Deutscher Bundestag **Drucksache 19/32590**

19. Wahlperiode 10.09.2021

Unterrichtung

durch die Bundesregierung

Cybersicherheitsstrategie für Deutschland 2021

1 Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriumdes Innern, für Bau und Heimat vom15. September 2021.

Seite

Seite

2 Zusammenfassung (Management Summary)

Die „Cybersicherheitsstrategie für Deutschland 2021“ bildet vorbehaltlich der Verfügbarkeit entsprechender Haushaltsmittel den strategischen Rahmen für das Handeln der Bundesregierung im Bereich der Cybersicherheit für die nächsten fünf Jahre.

Ausgangspunkt der Strategie ist eine Analyse der Bedrohungslage. Diese ist gekennzeichnet durch eine deutliche sowohl qualitative als auch quantitative Zunahme von Cyberangriffen, eine wachsende Angriffsfläche und neuartige Bedrohungsszenarien. Zudem steigt die potenzielle Schadenshöhe.

Sodann wird ein Überblick über die Institutionen gegeben, die in Deutschland einen Beitrag zur Cybersicherheit leisten. Die Cybersicherheitslandschaft umfasst zivilgesellschaftliche, wissenschaftliche, wirtschaftliche und staatliche Initiativen und Akteure.

Auf Grundlage der Analyse der Ausgangslage werden für die Cybersicherheitsstrategie 2021 vier übergreifende Leitlinien definiert:

1. „Cybersicherheit als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft etablieren“,
2. „Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken“,
3. „Digitalisierung sicher gestalten“ und
4. „Ziele messbar und transparent ausgestalten“.

Diese Leitlinien beschreiben Aspekte, die alle vier folgenden Handlungsfelder der Cybersicherheitsstrategie betreffen. Die Ausrichtung der strategischen Ziele der Handlungsfelder anhand der Leitlinien gewährleistet ihr kohärentes Ineinandergreifen.

In Handlungsfeld 1, „Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung“, werden die Bürgerinnen und Bürger beziehungsweise die Gesellschaft in den Mittelpunkt der Betrachtung gerückt. Die zehn strategischen Ziele des Handlungsfeldes sollen dazu beitragen, dass Bürgerinnen und Bürger die Chancen digitaler Technologien nutzen und sich hierbei sicher und selbstbestimmt in einer digitalisierten Umgebung bewegen können. Hierfür sehen die strategischen Ziele vor, Bürgerinnen und Bürger zu sensibilisieren, deren Cyberkompetenz zu steigern und den Verbraucherschutz in der digitalen Welt zu stärken. Zudem werden Regulierungsvorhaben beschrieben, die den Rahmen für selbstbestimmtes Handeln verbessern sollen.

Das Handlungsfeld 2 trägt die Überschrift „Gemeinsamer Auftrag von Staat und Wirtschaft“. Die 13 dort verorteten strategischen Ziele sollen die Cybersicherheit in der Wirtschaft insgesamt stärken, legen aber auch einen Fokus auf Kritische Infrastrukturen (KRITIS). Daneben werden insbesondere kleine und mittlere Unternehmen (KMU) in den Blick genommen. Die Ziele sehen vor, die vertrauensvolle und enge Zusammenarbeit zwischen Staat und Wirtschaft weiter auszubauen und die regulatorischen Rahmenbedingungen für die Wirtschaft fortzuentwickeln. Ziele, die die Förderung von Schlüssel- und Zukunftstechnologien zum Inhalt haben, sollen die Digitale Souveränität und die Wettbewerbsfähigkeit der Unternehmen im Bereich Cybersicherheit ausbauen.

Die staatlichen Akteure der Cybersicherheit und die notwendigen Entwicklungen in diesem Bereich werden in Handlungsfeld 3, „Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur“, in den Blick genommen. Die Ziele in diesem Handlungsfeld lassen sich drei Bereichen zuordnen: 1. Kompetenzverteilung und Zusammenarbeit zwischen den Behörden, 2. Fortentwicklung von Fähigkeiten und Befugnissen der Behörden und 3. neue Herausforderungen für staatliche Akteure im Cyberraum. Die 14 strategischen Ziele des Handlungsfeldes sollen insbesondere Barrieren einer effektiven Zusammenarbeit zwischen den Behörden abbauen und die sich stetig wandelnden Anforderungen im Cyberraum aufzeigen, für deren Erfüllung die Behörden mit ausreichenden Fähigkeiten und Befugnissen ausgestattet sein müssen.

Die Gewährleistung eines hohen Cybersicherheitsniveaus in Deutschland erfordert auch eine „aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik“. Dies wird in Handlungsfeld 4 mit insgesamt sieben strategischen Zielen adressiert. Zentral ist dabei das Engagement Deutschlands in der Europäischen Union (EU) und in der Organisation des Nordatlantikvertrages (NATO). Während Fragen der Harmonisierung von Regelungen im Rahmen des Gemeinschaftsrechts in allen Handlungsfeldern zu finden sind, befassen sich die Ziele dieses Handlungsfeldes mit der Weiterentwicklung der Grundlagen und Instrumentarien der Cybersicherheitspolitik dieser Organisationen. Darüber hinaus sollen das internationale Regelwerk für Staaten

im Cyberraum und die internationale Bekämpfung von Cyberkriminalität gestärkt werden. Auch Ziele der bilateralen Zusammenarbeit und vertrauensbildende Maßnahmen sind Gegenstand von Handlungsfeld 4.

Die Cybersicherheitsstrategie schließt mit der Darstellung eines transparenten Ansatzes für Umsetzung, Berichtwesen und Controlling der Strategie. Die Wirksamkeit der Umsetzung soll kontinuierlich verfolgt und überprüft werden. Zukünftige Evaluierungen werden systematisch vorbereitet.

3 Einleitung

Unsere Zeit ist geprägt von den neuen Möglichkeiten einer digitalisierten Welt. Technologien wie Künstliche Intelligenz (KI), vernetzte elektronische Geräte und neue innovative Kommunikationskanäle bringen große Veränderungen mit sich. Viele unserer alltäglichen Aufgaben, unabhängig ob im privaten, beruflichen oder behördlichen Kontext, werden durch neue Technologien erleichtert und beschleunigt. Immer mehr Prozesse verlagern sich in den Cyberraum. Die COVID-19-Pandemie hat dieser Entwicklung einen weiteren Schub gegeben.

Mit den zunehmenden Möglichkeiten können sich jedoch auch die Risiken im Cyberraum ändern oder vermehren. Um alle Chancen, Vorteile und Notwendigkeiten der Digitalisierung vollumfänglich ausschöpfen zu können, ist es zwingend erforderlich, sich vor diesen Risiken zu schützen. Der Staat hat die Pflicht, die rasanten Entwicklungen der Digitalisierung so im Interesse der Bürgerinnen und Bürger gemeinsam mit Wirtschaft, Wissenschaft und Zivilgesellschaft zu bewerten und aktiv zu gestalten, dass die erforderlichen Rahmenbedingungen für ein hohes Maß an Sicherheit und Schutz im Cyberraum gewährleistet werden.

Die Bürgerinnen und Bürger müssen Technologien auch zukünftig stets sicher, frei und selbstbestimmt nutzen können. Die Cyber- und Informationssicherheit ist kein notwendiges Übel, sondern Garant dafür, dass Digitalisierung nachhaltig erfolgreich ist.

Die von der Bundesregierung beschlossenen Cybersicherheitsstrategien für Deutschland aus den Jahren 2011[1] und 2016[2] bildeten wesentliche Weichenstellungen für eine zukunftsgerichtete Cybersicherheitspolitik.

So wurden beispielsweise für den Nationalen Cybersicherheitsrat (NCSR), das Nationale Cyber-Abwehrzentrum (Cyber-AZ) oder die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) in den Strategien die Grundlagen gelegt. Die Umsetzung von Zielen wie „Digitale Kompetenz bei allen Anwendern fördern“, „Kritische Infrastrukturen sichern“, „Strafverfolgung im Cyberraum intensivieren“ oder „Cybersicherheit international aktiv mitgestalten“ hat in den Strategien ihren Ausgangspunkt.

An diese Entwicklung knüpft die Cybersicherheitsstrategie 2021 an. Die darin beschriebenen Leitlinien, Maßnahmen und Ziele bilden die Grundlage für ein sicheres Deutschland im Cyberraum in den kommenden Jahren.

Cyber- und Informationssicherheit betrifft Staat, Wirtschaft, Wissenschaft und Gesellschaft gleichermaßen. Deshalb adressiert die Strategie alle Akteure und bindet sie ein.

Die Cybersicherheit ist eine Aufgabe der Gegenwart, aber auch eine der wichtigsten Aufgaben für die Zukunft. Verstärkt werden deshalb Schwerpunkte auf Zukunfts- und Schlüsseltechnologien gelegt.

Die deutsche Wirtschaft ist zukünftig noch stärker darauf angewiesen, im Cyberraum zu agieren. Transformationen sind in vollem Gange, beispielhaft seien hier Industrie 4.0 und Arbeiten 4.0 genannt. Diese müssen nachhaltig durch die Cyber- und Informationssicherheit abgesichert werden. Hierzu führt die Strategie die bewährte enge Zusammenarbeit von Staat und Wirtschaft fort und intensiviert diese in Form eines noch engeren Austauschs, eines verbesserten Schutzes und der Förderung sicherer Produkte und Dienstleistungen.

Aber auch die staatliche Cybersicherheitsarchitektur ist auf den Prüfstand zu stellen und zeitgemäß fortzuentwickeln.

Außerdem beabsichtigt die Bundesregierung, ihr Engagement auf europäischer und internationaler Ebene noch weiter auszubauen, und setzt verstärkt auf die Zusammenarbeit sowie ein koordiniertes Handeln mit ihren Partnern.

Nicht nur thematisch, auch strukturell wurde die Cybersicherheitsstrategie weiterentwickelt. Im Rahmen einer umfassenden Evaluierung unter Einbindung der Bundesministerien und ihrer Geschäftsbereichsbehörden, der Länder, von Wirtschaftsvertretern und von Vertretern der Zivilgesellschaft wurde festgestellt, dass sich die bisher definierten vier Handlungsziele „Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung“, „Gemeinsamer Auftrag Cybersicherheit von Staat und Wirtschaft“, „Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur“ sowie „Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik“ bewährt haben und sie weiterhin Bestand haben. Sie haben Querschnittscharakter und betreffen alle gesellschaftlichen Bereiche, unter die sich alle erforderlichen Maßnahmen subsumieren lassen.

---

[1] Abrufbar unter: https://www.cio.bund.de/Web/DE/Strategische-Themen/IT-und-Cybersicherheit/Cyber-Sicherheitsstrategie-fuer-Deutschland/cyber_sicherheitsstrategie_node.html

[2] Abrufbar unter: https://www.bmi.bund.de/cybersicherheitsstrategie/

Gleichzeitig wurden Themen wie „Digitale Souveränität“ identifiziert, die neu als Querschnittsthemen in allen Handlungsfeldern berücksichtigt werden müssen. Leitlinien führen durch die Fortschreibung der vorliegenden Cybersicherheitsstrategie, um ein Ineinandergreifen der einzelnen strategischen Ziele und Maßnahmen zu gewährleisten.

Als weitere wesentliche Neuerung gegenüber der letzten Cybersicherheitsstrategie soll die Umsetzung der Strategie kontinuierlich verfolgt und überprüft werden. Hierzu sind alle strategischen Ziele mit definierten Indikatoren hinterlegt, anhand derer der Erfolg der Strategie nachvollziehbar kontrolliert werden kann.

4 Zielstellung der Cybersicherheitsstrategie 2021

Die „Cybersicherheitsstrategie für Deutschland 2021“ ersetzt die „Cybersicherheitsstrategie für Deutschland 2016“. Sie bildet den ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung im Bereich Cybersicherheit für die nächsten fünf Jahre. Sie ist eine Fortschreibung, die inhaltlich auf Bewährtem der Strategien aus den Jahren 2011 und 2016 aufbaut und gleichzeitig neue Schwerpunkte setzt.

Die Strategie beschreibt die grundsätzliche, langfristige Ausrichtung der Cybersicherheitspolitik der Bundesregierung in Form von Leitlinien, Handlungsfeldern sowie strategischen Zielen. Sie hat einen aktiven gestaltenden Charakter und soll ein zielgerichtetes und abgestimmtes Zusammenwirken aller Akteure ermöglichen und fördern. Die Cybersicherheitsstrategie für Deutschland und die Cybersicherheitsstrategien der Länder ergänzen sich dabei gegenseitig und intensivieren damit die föderale Zusammenarbeit. Eingebettet in die Europäische Cybersicherheitsstrategie[3] trägt die Cybersicherheitsstrategie für Deutschland zudem auch zur Gestaltung der digitalen Zukunft Europas bei.

Der Steuerungsrahmen gemäß der NIS-Richtlinie[4] ist Bestandteil der Strategie. Wie in der Richtlinie gefordert, bilden die strategischen Ziele die Prioritätensetzungen der Bundesregierung ab, zudem werden in Kapitel 6 „Die Cybersicherheitslandschaft in Deutschland„ die Akteure der Cybersicherheitslandschaft benannt.

Die Cybersicherheitsstrategie

- beschreibt den Rahmen, in dem die Bundesregierung ihre Aktivitäten entfalten wird;
- schafft Transparenz und Nachvollziehbarkeit für alle Akteure aus Staat, Wirtschaft, Wissenschaft und Gesellschaft,
- fördert das aktive, zielgerichtete Zusammenwirken dieser Akteure,
- berücksichtigt die Vorgaben der EU,
- verankert ein Berichtswesen und Controlling auf strategischer Ebene und
- bereitet zukünftige Evaluierungen und eine kontinuierliche Weiterentwicklung systematisch vor.

Die Umsetzung der Ziele der Cybersicherheitsstrategie steht unter dem Vorbehalt der Verfügbarkeit entsprechender im Haushaltsplan veranschlagter Haushaltsmittel. Das Prinzip der Wirtschaftlichkeit und Sparsamkeit (vergleiche § 7 der Bundeshaushaltsordnung für den nationalen Haushalt) gilt entsprechend für den Haushalt der EU, soweit dieser in Anspruch genommen werden sollte.

Die Cyber- und Informationssicherheit grenzt an zahlreiche weitere Themen an und überschneidet sich teilweise mit diesen. Zu einigen dieser Themenstellungen hat die Bundesregierung eigene Strategien veröffentlicht. Diese werden in der Cybersicherheitsstrategie referenziert und überblicksartig erläutert, um ein Gesamtverständnis zu ermöglichen.

Die Themen hybride Bedrohungen und Datenschutz haben besonders große Schnittmengen mit der Cyber- und Informationssicherheit und müssen daher stets mitberücksichtigt werden. Der Themenbereich der hybriden Bedrohungen wird im Kapitel 5 „Cyberbedrohungslage„ einer genauen Betrachtung unterzogen.

Die Überschneidungen von Datenschutz und Cyber- und Informationssicherheit werden dadurch deutlich, dass zahlreiche Schutzziele des Datenschutzes auch für die Cyber- und Informationssicherheit Bedeutung haben. Seit dem Jahr 2018 stellen die Datenschutz-Grundverordnung[5] und die Richtlinie für den Datenschutz in den Bereichen Polizei und Justiz[6] auf europäischer Ebene sowie das Bundesdatenschutzgesetz[7] die zentralen datenschutzrechtlichen Regelungen dar. Dabei sind die datenschutzrechtlichen Schutzziele und die der Cyber- und Informationssicherheit weitgehend kohärent und teilweise sogar deckungsgleich (zum Beispiel bei den Schutzzielen der Integrität und Vertraulichkeit), können im Einzelfall aber auch in einem Spannungsverhältnis zueinander stehen

---

3 Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020JC0018

4 Die NIS-Richtlinie gibt den Mitgliedstaaten vor, dass sie in der Strategie einen Steuerungsrahmen schaffen müssen (siehe Artikel 7 Absatz 1 lit. b Richtlinie (EU) 2016/1148). Dieser muss eine Bestimmung enthalten, (i) wie die Ziele und Prioritäten der Strategie zu erreichen sind und (ii) welche staatliche Institution oder Private für deren Erreichung verantwortlich sind. Die Richtlinie ist abrufbar unter: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:32016L1148

5 Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

6 Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680

7 Abrufbar unter: http://www.gesetze-im-internet.de/bdsg_2018/

(zum Beispiel die datenschutzrechtliche Datenminimierung und das Sicherheitsinteresse an einer Protokollierung von Datenzugriffen). In diesen Fällen muss ein Ausgleich der widerstreitenden Interessen erfolgen, der beiden Schutzzielen zur weitestgehenden Wirksamkeit verhilft.

5 Cyberbedrohungslage

Informationstechnik (IT) ist ein integraler Bestandteil unseres gesellschaftlichen Lebens geworden. Kaum ein technisches Produkt kommt ohne IT aus. Während Anfang des 21. Jahrhunderts um die Jahrtausendwende die Prozessautomatisierung mittels IT im Vordergrund stand, erfolgt die Wertschöpfung bei heutigen IT-Systemen insbesondere durch deren Vernetzung und durch „intelligente“ Algorithmen.

Vernetzte IT-Systeme haben allerdings auch eine deutlich größere Angriffsfläche, insbesondere da diese zumeist aus aller Welt über das Internet erreichbar sind. Gleichzeitig führt die wachsende Komplexität der IT-Systeme und Algorithmen häufiger zu ungewolltem Systemverhalten und Sicherheitslücken in Systemen, sogenannten Schwachstellen. Angreifer nutzen daher die weltweite Erreichbarkeit der Systeme in Verbindung mit den Schwachstellen, um ihre kriminellen Absichten umzusetzen.

Dem Bestreben, die Sicherheit von IT-Systemen zu gewährleisten und zu verbessern, steht eine marktgetriebene dynamische Weiterentwicklung der IT gegenüber. In diesem Wettlauf treten daher nach wie vor regelmäßig Schwachstellen auf. Auch werden Vorgaben beziehungsweise etablierte Standards zum sicheren Betrieb von IT nicht immer hinreichend beachtet. Dafür tragen die Hersteller eine besondere Verantwortung, aber auch das Verhalten der Nutzer, Betreiber und Administratoren trägt einen wesentlichen Anteil zu sicheren IT-Systemen bei. Nur wenn alle beteiligten Akteure gut zusammenwirken, lassen sich Cyberangriffe zuverlässig erkennen und deren Wirkung erfolgreich verhindern oder abschwächen.

Dem Staat kommt dabei die Rolle zu, geeignete Rahmenbedingungen für sichere IT-Systeme zu schaffen. Beratungsangebote unter anderem des Bundesamts für Sicherheit in der Informationstechnik (BSI), staatlich geförderte Forschung und präventive Maßnahmen verschiedener Sicherheitsbehörden tragen dafür Sorge, dass Mindestanforderungen für die Gewährleistung von IT-Sicherheit geschaffen und eingehalten, Cyberangriffe erkannt und aufgeklärt sowie die Täterinnen oder Täter durch Sicherheits- und Strafverfolgungsbehörden ermittelt und zur Verantwortung gezogen werden – dies ist aufgrund von deren weltweitem Wirken oftmals eine besondere Herausforderung.

Trotz intensiver Bemühungen zur Gewährleistung von Cybersicherheit sehen wir heute eine deutliche Zunahme von Cyberangriffen. Dabei vermischt sich der klassische Cyberangriff im Sinne der Definition dieser Strategie zunehmend mit anderen Phänomenbereichen wie Erpressung, Desinformation, Betrug oder Beleidigung. Das Vorgehen der Täterinnen und Täter wird zudem immer ausgefeilter. Arbeitsteiliges Vorgehen bei der Durchführung von Cyberangriffen und der Entwicklung von Schadsoftware ist zwischenzeitlich der Regelfall. Dem kann nur geeignet begegnet werden, wenn alle Maßnahmen zur Gewährleistung von Cybersicherheit regelmäßig geprüft und angepasst werden. Diese Strategie ist einer der Bausteine dafür.

Deutschland setzt sich für ein freies, offenes, sicheres und globales Internet ein, in dem grundrechtlich verbürgte Freiheiten geschützt werden. Cybersicherheit ist auch ein Baustein, diese Werte zu gewährleisten.

5.1 Angriffsvektoren – welche Einfallstore ermöglichen den Angriff?

Unsichere IT-Systeme – sowohl Hard- als auch Software – stellen ein zentrales Einfallstor für Cyberangriffe dar. Je größer und komplexer Softwareprojekte werden und je mehr Personen dabei in die Erstellung eingebunden sind, desto häufiger entstehen Fehler in der Software, die als Schwachstellen durch Angreifer ausgenutzt werden können. Zwar sorgen zahlreiche Hersteller mittlerweile mit regelmäßigen oder kurzfristigen Updates dafür, festgestellte Schwachstellen zu schließen (Patchen). Jedoch lassen sich nicht immer alle Schwachstellen schließen und auch die schiere Anzahl an Schwachstellen verdeutlich den Bedarf, durch verbesserte Qualitätssicherungsprozesse das Aufkommen von Schwachstellen bereits vor Veröffentlichung zumindest zu reduzieren.

Weitere Ursachen für unsichere IT-Systeme sind fehlerhafte Konfiguration, mangelnde Schutzmechanismen oder Fehlbedienungen der Nutzerinnen und Nutzer. Auch diese Ursachen ermöglichen es unberechtigten Dritten, in fremde Systeme einzudringen und diese zu kompromittieren.

Zusätzlich erweitert die schnell anwachsende Zahl von mit dem Internet verbundenen Geräten (Internet of Things – IoT), wie beispielsweise Lautsprecher, Kühlschränke, Türklingeln, Fahrstühle und Werkzeugmaschinen sowie Medizingeräte, die Möglichkeit potenzieller Cyberangriffsszenarien. Dies wiegt umso schwerer, als viele IoT-Geräte oftmals nur über ein geringes Cybersicherheitsniveau verfügen. Die Schnelllebigkeit dieses Marktes führt häufig zu schlechter Qualität der Software mit großen Sicherheitslücken. Zudem sind Patches nicht oder nicht

über entsprechend lange Zeiträume oder nur stark verzögert verfügbar und gegebenenfalls in Ermangelung entsprechender Funktionen beziehungsweise Schnittstellen gar nicht erst einspielbar.

Für die Ausnutzung der Mehrzahl der Schwachstellen bedarf es zumeist auch eines aktiven Zutuns der Nutzenden. Für Angriffe über Schwachstellen wird teilweise auch fehlende Information von Nutzenden ausgenutzt. Der schnelle Klick auf einen unsicheren, schadhaften Link, die Installation von Software aus unbekannten Quellen oder das unbedachte Öffnen eines E-Mail-Anhangs sind typische Alltagsfälle für die Kompromittierung eines IT-Gerätes. Ohne sensibilisierte Nutzende wird ein hohes Niveau an Cybersicherheit daher kaum gelingen.

Zu beobachten ist zudem ein sich verstärkender Trend zu Supply-Chain-Angriffen. Hier wird durch den Angreifer eine Soft- oder Hardware während des Herstellungs- oder Pflegeprozesses verändert. Die Manipulation des Angreifers wird dann unmittelbar vom Hersteller mit dem Produkt ausgeliefert. Zum Beispiel wurde im Dezember 2020 bekannt, dass Angreifer ein Update eines Softwareherstellers manipuliert hatten. Die Installation des Updates erfolgte automatisiert. Da die Nutzenden regelmäßig den Updatemechanismen vertrauen, können typischerweise zahlreiche Systeme betroffen sein. Derartige Angriffe stellen ein besonderes Risiko dar, da die manipulierte Software häufig mit Administratorrechten installiert oder betrieben wird und Schutzmechanismen wie Virenscanner zumeist nicht ansprechen. Kundinnen und Kunden sowie Verbraucherinnen und Verbraucher sind regelmäßig arg- und schutzlos.

Insbesondere bewusst herbeigeführte Schwachstellen der Hardware zeigen, dass Cybersicherheit auch eine Frage Digitaler Souveränität ist, da ein nationaler Fertigungsprozess besser beaufsichtigt oder reguliert werden kann. Die Abhängigkeit von Systemen, deren Vertrauenswürdigkeit nicht kontrolliert werden kann, eröffnet potenzielle Einfallstore für Cyberakteure.

Die Chancen neuer Technologien wie KI oder Quantencomputing sind unbestritten. Damit verbunden sind aber auch neue Risiken. Beispielsweise basieren KI-basierte Verfahren häufig auf einem Trainingsprozess und lassen sich in ihrem Verhalten oftmals nicht vollständig nachvollziehen. Aus diesem Grund kann die Integrität dieser Algorithmen gegebenenfalls durch geschickte Auswahl der Eingabemuster oder Trainingsdaten beeinträchtigt werden. Bei einer Verkehrszeichenerkennung führten beispielsweise geschickte Manipulationen der Verkehrszeichen zu fehlerhaften Ausgaben. Um Risiken bei neuen Informationstechnologien zu begegnen, bedarf es jedoch weiterer Forschung und neu zu entwickelnder Technologien.

5.2 Bedrohungen – welche Entwicklungen werden bei Cyberangriffen festgestellt?

Die Durchdringung des gesellschaftlichen Lebens durch die IT hat zu verschiedensten neuen Bedrohungen geführt. Die Bereitstellung von Medien über das Internet lässt neue Wege zur Manipulation von Meinungen zu. Einfache Nutzung und weitgehende Anonymität haben unter anderem Falschmeldungen und Hassreden in Sozialen Medien ansteigen lassen. Auch die Verbreitung illegaler Inhalte wie Kinderpornographie und urheberrechtlich geschützter Inhalte über das Internet nimmt – insbesondere unter Ausnutzung von Anonymisierungsdiensten und Verschlüsselungsangeboten – nach wie vor zu.

Der eigentliche Fokus dieser Strategie liegt jedoch nicht auf Bedrohungen, bei denen die IT dazu genutzt wird, illegale Inhalte zu verbreiten oder auf Betrugsversuchen (Phishing), sondern auf Cyberangriffen, die die Verfügbarkeit, Integrität und Vertraulichkeit von IT-Systemen unmittelbar und maßgeblich beeinträchtigen. Damit einher gehen auch regelmäßig Verstöße gegen den Datenschutz durch Abschöpfung personenbezogener Daten. Cyberangriffe können auch als Mittel hybrider Bedrohungen zum Einsatz kommen. Typisch sind Cyberangriffe auch in den Phänomenbereichen Cyberkriminalität, Cyberterrorismus, Cyberspionage und Cybersabotage, deren Wirkungen zum Beispiel auf Kritische Infrastrukturen erhebliche wirtschaftliche und gesellschaftliche Folgen haben können.

5.2.1 Cyberkriminalität

Im Bereich der Cyberkriminalität ist der Einsatz von Ransomware, die den Zugang zu Daten oder Systemen blockiert, derzeit eine der größten Bedrohungen. Die Akteure greifen dort an, wo sie ungeschützte Schwachstellen finden, egal ob es sich um Unternehmen, Behörden oder private Nutzende handelt. Dem eigentlichen Cyberangriff folgen dann Erpressungsversuche, wie die Drohung der Veröffentlichung von Kundendaten im Netz, bis zur Androhung der Weitergabe sensibler Informationen an Konkurrenten. Ransomware verursacht zwischenzeitlich erhebliche Schäden, insbesondere auch, weil die betroffenen Stellen oftmals weltweit vernetzt sind und so große Bereiche von Unternehmen oder ganze Infrastrukturbereiche bei einem solchen Angriff ausfallen können. Eine ernstzunehmende Gefahr geht außerdem vom sogenannten „Big Game Hunting“ aus. Dabei fokussieren sich die

Angreifer auf besonders zahlungskräftige beziehungsweise lukrative Ziele, so dass die Aussicht auf hohe Lösegeldzahlungen besteht.

Sogenannte Distributed-Denial-of-Service (DDoS)-Angriffe überlasten IT-Systeme in der Regel durch Netzwerkverkehr und werden ebenfalls häufig für Erpressungsversuche genutzt. Oftmals finden diese Angriffe mittels Bot-Netzen statt. Dazu kapern Angreifer zuvor eine Vielzahl von IT-Systemen, die dann ferngesteuert genutzt werden, oder sie zweckentfremden teils fehlkonfigurierte, teils nicht absicherbare, aber öffentlich erreichbare Systeme, um das Zielsystem zu überlasten. Die dafür genutzte Schadsoftware hat sich über die Jahre deutlich fortentwickelt, so dass neben der Durchführung von DDoS-Angriffen häufig auch Zugriffe auf die Daten der Bots möglich sind, mittels derer vertrauliche Daten der Betroffenen gewonnen werden können. Dies ist ein typisches Einfallstor für die Erlangung von Zugangsdaten. Ein weiteres Feld für DDoS-Angriffe sind unliebsame Inhalte im Internet. So werden diese beispielsweise zur Behinderung von Parteiveranstaltungen genutzt. Dabei verschwimmen die Motive wie Hacktivismus oder staatliche Einflussnahme zunehmend.

5.2.2 Staatlich motivierte Cyberangriffe

Auf dem Gebiet staatlich motivierter Cyberangriffe wie Cyberspionage und Cybersabotage sehen sich staatliche und nichtstaatliche Einrichtungen sowie Wirtschaftsunternehmen zunehmend strategisch agierenden Cyberakteuren gegenüber. Die in diesen Bereichen zumeist tätigen Akteure – sogenannte Advanced Persistent Threat (APT)-Gruppen – zeichnen sich durch einen teils sehr hohen Ressourceneinsatz, eine hohe Durchhaltefähigkeit und umfassende technische Fähigkeiten aus. Dementsprechend werden deren Aktivitäten oftmals nachrichtendienstlichen Akteuren oder in ihrem Auftrag handelnden Gruppen zugerechnet.

Mit komplexen und langfristig angelegten Strategien versuchen diese Gruppen, unerkannt in IT-Systemen Fuß zu fassen. Neben der Nutzung solcher „Zugänge“ zum Zweck der Cyberspionage, um beispielsweise sensible Informationen zu stehlen, wurden zuletzt häufiger Aktivitäten zur Vorbereitung von Cybersabotagemaßnahmen festgestellt (sogenanntes Pre-Positioning). Da immer mehr Staaten entsprechende Cyberfähigkeiten entwickeln, werden Cyberangriffe von APT-Gruppen auf absehbare Zeit eine große Bedrohung bleiben. Erkennbar ist auch, dass teils eine Symbiose der Akteure im Bereich Cyberkriminalität und Cyberspionage beziehungsweise Cybersabotage vollzogen wird. Auch militärische Akteure arbeiten kontinuierlich am Aufbau eigener Cyberfähigkeiten; der Blick auf die Cyberbedrohungslage muss daher auch die militärische Komponente beinhalten.

5.2.3 Cyberangriffe im Rahmen hybrider Bedrohungen

Unter hybriden Bedrohungen wird das zielgerichtete Vorgehen staatlicher Akteure und ihrer nicht-staatlichen vorgelagerten Stellen (Proxies) verstanden, das eine große Bandbreite an verdeckten und offenen Mitteln umfassen kann. So können Angriffe im Cyberraum in weiteren Bereichen (zum Beispiel im Informationsraum) Wirkung entfalten, mit Aktivitäten in weiteren Bereichen konzertiert erfolgen oder der Vorbereitung weiterer Aktivitäten der illegitimen Einflussnahme dienen.

Gerade zwischen den Bereichen Cyber- und Informationsraum besteht ein enger Zusammenhang, da der Informationsraum zunehmend durch Informationstechnik gestaltet wird und sich durch einen hohen Grad der Vernetzung auszeichnet. Ein Beispiel für Angriffe im Sinne hybrider Bedrohungen sind Cyberspionageangriffe, die sensible Informationen rechtswidrig aus IT-Systemen abgreifen, um diese in einem zweiten Schritt manipulativ zu verbreiten und so im Informationsraum mittels Diskreditierung oder Desinformation schädliche Wirkung zu entfalten.

Cybersabotageangriffe können auch das Ziel verfolgen, in weiteren Bereichen, zum Beispiel in der Wirtschaft, insbesondere auch auf Kritische Infrastrukturen schädlich einzuwirken und die daraus folgenden Auswirkungen im Informationsraum manipulativ auszunutzen. Kritische Infrastrukturen sind für die Versorgung essenziell. Ein Ausfall führt zu großer Verunsicherung und liegt somit im potenziellen Fokus der Angreifer. Kritische Infrastrukturen bedürfen daher eines hohen Schutzniveaus. Die im Rahmen hybrider Bedrohungen eingesetzten Mittel ermöglichen es den jeweiligen Akteuren oft verhältnismäßig einfach, die Täterschaft und die dahinterliegenden Motivationen zu verschleiern beziehungsweise abzustreiten. Als ein Beispiel kann der mutmaßlich staatliche Cyberangriff mit einem als Ransomware getarnten Sabotagetool (NotPetya) im Jahr 2017 angesehen werden.

Propaganda und Desinformation können besonders dann zu einer großen Gefahr werden, wenn diese durch Cyberangriffe auf glaubwürdigen Plattformen verbreitet werden. Web-Angebote von Medienunternehmen bedürfen daher eines hohen Schutzes vor Cyberangriffen.

Cyberangriffe im Rahmen hybrider Bedrohungen unterscheiden sich technisch zunächst nicht von anderen Cyberangriffen, zu denen diese Strategie Aussagen trifft. Die reguläre Nutzung digitaler Medien für Desinformation oder anderweitige illegitime Zwecke ist hingegen keine Frage der Cybersicherheit.

5.3 Assets – welche Güter sind bedroht?

Da unser Leben in nahezu allen Aspekten mit der IT verknüpft ist, können Cyberangriffe alle Lebensbereiche treffen. Der Ausfall der IT durch einen Cyberangriff kann beispielsweise zu Versorgungsengpässen führen. Daten werden zunehmend zu einem wertvollen Gut, etwa, wenn durch Cyberangriffe auf sensible Finanz- oder Gesundheitsdaten zugegriffen wird, um sie anschließend zum Gegenstand von Erpressung oder Verkäufen im Darknet werden zu lassen. Die weite Verbreitung und die Vielzahl von Informationsportalen im Internet ermöglichen die Verbreitung falscher Informationen auf scheinbar legitimen Angeboten, die erhebliche Unsicherheit in der Bevölkerung schüren können. Letztlich können Cyberangriffe zentrale Güter und Werte unserer Gesellschaft beeinträchtigen, wie Sicherheit, Wohlstand, Selbstbestimmung und Demokratie.

Ob Kommunikation mit Familie und Freunden, Online-Shopping und Online-Banking, Bezug staatlicher Leistungen oder demokratische Willensbildung: Die Digitalisierung prägt den Alltag der Menschen. Cyberangriffe, wie beispielsweise zum Zwecke des Identitäts- und Datendiebstahls oder zur Verbreitung von Desinformation, beeinträchtigen daher die Möglichkeiten, sich sicher und selbstbestimmt im Cyberraum zu bewegen.

Die Wirtschaft hängt in hohem Maße von funktionierenden, verlässlichen und integren IT-Infrastrukturen ab. Cyberangriffe auf Unternehmen sowohl in Deutschland als auch in aller Welt können in der eng verzahnten Produktionswelt mit komplexen Lieferverbindungen beziehungsweise Lieferketten enorme Dominoeffekte erzeugen, die massive wirtschaftliche Schäden mit sich bringen. Digitale Wirtschaftsspionage gefährdet unmittelbar den wirtschaftlichen Erfolg unserer Unternehmen, aber auch mittelbar die Wettbewerbsfähigkeit und Stabilität unserer Volkswirtschaft als Ganzes.

Kritische Infrastrukturen wie beispielsweise Strom- und Telekommunikationsnetze, Klinikverbünde oder Finanzsysteme sind für das Funktionieren des privaten, wirtschaftlichen und öffentlichen Lebens unerlässlich. Sie sind zunehmend von einer störungsfrei arbeitenden und integren IT-Infrastruktur abhängig. Eine Störung oder auch ein Ausfall durch einen IT-Sicherheitsvorfall kann zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Beeinträchtigungen der öffentlichen Sicherheit und Ordnung oder anderen dramatischen Folgen führen.

Angesichts der zunehmenden Digitalisierung der öffentlichen Verwaltung stellen Cyberangriffe auf staatliche Institutionen – neben den Gefährdungen durch eine Ausspähung sensibler Daten – unter anderem eine elementare Gefahr für die Funktionsfähigkeit und Integrität der staatlichen Leistungserbringung dar. Angriffe auf das parlamentarische System sind auch Angriffe auf die demokratische Willensbildung und die freiheitliche demokratische Grundordnung.

5.4 Fazit

Ob sich die Bedrohungslage im Cyberraum insgesamt erhöht hat oder ob die Bedrohungslage nur relativ zur zunehmenden Verbreitung der IT in allen Lebensbereichen gestiegen ist, ist schwer zu beantworten. Die hohe und stetig wachsende Durchdringung aller Lebensbereiche durch IT, verbunden mit der Schnelllebigkeit des Marktes, fehlenden Standards und teilweise auch schlechtem Design, hat jedoch das Risiko erhöht, dass Cyberangriffe größere Schäden oder Störungen bewirken und deren Auswirkungen über die eigentlich betroffene IT hinaus spürbar sein können. Dies gilt es zu verhindern. Auch ist die absolute Zahl der erfassten Cyberangriffe in den letzten Jahren durchgängig angestiegen.

Neue Technologien enthalten regelmäßig auch neue Risiken. Je häufiger diese eingesetzt werden, desto mehr steigt auch hier die Gefahr von Cyberangriffen. Die Gewährleistung von Cybersicherheit muss somit ein ebenso dynamischer Prozess sein, wie die Fortentwicklung der Informationstechnik selbst.

Stetige Aufmerksamkeit und situationsgerechte Anpassung der Cybersicherheitsmaßnahmen sowie die Entwicklung und der Einsatz von Technologien, deren Sicherheit bereits mit dem Design verknüpft ist, sind ein wichtiger Teil zur Lösung des Problems. Diese Strategie ist hierfür ein Baustein. Die fortwährende Sensibilisierung der Nutzenden und der Austausch von Wissen zu Cybergefahren zwischen allen Akteuren sind eine weitere Säule,

um Cybersicherheit zu gewährleisten. Verbunden mit der bewährten Arbeit der Sicherheitsbehörden auch im Cyberraum hat Deutschland gute Voraussetzungen, um sich auch den verändernden Cyberbedrohungen anzunehmen.

6 Die Cybersicherheitslandschaft in Deutschland

Cybersicherheit in Deutschland zu gewährleisten ist eine gesamtgesellschaftliche Aufgabe. Eine Vielzahl von Akteuren aus Staat, Wirtschaft, Wissenschaft und Gesellschaft leistet hierfür einen unverzichtbaren Beitrag. Auch jedem einzelnen Mitglied unserer Gesellschaft kommt Verantwortung für die Cybersicherheit zu. Eine umfassende und regelmäßig aktualisierte Liste der Akteure findet sich im „Online-Kompendium Cybersicherheit in Deutschland“[8].

Die Akteure und Initiativen zur Gewährleistung von Cybersicherheit in Deutschland lassen sich grundsätzlich folgenden Bereichen zuordnen, wirken zugleich aber häufig auch bereichsübergreifend zusammen:

1. Zivilgesellschaftliche Initiativen und Akteure
2. Wissenschaftliche Initiativen und Akteure
3. Wirtschaftliche Initiativen und Akteure
4. Staatliche Initiativen und Akteure

6.1 Zivilgesellschaftliche Initiativen und Akteure

Der Großteil der zivilgesellschaftlichen Akteure, die sich in Deutschland im Bereich Cybersicherheit engagieren, sind Vereine und Stiftungen. Hinzu kommt eine große Anzahl unabhängiger ehrenamtlicher Expertinnen und Experten. Diese Akteure erstellen unter anderem politische Analysen und Handlungsempfehlungen, sensibilisieren die Bevölkerung für Belange der Cybersicherheit, vermitteln Medienkompetenz und Technikverständnis und vernetzen verschiedene Gesellschaftsgruppen. Durch die Vielzahl zivilgesellschaftlicher Initiativen und Akteure gelingt es, einer großen Zahl von Adressaten ein ausdifferenziertes Angebot bereitzustellen.

6.2 Wissenschaftliche Initiativen und Akteure

Die Wissenschaft leistet insbesondere durch ihre Forschungstätigkeit in Form von Grundlagenforschung und angewandter Forschung theoretischer, experimenteller und industrieller Natur einen zentralen Beitrag zur Erhöhung der Cybersicherheit in Deutschland. Daraus resultierende Erkenntnisse und Innovationen in Form von Analysen, Handlungsempfehlungen, Lehrinhalten und Technologien bilden eine unverzichtbare Grundlage für konkrete Anwendungsfälle in Staat, Wirtschaft und Gesellschaft.

