Deutscher Bundestag **Drucksache 20/14532**

20. Wahlperiode 06.01.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Maximilian Funke-Kaiser, Konstantin Kuhle, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 20/14372 –

Auswirkungen von Cyberangriffen auf die Sicherheit und die Wirtschaft von Deutschland

Vorbemerkung der Fragesteller

Die Cybersicherheit ist die Achillesferse des digitalen Zeitalters und ein entscheidender Faktor für die Sicherheit Deutschlands. Die wachsende Bedrohungslage im Cybersicherheitsbereich wird nicht nur durch technische Entwicklungen, sondern auch durch geopolitische Spannungen, wie den russischen Angriffskrieg gegen die Ukraine, geprägt (Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2024, S. 22).

Cybersicherheit ist daher nicht nur ein technologisches, sondern auch ein sicherheitspolitisches und gesellschaftliches Kernanliegen. Cyberangriffe stellen auch eine der größten Herausforderungen für die deutsche Wirtschaft dar. Laut einer aktuellen Studie im Auftrag des Bitkom beläuft sich der durch Cyberkriminalität verursachte Schaden auf rund 267 Mrd. Euro – ein alarmierender Wert (www.behoerden-spiegel.de/2024/08/28/267-milliarden-euro-schaden-durch-cyber-angriffe/#:~:text=Eine%20neue%20Studie%20im%20Auftrag,noch%20206%20Milliarden%20Euro%20gewesen). Ein umfassender Schutz unserer informationstechnischen Systeme ist unabdingbar, um die Sicherheit von Bürgern, Unternehmen und kritischen Infrastrukturen zu gewährleisten und die demokratische Integrität zu schützen (BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 91).

Die bisherige Verteilung der Aufgaben und Zuständigkeiten der Cybersicherheit auf Bundesebene steht bereits seit einiger Zeit in der Kritik. Im Kern geht es dabei um den Interessenkonflikt zwischen der Offenlegung von Sicherheitslücken durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Zurückhaltung und Nutzung von Sicherheitslücken, beispielsweise durch das Bundesamt für Verfassungsschutz oder das Bundeskriminalamt. All diese Institutionen sind nachgeordnete Behörden unter dem Dach des Bundesministeriums des Innern und für Heimat (BMI) – mit unterschiedlichen Interessen. Aus diesem Grund wird von Expertinnen und Experten bereits seit Jahren gefordert, dass das BSI unabhängiger vom BMI aufgestellt wird, damit es in seiner Rolle als glaubwürdiger und vertrauenswürdiger Ansprechpartner für IT-Sicherheitsbelange auftreten kann (zum Beispiel Kipker; Mayr, Zur Unabhängigkeit des BSI, Datenschutz und Datensicherheit, 2023, S. 790 ff.).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 6. Januar 2025 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Dies hat zuletzt auch die Präsidentin des BSI in ihrer Stellungnahme zur Anhörung zum Gesetzentwurf zur Umsetzung der NIS (Netzwerk- und Informationssicherheit)-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung betont (www.bundestag.de/resource/blob/1027138/0e7d977acf676897233c034b842807be/20-4-523-C.pdf#page3).

Um die Informationssicherheit auf nationaler Ebene zu koordinieren, existiert in vielen Ländern bereits ein Chief Information Security Officer (CISO) (www.cio.gov/handbook/key-stakeholders/ciso/, https://cyber.gouv.fr/en/what-we-do , www.canada.ca/en/treasury-board-secretariat/corporate/mandate/chief-information-officer.html).

Für die Bundesverwaltung gibt es nach wie vor keinen Koordinator, der ressortübergreifend für die Etablierung entsprechender Risikoanalysen, Schutzzielen und einem Managementsystem zuständig ist. Expertinnen und Experten fordern, dass ein solcher CISO-Bund mit entsprechenden Durchsetzungsbefugnissen ausgestattet (Kipker, Stellungnahme zur Anhörung zum Gesetzentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung) und beim BSI angesiedelt wird, weil dort die Expertise zur Informationssicherheit liegt. Im aktuellen Gesetzentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung ist zwar ein Koordinator für die Informationssicherheit vorgesehen (§ 48 des BSI-Gesetzes (Neufassung (BSIG-E)), allerdings ist seine Stellung innerhalb der Bundesverwaltung und seine konkreten Kompetenzen noch nicht geregelt.

1. Wie viele Cyberangriffe auf deutsche Bundesbehörden wurden in den letzten zwölf Monaten registriert, wie viele hiervon waren erfolgreich, welche Schäden sind aus diesen erfolgreichen Angriffen jeweils entstanden (bitte jeweils nach Behörden aufschlüsseln), und wie werden diese Cyberangriffe und ihre Auswirkungen von der Bundesregierung erfasst?

Im Zeitraum vom 1. Januar 2024 bis 30. Dezember 2024 sind dem Bundesamt in der Informationssicherheit (BSI) 80 gemeldete „IT-Sicherheitsvorfälle“ erfasst worden. 17 davon waren erfolgreich und betrafen die Installation von Schadsoftware, die unautorisierte Systemnutzung sowie den Datenabfluss. Eine Aufschlüsselung nach Behörden ist aufgrund der Vertraulichkeit gegenüber den meldenden Behörden nicht möglich. Behörden müssen dem BSI Cyberangriffe gemäß der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) melden.

