www.iss.net;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [10.09.2006].

Itseccity (2007); http://www.itseccity.de / http://www.itseccity.de/
Erstellungsdatum [22.10.07], Verfügbarkeitsdatum [22.10.07]

ITSecurity / IT-Security; http://www.itsecurity.com/ss.htm;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.06.2006].

IT-Security (2004); IT-Security; http://silicon.de in Witt, Bernhard, C. 2006 / http://silicon.de Studie aus IT-Security 2004 in Witt, Bernhard, C.; IT-Sicherheit kompakt und verständlich; Eine praxisorientierte Einführung; Vieweg, 1. Auflage 2006.

Jahnke, Bernd (2008); Enzyklopaedie der Wirtschaftsinformatik Online Lexikon; http://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/technologien-methoden/Informatik--Grundlagen/Kryptographie/index.html] Erstellungsdatum [2008]; Verfügbarkeitsdatum [22.09.2009].

Jlussi, Dennis (2007); http://www.jlussi.eu / Jlussi, Dennis; IT-Sicherheit und §202c StGB;
http://www.jlussi.eu/wp-content/uploads/2007/10/jlussi_leitfaden_web.pdf;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Kästner, Sven (2005) in Spiegel Online; http://www.spiegel.de / Kästner, Sven (2005) Polizeidaten bei Ebay, Geheimes Schnäppchen, in Spiegel Online; http://www.spiegel.de/netzwelt/web/0,1518,349435,00.html;
Erstellungsdatum [02.04.2005]; Verfügbarkeitsdatum [22.09.2008].

Kluck, M. (2003); http://server02.is.uni-sb.de / Kluck, M.; Terminosaurus-Rex: Die Informationswissenschaft in Begriffen, Informationsbedarfsanalyse, Methoden der Informationsanalyse in Buder, M. (Hrsg.); Grundlagen der praktischen Information und Dokumentation. München et al.: K.G. Saur., http://server02.is.uni-sb.de/trex/index.php?id=1.8.2.;
Erstellungsdatum [2003]; Verfügbarkeitsdatum [22.09.2005].

Kommission der Europ. Gemeinschaften; http://spam.trash.net / Kommission der Europ. Gemeinschaften; http://spam.trash.net/was.shtml;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Konetzny, Michael; http://www.mkonetzny.de / Konetzny, Michael; http://www.mkonetzny.de/aufsatz/olap.htm; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Kühner, Klaus; Völkner, Jörg (2006); http://www.secorvo.de / Kühner, Klaus; Völkner, Jörg; Aufbau eines zertifizierten Information Security Management Systems, Secorvo White Paper, Case Study Aufbau und Zertifizierung eines ISMS nach BS7799-2:2002/ISO 27001, http://www.secorvo.de/whitepapers/secorvo-wp13.pdf; Erstellungsdatum [24.09.2006]; Verfügbarkeitsdatum [22.09.2008].

Landesamt für Verfassungsschutz Baden-Württemberg (2006); http://www.Verfassungsschutz.bayern.de / Landesamt für Verfassungsschutz Baden-Württemberg; Bayrisches Landesamt für Verfassungsschutz; Wirtschaftsspionage in Baden-Württemberg und Bayern, Daten – Fakten – Hintergründe, http://www. Verfassungs-schutz.bayern.de/imperia/md/content/lfv_internet/service/wirtschaftsspionage_bay_bw_2006.pdf; Erstellungsdatum [2006]; Verfügbarkeitsdatum [16.08.2007].

Luckhardt, Norbert (2006); http://www.it-sa.de / Luckhardt, Norbert; Die <kes>/Microsoft-Sicherheitsstudie 2006; http://www.it-sa.de/fileadmin/itsa_files/Handouts/2006/RO_Mo_12_00_Luckhardt.pdf?PHPSESSID=9; Erstellungsdatum [2006]; Verfügbarkeitsdatum [22.09.2008].

Lusk, Bill (2007); http://media.www.marshallparthenon.com / Lusk, Bill; Precautions may prevent laptop theft, in The Parthenon Online, http://media.www.marshallparthenon.com/media/storage/paper534/news/2007/04/25/News/Precautions.May.Prevent.Laptop.Theft-2879374.shtml; Erstellungsdatum [25.04.2007]; Verfügbarkeitsdatum [22.09.2008].

