Bundesministerium
des Innern



# Evaluierung der Cybersicherheitsstrategie für Deutschland 2021

**Inhaltsverzeichnis**

# 1 Zusammenfassung

Mit der Evaluierung der am 8. September 2021 vom Bundeskabinett verabschiedeten Cybersicherheitsstrategie für Deutschland (CSS) 2021 kommt das BMI einer in Ziffer 9.4 der CSS enthaltenen Verpflichtung nach. Ziel der Evaluierung ist es, den aktuellen Stand der Umsetzung der strategischen Ziele und Maßnahmen der CSS darzustellen.

Hierfür wurde in einem mehrstufigen Verfahren ein möglichst breites Stimmungsbild der Ressorts, des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der betroffenen Stakeholder aus Ländern, Wirtschaft, Wissenschaft und Zivilgesellschaft eingeholt. Die Beteiligten erhielten jeweils einen auf ihre Zuständigkeiten zugeschnittenen Online-Fragebogen.

Die Auswertung zeigt, dass ein großer Teil der Maßnahmen der CSS umgesetzt wurde oder sich zumindest in Umsetzung befindet. Dies entspricht auch der Wahrnehmung der befragten Stakeholder. Die meisten umgesetzten Maßnahmen befinden sich im Handlungsfeld 2 der CSS (35%), das die Cybersicherheit der Wirtschaft zum Gegenstand hat. Kritik wurde u.a. an den nationalen Zertifizierungen, der mangelnden Einbeziehung kleiner und mittlerer Unternehmen (KMU) sowie hinsichtlich der Rolle des Nationalen Cyber-Sicherheitsrats (NCSR) geäußert.

Noch am Anfang steht die Umsetzung vieler Maßnahmen in Handlungsfeld 3, das sich mit der Kompetenzverteilung und Zusammenarbeit der staatlichen Akteure befasst. Hier befinden sich noch 38% der Maßnahmen in Planung und 46% in Umsetzung. Begründet werden könnte dies damit, dass die zur Stärkung der Bund-Länder-Zusammenarbeit angestrebte Grundgesetz-Änderung nicht realisiert werden konnte und mit den aktuellen Mehrheitsverhältnissen nicht mehr umgesetzt werden kann und daher nach Alternativen gesucht wird.

Auffällig ist, dass zum Teil bei einzelnen Maßnahmen - insbesondere im Handlungsfeld 1, das die Gesellschaft in den Fokus nimmt - eine Diskrepanz zwischen der Einschätzung der federführenden Ressorts und der Wahrnehmung der beteiligten Stakeholder festzustellen ist. Dies betrifft etwa die Fortentwicklung der Telematikinfrastruktur oder den Umgang mit Schwachstellen („Coordinated Vulernability Disclosure“). Insbesondere mit den Maßnahmen, die als „abgeschlossen“ gelten, von den Experten aber mit „nicht umgesetzt“ bewertet werden, sollte eine kritische Auseinandersetzung erfolgen.

# 2 Einleitung

## 2.1 Evaluierungsauftrag

Die vom Bundeskabinett am 8. September 2021 verabschiedete Cybersicherheitsstrategie für Deutschland 2021 ersetzt die CSS aus dem Jahr 2016 und bildet den ressortübergreifenden strategischen Rahmen für Aktivitäten der Bundesregierung im Bereich der Cybersicherheit für den Zeitraum von 2021 bis 2026. Es handelt sich dabei um eine Fortschreibung, die inhaltlich auf den Strategien der Jahre 2011 und 2016 aufbaut und gleichzeitig neue Schwerpunkte setzt. Die bisherigen Strategien wurden jeweils vor Ablauf ihres Geltungszeitraums einer Evaluierung unterzogen. Entsprechend sieht auch die CSS 2021 eine Evaluierung spätestens nach vier Jahren vor (vgl. Ziffer 9.4 der CSS 2021). Diese Evaluierung soll die Erreichung der gesteckten Ziele überprüfen und einen Ausblick für die Fortschreibung geben. Das Bundesministerium des Innern (BMI) hat als federführendes Ressort die Koordination übernommen. Die Bundesressorts, das BSI, Vertreter aus Ländern, Wirtschaft, Wissenschaft und Zivilgesellschaft wurden über den NCSR in den Prozess einbezogen.

## 2.2 Gegenstand der Evaluierung

Die CSS 2021 beschreibt die grundsätzliche Ausrichtung der Cybersicherheitspolitik der Bundesregierung in Form von Leitlinien, Handlungsfeldern sowie strategischen Zielen. Die vier Handlungsfelder (HF) lauten:

- HF 1: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

  Hier steht die Gesellschaft im Fokus. Die Menschen in Deutschland sollen die Chancen digitaler Technologien nutzen und sich sicher und selbstbestimmt in einer digitalen Umgebung bewegen können.

- HF 2: Gemeinsamer Auftrag von Staat und Wirtschaft

  Dieses Handlungsfeld ist darauf ausgerichtet, die Cybersicherheit in der Wirtschaft insgesamt und der Kritischen Infrastrukturen im Besonderen zu sichern und zu stärken. Besonderes Augenmerk liegt hierbei auf kleinen und mittleren Unternehmen.