6.3 Wirtschaftliche Akteure und Initiativen

Wirtschaftliche Akteure und Initiativen engagieren sich in einem breiten Themenspektrum der Cybersicherheit. Sie entwickeln unter anderem innovative technische Lösungen, bringen sich bei der Weiterentwicklung sicherheitsrelevanter Standards und Normen ein und treiben in themenspezifischen Arbeitsgruppen die Vernetzung und Kompetenzentwicklung voran. Cybersicherheit ist für wirtschaftliche Akteure auch ein zentraler Standort- und Wettbewerbsfaktor. Netzwerke, wie beispielsweise die Allianz für Cybersicherheit, der UP KRITIS oder die Initiative Wirtschaftsschutz, leisten daher einen Beitrag zur Stärkung des Wirtschaftsstandortes Deutschland.

6.4 Staatliche Initiativen und Akteure

Dem Staat kommen bei der Gewährleistung eines hohen Cybersicherheitsniveaus eine herausgehobene Rolle und eine hohe Verantwortung zu. Das staatliche Aufgabenfeld reicht von der Prävention, der Bedrohungslagebilderstellung, der Detektion, der Gefahrenabwehr, der Vorfallsbewältigung und der Strafverfolgung über die Spionageabwehr und die nachrichtendienstliche Vorfeldaufklärung bis hin zur Cyberaußenpolitik und zur Cyberverteidigung. Entsprechend sind auf Bundes- und Landesebene zahlreiche Akteure aktiv, die sich im Rahmen ihrer jeweiligen Zuständigkeiten intensiv mit den Bedrohungen aus dem Cyberraum befassen. Die Aktivitäten des Bundes gliedern sich dabei in eine strategische und eine operative Ebene.

6.4.1 Strategische Ebene

Die strategische Ausrichtung der Cybersicherheitsvorhaben und die Aufsicht über deren Umsetzung sind Aufgabe der Ministerien. Nach dem Ressortprinzip steuern die Ressorts die Aktivitäten in ihrem Bereich eigenständig und

[8] Abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/online-kompendium-nationaler-pakt-cybersicherheit.pdf?__blob=publicationFile&v=4

eigenverantwortlich. Auf Bundesebene kommt dem Bundesministerium des Innern, für Bau und Heimat (BMI) im Bereich der Cybersicherheitsinnenpolitik und dem Auswärtigen Amt im Bereich der Cyberaußenpolitik zusätzlich eine koordinierende Funktion zu. Die Cyberverteidigung fällt in die Zuständigkeit des Bundesministeriums der Verteidigung (BMVg).

Der NCSR ist strategischer Ratgeber der Bundesregierung. Er wurde mit der „Cybersicherheitsstrategie für Deutschland 2011“ eingeführt und mit der „Cybersicherheitsstrategie für Deutschland 2016“ weiterentwickelt. Durch seine Zusammensetzung aus Vertretern aus Bund, Ländern und Kommunen sowie der Wirtschaft kommt ihm eine Scharnierfunktion zwischen den relevanten Akteuren in der deutschen Cybersicherheitslandschaft zu. Seit Oktober 2018 berät zudem eine ständige wissenschaftliche Arbeitsgruppe den NCSR aus Perspektive der Forschung zu Entwicklungen und Herausforderungen einer sicheren und vertrauenswürdigen Digitalisierung.

Die zuständigen Gremien für die strategische Ausrichtung des Informationssicherheitsmanagements des Bundes und die Umsetzung des Kabinettsbeschlusses der „Leitlinie für Informationssicherheit in der Bundesverwaltung (Umsetzungsplan – UP Bund)“ sind der IT-Rat sowie die AG Informationssicherheitsmanagement des IT-Rates. Beim BMI ist die Rolle der oder des Beauftragten der Bundesregierung für Informationstechnik verankert, der oder dem unter anderem die Aufgabe der Steuerung des Informationssicherheitsmanagements auf Grundlage des UP Bund zufällt.

6.4.2 Operative Ebene

Die operative Umsetzung der strategischen Vorgaben und Zielsetzungen erfolgt insbesondere durch die Geschäftsbereichsbehörden des Bundeskanzleramtes und der Ministerien. Den nachfolgend dargestellten Aufgabenbereichen und Akteuren kommt dabei eine besondere Bedeutung zu.

Das BSI ist die zentrale Stelle für Informationssicherheit des Bundes. Im BSI sind das Bundes Security Operations Center (BSOC), das Computer Emergency Response Team des Bundes (CERT-Bund) und das Nationale IT-Lagezentrum verortet. Letzteres wächst in besonderen Lagen zum Nationalen IT-Krisenreaktionszentrum auf. Darüber hinaus ist das BSI für die Sicherheit und den Schutz der Informationstechnik und der Netze des Bundes sowie der nationalen Kritischen Infrastrukturen zuständig und gestaltet die Informationssicherheit in der Digitalisierung durch Prüfungs-, Standardisierungs-, Zertifizierungs-, Zulassungs- und Beratungsleistungen für Staat, Wirtschaft und Gesellschaft und arbeitet hierzu eng mit Akteuren aus allen Bereichen zusammen.

Das Bundesamt für Verfassungsschutz (BfV) dient dem Schutz der Inneren Sicherheit und informiert die Bundesregierung und die Öffentlichkeit über die Sicherheitslage. Es ist zuständig für die Sammlung und Auswertung von Informationen über nachrichtendienstlich gesteuerte sowie extremistisch oder terroristisch motivierte Cyberangriffe. Der Militärische Abschirmdienst (MAD) schirmt die Bundeswehr bereits außerhalb des Verteidigungs- oder Spannungsfalles sowie bei Einsätzen gegen Spionage und Sabotage sowie Extremismus und Terrorismus im Cyberraum ab. Dem Bundesnachrichtendienst (BND) obliegt die Aufgabe, die erforderlichen Informationen zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für Deutschland sind, auch im Cyberraum zu sammeln und auszuwerten. Das Kommando Cyber- und Informationsraum der Bundeswehr (KdoCIR) koordiniert die Cyberverteidigung in der Bundeswehr.

Für die Gefahrenabwehr sind in Deutschland grundsätzlich die Länder zuständig. Dem Bund stehen in bestimmten Bereichen gefahrenabwehrrechtliche Sonderzuständigkeiten zu (zum Beispiel in den Bereichen internationaler Terrorismus, Sicherheit auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes, Grenzschutz oder Eigensicherung), die sich auch auf den Cyberraum erstrecken. Diese Zuständigkeiten werden vom Bundeskriminalamt (BKA), der Bundespolizei (BPOL) und dem BSI wahrgenommen. Die Strafverfolgung im Cyberraum ist Aufgabe der Justiz mit Unterstützung durch die Landeskriminalämter und Polizeibehörden der Länder, beziehungsweise durch das BKA und die BPOL im Rahmen ihrer jeweiligen Zuständigkeiten.

Die Abstimmung zwischen den benannten sowie weiteren relevanten Behörden auf der operativen Ebene erfolgt unter anderem im Cyber-AZ, das bereits 2011 als zentrale Informations- und Koordinationsplattform eingerichtet und über die Jahre weiterentwickelt wurde.

Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) wirkt im Schwerpunkt als Dienstleister für die Sicherheitsbehörden im Geschäftsbereich des BMI mit dem Ziel, deren Cyberfähigkeiten und Digitale Souveränität zu stärken.

Zudem kommt den Behörden und Gesellschaften im Besitz des Bundes eine besondere Bedeutung zu, die mit dem sicheren Betrieb der IT-Infrastruktur des Bundes betraut sind. Hierzu zählen die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) als Bundesnetzbetreiberin, das Informationstechnikzentrum Bund sowie das Auswärtige Amt als Betreiber seiner Auslands-IT.

6.4.3 Die Zusammenarbeit zwischen Bund und Ländern

Die vielfältigen staatlichen Aufgaben im Cyberraum können nur durch eine gemeinsame Anstrengung von Bund und Ländern erfüllt werden. Eine intensive Verzahnung der Aktivitäten der Bundes- und Landesebene auf dem Wege einer kooperativen und komplementären Zusammenarbeit ist hierbei unumgänglich.

Zentrale Gremien zur Abstimmung der Bund-Länder-Zusammenarbeit auf strategischer Ebene sind die Innenministerkonferenz und deren Länderarbeitsgruppe Cybersicherheit sowie der IT-Planungsrat und dessen AG Informationssicherheit. Letztere sind auch für das Informationssicherheitsmanagement zwischen Bund und Ländern zuständig.

Auch auf operativer Ebene bestehen zahlreiche Formate der Zusammenarbeit zwischen Bund und Ländern. Nur beispielhaft sind hier die vertrauensvolle Zusammenarbeit der Verfassungsschutzbehörden aus Bund und Ländern im Verfassungsschutzverbund zu nennen, der intensive Austausch im Verwaltungs-CERT-Verbund (VCV) oder die enge Abstimmung der Landeskriminalämter mit dem BKA als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei. Die immer häufiger seitens der Länder eingerichteten zentralen Koordinierungsstellen für Cybersicherheit sind in diese operative Zusammenarbeit ebenfalls eng eingebunden. Das Nationale Verbindungswesen des BSI gestaltet die Beziehungen des BSI zu nationalen Partnern und steht den Ländern als Ansprechpartner auf regionaler Ebene zur Verfügung.

7 Leitlinien der Cybersicherheitsstrategie

Die in der „Cybersicherheitsstrategie für Deutschland 2021“ erstmals aufgeführten strategischen Ziele und operativen Maßnahmen werden im Licht von Leitlinien betrachtet, geprüft und umgesetzt. Die Leitlinien leiten sich aus den die Handlungsfelder übergreifenden Interessen und Belangen ab und dienen zur Bündelung und Fokussierung, um so ein kohärentes Ineinandergreifen der einzelnen strategischen Ziele und Maßnahmen zu gewährleisten.

7.1 Leitlinie: „Cybersicherheit als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft etablieren“

Cyberbedrohungen und Cyberkriminalität betreffen nicht nur den Staat, sondern auch Unternehmen, wissenschaftliche Einrichtungen, Vereine sowie die Bürgerinnen und Bürger. Um in diesem Umfeld ein hohes Sicherheitsniveau gewährleisten zu können, müssen alle Akteure ihren Beitrag zur Bewältigung von Cyberbedrohungen leisten. Die Bundesregierung versteht Cybersicherheit daher als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft. Dies setzt ein kooperatives Vorgehen sowie eine vertrauensvolle Zusammenarbeit voraus, um gemeinsame Antworten auf Cyberbedrohungen finden zu können.

Bedrohungen im Cyberraum machen nicht an Ländergrenzen halt. Deutschland ist, wie in vielen anderen Bereichen auch, im Bereich Cybersicherheit in ein Netz europäischer und internationaler Zusammenarbeit eingebunden, weshalb Cybersicherheit auch nur in Kooperation mit unseren europäischen und internationalen Partnern gewährleistet werden kann.

7.2 Leitlinie: „Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken“

Das Thema Digitale Souveränität hat seit 2016 deutlich an Relevanz und Aufmerksamkeit gewonnen. Digitale Souveränität wird hier (aus Sicht der Bundesregierung) verstanden als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“[9]. Digitale Souveränität hat somit auch für die Cyber- und Informationssicherheit eine wesentliche Bedeutung; sichere Technologien und Lösungen sowie entsprechende Fähigkeiten, die Chancen und potenziellen Risiken digitaler Technologien erkennen und bewerten zu können, sind eine wesentliche Voraussetzung für die Digitale Souveränität. Ein hohes Cybersicherheitsniveau trägt so zur Stärkung der Digitalen Souveränität von Bürgerinnen und Bürgern, Wirtschaft, Wissenschaft und Staat bei. Auf europäischer Ebene bedeutet Digitale Souveränität eine stärkere wirtschaftliche und sicherheitspolitische Vernetzung mit strategisch wichtigen Partnern, um Abhängigkeiten zu mindern und die politische Handlungs- beziehungsweise Gestaltungsfähigkeit zu bewahren.

Digitale Souveränität ist daher eine zentrale Leitlinie der Cybersicherheitsstrategie 2021 und ein Handlungsmotiv in allen vier Handlungsfeldern. Schwerpunktbereiche sind unter anderem

- die anwendungsorientierte Forschung und Entwicklung sowie der Forschungstransfer (Handlungsfeld 1),
- die Cybersicherheit als Qualitätsmerkmal „Made in Germany“ (Handlungsfeld 2),
- die staatlichen Fähigkeiten zur Beurteilung neuer Technologien und Beauftragung europäischer Anbieter und zur Eigensicherung der Verwaltung (Handlungsfeld 3),

---

[9] Vergleiche Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, abrufbar unter: https://www.it-planungsrat.de/beschluesse/beschluss/ag-cloud-computing-und-digitale-souveraenitaet

- eine gemeinsame Vision und Strategie der EU für Cybersicherheit und europäische Digitale Souveränität (Handlungsfeld 4).

Bei näherer Betrachtung wird deutlich, dass je nach Akteur und Kontext unterschiedliche Aspekte und Dimensionen Digitaler Souveränität im Vordergrund stehen. Das Thema Digitale Souveränität stellt sich somit mit einer hohen Komplexität und Vielfalt dar und wird je nach Handlungsfeld entsprechend differenziert betrachtet.

Initiativen und Anliegen der Bundesregierung

Mit dem am 12. Februar 2020 von der Bundesregierung beschlossenen neuen „Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie“[10] sollen die industriellen Kernfähigkeiten und strategisch relevanten Entwicklungskapazitäten in Deutschland und der EU erhalten und gefördert werden. Diese Strategie bildet den Rahmen für die Politik der Bundesregierung hinsichtlich der Sicherheits- und Verteidigungsindustrie und ist damit wesentliche Leitlinie zum Schutz der Digitalen Souveränität. Damit hat die Bundesregierung bereits entsprechende Maßnahmen in fünf Bereichen benannt:

- Forschung, Entwicklung und Innovationen stärken,
- Rahmenbedingungen für eine effiziente Produktion setzen,
- Beschaffungswesen optimieren,
- Exporte politisch flankieren und verantwortungsvoll kontrollieren und
- Schutz von Sicherheitsinteressen.

Insbesondere sollen zum Schutz der Sicherheitsinteressen Digitale Souveränität und Resilienz gegenüber hybriden Bedrohungen erlangt und die Abhängigkeit von ausländischen Informationstechnologien reduziert werden. Neben den Prüfmechanismen nach dem Außenwirtschaftsgesetz und der Außenwirtschaftsverordnung arbeitet die Bundesregierung an flexiblen und strategisch einsetzbaren Instrumenten als Antwort auf drohende Ausverkäufe zukünftiger sicherheits- und verteidigungsindustrieller Schlüsseltechnologien. Dazu soll auch die Einrichtung eines IT-Sicherheitsfonds vorangetrieben werden, um aktiv unerwünschten Übernahmen begegnen zu können.

Im Bereich „Forschung, Entwicklung und Innovationen stärken“ wird die im Sommer 2020 eingerichtete Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) ambitionierte Forschungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit und diesbezüglicher Schlüsseltechnologien zur Bedarfsdeckung Deutschlands im Bereich der Inneren und Äußeren Sicherheit beauftragen und finanzieren.

Um Ideen mit Marktpotenzial im Bereich der IT-Sicherheit schneller in die Anwendung zu bringen, hat die Bundesregierung die Initiative „StartUpSecure“ ins Leben gerufen. Darin werden Unternehmensgründungen im Bereich der IT-Sicherheit gefördert. Für die Begleitung der jungen Gründungen wurden an den nationalen Kompetenzzentren für IT-Sicherheitsforschung ATHENE (Darmstadt), CISPA (Saarbrücken) und KASTEL (Karlsruhe) sowie an der Ruhr-Universität Bochum Inkubatoren eingerichtet.

Im Bereich Forschung zum Zukunftsthema 6G hat die Bundesregierung das Ziel ausgerufen, dass Deutschland eine führende Rolle als Anbieter vertrauenswürdiger Kommunikationstechnologie in der Weltwirtschaft einnimmt und frühzeitig den technologischen Wandel mitgestaltet. In einem ersten Schritt ist der Aufbau von vier 6G-Forschungs-Hubs und einer Plattform für zukünftige Kommunikationstechnologien und 6G geplant.

Mit Blick auf die öffentliche Verwaltung hat der IT-Planungsrat im März 2021 die „Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung“ beschlossen. Diese führt neben den strategischen Zielen „Wechselmöglichkeit“, „Gestaltungsfähigkeit“ und „Einfluss auf Anbieter“ verschiedene Lösungsansätze und Maßnahmen zur Stärkung der Digitalen Souveränität der Verwaltung aus. Hierbei ist neben rechtlichen Rahmenbedingungen und dem Aufbau von Kompetenzen beziehungsweise Expertenwissen auch die Diversifizierung mit bedarfsgerechten Open-Source-basierten IT-Lösungen als Maßnahme zu nennen.

Unter dem Dach der von der Bundesregierung geförderten Initiative „QuNET“[11] entwickeln die Fraunhofer-Gesellschaft, die Max-Planck-Gesellschaft und das Deutsche Zentrum für Luft- und Raumfahrt seit Ende 2019

[10] Abrufbar unter: https://www.bmwi.de/Redaktion/DE/Artikel/Branchenfokus/Industrie/branchenfokus-sicherheits-und-verteidigungsindustrie.html

[11] Abrufbar unter: https://www.qunet-initiative.de/

Technologien für ein Pilotnetz zur Quantenkommunikation in Deutschland. Dieses soll zukünftig der abhör- und manipulationssicheren Datenübertragung dienen.

7.3 Leitlinie: „Digitalisierung sicher gestalten“

Im Vergleich zu 2016 hat die digitale Transformation von Staat (zum Beispiel E-Government-Gesetz, Onlinezugangsgesetz [OZG], IT-Konsolidierung, mobiles Arbeiten), Wirtschaft (zum Beispiel Sicherheitsanforderungen an 5G-Netze) und Gesellschaft (zum Beispiel der elektronische Identitätsnachweis [eID]) wesentlich an Dynamik gewonnen. Im Jahr 2020 stiegen die Anforderungen und Erwartungshaltungen an die Digitalisierung zudem sprunghaft durch die COVID-19-Pandemie.

Cyber- und Informationssicherheit ist eine Grundvoraussetzung für das Gelingen der Digitalisierung in Deutschland. Ohne deren sichere Ausgestaltung können die Menschen sich nicht frei und selbstbestimmt in einer digitalisierten Umgebung bewegen. Ein hohes Niveau an Cybersicherheit ermöglicht es hingegen, Potenziale der Digitalisierung voll zu nutzen und Gefahren selbstbewusst und selbstbestimmt zu begegnen. Daher wird das Thema „Digitalisierung sicher gestalten“ als Leitlinie der Cybersicherheitsstrategie 2021 in allen Handlungsfeldern durch entsprechende strategische Ziele adressiert.

Initiativen und Anliegen der Bundesregierung

Die Bundesregierung hat verschiedene Initiativen und Maßnahmen vorangebracht, um den digitalen Wandel in Deutschland zu gestalten. Die aktuelle Umsetzungsstrategie „Digitalisierung gestalten“[12] adressiert verschiedene Schwerpunktvorhaben zur Umsetzung digitalpolitischer Maßnahmen, unter anderem in den Bereichen digitale Kompetenzen, Infrastruktur, digitale Transformation von Staat und Gesellschaft sowie zur Ethik für eine digitale Gesellschaft.

Beispiele:

- Im Cybercluster der Universität der Bundeswehr München wird neben der Forschung und Entwicklung am Forschungsinstitut CODE die wissenschaftliche Aus-, Fort- und Weiterbildung insbesondere von Offizieren und Beschäftigten des Bundes mit dem Schwerpunkt Cybersicherheit durchgeführt.
- Unter dem Namen „Digital. Sicher. Souverän.“ hat die Bundesregierung ein neues Forschungsrahmenprogramm zur IT-Sicherheit aufgesetzt.
- Mit der Gründung der Cyberagentur werden ressortübergreifend Forschungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit und diesbezüglicher Schlüsseltechnologien zur Bedarfsdeckung im Bereich der Inneren und Äußeren Sicherheit Deutschlands möglich.

Mit der „Netzstrategie 2030 für die öffentliche Verwaltung“ [13] wurde die Netzstrategie der Bundesregierung aus dem Jahr 2013 überarbeitet und fortgeschrieben. Damit wurde den gestiegenen Anforderungen im Bereich der Kommunikationsfähigkeit der gesamten öffentlichen Verwaltung Deutschlands, neuen technischen Entwicklungen und den erhöhten Sicherheitsanforderungen Rechnung getragen. Ziel ist es, einen Informationsverbund der öffentlichen Verwaltung Deutschlands („IVÖV“) in Betriebsverantwortung der Bundesnetzbetreiberin (BDBOS) zu etablieren. Hierzu wurden folgende strategische Ziele definiert:

- Nationale Digitale Souveränität,
- Leistungsfähigkeit der Netzinfrastruktur,
- Informationssicherheit & Datenschutz & Geheimschutz,
- Zukunftsfähigkeit und Flexibilität und
- Digitale und ebenenübergreifende Zusammenarbeit.

[12] Abrufbar unter: https://www.bundesregierung.de/breg-de/service/publikationen/digitalisierung-gestalten-1605002

[13] Abrufbar unter: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/Moderne-Verwaltungskommunikation/netzstrategie_2030_fuer_die_oeffentliche_verwaltung.html?nn=4624892

Zur Umsetzung dieser strategischen Ziele wurden folgende strategische Handlungsfelder definiert und ein dazugehöriger Umsetzungskatalog erstellt:

- Strategische Ausgestaltung der Fertigungstiefe,
- Weiterentwicklung der aktiven Dienstleistersteuerung,
- Konsolidierung von Weitverkehrsnetzen,
- Internetressourcen und Standardisierung,
- Gewährleistung von Informationssicherheit, Datenschutz und Geheimschutz in Netzinfrastrukturen der öffentlichen Verwaltung,
- Weiterentwicklung des Anforderungs- und Nutzermanagement sowie der Diensteentwicklung und
- Förderung von Innovationen und Schlüsseltechnologien für eine bürgernahe und moderne Verwaltung.

Somit ist die „Netzstrategie 2030 für die öffentliche Verwaltung“ ein wichtiger Baustein, um Cybersicherheit in Deutschland zu gewährleisten.

7.4 Leitlinie: „Ziele messbar und transparent ausgestalten“

Die Transparenz staatlichen Handels ist wichtig für das Vertrauen von Bürgerinnen und Bürgern in den Staat. Der Nutzen und die Wirkung staatlicher Initiativen müssen entsprechend nachvollziehbar sein. Im Rahmen der Cybersicherheitsstrategie 2021 werden daher erstmals die Themen Messbarkeit und Transparenz adressiert. Umsetzung und zukünftige Fortschreibungen können so systematisch vorbereitet werden.

Um den Erfolg der Cybersicherheitsstrategie 2021 bewerten zu können, wird die Zielerreichung sowohl zum Ende der Laufzeit abschließend evaluiert als auch während der Laufzeit regelmäßig überprüft. Hierfür werden in allen Handlungsfeldern die angestrebten Ziele messbar formuliert. Für jedes strategische Ziel werden Indikatoren entwickelt, um die Zielerreichung überprüfen zu können.

Die Cybersicherheitsstrategie 2021 unterscheidet zwischen strategischen Zielen und operativen Maßnahmen:

Strategische Ziele

Strategische Ziele definieren SMARTe (spezifische, messbare, aktiv beeinflussbare, realistische und terminierte) Ziele innerhalb eines Handlungsfeldes, die im Rahmen der Umsetzung der Cybersicherheitsstrategie erreicht werden sollen. Strategische Ziele adressieren die Herausforderungen des Handlungsfeldes und beschreiben einen Zustand, der durch die Strategie angestrebt wird. Strategische Ziele werden spezifisch und konkret formuliert, um überprüfbar zu sein. Für jedes strategische Ziel werden zudem Indikatoren definiert, um die Zielerreichung messen zu können. Die strategischen Ziele sollen grundsätzlich innerhalb eines Zeitraums von fünf Jahren erreichbar sein.

Maßnahmen

Maßnahmen beschreiben Aktivitäten, mit denen die strategischen Ziele erreicht werden sollen. Sie müssen in ihrer Gesamtheit geeignet sein, das jeweilige strategische Ziel in der Laufzeit der Cybersicherheitsstrategie 2021 vollständig zu erreichen. Maßnahmen können beispielsweise einzelne Projekte oder fortlaufende Maßnahmen sein. Die Maßnahmen sind nicht Gegenstand der Strategie, sie werden als fortlaufende Aktivitäten nachgelagert geplant und umgesetzt (vergleiche Kapitel 9 „Umsetzung, Berichtswesen, Controlling und Evaluierung der Cybersicherheitsstrategie“).

8 Handlungsfelder der Cybersicherheitsstrategie

Im folgenden Kapitel werden die Handlungsfelder der Strategie beschrieben und mit den strategischen Zielen verknüpft. Getragen durch das Verständnis, dass Cybersicherheit nur gemeinsam gewährleistet werden kann (siehe Kapitel 7.1 Leitlinie „Cybersicherheit als eine geminsame Aufgabe vo Staat, Wirtschaft, Wissenschaft und Gesellschaft etablieren“), werden die bewährten Handlungsfelder

1. Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung,
2. Gemeinsamer Auftrag von Staat und Wirtschaft,
3. Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur und
4. Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik

beschrieben. Die strategischen Ziele wurden nach ihrer primären Schwerpunktsetzung den Handlungsfeldern zugeordnet. Einige Ziele sind hinsichtlich der benötigten Akteure, der Schwerpunkte in der Umsetzung oder hinsichtlich der zu erzielenden Wirkung nicht eindeutig nur einem Ziel zuzuordnen. In der Umsetzung ist darauf zu achten, dass alle erforderlichen Akteure eingebunden werden und übergreifend agiert wird.

8.1 Handlungsfeld 1: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

Damit Bürgerinnen und Bürger die Chancen digitaler Technologien nutzen können, müssen sie sich sicher und selbstbestimmt in einer digitalisierten Umgebung bewegen. Sie müssen neben den Chancen auch die Risiken digitaler Technologien erkennen, bewerten und die Herausforderungen durch eigenes Handeln wirksam bewältigen können.

Einen wichtigen Beitrag, um die Beurteilungskompetenz der Bürgerinnen und Bürger zu steigern, leisten etwa Kennzeichnungen von Produkten und Dienstleistungen, die deren Konformität zu IT-Sicherheitsstandards belegen.

Insgesamt hat die Bundesregierung mehrere Möglichkeiten, um die „Cybersicherheitskompetenz“ der Gesellschaft zu steigern: Sie kann Maßnahmen ergreifen und Produkte anbieten, die die Bürgerinnen und Bürger sensibilisieren, sie kann Maßnahmen des klassischen Verbraucherschutzes ergreifen und sie kann anhand von Regulierungsmaßnahmen einen Rahmen schaffen, der sicheres und selbstbestimmtes Handeln fördert. Hieran orientieren sich die folgenden Ziele.

8.1.1 Digitale Kompetenzen bei allen Anwenderinnen und Anwendern fördern

Warum ist das Ziel relevant?

Das Bewusstsein für sicheres Verhalten im Cyberraum ist bei allen Nutzenden, von Bürgerinnen und Bürgern über kleine wie große Unternehmen bis hin zu allen staatlichen Stellen zentrale Voraussetzung für den Schutz vor Cyberrisiken und digitaler Sorglosigkeit.

Wo stehen wir?

Digitale Kompetenzen zu schaffen, ist ein fortlaufender Prozess, der sich parallel zu neuen Technologien und Trends mitentwickeln muss. In den letzten Jahren ist es gelungen, das Bewusstsein für die Relevanz von IT-Sicherheit bei allen Akteuren deutlich zu steigern. Zahlreiche staatliche und nichtstaatliche Projekte leisten gute Aufklärungsarbeit, die fortgeführt und intensiviert werden muss. Insbesondere im Bereich der schulischen und betrieblichen Bildung sollte das Wissen rund um IT-Sicherheit jedoch noch zielgerichteter gestärkt werden.

Das Bundesministerium für Bildung und Forschung (BMBF) begegnet diesen Herausforderungen mit gezielter Forschungsförderung, beispielsweise im Förderschwerpunkt „Unterstützung von Bürgerinnen und Bürgern bei der privaten IT-Sicherheit“[14] oder mit Förderrichtlinien wie „Sichere Industrie 4.0 in der Praxis“[15] sowie durch die Förderung des „Forum Privatheit“[16], das sich interdisziplinär mit gesellschaftlich relevanten Fragen zum Schutz der Privatheit auseinandersetzt und kontinuierlich zu Cyberrisiken und Datenschutzfragen sensibilisiert.

Auch die seit März 2021 laufende bundesweite Informations- und Sensibilisierungskampagne zur IT-Sicherheit „#einfachaBSIchern“ des BMI und des BSI sowie die Verbraucherschutzseiten des BSI[17] zielen auf die digitale Kompetenz, in dem sie die Anwenderinnen und Anwender für Risiken im Cyberraum sensibilisieren und informieren.

Seit 2006 bietet der durch das BMI geförderte Verein Deutschland sicher im Netz (DsiN) vielfältige Hilfestellungen für Bürgerinnen und Bürger sowie kleinere Unternehmen. Dazu gehören die Angebote der „Digitalen Nachbarschaft“ für Vereine und ehrenamtliche Engagierte für Sicherheit im Netz[18], „PolisiN – Politiker:innen sicher im Netz“[19] für ehren- und hauptamtliche Mandatsträger sowie „BottomUp – Berufsschulen für IT-Sicherheit“[20] für Schutzkompetenzen in der Dualen Ausbildung. Mit der durch das Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Transferstelle „IT-Sicherheit im Mittelstand“ (TISiM) betreibt DsiN im Verbund mit weiteren Partnern aus Wirtschaft und Wissenschaft bundesweit 80 Anlaufstellen, um insbesondere kleine Unternehmen, Selbstständige und Freiberufler bei der Umsetzung von IT-Sicherheitsmaßnahmen zu begleiten.

Was wollen wir erreichen?

Das erforderliche Bewusstsein und Verständnis von KMU, Bildungs- und Sozialeinrichtungen, Verbänden, Vereinen, Verbraucherinnen und Verbrauchern im Umgang mit immer komplexer werdenden Technologien, Dienstleistungen und Geschäftsmodellen wird gefördert.

Die Vermittlung digitaler Kompetenzen ist Bestandteil einer breiten Ausbildung an Schulen, Hochschulen, Universitäten und im betrieblichen Umfeld. Zudem können Anwenderinnen und Anwender auf zielgruppenspezifische Informations- und Unterstützungsangebote zu allen Fragen der Informations- und Cybersicherheit zurückgreifen sowie unter anderem ihr Kompetenzniveau über den vom BMI geförderten DsiN-Digitalführerschein[21] zertifizieren lassen. Diese werden weiter ausgestaltet und ausgebaut.

Dadurch verfügen Anwenderinnen und Anwender über digitale Kompetenzen und können die Vorteile der Digitalisierung nutzen. Sie verfügen über ein Problembewusstsein im Hinblick auf Cyberrisiken und sind in der Lage, die Sicherheit von Anwendungen und Diensten zu bewerten und entsprechend risikobewusst zu agieren.

Welche Wirkung erwarten wir?

Wirtschaft (insbesondere KMU), Wissenschaft und Gesellschaft sind resilienter gegenüber den Gefahren im Cyberraum. Sie nutzen die Vorteile der Digitalisierung und wissen mit ihren Herausforderungen umzugehen und sich zu schützen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Der durch das BMI geförderte Digitalführerschein wird in der Bevölkerung gut nachgefragt und trägt zur Steigerung der Digitalkompetenzen bei den Bürgerinnen und Bürgern – sowohl im privaten als auch im beruflichen Kontext – bei.
- Informationsangebote des BSI werden durch Verbraucherinnen und Verbraucher vermehrt angenommen.

---

14 Abrufbar unter: https://www.bmbf.de/foerderungen/bekanntmachung-3160.html
15 Abrufbar unter: https://www.bmbf.de/foerderungen/bekanntmachung-2019.html
16 Abrufbar unter: https://www.bmbf.de/foerderungen/bekanntmachung-2547.html
17 Abruf unter: https://www.bsi.bund.de/VerbraucherInnen
18 Abrufbar unter: https://www.digitale-nachbarschaft.de/
19 Abrufbar unter: https://polisin.de/
20 Abrufbar unter: https://www.dsin-berufsschulen.de/
21 Abrufbar unter: https://www.sicher-im-netz.de/dsin-digitalfuehrerschein

- Verbraucherinnen und Verbraucher sind sensibilisiert und informiert, sie beschäftigen sich verstärkt mit Cybersicherheitsthemen und können Cyberrisiken besser einschätzen und ihnen entgegentreten.
- Die Zahl der von Cyberangriffen betroffenen Privatpersonen ist rückläufig.

8.1.2 Anwenderfreundlichkeit sicherheitstechnischer Lösungen steigern

Warum ist das Ziel relevant?

Gerade bei IT-Sicherheitslösungen, die zum Teil sehr spezielle Anforderungen erfüllen müssen, spielt Anwenderfreundlichkeit bei der Entwicklung oftmals eine untergeordnete Rolle. Sie ist aber wesentlich für die Akzeptanz und damit die aktive Nutzung entsprechender Produkte. Hinzu kommt, dass auch die (Ausfall-) Sicherheit beziehungsweise „Festigkeit“ eines Produktes, also der Schutz vor Fehlfunktionen oder vor Cyberangriffen, wesentlicher Bestandteil der Nutzererfahrung ist, der mit zunehmender Abhängigkeit von IT mehr und mehr an Bedeutung gewinnt.

Wo stehen wir?

Dass sich Informationssicherheit und Anwenderfreundlichkeit nicht ausschließen, zeigen mittlerweile vielfach standardmäßig eingesetzte IT-Sicherheitsmaßnahmen. Beispielhaft zu nennen sind hier die Ende-zu-Ende-Verschlüsselung sowie die sogenannte Zwei-Faktor-Authentifizierung. Deren Anwenderfreundlichkeit ist Hauptgrund für ihre breite Verwendung.

Da jedoch Ausschreibungen von Sicherheitslösungen im Regelfall besonders preissensitiv sind, den Anwenderinnen und Anwendern in der Regel keine Nutzungsalternative zur Verfügung steht und die Nutzererfahrung bei der Realisierung in der Regel eine untergeordnete Rolle spielt, sind Sicherheitslösungen heute oftmals anwenderunfreundlich und werden in der Folge nicht genutzt.

Die bestehende Diskrepanz der Nutzerzahlen zwischen Messenger-Diensten und anderweitigen Sicherheitslösungen (zum Beispiel VPN-Lösungen) verdeutlicht, dass die fachliche Eignung eines Sicherheitsproduktes allein nicht ausreicht, um Anwenderinnen und Anwendern die sinnvolle Nutzung oder IT-Dienstleistern eine skalierbare Lösungsbereitstellung zu ermöglichen. Nur wenn bei der Entwicklung die drei Dimensionen „Sicherheit“, „Anwenderfreundlichkeit“ und „Betriebsführung“ berücksichtigt werden, kann der erwünschte Sicherheitsgewinn auch entfaltet werden.

Was wollen wir erreichen?

Wir haben geprüft, inwiefern in der Bundesverwaltung eingesetzte Sicherheitslösungen entweder anwenderfreundlicher ausgeschrieben oder anwenderfreundliche Lösungen sicherer ausgestaltet werden können.

Wir fördern die Integration prüfbarer Sicherheitseigenschaften in anwenderfreundlichen, marktgängigen IT-Produkten. Best Practices hierfür sind unter anderem die am Markt gängigen Messenger-Apps, die mittlerweile zu einem Großteil Ende-zu-Ende-Verschlüsselung anbieten, ohne dass spürbare Einschränkungen in der Bedienbarkeit wahrnehmbar sind.

Welche Wirkung erwarten wir?

Anwenderfreundlichkeit, Ergonomie, aber auch Leistungsfähigkeit von Sicherheitslösungen entsprechen den erforderlichen, erwünschten sowie gleichermaßen erwarteten Eigenschaften marktgängiger Geräte und Lösungen. Marktgängige Lösungen werden mittels der Integration von IT-Sicherheitseigenschaften sicherer. Nachdem Entwicklung und Sicherheitsbetrachtung neu ausgerichtet wurden, wird die (Investitions-) Bereitschaft für Einsatz und Nutzung sicherheitstechnischer Lösungen steigen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Bundesregierung hat Anforderungen an die Anwenderfreundlichkeit sicherheitstechnischer Lösungen in ihre Ausschreibungen aufgenommen.

- Die Forschung und Entwicklung im Bereich anwenderfreundlicher Sicherheitslösungen wurde intensiviert. Die Themen Usable Security und Security-by-Design haben verstärkt Einzug in Programme und Richtlinien der Forschungsförderung erhalten.
- Die Anzahl marktgängiger, anwenderfreundlicher Produkte, die IT-Sicherheitseigenschaften integriert haben, wie zum Beispiel Ende-zu-Ende-Verschlüsselung, ist gestiegen.
- Die Nutzung von Produkten mit IT-Sicherheitseigenschaften ist gestiegen.

8.1.3 Staatliche Angebote des digitalen Verbraucherschutzes ausbauen

Verbandsklagerecht und Nutzung von Synergien mit Verbraucherzentralen

Verbraucherverbände können mittels des Verbandsklagerechts (zum Beispiel Unterlassungsklagegesetz oder Gesetz gegen unlauteren Wettbewerb) gerichtlich durchsetzen, dass Unternehmen bestimmte verbraucherschutzrechtswidrige Geschäftspraktiken unterlassen müssen, ohne dass die Verbände in eigenen Rechten betroffen sind. Das BSI kann mit seiner fachlichen Expertise im Bereich der IT-Sicherheit und im Rahmen seines gesetzlichen Auftrags dieses Vorgehen der Verbraucherzentralen mittelbar unterstützen, indem es informationstechnische Produkte zur Erfüllung seiner gesetzlichen Aufgaben untersucht und die hieraus gewonnenen Erkenntnisse unter Einhaltung der gesetzlichen Vorgaben Dritten zur Verfügung stellt. Ebenso darf das BSI die Verbraucherzentralen allgemein in Fragen der Sicherheit der Informationstechnik beraten. Im Ergebnis kann das BSI daher dazu beitragen, dass Synergieeffekte auch durch die Verbraucherzentralen zur Stärkung des Verbraucherschutzes im Bereich der IT-Sicherheit genutzt werden können.

Warum ist das Ziel relevant?

Durch die zunehmende Vernetzung von Informations- und Unterhaltungselektronik, Haushaltsgeräten oder anderen Gegenständen des täglichen Gebrauchs sowie die Nutzung digitaler Dienste entstehen neue Risiken und potenzielle Angriffsflächen. Sicherheit wird daher im Sinne eines „digitalen Verbraucherschutzes“ immer wichtiger – für einzelne Anwenderinnen und Anwender ebenso wie für die Gesellschaft.

Wo stehen wir?

Die Bundesregierung widmet sich mit ihren Angeboten bereits der Information und Sensibilisierung der Verbraucherinnen und Verbraucher. So unterhält zum Beispiel das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) auf seiner Homepage ein Verbraucherportal und fördert die DsiN-Projekte „Digital-Kompass plus“[22] und den durch das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) geförderten „Digitalen Engel“[23] zur Befähigung von älteren Menschen in ländlichen Regionen. Ebenso stellt das BSI Broschüren und Wegweiser[24] für den digitalen Alltag zur Verfügung und stellt über die „Cyberfibel“[25] zusammen mit DsiN umfassende Hilfestellungen für Wissensvermittler im digitalen Verbraucherschutz bereit. Der digitale Verbraucherschutz wurde im Rahmen des IT-Sicherheitsgesetzes im Mai 2021 als Aufgabe des BSI etabliert und der gesamtgesellschaftliche Dialog zur Cybersicherheit verstetigt.

Was wollen wir erreichen?

Die staatlichen Angebote des digitalen Verbraucherschutzes sind ausgebaut und das Vertrauen der Bürgerinnen und Bürger in die staatliche Unterstützung bei der Nutzung neuer Technologien ist gestärkt. Das BSI steht als Ansprechpartner zur Verfügung und hat dazu sein Service- und Informationsangebot ausgebaut. Auf Basis einer erweiterten Marktbeobachtung für Verbraucherprodukte und -dienste sowie im Austausch mit den entsprechenden Anbietern stellt das BSI sicherheitsrelevante Informationen bereit.