McAfee Inc (2007); http://www.mcafee.com / McAfee Inc; Sicherheitsrisiko Mitarbeiter. Beschäftigte europäische Unternehmen öffnen dem Missbrauch von Geschäftsdaten Tür und Tor, http://www.mcafee.com/de/about/press/corporate/2007/20070208_172724_m.html; Erstellungsdatum [2007]; Verfügbarkeitsdatum [22.09.2008].

Meyer (2003); http://www.net-lexikon.de / Meyer: Trojanisches Pferd http://www.net-lexikon.de/Trojanisches-Pferd.html;
Erstellungsdatum [10.10.2003]; Verfügbarkeitsdatum [22.09.2008].

Mummert Consulting (2005);http://www.presseportal.de / Mummert Consulting: Studie IT-Security 2004 der Firma Mummert Consulting zitiert in Forthmann Jörg www.presseportal.de IT-Sicherheit: Unternehmen beachten ROSI zu wenig.
Erstellungsdatum [15.02.2005]; Verfügbarkeitsdatum [16.02.2005].

Nadir; http://www.nadir.org / Nadir;
http://www.nadir.org/nadir/archiv/Repression/abhoerratgeber/node9.html;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Nessus; http://www.nessus.org / Nessus; http://www.nessus.org;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Pendse, Nigel; Chreeth, Richard; (1995); http://www.busintel.com / Pendse, Nigel; Chreeth, Richard; Synopsis of the OLAP Report;
http://www.busintel.com/,
Erstellungsdatum [1995]; Verfügbarkeitsdatum [22.09.2008].

Pfitzmann, Andreas (2007); http://dud.inf.tu-dresden.de / Pfitzmann, Andreas; An Introduction to Digital Identity; http://dud.inf.tu-dresden.de/literatur/Trondheim20070508_OECDf.pdf;
Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Pfitzmann, Andreas (a); http://dud.inf.tu-dresden.de / Pfitzmann, Andreas; Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft; http://dud.inf.tu-dresden.de/literatur/MoegGrenzderNutzuebIuK-Sys-V1-0.pdf;
Erstellungsdatum [26.09.2007]; Verfügbarkeitsdatum [22.09.2008].

Pfitzmann, Andreas; http://dud.inf.tu-dresden.de / Pfitzmann, Andreas; Biometrie – wie einsetzen und wie keinesfalls? Wie umgehen mit Sicherheitsproblemen von Biometrie und Sicherheits- und Datenschutzproblemen durch Biometrie?;

http://dud.inf.tu-dresden.de/literatur/Duesseldorf2005.10.27Biometrie.pdf; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

PriceWaterhouseCoopers (2005); http://www.pwc.de / PriceWaterhouse-Coopers; Wirtschaftskriminalität. Der Täter stammt meist aus den eigenen Reihen; http://www.pwc.de/portal/pub/!ut/p/kcxml/; Erstellungsdatum [2005]; Verfügbarkeitsdatum [22.09.2008].

Quality (2005); http://www.quality.de / Quality; http://www.quality.de/lexikon/total_cost_of_ownership.htm; Erstellungsdatum [8.05.2005]; Erstellungsdatum [unbekannt];

Sager, Michael (2005); http://www.wwsinternational.net / Sager, Michael; IDC White Paper. Ruggedised PCs in Today´s Mobile Computing World, Sydney, http://www.wwsinternational.net/pdfs/toughBook/IDC%20Panasonic%20Whitepaper%20Ruggedised%20PCs.pdf; Erstellungsdatum [2005]; Verfügbarkeitsdatum [22.09.2008].

Salvenmoser, Steffen; Kruse, Lars Heiko (2005); http://www.pwc.de / Salvenmoser, Steffen; Kruse, Lars Heiko; Wirtschaftskriminalität als Unternehmensrisiko, http://www.pwc.de/fileserver/RepositoryItem?itemID=82750; Erstellungsdatum [2005]; Verfügbarkeitsdatum [16.08.2007].

Schwickert (2000); http://wi.uni-giessen.de / Schwickert; http://wi.uni-giessen.de/gi/dl/det/Schwickert/1161/; Erstellungsdatum [2000]; Verfügbarkeitsdatum [22.03.2005].