- HF 3: Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur

  Hier werden die staatlichen Akteure adressiert. Konkret geht es um die Kompetenzverteilung und Zusammenarbeit zwischen den Akteuren, die Fortentwicklung von deren Fähigkeiten und Befugnissen sowie um neue Herausforderungen für staatliche Akteure im Cyberraum.

- HF 4: Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik

Die Gewährleistung eines hohen Cybersicherheitsniveaus in Deutschland erfordert eine aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik. Zentral ist dabei das Engagement Deutschlands in der EU und der NATO.

Jedem der vorgenannten Handlungsfelder sind strategische Ziele (8.1.1. bis 8.4.7.) in der CSS 2021 zugewiesen. Für jedes strategische Ziel wird in der CSS detailliert dargestellt, was konkret erreicht werden soll und anhand welcher Kriterien die Bundesregierung die Erreichung des Ziels überprüfen wird.

## 2.3 Ziel der Evaluierung

Das Hauptziel der Evaluierung besteht darin, den aktuellen Stand der Umsetzung der strategischen Ziele und Maßnahmen der CSS darzustellen. Die Ergebnisse sollen Handlungsempfehlungen für eine Fortschreibung der CSS liefern.

## 2.4 Methode und Konzeption

Für die vorliegende Evaluierung wurde in einem mehrstufigen Verfahren ein möglichst breites Stimmungsbild der Ressorts und betroffenen Stakeholder eingeholt, um aussagekräftige Evaluierungsergebnisse ermitteln zu können. Konkret wurde wie folgt vorgegangen:

- Ressortabfrage: Die Ressorts mit federführender Zuständigkeit für Maßnahmen in der CSS wurden aufgefordert, den Umsetzungsstand der ihnen zugewiesenen strategischen Ziele zu bewerten. Dazu wurde ein Online-Fragebogen erstellt, der für jedes strategische Ziel anhand der in der CSS 2021 zur Überprüfung der Zielerreichung definierten Kriterien konkrete Aussagen enthält. Zu jeder der Aussagen konnte der aktuelle Stand der Umsetzung auf einer mehrstufigen Antwortskala (von „abgeschlossen“, „in Umsetzung“, „in Planung“ bis „verworfen“) angegeben werden.
- Stakeholder-Befragung: Experten von Ländern, Wirtschaft, Wissenschaft, Zivilgesellschaft und das BSI erhielten ebenfalls einen jeweils auf sie zugeschnittenen, strukturierten Online-Fragebogen. Die Einladung zur Teilnahme erfolgte durch das Statistische Bundesamt mit einem individualisierten Link. Abgefragt wurde hier, inwiefern die strategischen Ziele aus Sicht der Stakeholder erreicht wurden und welche Herausforderungen aus ihrer Sicht bestehen. Die von den Stakeholdern zu bewertenden Aussagen bezogen sich – wie bei der Ressortabfrage – auf die in der CSS 2021 angelegten Kriterien zur Zielerreichung. Sie wurden gebeten, den Grad ihrer Zustimmung auf einer vorgegebenen Antwortskala („trifft zu“, „trifft eher zu“, „teils, teils“ , „trifft eher nicht zu“, „trifft nicht zu“) anzugeben.

- Auf Seiten der Länder koordinierte Hessen, das die Länder auch im NCSR vertritt, die Beantwortung des Fragebogens. Die Beantwortung seitens der Wissenschaft erfolgte über die Wissenschaftliche AG des NCSR. Für die Wirtschaft wurden die Verbände und Vereine, die Mitglieder im NCSR sind, befragt (DIHK, CSSA e.V., BDI, Bitkom, BDEW, UP KRITIS). Für die Zivilgesellschaft wurden neben interface als Mitglied des NCSR auch der Chaos-Computer-Club e. V., Deutschland Sicher im Netz e.V., der Verbraucherzentrale Bundesverband sowie die Gesellschaft für Informatik e.V. befragt.
- Datenanalyse: Die Einschätzungen zum Umsetzungsstand wurden ausgezählt, Zusammenhangsanalysen erstellt und die Freitextantworten inhaltlich ausgewertet, um Trends, Erfolgsfaktoren und Hemmnisse zu identifizieren.

Die Fragebögen wurden im Mai versandt und die Daten im Juni ausgewertet. Die getroffenen Bewertungen wurden somit nach Stand Juni 2025 abgegeben.

## 2.5 Art und Inhalt der Rückmeldungen

Alle 21 federführenden Ressorts haben ihre Rückmeldungen fristgerecht eingereicht. 5 Wirtschaftsverbände und 3 zivilgesellschaftliche Vereine haben an der Befragung teilgenommen. Aus der Wissenschaftlichen AG des NCSR gab es 2 Rückmeldungen. BSI und die Länder (Hessen stellv. für alle Länder) gaben jeweils einen Fragebogen ab. Die Stakeholder-Beteiligung zeigte somit eine gute Abdeckung aller relevanten gesellschaftlichen Gruppen.

