GovCERT AUSTRIA

CERT.at

BERICHT
INTERNET-SICHERHEIT
ÖSTERREICH 2014

GESAMTAUSGABE

Wien, am 15. Jänner 2015

1. INHALTSVERZEICHNIS

Impressum:

Medieninhaber und Verleger: nic.at GmbH, Computer Emergency Response Team Austria, Karlsplatz 1/3, 1010 Wien. Diese Publikation wurde in Kooperation mit dem Bundeskanzleramt erstellt. **Projektleitung**: Mag. Robert Schischka, CERT.at und Ing. Roland Ledinger, BKA. **Konzeption und Redaktion**: pantarhei corporate advisors (Mag. Markus Gruber, Mag. Stefanie Bramböck, Mag. Julija Palatin), **Herstellungsort**: Wien. Jänner 2015.

2. ABBILDUNGSVERZEICHNIS

3. VORWORT STAATSEKRETÄRIN MAG. SONJA STEßL

Die stetige Vernetzung und Digitalisierung unserer Gesellschaft ließ das Internet zu einer kritischen Infrastruktur in allen Wirtschafts- und Lebensbereichen werden. Experten sind sich einig, dass die Bedeutung von Internet-Sicherheit steigen wird, da eine vernetzte Welt auf das verlässliche Funktionieren von Informations- und Kommunikationstechnologie (IKT) angewiesen ist. IKT sorgt als Wachstumsmotor maßgeblich für Wohlstand, Innovation und Sicherung des Wirtschaftsstandortes, sowohl international als auch in Österreich. Es ist daher erforderlich, die optimalen Rahmenbedingungen für Internet-Sicherheit und den Einsatz neuester Technologien zu schaffen.

Die erweiterten Chancen und Möglichkeiten, die durch die Professionalisierung der Informations- und Kommunikationstechnologie ermöglicht werden, öffnen jedoch auch immer wieder neue Tore für Angreifer aus dem Netz. Der vorliegende CERT-Bericht fasst unter anderem die wichtigsten Cyber Security Themen sowie Zahlen und Fakten des letzten Jahres zusammen. Es zeigt sich dabei, dass die Angriffe zahlreicher und vor allem komplexer geworden sind.

Die Herausforderung im Bereich Internet-Sicherheit besteht darin, Risiken möglichst früh zu antizipieren, um in Folge rasch und effektiv reagieren zu können. Cyber Security Übungen, wie die heuer stattgefundene nationale Übung „CE.AT 2014" im Rahmen der EU-Initiative „Cyber Europe 2014" sind daher wichtig und notwendig, um sowohl den öffentlichen als auch privaten Sektor für diese Risiken zu sensibilisieren und zu trainieren.

Die Bundesregierung übernimmt gemeinsam mit den Expertinnen und Experten von GovCERT Austria und CERT.at die Verantwortung für die Behandlung aber vor allem für die Verhinderung von Sicherheitsvorfällen im Bereich IKT. Österreich setzt seit Jahren zahlreiche Aktivitäten zur Erhöhung des Sicherheitsbewusstseins und ist internationales Vorbild im Bereich E-Government. Dennoch muss auch in Zukunft die Gewährleistung von IKT-Sicherheit eine zentrale und gemeinsame Aufgabe von Staat, Wirtschaft und Gesellschaft sein. Der Umgang und das Bewusstsein für IKT und unsere Daten müssen auch in Zukunft thematisiert werden, damit wir weiterhin in der Lage sind, die richtigen Maßnahmen für Sicherheit im Internet zu setzen.

Mag. Sonja Steßl
Staatssekretärin für Verwaltung und Öffentlichen Dienst im Bundeskanzleramt

4. VORWORT ROLAND LEDINGER UND ROBERT SCHISCHKA

Digitale Angreifer hatten im vergangenen Jahr erneut Hochsaison. Kaum ein Tag verging, an dem nicht über Cyber Angriffe auf Unternehmen, Staaten und Organisationen oder neue Bedrohungsformen aus dem Internet berichtet wurde. Da die digitale Schattenwirtschaft bei ihren globalen Aktivitäten auf Landesgrenzen keine Rücksicht nimmt, ist auch Österreich vermehrt in den Mittelpunkt von Angriffen gerückt – zahlreiche Vorfälle der jüngsten Zeit bringen dies deutlich zum Ausdruck.

Mit dem Internet-Sicherheitsbericht 2014 blicken die Experten von CERT.at und GovCERT Austria auf die relevantesten Themen und Vorfälle der österreichischen IT-Sicherheitslandschaft zurück und zeigen auf, was getan wurde, um den österreichischen Teil des Internets sicherer zu machen. Neben ständiger Beobachtung der IT-Sicherheitslage und dem Ergreifen von Sofortmaßnahmen setzen CERT.at und GovCERT Austria dabei vor allem auf verstärkte Vernetzung, Zusammenarbeit und Prävention. Durch die ständige Intensivierung der Kooperation und den regelmäßigen Austausch mit anderen CERTs in Europa sowie mit Betreibern kritischer Infrastrukturen – öffentlich wie auch privat – gelang es, das Thema Cyber Sicherheit noch stärker im Bewusstsein zu verankern.

Den zentralen Handlungsrahmen für alle von CERT.at und GovCERT Austria gesetzten Aktivitäten bildet dabei die Österreichische Strategie für Cyber Sicherheit (ÖSCS). Damit ist es Österreich gelungen, allen voran aufgrund der breiten Einbindung von öffentlicher Hand, Privatwirtschaft und weiteren system-relevanten Playern, ein internationales Best-practise Beispiel im Umgang mit Cyber Sicherheitsbedrohungen zu etablieren. Damit ist Österreich bestmöglich auf aktuelle und künftige Cyber Angriffe vorbereitet und räumt dem Thema Cyber Sicherheit auch auf politischer, wirtschaftlicher und gesellschaftlicher Ebene höchste Priorität ein. Denn der Cyber Raum eröffnet eine Vielzahl von Chancen und Möglichkeiten. Um die Vorteile, die unsere globalisierte Welt verspricht, nutzen zu können, muss die digitale Infrastruktur verlässlich und sicher funktionieren. Daher ist die Gewährleistung von Cyber Sicherheit eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft. Nicht nur im vergangenen Jahr 2014, sondern auch darüber hinaus.


© HBF

Roland Ledinger
Leiter des Bereichs IKT-Strategie des Bundes im Bundeskanzleramt


© CERT.at

Robert Schischka
Leiter des Computer Emergency Response Teams (CERT.at)

5. Der Mythos vollständiger Online-Sicherheit

Attacken aus dem Netz, unterschiedliche Schadsoftware und Schwachstellen wie Heartbleed haben 2014 weltweit Schäden in der Höhe von mehreren Hundert Milliarden US-Dollar verursacht – und daher auch das mediale Bild geprägt. Welchen Gehalt diese Begriffe haben und wie es um die Sicherheit im Netz tatsächlich steht, erörtern die Experten von CERT.at und GovCERT Austria im Rahmen des aktuellen Internet-Sicherheitsberichts 2014.

Die Folgen der Snowden-Enthüllungen

Im Sommer 2013 wurde die Welt durch brisante Enthüllungen über die Vorgangsweise der westlichen Geheimdienste erschüttert. Edward Snowden, der Aufdecker der NSA-Spionage- und Überwachungsaffäre hat damit einen Sturm an weltweiter Entrüstung in Gang gesetzt. Auch 2014 war die NSA-Affäre allgegenwärtig und noch immer kommen neue Enthüllungen über die weit verzweigten Spionage- und Überwachungstätigkeiten ans Licht. Snowden hat maßgeblich dazu beigetragen, dass den Themen Privacy, Verschlüsselung, Datenschutz und Internet-Sicherheit eine weltweit noch nie dagewesene Aufmerksamkeit wiederfährt – wenngleich das Internet dadurch noch nicht per se zu einem sichereren Ort geworden ist.

Die Ursache für diese Entwicklung liegt auf der Hand: Der technologische Fortschritt nimmt stetig zu und mit ihm auch die Möglichkeit, sich mittels verbotener Handlungen durch ebendiesen zu bereichern. Je mehr wir unser Leben mit den technologischen Möglichkeiten bereichern und neuen Technologien Eingang in unsere privatesten Bereiche gewähren, desto mehr laufen wir Gefahr, Opfer von Cyber Angriffen zu werden. Nicht nur Internet-NutzerInnen zeigen sich mehr als erfreut über voranschreitende Vernetzung und schnellere Breitbandverbindungen, auch Cyber Angreifer begrüßen die neuen Möglichkeiten, wie etwa die Kriminalstatistik des Bundesministeriums für Inneres belegt:

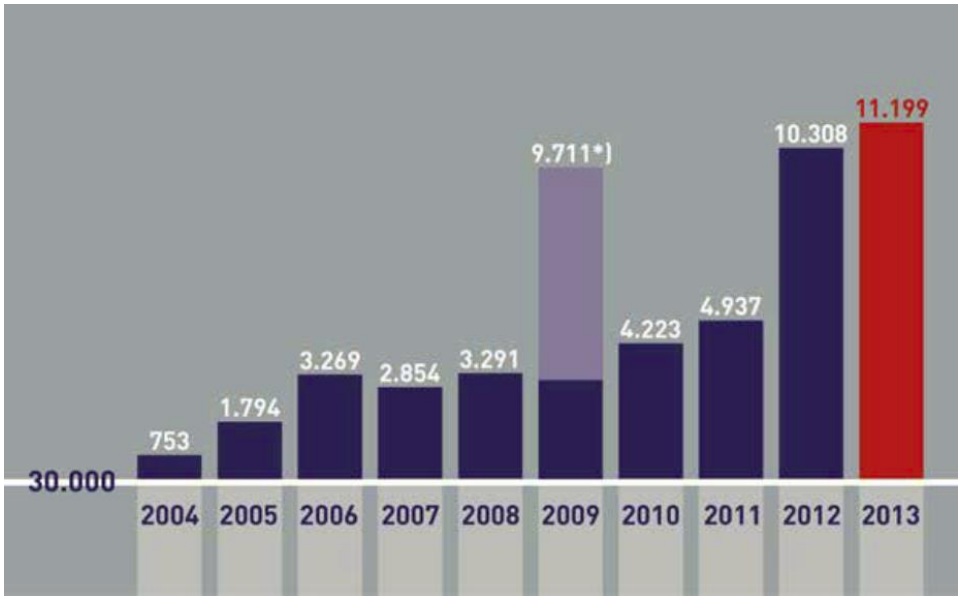


Abbildung 1: Cybercrime: Entwicklung in Österreich von 2004 bis 2013, Quelle: Polizeiliche Kriminalstatistik des BM.I

Von Heartbleed bis Dropbox: 2014 hatte viel zu bieten

Besonders weitreichendes Interesse in Österreich hat im Jahr 2014 der „Heartbleed"-Vorfall nach sich gezogen. Hierbei handelte es sich um einen schwerwiegenden Programmfehler in älteren Versionen der Open-Source-Bibliothek OpenSSL, durch den über verschlüsselte TLS-Verbindungen auch private Daten von KundInnen und Servern ausgelesen werden konnten.

Ein weiteres Phänomen, das zwar nicht neu, aber auch 2014 ein unliebsamer Begleiter zahlreicher Internet-NutzerInnen in Österreich war, ist Phishing. Dabei handelt es sich um eine Angriffsform, bei der Passwörter abgegriffen (gefischt) werden sollen. Zum Einsatz kommen dabei gefälschte Webseiten und E-Mails, in denen NutzerInnen aufgefordert werden, ihre Zugangsdaten bekannt zu geben. Dies betrifft sowohl Online-Banking-Daten als auch Dienste wie Webmail, Social Media, Onlinespiele oder E-Commerce-Seiten.
Phishing ist eine Form des Social Engineering, eine soziale Manipulation, welche danach trachtet, die Gutgläubigkeit oder mangelnde Aufmerksamkeit eines Menschen auszunutzen. Mit Hilfe dieser personenbezogenen Daten erreichen die Angreifer ihr vordergründiges Ziel, sie wollen damit zu Geld kommen.

Weitere Bedrohungen prägten das Bild: So hat 2014 das FBI (Federal Bureau of Investigation) US-amerikanische Unternehmen vor „zerstörerischen Folgen" möglicher Cyber Angriffe gewarnt, wie die Nachrichtenagentur Reuters meldete. Auslöser war der sogenannte Sony-Hack. Dabei ist es Hackern gelungen, in das Netz von Sony Pictures Entertainment einzudringen, Terabytes an Firmendaten zu kopieren und das dortige Netz vollständig lahmzulegen. Einige unveröffentlichte Filme, viele E-Mails und vertrauliche Geschäftsdokumente wurden anschließend illegal im Internet verbreitet.

Interessant ist, dass die dabei verwendete Schadsoftware von 90% der heute im Privatsektor verwendeten Sicherheitsprogramme nicht entdeckt worden wäre. Auch der öffentliche Bereich hätte diese Malware mit hoher Wahrscheinlichkeit nicht bemerkt, so die Aussage des FBI.

Ein ähnlich gelagerter Fall ist jener, der unter dem Namen iCloud-Hack Anfang September 2014 publik wurde: Hackern war es gelungen, die Passwörter zahlreicher US-Stars zu knacken und Nacktfotos aus der iCloud zu entwenden, die anschließend im Internet verbreitet wurden.

