Bundesministerium
des Innern
und für Heimat

Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat

Ziele und Maßnahmen für die 20. Legislaturperiode

Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat

Ziele und Maßnahmen für die 20. Legislaturperiode

Inhalt

Einleitung

Im April 2022 hat Bundesinnenministerin Nancy Faeser ihr Programm „Digitalpolitische Ziele und Maßnahmen bis 2025 des Bundesministeriums des Innern und für Heimat“ vorgestellt. In diesem wird skizziert, mit welchen Projekten u. a. aus den Bereichen Digitalisierung der Verwaltung, Datenpolitik und Cybersicherheit sie das Land bis 2025 voranbringen will. Die vorliegende Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat konkretisiert dieses Digitalprogramm im Bereich Cybersicherheit.

Der Krieg in der Ukraine verdeutlicht einmal mehr, wie essenziell Cybersicherheit für einen modernen, hochtechnologisierten und digitalisierten Industriestaat wie Deutschland ist: gezielte Angriffe auf Kritische Infrastrukturen (KRITIS), Aktionen von (auch staatlich gelenkten) Cyberkriminellen, „Kollateralschäden“ durch Angriffe auf mit der hiesigen Wirtschaft verbundene Unternehmen, gezielte Desinformationen oder Angriffe auf bzw. Sabotage von staatlichen Strukturen sind geeignet, die Funktionsfähigkeit unseres Gemeinwesens und unserer Wirtschaft massiv und anhaltend zu beeinträchtigen oder gar zu unterbrechen. Die Stärkung der Cyber-Resilienz von Bundesbehörden, weiteren staatlichen und zivilen Infrastrukturen und insbesondere den Kritischen Infrastrukturen duldet daher ebenso wie die Modernisierung der Cybersicherheitsarchitektur, der Ausbau sicherer Infrastrukturen, der digitale Verbraucherschutz und die Sicherung der Verfügbarkeit von vertrauenswürdiger Technik keinen Aufschub. Die Bürgerinnen und Bürger erwarten von ihrer Regierung zu Recht, dass sie vorausschauend handelt, ein Funktionieren dieser Strukturen sicherstellt und die Gesellschaft vor Gefahren im digitalen Raum schützt. Dazu gehört auch, die Cyberfähigkeiten der Sicherheitsbehörden zu stärken und eigene Entwicklungsfähigkeiten auszubauen. Dies ist unerlässlich, damit unsere Polizeien und Nachrichtendienste ihren gesetzlichen Auftrag souverän erfüllen können.

Wir sorgen deshalb mit den folgenden Maßnahmen für eine effektive und effiziente Aufstellung im Cyberraum und ein höchstmögliches Schutzniveau in der Cybersicherheit.

1. Cybersicherheitsarchitektur modernisieren und harmonisieren

Wir streben eine effizientere und klarere Aufgabenverteilung in der Cybersicherheitsarchitektur an und verzahnen alle Akteure miteinander in sinnvoller Weise. Hierfür untersuchen wir die Wirksamkeit der derzeitigen Aufgabenwahrnehmung aller Akteure und prüfen die Effektivität der aktuellen Zuständigkeitsverteilung und der behördenübergreifenden Zusammenarbeit. Dies gilt sowohl für die Zusammenarbeit der Bundesbehörden miteinander als auch für das Wirken zwischen Bund und Ländern.

Maßnahmen und Ziele in der 20. Legislaturperiode:

- Ausbau des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu einer Zentralstelle im Bund-Länder-Verhältnis
- Anpassung der Zuständigkeitsverteilung im Bereich der Gefahrenabwehr im Cyberraum
- Weiterentwicklung der Cybersicherheitsstrategie für Deutschland 2021
- Fortentwicklung des Nationalen Cyberabwehrzentrums
- Stärkung des Nationalen Cyber-Sicherheitsrates
- Unabhängigere Aufstellung des Bundesamtes für Sicherheit in der Informationstechnik