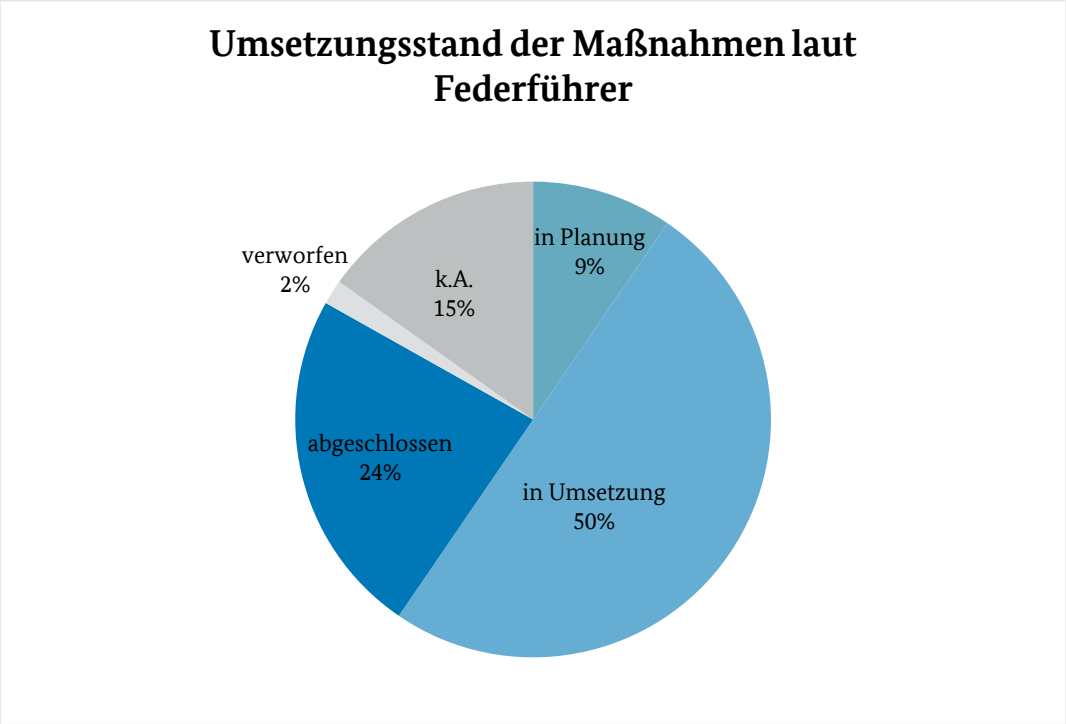
Die Ergebnisse verdeutlichen sowohl die Fortschritte als auch den noch bestehenden Handlungsbedarf in einzelnen Bereichen. Insbesondere die differenzierten Bewertungen der Stakeholder tragen dazu bei, die Wirkung der Maßnahmen im gesellschaftlichen Kontext einzuschätzen.