Eine neue Form des Phishing kombinierten im Jahr 2014 Cyber Angreifer erstmals mit dem beliebten Online-Speicherdienst Dropbox. Dabei wurde in einem öffentlichen Dropbox-Ordner eine gefälschte Login-Seite hinterlegt, um die eingegebenen Daten (Username und Passwort) der NutzerInnen zu erhalten. Interessant bei diesem Angriff war die Tatsache, dass die verwendete URL teilweise mit der echten Dropbox-Domain übereinstimmte und dadurch besonders gut getarnt war.

Cyber Kriminalität und Wirtschaftsspionage nehmen zu

Als wäre dies nicht genug, prognostiziert der IT-Sicherheitsanbieter Trend Micro, dass Hackerangriffe 2015 zu einem Massenphänomen werden. Auch aus dem Microsoft Security Intelligence Report 2014, der sich insbesondere mit der Verwundbarkeit von Software und in diesem Zusammenhang mit Malware auseinandersetzt, kann ein weiterer Trend abgeleitet werden: Firmen, und hierbei vor allem Industrie-Unternehmen, sind verstärkt von Cyber Angriffen bzw. Wirtschaftsspionage betroffen. Hintergrund dafür ist, dass ihre Daten interessanter und aus ökonomischer Sicht besonders wertvoll sind. Bei Betrachtung der zugrundeliegenden Studien wird ersichtlich, dass hier gravierender Aufholbedarf bezüglich der Sicherheitsvorkehrungen besteht. So werden lediglich 6,1% der Unternehmen als sehr sicher eingestuft, 9,3% als wenig sicher und 59, 6% werden als mittel sicher angesehen.

Hacking – ein aufstrebender Wirtschaftszweig

Im vergangenen Jahr wurde durch Cyber Angriffe weltweit ein Schaden von 113 Milliarden US-Dollar verzeichnet, die durchschnittlichen Kosten eines Angriffsfalles belaufen sich auf 298 US-Dollar, wie aus dem Norton Report 2013 von Symantec hervorgeht. Wenngleich die Genauigkeit solche Zahlen immer auch hinterfragt werden sollte, ist die Größenordnung insgesamt jedoch sehr beachtenswert.

Hacker halten mit ihren Angriffen IT-ExpertInnen auf der ganzen Welt auf Trab. Dem überwiegenden Teil der Attacken liegt dabei ein ausgeprägtes wirtschaftliches Interesse zugrunde. Denn in der Welt der Cyber Angreifer wird, wie in allen anderen Bereichen, ein reger Handel betrieben. Die Güter in diesem System sind allerdings keine klassischen Konsum- oder andere materiellen Güter, sondern persönliche Daten. Neben diesen Daten werden in der arbeitsteiligen Welt des Cyber Crime auch Software, Malware-as-a-service und Hosting-Dienste gehandelt. Ebenso gibt es Geldwäscher, Hehler und Data-broker, die im Netz ihr Unwesen treiben. Die Ökonomisierung des Hacking ist zweifelsohne eine Entwicklung, die auch 2014 und darüber hinaus voranschreiten wird.

Es geht immer ums Geld

Eben diese gestohlenen Daten machen Cyber Angreifer auf verschiedene Art und Weise zu Geld. Brian Krebs, IT-Sicherheitsexperte und früherer Journalist der Washington Post zeichnet in seinem Blog die Fehleinschätzung vieler InternetnutzerInnen auf, nach der ihr privater PC für Angreifer nicht wertvoll sei. Dies stimmt jedoch leider überhaupt nicht. Praktisch jede Aktivität im Netz kann in Geld umgewandelt werden, egal ob es sich nun um Zugangsdaten für Facebook, E-Mail-Accounts oder die Transformation eines PCs in einen Webserver handelt. Letzterer Punkt kann etwa dazu führen, dass man unwissend als Plattform für Kinderpornographie und Phishing Attacken missbraucht wird.

Zu den häufigsten Varianten, Daten in bare Münzen zu verwandeln, zählen der Verkauf von E-Mail-Listen an Spammer und die Weitergabe von Zugangsdaten an Identitätsdiebe. In weiterer Folge lässt sich dadurch Malware installieren, die beispielsweise wiederrum die Grundlage für Spionage mittels Webcam und Mikrofon oder Kreditkartenmissbrauch ist.

Besonders beliebt unter Angreifern ist die Installation von Programmen, die alle Tastendrücke und somit alle Passwörter und Login-Daten mitschreiben. Hierdurch kann Schaden für Betroffene auf vielfältige Weise entstehen, vom Online-Shopping bis zu hin zur Erpressung mit kompromittierenden Bildern und Informationen.

Auch Ransomware hat im Jahr 2014 nichts von seiner Gefährlichkeit und Aktualität verloren. „Ransom" steht dabei für „Lösegeld" und bezeichnet eine bösartige Schadsoftware, die den PC sperrt und erst gegen Lösegeld wieder freigibt. Ein aktuelles Beispiel dazu ist CryptoWall 2.0. Man erhält hierbei die Nachricht, dass alle Dateien verschlüsselt werden und nur gegen die Bezahlung eines Geldbetrages der Entschlüsselungscode zugeschickt wird. Bei Nicht-Bezahlung würden alle Dateien des PCs für immer gelöscht werden, so lautet die Drohung.

Wie die AutorInnen des Verizon's 2014 Data Breach Investigations Report konstatieren, ereignete sich zuletzt eine Verschiebung von globalen Attacken hin zu breit angelegten, spezialisierten Angriffen auf Kreditkarten- und Bezahlsysteme. Ein Trend, der sich auch 2014 fortsetzte. Wichtigste Erkenntnis: Je schneller Sicherheitslücken erkannt und darauf reagiert wird, desto weniger Schaden entsteht für betroffene Personen und Firmen.

Smartphones rücken verstärkt in den Fokus der Angreifer

Neben Angriffen auf herkömmliche PC-Systeme war 2014 auch gezeichnet von einer Zunahme des Interesses von Angreifern an mobilen Devices. Trotz Siegeszug von Smartphone, Tablet & Co. wird bei diesen Geräten noch immer weniger stark auf Sicherheit geachtet, als es bei klassischen PCs oder Laptops der Fall ist. In Anbetracht der Tatsache, dass gerade Smartphones eine Vielzahl persönlicher Daten beherbergen und ein Verlust, Diebstahl oder Angriff darauf weitreichende Folgen hat, ist höchste Vorsicht geboten. So geht ebenfalls aus dem Norton Report 2013 hervor, dass 63% der Smartphone-NutzerInnen und 30% der Tablet-NutzerInnen über keine grundlegenden Sicherheitsvorkehrungen verfügen. Oft fehlt sogar das Setzen eines PIN-Codes zum Entsperren des Smartphones.

Ein Schutz, der niemals vollständig ist

Zwar kann man sich vor Cyber Angriffen auf sehr vielfältige Weise schützen. Dennoch: vollständige Sicherheit kann und wird es niemals geben. Programme, die heute noch unsere Sicherheit gewährleisten, können bereits morgen veraltet sein und krimineller Energie neue Angriffsflächen bieten. Prominentestes Beispiel dafür ist Windows XP. Mehr als 12 Jahre nach Veröffentlichung ist Windows XP nach wie vor auf rund einem Drittel der weltweiten Rechner installiert. Für den „Oldtimer unter den Betriebssystemen" werden keine Sicherheitsupdates mehr angeboten, was es zu einem gefundenen Fressen für jeden Angreifer macht.

Die Grauzone zwischen vollständiger Unsicherheit und perfekter Absicherung ist jedoch sehr breit. Bereits erste einfache Maßnahmen bringen daher einen signifikanten Sicherheitsgewinn. So ist etwa der Browser Google Chrome mit aktivierten Autoupdates auf Windows XP ein großer Fortschritt gegenüber einem Internet Explorer 6.

Gesunder Menschenverstand und Eigenverantwortung wichtiger denn je

Insbesondere die Verschlüsselung von Daten ist im Jahr 2014 verstärkt in den Fokus gerückt. Selbst Snowden sprach bereits 2013 davon, dass gute Kryptografie funktioniert, daran hat sich auch bis heute nichts geändert. Ordnungsgemäß implementierte und starke Verschlüsselungssysteme gehören damit zu den wenigen Sicherheitsvorkehrungen, auf die man sich verlassen kann. Auch wenn die NSA versucht Verschlüsselungen zu brechen, gibt es bereits viele Verschlüsselungsmaßnahmen, die auch von der NSA nicht ausgehebelt werden können.

Neben der Verschlüsselung werden jedoch auch die Eigenverantwortung der NutzerInnen und der Schutz eigener Daten immer wichtiger. Höchste Vorsicht im Umgang mit persönlichen Daten und der Einsatz aktueller Anti-Schadsoftware sind unverzichtbar. In Kombination mit gesundem Menschenverstand machen Internet-NutzerInnen dadurch Cyber Angreifern das Leben so schwer wie nur möglich.

Ausgewählte Schlagzeilen des Jahres 2014 im Rückblick:

- Steckt die NSA hinter "Heartbleed"? (Der Standard, 14.11.2014)
- Grazer Forscher: Gängige Verschlüsselung hält 41 Jahre (Der Standard, 28.8.2014)
- "Wer nicht verschlüsselt, ist Freiwild" (Der Standard, 7.8.2014)
- Online-Banking: Raiffeisen warnt vor Trojaner (Die Presse, 1.12.2014)
- Datenklau bei den Maturareisen (Kurier, 3.12.2014)
- Sony-Hack: Nordkorea bestreitet Beteiligung nicht (Futurezone, 2.12. 2014)
- Heartbleed bedroht kritische Industrie-Kontrollsysteme (Futurezone, 19.7.2014)
- US-Geheimdienste nutzen Sicherheitslücken für Spionage (Kurier, 29.4.2014)
- Rekord-Datendiebstahl: 1,2 Mrd. Profildaten weg! (Heute, 6.8.2014)
- Massiver Datenklau bei Google Mail (Heute, 12.9.2014)

6. VORSTELLUNG VON CERT.AT UND GOVCERT AUSTRIA

CERT.at – die österreichische Internet-Feuerwehr

CERT.at ist das österreichische Computer Emergency Response Team (CERT) und wurde 2008 gemeinsam mit GovCERT Austria vom Bundeskanzleramt in Kooperation mit nic.at eingerichtet. Die klassischen Aufgaben eines Computer Emergency Response Teams sind mit jenen einer Feuerwehr vergleichbar: Das CERT-Team wird nämlich in erster Linie bei akuten Sicherheitsbedrohungen und Ereignissen aktiv. Dies geschieht durch Verständigung von betroffenen Stellen oder auf Basis eigener Recherchen.

Darüber hinaus ist CERT.at jedoch auch für vorbeugende Maßnahmen, wie Früherkennung, Vorbereitung für Notfälle, Öffentlichkeitsarbeit und Beratung zuständig. CERT.at versteht sich auch als Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse in Österreich und dient als vertrauenswürdige und anerkannte Informationsdrehscheibe. Zusätzlich – durch die internationale Vernetzung – ist CERT.at auch der „international sichtbare Partner" für ausländische CERTs. Das Team von CERT.at besteht derzeit aus über zehn Personen und wird von Robert Schischka geleitet.

Abbildung 2: Logo von CERT.at, dem Computer Emergency Response Team

CERT.at – Wie wir arbeiten

CERT.at sammelt Informationen zu Sicherheitsproblemen im österreichischen Internet, wie etwa infizierte Windows-PCs, manipulierte Webseiten oder fehlkonfigurierte Server. Dazu stützt sich CERT.at neben der eigens entwickelten Sensorik primär auf Quellen innerhalb der internationalen Gemeinschaft der IT-Sicherheitsbranche. Mit einer eigens entwickelten Sensorik überprüft CERT.at proaktiv das österreichische Internet auf potenzielle und tatsächliche Bedrohungen. Zusätzlich bearbeitet CERT.at akribisch alle eingehenden Meldungen über sicherheitsrelevante Vorkommnisse und entscheidet anlassbezogen über die weitere Vorgehensweise. Handelt es sich tatsächlich um Bedrohungen und ist ein akutes Eingreifen notwendig, so liegt die Hauptarbeit von CERT.at in weiterer Folge darin, die jeweiligen Internet Service Provider (ISPs) bzw. Domaineigentümer darüber zu informieren. Dabei werden Handlungsanleitungen bereitgestellt und Informationen geteilt, wie Bedrohungen am besten beseitigt werden können. CERT.at hat hierbei eine vorwiegend beratende und unterstützende Rolle, denn die tatsächliche Problembeseitigung kann letztlich nur durch die Betroffenen selbst erfolgen.

Weiters führt CERT.at tägliche Quellenbeobachtungen durch und fasst diese in einer Mailingliste zusammen. Auch werden auf www.cert.at Warnungen über IT-Sicherheitsprobleme veröffentlicht, um diese möglichst rasch der interessierten Öffentlichkeit zur Verfügung zu stellen.

Im Einsatz für mehr Internetsicherheit arbeitet CERT.at auch intensiv mit ausländischen CERTs zusammen und pflegt einen regen Informations- und Erfahrungsaustausch mit ExpertInnen aus aller Welt.