2. Cyberfähigkeiten und digitale Souveränität der Sicherheitsbehörden stärken

Durch den Ausbau und die Stärkung technischer Ermittlungs- und Analysefähigkeiten und -instrumente bei den Sicherheitsbehörden werden wir dafür sorgen, dass diese mit dem technologischen Wandel im digitalen Raum Schritt halten können und ihre gesetzlichen Aufgaben bei der Gefahrenabwehr und Strafverfolgung weiterhin bedarfsgerecht wahrnehmen. Durch den Ausbau der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) werden die Sicherheitsbehörden mit technischen Lösungen gezielt in ihren Ermittlungs- und Analysefähigkeiten unterstützt und die Abhängigkeit der Sicherheitsbehörden von außereuropäischen Herstellern reduziert. Polizei und Nachrichtendienste profitieren gleichermaßen vom Ausbau eigener nationaler Entwicklungsfähigkeiten und von einer zentralen Bündelung der Investitionen und Entwicklungsfähigkeiten bei ZITiS.

Maßnahmen und Ziele in der 20. Legislaturperiode:

- Erstellen einer umfassenden Digitalisierungsstrategie für das Bundesamt für Verfassungsschutz (BfV)
- Modernisierung der IT-Infrastruktur im BfV
- Fortentwicklung der Cyberfähigkeiten des BfV und deren Nutzbarmachung im Verfassungsschutzverbund, insbesondere Modernisierung von
  - Recherche-Tools zur Aufklärung von Extremismus in sozialen Medien sowie
  - Datenhaltungs- und Analysesystemen bzw. -tools in der Aufklärung und Früherkennung staatlich gesteuerter Cyberangriffe
- Verbesserte Befugnisse zur Aufklärung technischer Sachverhalte bei Cyberangriffen fremder Mächte
- Stärkung und Ausbau der Zentralstellenfunktion des BfV im Verfassungsschutzverbund

- Ausbau und Modernisierung der Ermittlungsfähigkeiten und -instrumente des Bundeskriminalamtes (BKA) und der Bundespolizei im digitalen Raum in den Bereichen Automotive IT, Internet der Dinge und Verschlüsselung sowie bei der polizeilichen Nutzung Künstlicher Intelligenz
- Etablierung eines wirksamen Schwachstellenmanagements, inklusive Installation der behördlichen Prozesse
- Schaffung einer gesetzlichen Grundlage für die ZITiS
- Ausbau der ZITiS als zentraler Dienstleister für die Sicherheitsbehörden sowie Auf- und Ausbau eigener nationaler Entwicklungsfähigkeiten und Bewertungskompetenz bei der ZITiS

3. Cybercrime und strafbare Inhalte im Internet bekämpfen

Kriminalität verlagert sich zunehmend in den digitalen Raum. Die stetig wachsenden Fall- und Schadenszahlen erfordern effektive Maßnahmen für eine erfolgreiche Bekämpfung von Cybercrime. Dies gilt vor allem für das Phänomen der Erpressung durch Ransomware. Darüber hinaus hat es höchste Priorität, Kinder und Jugendliche vor sexueller Gewalt zu schützen. Dazu werden wir uns mit einer nationalen Strategie robust aufstellen und mit gezielten Maßnahmen entschieden gegen Täter, ihre Netzwerke und ihre Verbreitungsstrategien vorgehen. Insbesondere werden wir Prozesse zur konsequenten Meldung, Verfolgung und Löschung von Missbrauchsdarstellungen einrichten. Dabei spielt die partnerschaftliche Zusammenarbeit zwischen der Internetwirtschaft, der Zivilgesellschaft und den Behörden eine herausragende Rolle.

Die Bekämpfung der Hasskriminalität ist ebenfalls ein Schwerpunktthema. Wir dulden nicht, dass Menschen aus Angst vor Bedrohungen und Gewalt ihre Meinung im Netz nicht mehr frei äußern und intensivieren unsere Anstrengungen, sodass Täter zeitnah identifiziert und strafrechtlich verfolgt werden.