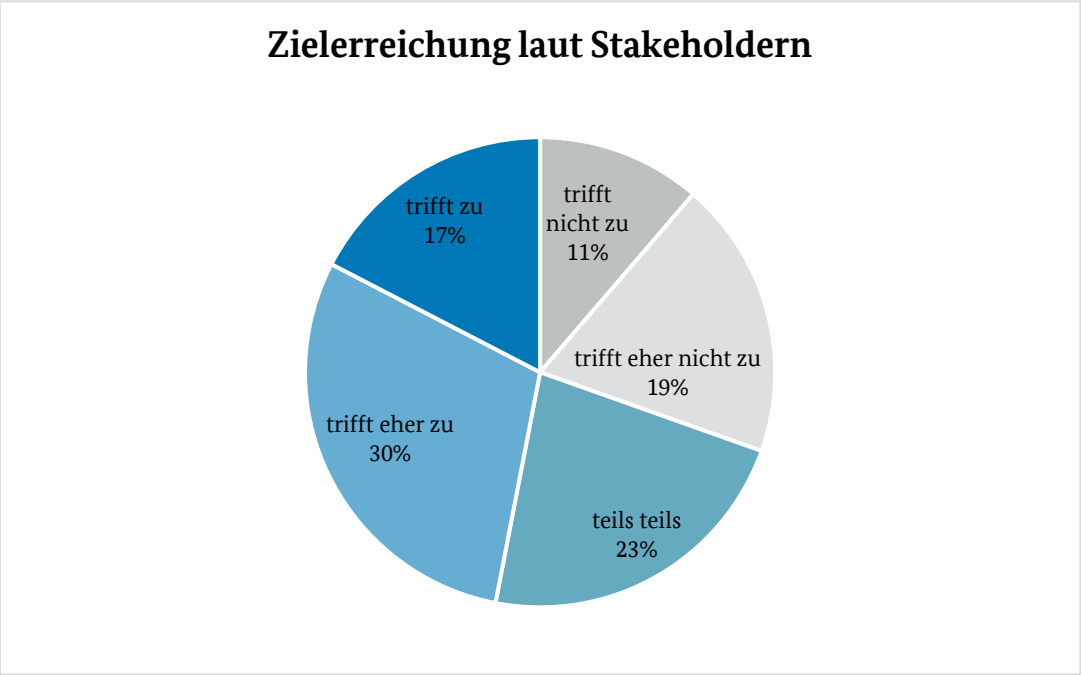
# 3 Auswertung der Ergebnisse

Die Auswertung der im Rahmen der Evaluierung gewonnenen Ergebnisse erfolgte in zwei Schritten. Zunächst wurde eine quantitative Auswertung zum Umsetzungsstand der in der CSS enthaltenen Maßnahmen vorgenommen und grafisch dargestellt. In einem weiteren Schritt erfolgte eine qualitative Auswertung der Freitextantworten der befragten Ressorts und Stakeholder zu den einzelnen Maßnahmen.

## 3.1 Quantitative Auswertung

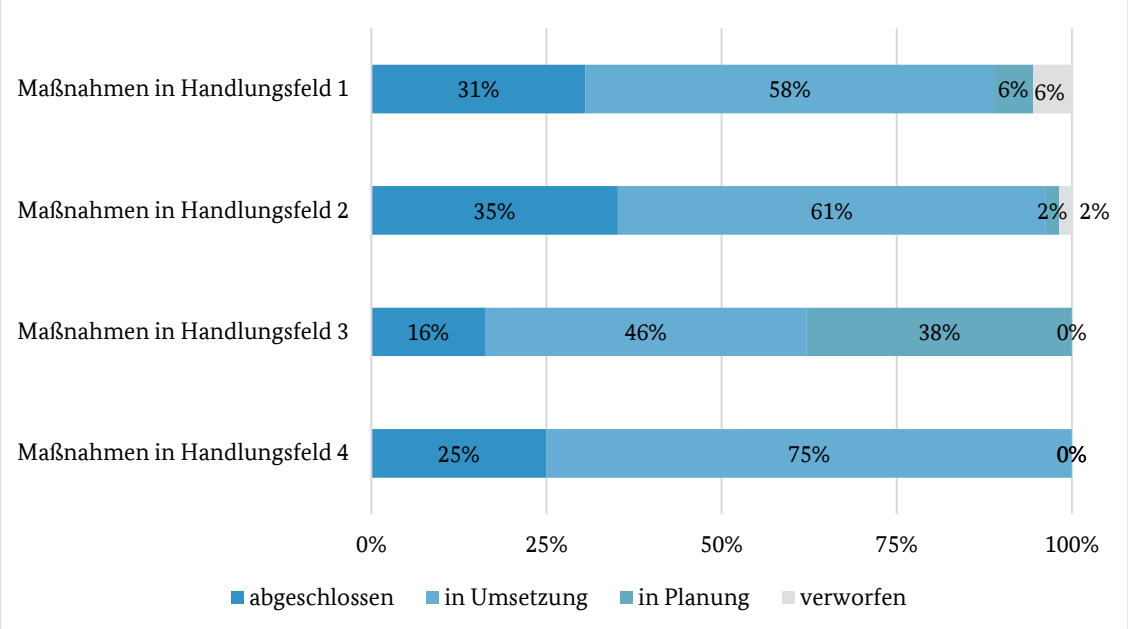
Insgesamt wurden 178 Maßnahmen untersucht. Der aktuelle Umsetzungsstand laut den federführenden Ressorts gliedert sich wie folgt:






Diese Auswertung zeigt, dass laut den Ressorts ein großer Teil der Maßnahmen umgesetzt wurde (24%) oder sich in der Umsetzung befindet (50%) und dies bei den Fachexperten auch wahrgenommen wird.

### 3.1.1 Clusterung nach Handlungsfeldern und Umsetzungsstatus




Im Handlungsfeld 2 „Gemeinsamer Auftrag von Staat und Wirtschaft“ ist der höchste Anteil von abgeschlossenen Maßnahmen mit 31 % zu verzeichnen – Beispielsweise ist Anzahl der

Nutzer des Unterstützungsangebots des BSI nachweislich gestiegen (Maßnahme 8.2.2.4) und es wurde ein interministerieller Ausschuss IKT-Standardisierung für die Cybersicherheit gegründet (Maßnahme 8.2.6.3) . Im Handlungsfeld 2 befindet sich außerdem der Großteil der Maßnahmen bereits in Umsetzung (58 %) wie beispielsweise die Steigerung der Anzahl der Angebote der Initiative Wirtschaftsschutz und ihrer Partner für Unternehmen, Forschungseinrichtungen und Kommunen (Maßnahme 8.2.2.6) oder die Etablierung eines Information-Sharing-Portals (Maßnahme 8.2.3.1).