Der CERT-Beirat
In seiner strategischen Ausrichtung wird CERT.at durch einen eigenen CERT-Beirat unterstützt. Dieser bringt als beratendes Organ weitere Sichtweisen und Themenvorschläge ein. Die Mitglieder des Beirats repräsentieren dabei einen Querschnitt der Internet-Community in Österreich, fungieren als BotschafterInnen von CERT.at und unterstützen damit die Vernetzung des Themas Internetsicherheit in Gesellschaft und Politik.

Was CERT.at nicht ist
CERT.at ist keine Ermittlungsbehörde und befasst sich daher nicht mit dem Thema der Strafverfolgung im Internet. So hat CERT.at kein Durchgriffsrecht auf die Netzwerkinfrastruktur Österreichs und kann daher bei Security Incidents nur koordinierend und beratend aktiv werden.

Auch ist CERT.at keine isoliert arbeitende Einrichtung, sondern vielmehr eine koordinierende und informierende Stelle, die bei Angriffen auf Rechner sofort mit den jeweiligen Netzbetreibern und zuständigen Security Teams in Kontakt tritt. CERT.at verfügt über keine „Wunderwaffe" gegen Sicherheitsprobleme. Die Experten von CERT.at sehen sich selbst als die „Österreichische Internet-Feuerwehr", die im Falle des Falles Hilfe zur Verfügung stellt und in enger Abstimmung mit anderen Beteiligten den österreichischen Teil des Internets von Problemen befreit – auf Basis eines freiwilligen Angebots.

GovCERT Austria – die SpezialistInnen im Behördenbereich
GovCERT Austria ist das Government Computer Emergency Response Team für die öffentliche Verwaltung und die kritische Informations-Infrastruktur (KII) in Österreich. Dabei erfüllt GovCERT Austria auf nationaler Ebene eine Koordinationsfunktion für die einzelnen Stellen der öffentlichen Verwaltung und den Betreibern kritischer Infrastruktur. Auf internationaler Ebene agiert GovCERT Austria als österreichische Kontaktstelle für ausländische Regierungen und internationale Organisationen bei Fragen der IKT-Sicherheit. Es tauscht Informationen und Warnungen mit diesen aus und leitet sie bei Bedarf an inländische InteressentInnen weiter. GovCERT Austria erfüllt dabei seine Arbeit und Aufgaben in enger Personalunion mit CERT.at.

Abbildung 3: Logo von GovCERT Austria, dem Computer Emergency Response Team für die öffentliche Verwaltung

Wichtige Player der Österreichischen Strategie für Cyber Sicherheit (ÖSCS)

Eine effektive Cyber Sicherheitsstrategie bedarf eines dichten und qualitativ hochwertigen Netzwerkes aller Cyber Security Stakeholder und Strukturen. Dazu gehört auch die Einrichtung eines starken und umfassenden Cyber Security Krisenmanagements. Im Rahmen der ÖSCS agieren CERT.at und GovCERT Austria als relevante sektorale Meldestellen, die bei Cyber Vorfällen gemeinsam mit weiteren Stellen des öffentlichen und privaten Bereiches aktiv werden. Sie sind die erste Anlaufstelle für Fragen zur Sicherheit im österreichischen Teil des Internets und richten sich dabei primär an Unternehmen, den öffentlichen Sektor, Banken, Institutionen des Gesundheitswesens und große Infrastrukturbetreiber (Telekom, Energie, öffentlicher Verkehr).

CERT-Verbund für mehr Datensicherheit

Wir leben in einer Gesellschaft, die zunehmend von digital vernetzten Informations- und Kommunikationssystemen abhängig ist. Um diese für das Funktionieren unserer Gesellschaft essenziellen Systeme verstärkt zu schützen, wurde Ende 2011 auf Initiative des österreichischen GovCERT Austria und des BMLVS ein Österreichischer CERT-Verbund ins Leben gerufen. Im Mittelpunkt der Zusammenarbeit stehen der Schutz von IKT-Infrastrukturen, der Informationsaustausch und die rasche Reaktion auf Bedrohungen. Im Rahmen einer Kooperation arbeiten öffentliche Verwaltung und Privatwirtschaft eng zusammen, um eine ganzheitliche Sichtweise im Kampf gegen Cyber Bedrohungen zu entwickeln. Mitglieder des CERT-Verbunds sind neben GovCERT Austria/CERT.at unter anderem das das ACOnet CERT, Raiffeisen-IT CERT, das Bundesrechenzentrum, WienCERT, das milCERT und andere. Durch die Zusammenarbeit soll nicht nur die Qualität der Services steigen, sondern auch ein für den möglichen Ernstfall relevanter Wissensvorsprung aufgebaut werden.

Weitere Informationen:

- Bundeskanzleramt Österreich: https://www.bka.gv.at/site/7863/default.aspx
- Digitales Österreich: http://www.digitales.oesterreich.gv.at
- Österreichische Strategie für Cyber Sicherheit (PDF): https://www.bka.gv.at/DocView.axd?CobId=50748
- Bericht Cyber Sicherheit 2014 (PDF): https://www.bka.gv.at/DocView.axd?CobId=55935

7. Rückblick auf die Aktivitäten von CERT.at und GovCERT Austria 2014

Die Internet-Feuerwehr ist nicht nur dann zur Stelle, wenn IT-sicherheitstechnisch Feuer am Dach ist. Neben Soforthilfe bei Angriffen aus dem Netz leisten CERT.at und GovCERT Austria zusätzlich auch wichtige Aufklärungs- und Präventionsarbeit.

Das Karussell der Schadenshöhen dreht sich

Die Fakten sprechen eine deutliche Sprache: Eine Studie des Antivirensoftware-Herstellers McAffee hat erhoben, dass Cyber Angriffe weltweit jährlich Schäden in der Höhe von rund 445 Milliarden US-Dollar (umgerechnet rund 330 Milliarden Euro) anrichten. Davon sind 160 Milliarden US-Dollar auf den Diebstahl persönlicher Informationen zurückzuführen. Alleine in der EU kosten Cyber Angriffe rund 150.000 Arbeitsplätze pro Jahr. In den USA sind rund 200.000 Jobs davon betroffen. Glaubt man anderen Berechnungen, wie etwa dem unabhängigen Center for Strategic and International Studies (CSIS), so ist die Schadenshöhe mit weltweit bis zu 575 Milliarden US-Dollar (rund 459,1 Milliarden Euro) sogar noch größer.

Bedrohungen kennen keine Ländergrenzen

Das CSIS hat außerdem festgestellt, dass gemessen an der Wirtschaftsleistung der Schaden durch Angriffe aus dem Netz in Deutschland am größten ist. So belaufen sich die Auswirkungen durch Cyber Angriffe im Nachbarland Österreichs auf rund 1,6% des Bruttoinlandsprodukts (BIP). Damit liegt Deutschland vor den Niederlanden (1,5%), den USA und Norwegen (je 0,64%) und China (0,63%). Allein in den USA, in China, Japan und Deutschland erreichten die Schäden eine Summe von etwa 200 Millionen US-Dollar. EU-weit macht der Schaden 0,41 Prozent des BIP aus.

Fast jedes Unternehmen betroffen

Die Intensität von Cyber Angriffen nimmt ständig zu. Wie stark dieses Ausmaß ist, hat vor kurzem die Deutsche Telekom auf den Punkt gebracht: IT-SicherheitsexpertInnen haben im Rahmen des Cyber Security Summit 2014 in Bonn bekanntgegeben, dass alleine die Deutsche Telekom täglich bis zu eine Million Attacken auf ihr Netz zählt. Das sind natürlich nicht alles gezielte Angriffe, sondern zeigt vielmehr, wie hoch das Hintergrundrauschen im Netz geworden ist. Laut dem Telekom-Report zur Cyber Kriminalität haben im Jahr 2014 neun von zehn deutschen Firmen Angriffe von außen registriert. Eine Studie des Beratungsunternehmens KPMG weist darüber hinaus auch Zahlen für Österreich aus. Laut dieser Erhebung war in den vergangenen zwei Jahren jedes vierte Unternehmen in Österreich von Cyber Angriffen betroffen. Die durchschnittliche Schadenshöhe beläuft sich dabei auf fast 400.000 Euro.

Cyber Angriffe fordern IT-Sicherheitsexperten

Die Zunahme an Angriffen aus dem Internet fordern auch IT-SicherheitsexpertInnen weltweit und in Österreich heraus. So hatte die Internet-Feuerwehr CERT.at und GovCERT Austria im Jahr 2014 alle Hände voll zu tun, um die Sicherheit österreichischer Behörden, Unternehmen und PrivatanwenderInnen zu verbessern. Denn eines steht zweifelsohne fest: Österreich ist längst keine Insel der Seligen mehr, wie CERT.at und GovCERT Austria im Rahmen ihrer täglichen Arbeit erleben.

Alle 8,6 Sekunden betritt ein neuer Schädling die digitale Bühne

Die verwendeten Techniken und Schadprogramme von Internet-Angreifern sind vielfältig und komplex – und entwickeln sich mit rasender Geschwindigkeit weiter. ExpertInnen von G DATA Security Labs haben im Rahmen des Malware Reports für das erste Halbjahr 2014 ermittelt, dass alle 8,6 Sekunden ein neuer Computerschädling für Windows PCs und Notebooks die digitale Bühne betritt. Die Prognose für das gesamte Jahr 2014 ist eindeutig: Die Marke von 3,5 Millionen neuer Schadprogrammtypen wird erstmalig übertroffen werden.

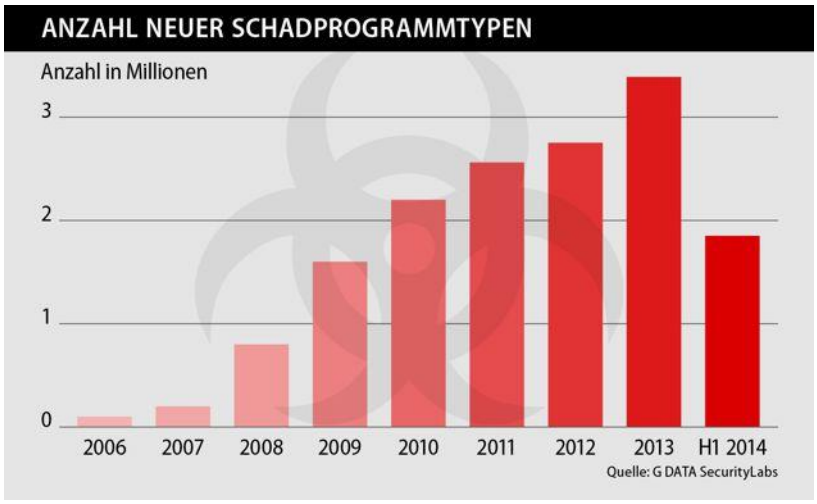


Abbildung 4: Anzahl neuer Schadprogrammtypen im Zeitverlauf, Quelle: G DATA SecurityLabs

Besonders starke Zuwächse gibt es insbesondere im Bereich der Banking-Trojaner, die 2014 ein neues Allzeithoch erreicht haben. Die Analyse der Top 25 Banking-Angriffsziele zeigt, dass KundInnen amerikanischer Banken und Bezahldienste mit 48% am stärksten ins Visier genommen werden. Nicht weiter verwunderlich, verfügen Cyber Angreifer mit diesen Trojanern doch über ein sehr profitables „Geschäftsmodell" in der Untergrundökonomie.

Abbildung 5: Länderverteilung der Top 25 Banking-Trojaner-Ziele (H1/2014), Quelle: G DATA SecurityLabs

Neben den Banking-Trojanern setzte auch Adware ihren Höhenflug fort. Seit dem 2. Halbjahr 2012 haben die Zahlen neuer Schadprogrammtypen dieser Kategorie um das 16-fache zugenommen. 14% aller neuen Signaturvarianten entfallen aktuell auf Adware. Diese „potentiell unerwünschten Programme" (PUP) sind keine Malware im klassischen Sinn. AnwenderInnen empfinden diese aber als durchaus störend. Vor allem, da einmal eingefangen, Adware oft schwer wieder zu deinstallieren ist.

Sammelbegriff „Malware"

Das breite Spektrum der Schadsoftware wird unter dem Begriff „Malware" zusammengefasst und umfasst eine Fülle an verschiedenen Bedrohungsformen. Dazu gehören Computerviren und -würmer, Trojaner, Spyware, Ransomware, Adware, Exploit-Packs und viele mehr. CERT.at beobachtet intensiv die Entwicklung von Malware und anderen Bedrohungsformen im Internet und gibt im Anlassfall proaktiv Sicherheitswarnungen heraus. Zusätzlich unterstützt die Internet-Feuerwehr IT-Verantwortliche durch die Weitergabe von Know-how und leistet auch wichtige Präventions- und Aufklärungsarbeit in der Öffentlichkeit. Dadurch tragen CERT.at und GovCERT Austria bei, das Internet in Österreich sicherer zu machen.

Die Internet-Sicherheitslage Österreichs 2014

CERT.at und GovCERT Austria führen umfangreiche Statistiken, mit denen sich ein aussagekräftiges Bild über die aktuelle Internet-Sicherheitslage Österreichs geben lässt. Wichtige Kennzahlen dafür sind Reports, Incidents und Investigations.