Die Kooperation des BSI mit den Verbraucherzentralen führt zu Synergieeffekten im Bereich technischer Expertise und dem Verbandsklagerecht.

---

22 Abrufbar unter: https://www.digital-kompass.de/

23 Abrufbar unter: https://www.digitaler-engel.org/

24 Abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Broschueren/broschueren_node.html

25 Abrufbar unter: https://www.cyberfibel.de/

Über einen Beirat Digitaler Verbraucherschutz beim BSI sollen Vertreterinnen und Vertreter aus den etablierten Disziplinen des Digitalen Verbraucherschutzes das BSI in Fragen des Digitalen Verbraucherschutzes unabhängig beraten.

Welche Wirkung erwarten wir?

Mit einer zielgruppengerechten Ansprache durch Informationsübermittlung und Hilfestellung wird das Cybersicherheitsniveau und damit auch die gesellschaftliche Widerstandsfähigkeit gegen Cybergefahren jeglicher Art deutlich erhöht. Die Sicherheitseigenschaften von Verbraucherprodukten wurden als ein Kriterium zur Kaufentscheidung etabliert. Infolgedessen berücksichtigen mehr Hersteller die IT-Sicherheitsaspekte ihrer Produkte.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das BSI führt eine Marktbeobachtung von IT-Produkten und Dienstleistungen für den Verbrauchermarkt sowie eigene Testungen dieser durch.
- Das BSI hat für die grundsätzliche Beratung, Erfassung, Koordinierung, Beantwortung und Dokumentation von Anfragen der Zielgruppen Staat, Wirtschaft und Gesellschaft ein zentrales Service-Center eingerichtet (Multichannel First-Level-Support).
- Zielgruppenspezifische Bedarfe der Bürgerinnen und Bürger werden ermittelt, um diese Erkenntnisse in adressatengerechte Sensibilisierungsmaßnahmen einfließen zu lassen.
- Beim BSI ist ein Beirat Digitaler Verbraucherschutz dauerhaft etabliert.

8.1.4 Europäisch einheitliche Sicherheitsanforderungen

Warum ist das Ziel relevant?

Die Cybersicherheit von im Markt befindlichen Produkten, aber auch Diensten ist bisweilen unzureichend und auch nicht transparent nachvollziehbar. Diesem Umstand sollte mit einer Erhöhung des Cybersicherheitsniveaus auf europäischer Ebene begegnet werden. Insbesondere sollten EU-weit einheitlich verbindliche IT-Sicherheitsanforderungen eingeführt werden.

Wo stehen wir?

Unter der deutschen EU-Ratspräsidentschaft 2020 wurden Ratsschlussfolgerungen zur Cybersicherheit vernetzter Geräte erarbeitet, die einen wichtigen Anstoß für EU-weit einheitliche, anerkannte und rechtlich verbindliche IT-Sicherheitsanforderungen gegeben haben. Um Verbraucherinnen und Verbrauchern ein klareres Verständnis von in Produkten vorhandenen Cybersicherheitseigenschaften zu ermöglichen, wird mit dem IT-Sicherheitsgesetz 2.0 ein nationales freiwilliges IT-Sicherheitskennzeichen eingeführt.

Was wollen wir erreichen?

Verbraucherinnen und Verbraucher können darauf vertrauen, dass Produkte und Dienste einem angemessenen Cybersicherheitsniveau entsprechen und die Einhaltung der erforderlichen Cybersicherheitseigenschaften europaweit einheitlich geregelt ist.

Die Konformität zu EU-weit gültigen, verbindlichen IT-Sicherheitsanforderungen wird in geeigneter Weise auf den Produkten transparent gemacht. Die Bundesregierung hat das nationale, freiwillige IT-Sicherheitskennzeichen als möglichen Ansatz in die Diskussion eingebracht.

Welche Wirkung erwarten wir?

Verbraucherinnen und Verbraucher werden durch die Nutzung gekennzeichneter Produkte geschützt und ihr Vertrauen in diese wird erhöht. Durch verbindliche IT-Sicherheitsanforderungen werden das Cybersicherheitsniveau im europäischen Binnenmarkt insgesamt erhöht sowie das Sicherheitsbewusstsein in Unternehmen und Wissenschaft gestärkt. Infrastruktur, Mitarbeitende, Produkte und Dienstleistungen werden resilienter gegen Cyberangriffe. Gleichzeitig wird durch verbindliche IT-Sicherheitsanforderungen die Wettbewerbsfähigkeit europäischer Unternehmen gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Infrastrukturen und Kompetenzen zur Marktüberwachung wurden beim BSI aufgebaut und genutzt und kommen insbesondere beim IT-Sicherheitskennzeichen zum Einsatz.
- Das IT-Sicherheitskennzeichen wird in der Fläche von Verbraucherinnen und Verbrauchern sowie Herstellern oder Dienstleistern angenommen und akzeptiert, die Anzahl erteilter nationaler IT-Sicherheitskennzeichen steigt kontinuierlich.
- Es werden verbindliche IT-Sicherheitseigenschaften auf EU-Ebene eingeführt und durch ein geeignetes europäisches Kennzeichen (zum Beispiel die CE-Kennzeichnung oder als explizites IT-Sicherheitskennzeichen) für Verbraucherinnen und Verbraucher transparent gemacht.
- Verbindliche IT-Sicherheitsanforderungen für IT-Verbraucher-Produkte werden in Folge der Ratsschlussfolgerungen zur Cybersicherheit vernetzter Produkte auf europäischer Ebene vorbereitet und umgesetzt.

8.1.5 Sichere elektronische Identitäten gewährleisten

Warum ist das Ziel relevant?

Im digitalen Zeitalter sind sichere elektronische Identitäten (eIDs) wesentlich für viele alltägliche Tätigkeiten. Sie sind relevant für Wirtschaft, Wissenschaft und private Nutzende. Für staatliches Handeln sind sie sogar ein unverzichtbarer Grundbaustein. Die Festlegung von Anforderungen an eID-Verfahren sowie deren Absicherung sollten daher durch den Staat erfolgen, damit eine einheitliche übergreifende Lösung für alle Anwendungsbereiche geschaffen wird.

Vertrauenswürdige eIDs stärken die Digitale Souveränität und den Binnenmarkt Europas, indem sie einen digitalen Identitätsnachweis gegenüber Diensteanbietern im Internet ermöglichen. Eine Digitalisierung der Verwaltung (zum Beispiel Umsetzung des OZG) setzt sichere und nutzerfreundliche Identitäten voraus. Für deren Umsetzung und als Basis für ein Identitätsökosystem mit der Wirtschaft werden geeignete, in der Bevölkerung breit akzeptierte elektronische Identifizierungsmittel mit der dazugehörigen eID-Infrastruktur benötigt.

Elektronische Identitäten haben das Potenzial, die wirtschaftliche Entwicklung von Volkswirtschaften zu fördern – durch Optimierung von Prozessen und Lieferketten, den nahtlosen und sicheren Austausch vertrauenswürdiger Informationen, Zeitersparnis für Bürgerinnen, Bürger und Unternehmen sowie die Reduktion von Betrugsmöglichkeiten. Dieses Potenzial gilt es auch für Deutschland flächendeckend zu erschließen. Ein zentraler Baustein dafür ist die staatliche deutsche Online-Ausweisfunktion: Dieses international als hochsicher anerkannte Identifizierungsmittel (gemäß eIDAS-Verordnung für das höchstmögliche Vertrauensniveau notifiziert) ist die Grundlage für die hoheitliche Identifizierung. Identität hat jedoch viele Facetten und ist je nach Anwendungsfall deutlich weiter zu verstehen als nur die Angaben auf dem Personalausweis, dem elektronischen Aufenthaltstitel oder der eID-Karte für Bürgerinnen und Bürger der EU, die bei der Online-Ausweisfunktion verwendet werden. Neben der Möglichkeit, mit Hilfe der Online-Ausweisfunktion nachzuweisen, dass Ausweisinhaberinnen und -inhaber sind, wer sie behaupten zu sein, können daher weitere Attribute für weitere digitale Identitäten bedeutend sein, zum Beispiel ein bestimmter Schul- oder Studienabschluss.

Wo stehen wir?

Bürgerinnen und Bürger erledigen Behördliches und Geschäftliches zunehmend mit ihren Smartphones. Sie sollen daher künftig ihre Online-Ausweisfunktion direkt in ihren Smartphones speichern können und sich künftig auch ohne Ausweiskarte nur mit dem Smartphone innerhalb weniger Sekunden sicher digital ausweisen können.

Um das Potenzial von eIDs zu identifizieren, wurde eine interministerielle Projektgruppe gegründet mit dem Ziel, die digitale Identität im Alltag einfacher und komfortabler nutzbar zu machen.

Das BSI gestaltet dafür sichere eIDs durch die Entwicklung von Spezifikationen und die Mitarbeit bei der Pilotierung und Umsetzung neuer Technologien, insbesondere für das smartphonebasierte Online-Ausweisen. Zugleich soll das kartenbasierte Online-Ausweisen für die Bürgerinnen und Bürger durch neue Zusatzdienste und Verbesserungen nutzerfreundlicher werden. Auch privatwirtschaftliche Unternehmen unterhalten auf Basis ihrer Geschäftsmodelle ein umfassendes Identitätsmanagement. Der sichere staatliche Online-Ausweis kommt hierbei teilweise zum Einsatz, ist aber ein Identifizierungsangebot neben anderen Angeboten. Die verschiedenen Identifizierungsangebote sind in der Regel nicht interoperabel und hinsichtlich der Datenverwendung unterschiedlich ausgestaltet. Zudem ist der Markt stark fragmentiert. Mit der zunehmenden Durchdringung immer weiterer Lebensbereiche mit Technologie sowie den Geschäftsinteressen der privatwirtschaftlichen Anbieter von Identifizierungslösungen bedarf es zur Stärkung der Digitalen Souveränität eines verstärkten staatlichen Angebotes, das Sicherheit, Datenschutzkonformität, Selbstsouveränität, Nutzerfreundlichkeit sowie flexible und weitverbreitete Einsatzmöglichkeiten bietet.

Was wollen wir erreichen?

Der Online-Ausweis auf dem Smartphone ist aus dem Personalausweis abgeleitet und kann im Sicherheitselement des Smartphones gespeichert werden. Diese Smart-eID kann neben der Ausweiskarte für den Identitätsnachweis im Internet gegenüber Unternehmen und Behörden verwendet werden. Die Wirtschaft bietet mehr Anwendungen für den Online-Ausweis und die Smart-eID an. Die Smart-eID ist seitens der Europäischen Kommission notifiziert und somit ein EU-weit anerkanntes Identifizierungsmittel.

Welche Wirkung erwarten wir?

Mit dem Online-Ausweis auf dem Smartphone werden die breite Akzeptanz und Verbreitung der eID-Sicherheitsinfrastruktur in Deutschland geschaffen beziehungsweise ausgebaut und ein Beispiel für sichere Smartphone-Anwendung in der EU gegeben.

Sichere, staatlich geprüfte eIDs schaffen Vertrauen in Technologie, sie schaffen neue Möglichkeiten der Wertschöpfung und schützen unter anderem vor Straftaten auf Basis digitalen Identitätsdiebstahls.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl der Downloads und Installationen der Ausweis-App2 (inklusive Ausweis-Applet) auf dem Smartphone ist gestiegen.
- Die Anzahl aktiver Nutzerinnen und Nutzer des Online-Ausweises ist gestiegen.
- Die Anzahl der Internetangebote für den Online-Ausweis ist gestiegen.
- Die Smart-eID ist seitens der Europäischen Kommission notifiziert und somit ein EU-weit anzuerkennendes Identifizierungsmittel.
- Ein Identitätsökosystem mit der Wirtschaft wurde pilotiert.
- Die Smart-eID ist für das Smartphone bereitgestellt. Es wird eine sichere eID-Infrastruktur für Smartphones angeboten.
- Das kartenbasierte Online-Ausweisen mit dem Personalausweis, dem elektronischen Aufenthaltstitel und der eID-Karte für Unionsbürgerinnen und -bürger ist anwendungsfreundlich ausgestaltet.

8.1.6 Elektronische Identitäten (von Personen und Dingen) im weiteren Sinne und Authentizität und Integrität von Algorithmen, Daten und Dokumenten absichern

Warum ist das Ziel relevant?

Die fortschreitende Digitalisierung ist bereits heute das Ergebnis einer enormen Vernetzung von physischen Objekten, Algorithmen, Daten, Dokumenten und Personen. Die Anzahl und auch die Vernetzung der Teilnehmenden unterschiedlicher digitaler Netzwerke wird in Zukunft stetig zunehmen. Beispiele hierfür sind unter anderem IoT, vernetzte Fahrzeuge, verteilte KI-Systeme, Energienetzwerke und digitale Lernplattformen. Eine Absicherung der Identitäten (Personen und Objekte) beziehungsweise der Authentizität und Integrität (Daten, Algorithmen und Dokumente) der Teilnehmenden dieser Netzwerke ist Grundvoraussetzung für das Vertrauen in diese Netzwerke und damit für die Digitalisierung.

Wo stehen wir?

Identitäten spielen aktuell eine zentrale Rolle in der Digitalisierung. Neben der Identität einer Person aus dem Online-Ausweis[26] gibt es zahlreiche weitere Identitäten, die stetig an Bedeutung zunehmen. Hierzu zählen neben den nicht hoheitlichen Identitäten von Personen, wie zum Beispiel der Schülerausweis und Identitäten von Personen in elektronischen Medien (mediale Identitäten), auch die Identitäten physischer Objekte, wie zum Beispiel von Fahrzeugen oder Sensoren. Zudem spielen die Authentizität und die Integrität von Algorithmen (etwa neuronalen Netzen), von Dokumenten (zum Beispiel Zeugnissen) und von Daten (zum Beispiel Flugrouten und Start- und Landeanweisungen im Luftverkehr) eine bedeutende Rolle.

Diese Identitäten beziehungsweise ihre Authentizität und Integrität können mit hinreichendem Aufwand gefälscht werden. Dies kann Schäden hinsichtlich Finanzen, Gesundheit und persönlicher Reputation nach sich ziehen. Vulnerabilitäten und angemessene Verteidigungsstrategien sind in vielen Fällen Gegenstand aktueller Forschung. So wird die Fälschung medialer Identitäten mittels Methoden der KI (Deep Fakes) auch für Laien immer einfacher und kann für Betrugsversuche oder zur gezielten Beeinflussung von Meinungen eingesetzt werden.

Was wollen wir erreichen?

Die Sicherheit der Identifikation von Teilnehmenden digitaler Netzwerke in unterschiedlichen Anwendungsgebieten ist erhöht. Hierzu werden Grundlagentechnologien wie biometrische Verfahren und hardwarebasierte Identifikationsmerkmale (Physical Unclonable Functions) zusammen mit deren Widerstandsfähigkeit gegenüber Angriffen untersucht und dokumentiert, sowie robuste Absicherungsmethoden entwickelt. Automatisierte Medienfälschungen, insbesondere mittels Methoden der KI, und Angriffe auf biometrische Systeme, zum Beispiel durch die Fusion der biometrischen Merkmale mehrerer Personen (Morphing), wurden einerseits nachvollzogen, andererseits wurden Detektions- und Verteidigungsmaßnahmen grundlegend verbessert. Bewertungsverfahren für Authentisierungs- und Identifizierungsverfahren, die das erforderliche Vertrauensniveau berücksichtigen, werden entwickelt und mittelfristig in Form von Technischen Richtlinien veröffentlicht. Auf dieser Grundlage werden anschließend die Erkenntnisse in nationale und internationale Standardisierungsgremien eingebracht. Public Key Infrastrukturen (technische und organisatorische Infrastrukturen, kurz PKI), die es ermöglichen, kryptografische Schlüsselpaare auszurollen und zu verwalten, werden sicherer gemacht und eID-Interoperabilitätsinfrastrukturen umgesetzt und gepflegt.

Die Integritätssicherung, der Echtheitsnachweis und, bei Bedarf, die Langzeitsicherung von Dokumenten und Daten aus verschiedenen Anwendungsbereichen, wie intelligente Transportsysteme, Smart Metering, Industrie 4.0, elektronische Aufzeichnungssysteme, digitale Bildung, sind mittels verschiedener Technologien weiterentwickelt. Wo möglich und sinnvoll sollten bestehende Standards berücksichtigt werden.

Welche Wirkung erwarten wir?

Mit der Erhöhung der Sicherheit digitaler Netzwerke wird deren Betrieb robuster und das Vertrauen in sie gestärkt. Hierdurch erfolgen eine verstärkte Nutzung und damit insgesamt eine beschleunigte Digitalisierung.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

---

[26] Vergleiche strategisches Ziel 8.1.5 „Sichere elektronische Identitäten gewährleisten“.

- Bewertungsverfahren für Authentisierungs- und Identifizierungsverfahren, die das erforderliche Vertrauensniveau berücksichtigen, wurden entwickelt und einheitlich etabliert. Beispielsweise sind die Sicherheitsanforderungen an Identifizierung- und Authentisierungsmethoden für den Zugang zu digitalen Bildungsangeboten standardisiert.
- In der Biometrie wurden die Aspekte unterschiedlicher Angriffsmethoden detailliert untersucht und dokumentiert und deren Prävention und Detektion systematisch verbessert und praxistauglich umgesetzt. Entsprechende technische Richtlinien wurden veröffentlicht beziehungsweise fortentwickelt.
- Methoden zur zuverlässigen Identifikation drahtloser Geräte mithilfe von Physical Fingerprinting (individuelle Merkmale ihrer elektronischen Bauteile) wurden entwickelt und demonstriert.
- Die Sicherheit von PKI, die dem Ausrollen und Verwalten von kryptografischen Schlüsselpaaren dienen, wurde fortentwickelt, eID-Technologien und PKI wurden fortentwickelt und sichere eID-Interoperabilitätsinfrastrukturen wurden etabliert. Sie werden regelmäßig gepflegt. Ein PKI-Baukasten für Digitalisierungsprojekte wurde etabliert durch die Modularisierung von PKI-Vorgaben und einheitliche Vorgaben für Sicherheitselemente.
- Die Sicherheit von Integritätssicherungsverfahren und Langzeitsicherungstechnologien, basierend auf Technischen Richtlinien des BSI, ist wesentlich erhöht. Entsprechende Technische Richtlinien wurden dementsprechend weiterentwickelt.
- Ein sicherer Siegelserver, der die Überprüfbarkeit von Herkunft und Integrität elektronischer Dokumente sicherstellt, wurde umgesetzt, und digitale Siegel beziehungsweise signierte Barcodes zum Integritätsschutz und zum Echtheitsnachweis von Papierdokumenten und Daten wurden für neue Anwendungsgebiete fortentwickelt.

8.1.7 Voraussetzungen für sichere elektronische Kommunikation und sichere Web-Angebote schaffen

Warum ist das Ziel relevant?

Eine sichere und interoperable Kommunikation und sichere Webangebote sind Grundvoraussetzungen für eine erfolgreiche Digitalisierung in verschiedensten Anwendungsbereichen, wie zum Beispiel der Fahrzeug-zu-Fahrzeug- und der Fahrzeug-zu-Cloud-Kommunikation, der elektronischen Post, dem Gesundheitswesen und der Umsetzung des OZG.

Wo stehen wir?

Im Bereich der Umsetzung des OZG hat das BSI Vorgaben in Form Technischer Richtlinien an den Betrieb interoperabler Nutzerkonten (Bürgerkonten) als Identifizierungskomponenten für Online-Verwaltungsleistungen formuliert, mit Bund und Ländern abgestimmt und veröffentlicht. Eine Umsetzung der Anforderungen durch die Lösungen von Bund und Ländern steht noch aus. Parallel sind im Rahmen einer Pilotierung Vorgaben an Postfächer der interoperablen Nutzerkonten zu formulieren und umzusetzen.

Im Bereich der Telematikinfrastruktur 2.0 stimmt das BSI zurzeit mit der gematik GmbH die Konzeption für die Telematikinfrastruktur 2.0 ab. Geplante Finalisierung der Abstimmung ist Ende 2021.

Was wollen wir erreichen?

Ziel ist die (Fort-)Entwicklung anwendungsspezifischer kryptografischer Vorgaben für die sichere und interoperable Verwendung von Kommunikationsprotokollen und deren Einbringung als Stand der Technik in Gesetzesvorhaben. Anwendungsspezifische kryptografische Vorgaben, Prüfkriterien und Profile werden für weitere Anwendungsfälle erweitert, unter anderem für den Mobilitätsbereich, den Gesundheitsbereich, die Verwaltung und den Bereich Industrie 4.0.

Welche Wirkung erwarten wir?

Durch eine geeignete Umsetzung der Maßnahmen ist ein gesteigertes Vertrauen in die Digitalisierung in wichtigen Anwendungsgebieten und damit eine verstärkte Nutzung entsprechender Produkte zu erwarten.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Im Mobilitätsbereich ist die IT-Sicherheit der Kommunikation zwischen Fahrzeugen und der Cloud-Anbindung von Fahrzeugen erhöht.
- In der kontinuierlichen Fortentwicklung der Telematikinfrastruktur sind sowohl die Nutzung stationärer Anwendungen als auch neu eingeführte mobile Nutzungsmöglichkeiten von TI-Anwendungen für Versicherte und Leistungserbringer zu jedem Zeitpunkt sicher.
- Neben De-Mail steht der Verwaltung mit den Postfächern der Interoperablen Nutzerkonten ein weiterer sicherer Kommunikationsweg zur Verfügung. Dies wird durch eine mit Bund und Ländern abgestimmte Technische Richtlinie des BSI sichergestellt. Zur sicheren Umsetzung des OZG wurde eine Technische Richtlinie erstellt.

8.1.8 Verantwortungsvoller Umgang mit Schwachstellen – Coordinated Vulnerability Disclosure fördern

Warum ist das Ziel relevant?

Das zügige Schließen erkannter Sicherheitslücken in Systemen, Produkten und Dienstleistungen ist ein Eckpfeiler der Cybersicherheit. Wer eine Sicherheitslücke entdeckt, sollte sich unmittelbar und vertrauensvoll an den Hersteller des betroffenen Produktes beziehungsweise an den Anbieter der betroffenen Dienstleistung wenden, damit erkannte Sicherheitslücken in einem angemessenen Zeitraum mittels eines Patches oder Updates geschlossen werden. Dabei muss sorgsam abgewogen werden, ob eine öffentliche Kommunikation der Sicherheitslücken erfolgen sollte, bevor entsprechende Updates oder Patches verfügbar sind. Die Umsetzung dieser Anforderungen in einem abgestimmten Prozess nennt sich Coordinated Vulnerability Disclosure (CVD).

Wo stehen wir?

In der Praxis besteht bis heute kein allgemein gültiger Rahmen, der beschreibt, welche Akteure in welchem Umfang und mit welchen Methoden und Instrumenten Sicherheitslücken finden und den Herstellern melden dürfen. Die Frage des Umgangs wird deshalb von den Unternehmen selbst beantwortet. Dies führt dazu, dass einige Unternehmen unter anderem Bug-Bounty-Programme (Initiativen zur Identifizierung, Behebung und Bekanntmachung von Fehlern) unterhalten, um einen monetären Anreiz für ein koordiniertes Vorgehen (im Sinne des CVD) zu bieten, und andere Unternehmen gerichtlich gegen das Aufdecken vorgehen, weil sie ihre Rechte verletzt sehen. In der Folge besteht Unsicherheit, die dazu führt, dass gewisse Softwareprodukte nicht mehr untersucht werden oder aber Erkenntnisse zu kritischen Sicherheitslücken nicht zeitnah den Herstellern gemeldet werden.

Was wollen wir erreichen?

Zur Stärkung einer proaktiven Schwachstellen-Governance genießen innerhalb eines von der Bundesregierung entwickelten Rahmens Handelnde Rechtssicherheit, wenn sie mit ihren Erkenntnissen über Sicherheitslücken an betroffene Unternehmen herantreten. Sie haben zuverlässige Kontaktstellen, denen sie ihre Erkenntnisse melden können. Dies können eine verpflichtend einzurichtende Kontaktstelle im Unternehmen selbst oder das BSI als öffentliche und vermittelnde Stelle sein.

Der Gesetzgeber nimmt die betroffenen Unternehmen in die Pflicht, Kontaktstellen sowie Prozesse vorzuhalten, um gemeldete Schwachstellen in einem angemessen kurzen Zeitraum schließen zu können. Dabei wird geprüft, inwiefern Rechte und Pflichten auf beiden Seiten des CVD geregelt werden, beispielsweise eine Sperrfrist für Veröffentlichungen, eine verbindliche Frist für Patches oder Updates. Es existiert ein zwischen BSI und Herstellern oder Dienstleistern koordiniertes Vorgehen, das über den reinen Informationsaustausch hinausgeht. Dies betrifft auch Schwachstellen in den IT-Lieferketten von Produkten und Dienstleistungen (Supply Chain Security).

IT-Sicherheitslücken werden einerseits schnellstmöglich an betroffene Unternehmen gemeldet. Andererseits bestehen unternehmensinterne Prozesse, die eine zügige Prüfung und Schließung der gemeldeten Sicherheitslücke in Form eines Patches oder Updates ermöglichen.

Das BSI ist auf Basis seines CVD-Prozesses an dem Austausch beteiligt. Hierdurch unterstützt es das Melden von Sicherheitslücken als neutrale und fachlich kompetente Vermittlungsinstanz. Es warnt gegebenenfalls öffentlichkeitswirksam und bringt Erkenntnisse der Schwachstellenlandschaft in das nationale Cyberbedrohungslagebild

sowie in die allgemeine und branchenspezifische Gefährdungslage (insbesondere Kritische Infrastrukturen) ein. Anwenderinnen und Anwender werden schnellstmöglich vor Sicherheitslücken gewarnt und über mögliche Schutzmaßnahmen informiert.

Es wird sichergestellt, dass vertrauliche Detailinformationen über Sicherheitslücken nicht an Unbefugte gelangen, bevor entsprechende Patches oder Updates bereitstehen. Die speziellen Interessen der Sicherheitsbehörden werden in dem strategischen Ziel 8.3.10 „Den verantwortungsvollen Umgang mit Zero-Day-Schwachstellen und Exploits fördern“ adressiert.

Welche Wirkung erwarten wir?

Anwenderinnen und Anwender, Kritische Infrastrukturen und Institutionen von besonderem öffentlichen Interesse sind besser vor Cyberangriffen geschützt, da IT-Sicherheitslücken in Systemen, Produkten und Dienstleistungen zügig kommuniziert und behoben werden, geeignete Schutzmaßnahmen ergriffen werden und vertrauliche Detailinformationen über IT-Sicherheitslücken vor der Behebung des Problems nicht in die Hände maliziöser Cyberakteure gelangen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es besteht Rechtssicherheit für das Suchen und Finden von Sicherheitslücken.
- Die Bundesregierung regelt die Beteiligung des BSI an CVD-Ereignissen und veröffentlicht einen abgestimmten Prozess zur verantwortungsvollen Veröffentlichung von Schwachstellen (CVD-Prozess).
- Entdeckte Sicherheitslücken werden zunehmend gemeldet.
- Anreizstrukturen für Hersteller und Dienstleister, gemeldete Lücken in einem angemessenen Zeitraum zu schließen, wurden gestärkt.

8.1.9 Verschlüsselung als Voraussetzung eines souveränen und selbstbestimmten Handelns flächendeckend einsetzen

Warum ist das Ziel relevant?

Verschlüsselung stellt die Wahrung von Vertraulichkeit, Integrität und Authentizität digitaler Informationen sicher und ist deshalb ein wesentlicher Eckpfeiler der Cyber- und Informationssicherheit. Der Einsatz von Verschlüsselungsverfahren schützt die Nutzenden aus Staat, Wirtschaft und Gesellschaft effektiv vor Diebstahl, Spionage oder Sabotage persönlicher, geschäftlicher oder hoheitlicher digitaler Information und Kommunikation. Sie schaffen Vertrauen und erhöhen dadurch die Akzeptanz für die Nutzung neuer Technologien. Allerdings sind Verschlüsselungsverfahren einem sich ständig verändernden Bedrohungspotential ausgesetzt, was deren kontinuierliche Bewertung und Fortentwicklung zwingend erforderlich macht.

Mit zunehmenden Entwicklungen im Bereich Quantentechnologie verschärft sich diese Notwendigkeit, da viele heute eingesetzte Verschlüsselungsverfahren zukünftig nicht mehr sicher sein werden. Dieses Ziel fokussiert auf die Interessen der Gesellschaft und Wirtschaft. Die speziellen Interessen der Sicherheitsbehörden werden in dem strategischen Ziel 8.3.9 „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung gewährleisten“ adressiert.

Wo stehen wir?

Seit Veröffentlichung der letzten Cybersicherheitsstrategie im Jahr 2016 hat sich der Einsatz von Verschlüsselungsverfahren vor allem im Bereich der Unternehmen und Organisationen aus Sicht der Cyber- und Informationssicherheit positiv entwickelt. Unternehmen schützen ihre Organisationsnetzwerke mit VPN-Lösungen oder nehmen entsprechende verschlüsselte IT-Dienstleistungen in Anspruch.

Private Nutzende wiederum profitieren von den sicheren Angeboten der Ende-zu-Ende-verschlüsselten Messenger-Dienste, den mittlerweile weitgehend standardisiert eingesetzten TLS-Protokollen im World Wide Web oder dem zunehmenden Einsatz von Verschlüsselung bei Cloud-Dienstleistungen.

Dabei bleibt festzuhalten, dass ein Großteil der Nutzenden in Deutschland (außer in Messenger-Diensten) kaum Verschlüsselungslösungen (zum Beispiel VPN-Apps) nutzt und die Absicherung ihrer Informationen den kommerziellen Anbietern überlässt. Doch gerade im rasant wachsenden Markt des IoT sind verschlüsselte Produkte bislang in der Minderzahl. Diese Entwicklung ist bedenklich, da IoT-Produkte künftig in besonderem Maße in das tägliche Leben integriert werden, ohne die entstehenden Daten eigenständig abzusichern. Dieses Verhalten vergrößert die Angriffsfläche erheblich. Mittels Verschlüsselung könnte die Nutzung von IoT erheblich sicherer werden.

Was wollen wir erreichen?

Die Bundesregierung schafft Vertrauen und Verlässlichkeit in die Digitalisierung, indem sie auch weiterhin den flächendeckenden Einsatz sicherer Verschlüsselungstechnologien fördert und sich für den Abbau rechtlicher, wirtschaftlicher und technischer Hemmnisse beim Einsatz von Verschlüsselungslösungen einsetzt.

Dabei setzt sich die Bunderegierung international gegen die Einführung von Verboten des Einsatzes von Verschlüsselungstechnologien ein und sieht auch von eigenen Verboten ab.

Weiterhin fördert die Bundesregierung die Entwicklung neuer Verschlüsselungslösungen, insbesondere im Bereich der Post-Quanten-Kryptografie, indem sie die Kryptologie als wissenschaftliche Disziplin fördert, Marktanreize zur Produktentwicklung setzt, verstärkt Eigenentwicklungen und Entwicklungsbeteiligungen anstößt und am Markt verfügbare Produkte mittels Zulassung und Zertifizierung auf ihre Verlässlichkeit hin prüft.

Welche Wirkung erwarten wir?

Die konsequente Verschlüsselung digitaler Kommunikation und Speicherung erschwert den unerlaubten Zugriff und die Ausnutzung erheblich. Staat, Wirtschaft und Gesellschaft werden besser vor Cyberrisiken geschützt. Des Weiteren schaffen sichere Kommunikationsmöglichkeiten Vertrauen und Verlässlichkeit in einer digitalisierten Umgebung. Dies eröffnet Chancen für die Digitalisierung weiterer Lebensbereiche, für neue Geschäftsmodelle und weitere technische Innovationen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es wurden Initiativen zur Förderung von Verschlüsselung in Wissenschaft, Wirtschaft, Gesellschaft sowie in internationale Gremien, die diesen Zweck verfolgen, eingebracht.
- Es wurden weitere Initiativen nach dem Vorbild der Implementierung von Post-Quanten-Kryptografie in Open Source Produkten etabliert.
- Die Höhe der Fördermittel für Grundlagen- und Anwendungsforschung in der Kryptografie ist gestiegen.
- Die Anzahl geprüfter und zugelassener beziehungsweise zertifizierter Verschlüsselungslösungen ist gestiegen.
- Bürgerinnen und Bürger sowie Unternehmen verwenden mehr sicher verschlüsselte Kommunikationsmittel.

8.1.10 IT-Sicherheit durch KI und IT-Sicherheit für KI gewährleisten

KI-Strategie für Deutschland

KI birgt als Schlüsseltechnologie großes Potenzial für Wirtschaftswachstum und Produktivitätszuwächse. Um dieses Potenzial zum Wohle der Menschen und der Umwelt verantwortungsvoll, sicher und gemeinwohlorientiert zu fördern und zu nutzen, hat die Bundesregierung mit der „Strategie Künstliche Intelligenz“ (KI-Strategie) einen Handlungsrahmen entwickelt und weitreichende Maßnahmen beschlossen.

Mit der 2018 verabschiedeten und 2020 fortgeschriebenen Strategie hat die Bundesregierung ihr Engagement für die Zukunftstechnologie KI weiter gestärkt: Bis 2025 werden die Investitionen des Bundes für KI aus Mitteln des Konjunktur- beziehungsweise Zukunftspaketes von drei auf fünf Milliarden Euro erhöht.

Die Strategie ist abrufbar unter www.ki-strategie-deutschland.de/home.html.

Warum ist das Ziel relevant?

KI ist eine der zentralen Schlüsseltechnologien des 21. Jahrhunderts und Treiber für die fortschreitende Digitalisierung von Produkten, Dienstleistungen und Prozessen. Bereits heute beeinflusst KI sicherheitskritische Prozesse und Entscheidungen, zum Beispiel im Kontext von Biometrie, Gesundheitswesen oder Mobilität.

Für Cybersicherheit ergeben sich durch den zunehmenden Einsatz von KI neue Chancen, aber auch Risiken: Mithilfe von KI-Systemen können Sicherheitslücken identifiziert oder Angriffe zeitnah erkannt und abgewehrt werden. Bestehende Instrumente zur Verteidigung gegenüber Cyberangriffen können effizienter gestaltet und neue Instrumente entwickelt werden.

Gleichzeitig führt der verstärkte Einsatz KI-basierter Systeme für die Automatisierung von Prozessen und Entscheidungen zu neuen Sicherheitsbedrohungen, die von etablierten IT-Sicherheitsstandards bisher nicht abgedeckt werden.

Wo stehen wir?

KI-basierte Systeme werden zunehmend genutzt und kommen in verschiedensten Szenarien zum Einsatz. Bislang fehlen einheitliche Kriterien, Methoden und Werkzeuge zur Bewertung von KI-Systemen. Mit dem derzeit auf europäischer Ebene verhandelten Verordnungsentwurf AI Act[27] der Kommission werden jedoch Regulierungsanforderungen mit entsprechenden Prüfkriterien entwickelt, die dann auch in Deutschland umgesetzt werden müssen. Die Bundesregierung fördert verschiedene Maßnahmen in Forschung und Wirtschaft im Bereich KI. Sie bringt ihre Expertise in nationale und internationale Standardisierungsprozesse ein und gestaltet damit aktiv Normen und Standards.

Was wollen wir erreichen?

KI-Systeme erreichen ein von ihrem jeweiligen Einsatzzweck abhängiges, möglichst hohes IT-Sicherheitsniveau und werden gleichzeitig zur Gewährleistung eines hohen IT-Sicherheitsniveaus eingesetzt (IT-Sicherheit für KI und IT-Sicherheit durch KI). Die Einsatzmöglichkeiten von KI-Systemen zum Schutz von (staatlichen) IT-Systemen werden hierfür fortlaufend geprüft.

Der Regulierungsrahmen von IT-Sicherheitsanforderungen schließt die Sicherheit von KI-Systemen mit ein. Für KI-Systeme gibt es klar definierte IT-Sicherheitsanforderungen, welche die Besonderheiten der Systeme berücksichtigen. Die Sicherheitseigenschaften von KI-basierten Systemen können durch effektive und effiziente Prüfkriterien und -methoden evaluiert werden. Diese berücksichtigen insbesondere auch neuartige Angriffstechniken, die die spezifischen Eigenschaften von KI-Systemen ausnutzen. Dies gilt es insbesondere auch im europäischen AI Act zu berücksichtigen, damit dort hohe IT-Sicherheitsstandards gesetzt werden für KI-Anwendungen, deren Risiko als hoch bewertet wird.

IT-Sicherheit ist ein Grundbaustein, der bei der Entwicklung von KI-Systemen berücksichtigt wird (Security-by-Design). Diese erfüllen ein von ihrem jeweiligen Einsatzzweck abhängiges IT-Sicherheits-Niveau.

---

[27] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206

Neben dem Schutz KI-basierter Systeme (IT-Sicherheit für KI) werden KI-basierte Systeme auch für bessere Analyse- und Darstellungsformate sowie bessere Schutzmaßnahmen genutzt (IT-Sicherheit durch KI). Insbesondere werden diese bei der Erkennung von Angriffen auf Netzwerke oder durch die Sicherheitsbehörden im Rahmen der Strafverfolgung eingesetzt. Dabei ist zu beachten, dass es insbesondere in Bezug auf Hasskriminalität immer einer Beurteilung des Kontextes bedarf, die KI nicht leisten kann.

In einem gemeinsamen Prozess mit Partnern aus Forschung, Wirtschaft und Verwaltung entwickelt die Bundesregierung die technologischen Grundlagen zur Bewertung solcher Systeme und überführt sie in die Praxis. Dabei setzt sich die Bundesregierung für die Durchsetzung europäischer Werte in KI-Produkten und KI-Dienstleistungen weltweit ein.

Welche Wirkung erwarten wir?

Durch die Gewährleistung einer nachweisbaren Sicherheit von KI wird ein wichtiger Grundstein für die Akzeptanz und den Erfolg dieser für die Digitalisierung essenziellen Schlüsseltechnologie gelegt. Nur so können die Chancen der Technologie für Staat, Wirtschaft und Gesellschaft ausgeschöpft werden. Zudem wird so das Vertrauen der Benutzerinnen und Benutzer in KI-basierte Systeme aufgebaut und aufrechterhalten.

Gleichzeitig wird die Sicherheit von Staat, Wirtschaft und Gesellschaft durch den Einsatz von KI für IT-Sicherheitsanwendungen sowie durch die bessere Absicherung von KI-Systemen erhöht. Im Ergebnis werden auch die nationale und die europäische Wirtschaft gefördert und damit die Digitale Souveränität in einem globalen KI-Markt gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl und Qualität wissenschaftlicher Publikationen, die sich mit KI-spezifischen Angriffsvektoren und entsprechenden Gegenmaßnahmen und deren Einsatz in relevanten Anwendungsbereichen auseinandersetzen, ist signifikant gestiegen.
- Die Bundesregierung hat erfolgreich darauf hingewirkt, dass IT-Sicherheitsaspekte in der kommenden KI-Regulierung auf EU-Ebene sowie in der Umsetzung auf nationaler Ebene angemessen berücksichtigt werden.
- Es wurden Prüfkriterien, -werkzeuge und -methoden entwickelt, um Cybersicherheitsaspekte KI-basierter Systeme zu evaluieren. In relevanten, besonders kritischen Anwendungsbereichen wurden hierzu entsprechende Technische Richtlinien veröffentlicht, die als Grundlage für Standardisierungsvorhaben genutzt werden.
- KI-Systeme werden verstärkt und erfolgreich zur Angriffserkennung und -abwehr eingesetzt.

8.2 Handlungsfeld 2: Gemeinsamer Auftrag von Staat und Wirtschaft

Unternehmen in Deutschland sind regelmäßig Ziel von Cyberangriffen. Allein die von Ransomware-Angriffen verursachten Schäden, bei denen den Betroffenen der Zugang auf ihre Daten oder Systeme blockiert wird, sind erheblich. Zudem nimmt die Anzahl neuer Schadprogramm-Varianten zu und es werden immer wieder kritische Schwachstellen in weitverbreiteten Software-Produkten lokalisiert.