Für diese Aufgaben müssen unseren Sicherheitsbehörden im digitalen Raum die besten Fähigkeiten und Werkzeuge zur Verfügung stehen. Diese werden wir konsequent ausbauen und erweitern.

Maßnahmen und Ziele in der 20. Legislaturperiode:

- Weiterer Ausbau der Abteilung Cybercrime beim BKA
- Ausbau der zentralen Kompetenz- und Service-Dienstleistungen des BKA zur Bekämpfung von Cybercrime
- Stärkung der internationalen Zusammenarbeit des BKA im Bereich Cybercrime, u.a. im Rahmen internationaler Counter-Ransomware-Initiativen
- Förderung eines EU-weiten Rechtsrahmens zur Verhinderung und Bekämpfung des sexuellen Missbrauchs von Kindern, dabei insbesondere Verhinderung der Verbreitung von Kindesmissbrauchsdarstellungen im Internet
- Entwicklung einer nationalen Strategie zur Bekämpfung der sexuellen Gewalt gegen Kinder
- Erstellung eines jährlichen Bundeslagebildes „Sexuelle Gewalt gegen Kinder“
- Personelle und technische Stärkung des BKA bei der Bekämpfung der sexuellen Gewalt gegen Kinder
- Erstellung eines zentral durch das BKA koordinierten und bundesweit abgestimmten Melde- und Löschprozesses bei Missbrauchsdarstellungen im Internet
- Intensivere Bekämpfung strafbarer, insbesondere rechtsextremistischer Internetinhalte, u.a. durch Stärkung vorhandener Strukturen beim BKA
- Ausbau der Ermittlungsfähigkeiten der Bundespolizei im Phänomenbereich Cyberkriminalität durch personelle und technische Stärkung
- Konsequenter Ausbau der ZITiS, um digitale Ermittlungswerkzeuge für die Sicherheitsbehörden zur Stärkung der Auswerte- und Analysefähigkeiten im Kampf gegen Cybercrime zu entwickeln

4. Cybersicherheit der Behörden des Bundes stärken

Angesichts der aktuellen Verschärfung der Sicherheitslage in Europa ist eine Neujustierung auch beim Eigenschutz der Behörden des Bundes dringend notwendig. Deutschland steht vor einer kontinuierlich zunehmenden Bedrohungslage im Cyberraum. Der Eigenschutz staatlicher Strukturen ist eine Grundvoraussetzung für die Aufrechterhaltung staatlicher Handlungs- und Arbeitsfähigkeit. Daher ist die Bundesregierung vorrangig gefordert, eine signifikante Erhöhung der Cyber-Resilienz der Behörden des Bundes sicherzustellen. Der Bund muss die Schutzmaßnahmen in seiner IT-Sicherheitsarchitektur unverzüglich an die gesteigerte Bedrohungslage anpassen. Nachstehende Verstärkungsmaßnahmen sind unerlässlich.

Maßnahmen und Ziele in der 20. Legislaturperiode:

- Stärkere gesetzliche Verankerung der Informationssicherheit und Umsetzung eines Verstärkungsprogramms für die Cybersicherheit des Bundes mit der Einrichtung eines Chief Information Security Officers für den Bund (CISO BUND) und eines Kompetenzzentrums zur operativen Sicherheitsberatung des Bundes
- Etablierung des Grundsatzes „security by design and by default“ in der Bundesverwaltung
- Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und -Systemen für sichere Kommunikation sowie Investition in Quantencomputing und Post-Quanten-Kryptografie
- Investition in Quantencomputing beim BSI zur Gewährleistung der sicheren Regierungskommunikation
- Steigerung der Hochverfügbarkeit der Rechenzentren des Bundes
- Weiterentwicklung des Informationssicherheitsmanagements des Bundes

5. Cyber-Resilienz Kritischer Infrastrukturen stärken

Abhängigkeiten der KRITIS-Betreiber von Verfügbarkeiten in den IT-Lieferketten können im Schadens- und Krisenfall schnell von existenzieller Bedeutung sein. Ergänzend zur bereits erforderlichen Prüfung der Vertrauenswürdigkeit von Herstellern soll daher künftig auch die Verfügbarkeit von Ressourcen wie Softwarelizenzen, Clouddiensten und Wartungsdienstleistungen sowie von Ersatzteilen (z. B. Netzwerkkomponenten) besser sichergestellt werden.