„Reports" bezeichnen eingehende Meldungen an CERT.at. Nicht alle davon beschreiben einen Sachverhalt, der von CERT.at als relevanter Vorfall (Incident) eingestuft wird und eine aktive Behandlung erfordert. Typische Gründe für eine Beurteilung als irrelevanter Vorfall sind etwa:

- Meldungen zu Problemen, die bereits bereinigt wurden
- Falschmeldungen von einfachen Suchalgorithmen
- mangelnde Zuständigkeit von CERT.at
- generische Anfragen
- oder andere E-Mail-Irrläufer/Spam

Als „Incidents“ werden jene Fälle eingestuft, die tatsächlich ein Sicherheitsrisiko darstellen. Bei diesen schreitet CERT.at ein und informiert beispielsweise betroffene Unternehmen, Organisationen oder PrivatanwenderInnen über IT-Sicherheitsbedrohungen und unterstützt bei Bedarf bei der Problemlösung. Diese Kontaktaufnahme wird im CERT.at Ticketsystem als „Investigation“ bezeichnet.

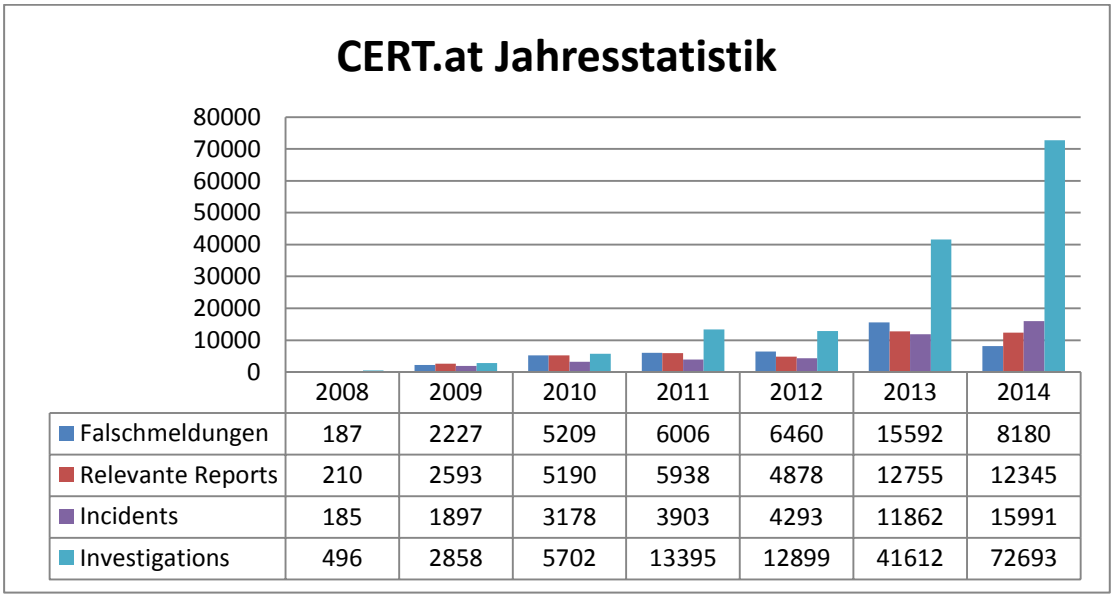
Bei der Interpretation der nun folgenden Grafiken und Statistiken muss man folgende Einschränkungen beachten:

1. Eine Verbesserung in der Sensorik besitzt oft viel mehr Einfluss auf die Kurve, als eine Veränderung der dahinterliegenden Vorfälle. Wenn etwa durch eine Polizeiaktion in den USA plötzlich Daten zu einem Botnet verfügbar werden, dann bedeutet dies einen plötzlichen und großen Sprung in den CERT.at Statistiken. In Wirklichkeit wurde das Botnet aber über eine längere Zeit hinweg aufgebaut.

2. Diese Zahlen spiegeln daher stärker die Arbeit von CERT.at wider, als dass sie eine genaue Aussage über die Sicherheitslage in Österreich abgeben.

3. Nicht alle Vorfälle sind gleichwertig relevant: Ein Incident kann sowohl ein fehlkonfigurierter Surf-PC in einer Jugendherberge sein, als auch ein Einbruch in einen Webshop mit dem Verlust tausender KundInnendaten.

4. Viele der Incidents behandeln bereits aggregierte Informationen. So etwa generiert die Sensorik zu falsch konfigurierten Nameservern einen Report pro Tag, unabhängig wie viele einzelne IP-Adressen enthalten sind. Die ausgehenden Mails an die Netzbetreiber können ebenfalls von einem einzelnen Vorfall bis hin zu einer langen Liste an betroffenen KundInnen reichen.



	2008	2009	2010	2011	2012	2013	2014
Falschmeldungen	187	2227	5209	6006	6460	15592	8180
Relevante Reports	210	2593	5190	5938	4878	12755	12345
Incidents	185	1897	3178	3903	4293	11862	15991
Investigations	496	2858	5702	13395	12899	41612	72693

Abbildung 6: CERT.at Jahresstatistik mit Übersicht über Reports, Incidents und Investigations im Zeitverlauf, Quelle: CERT.at

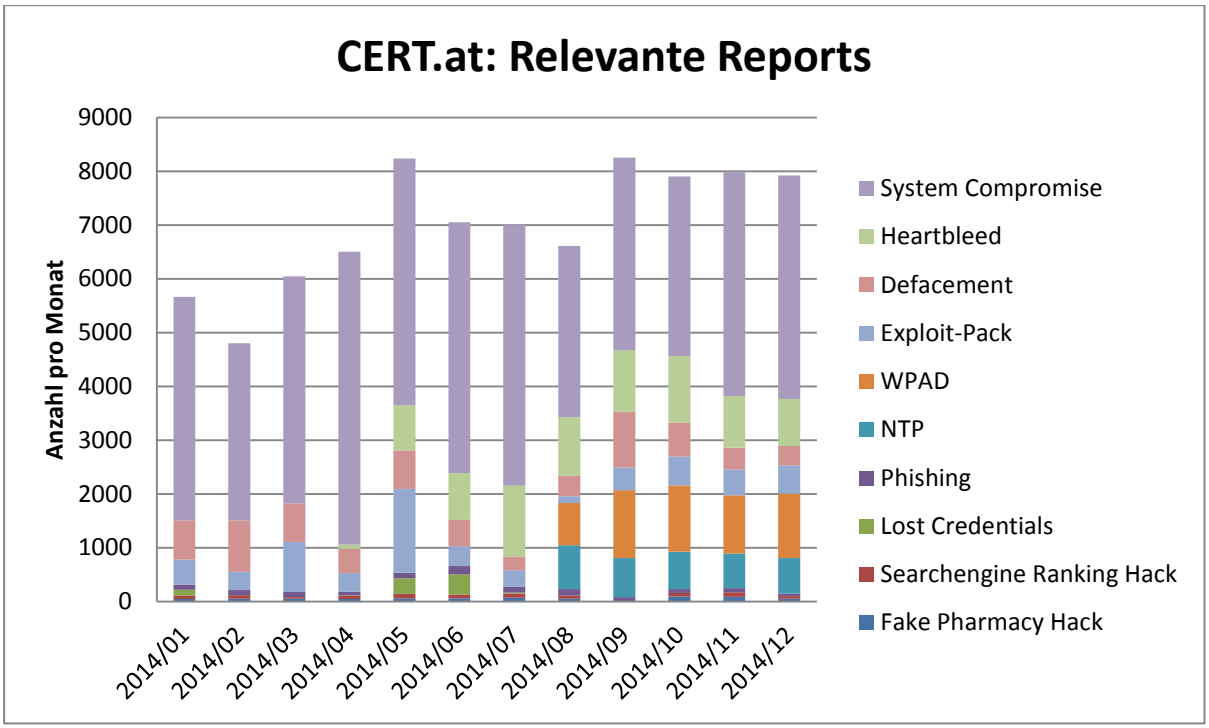


Abbildung 7: Klassifizierung der relevanten Reports nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

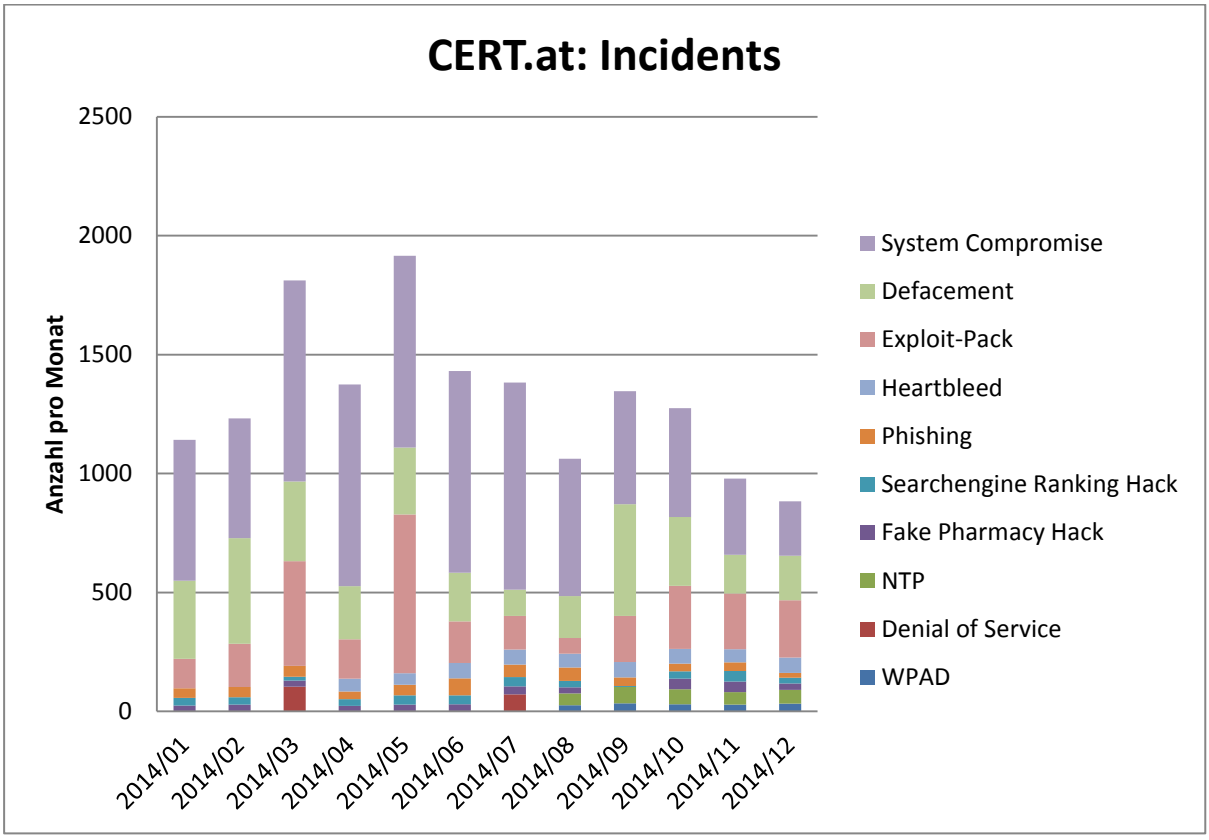


Abbildung 8: Klassifizierung von Incidents nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

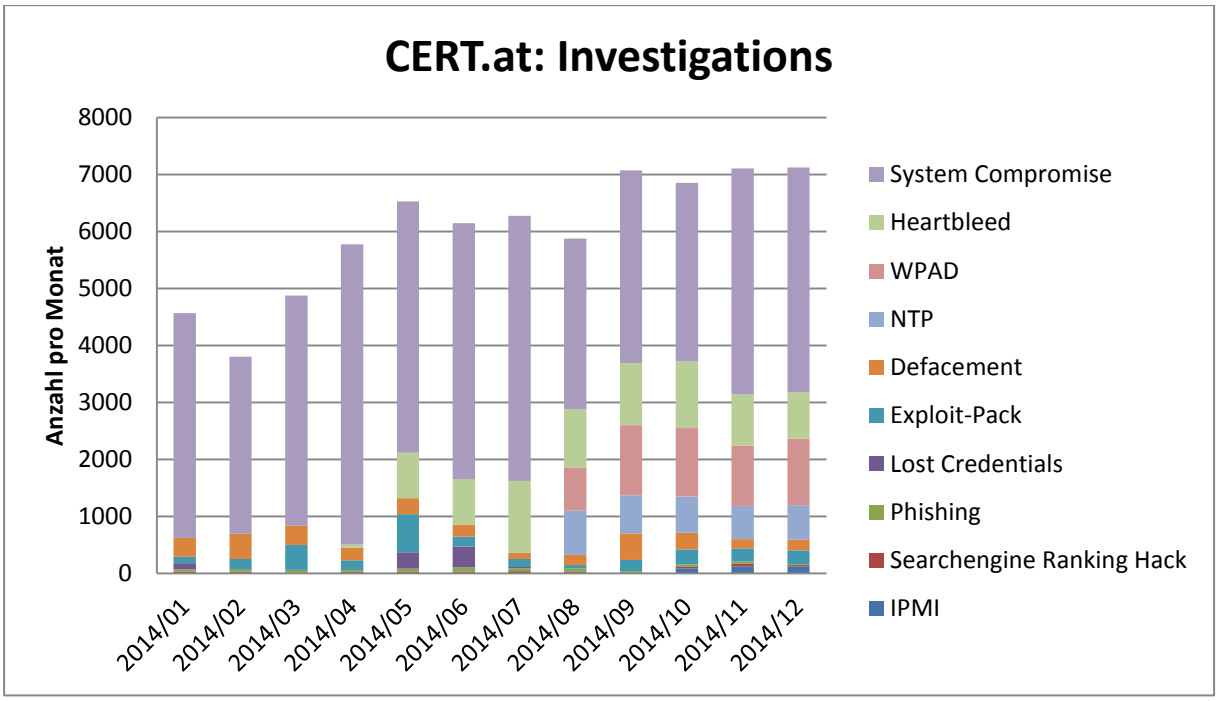


Abbildung 9: Klassifizierung der von CERT.at durchgeführten Investigations nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Kategorien

Vorfälle werden in diversen Kategorien klassifiziert, die im Folgenden näher beschrieben werden.