Ähnlich ist das Bild in Handlungsfeld 4 mit 25 % abgeschlossen (Beispiel: Der Cyberkapazitätsaufbau ist in internationalen Gremien als Thema etabliert und wurde in relevanten Policy-Dokumenten verankert [Maßnahme 8.4.5.1] ; die Anzahl der polizeilichen Aufbauhilfemaßnahmen für ausländische Sicherheitsbehörden zur Bekämpfung grenzüberschreitender Cyberkriminalität ist gestiegen. [Maßnahme 8.4.6.2]) und 75 % in Umsetzung befindlichen Maßnahmen (Beispiel: NIS-Richtlinie wird überarbeitet und diese neue NIS-Richtlinie 2.0 in nationales Recht umgesetzt [Maßnahme 8.4.1.2]).

Im Handlungsfeld 3 „Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur“ befinden sich zahlreiche Maßnahmen zumindest bereits in Planung (38 %; Beispiel: Das „Kompetenzzentrum Operative Sicherheitsberatung Bund“ des BSI wurde eingerichtet und hat seine Arbeit aufgenommen) und in Umsetzung (46 %; Beispiel: Die Grundlagen für den behördenübergreifenden Austausch von Informationen im Cyber-AZ wurden angepasst.), was das hohe Potenzial verdeutlicht.

Zwei verworfene Maßnahmen sind in Handlungsfeld 1 „Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung“ zu verorten. Die Gründe dafür sind vor allem haushalterischer Natur. So wurde im Bereich der Gewährleistung sicherer elektronischer Identitäten das Projekt „Smart-eID“ zwar bis zur Produktreife entwickelt, aber aufgrund von Wirtschaftlichkeitsbetrachtungen nicht in Betrieb genommen.

Im Handlungsfeld 1 wurde außerdem die Maßnahme 8.2.1.1 verworfen : „Erstellung eines Konzeptpapiers zu den Beratungsprozessen der Bundesregierung durch den NCSR“. Das Gremium hat sich im Verlauf der LP auf alternative Elemente zur Weiterentwicklung geeinigt und diese auch umgesetzt.

### 3.1.2 Korrelation Umsetzungsstatus und Zustimmung

| | | Wahrnehmung laut Fachexperten | | | | |
|---|---|---|---|---|---|---|
| | | Trifft zu | Trifft eher zu | Teils, teils | Trifft eher nicht zu | Trifft nicht zu |
| **Umsetzungsstatus laut FF** | abgeschlossen | 30% | 52% | 7% | 11% | 0% |
| | in Umsetzung | 14% | 22% | 30% | 25% | 9% |
| | in Planung | 11% | 11% | 11% | 22% | 45% |
| | Verworfen | 0% | 0% | 33% | 0% | 67% |

Von den Ressorts für „abgeschlossen“ erklärte Maßnahmen wurden von Experten aus Ländern, Wirtschaft, Wissenschaft und Zivilgesellschaft sowie dem BSI in den meisten Fällen auch als umgesetzt wahrgenommen (82 % stimmen ganz oder eher zu). Das zeigt, dass umgesetzte Maßnahmen auch tatsächliche Außenwirkung haben.

In Umsetzung befindliche Maßnahmen wurden von den Experten teilweise als bereits umgesetzt wahrgenommen (35 % stimmen ganz oder eher zu), teilweise allerdings noch nicht als umgesetzt wahrgenommen (34 % stimmen nicht oder eher nicht zu). Bei Maßnahmen, die in Planung sind, gaben die Experten in den meisten Fällen an, bisher auch keine Umsetzung wahrgenommen zu haben (66 % stimmen nicht oder eher nicht zu). Begründet werden könnte dies mit der regierungsseitigen Außenkommunikation bei der Planung und Umsetzung der Maßnahmen. Es könnte in Erwägung gezogen werden, verstärkt über laufende Projekte bzw. Gesetzgebungsverfahren zu informieren.

### 3.1.3 Besondere Auffälligkeiten

Folgende Maßnahmen heben sich durch eine Diskrepanz zwischen administrativem Umsetzungsstand und der Wahrnehmung der Stakeholder hervor und sollten bei der weiteren Strategieentwicklung berücksichtigt werden:

*Abgeschlossene Maßnahmen mit kritischer Expertenbewertung:*

HF 1: In der kontinuierlichen Fortentwicklung der Telematikinfrastruktur sind sowohl die Nutzung stationärer Anwendungen als auch neu eingeführte mobile Nutzungsmöglichkeiten von IT-Anwendungen für Versicherte und Leistungserbringer zu jedem Zeitpunkt sicher. (8.1.7.2)

HF 1: Es besteht Rechtssicherheit für das Suchen und Finden von Sicherheitslücken. (8.1.8.1)

HF 2: Förderprogramme, die auch auf Unterstützung der IT-Sicherheit von kleinen und mittleren Unternehmen, einschließlich Handwerk und freien Berufen, abzielen (insbesondere „go-digital“ und „Digital Jetzt“), sind bekannt und werden nachgefragt. (8.2.4.3)

Obwohl das federführende Ressort die Maßnahme 8.1.7.2 „In der kontinuierlichen Fortentwicklung der Telematikinfrastruktur sind sowohl die Nutzung stationärer Anwendungen als auch neu eingeführte mobile Nutzungsmöglichkeiten von IT-Anwendungen für Versicherte und Leistungserbringer zu jedem Zeitpunkt sicher“ als „abgeschlossen“ eingestuft hat, wurde dies von den Experten insgesamt als „eher nicht umgesetzt“ bewertet.