Insbesondere Kritische Infrastrukturen sind von zentraler Bedeutung für die Funktionsfähigkeit des Gemeinwesens. Durch ihren Ausfall oder ihre Beeinträchtigung entstehen Versorgungsengpässe, die eine Gefahr für die öffentliche Sicherheit darstellen. Mit dem BSI-Gesetz[28] ist ihr Schutz deshalb gesetzlich verankert.

In Deutschland ansässige Unternehmen müssen in der Lage sein, sich selbst und ihre Kundinnen und Kunden angemessen vor Cyberangriffen zu schützen. Hierzu gehören in der Regel das zeitnahe Einspielen von Updates sowie eine Sensibilisierung der Mitarbeiterinnen und Mitarbeiter. Je nach Anforderung an die Sicherheitsbelange des jeweiligen Unternehmens sollten auch regelmäßige Schulungen des Personals selbstverständlich sein sowie die Einführung und der Unterhalt eines Informationssicherheitsmanagementsystems (ISMS) nach nationalen oder internationalen Normen wie zum Beispiel der ISO 27001 oder dem BSI IT-Grundschutz. Ebenso stehen die Hersteller in der Pflicht, eigene Qualitätssicherungsmaßnahmen mit Blick auf die Gewährleistung hochqualitativer

[28] Abrufbar unter: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

Produkte auszubauen, in ihren Produkten gefundene Sicherheitslücken zeitnah zu schließen und damit zum Schutz der Nutzenden zu einem hohen Cybersicherheitsniveau in Deutschland beizutragen.

Zukunfts- und Schlüsseltechnologien wie IoT, KI, Blockchain, Big Data oder Quantentechnologie sorgen für Innovationssprünge und verändern die Rahmenbedingung für die Cybersicherheit in Deutschland. Sie eröffnen neue Potenziale, um bestehende Instrumente der Cybersicherheit zu verbessern. Gleichzeitig können hierdurch neue Cyberrisiken entstehen. Um Anwenderinnen und Anwender zu schützen, muss die Sicherheit der Schlüsseltechnologien deshalb bereits als zentraler Baustein im Entwicklungsprozess verankert und im Sinne eines Security-by-Design-Ansatzes gelebt werden.

Eine exzellente IT-Sicherheitsforschung sowie gut ausgebildete IT-Sicherheitsfachkräfte sind dabei wichtige, nachhaltige Grundpfeiler für die Wahrung der Cybersicherheit.

Die Bundesregierung wird Maßnahmen erarbeiten, um die bereits bestehende, vertrauensvolle und enge Zusammenarbeit von Staat und Wirtschaft fortzuführen. Das Fundament ist eine starke deutsche IT-Wirtschaft, die durch eine moderne Wirtschaftspolitik zu fördern ist.

Um die Cybersicherheit der Wirtschaft zu stärken, bedarf es folglich einerseits einer Kooperation von Staat und Wirtschaft; die Bundesregierung ist aber auch gehalten, die erforderlichen Rahmenbedingungen zu schaffen. An diesen beiden Ansätzen orientieren sich die folgenden Ziele.

8.2.1 Den NCSR in seiner Koordinierungsfunktion für die Cybersicherheitslandschaft stärken

Warum ist das Ziel relevant?

Die Digitalisierung hat alle Lebens- und Wirtschaftsbereiche erfasst. Die Gewährleistung eines hohen Maßes an Cybersicherheit nimmt daher eine gesamtgesellschaftliche Bedeutung ein. Um dieser Entwicklung Rechnung zu tragen, muss der NCSR in seiner strategischen Beratung der Bundesregierung die verschiedenen Perspektiven aus Wirtschaft und Gesellschaft bündeln und diese stärker formalisieren.

Wo stehen wir?

Der 2011 als Impulsgeber und strategischer Ratgeber etablierte NCSR ist das in der deutschen Cybersicherheitslandschaft höchstrangig besetzte Gremium. Er erhielt durch die Cybersicherheitsstrategie 2016 einen erweiterten Auftrag zur Identifizierung langfristiger Handlungsnotwendigkeiten und Trends sowie zur Erarbeitung von Handlungsempfehlungen. Zu diesem Zweck wurde 2017 ein Fachbeirat eingerichtet, dessen Empfehlungen in einem Abschlussbericht zusammengefasst wurden. Der Fachbeirat hat unter anderem die dauerhafte Begleitung der Arbeit des NCSR durch eine wissenschaftliche Arbeitsgruppe empfohlen, die in regelmäßigen Abständen Impulspapiere erarbeitet und diese auch der Öffentlichkeit zur Verfügung stellt.

Was wollen wir erreichen?

Der NCSR soll künftig seine Rolle als Impulsgeber für Fragen der Cybersicherheit noch stärker als bisher wahrnehmen. Hierfür ist seine Rolle als strategischer Berater der Bundesregierung ausgebaut und bedarfsorientiert formalisiert worden. Ebenso entwickelt er eine größere Strahlkraft in Wirtschaft, Wissenschaft und Gesellschaft hinein und begleitet dauerhaft die Umsetzung und Fortentwicklung der Cybersicherheitsstrategie.

Zu diesem Zweck ermitteln wir, wie die Zusammenarbeit und das bereits in der Cybersicherheitsstrategie 2016 eingeführte Berichtswesen an das Bundeskabinett verbindlicher gestaltet werden können. Darüber hinaus werden wir Möglichkeiten für eine stärkere Wirkung in die Öffentlichkeit hinein sowie eine vertiefte Einbindung von Wirtschaft, Wissenschaft und Zivilgesellschaft in die Arbeit des NCSR prüfen.

Welche Wirkung erwarten wir?

Wir erwarten vom NCSR eine umfassendere Perspektive auf Themen der Cybersicherheit. Der erweiterte Austausch soll ein tiefergehendes Verständnis für die Positionen der beteiligten Akteure untereinander ermöglichen. Die erweiterten Möglichkeiten des NCSR, mit wahrnehmbaren Impulsen in die Wirtschaft und Gesellschaft hineinzuwirken, sollen nicht zuletzt die Kohärenz der Aktivitäten in der Cybersicherheitslandschaft stärken.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand des folgenden Kriteriums überprüfen:

- Es wurde ein in der Bundesregierung und mit dem NCSR abgestimmtes Konzeptpapier erarbeitet. Dieses zeigt Maßnahmen auf, mit denen zum einen ein zielorientierterer Beratungsprozess der Bundesregierung durch den NCSR ermöglicht wird und zum anderen den Entscheidungsträgerinnen und Entscheidungsträgern in den jeweiligen zuständigen Gremien eine umfassendere Perspektive auf die Cybersicherheitslandschaft eröffnet wird.

8.2.2 Die Zusammenarbeit von Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft im Bereich der Cybersicherheit verbessern

Warum ist das Ziel relevant?

Eine nachhaltige Stärkung der Cybersicherheit in Deutschland kann nur in einem gemeinschaftlichen Schulterschluss von Staat, Wirtschaft sowie Zivilgesellschaft und Wissenschaft erreicht werden.

Die gesamtgesellschaftliche Zusammenarbeit muss weiter verbessert und durch neue Kooperationsmodelle gestärkt werden. So werden die Verbraucherinnen und Verbraucher, Wissenschaftlerinnen und Wissenschaftler sowie Entscheidungsträgerinnen und -träger der Wirtschaft und des Staates über Cybersicherheitsrisiken und -gefahren aufgeklärt und bei der Prävention unterstützt. Außerdem können staatliche Angebote und realisierbare Vorgaben zielgenau und praxistauglich entwickelt werden.

Wo stehen wir?

Wirtschaftsvertreterinnen und -vertreter werden bereits in vielen Bereichen und Prozessen integriert. Enge Kooperationen zwischen Staat und Wirtschaft existieren insbesondere im Bereich der Kritischen Infrastrukturen und für den Wirtschaftsschutz. Etablierte Foren sind unter anderem der UP KRITIS, die Allianz für Cybersicherheit, der „Dialog für Cybersicherheit“ des BSI oder die Initiative Wirtschaftsschutz[29].

Das BMWi unterstützt KMU bei der Digitalisierung und der IT-Sicherheit. Hier werden Anwenderinnen und Anwender durch gut verständliche, neutrale, praxisorientierte Informationen sowie durch konkrete Hilfe bei der Konzeption und Umsetzung unterstützt.

Im Nationalen Pakt Cybersicherheit wurde im April 2021 eine gesamtgesellschaftliche Erklärung zur Cybersicherheit zwischen Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft abgestimmt und veröffentlicht. In der finalisierten Erklärung wurden 13 Handlungsfelder benannt, an deren Umsetzung alle Gesellschaftsgruppen gemeinschaftlich arbeiten sollten[30].

Dieser Dialog lebt von einer lebendigen Zusammensetzung der Teilnehmenden, steht aber noch am Anfang und soll aufbauend auf den Erkenntnissen aus dem Nationalen Pakt Cybersicherheit gestärkt werden.

Was wollen wir erreichen?

Im Rahmen von Angeboten der zuständigen staatlichen Stellen werden Wirtschaft, Wissenschaft und Gesellschaft bei der Gestaltung von Cybersicherheit aktiv beteiligt. Der Austausch bietet Raum, um gemeinsam nachhaltige Handlungsoptionen und Lösungen im Bereich der Cybersicherheit zu entwickeln. Themen und Bedarfe der verschiedenen Gruppen werden frühzeitig erkannt und fließen in die Arbeit der staatlichen Akteure ein.

Provider und IT-Sicherheitsdienstleister setzen Anforderungen an IT-Sicherheitsprodukte und -systeme um und können durch ihren direkten Kontakt mit Anwenderinnen und Anwendern Herausforderungen und Trends frühzeitig erkennen. Staatliche Stellen beziehen sie deshalb frühzeitig in die Festlegung gesetzlicher Anforderungen für IT-Sicherheitsprodukte ein und suchen gemeinsam mit ihnen nach einer realisierbaren Umsetzungsmöglichkeit.

---

[29] Die Initiative Wirtschaftsschutz (www.wirtschaftsschutz.info) als durch das BMI koordinierte Initiative zur Umsetzung der Nationalen Strategie für Wirtschaftsschutz analysiert gemeinsam mit Experten von Sicherheitsbehörden (BfV, BKA, BND und BSI) sowie Spitzenwirtschafts- und Sicherheitsverbänden (BDI, DIHK, ASW Bundesverband und BDSW) die Risikolage und entwickelt Handlungskonzepte für einen ganzheitlichen Wirtschaftsschutz.

[30] Abrufbar unter: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/nationaler-pakt-cybersicherheit/gesamtgesellschaftliche-erklaerung/gesamtgesellschaftliche-erklaerung-artikel.html

Welche Wirkung erwarten wir?

Die Fortentwicklung eines gesamtgesellschaftlichen Dialogs im Bereich der IT-Sicherheit führt zu einer gesteigerten Akzeptanz staatlicher Institutionen. Dies erleichtert die Zusammenarbeit und hilft, die Präsenz von Cybersicherheitsthemen auf allen Ebenen der Anwendung von IT zu erhöhen.

Eine gestärkte Zusammenarbeit durch Kooperationsmodelle ermöglicht Multiplikatoreffekte bei der Wissensvermittlung. Auf Basis bestehender Kooperationsbeziehungen kann ein Austausch bereits zu Beginn von Entwicklungsvorhaben und im Rahmen der Definition von Prozessen erfolgen. Ergebnisse können hierdurch anwenderfreundlicher gestaltet sowie Zeitersparnisse und Synergien realisiert werden.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl der Mitgliedschaften in der Allianz für Cybersicherheit ist gestiegen.
- Der gesamtgesellschaftliche Dialog im Bereich der IT-Sicherheit beim BSI ist fortentwickelt, in dem gemeinschaftlich an den akuten Themen der IT-Sicherheit gearbeitet wird.
- Die Bundesregierung wird aktiv auf die Umsetzung der 13 Handlungsfelder aus der gesamtgesellschaftlichen Erklärung des Nationalen Pakts Cybersicherheit hinwirken, dazu Stakeholder gewinnen und die Umsetzung nachvollziehbar dokumentieren.
- Staatliche Unterstützungsangebote, unter anderem in Form verschiedener Kooperationsmodelle sowie über Social Media und Newsletter, sind erweitert und die Anzahl der Nutzerinnen und Nutzer der Angebote ist gestiegen.
- Der Anteil großer Schadprogrammwellen, die mittels technischer Sensoren entdeckt werden, ist gestiegen.
- Die Anzahl der Angebote der Initiative Wirtschaftsschutz für Unternehmen, Forschungseinrichtungen und Kommunen ist gestiegen.
- Das Mittelstand-Digital-Netzwerk des BMWi ist bekannt und seine Angebote zur IT-Sicherheit werden von der Wirtschaft und insbesondere von KMU genutzt.

8.3.3 Eine kooperative Kommunikationsplattform zu Cyberangriffen zwischen Staat, Wirtschaft, Wissenschaft und Gesellschaft aufbauen

Warum ist das Ziel relevant?

Die von Cyberangriffen betroffenen Organisationen in Staat, Wirtschaft, Wissenschaft und Gesellschaft benötigen für die Detektion dieser Angriffe nutzbare technische Informationen. Diese Informationen basieren auf Analysen der Cyberangriffe, die beispielsweise Bundesbehörden und IT-Sicherheitsdienstleister durchführen. Wenn die betroffenen Organisationen effektiv und effizient mit den technischen Informationen versorgt werden, kann dies zu einer signifikanten Verringerung oder gar Verhinderung von Schäden durch Cyberangriffe führen.

Wo stehen wir?

Cyberangriffe werden durch eine Vielzahl von Akteuren abgewehrt. In der Folge sind die notwendigen Informationen für eine effektive Abwehr von Cyberangriffen oftmals fragmentiert und stehen den betroffenen Organisationen nicht immer zeitnah und vollumfassend zur Verfügung. Die Zusammenarbeit mit Providern wurde zwar verstärkt (wie in der „Cybersicherheitsstrategie für Deutschland 2016“ genannt). Sie stellt aber nur einen Teil des notwendigen Informationsaustausches dar.

Was wollen wir erreichen?

Für den Erfolg ist es erforderlich, dass alle an der Cyberabwehr beteiligten Organisationen in ihrem jeweiligen Verantwortungsbereich so weit Informationen beitragen, wie Datenschutz und Geheimhaltungspflichten es ermöglichen. Die Detektionsleistung ist insbesondere auch in der Fläche der öffentlichen Kommunikationsnetze durch das Einbeziehen der Provider zu verbessern. Der Staat als neutraler Vermittler zwischen den Teilnehmenden schafft für den Informationsaustausch die notwendige Basis für eine kooperative Kommunikationsplattform

(Information Sharing Plattform). Durch den vertrauensvollen Austausch aller beteiligten Organisationen kann die Informationsbasis über Cyberangriffe zur Verbesserung der Cyberabwehr für alle beteiligten Organisationen erweitert werden.

Zu Cyberangriffen werden allgemeine Informationen und insbesondere technische Merkmale für die Detektion zwischen den betroffenen und auswertenden Organisationen (zum Beispiel BSI, Sicherheitsbehörden, IT-Sicherheitsdienstleistern und große Unternehmen) über die Kommunikationsplattform effizient ausgetauscht. Dies ermöglicht eine bessere Bedrohungsanalyse und zielgenaue Cyberabwehr. Die Informationen werden effizient, das heißt insbesondere auch soweit rechtlich und technisch möglich automatisiert, geteilt und erreichen eine hohe Reichweite. Die Informationen sind zudem an die Fähigkeiten der jeweiligen Nutzergruppe (zum Beispiel KMU) angepasst. Sensible Informationen werden im Rahmen des Informationsaustausches wirksam geschützt.

Welche Wirkung erwarten wir?

Durch freiwillige Teilnahme möglichst vieler von Cyberangriffen betroffener Organisationen am Informationsaustausch über die kooperative Kommunikationsplattform (Information Sharing Portal) ist die Detektion von Cyberangriffen erfolgreicher und lässt eine schnellere Abwehr und Attribuierung zu. Die bessere Vernetzung führt zu einer verstärkten Sensibilisierung insbesondere von Unternehmen und Wissenschaft. Der Schaden durch Cyberangriffe wird reduziert oder verhindert.

Für die Schaffung einer Informationsbasis zu Cyberangriffen erhalten unter Einhaltung von Datenschutz und Geheimhaltungspflichten insbesondere die IT-Sicherheitsdienstleister und für die Cyberabwehr sowie Cyberverteidigung zuständigen staatlichen Behörden die notwendigen Informationen zu Cyberangriffen aus den Detektionsergebnissen der betroffenen Organisationen und tauschen diese auch für bessere Analyseergebnisse aus. Dies ermöglicht fortlaufend die Analyse von Cyberangriffen zu verbessern und die Erstellung neuer, zielgenauerer technischer Merkmale zur Detektion. Dies wird zur Stärkung der Abwehr in Unternehmen und öffentlichen Netzen eingesetzt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die neue kooperative Plattform „Information Sharing Portal“ für den freiwilligen Austausch von Informationen zu Cyberangriffen ist etabliert.
- Sensitive Detailinformationen werden unter Einhaltung unter anderem der geltenden rechtlichen Regelungen und der bestehenden Übermittlungsvorschriften vertrauensvoll behandelt und so wirksam gegen Missbrauch geschützt.
- Anreize für die Teilnahme am Informationsaustausch und für das Teilen von Informationen wurden gestärkt.
- Die Anzahl der zwischen den betroffenen Organisationen ausgetauschten allgemeinen Informationen und technischen Merkmalen zu Cyberangriffen hat zugenommen und den Schutz vor Schäden durch Cyberangriffe verbessert.

8.2.4 Unternehmen in Deutschland schützen

Warum ist das Ziel relevant?

Die Gefahren, denen Unternehmen in Deutschland im Kontext von Cyberangriffen ausgesetzt sind, sind vielgestaltig und dynamisch. Insbesondere KMU sind den Herausforderungen aufgrund von Mängeln an Ressourcen und Wissen nicht ausreichend gewachsen. Sie benötigen daher besondere Förderung für einen ausreichenden Schutz vor Cyberangriffen. Sie stellen zahlenmäßig jedoch den größten Anteil an allen Unternehmen dar.

Wo stehen wir?

Es bestehen vielfältige Initiativen zum Austausch zwischen Staat und Wirtschaft zu Fragen der Cybersicherheit, wie beispielsweise die „Initiative IT-Sicherheit in der Wirtschaft“[31] des BMWi, die Allianz für Cybersicherheit oder das vom BMI und vom Bundesverband der Deutschen Industrie (BDI) ins Leben gerufene „Cyberbündnis mit der Wirtschaft“.

[31] Abrufbar unter: https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Home/home.html

Auch in der seit 2016 etablierten Initiative Wirtschaftsschutz werden die unternehmerischen Gefahren in der Cyberwelt kontinuierlich miteinbezogen. Darüber hinaus stehen auch die Nachrichtendienste, beispielsweise die Fallaufnahme des BfV oder der Cyber-Intelligence-Bereich des BND, und Polizeibehörden den Unternehmen als vertrauensvolle Ansprechpartner zur Verfügung. Dies wird ergänzt durch die zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes, die speziell für Unternehmen sowie öffentliche und nichtöffentliche Institutionen eingerichtet worden sind, um als kompetente Ansprechpartner IT-Sicherheitsvorfälle aus diesen Bereichen entgegenzunehmen und zeitnah Erstmaßnahmen mit anschließender Zuweisung an die zuständigen Ermittlungsstellen zu veranlassen.

Was wollen wir erreichen?

Die Zusammenarbeit zwischen Staat und Wirtschaft wurde weiter ausgebaut. Die Dialog- und Informationsaustauschplattformen zwischen Staat und Wirtschaft sind gestärkt, darunter fallen der UP KRITIS, die Allianz für Cybersicherheit, der Nationale Pakt Cybersicherheit, das Cyberbündnis mit der Wirtschaft sowie die Initiative Wirtschaftsschutz.

Die Interaktion der Unternehmen mit den zuständigen Stellen in den Teilbereichen Prävention, Detektion und Reaktion der Cybersicherheit ist gestärkt. Unternehmen tragen hierdurch mehr zur Detektion und Aufklärung von Cybersicherheitsbedrohungen bei. Cybersicherheit ist integraler Bestandteil eines ganzheitlichen Wirtschaftsschutzes.

Maßnahmen zum Schutz von Unternehmen (insbesondere KMU), Rüstungsindustrie und Unternehmen mit deutscher Schlüsseltechnologie werden in Abstimmung mit und im Zusammenwirken von Bund und Ländern durchgeführt. Dabei wird das funktionsfähige Netzwerk des Wirtschaftsschutzes im Verfassungsschutzverbund einbezogen. Die Maßnahmen der „Initiative IT-Sicherheit in der Wirtschaft“ samt der TISiM werden umgesetzt und Förderprogramme (zum Beispiel „go-digital“[32] und „Digital Jetzt“[33]) bedarfsorientiert fortentwickelt. Das Netzwerk der Mittelstand-Digital-Zentren ist insbesondere im Hinblick auf das Querschnittsthema IT-Sicherheit weiterentwickelt.

Das Informationsangebot zur Unterstützung von Unternehmen ist bedarfsgerecht ausgebaut. Die Unternehmen und insbesondere KMU sind für IT-Sicherheit sensibilisiert, sie besitzen ein erhöhtes Problembewusstsein für Cyberrisiken und verfügen über entsprechende Beurteilungs- sowie Lösungskompetenzen. IT-Sicherheitsmaßnahmen von Unternehmen, insbesondere KMU, werden unterstützt. Dazu sind die Unterstützungsangebote des BSI in Richtung Wirtschaft insbesondere im Rahmen der Allianz für Cybersicherheit ausgebaut.

Welche Wirkung erwarten wir?

Unternehmen (insbesondere KMU und Handwerk) werden bei der Umsetzung von IT-Sicherheitsmaßnahmen gezielter unter Berücksichtigung des jeweiligen Cyberrisikos unterstützt und haben das Wissen, um organisatorische, technische und personelle Maßnahmen effizient zu initiieren. Sie sind hierdurch in der Lage, sich effektiv vor Cyberangriffen zu schützen. Hierdurch wird die Wettbewerbsfähigkeit der deutschen Wirtschaft gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Angebote der Mittelstand-Digital-Zentren werden durch die Wirtschaft angenommen.
- Die TISiM ist insbesondere bei KMU und Handwerk bekannt und ihre Angebote werden nachgefragt.
- Förderprogramme, die auch auf Unterstützung der IT-Sicherheit von KMU, einschließlich Handwerk und freie Berufe, abzielen (insbesondere „go-digital“ und „Digital Jetzt“), sind bekannt und werden nachgefragt.
- Die Anzahl der Mitglieder und Angebote in der Allianz für Cybersicherheit ist gestiegen.
- Die Anzahl der Nutzenden der Unterstützungsangebote des BSI ist nachweislich gestiegen.
- Die Umsetzung empfohlener Cybersicherheitsvorkehrungen ist gestiegen.

---

[32] Abrufbar unter: https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/foerderprogramm-go-digital.html

[33] Abrufbar unter: https://www.bmwi.de/Redaktion/DE/Dossier/digital-jetzt.html

- Der prozentuale Anteil betroffener Unternehmen, die nach BSI-Warnungen reagiert und ihre Sicherheitslücken geschlossen haben, ist gestiegen.
- Die „Initiative Wirtschaftsschutz“ hat Projekte zum ganzheitlichen Schutz der Wertschöpfungskette vor Know-how- und Informationsabfluss etabliert.

8.2.5 Die deutsche digitale Wirtschaft stärken

Warum ist das Ziel relevant?

Die Wirtschaft kann einerseits auf einer Vielzahl von Innovationen und Erfolgen aufbauen, befindet sich aber gleichzeitig in einem herausfordernden internationalen Wettbewerb. Neben neuen Anwendungsfeldern, wie SmartHome und SmartCity, ist insbesondere auch die Digitalisierung klassischer Wirtschaftszweige relevant. Um die führende Rolle der deutschen Wirtschaft auch in der digitalisierten Zukunft zu sichern, in weiteren Wirtschaftszweigen zu ermöglichen und die Digitale Souveränität zu stärken, bedarf es gezielter Maßnahmen. Dabei sind auch die zugehörigen Lieferketten zu berücksichtigen.

Wo stehen wir?

Einerseits dominieren ausländische Firmen wichtige Digitalisierungsfelder, insbesondere jene, die datengetrieben sind. Andererseits zählen Deutschland und Europa in vielen Forschungsbereichen der Digitalisierung zur Weltspitze und sind für ihre hohen Standards bekannt. In diesem Spannungsfeld müssen die Firmen in die Lage versetzt werden, ihre Vorteile zu nutzen, um konkurrenzfähig zu bleiben oder konkurrenzfähig zu werden.

Was wollen wir erreichen?

Durch die gezielte Förderung von Schlüsseltechnologien[34], durch Beratung, Zuwendungen, gemeinsame Projekte und die Vernetzung mit relevanten Forscherinnen und Forschern soll die deutsche Digitalwirtschaft gezielt gestärkt werden. Eine weitere Stärkung soll sich aus der Kooperation mit Gremien zur gemeinsamen Entwicklung von Handlungsempfehlungen und Standards für wichtige Anwendungsbereiche (zum Beispiel in der Elektromobilität oder bei den Smart-Home-Produkten) ergeben.

Konkret sollen durch die Erhöhung der IT-Sicherheit ihrer Produkte beziehungsweise durch die Entwicklung von Produkten zur Erhöhung der IT-Sicherheit folgende Wirtschaftszweige und Lieferketten gezielt gestärkt werden: Mobilitäts- und Automobilindustrie, Energiewirtschaft, Smart Home beziehungsweise IoT und Smart Cities, Industrie 4.0, Gesundheitswesen, Finanzwesen und die IT-Sicherheits-Industrie mit den Feldern Biometrie, Langzeitsicherung und Quantentechnologie**.**

Die Smart-Metering-PKI, eine zentrale Infrastrukturkomponente für die Digitalisierung der Energiewende, wird erfolgreich und mit wachsender Nutzerzahl betrieben. Die BMWi-BSI-Roadmap zur Entwicklung technischer Eckpunkte für die Einsatzbereiche Smart Grid (Intelligentes Stromnetz), Smart Mobility (intelligente Mobilität) und Smart-beziehungsweise Sub Metering (intelligente Energieverbrauchsmessung, auch in Mehrparteienhäusern) wurde im Rahmen mehrerer Standardisierungsprojekte umgesetzt.

Welche Wirkung erwarten wir?

Durch eine geeignete Umsetzung sind einerseits Produkte mit erhöhter IT-Sicherheit und andererseits innovative Produkte, die die IT-Sicherheit erhöhen, zu erwarten. Konsequenz sind eine größere Wettbewerbsfähigkeit, eine größere Akzeptanz und eine größere Verbreitung dieser Produkte. Dank Innovationen durch Forschung und Vernetzung kann die deutsche Digitalwirtschaft eine internationale Vorreiterrolle einnehmen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Datenübertragung von und zu Mobilitätsdatenräumen sowie autonome Fahrfunktionen wurden abgesichert, die Resistenz gegen Angriffe auf die Sensorik von Fahrzeugen wurde gesteigert und entsprechende

[34] Vergleiche strategische Ziele 8.1.10 „IT-Sicherheit durch KI und IT-Sicherheit für KI gewärleisten“ und 8.2.9 „IT-Sicherheit durch Quantentechnologie gewährleisten.

Technische Richtlinien wurden veröffentlicht. Die (Typ-)Genehmigung und Marktbeobachtung von Kraftfahrzeugen und Kraftfahrzeugteilen zur Gewährleistung der Cybersicherheit wurde vom BSI in Zusammenarbeit mit dem Kraftfahrtbundesamt gestaltet.

- Die Smart-Metering-PKI, eine zentrale Infrastrukturkomponente für die Digitalisierung der Energiewende, wird erfolgreich und mit wachsender Nutzerzahl betrieben. Die BMWi-BSI-Roadmap zur Entwicklung technischer Eckpunkte für die Einsatzbereiche Smart Grid (Steuerbare Verbrauchs- und Erzeugungsanlagen), Smart Mobility (Integration der Ladesäuleninfrastruktur von Elektromobilen) und Smart beziehungsweise Sub Metering (Spartenübergreifende Verbrauchsmessung wie Strom, Gas, Wasser, Heizen beziehungsweise Wärme) wurde im Rahmen mehrerer Standardisierungsprojekte umgesetzt. Im Bereich Smart Home beziehungsweise Consumer-IoT wurden Standards, Normen, Technische Richtlinien und Prüfkriterien (zum Beispiel Prüfspezifikation Router-TR) unter anderem für die Anwendung in Verbindung mit nationalen und internationalen Labeling- und Zertifizierungsverfahren (zum Beispiel im Rahmen des Cybersecurity Act) in Zusammenarbeit mit erforderlichen Stakeholdern aus Staat, Wirtschaft und Gesellschaft entwickelt.
- Im Bereich Smart Cities wurden bestehende kommunale IoT-Infrastrukturen analysiert, Handlungsempfehlungen für deren sicheren Aufbau und Betrieb erstellt, Technische Richtlinien und Standards für Schlüsseltechnologien und Plattformen in Kooperation mit erforderlichen Stakeholdern aus Staat, Wirtschaft und Gesellschaft erarbeitet. Zudem wurden rechtliche Rahmenbedingungen für eine verbindliche Umsetzungsverpflichtung der Maßnahmen zur Verbesserung der IT-Sicherheit in kritischen Einsatzbereichen geschaffen.
- Im Bereich Industrie 4.0 wurde im internationalen Rahmen ein Konzept von Vertrauensinfrastrukturen für den Aufbau digitaler Wertschöpfungsnetze abgestimmt, es wurden Handlungsempfehlungen (Best Practices) für KMU zur Umsetzung wichtiger Komponenten von Vertrauensinfrastrukturen erstellt. Zudem wurden Dienstleistungsschnittstellen für eine sichere Digitalisierung und Industrie 4.0 geschaffen.
- Im Gesundheitswesen wurde ein Katalog von Sicherheitsanforderungen für Digitale Gesundheitsanwendungen im Rahmen des Zulassungsverfahrens etabliert, die Aktivitäten zur digitalen Pandemiebekämpfung wurden fortgeführt. Die Initiativen im Gesundheitswesen wurden auf den Bereich des Rettungswesens erweitert.
- Im Finanzwesen wurden die Sicherheitsanalysen von Online-Bezahlvorgängen kommuniziert und fortgeschrieben und die Sicherheitsanforderungen an Biometrie-Anwendungen für die Zwei-Faktor-Authentisierung etabliert.

8.2.6 Einen einheitlichen europäischen Regulierungsrahmen für Unternehmen schaffen

Warum ist das Ziel relevant?

Der Regulierungsrahmen für die Cybersicherheit von Produkten und Dienstleistungen ist national und international uneinheitlich. Er verteilt sich auf eine Vielzahl von Standards, Normen und Gesetzen. Teilweise sind verbindliche Vorgaben nicht oder nur unzureichend vorhanden. Die Zuordnung der jeweils relevanten Regulierungen ist zudem fehleranfällig und aufwendig.

Im Bereich der Überwachungstechnik führen die aktuellen EU-Regelungen gerade dazu, dass Hersteller ihren Sitz aus den EU-Mitgliedstaaten in Nicht-EU-Staaten verlegen, da der Import von dort in die EU deutlich einfacher ist als der Export aus der EU in Nicht-EU-Staaten. Dies führt etwa im Bereich der Telekommunikationsüberwachung (TKÜ), der Digitalen Forensik und der Big-Data-Analyse zu einem Technologieverlust und wirkt der angestrebten Digitalen Souveränität entgegen.

Wo stehen wir?

Das Ziel, nur solche Geräte in Verkehr zu bringen, die Schutz vor grundlegenden Cybersicherheitsrisiken versprechen, lässt sich nur auf EU-Ebene erreichen. Die Kommission beabsichtigt daher, an vernetzbare Geräte entsprechende Anforderungen als Voraussetzung für eine Bereitstellung auf dem Markt zu stellen. Dieser Schritt würde die Situation bereits kurz- bis mittelfristig erheblich verbessern, da kein neues Rechtsetzungsvorhaben initiiert werden muss. Die Wirkung setzt dementsprechend schneller ein. Dieses Vorhaben wird daher von Deutschland ausdrücklich unterstützt.

Was wollen wir erreichen?

EU-weit sind einheitliche gesetzliche Anforderungen inklusive Marktzugangsregelungen sowie Normen und Standards für Unternehmen im Bereich der Cybersicherheit definiert. Doppelregulierungen werden vermieden. Die Bundesregierung setzt sich abgestimmt in nationalen, europäischen und internationalen Standardisierungs- und Normungsgremien dafür ein, dass einheitliche Normen und Standards für Unternehmen in der EU entwickelt und eingeführt werden. Die NIS Richtlinie 2.0[35] der EU wird aktiv mitgestaltet und deutsche Belange werden in den Nachfolgelegislativakt eingebracht. Sektorspezifische Legislativvorschläge, wie zum Beispiel der DORA Verordnungsvorschlag für den Finanzsektor[36], werden aktiv begleitet.

Die internationale Zusammenarbeit, ebenso wie die Gremienarbeit im Bereich der Standardisierung ist gestärkt. Die internationale Wettbewerbsfähigkeit der nationalen und europäischen Standardisierungs- und Zertifizierungsstellen ist erhöht, die Verfahren bleiben international führend.

Auch mit Blick auf Digitale Souveränität engagiert sich Deutschland in den europäischen und internationalen Normungsgremien. Eine strategisch ausgerichtete Standardisierungspolitik ist gerade im Umfeld von Informations- und Kommunikationstechnik (IKT), Software und KI erforderlich. Dazu wird ein interministerieller Ausschuss Informations- und Kommunikationstechnologie-Standardisierung eingerichtet, mit dem Cybersicherheit gefördert und die Mitbestimmung in den europäischen und weltweiten Standardisierungsgremien gesichert wird. Die für die wesentlichen Technologiefelder relevanten Stakeholder (Bundesressorts, Wirtschaft, Forschung und Normierungsorganisationen) werden daran beteiligt.

Für den Einsatz beziehungsweise das Inverkehrbringen vernetzter Geräte innerhalb der EU werden die Verhandlungen auf EU-Ebene für einen horizontal wirkenden, einheitlichen Rechtsrahmen aufgenommen, der, wo es nötig ist, durch spezialgesetzliche, sektorale Regelungen ergänzt wird. Die Bundesregierung hat dies maßgeblich stimuliert und unterstützt den Prozess aktiv. So wird sichergestellt, dass ausreichend sichere Produkte innerhalb der EU in Umlauf gebracht und vernetzt werden.

Welche Wirkung erwarten wir?

Die Schaffung eines einheitlichen europäischen Regulierungsrahmens für Unternehmen führt unter anderem zu besserem Marktzugang, da Produkte und Dienstleistungen besser vergleichbar gemacht werden. Die Unternehmen profitieren von einheitlichen europaweiten Standards, die die Bürokratieaufwände reduzieren und ihre Wettbewerbsfähigkeit stärken.

Durch standardisierte Produktqualität und -sicherheit wird das Vertrauen der Verbraucherinnen und Verbraucher erhöht. Die Interoperabilität zwischen Produkten und Dienstleistungen kann durch Normungen verbessert werden. Auch dienen die Normungen als Türöffner und können den Export zum EU-Binnenmarkt oder weltweit fördern.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Doppelregulierungen für Unternehmen sind minimiert.
- Deutschland bringt sich aktiv bei der Erstellung eines EU-weit einheitlichen, horizontalen Rechtsrahmens für die Cybersicherheit und sektorale Cyberregulierungen ein.
- Ein interministerieller Ausschuss IKT-Standardisierung für die Cybersicherheit ist gegründet.
- Die Anzahl der beteiligten Stakeholder und Technologiefelder im interministeriellen Ausschuss IKT-Standardisierung für die Cybersicherheit ist gestiegen.

[35] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020PC0823

[36] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020PC0595

8.2.7 Forschung und Entwicklung resilienter, sicherer IT-Produkte, Dienstleistungen und Systeme für den EU-Binnenmarkt fördern

Warum ist das Ziel relevant?

Die IT-Sicherheitsforschung von heute führt zu den Innovationen von morgen. Sie ist notwendig, um die Resilienz von IT-Systemen und die Digitale Souveränität zu stärken. Während das Ziel 8.2.6 „Einen einheitlichen europäischen Regulierungsrahmen für Unternehmen schaffen“ auf die gezielte Zusammenarbeit von Staat und Experten der Wirtschaft abzielt, richtet sich dieses Ziel in der Wirkung an die breite Allgemeinheit.

Wo stehen wir?

Deutschland und Europa verfügen über eine solide wissenschaftliche Basis in der IT-Sicherheitsforschung. Mit dem Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015-2020“ wurden frühzeitig die Weichen gestellt. Mit dem Nachfolgeprogramm „Digital. Sicher. Souverän“ wird die IT-Sicherheitsforschung in Deutschland seit 2021 weiter konsequent und zielgerichtet vorangetrieben.

Mit dem Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE, dem CISPA Helmholtz-Zentrum für Informationssicherheit und dem Institut für Informationssicherheit und Verlässlichkeit KASTEL fördert das BMBF Forschungseinrichtungen an der Weltspitze der IT-Sicherheitsforschung. Exzellente IT-Sicherheitsforschung betreiben darüber hinaus das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC), das Fraunhofer-Institut für Sichere Informationstechnologie (SIT), das Max-Planck-Institut für Sicherheit und Privatsphäre, das Forschungsinstitut CODE an der Universität der Bundeswehr München sowie eine Vielzahl weiterer international sichtbarer Forschungsgruppen an Universitäten und anderen Einrichtungen.

Mit der Cyberagentur werden ressortübergreifend ambitionierte Forschungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit und diesbezüglicher Schlüsseltechnologien zur Bedarfsdeckung im Bereich der Inneren und Äußeren Sicherheit Deutschlands beauftragt und finanziert.

Neben der Wissenschaft und Großunternehmen sind KMU sowie Start-ups als Rückgrat des deutschen Mittelstands Treiber von Innovationen. Mit den sehr erfolgreichen Maßnahmen „StartUpSecure“[37] und „KMU-innovativ“[38] unterstützt das BMBF Forschung und Transfer in diesem wichtigen Wirtschaftszweig.

Aufgrund eines nur sehr kleinen Business Eco Systems, das heißt eines Verbundes von Unternehmen, die auf eine gemeinsame Wertschöpfung ausgerichtet sind, insbesondere für Hochsicherheitsprodukte, sind Investitionen von Sicherheitsunternehmen in Fort- und Neuentwicklungen oftmals gering. Die Bereitschaft nimmt mit höher abzudeckenden Verschlusssachen-Graden ab.

Was wollen wir erreichen?

Die IT-Sicherheitsforschung zu Zukunftstechnologien sowie zu Cyberbedrohungen liefert wichtige und relevante Erkenntnisse. Hierfür werden Universitäten, Hochschulen und Forschungseinrichtungen genauso wie Unternehmen und forschende öffentliche Einrichtungen gezielt gefördert, wird Nachwuchs für IT-Sicherheit begeistert und ausgebildet sowie die Bund-Länder übergreifende Zusammenarbeit in der Forschung gestärkt.

Grundlegende IT-Sicherheitstechnologien werden als offene Technologien zugänglich und dadurch transparent, nachvollziehbar und leichter einsetzbar gemacht.

Im Sinne eines „Netzwerke-schützen-Netzwerke“-Ansatzes wird die Vernetzung von wirtschaftlichen, wissenschaftlichen und zivilgesellschaftlichen Akteuren untereinander gefördert. Der Wissenstransfer in die Wirtschaft ist gesichert. Um Erkenntnisse aus der Forschung in marktfähige Produkte oder in die fachliche Anwendung zu überführen, werden Kooperationen zwischen Forschung, Wirtschaft und staatlichen Einrichtungen gefördert und Anreize für Ausgründungen geschaffen. Dadurch können Synergien genutzt und zusätzliche Forschungserkenntnisse generiert werden.

Die Entwicklung und Einführung zukunftsweisender Technologien (zum Beispiel der Mobilfunknetze der 5. und 6. Generation) ist von hoher strategischer Bedeutung für die Wahrung der Digitalen Souveränität in Deutschland

---

[37] Abrufbar unter: https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/startup-secure

[38] Abrufbar unter: https://www.bmbf.de/bmbf/de/forschung/innovativer-mittelstand/kmu-innovativ/kmu-innovativ_node.html

und der EU. Um das zu ermöglichen, werden entsprechende offene Basistechnologien, insbesondere offene und sichere Standards und Normen für Hard- und Software, und interoperable Schnittstellen aktiv von staatlicher Seite gefördert und mit geeigneten Regulierungsansätzen begleitet. Dadurch wird langfristig eine stärkere Technologiebasis für die Wertschöpfung etabliert.