Um bei Cybersicherheitsvorfällen schnell handlungsfähig zu sein, sollten KRITIS-Betreiber dicht an das BSI-Lagezentrum angebunden werden. Für jeden KRITIS-Sektor sollte daher ein sektorspezifisches Cyber Emergency Response Team (CERT) von den KRITIS-Betreibern etabliert werden.

Zudem werden wir vom BSI vorab entwickelte „Awareness- und Cyber-Resilienz-Projekte“ für KMU durch Dienstleister der Allianz für Cybersicherheit am Markt anbieten. Kleine und mittlere Unternehmen (KMU) sind vielerorts das Rückgrat der Wertschöpfungskette und auch als Dienstleister für viele KRITIS-Betreiber tätig. Gleichzeitig spielt Cyber-Resilienz für KMU aber oft nur eine untergeordnete Rolle, da die Kernkompetenz im operativen Betrieb liegt oder Cybersicherheitsaspekte generell eher als Kostentreiber gesehen werden.

Maßnahmen und Ziele in der 20. Legislaturperiode:

- Förderung von Investitionen für Cyber-Resilienzmaßnahmen in KMU, die dem KRITIS-Sektor angehören
- Einrichtung von Awareness- und Cyber-Resilienz-Projekten, die vom BSI und von externen Dienstleistern angeboten werden
- Berücksichtigung der Sicherheit von IT-Lieferketten im Rahmen der gesetzlichen KRITIS-Regulierung
- Prüfung der Etablierung sektorspezifischer CERTs für KRITIS-Betreiber und enge Ankopplung an das BSI-Lagezentrum

6. Schutz ziviler Infrastrukturen vor Cyberangriffen

Neben Unternehmen aus dem KRITIS-Bereich kommt den sonstigen zivilen Digitalinfrastrukturen wachsende Bedeutung zu. Schon heute fördern wir den Informationsaustausch u. a. in der Allianz für Cybersicherheit mit mehr als 6.000 teilnehmenden Unternehmen und Institutionen. Wir bauen beim BSI eine kooperative Kommunikationsplattform für den effektiven und effizienten Austausch von Informationen zu Cyberangriffen auf (BSI Information Sharing Plattform – BISP). So soll sichergestellt werden, dass beispielsweise Schäden durch Ransomware erheblich reduziert werden.

In einem ersten Schritt werden wir die bestehenden Informationsangebote des BSI und angeschlossener Institutionen bündeln und einer breiteren Nutzergemeinschaft, insbesondere KMU, auf einer zentralen Plattform, dem „BSI Information Sharing Portal“ (BISP), anbieten. In einem zweiten Schritt soll diese Plattform zu einem zivilen Cyberabwehrsystem (ZCAS) ausgebaut werden, das zentrale Elemente einer „zivilen Netzverteidigung“ enthält, mit denen aktiv und automatisiert auf Cyberangriffe reagiert werden kann.

Maßnahmen und Ziele in der 20. Legislaturperiode:

- Aufbau eines BSI Information Sharing Portals (BISP)
- Konzeption und initialer Aufbau eines zivilen Cyberabwehrsystems (ZCAS)

7. Digitale Souveränität in der Cybersicherheit stärken

Mit zunehmender Digitalisierung wandeln sich auch die Bedrohungen im Cyberraum. Nahezu täglich werden wir mit neuen Angriffsvarianten konfrontiert. Die Anforderungen an die Cybersicherheit insbesondere der KRITIS-Unternehmen müssen daher mit voranschreitender Digitalisierung und Vernetzung in einem ganzheitlichen Ansatz an neue Bedrohungslagen angepasst werden. Gleiches gilt für neue und disruptive Technologiefelder wie automatisiertes Fahren, Telemedizin und Smart-City-Lösungen. Dabei gilt es vor allem sicherzustellen, dass nicht vertrauenswürdige Hersteller nicht am Ausbau der zugrunde liegenden Infrastrukturen beteiligt werden.