Ebenfalls in Handlungsfeld 1 hat das federführende Ressort beim Ziel 8.1.8 „Verantwortungsvoller Umgang mit Schwachstellen – CVD fördern“ die Maßnahme 8.1.8.1. „Es besteht Rechtssicherheit für das Suchen und Finden von Sicherheitslücken“ als „abgeschlossen“ angesehen, während dieser von den Experten aber als „eher nicht umgesetzt“ bewertet wurde. Der CVD-Prozess („Coordinated Vulnerability Disclosure“, also die koordinierte Offenlegung von Sicherheitslücken) sei vorhanden und werde aus Sicht des federführenden Ressorts von Sicherheitsforschenden genutzt. Experten hingegen fordern eine Harmonisierung mit bestehenden oder noch umzusetzenden (europäischen) Rechtsakten (wie etwa dem Cyber Security Act oder dem Cyber Resilience Act), um Doppelstrukturen zu vermeiden.

Im Handlungsfeld 2, Ziel 8.2.4 „Unternehmen in Deutschland schützen“ wurde die Maßnahme 8.2.4.3. „Förderprogramme, die auch auf Unterstützung der IT-Sicherheit von kleinen und mittleren Unternehmen, einschließlich Handwerk und freien Berufen, abzielen (insbesondere „go-digital“ und „Digital Jetzt“), sind bekannt und werden nachgefragt“ vom federführenden Ressort als „abgeschlossen“ bewertet, von Experten aber mit „eher nicht

umgesetzt“ eingeschätzt. Die Transferstelle IT-Sicherheit im Mittelstand (TISiM) sei laut Freitextantwort der Wirtschaft durch die Transferstelle Cybersicherheit im Mittelstand ersetzt worden. Die genannten Programme „go-digital“ und „Digital Jetzt“ befänden sich in der Abwicklung. Neue Anträge könnten nicht mehr gestellt werden, ein Titelansatz bestehe nur noch zur Abwicklung und Ausfinanzierung. Kritisiert wurde zudem, dass die Programme zwar etabliert seien, aber nicht flächendeckend genutzt würden.

*In Planung befindliche Maßnahmen mit positiver Expertenbewertung:*

HF 1: KI-Systeme werden verstärkt und erfolgreich zur Angriffserkennung und -abwehr eingesetzt (8.1.10.4).

HF 3: Die Zusammenarbeit zwischen den Ressort-IT-Sicherheitsbeauftragten des Bundes ist deutlich gestärkt, inhaltliche wie ggf. auch institutionelle Maßnahmen dazu sind getroffen. (8.3.5.3)

Obwohl im Handlungsfeld 1 im Ziel „IT-Sicherheit durch KI und IT-Sicherheit für KI gewährleisten“ der Indikator 8.1.10.4 „KI-Systeme werden verstärkt und erfolgreich zur Angriffserkennung und -abwehr eingesetzt“ vom federführenden Ressort als noch in Planung angegeben wird, bewerten Experten diesen Punkt bereits als „eher umgesetzt“.

Im Handlungsfeld 3 wurde im Ziel „Cyber- und Informationssicherheit der Bundesverwaltung stärken“ die Maßnahme 8.3.5.3 („Die Zusammenarbeit zwischen den Ressort-IT-Sicherheitsbeauftragten des Bundes ist deutlich gestärkt, inhaltliche wie ggf. auch institutionelle Maßnahmen dazu sind getroffen“) von den Experten als „umgesetzt“ bewertet, obwohl sie sich laut federführendem Ressort noch in Planung befindet. Zumindest mit dem ISB Netzwerk stellt das BSI eine Austausch- und Kommunikationsplattform unabhängig von Ressortgrenzen bereit.

## 3.2 Qualitative Auswertung

Die qualitative Analyse der Freitextkommentare nach Handlungsfeldern ergibt folgendes Bild:

Handlungsfeld 1: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

Viele Maßnahmen in diesem Handlungsfeld sind abgeschlossen oder zumindest weit fortgeschritten, insbesondere in den Bereichen der Förderung digitaler Kompetenzen und des Verbraucherschutzes. Die Zivilgesellschaft hob die positiven Effekte der Sensibilisierungskampagnen hervor. Die Informationskampagnen würden einen hohen Zulauf haben. Es wird jedoch eine bessere Zielgruppenansprache gefordert, um die Wahrnehmung zu verbessern. Die Informationsangebote des BSI für Privatpersonen wurden positiv hervorgehoben, wobei Anstrengungen unternommen werden sollten, diese noch einer größeren Öffentlichkeit bekannt zu machen. Belastbare Angaben zu von Cyberangriffen betroffenen Privatpersonen würden mangels gesetzlicher Meldepflichten nicht vorliegen. Der vom BMI geförderte Digitalführerschein werde in der Bevölkerung gut angenommen.