Mit dem Forschungsprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän“ wird die IT-Sicherheitsforschung in Deutschland weiter konsequent vorangetrieben.

Welche Wirkung erwarten wir?

Die Risiken für Wirtschaft, Staat und Gesellschaft durch neue Bedrohungslagen und Technologien werden verringert und die Widerstandskraft gegenüber einer sich ständig wandelnden Bedrohungslage wird unterstützt.

Durch den Transfer von Forschungsergebnissen, zum Beispiel in Form von Handlungsempfehlungen und Technologien, und die Kommerzialisierung von IT-Sicherheitslösungen wird die IT-Sicherheit von Wirtschaft, Bürgerinnen und Bürgern sowie des Staates gestärkt. Die Realisierung von Cybersicherheit wird für alle Akteure einfacher und günstiger.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl an Projekten und Unternehmen in der Forschung sowie der Umfang der Förderung des Forschungsrahmenprogramms der Bundesregierung ist gestiegen.
- Standards und Normen für offene Basistechnologien wurden mit Förderung entwickelt und erfolgreich erprobt sowie gegebenenfalls von Standardisierungs-, Normungs- oder Zertifizierungsgremien anerkannt (zum Beispiel Open RAN).
- IT-Sicherheitsforschung in Deutschland ist international anerkannt.
- Innovationen aus der IT-Sicherheitsforschung werden vermehrt durch Unternehmen und Startups umgesetzt beziehungsweise kommerzialisiert.
- Handlungsempfehlungen aufgrund der Forschungsergebnisse liegen vor.

8.2.8 Sicherheit von Zukunfts- und Schlüsseltechnologien im Sinne eines Security-by-Design-Ansatzes stärken

Warum ist das Ziel relevant?

Zukunfts- und Schlüsseltechnologien wie KI, IoT oder Robotik sind Treiber für die fortschreitende Digitalisierung von Produkten, Dienstleistungen und Prozessen. Um sicherzustellen, dass die hieraus entstehenden Innovationsimpulse nicht durch IT-sicherheitstechnische Risiken abgebremst werden, müssen Sicherheitsanforderungen von vornherein im Entwicklungsprozess berücksichtigt werden. Durch Security-by-Design werden sie bereits zu Beginn des Entwicklungsprozesses systematisch ermittelt und berücksichtigt, um spätere Aufwände zur Behebung von Sicherheitslücken zu verhindern oder zu minimieren.

Wo stehen wir?

Die Bundesregierung fordert Security-by-Design-Ansätze schon seit mehreren Jahren in der Forschungsförderung, zuletzt verstärkt durch die Förderung vertrauenswürdiger Mikroelektronik und IT-Systeme. Gerade für sicherheitskritische Anwendungen wie das autonome Fahren oder Industrie 4.0 treiben Wissenschaft und Wirtschaft entsprechende Lösungen voran. Dennoch findet der Ansatz heute insbesondere im Anwenderbereich noch keine ausreichende Berücksichtigung bei der Entwicklung digitaler Hard- und Software-Produkte und -Dienste. Security ist vielfach noch eine nach- oder nebenrangige Eigenschaft von Produkten und Diensten und steht als Verkaufsargument meist nicht im Fokus. Produkte und Dienstleistungen werden durch die höheren Qualitätsanforderungen in Produktion und Betrieb für die Sicherheitsanforderungen teurer und dadurch in ihrer Wettbewerbsfähigkeit gegenüber unsicheren Produkten und Diensten benachteiligt. In der Folge ist die IT-Sicherheit vieler Produkte und Dienste durchschnittlich oder gar schlecht.

Was wollen wir erreichen?

Bei der Entwicklung von Produkten und Lösungen auf Basis von Schlüssel- und Zukunftstechnologien wird der Security-by-Design-Ansatz von vornherein berücksichtigt.

Security-by-Design ist als Ansatz bei Entwicklerinnen und Entwicklern von Hard- und Software bekannt. Bei Projekten mit staatlicher Förderung oder Beauftragung wird der Security-by-Design-Ansatz weiter verstärkt angewendet. Die Planung und Ausgestaltung einer ganzheitlichen Sicherheitsarchitektur werden konsequent umgesetzt.

Bei der Einführung neuer Technologien im Rahmen von Projekten mit staatlicher Förderung oder Beauftragung für den produktiven Einsatz wird durch die im jeweiligen Fall zuständige Stelle im geeigneten Umfang eine Risikoreduzierung durch Security-by-Design und eine Folgenabschätzung für die Cybersicherheit gefördert. Dadurch können mögliche Risiken in einem frühen Stadium der Entwicklung reduziert und erkannt werden. Die Bundesregierung fördert damit die Entwicklung und Produktion vertrauenswürdiger IT-Systeme.

Entlang der gesamten Wertschöpfungskette stehen wettbewerbsfähig die Informationen zur Herstellung und Nutzung vertrauenswürdiger IT zur Verfügung. Zudem ist der Austausch mit wirtschaftlichen Akteuren zu Forschung, Entwicklung, Produktion und Betrieb zu vertrauenswürdiger IT etabliert. Die sich beteiligenden wirtschaftlichen Akteure bilden ein Netzwerk und tauschen sich zu den Technologien, Entwicklungswerkzeugen und Geschäftsmodellen aus.

Eine Infrastruktur für das Qualitätsmanagement vertrauenswürdiger IT auf Basis sicherer Hard- und Software als Open Source komplettiert die wettbewerbsfähige Bereitstellung der notwendigen Informationen. Hierdurch wird die Wettbewerbsfähigkeit vertrauenswürdiger IT-Systeme gefördert.

Welche Wirkung erwarten wir?

Indem Sicherheitseigenschaften bereits als Designkriterium bei der Entwicklung von Hard- und Software Lösungen auf Basis von Zukunfts- und Schlüsseltechnologien verankert werden, werden Systemfehler von vornherein vermieden und mögliche Angriffsflächen klein gehalten. Hierdurch wird die Sicherheit in der Anwendung von Schlüsseltechnologien sichergestellt.

Durch die Steigerung der Wettbewerbsfähigkeit vertrauenswürdiger IT-Lösungen steigt auch ihr Marktanteil und damit das allgemeine Cybersicherheitsniveau.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Einhaltung von Security-by-Design wird zunehmend Bestandteil in Vergabeverfahren in staatlich geförderten oder beauftragten Projekten für den produktiven Einsatz.
- Es sind Anforderungen, Kriterien und Standards festgelegt, die IT-Systeme erfüllen müssen, um als vertrauenswürdig zu gelten (einschließlich vertrauenswürdiger Elektronik).
- Entlang der Wertschöpfungskette vertrauenswürdiger IT-Systeme ist eine Organisations-, Qualitätssicherungs- und Kommunikationsinfrastruktur gegründet. Im Rahmen des Netzwerkes zu vertrauenswürdiger IT, das die wirtschaftlichen Akteure gebildet haben, werden Projekte zu verschiedenen Technologiefeldern bearbeitet.
- Die Anzahl der Stakeholder, die sich an dem Netzwerk zu vertrauenswürdiger IT beteiligen, ist gestiegen.
- Vertrauenswürdige IT-Produkte werden im Markt erfolgreich angeboten.

8.2.9 IT-Sicherheit durch Quantentechnologie gewährleisten

„Quantentechnologien“ nutzen die besonderen physikalischen Effekte auf der Ebene einzelner oder weniger Teilchen aus. Quantencomputer nutzen das für eine neuartige Rechenarchitektur aus, die für manche komplexen Probleme eine sehr viel effizientere Lösung ermöglicht. Dies ist eine Hilfe bei Optimierungsproblemen, gefährdet aber auch einige aktuelle kryptografische Verfahren und damit die Cybersicherheit. Quantenschlüsselaustausch ermöglicht mit Quanteneffekten kryptografische Schlüssel theoretisch abhörsicher auszutauschen und trägt so zu sichererer Kommunikation bei.

Warum ist das Ziel relevant?

Die Entwicklung im Bereich der Quantentechnologie schreitet rapide voran, mit enormem Potenzial und auch neuen Herausforderungen für die Cybersicherheit.

Quantencomputer eröffnen die Chance, verschiedene Optimierungsprobleme effizienter zu lösen als herkömmliche Computer. Sie haben aber auch das Potenzial, grundlegende mathematische Annahmen zu brechen, auf denen kryptografische Algorithmen beruhen, die derzeit weit verbreitet im Einsatz sind und die die Grundlage unserer IT-Sicherheit bilden. Hier gilt es, kryptografische Verfahren zu entwickeln, die auch mit Quantencomputern nicht gebrochen werden können (sogenannte Post-Quantum-Verfahren), und Kryptoagilität zu fördern, das heißt die Fähigkeit, modular kryptografische Verfahren im Betrieb durch andere zu ersetzen.

Daneben verspricht etwa der Quantenschlüsselaustausch die Möglichkeit, kryptografische Schlüssel sicher zu verteilen und damit sichere Datenübertragung zu ermöglichen. Dazu braucht es neben der physikalischen Technologie auch die Einbindung in Standardisierung in praktisch nutzbare, sichere Systemarchitekturen. Ebenfalls von hoher Relevanz ist Digitale Souveränität im Bereich Quantentechnologien. Es sollte der Anspruch der Bundesregierung sein, Expertise im Bereich Quantentechnologien für die Kernaspekte Quantencomputing, Quantenkommunikation und Post-Quanten-Kryptografie zu haben. Entscheidend ist zudem, dass auch Produkte aus Deutschland oder der EU zur Verfügung stehen.

Wo stehen wir?

Im Jahr 2020 hat die Bundesregierung deshalb beschlossen, zusätzlich zwei Milliarden Euro in die Förderung der Quantentechnologie zu investieren und es wurde eine „Roadmap Quantencomputing“[39] erarbeitet.

Das BMBF fördert sowohl die Erforschung und Entwicklung grundlegender Technologien als auch deren Transfer in Anwendungen sowie mehrere Projekte zur Entwicklung neuer Quantenprozessoren; ein Wettbewerb zum Aufbau von Hubs, d. h. Verbünden von unterschiedlichen Akteuren, und zum Bau kompletter Quantencomputer-Systeme wird neue Forschungs- und Entwicklungs-Strukturen etablieren. Ebenso fördert das BMBF Projekte zur Erforschung der Post-Quanten-Kryptografie. Durch das BSI wurden erste Empfehlungen zu Algorithmen für die Post-Quanten-Kryptografie sowie für die Migration zu quantensicherer Kryptografie veröffentlicht.

Was wollen wir erreichen?

Quantentechnologische Systeme werden zur Gewährleistung eines hohen IT-Sicherheitsniveaus eingesetzt und ihr Einsatz wird gefördert.

Die Auswirkungen von Quantencomputing auf die Cybersicherheit werden erforscht und technologische Innovationen für mehr Cybersicherheit genutzt. Dazu gehört beispielsweise die Erforschung des Einsatzes von Quantentechnologie (Quantencomputer und Sensoren) in der Seitenkanalanalyse.

Wichtige Voraussetzung für den Einsatz von Quantum Key Distribution (QKD) in hochsicheren Netzen ist die zertifizierbare Sicherheit von Produkten. Hierzu entwickelt die Bundesregierung ein Protection Profile gemäß Common Criteria, begleitet die Erstellung zusätzlich benötigter technischer Angaben durch Studien und erforscht quantitative und qualitative Aspekte der vorliegenden Sicherheitsbeweise.

Der mögliche Sicherheitsgewinn durch QKD wird nicht nur in Forschungsprototypen, sondern auch im realen Einsatz demonstriert, um die Praxistauglichkeit zu demonstrieren.

---

[39] Abrufbar unter: https://www.bundesregierung.de/breg-de/aktuelles/quantencomputing-1836542

Der Austausch von durch Quantencomputer gefährdeten Algorithmen durch neue, standardisierte Algorithmen wurde vorbereitet.

Welche Wirkung erwarten wir?

Durch die Nutzung der Potenziale und die Minimierung der Risiken, die durch quantentechnologische Systeme entstehen, wird ein nachhaltig hohes IT-Sicherheitsniveau zum Schutz von Staat, Wirtschaft und Gesellschaft gewährleistet. Zudem wird die technologische Souveränität Deutschlands in der Quantenkommunikation gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Im Bereich des Quantencomputing stehen bis 2025 Rechner mit mindestens 100 Qubits auf der Basis souveräner Technologie aus Deutschland und Europa bereit und stehen für Anwendungsuntersuchungen aus dem Sicherheitsbereich zur Verfügung.
- Im Hochsicherheitsbereich hat der Wechsel zu quantensicherer Kryptografie begonnen.
- In Staat, Wirtschaft und Gesellschaft ist die Dringlichkeit des Wechsels zu quantensichererer Kryptografie akzeptiert und in kritischen Bereichen eingeleitet. Pilot-Infrastrukturen binden Partner aus den verschiedenen Bereichen ein.
- Technologien und Lösungen der Quantenkommunikation von Anbietern aus Deutschland und Europa stehen für Staat, Wirtschaft und Gesellschaft zur Verfügung.
- Die Studie zur Realisierbarkeit von Quantencomputern wird fortgeführt und aktualisiert.

8.2.10 Prüf- und Abnahmeverfahren mit Innovationszyklen harmonisieren (Time-to-Market)

Warum ist das Ziel relevant?

Neue IT-Produkte und Dienstleistungen werden, unter anderem in den Bereichen Smart Home, Automotive, Medizintechnik und Energie in kurzen Innovationszyklen zur Markteinführung gebracht und ermöglichen insbesondere im Bereich von IoT-Anwendungen die zunehmende Vernetzung aller Lebensbereiche. Vor allem bei neu angebotenen Soft- und Hardwareprodukten ist es nicht ausgeschlossen, dass noch nicht alle sicherheitsrelevanten Aspekte betrachtet werden oder erkennbar sind. Kriminelle versuchen, potenzielle Schwachstellen auszunutzen, um in Systeme einzudringen oder sie für strafrechtlich relevante Zwecke zu missbrauchen. Abgesehen von einer konsequenten Strafverfolgung sollte der Staat den Unternehmen Unterstützung bieten, die Produkte von Anfang an sicherer und weniger anfällig zu gestalten.

Wo stehen wir?

Staatliche Stellen müssen in der Lage sein, Aufbau und Funktionen neuer IT-Produkte und Dienstleistungen zu verstehen und mit entsprechenden Anforderungen an diese Technologien ein Mindestmaß an Sicherheit bei deren Nutzung zu gewährleisten. Hierbei gilt es, maßvoll zu agieren, damit Innovationspotenziale genutzt werden und neue Prüfverfahren eine hohe Akzeptanz bei den Herstellern erzielen können.

Was wollen wir erreichen?

Staatliche Stellen müssen in der Lage sein, als kompetente und vertrauenswürdige Dienstleister verlässliche Sicherheitsaussagen zu neuen Technologien zu treffen und darauf aufbauend regulatorische Vorgaben zu machen, Informationen bereitzustellen und Empfehlungen zu geben.

Neue Prüf- und Abnahmeverfahren, die den beschleunigten Innovationszyklen der IT-Wirtschaft Rechnung tragen (Time-to-Market), sind implementiert. Die Qualität der Verfahren hat hierdurch keine Einbußen erfahren. Die Akzeptanz für die Berücksichtigung von Sicherheitseigenschaften steigt.

Um neben der sachgerechten Produkt- und Dienstleistungszertifizierung auch die Akzeptanz für Informationssicherheit in der Digitalisierung zu stärken, wird die Entwicklung neuer Zertifizierungsverfahren vorangetrieben. Produkte und Dienstleistungen werden sachgerecht zertifiziert. Dabei wird ein zwischen Mindeststandards und

Ressourceneinsatz ausgewogener Ansatz verfolgt. IT-Sicherheit besitzt hierdurch eine hohe Akzeptanz als Bestandteil digitaler Produkte und Dienstleistungen.

Damit dies neben dem staatlich-behördlichen Angebot gelingt, liegen geeignete Akkreditierungen für Prüf- und Konformitätsbewertungsstellen vor. Diese ergeben sich gegebenenfalls aus bestehenden Cybersecurity Act-Schemata, aber auch aus Akkreditierungsregeln der Deutschen Akkreditierungsstelle GmbH (DAkkS).

Welche Wirkung erwarten wir?

Mit der Implementierung neuer Prüf- und Abnahmeverfahren wird die Akzeptanz für die Berücksichtigung von Sicherheitseigenschaften erhöht.

Anwenderinnen und Anwender werden durch die sachgerechte Zertifizierung von Produkten und Dienstleistungen besser vor Cyberangriffen geschützt. Gleichzeitig wird die Innovationskraft der deutschen und europäischen Wirtschaft sichergestellt und nachhaltig gestärkt. IT-Sicherheit wird dabei als Qualitätsmerkmal der Produkte deutscher und europäischer Anbieter verankert. Die Angebotsbreite an qualitativen Prüf- und Abnahmeverfahren nimmt zu.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Für neuartige Anwendungsfelder stehen Technische Richtlinien zur Verfügung, deren Inhalte zeitnah in Standardisierungsgremien eingebracht werden.
- Neue Prüf-, Abnahme- und Zertifizierungsverfahren (beschleunigte Sicherheitszertifizierung, IT-Sicherheitskennzeichen, 5G, Medizinprodukte, (teil-) autonome Fahrzeuge, Energie, Marktaufsicht) sind etabliert.
- Neue Märkte sind zertifizierungstechnisch erschlossen.
- Die Anzahl erteilter Zertifikate ist gestiegen.
- Standards, Technische Richtlinien und Prüfspezifikationen im Bereich Smart Home beziehungsweise Consumer-IoT wurden geschaffen.

8.2.11 Schutz Kritischer Infrastrukturen weiter verbessern

Die Nationale Strategie zum Schutz Kritischer Infrastrukturen

Der Schutz Kritischer Infrastrukturen richtet sein Augenmerk auf jene Systeme, Einrichtungen und Anlagen, von deren Funktionieren die Bereitstellung gesellschaftswichtiger Dienstleistungen in besonderem Maße abhängt. Im Juni 2009 verabschiedete das Bundeskabinett die „Nationale Strategie zum Schutz Kritischer Infrastrukturen“ – kurz: KRITIS-Strategie – um den bereits laufenden Aktivitäten einen gemeinsamen Rahmen zu geben und die strategischen Weichen für eine ressortübergreifend abgestimmte Aufgabenwahrnehmung zu stellen. Zu den Kernelementen der Strategie gehört auch der All-Gefahren-Ansatz, der sowohl die Cybersicherheit als auch den sogenannten „physischen Schutz“ als Teilaspekte eines ganzheitlichen Schutzes Kritischer Infrastrukturen ausweist.

Die Strategie ist abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html.

Warum ist das Ziel relevant?

Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen. Sie zu sichern und so ihren Ausfall oder ihre Beeinträchtigung zu verhindern, ist damit bereits der Begriffsbestimmung nach ein relevantes Ziel und für das Funktionieren des Gemeinwesens und für den Schutz der Grundrechte Einzelner von hoher Bedeutung.

Wo stehen wir?

Mit dem BSI-Gesetz und der Verordnung zur Bestimmung Kritischer Infrastrukturen[40] liegt bereits seit mehreren Jahren ein Rechtsrahmen für die Cybersicherheit in Kritischen Infrastrukturen vor, der kontinuierlich weiterentwickelt wird. Gemäß den gesetzlichen Vorgaben haben die Betreiber Kritischer Infrastrukturen dem BSI regelmäßig Nachweise über technische und organisatorische Maßnahmen zur IT-Sicherheit vorzulegen. Im Gegenzug werden die Unternehmen in einen vertrauensvollen Informationsaustausch mit dem Bundesamt einbezogen. Auf Ebene von Bund und Ländern bestehen mit den Koordinierungsstellen (KOST) KRITIS der Länder und der AG KOST KRITIS zwischen Bund und Ländern wichtige Strukturen für eine koordinierende und vernetzende Behandlung von KRITIS-Belangen einschließlich der Cybersicherheit im Sinne eines All-Gefahren-Ansatzes.

Was wollen wir erreichen?

Staat und Wirtschaft arbeiten eng zusammen, um Kritische Infrastrukturen zu schützen und schnell auf Cybersicherheitsvorfälle reagieren zu können. Bedrohungen durch Cybersabotage werden frühzeitig erkannt. Relevante Informationen über Cybersicherheitsvorfälle sind für die zu schützenden Unternehmen und die zuständigen Behörden unverzüglich verfügbar.

Durch Prüfung der eingereichten Nachweise sowie der gegebenenfalls notwendigen Nachbesserungen ist ein Rückschluss auf die Verbesserung des Cybersicherheitsniveaus in den betroffenen Unternehmen möglich. Es ist wesentlich, dass reaktive Maßnahmen durch proaktive Maßnahmen ergänzt werden, beispielsweise durch das Vorhalten eines umfassenden Cyberbedrohungslagebildes mitsamt der Möglichkeit, etwaige Cyberangriffe (oder Vorbereitungen dazu) auf KRITIS frühzeitig im Vorfeld zu erkennen und abzuwehren.

Zum Schutz Kritischer Infrastrukturen vor IT-Störungen oder Cyberangriffen sind bestehende Anforderungen weiter ausgestaltet und die Umsetzung bei den KRITIS-Betreibern wird verstärkt unterstützt. Die Unterstützung von Betreibern Kritischer Infrastrukturen durch Behörden bei Cyber- und IT-Vorfällen wird priorisiert. Bestehende Mindestanforderungen an KRITIS-Betreiber im Hinblick auf die Absicherung von IT-Systemen orientieren sich dabei am Stand der Technik. Sie werden aufgrund der sich verändernden Bedrohungslage stetig überprüft und bei Bedarf angepasst. Dies kann auf Basis vorliegender Nachweise beurteilt und durch Vor-Ort-Prüfungen zusätzlich abgesichert werden.

KRITIS-Betreiber sind auf freiwilliger Basis an einen nationalen Informationsaustausch angeschlossen. Hierdurch ist die nationale Früherkennungsfähigkeit für maliziöse Aktivitäten von Cyberakteuren verbessert. KRITIS-Betreiber können aufgrund früher Hinweise schneller auf etwaige gegen sie gerichtete Cyberbedrohungen reagieren. Die bestehenden Warnangebote des BSI für Betreiber Kritischer Infrastrukturen sind auch für weitere Unternehmen und Einrichtungen in KRITIS-Sektoren mit Versorgungsauftrag geöffnet.

Welche Wirkung erwarten wir?

Die sichere Bereitstellung der Dienstleistungen Kritischer Infrastrukturen, zu denen unter anderem die Versorgung mit Strom, Wasser, Lebensmitteln und Kommunikation oder das Gesundheitswesen sowie viele weitere zählen, ist Grundvoraussetzung für die Versorgung der Bevölkerung sowie das Funktionieren von Staat, Wirtschaft und Gesellschaft. Eine erfolgreiche Absicherung der IT-Komponenten in Kritischen Infrastrukturen beugt Risiken vor und stabilisiert so die gesellschaftliche und wirtschaftliche Entwicklung.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Der Rahmen zur Durchführung von Vor-Ort-Prüfungen ist erweitert. Entsprechende Änderungen sind bis 2026 durchgeführt oder in Arbeit.
- Die Bundesregierung hat den Stand der Technik für weitere KRITIS-Branchen konkretisiert, soweit dieser nicht bereits auf der Grundlage bestehender EU-weiter oder internationaler Normungssysteme definiert ist.

[40] Abrufbar unter: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

- Die KRITIS-Betreiber können über einen nationalen Informationsaustausch zu Cyberangriffen ihre jeweilige Abwehr stärken.

8.2.12 Cybersicherheitszertifizierung

Warum ist das Ziel relevant?

Zertifizierung und Konformitätsbewertung der Sicherheitsaspekte von Produkten, Dienstleistungen und Prozessen schaffen Vertrauen und Vergleichbarkeit und fördern die Bestrebungen zu einem höheren Cybersicherheitsniveau.

Wo stehen wir?

Deutsche Zertifizierungen im Kontext der IT-Sicherheit sind weltweit anerkannt.

Durch den Cybersecurity Act[41] werden neue Zertifizierungsschemata entwickelt und eingeführt. Das BSI hat sich als zuverlässiger und vertrauenswürdiger Partner für den Nachweis hoher Anforderungen an die Cyber- und Informationssicherheit etabliert, befindet sich aber im internationalen Umfeld in zunehmendem Wettbewerb mit anderen nationalen Stellen.

Cybersecurity Act

Unter der Verordnung (EU) 2019/881 trat der Cybersecurity Act im Juni 2019 in Kraft. Dieser beinhaltet neben der Stärkung der Agentur der Europäischen Union für Cybersicherheit (ENISA) und deren Aufgabenweiterentwicklung auch die Einführung eines EU-weiten Zertifizierungsrahmens für die Cybersicherheit. Dies dient dem Ziel, den Bereich der Cybersicherheit und die damit verbundene Zertifizierung europäisch harmonisiert zu regeln und eine Fragmentierung des Binnenmarktes zu vermeiden. Unter Berücksichtigung der verschiedenen Vertrauenswürdigkeitsstufen niedrig (basic), mittel (substantial) und hoch (high) werden sukzessive spezielle Zertifizierungsschemata erarbeitet und implementiert. Diese gelten EU-weit, werden gleichermaßen von allen Mitgliedstaaten anerkannt und ersetzen existierende nationale beziehungsweise multilaterale Schemata mit gleichem Zertifizierungsinhalt. Beispielhaft ist hierbei die Überführung des SOGIS-MRA zu nennen, welches die sogenannten Common Criteria in ein europäisch harmonisiertes Schema überführt. Die Anwendung der Schemata des CSA ist grundsätzlich freiwillig angelegt. Jedoch besteht die Möglichkeit, entsprechende Zertifizierungserfordernisse oder EU-Konformitätserklärungen spezialgesetzlich vorzugeben.

Was wollen wir erreichen?

Die Umsetzung des im Cybersecurity Act verankerten Cybersicherheitszertifizierungsrahmens wird aktiv begleitet und die Erarbeitung von Zertifizierungsschemata vorangetrieben. Die internationale Wettbewerbsfähigkeit der nationalen Standardisierungs- und Zertifizierungsstellen ist erhöht, um auch weiterhin international führend zu bleiben. Das BSI wird sich für die Erfordernisse, die sich aus dem Cybersecurity Act und aus nationalen Zertifizierungsvorhaben ergeben, entsprechend aufstellen, so dass adäquate Zertifizierungsangebote bereitstehen. Wir wollen die Zertifizierungslandschaft modernisieren und mit Blick auf Time-to-Market-Aspekte interessante Zertifizierungsmöglichkeiten bieten. In der Funktion als Nationale Behörde für die Cybersicherheitszertifizierung wird das BSI aktiv an der Entwicklung und Gestaltung von Zertifizierungsschemata gemäß dem Cybersecurity Act mitwirken.

Welche Wirkung erwarten wir?

Das BSI baut seinen hervorragenden Ruf als Zertifizierungsstelle weiter aus und ist als Nationale Behörde für Cybersicherheitszertifizierung etabliert. Die verfügbaren Zertifizierungsangebote des BSI, aber auch von privaten Anbietern werden aktiv genutzt, um im Sinne der Vertrauensbildung für ein hohes Cybersicherheitsniveau in Europa beizutragen. Unternehmen und andere potenzielle Antragsteller von Zertifizierungen machen verstärkt Gebrauch von Zertifizierungsmöglichkeiten, auch ohne gesetzlich vorgeschriebenes Erfordernis.

[41] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019R0881

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das BSI bleibt die nationale Zertifizierungsbehörde mit den meisten behördlich erteilten IT-Sicherheitszertifikaten weltweit.
- Die angekündigten Zertifizierungsschemata im Rahmen des CSA sind erlassen und besitzen Gültigkeit: Common Criteria (EUCC), Cloud Services (EUCS), IoT und 5G.
- Die beschleunigte Sicherheitszertifizierung wurde international harmonisiert und im Rahmen des CSA als Zertifizierungsschema eingeführt.
- Die Anzahl zertifizierter Produkte unter der Aufsicht der Nationalen Behörde für die Cybersicherheitszertifizierung ist gestiegen. Die Anzahl von Unternehmen und Organisationen, die IT-Grundschutz anwenden, ist gestiegen.

8.2.13 Telekommunikationsinfrastrukturen der Zukunft sichern

Warum ist das Ziel relevant?

Die Mobilfunknetze der aktuellen, fünften Generation (5G) und der kommenden, sechsten Generation (6G) zeichnen sich durch virtualisierte Netzkomponenten aus. Zentrale Funktionen des Netzes werden allein durch Software realisiert. Teilweise kann diese auf allgemein verfügbarer Hardware betrieben werden. Mit der Virtualisierung geschaffene Angriffsflächen gilt es so klein wie möglich zu halten und verbleibende Risiken zu beherrschen.

Die europäischen Hersteller von Netztechnik befinden sich in einem intensiven Wettbewerb. Viele Anbieter von Mobilfunktechnologie sind heute verstärkt in Asien und den USA beheimatet, mit einer starken Tendenz zu oligopolistischen Marktstrukturen. Damit Deutschland und Europa nicht durch weiteren Verlust von Know-how und Abwanderung von Produktionskapazitäten in einseitige Abhängigkeiten geraten, ist es erforderlich, etablierte Anbieter in Deutschland und Europa zu stärken oder aufzubauen. Durch den Einsatz offener Basistechnologien wie Open RAN, eine herstellerunabhängige Mobilfunkarchitektur, können Abhängigkeiten von wenigen dominanten Netzausrüstern reduziert, der Markteintritt neuer, auch kleinerer europäischer Anbieter erleichtert, mehr Innovationen und aufgrund höherer Transparenz und Kontrolle mehr Sicherheit im Netz ermöglicht werden. Open RAN dient daher auch direkt der Stärkung der Digitalen Souveränität und der Cybersicherheit in Telekommunikationsnetzen[42].

Wo stehen wir?

Mobilfunknetze sind bereits heute Kritische Infrastrukturen im Sinne der BSI-Kritisverordnung. Zudem existiert ein Katalog mit Sicherheitsanforderungen für Telekommunikationsnetze. Im Rahmen eines technologie- und herstellerneutralen Ansatzes will die Bundesregierung die Anforderungen an die Sicherheit der Kommunikationsnetze deutlich erhöhen, ohne vorab konkrete Hersteller von Netzwerkkomponenten vom 5G-Netzausbau auszuschließen. Eine diesbezügliche Regelung wurde im Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) hinsichtlich sogenannter kritischer Komponenten (Produkte, die in bestimmten Kritischen Infrastrukturen eingesetzt werden) vorgenommen.

Forschung und Entwicklung im Telekommunikationsbereich haben in Deutschland gute Voraussetzungen und einen guten Ruf. Verbesserungsfähig ist die Überführung der wissenschaftlichen Leistungen in marktfähige Produkte deutscher Unternehmen.

Was wollen wir erreichen?

Die Sicherheit und Beherrschbarkeit der Telekommunikationsnetze – insbesondere der 5G-, zukünftigen 6G- und weltraumbasierten Infrastruktur als Rückgrat der Digitalisierung der Gesellschaft – werden über einen ganzheitlichen Ansatz fortlaufend evaluiert und an die neuen Gefährdungen angepasst. Im Bereich 6G wird früh und

[42] Vergleiche strategisches Ziel 8.2.7 „Forschung und Entwicklung resilienter, sicherer IT-Produkte, Dienstleistungen und Systeme für den EU-Binnenmarkt fördern“.

intensiv auf ein hohes Sicherheitsniveau hingearbeitet. Die Bundesregierung fördert die Forschung und Entwicklung eines ganzheitlichen 6G-Systems. Dies soll eine Grundlage für Akteure aus Deutschland schaffen, um die 6G-Standardisierung maßgeblich mitzuprägen und entsprechende Technologien in den Markt zu bringen. Entsprechende offene Basistechnologien, insbesondere offene und sichere Standards für Hard- und Software, und interoperable Schnittstellen werden aktiv von staatlicher Seite gefördert und mit geeigneten Regulierungsansätzen begleitet[43].

Deutsche und europäische Netzinfrastruktur- und Cloudanbieter sowie die Analyse und Erforschung neuer Cybersicherheitsrisiken in diesen Netzen werden gefördert.

Es sind Mechanismen entwickelt und in Kraft gesetzt, mittels derer aus Forschungsergebnissen marktfähige Produkte deutscher Firmen entstehen, die dauerhaft in Deutschland hergestellt werden. Sicherheitsstandards „Made in Germany“ nehmen hierdurch einen Platz auf dem Weltmarkt ein.

Welche Wirkung erwarten wir?

Durch die Förderung deutscher und europäischer Anbieter sowie die Weiterentwicklung eigener Kompetenzen in der Erforschung neuer Cybersicherheitsrisiken wird das souveräne Handeln Deutschlands im Cyberraum sichergestellt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Verfügbarkeit der Telekommunikationsnetze und deren Widerstandsfähigkeit gegenüber Störungen und Angriffen wurde erhöht.
- Die Vertraulichkeit der Telekommunikation ist bis auf die gesetzlich vorgesehenen Ausnahmen gewahrt; das Fernmeldegeheimnis wird aktiv geschützt.
- Die Integrität der Telekommunikationsnetze ist gewahrt.
- Software und Hardware der kritischen Komponenten wird vor ihrem Einsatz einer Überprüfung unterzogen, mit der Schwachstellen erkannt und beseitigt werden.
- Deutsche und europäische Unternehmen sind in den betreffenden Standardisierungsgremien präsent und prägen maßgeblich die Standardisierung zukünftiger Telekommunikationssysteme mit einer gesteigerten Anzahl von Standardisierungsbeiträgen.
- Die Anzahl der (Erst-) Anmeldungen standardessenzieller Patente in Europa ist gestiegen.
- Der Anteil standardessenzieller Patente aus Deutschland in den internationalen Standards ist gestiegen.
- Der Anteil deutscher und europäischer Netzkomponenten in Telekommunikationsnetzen ist gestiegen.
- Technologie-Roadmaps für den zukünftigen 6G-Standard wurden berücksichtigt, um frühzeitig wirksame und nachvollziehbare Kriterien und Maßstäbe in einem Sicherheitskatalog für 6G-Netzkomponenten zu definieren.

8.3 Handlungsfeld 3: Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur

Deutschland verfügt über eine leistungsfähige Cybersicherheitsarchitektur. Die Institutionen des Bundes arbeiten zur Gewährleistung der Sicherheit im Cyberraum eng zusammen. Der bereits langjährig etablierte intensive Austausch zwischen Bundes- und Landesbehörden wurde in den letzten Jahren in zentralen Bereichen weiter ausgebaut. Diese Kooperationen dienen einem Ziel: allen Menschen in Deutschland die freiheitliche Nutzung des digitalen Raumes zu ermöglichen und dabei auf ein größtmögliches Maß an Sicherheit vertrauen zu können.

Doch rasante Entwicklungen im Cyberraum stellen die staatlichen Akteure beständig vor neue Herausforderungen:

- Durch die mittlerweile alle Lebensbereiche durchdringende Digitalisierung wächst die Bedeutung, die die Cybersicherheit für die Funktionsfähigkeit von Gesellschaft, Wirtschaft und Staat einnimmt.

[43] Vergleiche strategisches Ziel 8.2.6 „Einen einheitlichen europäischen Regulierungsrahmen für Unternehmen schaffen“.

- Neue technologische Entwicklungen können neue Angriffsflächen bieten, aber auch neue Abwehrmöglichkeiten, die es zu erschließen gilt.
- Die Bereitschaft anderer Staaten, Cyberangriffe mit dem Ziel der Spionage, Sabotage und politischen Einflussnahme durchzuführen, steigt immer weiter.
- Angreifer professionalisieren sich zunehmend und entwickeln ihre Methoden und Techniken bei Cyberangriffen kontinuierlich weiter.

Diesen Herausforderungen kann nur effektiv begegnet werden, indem die Cybersicherheitsarchitektur in Deutschland einem permanenten Prozess der Überprüfung und Weiterentwicklung unterzogen wird:

- Das Zusammenspiel der staatlichen Institutionen muss fortlaufend strukturell und prozessual bewertet und gegebenenfalls angepasst werden, um Barrieren, die eine effektive Zusammenarbeit verhindern, weiter abzubauen. Dabei gilt es, die Zusammenarbeit zwischen Bund und Ländern stetig weiterzuentwickeln und Schnittstellen zu Akteuren außerhalb der (Bundes-)Verwaltung zu berücksichtigen. Alle Zuständigkeiten und Aufgaben innerhalb der Cybersicherheitsarchitektur müssen klar definiert sein.
- Es ist kontinuierlich zu prüfen, ob die staatlichen Institutionen über ausreichende Kompetenzen und Befugnisse verfügen, um die Sicherheit von Bürgerinnen und Bürgern, Wirtschaft und Staat auch im Cyberraum zu gewährleisten. Sollten Regelungs- oder Fähigkeitslücken identifiziert werden, sind diese zu schließen. Sollten sich Befugnisse als nicht mehr erforderlich erweisen, sind diese abzuschaffen.
- Zudem müssen für neue Herausforderungen im Cyberraum auch neue Mittel und Wege gefunden werden, diese schnell zu erkennen und ihnen wirksam begegnen zu können.

Mit den folgenden strategischen Zielen wollen wir, die Bundesregierung, diese Aufgaben angehen.

8.3.1 Die Möglichkeiten des Bundes zur Gefahrenabwehr bei Cyberangriffen verbessern

Warum ist das Ziel relevant?

In Deutschland sind für die Gefahrenabwehr grundsätzlich die Länder zuständig. Cyberangriffe stellen jedoch vielfach eine länderübergreifende Gefahr dar und haben häufig eine internationale Dimension. Zur Abwehr von Cyberangriffen ist zudem äußerst hohe technische Expertise erforderlich, die effektiv nur an wenigen Stellen in Deutschland aufgebaut werden kann. Soweit Cyberangriffe einen im Ausland liegenden Ausgangspunkt haben, kann die Abwehr dieser Angriffe zudem außen- und sicherheitspolitische Bezüge mit sich bringen, also kompetenziell an die Bundesebene adressiert sein.

Wo stehen wir?

Dem Bund stehen nach geltendem Verfassungsrecht lediglich in bestimmten Bereichen gefahrenabwehrrechtliche Sonderzuständigkeiten zu (zum Beispiel in den Bereichen Eigensicherung, internationaler Terrorismus, Grenzschutz oder Sicherheit auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes). In allen anderen Fällen kann der Bund wegen der grundsätzlichen Landeszuständigkeit für die Gefahrenabwehr selbst bei bedeutenden, komplexen und/oder länderübergreifenden Cybergefahrenlagen, die einer bundeseinheitlichen Lösung und vielfach auch internationaler Abstimmung bedürften, nicht selbst gefahrenabwehrend tätig werden. Diese Zuständigkeitsaufteilung wird der aktuellen und sich absehbar weiter verschärfenden Bedrohungslage im Cyberbereich nicht gerecht. Cybergefahren in Deutschland kann so dauerhaft nicht wirksam begegnet werden.

Was wollen wir erreichen?

Wir streben an, im Grundgesetz eine erweiterte Gesetzgebungs- und Verwaltungskompetenz des Bundes zur Abwehr von Gefahren zu verankern, die von besonders schweren und bedeutenden Cyberangriffen auf informationstechnische Systeme und Netze ausgehen. Darauf aufbauend ist zu klären, ob es entsprechend neuer oder ergänzter Aufgaben und Befugnisse der (Sicherheits-)Behörden des Bundes bedarf.

Welche Wirkung erwarten wir?

Durch die Schaffung einer erweiterten Gesetzgebungs- und Verwaltungskompetenz des Bundes für die Gefahrenabwehr besonders schwerer und bedeutender Cyberangriffe werden die Möglichkeiten für eine effektive Cyberabwehr erweitert. Gegen die Ursachen schwerer Cyberangriffe kann aktiv vorgegangen werden, um deren schädliche Wirkung im besten Fall komplett zu unterbinden. Damit steigt das gesamtstaatliche Cybersicherheitsniveau.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Durch eine Änderung des Grundgesetzes wurden die Möglichkeiten des Bundes zur Abwehr von Gefahren erweitert, die von besonders schweren und bedeutenden Cyberangriffen ausgehen.
- Für die (Sicherheits-)Behörden des Bundes wurden Aufgaben und Befugnisse zur Gefahrenabwehr im Cyberraum ausgebaut.