System Compromises

Unter „System Compromise" wird verstanden, dass ein Angreifer die Kontrolle über einen Computer erlangt hat. Die Mehrzahl dieser Fälle ist Schadsoftware auf Windows PCs: der betroffene PC ist Teil eines Botnetzes geworden. Was die Malware auf dem PC anrichtet, kann stark variieren. Dies reicht von fast nichts (bestes Beispiel: Conficker) über Spamversand, den Diebstahl von Passwörtern, Manipulationen beim Onlinebanking bis hin zur Erpressung.
Da CERT.at diese Kategorie über die ISPs behandelt, fließt die Zahle der betroffenen Systeme nur bedingt in die Zahl der Vorfälle ein: Ob die tägliche Mail an einen Internet Service Provider jetzt zehn oder zehntausend IP-Adressen enthält, geht in diese Statistik nicht ein.

Heartbleed

Danach folgt mit Heartbleed bereits jenes Thema, das IT-SicherheitsexpertInnen und Medien – weltweit wie auch in Österreich – in diesem Jahr besonders intensiv beschäftigt hat. Bei der unter der Bezeichnung Heartbleed im April 2014 erstmals bekannt gewordenen Schwachstelle im Programmcode des Sicherheitsprotokolls OpenSSL handelt es sich um einen trivialen Programmierfehler, der jedoch weitreichende Folgen hatte. Durch gezieltes Ausnützen der Sicherheitslücke war es Angreifern möglich, völlig unbemerkt Passwörter und andere, eigentlich geschützte Informationen von Web-Diensten auszulesen. Das Besondere bei Heartbleed war nicht die Sicherheitslücke an sich, sondern die große Anzahl der Betroffenen. Die Unterwanderung des bislang als sicher geltenden Internetprotokolls SSL hat

dazu geführt, dass sich Heartbleed binnen kürzester Zeit nach dessen Bekanntwerden zu einem der weltweit größten IT-Sicherheitsvorfälle entwickelt hat

Dem schnellen Eingreifen der Experten von CERT.at und der Vernetzung der IT-Sicherheitscommunity in Österreich ist es zu verdanken, dass von Heartbleed Betroffene rasch kontaktiert und Unterstützung bei der Beseitigung der Schachstelle erhalten haben – beispielsweise durch das Einspielen von Patches, mit denen das Leck relativ unkompliziert geschlossen werden konnte. Dadurch war es möglich, der Heartbleed-Lücke in Österreich rasch und vor allem signifikant entgegenzuwirken. Nichtsdestotrotz gibt es Ende 2014 noch immer einen – wenn auch verhältnismäßig – kleinen Teil vernachlässigter oder schlecht gewarteter Server, die anfällig für Heartbleed-Attacken sind. Diese stellen dadurch noch immer ein veritables Sicherheitsrisiko dar.

Im August 2014 hat CERT.at den Status von Heartbleed in Österreich in einem Bericht zusammengefasst. Inzwischen haben sich die Zahlen weiter verbessert:

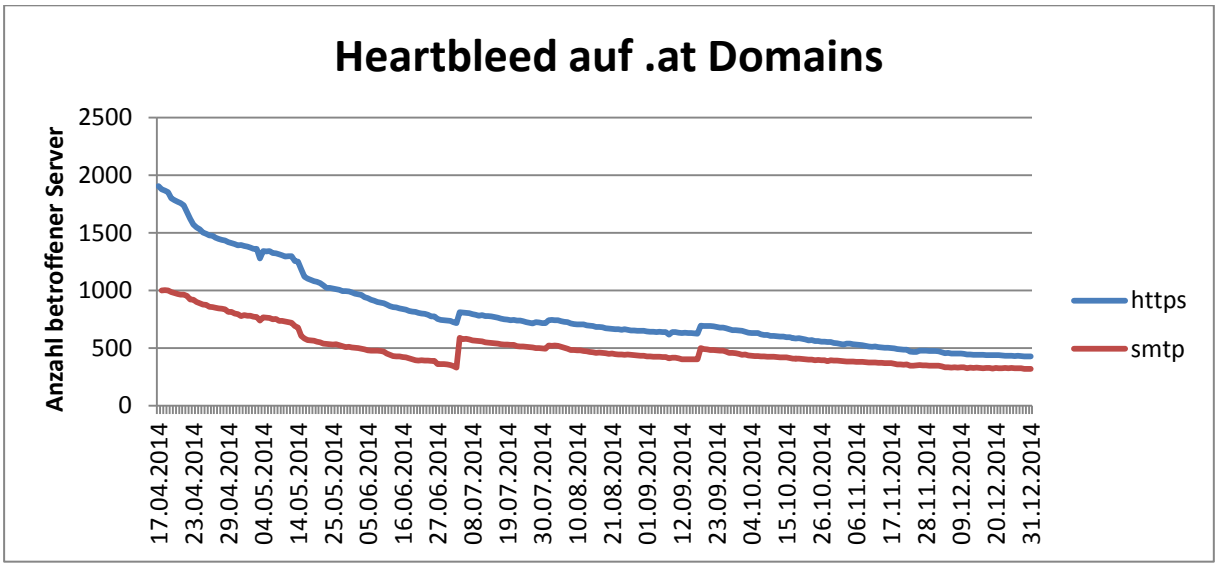


Abbildung 10: Anzahl der von Heartbleed betroffenen Server, Quelle: CERT.at

Gut sichtbar ist die Abnahme in der Zahl der verwundbaren Server Mitte Mai nachdem CERT.at begonnen hat, die Provider über Heartbleed-Probleme mit .at Domains zu informieren. Die Zacken nach oben (am 4.7.2014 und 18.9.2014) entstanden durch eine Aktualisierung der Domainliste und der Zuordnung auf IP-Adressen.

Windows Proxy Auto-Detection (WPAD)

Microsoft hat ein Protokoll spezifiziert, nachdem ein Webbrowser den richtigen Webproxy für das lokale Netz erkennen kann. Diese nutzt den speziellen Hostnamen „wpad", um sich von dort ein Konfigurationsfile zu holen. Aufgrund eines Konfigurationsfehlers greifen manche Windows-Clients aber auf wpad.co.at, wpad.or.at oder wpad.at zu. Zugriffe auf diese Domains werden von CERT.at als Sensorik für diese Konfigurationsprobleme benutzt.

Exploit-Packs, Defacements, Searchengine Ranking / Fake Pharmacy Hacks
Bei diesen Kategorien handelt es sich um manipulierte Webserver. Ein Defacement („Verunstaltung") ist einfach zu erkennen: Der Angreifer verändert das Aussehen der Webseite radikal, um zu beweisen, dass er einbrechen konnte. Typisch sind hier martialische Bilder auf schwarzem Hintergrund, gespickt mit Schmähungen, Slogans und Grüßen an andere Hackergruppen.

Exploit-Packs sind deutlich subtiler: In die Webseiten wird ein Code (oder auch nur ein Verweis darauf) eingebaut, der den Browser des Besuchers auf Schwachstellen abklopft. Findet das Exploit-Pack etwa ein veraltetes Java-Plugin, dann werden dessen Lücken genutzt, um Schadsoftware am PC des Besuchers zu installieren.

Manchmal fügt ein Webeinbrecher auch nur gezielt Links in den Inhalt der Webseite ein, um so das Google-Ranking für seine zwielichtigen Seiten zu manipulieren.

Noch trickreicher sind Fake Pharmacy Hacks: Hier wird ein Code in das Webveraltungssystem des Opfers eingeschleust, der den Google-Rank der Seite nutzt, um beispielsweise die Suche nach Potenzpillen auf die Webshops des Angreifers zu lenken.

Bewusstsein für Verschlüsselung steigt
Im Zuge des Heartbleed-Vorfalls hat CERT.at im Jahresverlauf 2014 weitere Aktivitäten gesetzt, um auf die Wichtigkeit von Privacy und Verschlüsselung hinzuweisen. Vorfälle wie zuletzt Heartbleed oder der anhaltende öffentliche Diskurs rund um die Enthüllungen von Edward Snowden haben aus Sicht der ExpertInnen auch ihre positiven Seiten: Im Umgang mit Privacy und Verschlüsselung kommt es anwender- wie auch anbieterseitig zu Bewegung. Der Schutz eigener Daten und der Privatsphäre im Internet haben für viele NutzerInnen zunehmende Priorität. Auch verschlüsseln immer mehr E-Mail-Anbieter mittlerweile Nachrichten während der Übertragung. Laut Google Transparenzbericht werden mit Stand Dezember 2014 bereits über drei Viertel (77%) aller ausgehenden Nachrichten von Gmail an andere Anbieter verschlüsselt übermittelt. Eingehend ist dies bereits fast bei sechs von zehn Mails (58%) der Fall.

Um Betreiber von Mail- und Webservern beim richtigen Set-up ihrer IT-Systeme zu unterstützen hat sich eine Gruppe engagierter IT-SicherheitsexpertInnen zusammengeschlossen und ein White Paper zu Kryptografie verfasst. Die BetterCrypto-Expertengruppe gibt darin einen Überblick über den aktuellen Stand der Technik in Sachen Verschlüsselung und will vor allem weniger erfahrene Systemadministratoren durch vorgeschlagene Einstellungen dabei unterstützten, ihre Systeme mit einfachen Mitteln sicherer zu machen. Das White Paper aus Österreich wurde bereits auf internationalen Sicherheitskonferenzen vorgestellt und wird mittlerweile weltweit referenziert.

Immer noch wirkungsvoll: Denial-of-Service-Attacken

Denial-of-Service (DoS) Attacken zählen zum Standard-Repertoire der Angreifer – und kommen selbst nach langer Zeit nicht aus der Mode. Die Idee des Angreifers ist eine einfache: Wenn ich schon nicht bei meinem Opfer einbrechen kann, so kann ich wenigstens seine Systeme so stören, dass sie nicht mehr von legitimen AnwenderInnen genutzt werden können. Dazu dient eine Flut von Anfragen an die Server, um diese – oder die Leitungen dorthin – zu überlasten.

Im Unterschied zu DoS (einer direkten Angriffsform, bei dem der Verursacher relativ einfach erkennbar wäre) bedienen sich Angreifer bei Distributed Denial of Service (DDoS) Attacken verteilter Ressourcen im weltweiten Netz. Dadurch lässt sich die Intensität von Angriffen verstärken und größerer, zumeist zielgerichteter Schaden verursachen. Sehr häufig bedienen sich Angreifer dabei vorhandener Botnetze. Das müssen aber nicht notwendigerweise infizierte Windows-PCs in Privathaushalten sein, auch Server oder manipulierte Router können dafür benutzt werden. Ein anderes Beispiel für ein solches Netz an infiltrierten Rechnern ist Brobot. Dieses Botnetz wurde beispielsweise von Herbst 2012 bis Mitte 2013 für eine große Attacke auf US-Finanzunternehmen eingesetzt. Dabei wurden nicht wie sonst üblich Heim-PCs, sondern Webserver benutzt, was zu einer immensen Steigerung der Brandbreiter der Angriffe führte. Gehackte Websites gab und gibt es auch in Österreich noch immer, wodurch österreichische Systeme quasi indirekt zu Mittätern wurden.

Reflection Angriffe als gefährliche Sonderform

CERT.at war 2014 auch mit einer Sonderform von DoS-Angriffen konfrontiert – nämlich so genannten Reflection Attacks. Diese Angriffe nutzen legitime Protokolle, die auf Basis von UDP (User Datagram Protocol) arbeiten, und bei denen daher der Absender einer Anfrage nicht verifiziert wird. Dazu gehören etwa DNS (Namensauflösung), NTP (Zeitserver), SSDP (Simple Service Discovery, ein Teil des Universal Plug and Play Standards), SNMP (Netzwerk Management). Angreifer nutzen dabei bereitwillig antwortende Server und unsicher konfigurierte Netzwerke aus, indem sie diesen Anfragen schicken. Die IP-Adresse des Opfers ist dabei als Absender-IP-Adresse eingetragen. Die meist kleinen Anfragen lösen von den Servern große Antworten aus, die alle an das Opfer geschickt werden. Dieses „Spiel über die Bande“ verstärkt den Datenverkehr um den Faktor 50 bis 1.000, was dazu führt, dass das Zielobjekt (zB der Server einer Bank oder eines kritischen Infrastrukturbetreibers) mit enormem Netzwerk-Traffic bombardiert wird. Als Resultat ist der angegriffene Server (oder die Leitung zu ihm) überlastet und nicht mehr ansprechbar. Besonders heimtückisch bei dieser Angriffsform ist, dass das Opfer nur die Pakete vom Reflektor (und nicht vom Angreifer selbst) wahrnimmt und der Reflektor seinerseits davon ausgeht, dass er legitime Anfragen beantwortet. Dies ist auch der Grund, warum Reflection Attacks nur schwer abzustellen sind.