Sendung Forschung aktuell am 31.01.2005 auf dem Sender Deutschland-funk; http://www.dradio.de / Sendung Forschung aktuell am 31.01.2005 auf dem Sender Deutschlandfunk; http://www.dradio.de/dlf/sendungen/forschak/344093/ Erstellungsdatum [31.01.2005]; Verfügbarkeitsdatum [01.02.05].

Silicon (2004); http://www01.silicon.de / Silicon; http://www01.silicon.de/cpo/itsecurity-news/detail.php?nr=10950&directory=itsecurity-news; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Spam; http://www.spam.com / Spam; http://www.spam.com/ci/ci_in.htm; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [10.04.2003].

Spiegel Online (2005);http:/www.spiegel.de / Spiegel Online, http:/www.spiegel.de/netzwelt/web/0,1518,349435,00.html; Erstellungsdatum [02.04.2005]; Verfügbarkeitsdatum [22.09.2008].

TerminosaurusRex (1993); http://server02.is.uni-sb.de / TerminosaurusRex; Die Informationswissenschaft in Begriffen, Informationsbedarf, http://server02.is.uni-sb.de/trex/index.php?id=1.8.2.5.; Erstellungsdatum [1993], Verfügbarkeitsdatum [22.09.2008].

Tools; http://tools.ba-ca.com / Tools; http://tools.ba-ca.com/l_de/glossar.html; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [13.07.2004].

TSS; http://tss.lcps.k12.nm.us / TSS; http://tss.lcps.k12.nm.us/CyberCrime%20Glossary.html; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Tu-Dresden; http://www.inf.tu-dresden.de / http://www.inf.tu-dresden.de/index.php?node_id=1013&ln=de ; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008]

Uni Mannheim; http://ncc.uni-mannheim.de / Uni Mannheim; http://ncc.uni-mannheim.de/bsi-webkurs/gsschul/gskurs/seiten/glossar/gloss_pz.htm; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [27.05.2005].

Van Eck, Wim; http://jya.com / Van Eck, Wim; Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? http://jya.com/emr.pdf; Erstellungsdatum [unbekannt]; Verfügbarkeitsdatum [22.09.2008].

Völkner, Jörg (2005); http://www.secorvo.de / Völkner, Jörg; BS 7799, Von Best Practice zum Standard, Secorvo White Paper, Informationssicherheits-Management nach BS 7799, im Überblick, http://www.secorvo.de/whitepapers/secorvo-wp10.pdf; Erstellungsdatum [27.09.2005]; Verfügbarkeitsdatum [22.09.2008].

Wijvertrouwenstemcomputersniet (2007); http://wijvertrouwenstemcomputersniet.nl/Deutsch Erstellungsdatum [05.03.2007]; Verfügbarkeitsdatum [04.06.2009]

Winkels, Heinz-Michael (2004); http://www1.logistik.fh-dortmund.de / Winkels, Heinz-Michael; Wirtschaftsspionage. Wie deutsche Unternehmen von ausländischen Geheimdiensten ausgeplündert und ruiniert werden; http://www1.logistik.fh-dortmund.de/IT-Sicherheit/ 07_Wirtschaftsspionage.pdf;
Erstellungsdatum [2004]; Verfügbarkeitsdatum [16.08.2007].

Wößner, Elke (2007); http://www.infowatch.com / Wößner, Elke; Sicherheit mobiler Geräte 2007;
http://www.infowatch.com/de/threats?chapter=162971949&id38;
Erstellungsdatum [2007];Verfügbarkeitsdatum [16.08.2007].

Zeit Online: (2008) „Schäubles Zeigefinger gehackt“ vom 30. März 2008 http://www.zeit.de/online/2008/14/fingerabdruck-schaeuble-ccc;
Erstellungsdatum [30.03.2008];Verfügbarkeitsdatum [04.06.2009].

Ziemann, Frank (2007); http://www.pcwelt.de / Ziemann, Frank;
http://www.pcwelt.de/start/sicherheit/sicherheitsluecken/news/84086/index.html;
Erstellungsdatum [14.06.2007]; Verfügbarkeitsdatum [22.09.2008].