8.3.2 Die technisch-operativen Einheiten des BSI zukunftsfähig ausgestalten und vernetzen

Warum ist das Ziel relevant?

Das BSI muss seine Fähigkeiten zur technisch-operativen Detektion von und Reaktion auf Cybersicherheitsvorfälle permanent an die sich dynamisch entwickelnde Bedrohungslage anpassen. Dabei braucht es technisch, personell und finanziell gut ausgestatte operative Einheiten, die mit den entsprechenden Einheiten anderer nationaler Stellen, Stellen der EU, der Länder, der Wirtschaft und der Wissenschaft bestens vernetzt agieren.

Wo stehen wir?

Die technisch-operativen Einheiten des BSI bestehen aus dem Nationalen IT-Lagezentrum, dem CERT-Bund, den Mobile Incident Response Teams (MIRTs) sowie dem BSOC.

Das nationale IT-Lagezentrum bündelt und bewertet aktuelle Beobachtungen und Aktivitäten im Cyberraum, um frühzeitig bedrohliche Lagen feststellen und zeitnah reagieren zu können. Dabei arbeitet das Nationale IT-Lagezentrum eng mit dem CERT-Bund als der zentralen Stelle im BSI für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen zusammen. Das CERT-Bund ist sowohl im Verwaltungs-CERT-Verbund (VCV) mit den Länder-CERTs als auch im deutschen CERT-Verbund mit den Teams großer Organisationen und Unternehmen organisiert.

Die MIRTs unterstützen vor Ort bei der Bewältigung gravierender Cybersicherheitsvorfälle und stehen einem steigenden Bedarf gegenüber. Aufgabe des BSOC ist es insbesondere, sicherheitsrelevante Ereignisse für die Regierungsnetze und IT-Systeme des Bundes zu detektieren und auszuwerten.

Was wollen wir erreichen?

Um ein möglichst umfassendes Bild der aktuellen Lage zu gewinnen, bauen das Nationale IT-Lagezentrum und die Beobachtungsstellen von Ländern, Wirtschaft und Wissenschaft ihre Informationskanäle aus und synchronisieren verstärkt ihre gewonnenen Lageinformationen.[44] Dies ermöglicht es CERTs von Bund, Ländern, Wirtschaft und Wissenschaft, Vorfälle noch effektiver zu bewerten, daraus gewonnene Erkenntnisse zu teilen und Reaktionsmaßnahmen einzuleiten. Hierzu wird das BSI seine Analysekapazitäten erhöhen, mehr Informationen und Erkenntnisse mit seinen Partnern teilen sowie die Informationen standardisiert und zielgruppengerecht aufbereiten. Die Vernetzungsstrukturen werden regelmäßig evaluiert und verbessert.

Die MIRTs sind technisch, personell und finanziell so ausgebaut, dass sie die steigenden Bedarfe Kritischer Infrastrukturen sowie von Institutionen im besonderen öffentlichen Interesse an professioneller Unterstützung vor Ort nachhaltig erfüllen können.

Das BSOC arbeitet mit den für Detektion zuständigen Stellen der Länder eng zusammen. Die Gründung eines SOC-Verbundes als Ergänzung des VCV mit hiervon abgegrenzten Aufgaben wird dabei in Betracht gezogen. Gleichzeitig ist das BSOC als nationale Koordinationsstelle für das von der EU-Kommission geplante Cyber Shield etabliert.

---

[44] Zur Stärkung des Informationsaustausches im Cyber-AZ siehe strategisches Ziel 8.3.4 „Das Syber-AZ weiterentwicheln".

Welche Wirkung erwarten wir?

Die technisch, personell und finanziell weiterentwickelten und besser vernetzten technisch-operativen Stellen des BSI sind in der Lage, schnell und effektiv zu handeln. Cybersicherheitsvorfälle in den Regierungsnetzen und in der Bundesverwaltung werden zeitnah und zuverlässig erkannt. Die Schadenswirkung von Cyberangriffen wird minimiert. Betroffene innerhalb und außerhalb der Bundesverwaltung werden bestmöglich bei der Bewältigung von Cybersicherheitsvorfällen unterstützt. Neue Angriffsmethoden und eine höhere Anzahl von Cyberangriffen können erkannt und bewältigt werden. Der Informationsaustausch zwischen Bund und Ländern und mittels des EU Cyber Shields erhöht die Erkennungsrate sicherheitsrelevanter Ereignisse und reduziert die Erfolgswahrscheinlichkeit von Angriffen spürbar.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das BSOC ist als nationale Verbindungsstelle der EU Cyber Shield-Initiative etabliert.
- Das BSOC kooperiert mit den zuständigen Länder-Stellen im Bereich der Detektion.
- Die MIRTs können den von Kritischen Infrastrukturen sowie von Institutionen im besonderen öffentlichen Interesse gemeldeten Unterstützungsbedarf zeitnah und effektiv erfüllen.

8.3.3 Die institutionalisierte Zusammenarbeit zwischen dem BSI und den Ländern stärken

Warum ist das Ziel relevant?

Der Cyberraum ist länderübergreifend hoch vernetzt. Um in diesem Umfeld ein möglichst einheitliches Sicherheitsniveau zu gewährleisten und effektiv auf Cyberbedrohungen zu reagieren, ist eine enge Zusammenarbeit zwischen Bund und Ländern unter Einbindung der Kommunen unabdingbar. Für die erforderliche intensive und dauerhafte gegenseitige Information, Abstimmung und Unterstützung bedarf es institutionalisierter Kooperationsformen.

Wo stehen wir?

Für die Bereiche Cyberkriminalität und Cyberspionage bestehen im Bund-Länder-Verhältnis bewährte Gremienstrukturen. Darüber hinaus sind das BKA und das BfV mit ihrer jeweiligen Zentralstellenfunktion bereits als tragende Säulen einer föderal integrierten Cybersicherheitsarchitektur ausgestaltet.

Auch im Aufgabenbereich des BSI gibt es im Bund-Länder-Verhältnis funktionierende Kooperationsplattformen – insbesondere im Bereich der präventiven Eigensicherung der Verwaltungen. Ebenso hat sich die Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz als Austauschplattform zwischen Bund und Ländern bewährt. Darüber hinaus wurde dem BSI die Unterstützung der Länder als gesetzliche Aufgabe übertragen. Aufgrund der grundgesetzlichen Zuständigkeitsverteilung zwischen Bund und Ländern ist diese jedoch auf eine ergänzende Hilfeleistung im Einzelfall im Rahmen der Amtshilfe beschränkt.

Was wollen wir erreichen?

Um die effektive Zusammenarbeit zwischen dem BSI und den Ländern zeitnah zu stärken, wird der Abschluss verbindlicher bilateraler Kooperationsvereinbarungen angestrebt, in denen die Schwerpunkte des gemeinsamen Engagements festgeschrieben werden. Die jeweilige Kooperationsvereinbarung führt die Felder, in denen eine Zusammenarbeit zwischen dem BSI und dem jeweiligen Land bereits stattfindet oder künftig stattfinden soll, in einer Vereinbarung zusammen und gibt dieser Kooperation einen planbaren und strukturierten Rahmen.

Um die institutionalisierte Zusammenarbeit zwischen Bund und Ländern zu vertiefen, wird darüber hinaus angestrebt, das BSI in seinem Aufgabenbereich zu einer Zentralstelle im Bund-Länder-Verhältnis auszubauen und somit – neben dem BKA im Polizeiwesen und dem BfV im Verfassungsschutzverbund – zur dritten Säule einer föderal integrierten Cybersicherheitsarchitektur weiterzuentwickeln. Als Zentralstellen ausgestaltete Bundesbehörden erlauben organisatorische Verbindungen verschiedener Bundes- und Landesbehörden zur dauerhaften gegenseitigen Information, Abstimmung und Unterstützung.

Welche Wirkung erwarten wir?

Durch die intensivere Zusammenarbeit zwischen Bund und Ländern auf Grundlage bilateraler Kooperationsvereinbarungen werden Ressourcen des Staates durch abgestimmtes Handeln und die Bündelung von Kompetenzen effektiver eingesetzt. Zielgruppen in Staat, Wirtschaft und Gesellschaft können breiter und zielgenauer adressiert werden. Der Wissens- und Kompetenztransfer zwischen Bund und Ländern nimmt zu.

Durch den Ausbau des BSI zur Zentralstelle wird ein weiterer Schritt zu einer effektiven Cybersicherheitsarchitektur gegangen. Auf die Zentralstellenfunktion des BSI kann eine kooperative und komplementäre Aufgabenverteilung zwischen Bund und Ländern gestützt werden, in deren Umsetzung ein umfassender Informationsaustausch gewährleistet ist und eine dauerhafte und regelmäßige gegenseitige Unterstützung stattfinden kann. Auf dieser Basis werden die Fähigkeit zur Prävention, Erkennung von und Reaktion auf Cyberbedrohungen und damit das gesamtstaatliche Cybersicherheitsniveau verbessert.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das BSI hat bilaterale Kooperationsvereinbarungen mit den Ländern abgeschlossen und führt auf deren Grundlage gemeinsame Vorhaben durch.
- Das BSI wurde durch Änderung des Grundgesetzes und nachfolgende einfachrechtliche Anpassungen zur Zentralstelle in seinem Aufgabenbereich im Bund-Länder-Verhältnis ausgebaut.

8.3.4 Das Cyber-AZ weiterentwickeln

Warum ist das Ziel relevant?

Cyberbedrohungen sowie Motivation und Ziel von Cyberangriffen sind oftmals nicht unmittelbar erkennbar. Je nach konkreter Fallgestaltung werden Cyberangriffe, Cyberbedrohungen und Cybergefahren daher regelmäßig nur einem Teil der zuständigen Behörden oder auch nur einzelnen betroffenen Einrichtungen bekannt. Darüber hinaus ist nicht immer gewährleistet, dass gesamtstaatlich relevante Sachverhalte zeitnah als solche erkannt werden. Dadurch wird eine angemessene Reaktion auf die Cybervorfälle erschwert.

Wo stehen wir?

Das Cyber-AZ ist eine 2011 gegründete Kooperations- und Informationsplattform, an der zurzeit das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für den Militärischen Abschirmdienst (BAMAD), das BSI, das BfV, das BKA, der BND, das Bundespolizeipräsidium (BPOLP) und das KdoCIR beteiligt sind. Es ist ein wesentlicher Bestandteil der Cybersicherheitsarchitektur Deutschlands, dessen Arbeitsweise sich stetig an aktuelle Entwicklungen anpassen muss. 2019 wurde die Zusammenarbeit im Cyber-AZ neu konzipiert. Damit wurden weitere Maßnahmen ergriffen, um die Fähigkeit zur koordinierten und kooperativen Bewältigung von Sachverhalten mit gesamtstaatlicher Relevanz auszubauen und den Informationsaustausch weiter zu verbessern.

Was wollen wir erreichen?

Das Cyber-AZ als zentrale Kooperations-, Kommunikations- und Koordinationsplattform der relevanten (Sicherheits-) Behörden wird in Abhängigkeit von der Entwicklung der Bedrohungslage fortentwickelt. Zur Stärkung des insbesondere ressortübergreifenden Informationsaustausches zu Cyberangriffen, Cyberbedrohungen und Cybergefahren werden die Grundlagen für den behördenübergreifenden Austausch von Informationen angepasst, der Austausch intensiviert und – soweit zur Zielerreichung geeignet – weitere Partner in die Arbeit des Cyber-AZ integriert; hierzu gehören insbesondere auch die Länder.

Durch den intensivierten Austausch, technisch unterstützte Lageinformationsverarbeitungs-, Auswerte- und Darstellungssysteme und dadurch verbesserte bedarfsgerechte Analysen wird die Berichterstattung des Cyber-AZ erweitert und verbessert. Der digitale Austausch auch von höher eingestuften Informationen zwischen allen teilnehmenden Institutionen soll möglich, die Auswertefähigkeit des Cyber-AZ beschleunigt und das Führen eines aktuellen, abgestimmten Gesamtlagebildes zur Cybersicherheitslage ermöglicht werden. Neue Berichtsformate des Cyber-AZ sollen zu Cyberangriffen in und Cybergefahren für Deutschland einen umfassenden und aktuellen Überblick gewährleisten. Dies schließt auch einen leistungsfähigen Informationsaustausch mit der Wirtschaft ein.

Zudem ist sichergestellt, dass bei komplexen Cyberlagen der Übergang von der Cyberabwehr zur Cyberverteidigung erkannt wird.

Welche Wirkung erwarten wir?

Informationen zu Cybersicherheitsvorfällen werden schneller unter Berücksichtigung aller betroffenen Behörden kommuniziert und komplexe Cyberlagen so besser behörden- und ressortübergreifend koordiniert.

Die Erweiterung des Cyber-AZ durch Einbindung weiterer ausgewählter Einrichtungen, Stellen oder Organisationen trägt dazu bei, zusätzliche Informationsquellen oder Handlungsoptionen zu erschließen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Grundlagen für den behördenübergreifenden Austausch von Informationen im Cyber-AZ wurden angepasst.
- Cybersicherheitsvorfälle und Cyberlagen werden schnell und effektiv bearbeitet.
- Ein umfassendes und aktuelles Cyberlagebild ist jederzeit verfügbar.

8.3.5 Cyber- und Informationssicherheit der Bundesverwaltung stärken

Warum ist das Ziel relevant?

Die Bundesverwaltung befindet sich inmitten eines Prozesses der digitalen Transformation. Eine digitale Verwaltung ist maßgeblich für ein funktionsfähiges, effizientes und modernes Staatswesen. Gleichzeitig steigt auch der Anteil digitaler Angebote des Bundes für Wirtschaft und Gesellschaft. Auch hier ist Cyber- und Informationssicherheit essenziell für die Funktionsfähigkeit und Vertrauenswürdigkeit der staatlichen digitalen Angebote.

Wo stehen wir?

Das Informationssicherheitsmanagement der Bundesverwaltung beruht auf dem vom Kabinett beschlossenen UP Bund. Der UP Bund ist die Informationssicherheitsrichtlinie des Bundes und formuliert die verbindlichen Rahmenbedingungen für den Schutz der in der Bundesverwaltung verarbeiteten Informationen und der dabei genutzten IT-Systeme, Dienste und Kommunikationsnetzinfrastrukturen des Bundes. Unter anderem regelt er die Einhaltung des IT-Grundschutzes sowie der vom BSI entwickelten Mindeststandards durch die Bundesbehörden. Laut UP Bund ist bei ressortübergreifenden Vorhaben frühzeitig, das heißt bereits in der Initiierungs- und Konzeptionsphase, sicherzustellen, dass die Aspekte der Informationssicherheit in angemessener Weise berücksichtigt werden. Das BSI ist in geeigneter Weise in beratender Rolle einzubinden.

Was wollen wir erreichen?

Die Cybersicherheitsarchitektur des Bundes soll auf strategischer Ebene gestärkt werden. Zudem soll auf operativer Ebene ein Kompetenzzentrum Operative Sicherheitsberatung Bund im BSI eingerichtet werden, um die Ressorts bei der Umsetzung von Sicherheitsvorhaben zu unterstützen. Darüber hinaus stärken wir die Rolle der Informationssicherheitsbeauftragten der Bundesverwaltung, indem wir hierfür eine gesetzliche Grundlage schaffen.

Welche Wirkung erwarten wir?

Wir verbessern und stärken das vorhandene Informationssicherheitsmanagement der Bundesverwaltung und die Unterstützung der Informationssicherheitsbeauftragten der einzelnen Bundesbehörden durch das BSI vor Ort. Außerdem stellen wir sicher, dass das BSI frühzeitig in die Digitalisierungsvorhaben des Bundes eingebunden wird. Informationssicherheit wird so zu einem natürlichen Bestandteil in der Digitalisierung der Bundesverwaltung.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die gesetzliche Grundlage für die Rolle der Informationssicherheitsbeauftragten der Bundesverwaltung wurde geschaffen.
- Die Überprüfung vorhandener Rollen und Schnittstellen im Informationssicherheitsmanagement auf Verbesserungspotential ist erfolgt. Ein Konzept für deren bedarfsweisen Ausbau beziehungsweise die Entwicklung neuer Rollen im Hinblick auf die Erhöhung der Cyber- und Informationssicherheit sowie die Zusammenarbeit der (Ressort-)Informationssicherheitsbeauftragten untereinander auf Ebene des Bundes liegt vor.
- Die Zusammenarbeit zwischen den Ressort-IT-Sicherheitsbeauftragten des Bundes ist deutlich gestärkt, inhaltliche wie ggf. auch institutionelle Maßnahmen dazu sind getroffen.
- Das Kompetenzzentrum Operative Sicherheitsberatung Bund des BSI wurde eingerichtet und hat seine Arbeit aufgenommen.
- Ein gezieltes Verstärkungsprogramm für die Cyber- und Informationssicherheit des Bundes ist ressortübergreifend abgestimmt und verabschiedet.

8.3.6 Cybersicherheit im Umfeld von Wahlen erhöhen

Warum ist das Ziel relevant?

Allgemeine, unmittelbare, freie, gleiche und geheime Wahlen sind das Fundament unserer Demokratie. Auch vor diesem Fundament macht die Digitalisierung nicht halt – das Internet dient als Informationsquelle für die politische Meinungsbildung, soziale Medien werden als Instrument für den Wahlkampf genutzt und nicht zuletzt erfolgt auch die Übermittlung der vorläufigen Wahlergebnisse digital. Die Absicherung des Wahlumfeldes ist daher auch eine Herausforderung für die Cybersicherheit.

Darüber hinaus ist gerade vor Wahlen die Gefahr von Einflussnahmeoperationen durch ausländische Nachrichtendienste erhöht. Ereignisse im Ausland verdeutlichen die Fähigkeiten und die grundsätzliche Bereitschaft zu Einflussnahmeversuchen durch Veröffentlichung ausspionierter kompromittierender oder auch manipulierter Daten.

Wo stehen wir?

Im Umfeld von Wahlen sensibilisieren die Behörden des Bundes relevante Akteure für Cybergefahren und beraten zur Informationssicherheit. Zudem entwickelt das BSI im Auftrag des Bundeswahlleiters Sicherheitsanforderungen zum Schutz der Ergebnisübermittlung von Bundestagswahlen. Die Aufklärung von Cyberangriffen zur Einflussnahme im Vorfeld von Wahlen nehmen die Nachrichtendienste in ihrer Funktion als Frühwarnsystem wahr.

Was wollen wir erreichen?

Um die Verwundbarkeit des zunehmend digitalisierten Wahlumfeldes und der Wahlinfrastruktur zu reduzieren, wird angestrebt, die Cybersicherheit im Umfeld von Wahlen zu erhöhen.

Die Behörden des Bundes unterstützen relevante Akteure im Wahlumfeld im Hinblick auf die Cybersicherheit. Im jeweiligen Zuständigkeitsbereich analysieren sie Risiken, identifizieren Sicherheitsanforderungen und stehen im politischen Raum als Ansprechpartner für Belange der Cybersicherheit im Zusammenhang mit Wahlen zur Verfügung.

Welche Wirkung erwarten wir?

Wahlen werden durch Erreichung eines angemessenen Sicherheitsniveaus des Wahlumfeldes mittels Prävention, Vorfeldaufklärung, Detektion und Reaktion geschützt. Das politische Umfeld ist sich der Bedrohungssituation im Cyberraum im Zusammenhang mit Wahlen bewusst und kann entsprechende Schutzmaßnahmen ergreifen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es existieren stets der Lageentwicklung angepasste Handlungsempfehlungen und ein Beratungsangebot für Wahlleitungen auf Bundes- und Landesebene.

- Zielgruppen des politischen Raumes werden für Belange der Cybersicherheit im Umfeld von Wahlen sensibilisiert.
- Es existiert ein fundiertes und auf den Aspekt „Wahlen“ spezifiziertes Cyberbedrohungslagebild, welches schädliche Akteure, deren Motive und Vorgehensweisen benennt.

8.3.7 Strafverfolgung im Cyberraum intensivieren

Warum ist das Ziel relevant?

Nicht nur die Zahl der von Cyberkriminalität betroffenen Computersysteme und Endgeräte steigt, sondern auch die Professionalität der Täterinnen und Täter. Einerseits versuchen Täterinnen und Täter weiterhin, mit möglichst geringem Aufwand möglichst viele Computer mit Schadsoftware zu infizieren, um beispielsweise Kontodaten und Passwörter zu stehlen. Andererseits gibt es jedoch auch immer mehr sehr gut vorbereitete und hoch organisierte Cyberangriffe auf ausgewählte Ziele (beispielsweise Wirtschaftsunternehmen oder Kritische Infrastrukturen), bei denen das Schadenspotenzial für die Betroffenen erheblich größer ist. Gleichzeitig bringen aktuelle technische Entwicklungen, wie beispielsweise Automotive IT oder IoT, immer neue Tatmöglichkeiten und Deliktsphänomene hervor.

Angesichts dieser sich entwickelnden Bedrohungslage im Cyberraum müssen die Sicherheitsbehörden des Bundes und der Länder ihre gesetzlichen Aufgaben zur Verfolgung von Straftaten in der digitalen Welt genauso wie in der analogen Welt wahrnehmen können. Hierzu benötigen sie ausreichende Befugnisse[45].

Wo stehen wir?

Die Computerstraftaten sind in den §§ 202a ff., 263a, 269 f. und 303a f. des Strafgesetzbuches geregelt. In den vergangenen Jahren sind eine Reihe von Änderungs- und Überarbeitungsvorschlägen für das Computerstrafrecht vorgelegt und diskutiert worden, unter anderem gab es mehrere Gesetzesinitiativen des Bundesrats.

Was wollen wir erreichen?

Die Sicherheitsbehörden des Bundes und der Länder benötigen ausreichende Befugnisse, um ihre Aufgaben in der digitalen Welt ebenso effektiv wahrnehmen zu können wie in der analogen Welt. Die Befugnisse werden daher fortlaufend überprüft und erforderlichenfalls an neue technische Entwicklungen angepasst. Dabei ist unter anderem zu prüfen, ob Ermittlungsmaßnahmen, wie TKÜ und Online-Durchsuchung, auch für die Ermittlung von Computerdelikten zur Verfügung stehen sollten.

Zudem sollen die geltenden strafrechtlichen Regelungen im Bereich des Computerstrafrechts auf Reformbedarf überprüft werden.

Welche Wirkung erwarten wir?

Die Arbeitsfähigkeit der Sicherheitsbehörden bleibt im digitalen Zeitalter erhalten. Sie können angemessen auf neue Deliktsphänomene und erhöhtes Gefahrenpotential im Cyberraum reagieren.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Befugnisse aus der Strafprozessordnung entsprechen den Anforderungen der Praxis.
- Für das Strafgesetzbuch werden, sofern eine Überprüfung entsprechenden Bedarf ergibt, Gesetzgebungsvorschläge vorgelegt.

[45] Zur internationalen Strafverfolgung und Bekämpfung von Cyberkriminalität siehe auch das strategische Ziel „Internationale Zusammenarbeit bei der Strafverfolgung stärken und internationale Cyberkriminalität bekämpfen“.

8.3.8 Zentrale Kompetenz- und Service-Dienstleistungen des BKA zur Bekämpfung von Cyberkriminalität ausbauen

Warum ist das Ziel relevant?

Im Rahmen seiner bestehenden Aufgaben unterstützt das BKA die Polizeien des Bundes und der Länder, indem zum einen operative Daten zur Verfügung gestellt werden und zum anderen modernste Technik für die kriminalpolizeiliche Arbeit gebündelt vorgehalten wird. Cyberkriminalität ist weiter zunehmend durch Angriffe gekennzeichnet, die in ihrem Auftreten in einem bestimmten Zeitraum quantitativ wellenförmig zu- und wieder abnehmen und dabei Geschädigte in mehreren Bundesländern oder aber im gesamten Bundesgebiet betreffen. Um einen Serienzusammenhang zu erkennen, ist eine umfängliche Koordination mit allen betroffenen Ermittlungsbehörden notwendig.

Wo stehen wir?

Das BKA hat mit dem Konzept der CyberToolBox begonnen, Informationen, Daten und Werkzeuge zur Verfügung zu stellen. Die CyberToolBox wurde Ende 2019 ausgerollt und als operatives Informationsportal etabliert. Die darin bereitgestellten Werkzeuge und Datensets wurden seitdem sukzessive ausgebaut. Aktuell nutzen über 5.000 Mitarbeiterinnen und Mitarbeiter von Strafverfolgungsbehörden die dort bereitgestellten Werkzeuge und innerhalb von zwölf Monaten konnten in mehr als 8.000 Fällen in den Ländern isoliert (zu gleichen Tat- beziehungsweise Täterstrukturen) geführte Ermittlungsverfahren zusammengeführt werden.

Das BKA unterstützt die Polizeidienststellen des Bundes und der Länder bei der Koordinierung beziehungsweise Durchführung von zentralen Ermittlungen im Zusammenhang mit Straftatenwellen.

Was wollen wir erreichen?

Der Austausch von Informationen, Kompetenzen und Tools zwischen dem BKA und den Polizeidienststellen des Bundes und der Länder im Rahmen der jeweils bestehenden Rechtsvorschriften ist qualitativ und quantitativ intensiviert. Die weiterentwickelte CyberToolBox befriedigt einen wesentlichen Teil der datenbasierten operativen Informations- und Unterstützungsbedürfnisse der Länder und eröffnet ihnen Zugang zu allen phänomenrelevanten Informationen, Daten und Werkzeugen, die sie benötigen. Eine bundesweite Community von Cyberkriminalitäts-Ermittlungsdienststellen befördert den direkten und effizienten Austausch operativer und ermittlungsrelevanter Erkenntnisse und Methoden.

Sofern durch eine oder mehrere Polizeidienststellen des Bundes oder der Länder oder durch das BKA eine Straftatenwelle festgestellt wird, koordinieren die genannten Behörden die Durchführung von „Zentralen Ermittlungen“, die langfristig verstärkt zu führen sein werden.

Welche Wirkung erwarten wir?

Diese Erweiterungen des Funktions- und Leistungsumfangs der CyberToolBox werden die Nutzerzahlen steigen lassen und eine höhere Anzahl von an das BKA übermittelten Operativdaten bewirken. Auf dieser Basis ist es dem BKA dann wiederum möglich, die notwendigen Zentralstellenaufgaben wahrzunehmen.

Beim Auftreten von Straftatenwellen trägt das Instrument der „Zentralen Ermittlungen“ zu einer bedarfsgerechten Auslastung der Polizeidienststellen und effektiven Ermittlungsführung bei, insbesondere zur Vermeidung von Doppelarbeit.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das Instrument der „Zentralen Ermittlungen“ wird häufiger angewandt.
- Die Nutzerzahl der CyberToolBox ist gestiegen.
- Die Anzahl der übermittelten fachlichen Anfragen an die CyberToolBox ist gestiegen.
- Die Treffer- und Auskunftsquote der CyberToolBox ist gestiegen.
- Die Anzahl der durch die CyberToolBox bereitgestellten Daten ist gestiegen.

8.3.9 Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung gewährleisten

Warum ist das Ziel relevant?

Immer mehr Kommunikationskanäle und Datenspeicherdienste werden durch Ende-zu-Ende-Verschlüsselung gesichert. Die sichere Verschlüsselung ist ein notwendiges Mittel zum Schutz der Grundrechte und der digitalen Sicherheit von Staat, Wirtschaft und Gesellschaft. Doch auch Kriminelle nutzen Verschlüsselungslösungen für die Vorbereitung und Durchführung von Straftaten. Die Verschlüsselung macht den Zugang zu Kommunikationsinhalten und deren Analyse im Rahmen einer rechtmäßig angeordneten TKÜ, die insbesondere bei schwersten Straftaten und der organisierten Kriminalität eine zentrale Erkenntnisquelle für die Ermittlungsbehörden darstellt, äußerst schwierig oder gar praktisch unmöglich.

Daher gilt es entsprechend dem Grundsatz „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“, die Privatsphäre und die Sicherheit der Kommunikation durch Verschlüsselung zu schützen. Gleichzeitig soll für die zuständigen Behörden die Möglichkeit aufrechterhalten werden, über einen rechtmäßigen Zugang zu Daten für legitime und klar definierte Zwecke im Rahmen der Bekämpfung schwerer und/oder organisierter Kriminalität, Kinderpornographie und Terrorismus – auch in der digitalen Welt – zu verfügen und die Rechtsstaatlichkeit zu wahren.

Wo stehen wir?

Die bisher etablierten Ausgleichsmaßnahmen der sogenannten Informationstechnischen Überwachung (Quellen-TKÜ) sowie die Onlinedurchsuchung sind wegen der operativen und technischen Herausforderungen in der Praxis auf Einzelfälle beschränkt.

Damit die Sicherheitsbehörden auch künftig in der Lage sind, ihre gesetzlichen Aufgaben vollständig zu erfüllen, sind neue Herangehensweisen in Bezug auf den unverschlüsselten Zugriff auf ursprünglich verschlüsselte Kommunikationsinhalte erforderlich.

Der Rat der Europäischen Union hat im Dezember 2020 eine Entschließung zum Umgang mit Verschlüsselung verabschiedet, in der die Notwendigkeit des Grundsatzes „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ hervorgehoben wird. Es soll ein Dialog mit den Technologieunternehmen geführt werden, um einen technikneutralen Ansatz für Ausgleichsmaßnahmen zur TKÜ zu finden unter Wahrung der grundrechtlichen Schutzvorgaben.

Was wollen wir erreichen?

Es bestehen die notwendigen Voraussetzungen, die den zuständigen Behörden einen rechtmäßigen Zugang zu Daten für legitime und klar definierte Zwecke im Rahmen der Bekämpfung schwerer und/oder organisierter Kriminalität, Kinderpornographie und Terrorismus einräumen und gleichzeitig die Privatsphäre, die Grundrechte und die Sicherheit der Kommunikation schützen.

Hierzu werden, zunächst in enger Abstimmung mit den Diensteanbietern, anderen betroffenen Interessenträgern und allen zuständigen Behörden, technische und operative Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation entwickelt. Um einem Missbrauch dieser Lösungen sowohl im europäischen als auch im internationalen Bereich vorzubeugen, werden technische, organisatorische und rechtliche Maßnahmen mit vorgesehen.

Welche Wirkung erwarten wir?

Die deutschen Sicherheitsbehörden können ihre gesetzlich vorgesehenen technischen Möglichkeiten der TKÜ auch bei verschlüsselten Inhalten effektiv wahrnehmen. Damit bleibt die TKÜ weiterhin ein zentraler Bestandteil der Ermittlungsmöglichkeiten und nachrichtendienstlichen Aufklärung. Die effektive Strafverfolgung und rechtzeitige Gefahrenabwehr bei schweren und schwersten Straftaten sowie die nachrichtendienstliche Aufklärung in hervorgehobenen Fällen ist dadurch weiterhin gewährleistet und unter anderem organisierte Kriminalität und Terrorismus können weiterhin wirksam bekämpft werden.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das Ziel eines europäischen Ansatzes unter Bezugnahme auf die Entschließung des Rates der EU zum Umgang mit Verschlüsselung mit Fokus auf einem technikneutralen Ansatz und dem dauerhaften Dialog mit den Diensteanbietern ist verankert.
- Technische und operative Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation sind in enger Abstimmung mit allen betroffenen Unternehmen, Interessenträgern und zuständigen Behörden auf europäischer Ebene entwickelt.
- Vorschläge für gesetzliche Grundlagen, die den rechtmäßigen und verhältnismäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation ermöglichen, wurden erarbeitet.

8.3.10 Den verantwortungsvollen Umgang mit Zero-Day-Schwachstellen und Exploits fördern

Eine Schwachstelle ist definiert als eine Sicherheitslücke in Soft- oder Hardware, die einzeln oder kombiniert genutzt werden kann, um (in der Regel unbemerkt) aktiven Zugriff auf ein Hard- oder Softwaresystem zu erhalten. Man unterscheidet zwischen sogenannten Zero-Day (auch 0-day), dem Hersteller unbekannten, und sogenannten n-Day Sicherheitslücken, die dem Hersteller bereits n Tage bekannt sind.

Ein Exploit (englisch *to exploit*: ausnutzen) ist ein Werkzeug oder eine systematische Möglichkeit (auch Beschreibung), um Schwachstellen und Fehlfunktionen von Hard- oder Software auszunutzen, um sich Zugriff auf die Daten oder Ressourcen zu verschaffen.

Warum ist das Ziel relevant?

Die Ziele, einerseits größtmögliche IT-Sicherheit zu gewährleisten, und andererseits die Notwendigkeit, Strafverfolgungs- und Sicherheitsbehörden die Erfüllung ihres gesetzlichen Auftrags zu ermöglichen, stehen in einem Spannungsverhältnis zueinander.

Dieses Spannungsverhältnis ist innerhalb der gesetzlichen Rahmenbedingungen und unter Bewahrung des größtmöglichen Schutzes für alle betroffenen (Grund-)Rechtsgüter aufzulösen. Im Interesse der Sicherheit, Vertraulichkeit und Integrität informationstechnischer Systeme ist es essenziell, dass erkannte Schwachstellen grundsätzlich geschlossen beziehungsweise zu diesem Zweck an die Hersteller gemeldet werden. Die Strafverfolgungs- und Sicherheitsbehörden müssen auch unter Berücksichtigung dieser Maßgaben ihrer Ermittlungs- und Aufklärungsarbeit weiterhin effektiv, gegebenenfalls mit restriktiven Ausnahmen, nachkommen können.

Wo stehen wir?

Die Nutzung von Zero-Day-Schwachstellen zu Zwecken der nachrichtendienstlichen Aufklärung, Gefahrenabwehr und Strafverfolgung erfolgt aktuell nach den für die jeweilige Sicherheitsbehörde geltenden internen Behördenvorgaben. Für diese im Einzelfall durchzuführende Nutzung gelten die allgemeinen Vorschriften.

Um diesen Prozess zu verbessern, wird an einer ausgewogenen behördenübergreifenden Strategie für den Umgang mit Schwachstellen für die Strafverfolgungs- und Sicherheitsbehörden gearbeitet (sogenannter Schwachstellenmanagementprozess – Vulnerability Equities Process).

Was wollen wir erreichen?

Eine ausgewogene behördenübergreifende Strategie zum Umgang mit Zero-Day-Schwachstellen nach den jeweils geltenden gesetzlichen Vorgaben bei den Strafverfolgungs- und Sicherheitsbehörden über bereits vorhandene interne Behördenvorgaben hinaus bringt die Interessen der Cyber- und Informationssicherheit sowie der Strafverfolgungs- und Sicherheitsbehörden in einen angemessenen Ausgleich. Grundlage dafür sind standardisierte Prozesse bei den Sicherheitsbehörden für einen sicheren und sachgerechten Umgang mit Schwachstellen und Exploits.

Kernpunkt dieser Prozesse ist die Risikoabwägung zwischen dem Gefährdungspotential von (Zero-Day-)Schwachstellen bei temporärer Ausnutzung durch die Sicherheits- und Strafverfolgungsbehörden und dem prognostizierten Nutzen für die nachrichtendienstliche Aufklärung, Gefahrenabwehr und Strafverfolgung (zur Einleitung des Coordinated Vulnerability Disclosure-Prozesses siehe strategisches Ziel 8.1.8 „Verantwortungsvoller Umgang mit Schwachstellen – Coordinated Vulnerability Disclosure fördern“).

Durch diesen Rahmen entsteht ein „verantwortungsvolles Schwachstellenmanagement“, welches klare Richtlinien für den Umgang mit Schwachstellen vorgibt. Der geschilderte Konflikt zwischen IT-Sicherheit und nachrichtendienstlicher Aufklärung, Gefahrenabwehr sowie Strafverfolgung wird so aufgelöst. Dabei steht der größtmögliche Schutz der Bevölkerung im Vordergrund. Abgewogen werden daher solche Gefahren, die Schwachstellen in informationstechnischen Systemen mit sich bringen, mit dem Erfolg bei der Erkennung und Abwehr schwerer Gefahren sowie einer effektiven Strafverfolgung, die mit Hilfe der Nutzung von (Zero-Day-)Schwachstellen erzielt werden können.

Welche Wirkung erwarten wir?

Das Sicherheitsniveau im Bereich der öffentlichen Sicherheit ist ebenso erhöht wie das Niveau der allgemeinen IT-Sicherheit. Inkonsistenzen im Umgang mit Zero-Day-Schwachstellen und Exploits sind beseitigt und es gibt einen verlässlichen nationalen Rahmen zum verantwortungsvollen Umgang mit diesen Instrumenten.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand des folgenden Kriteriums überprüfen:

- Es ist ein verbindliches Vorgehen etabliert, das den verantwortungsvollen Umgang mit Zero-Day-Schwachstellen und Exploits regelt.

8.3.11 Die Digitale Souveränität der Sicherheitsbehörden durch den Ausbau der ZITiS stärken

Warum ist das Ziel relevant?

Die Sicherheitsbehörden benötigen gerade in ihren kritischen Arbeitsfeldern der Cybersicherheit Lieferanten, die auch im Krisenfall zuverlässig zur Verfügung stehen. Sie sind auf Werkzeuge angewiesen, deren Funktionsweise auch vor dem Hintergrund ihrer Einsatzfähigkeit zur gesetzlichen Auftragserfüllung, wie zum Beispiel bei einer TKÜ, transparent dargelegt werden kann. Die hierfür notwendigen Kernfähigkeiten sind entsprechend aufzubauen und vorzuhalten, insbesondere, wenn sich Lieferketten verändern oder im Krisenfall nicht verlässlich sind. Dies ist unverzichtbar für die selbstbestimmte Aufgabenerfüllung der Sicherheitsbehörden und trägt im Sinne einer gesamtstaatlichen Handlungsfähigkeit maßgeblich zur Digitalen Souveränität Deutschlands bei.

Wo stehen wir?

Es ist im Schwerpunkt Aufgabe der ZITiS, für die Sicherheitsbehörden im Geschäftsbereich des BMI Werkzeuge und Methoden zu entwickeln, nachzuvollziehen, zu bewerten und zentral zur Verfügung zu stellen, deren Bündelung aufgrund gleichgelagerter Herausforderungen im Cyberraum bei Polizeien und Nachrichtendiensten erforderlich geworden ist.

Jedoch erfordert die hochdynamische technische Entwicklung für Sicherheitsanwendungen vor dem Hintergrund enormer Investitionen, die im Nicht-EU-Ausland in Zukunftstechnologien erfolgen, eine strategische Neuausrichtung, um auch künftig aus eigener Kraft handlungsfähig zu sein. Die Schwerpunktsetzung im Bereich der Forschung und Entwicklung ist beständig zu überprüfen und je nach technischem Fortschritt erforderlichenfalls anzupassen und dient als Grundlage für den Auftrag der ZITiS als Dienstleister für die Sicherheitsbehörden. Aktuell bestehen bei den eingesetzten und notwendigen technischen Lösungen häufig große Abhängigkeiten, insbesondere vom außereuropäischen Ausland. Ein gravierender Anteil der für die gesetzliche Auftragserfüllung eingesetzten technischen Geräte, Werkzeuge und Methoden der informationstechnischen Überwachung, Datenanalyse und Mustererkennung ist dementsprechend aufgrund fehlender industrieller Basis auf nationaler Ebene oder in der EU nicht im benötigten Umfang verfügbar. Ein selbstbestimmtes, unabhängiges Handeln der Sicherheitsbehörden ist in diesem Bereich trotz eigener Fähigkeiten daher aktuell nicht immer wie gewünscht möglich.

Was wollen wir erreichen?

Die ZITiS wird in die Lage versetzt, Werkzeuge und Methoden zu entwickeln, zu bewerten und zentral zur Verfügung zu stellen, die den Sicherheitsbehörden ein selbstbestimmtes Handeln ermöglichen, eine krisenfeste Versorgungssicherheit gewährleisten und deren Cyberfähigkeiten signifikant stärken.

Die zentrale Forschung und Entwicklung zugunsten eigener Werkzeuge und Methoden für diese Behörden wird bei der ZITiS im Rahmen des geltenden Rechts weiter ausgebaut. Gleichzeitig werden auch die weiteren Behörden anderer Ressorts ihre Vorhaben in Forschung und Entwicklung im Rahmen des jeweils geltenden Rechts weiter intensivieren.

Soweit kommerzielle Produkte zur Erfüllung des gesetzlichen Auftrages bei Polizeien, Nachrichtendiensten und im Geschäftsbereich des BMVg zum Einsatz kommen, sollen diese zur Erhöhung der Einsatzsicherheit möglichst umfassend geprüft werden.