In der Umsetzung bedienen sich Angreifer dabei verschiedener Protokolle. In Österreich wurden 2014 vor allem die Protokolle DNS, NTP und SSDP dafür benutzt. Es ist daher

essentiell, dass die entsprechenden Server nicht jede beliebige Anfrage beantworten, sondern nur jene von ihren legitimen Klienten.

CERT.at informiert seit 2014 alle österreichischen Netzbetreiber basierend auf Daten von Shadowserver, welche Server in deren Netzen für solche Angriffe missbraucht werden können: Dieser Dialog mit den ISPs zeigt erste Wirkung, bei manchen dieser Protokolle gibt es messbare Verbesserungen (etwa bei ntp-version, wo CERT.at in KW32 zu warnen begonnen hat), es bleibt aber für 2015 noch viel zu tun.

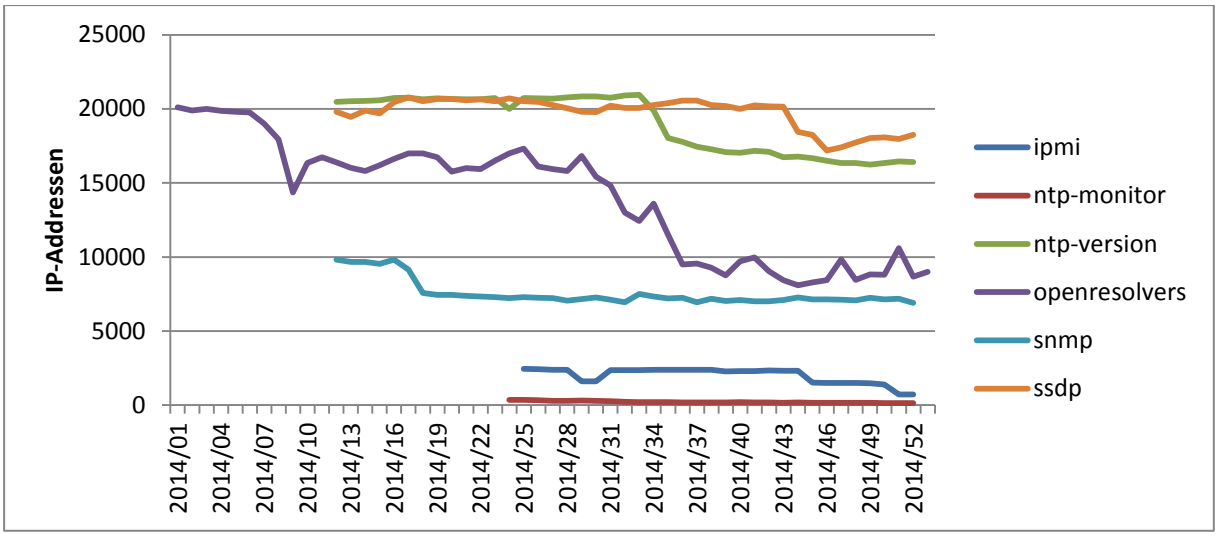


Abbildung 11: Überblick über die Entwicklung von Reflection Attacks im Jahr 2014, Quelle: CERT.at

Weitere Dauerbrenner: Ransomware, Spam, Phishing & Co.

Die Arbeit der IT-Sicherheitsexperten von CERT.at war auch 2014 durch den Kampf gegen bereits bekannte, aber sehr hartnäckige Bedrohungsformen gekennzeichnet. So ist Ransomware noch immer ein Dauerbrenner, der regelmäßig in neuen Ausprägungsformen AnwenderInnen das Leben schwer macht, indem Festplatten durch Schadsoftware verschlüsselt und "Lösegeld" für die Freigabe verlangt wird. Die früheren Versionen von Ransomware ließen sich noch austricksen, inzwischen ist die Evolution soweit fortgeschritten, dass die Daten ohne Hilfe der Erpresser nicht mehr wiederherstellbar sind. Ransomware ist daher ein weiterer Grund für eine seriöse Backup-Strategie.

Es reicht jedoch dabei nicht, die Daten einfach nur auf eine angesteckte USB-Festplatte zu sichern, da diese ebenfalls von der Ransomware verschlüsselt wird. Es ist egal, ob der Datenverlust durch Hardwaredefekte, Blitzeinschläge, Brand, Erpresser oder einfach nur durch Bedienungsfehler passiert, ein gutes Backup kann alle diese Fälle abfangen. Wie so oft, ist der erste Schritt zur IT-Sicherheit eine sorgfältige Betriebsführung.

Ebenfalls ein Dauerbrenner ist Phishing, also das Ausspähen von Zugangsdaten über gefälschte Webseiten und E-Mails. Generell gibt es auch dabei einen Trend zur persönlichen Kontaktaufnahme. Unter anderem haben sich 2014 mehrmals Angreifer als Microsoft Support MitarbeiterInnen ausgegeben, um Schadsoftware auf Rechnern installieren zu können. Angriffe über den Umweg via Social Media und Spam gehören leider auch weiterhin zum Alltag.

Auch die Manipulation und Veränderung von Webseiten, so genannte Defacements, haben sich in den letzten Jahren zu einem ernstzunehmenden Problem entwickelt. Besonders beliebt waren 2014 Angriffe über Erweiterungen wie beispielsweise Add-ons, Vorlagen, Designs udgl. von frei erhältlichen CMS Systemen. Vor allem die Installation von manipulierten Erweiterungen zu Webservern hat sich 2014 als neuer Trend herauskristallisiert.

8. Österreichische Strategie für Cyber Sicherheit

Die nationale und internationale Absicherung des Cyber Raums ist eine der obersten Prioritäten Österreichs. Mit der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) wurde von der Bundesregierung am 20. März 2013 ein umfassendes und proaktives Konzept zum Schutz des Cyber Raums und der Menschen in ebendiesem beschlossen. Die Strategie für Cyber Sicherheit bildet das Fundament der gesamtstaatlichen Zusammenarbeit in diesem Bereich. Die Implementierung der ÖSCS ist ein permanenter Prozess, der von mehreren Arbeitsgruppen vorbereitet, diskutiert und in weiterer Folge begleitet wird. Die ersten Ergebnisse und Empfehlungen der Arbeitsgruppen liegen nun vor, von denen wir nachfolgend einige vorstellen.

Neuer koordinativer Überbau

Ein wichtiges Kernelement in der Umsetzung der ÖSCS ist die Erarbeitung von Prozessen und Strukturen zur permanenten Koordination auf der operativen Ebene. Ziel des Aufbaus einer solchen operativen Koordinierungsstruktur ist es, sowohl auf politischer, strategischer wie auch operativer Ebene funktionierende Beziehungsstrukturen aufzubauen, um für künftige Sicherheitsvorfälle besser gerüstet zu sein.

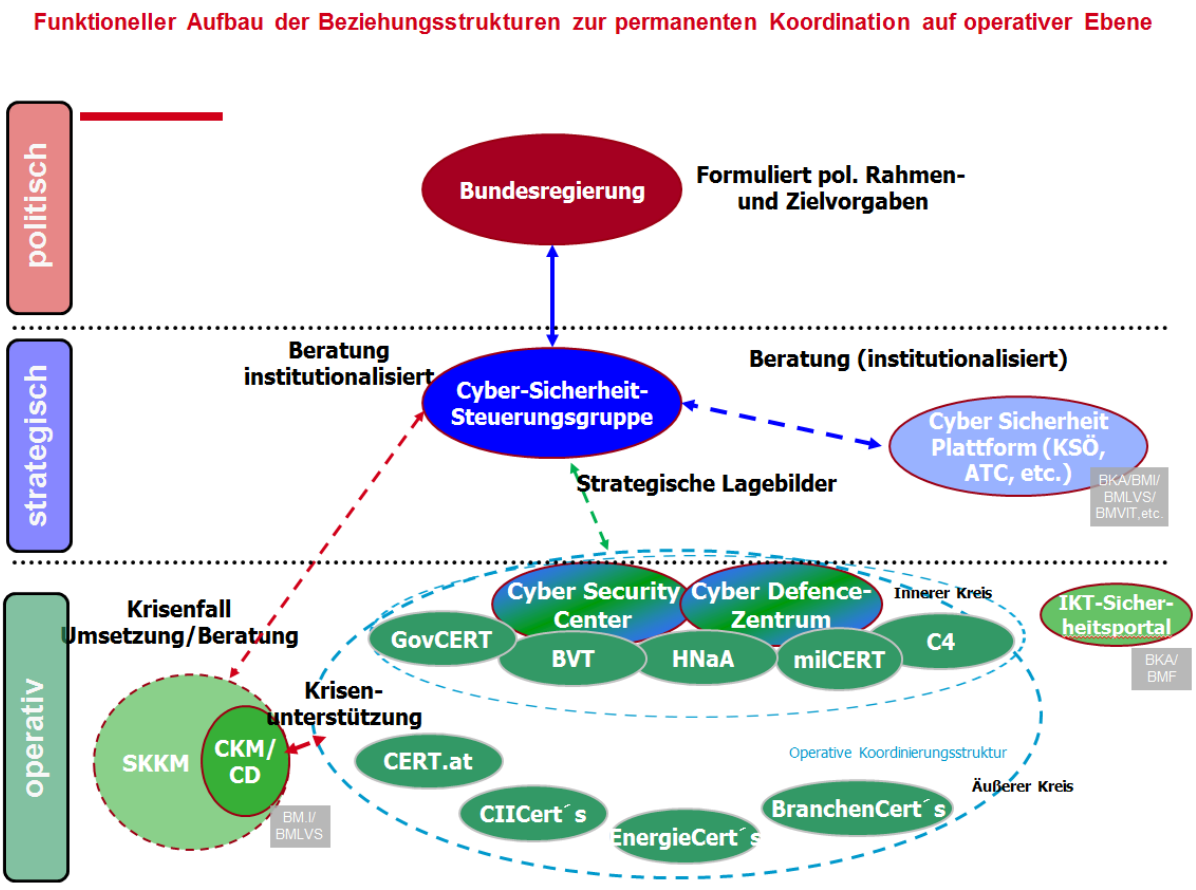


Abbildung 12: Darstellung des funktionellen Aufbaus der Beziehungsstrukturen im Rahmen der Österreichischen Strategie für Cyber Sicherheit (ÖSCS), Quelle: BKA

Die Grundprinzipien einer solchen operativen Struktur umfassen einen inneren Kreis gemäß Regierungsprogramm, der alle Cyber Security Organisationen Österreichs bündelt. Im äußeren Kreis organisieren sich darüber hinaus die Wirtschaftssektoren eigenständig, übernehmen Verantwortung im Sektor, bauen in diesem eigenständige Strukturen auf und fungieren dort quasi als Kommunikationsdrehscheibe und „Single Point of Contact" der Branche. Zum äußeren Kreis dieser operativen Struktur gehören sinnvollerweise auch Organisationen aus dem privaten Bereich (zB Unternehmens- oder Branchen-CERTs, insbesondere aus dem Bereich kritischer Infrastrukturen), die hier eine zentrale Rolle einnehmen.

Ausbau des sektorspezifischen Know-hows

Die aus der ÖSCS abgeleitete operative Struktur soll künftig sicherstellen, dass der Austausch aktueller Informationen rasch erfolgt, hochwertige und vor allem aktuelle Informationen und Analysemethoden in die Erstellung von Cyber Lagebildern einfließen und auf Basis dieser proaktiv gesamtstaatliche Cyber Sicherheitsmaßnahmen abgeleitet bzw. empfohlen werden können. Vor allem aber gewährleistet die operative Struktur die Unterstützung und Koordinierung von gesamtstaatlichen Notfallmaßnahmen im Anlassfall. Entscheidend dabei ist immer auch die Einbindung der bestehenden CERTs im staatlichen wie auch privaten Bereich zu sehen, ebenso wie weiterer Cyber Zentren (wie etwa das Cyber Security Center im BM.I oder das Cyber Defence Zentrum im BMLVS).

Gesamtstaatlicher Mehrwert

Der Vorteil dieses Systems liegt auf der Hand: Damit verfügt Österreich in Zukunft jederzeit über einen aktuellen Cyber Status und kann bei Bedarf entsprechende Maßnahmen vorbereiten, um mögliche Bedrohungen rechtzeitig abzuwehren. Vor allem die sektorspezifischen Stellen haben dabei eine hohe Relevanz. Sie verfügen ebenfalls über diese Informationen und setzen jeweils auf ihren eigenen Bereich abgestimmte Maßnahmen um. Gerade bei größeren Sicherheitsvorfällen übernimmt künftig eine zentrale Stelle die Koordination aller Akteure. Durch klare Aufgaben- und Rollenverteilung und die Stärkung der Kommunikationskette zwischen allen Beteiligten verbessert sich in letzter Konsequenz die Handlungsfähigkeit Österreichs enorm. Eine gemeinsame Koordinationsplattform bildet dafür eine wichtige Basis für den laufenden Erfahrungs- und Informationsaustausch. Um eine bestmögliche Umsetzung dieser Zielstruktur zu gewährleisten, befasst sich unter anderem auch eine eigene Arbeitsgruppe mit dem ordnungspolitischen Rahmen, der dafür erforderlich ist. Vorschläge und Ergebnisse dazu werden im Laufe des Jahres 2015 vorliegen.