Wir müssen daher unsere Cybersicherheitsforschung stärken. Erforderlich ist eine Förderung von Forschung, Entwicklung und Marktzugang von Produkten und Dienstleistungen mit Schwerpunkt Cybersicherheit insgesamt, insbesondere aber für moderne Kommunikationstechologien, für die 5G/6G-Netze. Auch die Vergabe von Forschungsaufträgen zur Stärkung der digitalen Souveränität durch die Agentur für Innovation in der Cybersicherheit GmbH sowie die Nutzbarmachung der erzielten Ergebnisse tragen zur Stärkung bei.

Maßnahmen und Ziele in der 20. Legislaturperiode:

- Stärkung der deutschen Cybersicherheitsforschung zur Erhöhung der Resilienz bei existenziellen Bedrohungen
- Förderung der Digitalen Souveränität insbesondere mit Blick auf die Kommunikationstechnologien 5G/6G
- Erweiterungen der Prüfmöglichkeiten des BSI im Hinblick auf die Vertrauenswürdigkeit von Herstellern, die sogenannte „kritische Komponenten“ für KRITIS-Betreiber bereitstellen (z. B. im Energie-, Gesundheits- oder Finanzwesen)
- Verstärkte Beauftragung von innovativen Forschungsvorhaben auf der Grundlage von (projizierten) Anwendungsfällen der Sicherheitsbehörden und der Cyberverteidigung

8. Krisenfeste Kommunikationsfähigkeit schaffen und Sicherheit der Netze ausbauen

Die erfolgreiche Umsetzung der Digitalisierungsvorhaben der öffentlichen Verwaltung erfordert eine moderne Kommunikationsplattform. Verlässliche und sichere Netze sind Basis jeglicher Zusammenarbeit der öffentlichen Verwaltung. Dabei müssen die Netzinfrastrukturen Schritt halten mit den Innovationszyklen und den steigenden Anforderungen an die Digitalisierung der Verwaltung. Hierfür müssen sie nicht nur technisch, sondern vor allem strategisch im Sinne der nationalen digitalen Souveränität kontinuierlich weiterentwickelt werden.

Die „Netzstrategie 2030 für die öffentliche Verwaltung“ stellt ein umfassendes Programm dar, um die Modernisierungsanforderungen an die Netze sinnvoll zu bündeln und die Etablierung eines Informationsverbundes der öffentlichen Verwaltung (Länder, Kommunen und Bund) zu erreichen.

Kommunikation ist das wichtigste Führungsmittel von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) und der Bundeswehr. Es besteht der dringende Bedarf, den Nutzern des Digitalfunks BOS eine bundesweite, sichere und hochverfügbare Breitbanddatenkommunikation als Ergänzung zum TETRA-Sprechfunk zu ermöglichen. Die Modernisierung der Netzinfrastruktur und des Digitalfunks BOS bildet somit eine wichtige Grundlage für die Verwaltungsmodernisierung.

Maßnahmen und Ziele in der 20. Legislaturperiode:

- Modernisierung der Weitverkehrsnetze gemäß der „Netzstrategie 2030 für die öffentliche Verwaltung“
- Zentrale Unterstützung der Behörden bei der Einführung von IPv6
- Einführung eines zentralen Videokonferenzsystems für die Bundesverwaltung
- Modernisierung des Digitalfunknetzes für Behörden und Organisationen mit Sicherheitsaufgaben
- Einrichtung einer Breitbandkommunikation im Digitalfunknetz

Impressum

Herausgeber

Bundesministerium des Innern und für Heimat, 11014 Berlin

Internet: www.bmi.bund.de

Stand

Juni 2022

Gestaltung

KOMPAKTMEDIEN Agentur für Kommunikation GmbH
Torstraße 49, 10119 Berlin

Bildnachweis

Michael Traitov stock.adobe.com

Artikelnummer BMI22011

Berlin 2022