Welche Wirkung erwarten wir?

Die ZITiS wird sich dadurch als wichtiger Baustein für eine gesamtstaatliche Cybersicherheit weiter etablieren sowie Herausforderungen agil und schnell angehen und Zukunftstechnologien als zentraler Dienstleister für die Sicherheitsbehörden insbesondere im Geschäftsbereich des BMI erschließen können.

Durch ein passgenaues Angebot der ZITiS an technischen Lösungen, Werkzeugen und Beratungsleistungen für die Sicherheitsbehörden werden die souveräne Handlungsfähigkeit deutscher Sicherheitsbehörden im digitalen Raum und ihre Unabhängigkeit von Unternehmen aus dem außereuropäischen Ausland gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die durch die ZITiS bereitgestellten Dienstleistungen und Eigenentwicklungen werden durch die Sicherheitsbehörden des Bundes in Anspruch genommen.
- Die Abhängigkeit der Sicherheitsbehörden von außereuropäischen Produkten und Lösungen ist gesunken.
- Die Verfügbarkeit hochspezialisierter Expertinnen und Experten in den Kernthemen ist gestiegen.
- Es wurden ausreichende eigene Fähigkeiten hinsichtlich der Eigenentwicklung kritischer oder risikobehafteter Systeme und Methoden der Sicherheitsbehörden aufgebaut.
- Die ZITiS verfügt über eine zentrale und in Anspruch genommene Evaluierungskompetenz für Produkte und Systeme, die aus globalen Lieferketten bezogen werden.

8.3.12 Das Cybersicherheitsniveau durch gestärkte Vorfeldaufklärung erhöhen

Warum ist das Ziel relevant?

Cyberangriffe werden unter anderem zur Spionage, politischen Einflussnahme oder Sabotage eingesetzt. Auch Deutschland steht im Fokus nachrichtendienstlicher Gruppierungen, die fortgeschrittene Angriffstechniken verwenden (APT). Darüber hinaus nutzen unter Anderem extremistische und terroristische Akteure – zum Teil als Dienstleistungen im Internet erwerbbare – Cybertechnologien für ihre Zwecke. Angesichts dieser Bedrohungen gilt es, umfassend für diese Gefahren zu sensibilisieren (Prävention), die Akteure, deren Motive und Fähigkeiten zu identifizieren (Aufklärung), konkrete Angriffe oder deren Vorbereitungen zu entdecken (Detektion), durch Information Maßnahmen zur Abwehr zu ermöglichen (Warnung) und die Urheber der Angriffe zu ermitteln (fachliche Attribuierung).

Die Frühwarnfunktion vor Cyberangriffen wird in der Cybersicherheitsarchitektur primär durch die Nachrichtendienste wahrgenommen.

Wo stehen wir?

Der wachsenden Bedeutung der nachrichtendienstlichen Aufklärung von Angreifern wurde durch organisatorische Maßnahmen in den Nachrichtendiensten des Bundes Rechnung getragen. So wurden beispielsweise mit der personellen Stärkung der Cyberabwehr des BfV und der Cyberauswertung im BND Maßnahmen ergriffen, die die Nachrichtendienste in die Lage versetzen, relevante Cyberakteure intensiver betrachten zu können. Durch die Aufstellung einer Referatsgruppe Cyberabschirmung hat sich auch das BAMAD für die Herausforderungen hinsichtlich der Bedrohungen aus dem Cyberraum gegen den Geschäftsbereich des BMVg besser ausgerichtet.

Was wollen wir erreichen?

Um auch zukünftig wesentliche Beiträge für die Bereiche der Prävention, Aufklärung, Detektion Warnung und fachlichen Attribuierung liefern zu können, ist es notwendig, sowohl die technischen als auch die fachlichen Fähigkeiten der Nachrichtendienste des Bundes zu stärken. Ferner achten wir darauf, dass die Nachrichtendienste des Bundes auch zukünftig, gemessen an der jeweiligen Bedrohungslage, über ausreichende gesetzliche Befugnisse zur Erfüllung ihres jeweiligen gesetzlichen Auftrags verfügen. Die technischen Analysefähigkeiten sollen durch regelmäßige Evaluierung und Anpassung von Analysetools, -umgebungen und Datenhaltungssystemen auf dem erforderlichen Stand gehalten und jeweils durch eine angemessene personelle Ausstattung hinterlegt werden.

Der notwendige Austausch mit anderen Nachrichtendiensten, Sicherheitsbehörden und sonstigen Stellen (einschließlich Wirtschaft) wird weiter verbessert mit dem Ziel, die dafür eingesetzten Ressourcen effektiver zu nutzen sowie die Cyberabwehr zu verbessern und der aktuellen Gefährdungslage anzupassen.

Welche Wirkung erwarten wir?

Durch eine effiziente und der Gefährdungslage angepasste Auftragsumsetzung der Nachrichtendienste des Bundes können Gefahren frühzeitig identifiziert, Risiken minimiert und das Entdeckungsrisiko der Urheber erhöht werden. Dadurch wird erreicht, dass die durch die Digitalisierung erhöhte Angriffsfläche durch weit im Vorfeld eines Cyberangriffs stattfindende Maßnahmen wieder reduziert wird und sich das nationale Cybersicherheitsniveau in Summe erhöht.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Nachrichtendienste des Bundes verfügen gemessen an der Bedrohungslage über ausreichende gesetzliche Befugnisse zur Wahrnehmung ihrer gesetzlichen Aufgaben.
- Erforderliche technische und personelle Voraussetzungen für die angemessene und effiziente Aufklärung und Abwehr von Cyberangriffen sind ausgebaut.
- Die verbesserte Früherkennung und Aufklärung von Cyberangriffen hat zur Erhöhung gegebener Warnhinweise zur Gefahrenabwehr, zur nachhaltigen Unterstützung der Präventionsarbeit sowie zur politischen Attribuierung von Cyberakteuren ausländischer Provenienz beigetragen.

8.3.13 Verteidigungsaspekte der Cybersicherheit stärken

Warum ist das Ziel relevant?

Cyberverteidigung ist als militärischer Teil der Gesamtverteidigung verfassungsmäßiger Auftrag der Bundeswehr und unterliegt den für Einsätze der Bundeswehr geltenden nationalen wie völkerrechtlichen Regelungen. Verteidigungsaspekte der gesamtstaatlichen Cybersicherheit sind gemäß Weißbuch 2016 originäre Aufgaben des BMVg und der Bundeswehr. Die Verteidigungsfähigkeiten der Bundeswehr im Cyberraum sind dabei auch wesentlicher Teil der Cybersicherheitsarchitektur. Im Spannungs- und Verteidigungsfall sind Cyberabwehr, Cyberaußen- und -Sicherheitspolitik sowie Cyberverteidigung sich ergänzende und etablierte Mittel, um die Risiken, die für Deutschland aus dem Cyberraum erwachsen, auf ein tragbares Maß zu reduzieren. Aufgrund der Charakteristika des Cyberraums und dessen hoher Dynamik gilt es, diese Mittel stets der Entwicklung anzupassen und geeignet weiterzuentwickeln. Dabei ist ein ressortübergreifender Ansatz zur Verteidigung im Cyberraum erforderlich.

Die Bundeswehr ist als hoch technisierte Armee im weltweiten Einsatz den Gefahren des Cyberraums fortlaufend ausgesetzt; gleichzeitig ist die Nutzung des Cyberraums Voraussetzung für die Einsatz- und Durchsetzungsfähigkeit der Streitkräfte.

Wo stehen wir?

Verantwortlichkeiten bei den Themen Cyber und IT sind an zentraler Stelle zusammengelegt und werden durch die Abteilung Cyber/Informationstechnik im BMVg sowie den Militärischen Organisationsbereich Cyber- und Informationsraum wahrgenommen; Cyberoperationsführung obliegt der Abteilung Strategie und Einsatz im BMVg. Neben der Zusammenführung bisher verteilter Fähigkeiten wurden neue Fähigkeiten aufgebaut.

Bereits außerhalb des Verteidigungs- oder Spannungsfalles sowie bei Einsätzen schirmt der MAD die Bundeswehr gegen Spionage und Sabotage sowie Extremismus und Terrorismus im Cyberraum ab. Als Nachrichtendienst im Geschäftsbereich des BMVg verfügt er über entsprechende gesetzliche Befugnisse und trägt so zur Auftragserfüllung der Streitkräfte bei.

Die Konzeption der Cyberverteidigung wird fortlaufend weiterentwickelt und an sich verändernde Gegebenheiten und Herausforderungen angepasst.

Was wollen wir erreichen?

Es gilt, die Wirksamkeit der Strukturen und Fähigkeiten vor dem Hintergrund des sich kontinuierlich und schnell weiterentwickelnden Cyberraumes hinsichtlich der Zielerreichung einer Reduzierung der Risiken im Cyberraum auf ein tragbares Maß zu überprüfen und gegebenenfalls anzupassen. Die Kernfähigkeiten im Cyber- und Informationsraum sind erhalten und ausgebaut. Systeme für die Sicherstellung der Kernführungsfähigkeit und die Erhöhung der Resilienz von Waffen- und Wirksystemen sind als kritische IT-Komponenten identifiziert. Sie sind zielgerichtet als vertrauenswürdige Systeme aufgebaut beziehungsweise durch solche ersetzt.

Die zur Erreichung dieser Ziele erforderlichen IT-Services sind priorisiert aufgebaut beziehungsweise erhalten.

Innerhalb der Bundesregierung ist ein Konzept für die Aufgabenwahrnehmung im Rahmen der Verteidigung im Cyberraum im Spannungs- und Verteidigungsfall ebenso wie in konventionellen Bereichen abgestimmt und wird regelmäßig beübt.

Weiterhin werden die Verteidigungsaspekte der Cybersicherheit im Rahmen der Landes- und Bündnisverteidigung sowie weitere Möglichkeiten der Reaktion auf Bedrohungen im Cyber- und Informationsraum unter Berücksichtigung rechtlicher Fragestellungen und mit dem Ziel der Konkretisierung untersucht.

Welche Wirkung erwarten wir?

Die Cyberverteidigung ist wirksam und passt sich den dynamischen Änderungen im Cyber- und Informationsraum kontinuierlich an.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es existiert ein abgestimmtes Konzept zur Verteidigung im Cyberraum im Spannungs- und Verteidigungsfall, das regelmäßig beübt wird.
- Die Netze und Systeme der Bundeswehr sind so geschützt, dass es durch Cyberangriffe keine wesentlichen Einschränkungen in der Verfügbarkeit gibt.
- Die Bundeswehr ist darauf eingestellt, verfügbare Ressourcen, insbesondere zur Incident Response, gemäß den rechtlichen Vorgaben für Amtshilfe zur Verfügung zu stellen. Dabei werden zum Beispiel im Bereich der Incident Response Teams regelmäßig Übungen durchgeführt.

8.3.14 Das Telekommunikations- und Telemedienrecht und die Fachgesetze an den technologischen Fortschritt anpassen

Warum ist das Ziel relevant?

Die gesetzlichen Befugnisse für die Aufgabenwahrnehmung der Sicherheitsbehörden in den verschiedenen Fachgesetzen und das Telekommunikationsgesetz müssen mit den technologischen Entwicklungen Schritt halten und entsprechend kontinuierlich angepasst werden. Die rasante Entwicklung bei Vernetzung und Kommunikation der Zukunft führt zu erheblichen Veränderungen, insbesondere in den Bereichen mobile Kommunikation, IoT und Automotive IT. Mit der Einführung der 5. Mobilfunkgeneration (5G) steht beispielsweise eine technologische Evolution mit disruptivem Charakter bevor. Die Anzahl der mobil vernetzten Geräte wird erheblich zunehmen, hierzu gehören beispielsweise Drohnen, Roboter, Kommunikations-Endgeräte, smarte Brillen, holographische Displays und vielfältige Sensoren, die jede Art von Alltagsgegenstand digitalisieren.

Diese Entwicklung wird durch fünf Megatrends gefördert, die vor allem die Anforderungen an das Mobilfunknetz der 6. Generation (6G) maßgeblich bestimmen werden:

- Vernetzte Maschinen,
- Mensch-Maschine-Kommunikation,
- Künstliche Intelligenz,
- Öffnung der mobilen Kommunikation durch Einführung offener, standardisierter Schnittstellen zwischen relevanten Netzkomponenten (Open RAN) und
- Nutzung der Mobilfunknetze zur Begegnung sozialer, politischer und gesellschaftlicher Herausforderungen.

Die Vielfalt der verfügbaren Dienste und damit einhergehender neuer Geschäftsmodelle werden weiter erheblich zunehmen. Somit eröffnen die bestehenden und insbesondere die neuen Kommunikationsdienste aber auch vielfältige Möglichkeiten zum Missbrauch dieser Technologien, zum Beispiel in den Phänomenbereichen um Cyberkriminalität, Extremismus oder internationaler Terrorismus beziehungsweise Hass und Hetze im Netz.

Wo stehen wir?

Die Sicherheitsbehörden stehen vor enormen technologischen und methodischen Herausforderungen, um sich an die sich rasant ändernden Gegebenheiten der digitalen Welt anzupassen. Bei der Kommunikation von Straftätern gewinnen zum Beispiel Messengerdienste, die speziell zur Vorbereitung von Straftaten entwickelt werden, sowie gehärtete Mobilfunkgeräte und Chatfunktionen bei Onlinespielen immer mehr an Bedeutung. Die im Jahr 2021 erfolgte umfassende Novellierung des Telekommunikationsgesetzes begegnet diesen Entwicklungen bereits mit gesetzlichen Anpassungen. Jedoch gilt es, fortwährend mit den technologischen Entwicklungen Schritt zu halten. Insofern werden auch nach abgeschlossener Telekommunikationsgesetz-Novelle Regelungsnotwendigkeiten im Telekommunikations- und Telemedienrecht und in den Fachgesetzen geprüft, damit die Sicherheitsbehörden auch in der digitalen Welt ihre Aufgaben wahrnehmen können und gleichzeitig Grundrechte möglichst effektiv schützen. Hierbei muss stets abgewogen werden zwischen den Anforderungen an eine effektive und technisch zeitgemäße Arbeit der Sicherheitsbehörden einerseits und dem Schutz hiervon betroffener Freiheitsrechte andererseits.

Was wollen wir erreichen?

Die gesetzlichen Befugnisse der Sicherheitsbehörden im Telekommunikations- und Telemedienrecht und den Fachgesetzen müssen regelmäßig an die stetigen Veränderungen bei Vernetzung und Kommunikation der Zukunft, insbesondere in den Bereichen mobile Kommunikation, IoT und Automotive IT, angepasst werden, damit keine Lücken in der Gefahrenabwehr und Strafverfolgung entstehen. Die TKÜ als zentrales Aufklärungs-, Ermittlungs- und Fahndungsinstrument der Sicherheitsbehörden des Bundes und der Länder hat eine herausgehobene Bedeutung in allen Phänomenbereichen (speziell in den Bereichen Organisierter Kriminalität und Terrorismus).

Für die Sicherheitsbehörden ist es deshalb von hoher Bedeutung, dieses Instrument auch angesichts der technischen Weiterentwicklung zu erhalten. Durch die Einführung neuer Dienste und Geschäftsmodelle dürfen die Fähigkeiten der Sicherheitsbehörden zur Kriminalitätsbekämpfung und zum Schutz der Bevölkerung vor schweren Straftaten einschließlich des Terrorismus nicht infrage gestellt werden.

Welche Wirkung erwarten wir?

Die Befugnisse der Sicherheitsbehörden in ihren jeweiligen weiteren Fachgesetzen, die mit entsprechenden Erlaubnissen im Telekommunikations- und Telemedienrecht korrespondieren müssen, müssen ihnen gestatten, ihre Aufgaben uneingeschränkt und dem technischen Fortschritt angepasst wahrzunehmen. Dies wird auch bei der Einführung von 6G zu beachten sein. Diese betrifft im Kern die einschlägigen Regelungen des Telekommunikationsgesetzes, Telemediengesetzes, Telekommunikation-Telemedien-Datenschutzgesetzes, der TKÜ-Verordnung sowie die jeweiligen korrespondierenden Gesetze zur Regelung der präventiven und repressiven Eingriffsbefugnisse der Sicherheitsbehörden wie Strafprozessordnung, Bundeskriminalamtgesetz, Zollfahndungsdienstgesetz, Bundesverfassungsschutzgesetz, Gesetz über den Bundesnachrichtendienst und Bundespolizeigesetz.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es wurde eine Systematik implementiert, die überprüft, ob ausreichende Fähigkeiten zur Wahrnehmung des gesetzlichen Auftrages der Sicherheitsbehörden in der digitalen Welt vorhanden sind.
- Die Erforderlichkeit gesetzlicher Anpassungen wird kontinuierlich geprüft.

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

Die zunehmende transnationale Vernetzung lässt auch die digitalisierte Welt stetig weiter zusammenrücken. Die Zusammenarbeit mit unseren internationalen Partnern in EU und NATO sowie mit weiteren Wertepartnern und die Einbindung nationaler Maßnahmen in europäische und internationale Prozesse sind daher für die Gewährleistung eines hohen Niveaus an Cybersicherheit in Deutschland unverzichtbar. Während diese Einbindung in allen Handlungsfeldern mitbedacht werden muss, adressiert das Handlungsfeld 4 diejenigen Ziele, für die sich Deutschland aktiv in die europäische und internationale Cybersicherheitspolitik einbringt.

Eine besondere Rolle spielt dabei das deutsche Engagement im Rahmen der EU mit folgenden übergeordneten Zielen: ein EU-weiter hoher Cybersicherheitsstandard, gemeinsames Agieren mit den EU-Partnern auf der internationalen Bühne sowie ein vertiefter Austausch bei der polizeilichen und justiziellen Zusammenarbeit unter Berücksichtigung bestehender Unionskompetenzen. Die Cybersicherheitsstrategie 2021 fügt sich insoweit in die Europäische Cybersicherheitsstrategie 2020 ein, um die kollektive Abwehrfähigkeit gegen Cyberbedrohungen in Europa gemeinsam zu stärken.

Im Nordatlantischen Bündnis bringt sich Deutschland bei der Weiterentwicklung der Cyberverteidigungspolitik der NATO ein. Maßgeblich sind dabei der Schutz der Netze und Systeme der NATO sowie die Resilienz der IT-Infrastruktur und Kritischen Infrastrukturen der NATO-Mitgliedstaaten in einem sich verändernden Sicherheitsumfeld.

Ebenso verfolgt Deutschland das Ziel, das internationale Regelwerk für Staaten im Cyberraum zu stärken. Die Bundesregierung beteiligt sich an Resolutionen sowie Erklärungen und bringt sich aktiv in internationale Diskussionen, insbesondere in den Vereinten Nationen (VN), ein, um diesen Prozess voranzubringen. Mit Hilfe internationaler Austauschplattformen und vertrauensbildender Maßnahmen, insbesondere im Rahmen der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), will Deutschland ein gegenseitiges Verständnis mit anderen Staaten in Bezug auf Cyberbedrohungen fördern. Durch eine Ausweitung der Unterstützung für den Aufbau von Cyberfähigkeiten in anderen Staaten leistet Deutschland ferner einen Beitrag zur Steigerung der globalen Cybersicherheit.

Gemeinsam mit internationalen Partnern, die unsere Werte teilen, setzt sich Deutschland für ein freies, offenes, sicheres und globales Internet ein. Hierzu wird auf nationaler und internationaler Ebene auch ein regelmäßiger Dialog mit Vertretern aus Zivilgesellschaft, Wissenschaft und Wirtschaft angestrebt.

Mit den folgenden strategischen Zielen wollen wir, die Bundesregierung, diese Aufgaben angehen.

8.4.1 Eine wirksame europäische Cybersicherheitspolitik aktiv gestalten

Warum ist das Ziel relevant?

Die rasant fortschreitende digitale Transformation sowie die zunehmende Vernetzung innerhalb der EU verdeutlichen den Bedarf, bei der Cybersicherheit europäische Lösungen zu finden. Deutschland versteht Cybersicherheit als eine zentrale Gestaltungsaufgabe für die EU (im Rahmen ihrer Kompetenzen) und setzt sich gemeinsam mit den EU-Partnern für eine leistungsfähige Cybersicherheitsarchitektur und einen verbesserten Informationsaustausch im EU-Kreis ein. Erforderlich sind die Fortentwicklung einer gemeinsamen Vision und Strategie im Bereich der Cybersicherheit sowie deren bedarfsbezogene Aktualisierung. Durch Mindeststandards in den Bereichen Prävention, Detektion und Reaktion kann europäische Cybersicherheitspolitik das Cybersicherheitsniveau in der gesamten EU verbessern.

Wo stehen wir?

Wir begreifen Cybersicherheit als Standortvorteil für die europäische Industrie. Sie soll Leitanbieter für sichere IT-Lösungen sein und so die Lebensqualität für die Bürgerinnen und Bürger stärken. Deutschland ist darüber hinaus treibende Kraft in den EU-Gremien im Sinne einer mitgliedstaatenübergreifenden Reaktionsfähigkeit und gesamtheitlichen Positionierung der EU nach außen und fördert ein gemeinsames Auftreten der EU in internationalen Gremien.

Zusammen mit ihren Mitgliedstaaten kann die EU mit der sogenannten „Cyber Diplomacy Toolbox“ in koordinierter Weise auf schädigende Cyberaktivitäten aus dem Ausland reagieren. Im Jahr 2020 verhängte der Rat der Europäischen Union erstmals restriktive Maßnahmen gegen Personen und Einrichtungen aus dem Ausland, die für verschiedene Cyberangriffe gegen EU-Mitgliedstaaten verantwortlich oder daran beteiligt waren.

Was ist die „Cyber Diplomacy Toolbox“?

Im Juni 2017 nahm der Rat der Europäischen Union die Schlussfolgerungen zum Rahmen für eine gemeinsame diplomatische Reaktion der EU auf schädigende Cyberaktivitäten an. Das Dokument gibt – wie eine Art Werkzeugkasten – der EU und ihren Mitgliedstaaten Instrumente an die Hand, um angemessen und entschlossen auf schädigende Cyberaktivitäten mit einem breiten Spektrum an diplomatischen, politischen und wirtschaftlichen Maßnahmen reagieren zu können. Die Toolbox enthält vorbeugende, kooperative, stabilisierende und restriktive Maßnahmen (Sanktionen) und mögliche Unterstützung der EU für die rechtmäßigen Reaktionen der Mitgliedstaaten.

Die Cyber Diplomacy Toolbox ist abrufbar unter https://www.consilium.europa.eu/de/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

Außerdem wurde im Jahr 2019 auf EU-Ebene der Cybersecurity Act verabschiedet, der ein neues Mandat für die Europäische Cybersicherheitsagentur ENISA definiert und einen gemeinsamen Zertifizierungsrahmen in der EU einführt.

Seit Anfang 2021 wird eine Überarbeitung der Netzwerk- und Informationssicherheitsrichtlinie im Rat und im Europäischem Parlament verhandelt, die sogenannte NIS-Richtlinie 2.0. Deutschland bringt sich in den Prozess aktiv und gestaltend ein.

Was wollen wir erreichen?

Deutschland wirkt auf eine aktive Positionierung der EU zusammen mit ihren Mitgliedstaaten in der internationalen Cybersicherheitspolitik sowie die kontinuierliche Weiterentwicklung des cyberaußenpolitischen Instrumentariums der EU hin, um die Handlungsfähigkeit der Union im Angesicht von Bedrohungen im Cyberraum weiter zu verbessern.

Deutschland bringt sich aktiv bei der gemeinsamen Vision und Strategie der EU für Cybersicherheit und europäische Digitale Souveränität ein und entwickelt diese kontinuierlich fort. Hierzu zählen insbesondere die in der EU-Cybersicherheitsstrategie identifizierten drei Handlungsbereiche Resilienz, technologische Souveränität und Führungsrolle, Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion sowie Förderung eines globalen offenen Cyberraums.

Deutschland unterstützt eine verstärkte Kooperation zwischen den EU-Mitgliedstaaten untereinander im Rahmen der rechtlichen Möglichkeiten und macht sich für eine vertiefte Zusammenarbeit auf EU-Ebene stark. Ziel ist es, innerhalb der EU noch stärker voneinander zu lernen und sich in Krisensituationen eng abzustimmen.

Die europäische und internationale operative Zusammenarbeit (wie etwa im Rahmen des EU-CSIRTs-Netzwerkes sowie CyCLO-Netzwerkes) ist als wichtiger Baustein einer wirksamen Cyberabwehr weiterentwickelt. Einzelnen Austauschforen sind jeweils klare Zuständigkeiten zugewiesen und Informations- und Abstimmungswege zwischen den Akteuren stringent gehalten.

Nationale Standards und Best-Practice-Ansätze der Cybersicherheit fließen aktiv in europäische Vorhaben und EU-Regulierungen ein.

Welche Wirkung erwarten wir?

Mit einer gemeinsamen Vision in der EU wird ein notwendiger Orientierungsrahmen geschaffen, der eine Richtung und Orientierung im Bereich Cybersicherheitspolitik vorgibt. Die gemeinsame Vision soll auch dabei helfen, dass alle EU-Mitgliedstaaten vereinbarte Mindeststandards einführen und umsetzen. Somit wird gewährleistet, dass einheitliche, anerkannte und abgestimmte Verfahren eingesetzt werden.

Durch die enge Zusammenarbeit mit der EU beziehungsweise mit den einzelnen Mitgliedstaaten wird der Informationsaustausch auf EU-Ebene verbessert. Die Mitgliedstaaten der EU haben zu allen wichtigen Themen der Cybersicherheitspolitik eine Position und vertreten diese aktiv. Durch den kontinuierlichen Austausch lernen die einzelnen EU-Mitgliedstaaten stärker voneinander. Bei anfallenden Krisensituationen kann somit eine enge Abstimmung erfolgen.

Ein gemeinsames Auftreten der EU-Mitgliedstaaten führt zu einer besseren Wirksamkeit und Stärkung in allen Bereichen der EU, aber auch beim Einbringen europäischer Positionen in internationale Verhandlungen. Botschaften werden durch ein EU-koordiniertes Auftreten verstärkt, der eigene Einfluss auf der Weltbühne gesteigert.

Durch eine gemeinsame Vision, abgestimmte Standards, verbesserten Informationsaustausch, Wissenstransfer, transnationale Vernetzung, klare Rechtsrahmen und größere Resilienz wird erwartet, dass das europäische und deutsche Cybersicherheitsniveau erhöht und vereinheitlicht wird sowie Ressourcen effektiver eingesetzt werden.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Grundlagen der europäischen Cybersicherheitspolitik werden kontinuierlich und gegebenenfalls anlassbezogen weiterentwickelt.
- Die NIS-Richtlinie wird überarbeitet und diese neue NIS-Richtlinie 2.0 in nationales Recht umgesetzt.
- Die strategischen Initiativen der EU-Cybersicherheitsstrategie 2020 werden gemeinsam mit unseren europäischen Partnern geprüft, konkret ausgestaltet und umgesetzt.
- In Abstimmung mit ihren europäischen Partnern reagiert die Bundesregierung angemessen auf Cybervorfälle[46].
- Die „Cyber Diplomacy Toolbox“ kommt unter Berücksichtigung etablierter Reaktionsmechanismen zur Anwendung und wird kontinuierlich überprüft und gegebenenfalls anlassbezogen weiterentwickelt.

8.4.2 Cybersicherheit und -verteidigung in der NATO mitgestalten

Warum ist das Ziel relevant?

Die NATO ist eine unverzichtbare Grundlage deutscher und euroatlantischer Sicherheit. Die NATO verbindet ihre Mitgliedstaaten in einer gleichermaßen politischen wie militärischen Organisation und bürgt seit über 70 Jahren für deren Souveränität, sicherheitspolitische Stabilität und territoriale Unversehrtheit. Zur Erfüllung ihrer Kernaufgaben ist die NATO auch auf einen ausreichenden Schutz vor Angriffen im und durch den Cyberraum angewiesen. Die Schwerpunkte der NATO in der Dimension Cyber liegen daher auf dem Schutz der NATO-eigenen Netze, der Stärkung der Resilienz der Mitgliedstaaten beim Schutz gegen Cyberbedrohungen sowie der Fähigkeit der Allianz zur Abschreckung und Verteidigung sowie anderer Reaktion auf Cyberbedrohungen.

Wo stehen wir?

Beim NATO-Gipfel 2016 verabschiedeten die NATO-Mitgliedstaaten mit dem „Cyber Defense Pledge“[47] eine politische Selbstverpflichtung zur Steigerung der Resilienz ihrer Netze und Infrastrukturen sowie zur schnellen und effektiven Reaktion auf Cyberangriffe. Zeitgleich wurde der Cyberraum als eine Dimension der Operationsführung anerkannt, in der sich die NATO ebenso wirksam verteidigen können muss wie in der Luft, zu Land und zur See. Beim NATO-Gipfel 2021 wurde eine neue Cyber-Verteidigungspolitik angenommen, die einen überarbeiteten Rahmen für Cyberverteidigung und Resilienzsteigerung in der NATO schafft.

---

[46] Die Attribuierung von Cyberangriffen bleibt weiterhin eine Kompetenz der Mitgliedstaaten. Darauf aufbauend besteht die Möglichkeit einer koordinierten oder gemeinsamen Attribuierung.

[47] Abrufbar unter: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

„Cyber Defense Pledge“

Im Juli 2016 bekräftigten die Staats- und Regierungschefs der NATO, im „Cyber Defense Pledge“ die nationalen Cybersicherheitsmaßnahmen zum Schutz von Netzen und Infrastrukturen zu stärken.

Neben einer Stärkung der nationalen Cybersicherheit sieht der Pledge eine Vertiefung der EU-NATO-Kooperation im Bereich Cybersicherheit, eine Verbesserung der Kooperation im Bereich der Cyberverteidigung und einen jährlichen Überprüfungsmechanismus vor.

Was wollen wir erreichen?

Die Cyberverteidigungspolitik der NATO als Eckpfeiler der nationalen und euroatlantischen Sicherheit ist weiterentwickelt und an ein sich veränderndes Sicherheitsumfeld angepasst.

Die Netze und Systeme der NATO sind durch ein hohes Maß an Cybersicherheit und Resilienz gegen Cyberangriffe geschützt.

Die NATO leistet einen wichtigen Beitrag zur Steigerung der Resilienz der NATO-Mitgliedstaaten durch die Umsetzung des „Cyber Defense Pledge“.

Die NATO bietet ein Forum für Austausch und Konsultationen zur Cybersicherheit und zur Reaktion auf bösartiges Verhalten im Cyberraum.

Durch die Weiterentwicklung des Cyberraums als Dimension der Operationsführung – im Rahmen des defensiven Mandats der NATO und im Einklang mit dem Völkerrecht – kann sich die NATO im Cyberraum genauso effektiv verteidigen und Operationen führen wie in den anderen Dimensionen. Hierfür hat Deutschland seine Bereitschaft angezeigt, die NATO in mandatierten Operationen und Missionen mit Cyberoperationen zur Erzielung militärischer Effekte zu unterstützen.

Die EU-NATO-Zusammenarbeit bei der Cyberverteidigung und -resilienz ist weiter gestärkt und es ist auf eine bessere Abstimmung bei der Reaktion auf Cyberbedrohungen hingewirkt, um deren Wirksamkeit zu erhöhen.

Deutschland unterstützt weiterhin die NATO mit nationalem Sachverstand bei der zukunftssicheren Ausgestaltung der Cyberverteidigungspolitik im Rahmen des Mandates der Allianz. Die Balance zwischen bündnisgemeinsamem Handeln und den souveränen Aufgaben der Mitgliedstaaten sowie zwischen den zivilen und militärischen Aspekten von Cybersicherheit wird gewahrt.

Welche Wirkung erwarten wir?

Es wird eine Stärkung der Cybersicherheit der NATO und der NATO-Mitgliedstaaten, eine Verbesserung der Handlungsfähigkeit der NATO bei Operationen des Krisenmanagements und eine Erhöhung der Verteidigungsfähigkeit der NATO erwartet.

Die Aufgaben der nationalen und bündnisgemeinsamen Verteidigung sowie für internationales Krisenmanagement und Stabilisierung können erfüllt werden.

Mit der Umsetzung des NATO „Cyber Defence Pledge“ werden die Cyberabwehr und Cyberverteidigung verstärkt. Im Verbund mit seinen Partnern bleibt Deutschland handlungsfähig.

Durch eine intensive EU-NATO-Zusammenarbeit werden der Informationsaustausch und die Abstimmung von Reaktionen auf schädigendes Verhalten aus dem Ausland verbessert.

Deutschland und die NATO bieten so insgesamt weniger Angriffsfläche für Cyberangriffe.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Grundlagen der NATO-Cyberverteidigungspolitik werden kontinuierlich überprüft und anlassbezogen weiterentwickelt.
- Es sind Verfahren etabliert, mit denen die NATO im Bedarfsfall in angemessenem Umfang mit nationalen Cyberfähigkeiten unterstützt werden kann.

- Die nationale Umsetzung entlang der Ziele des NATO „Cyber Defense Pledge“ wird fortgesetzt und vorangetrieben.
- Die EU-NATO-Kooperation im Bereich der Cybersicherheit und Cyberverteidigungspolitik wird gestärkt.

8.4.3 Völkerrecht und den normativen Rahmen für den Cyberraum stärken und auf verantwortliches Staatenverhalten hinwirken

Warum ist das Ziel relevant?

Cybersicherheit kann nicht einseitig auf nationaler Ebene erreicht werden, sondern muss durch entsprechende Aktivitäten auf internationaler Ebene flankiert werden. Jeder Versuch, den Cyberraum im Alleingang, also ausschließlich auf nationaler Ebene zu regeln, ist angesichts der umfassenden grenzüberschreitenden Interdependenzen nationaler Cybersysteme zum Scheitern verurteilt. Cybersicherheit kann nur durch die enge Zusammenarbeit zwischen Staaten und internationalen Organisationen, Zivilgesellschaft, Wirtschaft und Wissenschaft gewährleistet und gestärkt werden. Für dieses Ziel kommt dem Völkerrecht eine wesentliche Bedeutung zu; dementsprechend bildet die regelbasierte internationale Ordnung auch generell einen Grundpfeiler deutscher Außenpolitik. Daneben können freiwillige Selbstverpflichtungen für verantwortliches Staatenverhalten diesen völkerrechtlichen Rahmen ergänzen und weiter konkretisieren. Deutschland setzt sich daher weltweit dafür ein, das Völkerrecht, dessen Institutionen und auch freiwillige Verpflichtungen im Bereich der Cybersicherheit zu stärken und weiterzuentwickeln. Internationale Normenbildung ist für Vertrauen und Sicherheit im Cyberraum von zentraler Bedeutung.

Wo stehen wir?

Der Großteil der Staatengemeinschaft erkennt an, dass das Völkerrecht im Cyberraum Anwendung findet. In Diskussionen auf Ebene der VN sowie in Expertenkreisen wird weiter konkretisiert, was dies im Einzelnen bedeutet und wie einzelne Normen und Prinzipien des Völkerrechts, etwa jene der VN-Charta, im Cyberraum konkrete Anwendung finden. Weiter diskutiert wird auch, mit welchen freiwilligen Selbstverpflichtungen für verantwortliches Staatenverhalten der normative Rahmen für den Cyberraum weiter ausgebaut werden kann. Gleichzeitig gibt es immer wieder einzelne Staaten, die die Geltung des Völkerrechts ganz oder teilweise durch Erklärungen und Handlungen in Frage stellen.

Im März 2021 hat die Bundesregierung ein Positionspapier[48] veröffentlicht, das einen Beitrag zu den fortdauernden Diskussionen um die konkreten Anwendungsmodalitäten des Völkerrechts im Cyberraum leistet. Mit dem Papier bekräftigt Deutschland die Geltung und Relevanz des Völkerrechts als des zentralen multilateralen Ordnungsrahmens auch für Cyberoperationen und untermauert sein Bekenntnis zu einer völkerrechtsbasierten Cyberaußenpolitik.

Was wollen wir erreichen?

Der völkerrechtliche Rahmen für den Cyberraum und der Acquis rechtlich nicht bindender Normen für verantwortliches Staatenverhalten werden gestärkt. Deutschland wirkt auf ein international gemeinsames Verständnis zur Anwendung von Völkerrecht im Cyberraum und zu verantwortlichem Staatenverhalten hin. Leitbild der Bundesregierung ist dabei ein freies, offenes, globales und sicheres Internet. Deutschland engagiert sich zu diesen Themen aktiv und stimmt sich zugleich eng mit den EU-Partnern ab. Weiter fördert Deutschland Maßnahmen zur Wahrung internationaler Stabilität im Cyberraum sowie Maßnahmen zum Schutz von Menschenrechten auf nationaler, europäischer und internationaler Ebene.

Welche Wirkung erwarten wir?

Der von den meisten Staaten getragene Konsens, dass das existierende Völkerrecht auch im Cyberraum gilt, wird weiter stabilisiert und ausgebaut. Es wird dafür geworben, dass sich Staaten, die der Geltung des existierenden Völkerrechts beziehungsweise einzelner Völkerrechtsbereiche im Cyberraum bislang zurückhaltend gegenüberstehen, zur umfassenden Geltung des Völkerrechts im Cyberraum bekennen.

Durch eine fortgesetzte Diskussion steigt international das Bewusstsein über den völkerrechtlichen Rahmen sowie über rechtlich nicht bindende Normen für verantwortliches Staatenverhalten im Cyberkontext. Offene Fragen

[48] Abrufbar unter: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

werden identifiziert und auf eine Klärung hingewirkt. Die dadurch verbesserte Rechtssicherheit in Bezug auf die Anwendung des Völkerrechts im Cyberraum ermöglicht es staatlichen, darunter insbesondere auch deutschen, Behörden, unter Beachtung geltender rechtlicher Rahmenbedingungen effektiver auf Cyberbedrohungen zu reagieren.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Bundesregierung beteiligt sich bilateral, multilateral und im Austausch mit der Zivilgesellschaft auf Grundlage des im März 2021 veröffentlichten Positionspapiers an Diskussionen zur Anwendbarkeit des Völkerrechts im Cyberraum sowie zur Implementierung von Selbstverpflichtungen zu verantwortlichem Staatenverhalten.
- Deutschland ist an den relevanten Diskussionen auf VN-Ebene im Kontext der Cybersicherheit beteiligt und vertritt darin aktiv seine Positionen.
- Ein regelmäßiger Dialog auf internationaler und nationaler Ebene mit Gesellschaft, Wissenschaft und Wirtschaft zu Aspekten des normativen Rahmens für den Cyberraum ist etabliert.
- Deutschland beteiligt sich an Resolutionen und Erklärungen zum Thema Menschenrechte online sowie für ein freies, offenes, globales und sicheres Internet.

8.4.4 Vertrauensbildende Maßnahmen fördern

Warum ist das Ziel relevant?

Motivation und Ziele von schadhaftem Cyberverhalten sind häufig ebenso wenig unmittelbar erkennbar wie die Verantwortlichen für einen Cyberangriff. Gleichzeitig ist der Cyberraum international hoch vernetzt. Dadurch entsteht ein erhebliches Potential für Fehlwahrnehmungen und Fehleinschätzungen, die zu Spannungen zwischen Staaten führen können. Vor diesem Hintergrund sind Maßnahmen zur Transparenzsteigerung und Vertrauensbildung wichtig, um Konflikt- und Eskalationsrisiken vorzubeugen.

Wo stehen wir?

Die wichtige Rolle vertrauensbildender Maßnahmen für Sicherheit und Stabilität im Cyberraum wurde 2021 in den VN von allen Staaten anerkannt und bekräftigt. Für Deutschland ist insbesondere die OSZE die relevante regionale Sicherheitsorganisation. Die 57 OSZE-Teilnehmerstaaten haben 2013 und 2016 insgesamt 16 vertrauensbildende Maßnahmen beschlossen, die den Austausch zwischen Staaten fördern, erforderliche Kommunikationskanäle etablieren und Kooperation zu Cybersicherheitsfragen ermöglichen.

Was wollen wir erreichen?

Die Maßnahmen zur internationalen Vertrauensbildung sind gestärkt. Dabei werden bilaterale, regionale und internationale Austauschformate genutzt.

Neben der Weiterentwicklung vertrauensbildender Maßnahmen setzt sich Deutschland für eine Implementierung der vereinbarten Maßnahmen, insbesondere in der OSZE, ein.

Welche Wirkung erwarten wir?