Österreich ist auf dem richtigen Weg

Im Anlassfall ist entscheidend, dass die erarbeiteten bzw. vorgeschlagenen Prozesse in der Praxis auch praktikabel sind. Daher wurden jüngst abgehaltene Cyber Sicherheitsübungen (wie etwa die CE.AT 14 im Rahmen der Cyber Europe 2014) bereits vor einem neuen Hintergrund abgehalten. Die Ergebnisse der Übungsszenarien waren jedenfalls sehr

vielversprechend und zeigen, dass Österreich mit diesem Ansatz – auch im internationalen Vergleich – auf einem guten Weg ist.

Internationale Vernetzung immer wichtiger

Wie wichtig in der Abwehr von Cyber Sicherheitsbedrohungen die internationale Vernetzung ist, steht außer Zweifel. Denn nur in den seltensten Fällen lassen sich die Herkunft wie auch das Aktivitätsfeld von Angreifern auf ein geografisches Gebiet einschränken. Neben dem Ausbau von Koordinationsprozessen und –abläufen auf nationaler Ebene setzt sich Österreich im Kontext der internationalen Zusammenarbeit auch stark für weitere vertrauensbildende Maßnahmen ein (sog. Confidence Building Measures). Eine dieser Maßnahme ist beispielsweise die Benennung zentraler Points of Contact in den OSZE Staaten, die im Anlassfall zur Verfügung stehen, wenn es zu Cyber Vorfällen kommt. Österreich selbst verfügt mit dem GovCERT Austria bereits über einen national wie auch international etablierten Kontaktpunkt, der diese Rolle aktiv wahrnimmt.

Ausblick auf 2015: Ein neues Dach für bestehende Kooperationen

Um die Koordination aller Beteiligten in Zukunft noch besser zu gewährleisten soll sich im Laufe des Jahres 2015 eine eigene Cyber Security Plattform (CSP) konstituieren. Aufgabe dieser neuen Plattform wird es sein, unter anderem den periodischen Informationsaustausch zu wesentlichen Fragen der Cyber Sicherheit zwischen Stakeholdern aus Verwaltung, Wirtschaft sowie Wissenschaft und Forschung zu verbessern. Hinzu kommt die Initiierung von Kooperationen zwischen den beteiligten Partnern in den Bereichen Sensibilisierung und Ausbildung sowie Forschung und Entwicklung. Die Plattform soll dabei ein neues Dach für bereits bestehende Kooperationsformate bilden, wie zum Beispiel für: Austrian Trust Circle, das Cyber Sicherheit Forum des Kuratorium Sicheres Österreich, Zentrum für Sichere Informationstechnologie (A-SIT), Cyber Security Austria (CSA) und andere.

Weitere Informationen:

- Download der Österreichischen Strategie für Cyber Sicherheit (ÖSCS).
- Mehr über die ÖSCS auf der Website des Bundeskanzleramts unter: https://www.bka.gv.at/site/7863/default.aspx

9. NATIONALE UND INTERNATIONALE ZUSAMMENARBEIT

Gerade in der digitalen Welt endet Kriminalität nicht an Ländergrenzen. Ganz im Gegenteil: Viele organisierte Angreifer, die es mitunter auf die österreichische IT-Infrastruktur abgesehen haben, kommen aus dem Ausland oder steuern ihre Cyber Angriffe von ebendort. Hier unterscheiden sich die Cyber Angriffe eindrucksvoll von physischen Angriffsformen, die sich an Ort und Stelle ereignen.

Cyber Angriffen sind im wahrsten Sinne des Wortes keine Grenzen gesetzt. Dieser Umstand macht es notwendig, dass VertreterInnen kritischer Infrastrukturen sowohl auf nationaler, als auch auf internationaler Ebene miteinander kooperieren und sich gegenseitig über aktuelle Entwicklungen und potenzielle Gefahren austauschen.

CERT.at sowie GovCERT Austria nehmen regelmäßig an nationalen wie internationalen Übungen teil. Dabei werden Szenarien durchgespielt sowie die Kommunikation und Zusammenarbeit in der Praxis geprobt. Diese Übungen sind – ähnlich wie bei der Feuerwehr – Probeläufe, die den Ernstfall simulieren und darauf vorbereiten sollen. Im Fokus steht dabei die weitere Verbesserung der Problemlösungskompetenz.

Austrian Trust Circle (ATC)
Zur Steigerung der Internetsicherheit hat CERT.at bereits vor einigen Jahren gemeinsam mit dem Bundeskanzleramt den Austrian Trust Circle ins Leben gerufen. Es handelt sich hierbei um Security Information Exchanges in verschiedenen Sektoren der strategischen Informationsinfrastruktur. Der Austrian Trust Circle erlaubt den praxisnahen und vorbehaltlosen Austausch von führenden VertreterInnen kritischer Infrastrukturen (z.B. Banken, Energie- oder Telekommunikationsbetreiber) zu aktuellen Sicherheitsthemen – und gilt dadurch auch international als angesehenes Musterbeispiel für mehr Sicherheit.

Nationale Übungen
In Zukunft soll verstärkt auf nationale Übungen gesetzt werden. Die Schwerpunkte 2015 liegen auf technischer, operationeller sowie strategisch-politischer Ebene. Neben dem erfolgreich etablierten Austrian Trust Circle ist hierbei vor allem die CE.AT 2014 hervorzuheben.

Cyber Excercise CE.AT 2014
Die CE.AT 2014 war die bisher größte nationale sektorübergreifende Cyber Security Übung in Österreich. Sie fand im Rahmen der pan-europäischen Exercise Cyber Europe 2014 statt. Simuliert wurde der Ernstfall – ein Totalausfall des Stromnetzwerks in Österreich – der einen volkswirtschaftlichen Schaden in Höhe von 865 Millionen Euro zur Folge hätte. Innerhalb eines Tages wurden dabei Cyber Angriffe auf die IT-sensiblen Bereiche Telekommunikation, Energie und öffentliche Verwaltung simuliert.

Das Ergebnis war überaus positiv: Die Übung hat gezeigt, dass die Betreiber der österreichischen IT-Infrastruktur einen Cyber Angriff gut koordiniert behandeln können. Für die Zukunft sind weitere Kooperationsmaßnahmen zwischen öffentlicher Verwaltung und Privatwirtschaft geplant, die die Sicherheit und Koordinierung im Ernstfall erleichtern sollen. Der im Bundeskanzleramt angesiedelte Bundespressedienst soll hierbei als koordinierende Medienstelle etabliert werden. Zudem soll in naher Zukunft auch ein sektorenübergreifendes Melde- und Eskalationskonzept erstellt werden.

CERT-Verbund

Neben den Übungen gibt es auch nationale Kooperationen, die sich intensiv mit der IT-Sicherheit Österreichs beschäftigen. So wurde 2011 der CERT-Verbund als Kooperation österreichischer CERTs sowohl aus öffentlichen wie auch privaten Sektoren gegründet. Das Ziel dieser Kooperation ist die Bündelung der bestehenden Ressourcen und die optimale Nutzung des gemeinsamen Know-hows, um eine bestmögliche IKT-Sicherheit gewährleisten zu können.

Internationale Übungen

Mit der Beschließung der Digitalen Agenda für Europa im Jahr 2010 beschäftigt sich die EU verstärkt mit Themen rund um die Cyber Sicherheit. So soll der Austausch und die Kooperation zwischen Behörden und Unternehmen ebenso auf internationaler Ebene gefördert werden, um die Cyber Sicherheit global weiter auszubauen. Neben der europäischen Agentur für Netzwerksicherheit (ENISA), die die „Cyber Europe" Übungen koordiniert, ist auch die NATO in diesem Bereich mit der Cyber Coalition Serie aktiv.

Cyber Europe 2014

Anders als 2012 bestand die Cyber Europe 2014 aus zwei Teilen: Im April gab es eine technische Übung, in der die Fähigkeiten einzelner Teams geprobt wurden. Ihr folgte im Oktober ein zweiter Teil, in dem die Zusammenarbeit zwischen den Teams geprobt wurde (Operational Level Exercise). CERT.at und das GovCERT Austria mussten an diesem Tag sowohl die internationale Koordination wahrnehmen, als auch in der parallel stattfindenden CE.AT 2014 die nationale Rolle spielen.

Cyber Coalition 2014

Auf Initiative der NATO wird diese Übungsserie seit 2008 jährlich mit dem Ziel durchgeführt, Entscheidungsprozesse, technische und operationelle Abläufe sowie die Zusammenarbeit zwischen den Teilnehmenden zu üben. Unter der Leitung des milCERT und Kooperation des GovCERT Austria nahm Österreich erfolgreich an der Cyber Coalition 2014 teil. Diese Übung wurde als Anlass genommen, den Aufbau einer vom Internet komplett unabhängigen Notfall-Kommunikationsinfrastruktur zwischen milCERT und GovCERT Austria zu testen.

Österreichische Expertise auch international gefragt

Österreichs Expertise im Bereich Internet-Sicherheit genießt auch internationale Wertschätzung: So wurde 2014 L. Aaron Kaplan in den Vorstand von FIRST gewählt, der führenden globalen Organisation für Internet-Sicherheit. Mit über 200 Mitgliedern in 48 Ländern der Welt hat sich der Dachverband der CERT-Community (Computer Emergency Response Team) seit seiner Gründung 1990 dem aktuellen und bewerteten Informationsaustausch zu akuten Sicherheitsbedrohungen im Internet verpflichtet. Durch seine weltweit vernetzte Struktur ist FIRST die erste Anlaufstelle rund um das Thema globale Sicherheitsrisiken im Internet.

Weiterführende Informationen zu Organisationen und Behörden im Sicherheitsbereich:

- ÖSCS, http://www.bundeskanzleramt.at/DocView.axd?CobId=50748
- ENISA, http://www.enisa.europa.eu/
- Digitale Agenda für Europa, http://www.bka.gv.at/site/4295/default.aspx
- CyCon, https://ccdcoe.org/cycon/home.html
- Nato, http://www.nato.int/
- ITU, http://www.itu.int/en/Pages/default.aspx
- FIRST, http://first.org

10. SICHERER UMGANG MIT DEM WORLD WIDE WEB

Handlungsempfehlungen, Tipps und Tricks

Immer und überall vernetzt und erreichbar sein, sofort alle Informationen abrufbar, egal wo man sich aufhält. Die digitale Revolution hat sehr viele Annehmlichkeiten zu Tage gebracht. Leider wird aber häufig vergessen, dass die vielen Vorteile, die uns Internet, Smartphones, Tablets und Co. beschert haben, einen hohen Preis haben: Themen wie Cyber Sicherheit und Fragen rund um die gläsernen KonsumentInnen beschäftigen unsere Gesellschaft mehr denn je.

Auch wenn es vermehrt Fälle von Internetbetrug, Phishing, Schadstoffsoftware, Identitätsdiebstahl, Infektionen, Störfälle, Hacking, Spionage etc. gibt, sind KonsumentInnen nicht völlig der Willkür von Cyber Angreifern ausgesetzt. Es gibt hilfreiche Tipps und Dienste, die sich mit diesen Themen befassen und die – bis zu einem gewissen Grad – Sicherheit bieten. Fakt ist aber, dass es keine 100%-ige Sicherheit gibt, weder in der realen noch in der digitalen Welt. KonsumentInnen müssen sich selbst die Frage stellen, wogegen sie sich schützen wollen und entsprechende Maßnahmen dahingehend setzen.

Die wichtigsten Empfehlungen

Bereits durch wenige, einfach umzusetzende Maßnahmen lassen sich Bedrohungspotenziale verringern oder gänzlich vermeiden. Egal ob am Laptop, Tablet, Netbook, Smartphone etc. - unter Einhaltung der folgenden Grundregeln steigt die Cyber Sicherheit deutlich an:

Betriebssysteme und Anwendungen regelmäßig updaten

Wenn es um Hardware geht, wollen viele immer auf dem neuesten Stand der Technik sein. Sobald es sich aber um Software Aktualisierungen handelt, sind viele nachlässig. Dabei sind die meisten Updates schnell gemacht und schützen wirksam. Ohne aktualisierte Software kann die Hardware noch so modern und aktuell sein, gegen Cyber Angriffe kann sie wenig bis gar nicht schützen. Software Updates sind zudem wahre Allrounder, schließen sie nicht nur eventuelle Sicherheitslücken, sondern bieten kleine Systemverbesserungen und reparieren Fehler.