Handlungsfeld 2: Gemeinsamer Auftrag von Staat und Wirtschaft

Die Zusammenarbeit mit der Wirtschaft wird insgesamt als gelungen betrachtet. Große Unternehmen profitieren von Initiativen wie der Allianz für Cybersicherheit. Es wird jedoch angemerkt, dass KMU stärker in die Maßnahmen einbezogen werden sollten. Es gibt zudem Kritik an nationalen Zertifizierungen und es wird auf die Notwendigkeit europäischer Standards hingewiesen: Nationale Zertifizierungen [...] seien aus Sicht der Wirtschaft für die Industrie nicht geeignet. Hier seien mindestens europäische Verfahren anzustreben. Als zusätzliche Möglichkeit bestimmte funktionale Sicherheitseigenschaften eines Produktes zu überprüfen, sei eine Sicherheitszertifizierung hilfreich.

Ebenfalls wird bemängelt, dass der Nationale Cyber-Sicherheitsrat (NCSR) seiner Koordinierungsfunktion als strategisches Beratergremium bei der Zusammenarbeit zwischen Staat, Wirtschaft, Wissenschaft und Gesellschaft im Bereich der Cybersicherheit in großen Teilen nicht nachkomme. Die baldige Etablierung einer kooperativen Plattform für den niederschwelligen, freiwilligen Austausch von Informationen zu Cyberangriffen wird insbesondere von der Wirtschaft gefordert.

Handlungsfeld 3: Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur

In diesem Handlungsfeld bestehen weiterhin strukturelle Herausforderungen, insbesondere bei der Koordination zwischen Bund und Ländern. Dies gilt etwa für die strategischen Ziele 8.3.3 („Die institutionalisierte Zusammenarbeit zwischen BSI und den Ländern stärken“) und 8.3.4. („Das Nationale Cyberabwehrzentrum weiterentwickeln“). Die ursprünglich angestrebte

Grundgesetz-Änderung, die zwingend für den Ausbau des BSI zur Zentralstelle im Bund-Länder-Verhältnis erforderlich ist, konnte in der 20. LP nicht umgesetzt werden. Es wird derzeit geprüft, wie die Kooperation im Rahmen des verfassungsrechtlich Möglichen alternativ vertieft werden kann. In der Befragung wurden insbesondere die zwischen einzelnen Ländern und dem BSI abgeschlossenen Kooperationsvereinbarungen positiv hervorgehoben.

Handlungsfeld 4: Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik

Die internationalen Aktivitäten werden insgesamt positiv bewertet, insbesondere die Einbindung in EU-Programme. Herausforderungen bestehen jedoch aufgrund geopolitischer Rahmenbedingungen und divergierender Interessen internationaler Partner. Deutschland müsse seine Rolle in internationalen Gremien stärken.

Viele der im Handlungsfeld 4 genannten Maßnahmen sind „Daueraufgaben", die laufend zu erfüllen und nicht als „abgeschlossen" angesehen werden können (z.B. Maßnahme: „Deutschland informiert in bilateralen, regionalen und internationalen Foren über nationale Bewertungen und Entwicklungen im Cybersicherheitsbereich." zum Ziel: „Vertrauensbildende Maßnahmen fördern" (8.4.4).

Die Umsetzung der NIS2-Richtlinie ist steht hingegen kurz vor dem Abschluss (Maßnahme 8.4.1.2 zum Ziel 8.4.1: „Eine wirksame europäische Cyber-Sicherheitspolitik aktiv gestalten").

Über alle Handlungsfelder hinweg ist insgesamt anzumerken, dass einige Ziele nicht SMART (spezifisch, messbar, attraktiv, realistisch, terminiert) formuliert wurden. Somit sind sogenannte „Daueraufgaben", wie beispielsweise die Weiterentwicklung des „Cyber-Abwehrzentrums" (8.3.4) oder „Bilaterale und regionale Unterstützung und Kooperation zum Auf- und Ausbau von Cyber-Fähigkeiten (Cyber Capacity Building) stärken" (8.4.5) dauerhaft mit dem Status „in Umsetzung" zu kennzeichnen.

# 4 Fazit und Ausblick

Die Evaluierung zeigt, dass die Umsetzung der Cybersicherheitsstrategie 2021 insgesamt auf einem guten Weg ist. Ein Großteil der Maßnahmen ist laut den Ressorts abgeschlossen oder in der Umsetzung (ca. 74%). Die Übereinstimmung zwischen den Selbsteinschätzungen der Ressorts und den Bewertungen der externen Stakeholder (70 % stimmen zu, eher zu oder teilweise zu) ist ein positives Signal.

Allerdings macht die Analyse auch deutlich, dass insbesondere in der Zusammenarbeit zwischen Bund und Ländern noch Optimierungspotenzial besteht und dass die Abstimmungen mit europäischen und internationalen Partnern zu intensivieren sind. Digitale Kompetenzen von Anwendern können durch zielgruppengerechtere Ansprache verbessert werden.