Vertrauensbildenden Maßnahmen kommt sowohl eine präventive als auch eine deeskalierende Rolle zu. Es wird erwartet, dass der regelmäßige Austausch und die internationale Zusammenarbeit bei vertrauensbildenden Maßnahmen das gegenseitige Verständnis zu Bedrohungswahrnehmungen und zu nicht akzeptiertem Verhalten im Cyberraum erhöhen. Im Fall von Konflikten stehen Ansprechpartner zur Verfügung und es kann auf zuvor etablierte, verlässliche Kommunikationskanäle zurückgegriffen werden.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Deutschland informiert in bilateralen, regionalen und internationalen Foren über nationale Bewertungen und Entwicklungen im Cybersicherheitsbereich.
- Deutschland ist an den relevanten Diskussionen zu vertrauensbildenden Maßnahmen im Cybersicherheitsbereich auf internationaler und regionaler Ebene beteiligt und vertritt darin aktiv seine Position, insbesondere zur Anwendbarkeit des Völkerrechts im Cyberraum und zu verantwortlichem Staatenverhalten.
- Deutschland stellt sicher, dass die im Rahmen vertrauensbildender Maßnahmen von Deutschland benannten Ansprechpartnerinnen und -partner und vereinbarten Kommunikationskanäle verlässlich zur Verfügung stehen.

8.4.5 Bilaterale und regionale Unterstützung und Kooperation zum Auf- und Ausbau von Cyberfähigkeiten (Cyber Capacity Building) stärken

Warum ist das Ziel relevant?

Cyber Capacity Building ist angesichts der voranschreitenden digitalen Transformation und der global vernetzten Welt von zentraler Bedeutung. Cyberbedrohungen und -angriffe können bestimmte Staaten und Bevölkerungsgruppen in ihrer wirtschaftlichen, sozialen und politischen Entwicklung stark einschränken oder zurückwerfen. Wo Ressourcen, Infrastruktur und Kapazitäten für Cybersicherheit fehlen, entstehen besondere Bedarfe. Mit dem Auf- und Ausbau von Cyberfähigkeiten in Partnerländern und -regionen können dort Menschenrechte geschützt, Rechtsstaatlichkeit gestärkt und ein nachhaltiges Wirtschaftswachstum gefördert werden. Für die deutsche Entwicklungszusammenarbeit und die Partnerstaaten ist Cyber Capacity Building daher ein wichtiges Instrument, um die Chancen der Digitalisierung zu nutzen und den damit verbundenen Risiken entgegenzuwirken. Insbesondere dort, wo Menschen der Erstzugang zum Cyberraum dank entwicklungspolitischer Maßnahmen ermöglicht wird, müssen die Rahmenbedingungen und Kenntnisse für seine sichere und verlässliche Nutzung unterstützt werden. Hiervon profitiert auch die Cybersicherheit Deutschlands.

Wo stehen wir?

Der Generalsekretär der VN hat im Juni 2020 eine Roadmap zu digitaler Kooperation vorgelegt. Auch in der Cybersicherheitsstrategie der EU wird die Bedeutung von Cyber Capacity Building herausgestellt. Deutschland engagiert sich in bilateralen Projekten sowie darüber hinaus in einzelnen Projekten im multilateralen Rahmen.

Im Rahmen der Entwicklungszusammenarbeit fördert die Bundesregierung bereits eine Vielzahl an digitalen Projekten auf dem afrikanischen Kontinent. Stärkung und Schutz der digitalen Sicherheit ist eine wichtige Zukunftsaufgabe der deutschen Entwicklungszusammenarbeit, da ohne sie das Potenzial des digitalen Wandels nicht (voll) entfaltet werden kann. Cybersicherheit wird daher als Komponente in allen digitalen Projekten der Entwicklungszusammenarbeit mitgedacht.

Was wollen wir erreichen?

Die bilaterale und regionale Zusammenarbeit zum Aufbau von Cyberkapazitäten ist unter Einbeziehung internationaler Partner aus der Politik, Wirtschaft und Zivilgesellschaft weiterentwickelt, um das Potential der Digitalisierung nutzbar zu machen und Vulnerabilitäten zu senken. Cybersicherheit ist in Programmen zur Förderung der Digitalwirtschaft und bei Stabilisierungsmaßnahmen stärker integriert. Das Thema hat international weiter an Bedeutung gewonnen. Die Förderung und Koordinierung nationaler und internationaler Maßnahmen zum Kapazitätsaufbau sind sichergestellt.

Welche Wirkung erwarten wir?

Die bilaterale und multilaterale Zusammenarbeit erhöht die Cybersicherheit in Partnerstaaten nachhaltig. Demokratische und normative Werte und Ideale können weltweit verankert werden. Im Ergebnis vergrößert sich durch Cyber Capacity Building die globale Cybersicherheit insgesamt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Der Cyberkapazitätsaufbau ist in internationalen Gremien als Thema etabliert und wurde in relevanten Policy-Dokumenten verankert.

- Deutschland beteiligt sich an der Durchführung und/oder Unterstützung von Maßnahmen zum Cyberkapazitätsaufbau im nationalen, EU-, NATO- oder internationalen Kontext.

8.4.6 Internationale Zusammenarbeit bei der Strafverfolgung stärken und internationale Cyberkriminalität bekämpfen

Warum ist das Ziel relevant?

Cyberkriminalität ist ein weltweites Phänomen, das nicht an Ländergrenzen haltmacht. Eine effektive Strafverfolgung kann daher oftmals nur im Rahmen international koordinierter Ermittlungsverfahren erfolgen. Durch die Stärkung der internationalen Zusammenarbeit bei der Verfolgung von Cyberkriminalität kann es den zuständigen Stellen gelingen, noch bessere Ermittlungserfolge zu erzielen. Ein höheres Entdeckungsrisiko kann zu einem spürbaren Rückgang von Cyberkriminalität beitragen.

Wo stehen wir?

Die Fallzahlen im Bereich Cyberkriminalität nehmen weiter zu und gehen mit der wachsenden Verlagerung wirtschaftlicher und sozialer Aktivitäten in den digitalen Raum einher. Dies belegen die polizeilichen Fallzahlen sowie zahlreiche Studien und Phänomenanalysen. Darüber hinaus wird ein überdurchschnittlich großes Dunkelfeld vermutet, da nicht alle Angriffe angezeigt werden. Deutschland nimmt bei der Bekämpfung grenzüberschreitender Cyberkriminalität bereits heute eine bedeutende Rolle ein. Diese Rolle gilt es zu sichern und kontinuierlich auszubauen. Als Beispiel für eine erfolgreiche, international koordinierte Maßnahme ist die durch Deutschland initiierte Zerschlagung der Infrastruktur der „Emotet-Schadsoftware“ im Januar 2021 zu nennen.

Bei der internationalen Zusammenarbeit spielt das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität (European Cyber-Crime Centre – EC3) eine multilateral unterstützende Rolle. Das EC3 unterstützt die EU-Mitgliedstaaten bei der Analyse und Auswertung von Cyberkriminalität und koordiniert die grenzübergreifende Strafverfolgung.

Deutschland ist Unterzeichner des Übereinkommens des Europarates über Computerkriminalität („Budapest-Konvention“[49]), das mittlerweile 65 Vertragsstaaten zählt. Der völkerrechtliche Vertrag ist das erste internationale Übereinkommen, das Cyberkriminalität zum Gegenstand hat.

Im April 2018 hat die Europäische Kommission unter der Bezeichnung „E-Evidence“ ein Legislativpaket[50] auf den Weg gebracht, durch das es den EU-Mitgliedstaaten erstmals ermöglicht werden soll, grenzüberschreitend elektronische Beweismittel ohne Rückgriff auf den traditionellen Weg der Rechtshilfe zu erheben. Das Vorhaben wird derzeit auf EU-Ebene verhandelt.

Um die im E-Evidence-Dossier vorgesehenen Instrumente auch im Verhältnis zu den USA einsetzbar zu machen, führt die Europäische Kommission parallel zu den Beratungen auf EU-Ebene Verhandlungen mit dem US-Justizministerium zum Abschluss eines entsprechenden Verwaltungsabkommens.

Was wollen wir erreichen?

Deutschland unterstützt ausländische Strafverfolgungsbehörden mittels der polizeilichen Aufbauhilfe mit dem Ziel, grenzüberschreitender Cyberkriminalität, insbesondere mit ihren Auswirkungen auf Deutschland und Europa, frühzeitig entgegenzuwirken. Die effektive Bekämpfung internationaler Cyberkriminalität ist dadurch gestärkt und Möglichkeiten der grenzüberschreitenden Strafverfolgung sind verbessert.

Deutschland beteiligt sich an international koordinierten Ermittlungsverfahren. Europol und das EC3 übernehmen dabei eine multilateral unterstützende Rolle. Zum deutschen Engagement gehört ebenfalls die Teilnahme an und Ausrichtung von internationalen Erfahrungsaustauschen und Lösungsentwicklungen.

Deutschland wirbt bei Nicht-Vertragsstaaten für die Unterzeichnung der „Budapest-Konvention“ und setzt sich für ihre Umsetzung in nationales Recht ein. Ferner bringt sich Deutschland aktiv bei ihrer Fortentwicklung ein.

---

[49] Abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=treaty-detail&treatynum=185

[50] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52018PC0225

Welche Wirkung erwarten wir?

Durch den Austausch strategischer und operativer Informationen und das gemeinsame Arbeiten mit internationalen Partnern verbessert Deutschland seine Fähigkeiten bei der wirksamen Bekämpfung von Cyberkriminalität.

Durch den generalpräventiven Ansatz wird Deutschland ein weniger attraktives Ziel für Cyberangriffe. Mittels international koordinierter Ermittlungsverfahren und Strafverfolgung wird sichergestellt, dass Kritische Infrastrukturen sowie allgemein staatliche Einrichtungen, Unternehmen und Bürgerinnen und Bürger in Deutschland besser geschützt werden.

Die Möglichkeiten der internationalen Strafverfolgung werden durch eine zunehmende Anzahl an Beitrittsstaaten zur „Budapest-Konvention“ sowie einen zeitnahen Abschluss des E-Evidence-Dossiers gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl und Wertigkeit international koordinierter Auswerte- und Ermittlungsverfahren ist gestiegen.
- Die Anzahl der polizeilichen Aufbauhilfemaßnahmen Deutschlands für ausländische Sicherheitsbehörden ist gestiegen.
- Die Anzahl der Teilnahmen und Ausrichtungen Deutschlands von Konferenzen und Workshops zu den Themen international koordinierte Strafverfolgung und Cyberkriminalität ist gestiegen.
- Die „Budapest-Konvention“ wird durch weitere Staaten ratifiziert.

8.4.7 Gemeinsam in der EU an innovativen Lösungen für eine effektivere Bekämpfung von Kriminalität arbeiten

Warum ist das Ziel relevant?

Zur wirksamen Strafverfolgung von Kriminalität haben Ermittlerinnen und Ermittler hohen Bedarf an technischen Lösungen, die im operativen Bereich möglichst schnell zur Verfügung stehen müssen. Diese Lösungen basieren oft auf neuen und kombinierten Technologien. Ihre Erarbeitung benötigt einen hohen Einsatz an Fachexpertise und technischer Ausrüstung. Diese Ressourcen sind bei den europäischen Strafverfolgungsbehörden nicht gleichmäßig verteilt, der EU-Raum ist aber gleichmäßig von diesen Straftaten und der Notwendigkeit der technischen Unterstützung bei der Aufklärung und Strafverfolgung betroffen.

Die Erarbeitung innovativer Lösungen für eine effektivere internationale Zusammenarbeit der Strafverfolgungsbehörden liegt im gemeinsamen Interesse der EU-Mitgliedstaaten. Neben der tatsächlichen Erarbeitung von Methoden und Tools sind die Koordinierung von Bedarfen sowie der Expertenaustausch zentrale Punkte in diesem Aufgabenfeld.

Wo stehen wir?

Im Rahmen der deutschen EU-Ratspräsidentschaft ist es gelungen, ein Clearing Board auf europäischer Ebene (EuCB) einzurichten. Das Clearing Board, soll die Kommunikation und ad-hoc-Abstimmung zu kurzfristigen Bedarfen an Tools und Methoden zwischen der Arbeitsebene der Sicherheitsbehörden in den Mitgliedstaaten untereinander, auf EU-Ebene sowie mit Europol herstellen und kanalisieren.

Relevante Partner und Nachbarnetzwerke wie die ZITiS, das European Network of Forensic Science Institutes (ENFSI) und das European Network of Law Enforcement Technology Services (ENLETS) sind eingebunden.

Was wollen wir erreichen?

Das EuCB bietet einen tatsächlichen Mehrwert für Ermittler und ist operativ ausgerichtet. Insbesondere soll es:

- operative Bedarfe und Anforderungen für technische Lösungen unter Verwendung emergenter Technologien direkt von Anwendern (das heißt Strafverfolgungsbehörden) identifizieren und bündeln;
- im Europol Innovation Lab projektbezogene Zusammenarbeit von Expertinnen und Experten zu spezifischen, klar umrissenen operativen Fragestellungen mit technischem Bezug initiieren;

- Arbeitsergebnisse des Europol Innovation Lab und seiner Kerngruppen innerhalb der Strafverfolgungsbehörden verbreiten und als Forum für fachlichen Austausch von Experteninnen und Experten und Ermittlerinnen und Ermittlern der EU-Mitgliedstaaten dienen.

Welche Wirkung erwarten wir?

Durch die Zusammenarbeit bei der gemeinsamen Entwicklung innovativer Lösungen und dem Austausch mit europäischen Partnern verbessert Deutschland seine Fähigkeiten bei der wirksamen Bekämpfung von Kriminalität. Auch die europäischen Partner können von der deutschen Expertise profitieren und damit ihre Fähigkeiten bei der Bekämpfung von Kriminalität verbessern.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das EuCB ist eingerichtet.
- Das EuCB hat wertige, europäische Projekte zur wirksameren Bekämpfung von Kriminalität gebündelt, initiiert beziehungsweise koordiniert.
- Zwischen den Mitgliedern des EuCB, des Europol Innovation Labs sowie des EU Innovation Hub findet ein regelmäßiger Erfahrungsaustausch statt.

9 Umsetzung, Berichtswesen, Controlling und Evaluierung der Cybersicherheitsstrategie

Im folgenden Kapitel werden grundlegende Festlegungen zur Ausgestaltung der 7.4 Leitlinie: „Ziele messbar und transparent ausgestalten“ beschrieben. Sie dienen als Rahmen für die Umsetzung der Strategie, das noch einzurichtende Berichtswesen, das neu einzurichtende Strategische Controlling und die systematische Vorbereitung zukünftiger Evaluierungen.

Im Rahmen der Cybersicherheitsstrategie 2021 wird zwischen zwei Ebenen unterschieden:

- Strategische Ebene: Diese umfasst die strategischen Ziele und die Strategie selbst. Sie beinhaltet die Koordination und Einbindung der Ressorts durch das BMI.
- Operative Ebene: Diese umfasst die Maßnahmen unterhalb der strategischen Ziele und die Umsetzung in den Ressorts. Die Verantwortung obliegt den einzelnen Ressorts.

9.1 Umsetzung

Die zuständigen Ressorts verantworten die Umsetzung der Strategie auf operativer Ebene. Das heißt, sie sind gemäß Ressortprinzip für die Operationalisierung verantwortlich. Hierzu definieren die Ressorts Maßnahmen unterhalb der strategischen Zielebene der Strategie, verfolgen eigenverantwortlich deren Umsetzung und verantworten deren Kosten, Aufwände und Effektivität eigenständig.

Die konkrete Operationalisierung erfolgt durch Ressorts oder durch Geschäftsbereichsbehörden. Für das BMI sind die jeweiligen Ressorts die verantwortlichen Ansprechpartner.

Zur Umsetzung werden durch die Strategie keine verbindlichen Vorgaben gemacht. Im Ergebnis sollen die für das Strategische Controlling (siehe Kapitel 9.3 „Controlling“) notwendigen Informationen bereitgestellt werden. Für eine Vereinheitlichung wird das BMI „Best Practices“ zur Verfügung stellen.

Maßnahmen werden der Strategie nachgelagert erhoben und umgesetzt. Sie werden nach abgeschlossener Erhebung in Form eines fortzuschreibenden Maßnahmenkatalogs der Strategie beigefügt. Die Maßnahmen werden den verantwortlichen Ressorts zugeordnet.

Die Maßnahmenplanung kann in der Laufzeit der Strategie durch die Ressorts angepasst werden, beispielsweise um geänderten Rahmenbedingungen Rechnung zu tragen.

Die Umsetzung der Cybersicherheitsstrategie steht unter dem Vorbehalt der Verfügbarkeit entsprechender, im Haushaltsplan veranschlagter Haushaltsmittel.

9.2 Berichtswesen

Die zuständigen Ressorts übermitteln dem BMI eine Zusammenfassung nebst Bewertung des aktuellen Standes der erreichten Ziele anhand der definierten Indikatoren bis 31. März eines Jahres. Zusätzlich werden dem BMI Haushaltsmittel- und Personalbedarf sowie Ausgaben und Personalaufwand für die Cybersicherheitsstrategie 2021 mitgeteilt. Im Sinne eines einheitlichen Vorgehens stellt das BMI Berichtsformate (Templates) zur Verfügung.

Das BMI konsolidiert die Einzelberichte der Ressorts in einem Gesamtbericht über den Umsetzungsstand der Cybersicherheitsstrategie 2021. Das BMI legt acht Wochen nach Erhalt der Einzelberichte einen Entwurf des Gesamtberichtes zur Ressortabstimmung vor.

Das BMI bewertet gemeinsam mit den betroffenen Ressorts auf Basis des Gesamtberichtes den Umsetzungsstand der Cybersicherheitsstrategie 2021 und prüft, ob sich aus Änderungen der Bedrohungslage beziehungsweise geänderter Risikobewertung ein Anpassungsbedarf für die Cybersicherheitsstrategie ergibt. Die Umsetzung soll hinsichtlich Effektivität und Zielerreichung überprüft werden. Anpassungsbedürfnissen ist zunächst durch Änderungen in der Umsetzung Rechnung zu tragen. Einzelne Indikatoren können bei Einvernehmen der Ressorts hinzugefügt werden. Ist eine Änderung der Strategie selbst erforderlich, wird eine Evaluierung angestoßen.

9.3 Controlling

Im Rahmen seiner Koordinierungsrolle führt das BMI ein Controlling auf strategischer Ebene ein, im Folgenden mit Strategischem Controlling bezeichnet.

Das Strategische Controlling wird auf Ressort-Ebene etabliert. Das BMI übernimmt die Koordinierungsfunktion und bindet die betroffenen Ressorts ein. Das Strategische Controlling umfasst eine dauerhafte Überprüfung der

Zielerreichung und eine Risikobewertung. Um das Strategische Controlling möglichst effizient zu gestalten, sollen geeignete und bereits bestehende Erhebungen, Prüfungen und Kennzahlen zum Stand der Cybersicherheit in Bund und Ländern in die Indikatoren der Cybersicherheitsstrategie 2021 einfließen und gegebenenfalls ergänzt und vereinheitlicht werden.

Das BMI erstellt und stimmt mit den Ressorts ein Controlling-Konzept ab. In Folge wird die Koordinierungsfunktion systematisiert und verstetigt.

9.4 Evaluierungen der Cybersicherheitsstrategie 2021

Mit der Cybersicherheitsstrategie 2021 werden grundlegende Prozesse beschrieben und etabliert, die die Cybersicherheitsstrategie und zukünftige Strategien dauerhaft begleiten. Ziel ist es, die Umsetzung, zukünftige Evaluierungen und zukünftige Fortschreibungen systematisch vorzubereiten.

Evaluierungen sollen spätestens nach vier Jahren erfolgen. Evaluierungen sollen derart vorbereitet werden, dass Ziele mit nachvollziehbaren Indikatoren hinterlegt werden, die eine objektive Zielerreichung überprüfbar machen. Die strategischen Ziele sollen SMART (spezifisch, messbar, aktiv beeinflussbar, realistisch und terminiert) definiert sein. Die Indikatoren können auf geeignete Instrumente (Output) oder die zu erzielende Wirkung (Outcome) auf Staat, Wirtschaft und Gesellschaft abstellen. Grundsätzlich stellt eine Wirksamkeitsmessung die höherwertige Evaluierungsmethode dar. Gleichzeitig gilt es, den Aufwand der Evaluierung in einem angemessenen Verhältnis zum Aufwand der Maßnahme selbst und deren Optimierungspotenzial durch eine höherwertige Evaluierungsmethode zu halten.

Aktuelle Empfehlungen, wie zum Beispiel das „National Capabilities Assessment Framework“ der ENISA, werden bei einer Evaluierung berücksichtigt.

Zusätzlich erfolgen in Abhängigkeit der laufenden Legislaturperiode anlassbezogene Evaluierungen oder anlassbezogene Sachstandserhebungen, zum Beispiel bei Prüfungen durch den Bundesrechnungshof.

Insbesondere muss die Zielerreichung anhand definierter Indikatoren gemessen werden können. Für Evaluierungen kann es sinnvoll sein, Akteure außerhalb des Staates, zum Beispiel Hersteller, Dienstleister oder Hochschulen, einzubeziehen. Deshalb sollen hierfür Kommunikationsprozesse zwischen den Ressorts abgestimmt und implementiert werden.

Fortschreibungen sollen unter Berücksichtigung der laufenden Legislaturperiode nach vier bis sechs Jahren vorgenommen werden. Ergeben Evaluierungen bereits vorher wesentlichen Änderungsbedarf, kann eine Fortschreibung vorgezogen werden.

Nach Bewertung der Ergebnisse einer Evaluierung kann eine Fortschreibung der Strategie angestrebt werden. Besteht nur geringer Änderungsbedarf, kann das BMI die Fortschreibung bis zur nächsten Evaluierung aussetzen.

10 Glossar

Vorbemerkung: Die nachfolgenden Begriffsbestimmungen gelten für diese Cybersicherheitsstrategie und sollen deren inhaltliche Klarheit und Schlüssigkeit fördern. Die Gültigkeit von in anderen Zusammenhängen im Bereich Cybersicherheit gefundenen Definitionen bleibt hiervon unberührt.

Begriff	Erläuterung
Anwenderfreundlichkeit	Anwenderfreundlichkeit als Teil der Nutzererfahrung (englisch User Experience) umschreibt das Erlebnis beziehungsweise die Eindrücke einer Nutzerin oder eines Nutzers in der Interaktion mit einem Produkt oder einer Dienstleistung. Ziel des dahinterstehenden Produktdesigns ist es, die Nutzererwartung in die Interaktion zu erfüllen oder zu übertreffen.
Attribuierung	Attribuierung bezeichnet den Vorgang, den Urheber eines Cyberangriffs zu benennen.
Budapest-Konvention	Die „Budapest-Konvention“ ist ein internationales Übereinkommen des Europarates, welches Cyberkriminalität zum Gegenstand hat. Sie beinhaltet (i) die Kriminalisierung von Verhaltensweisen, die von illegalem Zugriff, Daten- und Systemeingriffen bis hin zu computerbezogenem Betrug und Kinderpornografie reichen; (ii) verfahrensrechtliche Instrumente zur Untersuchung von Cyberkriminalität und zur Sicherung elektronischer Beweismittel im Zusammenhang mit jeglicher Straftat; und (iii) eine effiziente internationale Zusammenarbeit. Das Übereinkommen wird durch ein Zusatzprotokoll ergänzt, das die Kriminalisierung von Handlungen rassistischer und fremdenfeindlicher Natur, die mit Hilfe von Computersystemen begangen werden, zum Gegenstand hat. Die Verhandlungen eines zweiten Zusatzprotokolls dauern derzeit noch an. Ziel des zweiten Zusatzprotokolls ist eine verstärkte internationale Zusammenarbeit bei der Sicherung und betreffend den Zugriff auf elektronische Beweismittel im Strafverfahren durch Behörden in anderen Ländern.
Cloud	Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Die im Rahmen von Cloud Computing angebotenen Dienstleistungen umfassen das komplette Spektrum der Informationstechnik und beinhalten Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.
Common Criteria	Mit den Common Criteria for Information Technology Security Evaluation (kurz: Common Criteria) wurde ein internationaler Standard (ISO 15408) für die Bewertung und Zertifizierung der Sicherheit von Computersystemen geschaffen, so dass Komponenten oder Systeme nicht in verschiedenen Ländern mehrfach zertifiziert werden müssen.
Cyberabwehr	Cyberabwehr umfasst alle Maßnahmen mit dem Ziel, den Erfolg von tatsächlichen oder geplanten Cyberangriffen zu verhindern oder abzuschwächen.
Cyberangriff	Ein Cyberangriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyberraum, die zum

Begriff	Erläuterung
	Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen. Ein besonders schwerer und bedeutender Cyberangriff liegt vor, wenn deren potenzielle Auswirkungen geeignet sind, überregionalen oder in seiner Konsequenz weitreichenden Schaden oder eine Störung des staatlichen Handelns zu verursachen. Indikatoren hierfür können die Betroffenheit Kritischer Infrastrukturen oder anderer systemrelevanter Einrichtungen, die Einbettung in hybride Einflussnahmen oder der sich abzeichnende Bedarf eines gesamtstaatlichen Handelns sein.
Cyberkriminelle	Cyberkriminelle sind Akteure, die auf informationstechnischem Wege oder unter Zuhilfenahme von IT kriminelle Handlungen vornehmen (beispielsweise Erpressung).
Cyberraum	Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, das durch beliebige andere Datennetze erweitert werden kann.
Cybersicherheit	Cybersicherheit ist die IT-Sicherheit der im Cyberraum auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme.
Cyberterroristen	Cyberterroristen sind ideologisch motivierte Akteure, die Cyberangriffe nutzen, um Ziele zu beschädigen oder zu zerstören, ihre Ideologie zu verbreiten oder ihren Einfluss auszuweiten.
Cyberverteidigung	Cyberverteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und der vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyberraum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind oder zur Abwehr von (militärischen) Cyberangriffen und damit dem Schutz eigener Informationen, IT, sowie Waffen- und Wirksysteme dienen. Dazu gehören auch die Nutzung und Mitgestaltung von Strukturen, Prozessen und Meldewesen der Cyberabwehr unter verteidigungsrelevanten Aspekten und Situationen.
Datenschutz	Mit Datenschutz wird der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten bezeichnet (nicht zu verwechseln mit Datensicherheit).
Denial of Service	Der englische Fachbegriff Denial of Service (DoS) bedeutet „außer Betrieb setzen“. Technisch wird von einem Angreifer hierbei durch das Absetzen massenhafter Anfragen an ein IT-System dieses zur Überlastung gebracht und so deren Verfügbarkeit ganz oder teilweise eingeschränkt.
Distributed Denial of Service	Bei einem „verteilten“ DoS-Angriff (DDoS) werden von Angreifenden anstelle von einzelnen Systemen eine Vielzahl von IT-Systemen zum Angriff genutzt. Die hohe Anzahl der gleichzeitig angreifenden IT-

Begriff	Erläuterung
	Systeme macht diese Art von Angriffen schwer mitigierbar und damit besonders wirksam.
Desinformation	Desinformation ist gezielt verbreitete falsche oder irreführende Information. Sie ist zu unterscheiden von falscher oder irreführender Information, die ohne Täuschungsabsicht erfolgt.
Detektion	Unter Detektion versteht man das Erkennen von cybersicherheitsrelevanten Ereignissen, wie etwa Indikatoren von Cyberangriffen, in den eigenen IT-Systemen und -Netzen beziehungsweise im Rahmen der Vorfeldaufklärung. Die Angriffserkennung erfolgt beispielsweise durch den Abgleich der verarbeiteten Daten mit Informationen und technischen Mustern, die auf maliziöses Verhalten hindeuten. Moderne Detektion setzt zur Bewältigung hoher Angriffsintensität verstärkt auf technisch gestützte Angriffserkennung, aber auch organisatorische und personelle Maßnahmen spielen weiter eine wichtige Rolle.
Digitale Souveränität	Digitale Souveränität beschreibt die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.
Digitale Wirtschaft	Die digitale Wirtschaft (Digitalwirtschaft) beschreibt den Umbruch, der heutzutage durch die Technologisierung in der Wirtschaft stattfindet. Neben einer angestrebten effizienteren und effektiveren Ausgestaltung bestehender Geschäftsprozesse ermöglicht Digitalisierung vor allem Innovation bei der Erschließung und Entstehung völlig neuer Geschäftsfelder und -modelle.
E-Government	Der englische Begriff E-Government (Elektronische Verwaltung) meint das Dienstleistungsangebot der öffentlichen Verwaltung im Internet, das es den Kundinnen und Kunden der Verwaltung erlauben soll, Behördengänge so weit wie möglich elektronisch abzuwickeln.
Ende-zu-Ende-Verschlüsselung	Die Ende-zu-Ende-Verschlüsselung ist eine durchgängige Verschlüsselung zwischen Absender und Empfänger.
Exploit	Ein Exploit (englisch to exploit: ausnutzen) ist ein Werkzeug oder eine systematische Möglichkeit (auch Beschreibung), um Schwachstellen und Fehlfunktionen von Hard- oder Software auszunutzen, um sich Zugriff auf die Daten oder Ressourcen zu verschaffen.
EU-Cybersecurity Act	Der europäische Rechtsakt zur Cyber-Sicherheit (Cybersecurity Act, CSA) ist am 27. Juni 2019 in Kraft getreten. Kernelemente der Verordnung sind ein permanentes Mandat für die europäische Cyber-Sicherheitsagentur ENISA sowie die Einführung eines einheitlichen europäischen Zertifizierungsrahmens für IKT-Produkte, -Dienstleistungen und -Prozesse.
European Cybercrime Centre	Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (European Cybercrime Centre, EC3) wurde im Jahr 2013 bei Europol eingerichtet, um die Strafverfolgungsmaßnahmen gegen Cyberkriminalität

Begriff	Erläuterung
	in der EU zu stärken und so zum Schutz der europäischen Bürgerinnen und Bürger, Unternehmen und Regierungen vor Online-Kriminalität beizutragen.
Europol	Das Europäische Polizeiamt (Europol) ist eine Agentur der EU, die die Strafverfolgungsbehörden der EU-Mitgliedstaaten bei der Bekämpfung organisierter und schwerer internationaler Kriminalität sowie Terrorismus unterstützt.
Hybride Bedrohung	Die Bundesregierung versteht unter hybriden Bedrohungen verschiedene Formen illegitimer Einflussnahme fremder Staaten, die sich insbesondere gegen die Sicherheitsinteressen oder die souveräne politische Willensbildung der Bundesrepublik Deutschland richten.
Informationssicherheit	Informationssicherheit hat den Schutz von Informationen zum Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein.
Informationstechnik	Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.
IT-Grundschutz	IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von Informationsverbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen umgesetzt sind, die als Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen und Institutionen mit normalem Schutzbedarf hinreichend absichern.
IT-Sicherheit	IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Informationen und IT durch angemessene Maßnahmen geschützt sind.
Kritische Infrastrukturen	Kritische Infrastrukturen (KRITIS) sind Einrichtungen, Anlagen oder Teile davon, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.
Kryptografie	Kryptografie ist die Wissenschaft der Verschlüsselung von Informationen in „Geheimschriften“. Damit soll verhindert werden, dass Dritte Informationen einsehen können, die nicht für sie bestimmt sind.

Begriff	Erläuterung
Nationaler Pakt Cybersicherheit	Mit dem Koalitionsvertrag der aktuellen Legislaturperiode wurde der Nationale Pakt Cybersicherheit ins Leben gerufen. Ziel dieses Paktes ist es, alle gesellschaftlich relevanten Gruppen, Hersteller, Anbieter und Anwendenden sowie die öffentliche Verwaltung in gemeinsamer Verantwortung für digitale Sicherheit in einen Nationalen Pakt einzubinden.
Open RAN	Open RAN ist ein Standardisierungsprojekt, das von privatwirtschaftlichen Initiativen wie der O-RAN Alliance und dem Telecom Infra Project entwickelt und vorangetrieben wird. Beteiligt sind eine Vielzahl von Firmen aus der gesamten Wertschöpfungskette der IKT, wie Netzbetreiber, Komponentenhersteller oder Softwarefirmen, die in den diversen Arbeitsgruppen dieser beiden Organisationen tätig sind. Ziel ist es unter anderem, technische Spezifikationen zu erstellen, die es auch anderen Ausrüstern erlauben beziehungsweise erheblich erleichtern, ihre Produkte einzubringen, um mehr Wettbewerb und offene Schnittstellen zwischen den Komponenten zu ermöglichen. Schwerpunkte liegen beispielsweise in der Entwicklung eines Referenzdesigns für sogenannte White-Box Hardware sowie in der Entwicklung der Software für die einzelnen RAN-Komponenten. Ferner soll mittels Labor- und Feldversuchen sichergestellt werden, dass die Hard- und Softwarekomponenten der verschiedenen Hersteller auch in der Realität interoperabel sind. Als weiteren Schritt strebt die Bundesregierung an, die erstellten Spezifikationen für offene Schnittstellen durch Überführung in eine anerkannte Standardisierungsorganisation (ETSI, European Telecommunications Standards Institute) aufwerten zu lassen.
Patch	Ein Patch ist ein Software-Programm, das unter anderem Programmierfehler oder Schwachstellen in Anwendungs- oder Systemsoftware oder Firmware behebt.
Post Quantenkryptografie	Unter Post-Quanten-Kryptografie versteht man kryptografische Verfahren, von denen angenommen wird, dass sie auch mit Hilfe eines Quantencomputers nicht in realistischer Zeit zu brechen sind. Im Gegensatz zur Quantenkryptografie können diese Verfahren auf klassischer Hardware implementiert werden. Alternativ werden mit der Quantenkryptografie Sicherheitsmechanismen vorgeschlagen, die selbst auf quantenmechanischen Prinzipien basieren. Insgesamt sind Quantenkryptografie und Post-Quanten-Kryptografie auf verschieden Prinzipien beruhende Verfahren, die nicht als Konkurrenten, sondern als gegenseitige Ergänzungen gesehen werden können.
Provider	Provider ist ein Dienstanbieter mit verschiedenen Schwerpunkten, zum Beispiel Netz-Provider, der als Mobilfunkprovider, Internet-Service-Provider oder Carrier die Infrastruktur für den Daten- und Sprachtransport bereitstellt, oder Service Provider, der über die Netzzugangs-Bereitstellung hinausgehende Dienstleistungen erbringt.
Quantencomputing	Quantencomputer sind Rechner, die gezielt quantenmechanische Prinzipien ausnutzen, um damit bestimmte Berechnungen deutlich schneller als mit herkömmlichen Computern ausführen zu können. Diese sogenannte „Quantenüberlegenheit“ (englisch „*Quantum Supremacy*“)

Begriff	Erläuterung
	konnte mittlerweile für einige spezifische Problemstellungen demonstriert werden.
Quantenkommunikation	Quantenkommunikation, insbesondere die Verteilung kryptografischer Schlüssel mithilfe quantenmechanischer Effekte (englisch Quantum Key Distribution, QKD), ist eine Technologie, die eine sichere Datenübertragung auf Basis physikalischer Prinzipien anstelle mathematischer Vermutungen verspricht. QKD benötigt einen zusätzlichen klassischen Kommunikationskanal.
Ransomware	Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch „Ransom“) wieder freigeben.
Schwachstelle	Eine Schwachstelle (englisch Vulnerability) ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution.
UP KRITIS	Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und staatlichen Stellen wie dem BSI.
Update	Ein Update ist eine neue Version beziehungsweise Ergänzung einer Software oder Firmware, die Programm- oder Funktionsmängel korrigiert oder Programm- oder Funktionsverbesserungen enthält.
Verschlüsselung	Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit einer Zusatzinformation, die „Schlüssel“ genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.
Völkerrecht	Das Völkerrecht ist das zentrale Element der regelbasierten internationalen Ordnung. Beim Völkerrecht handelt es sich um eine Rechtsordnung, welche durch die Kooperation souveräner, gleichberechtigter Staaten sowie gegebenenfalls anderer Völkerrechtssubjekte auf Grundlage gegenseitiger Übereinstimmung geschaffen wurde und fortgebildet wird. Anders als bei innerstaatlichen Rechtsordnungen gibt es keinen übergeordneten zentralen Gesetzgeber, der allgemeingültige Rechte und Pflichten schafft, an die sich alle Staaten zu halten haben. Vielmehr geschieht dies durch Selbstbindung, da die Akzeptanz und Geltungskraft des Völkerrechts insgesamt auf ein zwischenstaatliches Konsensprinzip zurückgeführt werden kann. Dementsprechend sind internationale Übereinkünfte (das so genannte Völkervertragsrecht) oder eine Staatenpraxis, die von einer entsprechenden Rechtsüberzeugung getragen wird (das sogenannte Völkergewohnheitsrecht) sowie die von den meisten Staaten innerstaatlich anerkannten Regeln, die auch auf zwischenstaatliche Ebene übertragbar sind (so genannte allgemeine Rechtsgrundsätze), verbindliche Rechtsquellen der Völkerrechtsordnung.

Begriff	Erläuterung
Zentralstelle	Als Zentralstellen ausgestaltete Bundesbehörden erlauben organisatorische Verbindungen verschiedener Bundes- und Landesbehörden zur dauerhaften gegenseitigen Information, Abstimmung und Unterstützung. Dies ermöglicht, den Aufbau von Doppelstrukturen in Bund und Ländern zu vermeiden.
Zero-Day-Schwachstelle	Eine Zero-Day-Schwachstelle ist eine dem Hersteller unbekannte Schwachstelle in informationstechnischen Systemen.
5G beziehungsweise 6G	5G beziehungsweise 6G bezeichnen Netzstandards der fünften beziehungsweise sechsten Mobilfunkgeneration und sind damit direkte Nachfolger von LTE (4G) und UMTS (3G). Die neuen Standards zielen insbesondere auf höhere Datenraten und geringe Latenz, verbesserte Kapazität und ein intelligentes Netz ab. Für Unternehmen eröffnen sich neue Möglichkeiten bei der Digitalisierung. So können 5G-beziehungsweise 6G-Netze beispielsweise den Datenaustausch innerhalb und zwischen Firmen verbessern oder die Anlagensteuerung mittels Maschine-zu-Maschine-Kommunikation revolutionieren. Für Verbraucherinnen und Verbraucher bedeutet die Technik ein in Zukunft deutlich schnelleres mobiles Netz und eine wachsende Zahl vernetzter Gegenstände im alltäglichen Umfeld.

11 Abkürzungsverzeichnis

Abkürzung	Erläuterung
APT	Advanced Persistent Threat
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BDI	Bundesverband der Deutschen Industrie
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern, für Bau und Heimat
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft und Energie
BND	Bundesnachrichtendienst
BPOL	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSOC	Bundes Security Operations Center
CERT	Computer Emergency Response Team
CVD	Coordinated Vulnerability Disclosure
Cyberagentur	Agentur für Innovation in der Cybersicherheit GmbH
Cyber-AZ	Nationales Cyber-Abwehrzentrum
DDoS	Distributed Denial of Service
DsiN	Deutschland sicher im Net
EC3	Europäische Zentrum zur Bekämpfung der Cyberkriminalität (European Cyber-Crime Centre)
eID	Elektronische Identität
ENISA	Agentur der Europäischen Union für Cybersicherheit

Abkürzung	Erläuterung
EU	Europäische Union
EuCB	Clearing Board auf europäischer Ebene
IoT	Internet of Things
IKT	Informations- und Kommunikationstechnik
ISO	International Organization for Standardization
IT	Informationstechnik
KdoCIR	Kommando Cyber- und Informationsraum
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastrukturen
KMU	Kleine und mittlere Unternehmen
MAD	Militärischer Abschirmdienst
MIRT	Mobile Incident Response Team
NATO	North Atlantic Treaty Organization oder Nordatlantisches Bündnis
NCSR	Nationaler Cybersicherheitsrat
NIS-Richtlinie	Europäische Richtlinie zur Netzwerk- und Informationssicherheit
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
OZG	Onlinezugangsgesetz
QKD	Quantum Key Distribution oder Quantenschlüsselaustausch
PKI	Public-Key-Infrastruktur
SOC	Security Operations Center
TISiM	Transferstelle „IT-Sicherheit im Mittelstand“
TKÜ	Telekommunikationsüberwachung
UP Bund	Umsetzungsplan Bund 2017
VCV	Verwaltungs-CERT-Verbund

Abkürzung	Erläuterung
VN	Vereinte Nationen
VPN	Virtual Private Network
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333