Nicht benötigte Software und Dienste deaktivieren

Ist ein Programm nicht installiert, kann es auch nicht gehackt werden. So banal dies klingt, so erfolgversprechend ist es auch. Wenn man Java nicht braucht, dann weg damit vom PC. Geht das nicht, so sollte man wenigstens „click-to-run" aktivieren: Diese Funktionalität im Browser erschwert den Exploit-Packs massiv die Arbeit – und macht im Fall von Flash auch so manche werbeüberladene Webseite wieder erträglich. Gerade Funktionen wie GPS, Bluetooth und WLAN sind ein Schlupfloch für schadhafte Software und vereinfachen Datenspionage. Der Datenaustausch über WLAN oder Bluetooth ist oft nur mangelhaft gesichert und kann relativ leicht ausspioniert werden. Indem diese Funktionen eingeschaltet bleiben, kann schadhafte Software auf das (mobile) Endgerät zugreifen. Deshalb sollte WLAN nur dann eingeschaltet

werden, wenn auf ein lokales WLAN-Netzwerk zugegriffen wird. Ebenso sollte die Bluetooth-Funktion nur genutzt werden, wenn sie unmittelbar benötigt wird. Das kann nicht nur vor unerwünschten Angriffen bewahren, sondern spart zudem auch Energie.

Virenschutzprogramme installieren

Anti-Viren Programme sind ein klassisches und zuverlässiges Mittel, um die Cyber Sicherheit zu erhöhen. Virenschutzprogramme durchsuchen die Software nach Infektionen aller Art (Viren, Würmer und Trojaner) und blockieren bzw. beseitigen diese, wenn möglich. Doch auch bei Anti-Viren Software gilt: Nur regelmäßige Software Updates stehen für die gewünschte Sicherheit. Eine einmalige Installation der Software ist langfristig kein Sicherheitsgarant.

Achtung: Auch ein aktuelles AV-Programm macht den PC nicht unverwundbar. Dies lässt sich gut mit den Sicherheitsfeatures aktueller Autos vergleichen: ABS, ESP, Airbags oder Gurte verringern die Chance auf einen Unfall oder minimieren den Schaden eines solchen, aber können nicht jeden Fahrfehler kompensieren.

Gesunder Menschenverstand

Oft genug ist der Mensch das schwächste Glied in der Verteidigungskette. Ein Angreifer braucht keine technisch ausgefeilten Programme, wenn er sein Opfer dazu überreden kann, selbst Sicherheitsmechanismen auszuschalten, Warnhinweise wegzuklicken oder die Schadsoftware selber zu installieren. Wir lernen ganz bewusst unseren Kindern, wie sie sich auf der Straße verhalten sollten, dass sie nicht jedem vertrauen und nicht alles annehmen sollten. Ganz ähnliche Prinzipien gelten auch für das Internet.

Vorsicht bei öffentlich zugänglichen WLAN-Hotspots

Flughäfen, Hotels, öffentliche Plätze – mittlerweile wird überall die Möglichkeit geboten (kostenlos) einen WLAN Hotspot zu nutzen. Dieser Service wird von vielen als sehr angenehm empfunden, jedoch sollte man sich nicht auf alles verlassen, was gratis ist. Solche Hotspots bieten Angreifern Zugang auf den Netzwerkverkehr: Es ist daher essentiell, dass InternetnutzerInnen keine Passwörter im Klartext übertragen und sie die Kommunikationspartner authentisieren. Am besten wäre es, solche Hotspots rein als Trägermedium für ein Virtual Private Network (VPN) zu nutzen: Dann haben Mitlauscher am Funk keinen Einblick in die Kommunikation.

Apps aus sicheren Quellen beziehen

Wenn Apps bewusst schadhaft sind – sogenannte Malware – speichern sie Informationen über das Benutzerverhalten und geben Benutzerdaten (gewinnbringend) an Dritte weiter. Apps sollten daher nur aus einem offiziellen App-Store bezogen werden. Eine 100%-ige Garantie für schadfreie Apps ist das zwar nicht, jedoch hat man über einen offiziellen Store zumindest die Möglichkeit Apps innerhalb eines gewissen Zeitraums wieder zu deinstallieren. Gratis-Apps bzw. deren Zugriffsberechtigungen sollten generell hinterfragt werden.

Vermeiden sie unnötige Softwarebeigaben

Aktuell ist das „pay-per-install" Modell zur Subventionierung von an sich legitimen Produkten sehr populär. Dabei zahlen die Hersteller von Software Geld an diejenigen, die ihre Programme auf möglichst viele PCs installieren. Das reicht von Testversionen von Antiviren-Software auf neuen PCs bis hin zu Beigaben beim Download von Gratis-Software. So muss man etwa beim Download des Flash-Plugins oder bei vielen Programmen von Softwaresammlungen explizit die Mitinstallation von dubioser Software abwählen.

Endgeräte nicht unbeaufsichtigt lassen und Bildschirmsperre aktivieren

Mobile Endgeräte, dazu zählen neben Smartphones auch Tablets & Co., werden, im Gegensatz zur Brieftasche, gerne zur Schau gestellt. So sind sie nicht nur im Blickfeld des Eigentümers, sondern auch fremder Personen und wie man weiß, macht Gelegenheit Diebe. Viele KonsumentInnen unterschätzen nach wie vor die Wirkung von Bildschirmsperren. Der Code/Muster muss zwar bei jeder Aktion erneut eingegeben werden, trägt dafür aber wesentlich zum Schutz des Geräts und der darauf abgespeicherten Daten bei. Im Zweifelsfall sind PIN-Codes einem „Wisch-Muster" als Bildschirmsperre vorzuziehen, da diese weniger gut ausgespäht werden können bzw. nicht so einfach nachzuverfolgen sind.

Die IT-Sicherheit beschäftigt nicht nur PrivatanwenderInnen, sondern ist auch ein großes Thema bei Unternehmen. Dort ist es aber deutlich schwieriger, die Handlungsempfehlungen in wenigen Punkten zusammenzufassen. Die Anforderungen eines generischen KMU unterscheiden sich deutlich von denen eines Großunternehmens. Auch muss sich ein High-Tech Startup anders schützen als ein Installateur-Betrieb. Während ein KMU primär mit seinem/r IT-BetreuerIn das Thema Sicherheit und Business Continuity klären muss, gibt es für größere Unternehmen eine Reihe von Standards, welche die sinnvollen Maßnahmen darlegen. Diese wären etwa das A-SIT Sicherheitshandbuch, der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder ISO 27k. In diesem Bereich helfen auch gerne entsprechende ExpertInnen von Consultingfirmen.

Weiterführende Informationen zum Thema Sicherheit unter:

- www.onlinesicherheit.gv.at
- Öffentliche Sicherheit, ein Magazin des Innenministeriums
- Computer Emergency Response Team: Cert.at

11. CYBER SECURITY TRENDS – WAS BRINGT DIE ZUKUNFT?

Wohin genau sich die Welt des Internets, der IT und damit der Cyber Security entwickelt, kann wohl niemand mit Sicherheit sagen. Dennoch können Trends identifiziert werden, die IT-Verantwortliche auch in Zukunft beschäftigen und vor neue Herausforderungen stellen werden.

Mobilität nimmt weiter zu
Überall und ständig erreichbar sein. Der Trend der zunehmenden Mobilität, auch "Computing Everywhere" genannt, ist nach wie vor ein steigender. Neben den damit einhergehenden Sicherheitsrisiken ändert sich auch zunehmend das Verhalten der BenutzerInnen. Die Anforderungen an Benutzerfreundlichkeit, Qualität und ganzheitliches Service nehmen zu, gleichzeitig werden dadurch neue Angriffstore geöffnet und die Gefahr der missbräuchlichen Verwendung der immer größer werdenden Datenmenge steigt.

Auch der Trend der Anwendungen von Cloud-Lösungen setzt sich fort. Die Cloud wird sowohl im privaten als auch im Unternehmensbereich verwendet, um den Mobilitätsanforderungen gerecht zu werden. Die steigende Verbreitung von Smartphones, Tablets und leistungsstarke Datennetze sowie soziale Netzwerke sind Treiber dieses Trends. Der Bedarf an sicheren Cloud-Lösungen und innovativen Mechanismen zum Schutz dieser Daten nimmt damit auch in Zukunft zu.

Das "Internet der Dinge" weitet sich aus
Die zunehmende Entwicklung hin zum „Internet of Things" (IoT), also die Vernetzung von Gegenständen wie Autos, Haushaltsgeräte etc. mit dem Internet wird zahlreiche neue Herausforderungen für die Cyber Sicherheit mit sich bringen. Laut einer Studie von Gartner wird die Zahl der mit dem Internet verbundenen Geräte von 4,9 Milliarden im Jahr 2015 auf 25 Milliarden im Jahr 2020 ansteigen. Dieser Trend, der im deutschsprachigen Raum auch unter dem Begriff „Industrie 4.0" subsummiert wird, umfasst dabei alle Industrien, Branchen und auch den privaten Bereich.

Der größte Treiber hinsichtlich der Anzahl der verbundenen Geräte ist laut Gartner der Consumer Bereich. 2014 gibt es hier 2,2 Milliarden Geräte, 2020 sind es bereits 13 Milliarden. Die höchste Steigerungsrate ist jedoch in der Auto-Branche zu erwarten, hier steigt die Anzahl der vernetzten Geräte allein von 2014 auf 2015 bereits um 96% (siehe dazu die folgende Abbildung).

Table 1: Internet of Things Units Installed Base by Category

Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2.874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

Source: Gartner (November 2014)

Abbildung 13: Übersicht über die Anzahl der verbundenen Geräte im Consumer Bereich im Zeitverlauf, Quelle: Gartner

Das „Internet der Dinge" schafft zahlreiche neue, miteinander vernetzte Plattformen, Lösungen und Anwendungen. Damit einhergehend steigen die Komplexität der IKT-Architektur und somit auch die Anforderungen an dementsprechende Sicherheits-Infrastrukturen.

Anwendungen müssen Risiken proaktiv erkennen

Es scheint nun fast so, als würden die zu erwartenden IT-Trends das Internet zu einem zunehmend unsichereren Ort machen. Eine 100%-ige Sicherheit im Netz wird auch nie zu gewährleisten sein. Es sind jedoch Trends zu erkennen, dass sich auch die Maßnahmen der Internet-Sicherheit weiterentwickeln. Das Aufkommen und die zunehmende Einführung integrierter und ganzheitlicher Cyber Security Lösungen zählen hier ebenso dazu, wie die Entwicklung von proaktiven und risikobewussten Anwendungen. Ziel dabei ist, dass Anwendungen oder beispielsweise Apps Risiken von sich aus erkennen, situativ darauf reagieren und damit eine Art Selbstschutz besitzen.

Entwicklung eines „digitalen Bauchgefühls"

Neben all den aufgezählten Trends ist aber wohl der folgende Trend ein ewig gültiger und vor allem sehr wichtiger: Die Verwendung des gesunden Hausverstands im Umgang mit IT und den eigenen Daten. Nur wenn eine gewisse Grundskepsis und ein Bewusstsein für das eigene Tun und Handeln im Netz entwickelt wird, können Risiken und Angriffe minimiert und die Vorteile der IT ausgeschöpft werden.

12. ABKÜRZUNGSVERZEICHNIS

Abkürzung	Erklärung
ABS	Antiblockiersystem
AbwA	Abwehramt
ACOnet	Austrian Academic Computer Network (österreichisches Wissenschafts-, Forschungs- und Bildungsnetzwerk)
App	Application
A-SIT	Zentrum für Sichere Informationstechnologie
ATC	Austrian Trust Circle
AV Programm	Anti-Viren Programm
BIP	Bruttoinlandsprodukt
BKA	Bundeskanzleramt
BM.I	Bundesministerium für Inneres
BMF	Bundesministerium für Finanzen
BMLVS	Bundesministerium für Landesverteidigung und Sport
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BPD	Bundespressedienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
CE.AT	Übung Cyber Europe Austria
CERT	Computer Emergency Response Team
CII	Critical Infrastructure Information
CMS	Content Management System
CSA	Cyber Security Austria
CSIS	Center for Strategic and International Studies
CSP	Cyber Security Plattform
CyCon	NATO Cooperative Cyber Defence Centre of Excellence
DDoS	DistributedDenial of Service Attack
DNS	Domain Name System
DoS	Denial-of-Service Attack
ENISA	Europäische Agentur für Netzwerksicherheit
ESP	Elekronisches Stabilitätsprogramm
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
GovCERT Austria	Computer Emergency Response Team für die öffentliche Verwaltung
GPS	Global Positioning System
HNaA	Heeresnachrichtenamt
IDS	Intrusion Detection System
IKT	Informations- und Kommunikationstechnologie
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
ISO	International Organization for Standardization

Abkürzung	Erklärung
ITU	International Telecommunication Union
KII	Kritische Informations-Infrastruktur
KSÖ	Kuratorium Sicheres Österreich
LAN	Local Area Network
milCERT	militärisches Computer Emergency Response Team
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
NTP	Network Time Protocol
OpenSSL	Open Secure Sockets Layer
ÖSCS	Österreichische Strategie für Cyber Sicherheit
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PC	Personal Computer
PIN	Persönliche Identifikationsnummer
PUP	potenziell unterwünschte Programme
SIR	Security Intelligence Report, herausgegeben von Microsoft
SKKM	Staatliches Krisen- und Katastrophenschutzmanagement
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discovery Protocol
SSL	Secure Sockets Layer
STS	Staatssekretär/in
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPAD	Windows Proxy Auto-Detection