Es wird angestrebt, die Fortschritte künftig regelmäßig nachzuhalten, um die Wirkung der Maßnahmen regelmäßig zu evaluieren und gegebenenfalls bei etwaigen Umsetzungsdefiziten nachzusteuern. Eine solche Steuerung war zwar bereits in Ziffer 9.3 der CSS 2021 vorgesehen, konnte aber faktisch nicht realisiert werden. Dazu müssen die Ziele der Fortentwicklung SMART formuliert werden, um den genauen Umsetzungsstatus besser nachvollziehen zu können.

Im Koalitionsvertrag für die 21. Legislaturperiode haben die Koalitionspartner CDU, CSU und SPD festgehalten, dass die Nationale Cybersicherheitsstrategie mit dem Ziel einer klaren Rollen- und Aufgabenverteilung fortentwickelt werden soll. Dies entspricht der Regelung in Ziffer 9.4 der Cybersicherheitsstrategie 2021, derzufolge nach Bewertung der Ergebnisse der Evaluation eine Fortschreibung der Strategie angestrebt werden kann.

Bei der Weiterentwicklung der CSS werden nicht nur die im Rahmen der Evaluierung gewonnenen Erkenntnisse einfließen, sondern auch Vorgaben aus dem europäischen Rechtsrahmen, die 2021 noch nicht in Kraft waren. Diesbezüglich ist insbesondere Art. 7 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (nachfolgend kurz NIS-2 Richtlinie) zu erwähnen. Demzufolge hat jeder Mitgliedsstaat (MS) eine nationale Cybersicherheitsstrategie zu erlassen, die die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus enthält. In Art. 7 Abs. 1 lit a) bis h) der NIS-2 Richtlinie werden die einzelnen Bestandteile der Cybersicherheitsstrategie aufgeführt und in Abs. 2 durch von den MS in diesem Rahmen anzunehmende Konzepte ergänzt.

In Ziffer 9.4 der CSS ist festgehalten, dass auch Empfehlungen der Agentur der Europäischen Union für Cybersicherheit (ENISA) bei der Evaluierung zu berücksichtigen sind. Die MS werden gem. Art. 7 Abs. 4 der NIS-2 Richtlinie bei der Entwicklung bzw. Aktualisierung ihrer Cybersicherheitsstrategien durch ENISA unterstützt. Dazu hat ENISA im Dezember 2020

bereits den Rahmen zur Bewertung nationaler Fähigkeiten („National Capabilities Assessment Framework“, kurz NCAF) entwickelt. Das NCAF soll den MS bei der Selbsteinschätzung ihrer Nationalen Cybersicherheitsstrategien helfen, indem diese anhand konkreter Fragen den Grad der Zielerfüllung bestimmen. Aktuell wird das NCAF von ENISA unter Verwendung von 20 aus der NIS-2 Richtlinie abgeleiteten strategischen Ziele überarbeitet. Die von den Cybersicherheitsstrategien der MS zu erfüllenden strategischen Ziele lauten wie folgt:

- Bekämpfung der Cyberkriminalität
- Balance zwischen Sicherheit und Privatsphäre
- Entwicklung eines umfassenden Rahmens für das Krisenmanagement
- Internationale Zusammenarbeit
- Schaffung vertrauenswürdiger Mechanismen für den Informationsaustausch
- Verbesserung der Incident Preparedness und Reaktion
- Einführung von Maßnahmen für das Cybersicherheitsrisikomanagement
- Einrichtung von Mechanismen für die Meldung von Vorfällen
- Förderung von Forschung und Entwicklung
- Verbesserung der Cybersicherheit der Lieferkette
- Schutz kritischer Sektoren
- Stärkung der Cyberresilienz und -hygiene des Privatsektors
- Förderung des Cybersicherheitsbewusstseins und der Cyberhygiene
- Verbesserung der Entwicklung von Cybersicherheitskompetenzen
- Sichere digitale Identität und Aufbau von Vertrauen in digitale öffentliche Dienste
- Erstellung einer Risikobewertung auf nationaler Ebene
- Stärkung der nationalen Cybersicherheits-Governance
- Einführung von Verfahren der gegenseitigen Unterstützung
- Erstellen einer CVD-Richtlinie
- Aktiven Cyber-Schutz fördern

Ein erster Entwurf des überarbeiteten NCAF wird voraussichtlich im September 2025 vorgestellt und kann dann bereits bei der Fortschreibung verwendet werden.

Daneben werden bei der Fortschreibung auch die Erkenntnisse aus dem VS-NfD eingestuften Bericht des Bundesrechnungshofes (BRH) (VII4 - 0000583/IV VS-NfD) vom 21. Mai 2025 an den Haushaltsausschuss des Deutschen Bundestages gem. § 88 Abs. 2 BHO zur Cybersicherheit zu beachten sein. In diesem Bericht hat der BRH konkrete Aspekte hinsichtlich Aufbau und Struktur der CSS 2021 bemängelt.

**Impressum**

**Herausgeber**
Bundesministerium des Innern, 11014 Berlin
Internet: www.bmi.bund.de

**Stand**
August 2025

**Artikelnummer**
BMI25069

Weitere Publikationen der Bundesregierung zum Herunterladen und zum Bestellen finden Sie unter:
www.publikationen-bundesregierung.de