2. Wie viele Cyberangriffe auf Einrichtungen der kritische Infrastrukturen wurden in den letzten zwölf Monaten registriert, wie viele hiervon waren erfolgreich (bitte nach jeweiligem Industriebereich aufschlüsseln), welche Schäden sind aus diesen erfolgreichen Angriffen jeweils entstanden, und wie werden diese Cyberangriffe und ihre Auswirkungen von der Bundesregierung erfasst?

Die Betreiber kritischer Infrastruktur (KRITIS-Betreiber) sind gemäß § 8b Absatz 4 BSIG verpflichtet, Cybersicherheitsvorfälle unverzüglich dem BSI zu melden.

Die Anzahl der gemeldeten Vorfälle wird je Quartal auf der Website des BSI veröffentlicht: www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html

Im Sinne der Fragestellung liegen der Bundesregierung keine Erkenntnisse über mögliche Schäden vor.

3. Wie stellt die Bundesregierung sicher, dass Unternehmen, die dem Einfluss autoritärer Regime unterliegen, nicht beim Ausbau von kritischen Infrastrukturen beteiligt werden (zum Beispiel 5G und zukünftig 6G-Ausbau), welche Maßnahmen hat die Bundesregierung bereits ergriffen?

Das Bundesministerium des Innern und für Heimat (BMI) kann gemäß § 9b Absatz 2 des BSI-Gesetzes den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber der kritischen Infrastruktur im Benehmen mit den in § 10 Absatz 1 des BSI-Gesetzes aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach § 9b Absatz 1 des BSI-Gesetzes untersagen oder Anordnungen erlassen, sofern der Einsatz die öffentliche Ordnung oder Sicherheit Deutschlands voraussichtlich beeinträchtigt. Im Rahmen der Prüfung des BMI ist u. a. festzustellen, ob der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird, ob der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit Deutschlands oder eines anderen Mitgliedstaates der Europäischen Union, des Nordatlantikvertrages oder auf deren Einrichtungen hatten, und ob der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen Deutschlands, der Europäischen Union oder des Nordatlantikvertrages steht.

Die öffentlichen 5G-Mobilfunknetze sind elementarer Bestandteil der kritischen Infrastruktur in Deutschland und von entscheidender Bedeutung für Wirtschaft und Gesellschaft, unter anderem für die Funktionsfähigkeit von Sektoren wie Energie, Verkehr, Gesundheit und Finanzen. Für die Bundesregierung hat die Sicherheit sowie die technologische und digitale Souveränität Deutschlands im Bereich der 5G-Mobilfunknetze daher höchste Priorität. Nach umfangreichen Ermittlungen hat das BMI im 2. Quartal 2024 individuelle Verhandlungen mit den Mobilfunkbetreibern Deutsche Telekom, Vodafone und Telefónica geführt. Die Verhandlungen über den weiteren Einsatz kritischer Komponenten in den 5G-Mobilfunknetzen konnte das BMI im Juli 2024 mit einer Einigung abschließen. Mit den Verträgen mit den Mobilfunkbetreibern wurden die vom BMI geführten Prüfverfahren nach § 9b Absatz 4 des BSI-Gesetzes abgeschlossen. Die Verträge verpflichten die Mobilfunkbetreiber, bis spätestens Ende 2026 keine kritischen Komponenten der Hersteller Huawei und ZTE mehr in ihren 5G-Kernnetzen einzusetzen. Außerdem sind die Mobilfunkbetreiber verpflichtet, bis Ende 2029 die kritischen Funktionen der 5G-Netzwerkmanagementsysteme der Hersteller Huawei und ZTE in ihren Zugangs- und Transportnetzen des 5G-Mobilfunknetzes durch technische Lösungen anderer Hersteller zu ersetzen. Parallel zu der Einigung wurde die Einrichtung eines Forums verabredet, um gemeinsam Lösungen für die Umsetzung und Förderung der in den Verträgen vereinbarten Ziele zu erarbeiten. An dem Forum sollen sich neben der Bundesregierung alle Betreiber von 5G-Mobilfunknetzen sowie Industriepartner und Hersteller beteiligen.

Das Forum soll auch einen strukturierten Dialog über offene Schnittstellen, 6G-Standards, den Schutz der Netze sowie Informations- und Cybersicherheit gewährleisten.

Die Forschung zu 6G-Mobilfunktechnologien wird im Rahmen des Forschungsprogramms „Souverän. Digital. Vernetzt.“ des Bundesministeriums für Bildung und Forschung (BMBF) gefördert. Ein Ziel des Programms ist die technologische Souveränität Deutschlands und Europas im Bereich 6G. Die

„Leitinitiative Hyperkonnektivität“ des BMBF verankert zudem grundlegende Paradigmen wie Vertrauenswürdigkeit in der Forschung zu 6G.

Die Bundesregierung hat darüber hinaus in ihrer Nationalen Sicherheitsstrategie beschlossen, kritische Infrastrukturen wie die öffentlichen 5G-Mobilfunknetze besser zu schützen und Abhängigkeiten von einzelnen Zulieferern zu verringern. Insbesondere die Telekommunikationsnetze sind vor hybriden Bedrohungen und Cyberangriffen zu schützen, die schnell zu einer existentiellen Bedrohung werden können. Um kritische Verwundbarkeiten und Abhängigkeiten zu vermeiden, ist daher auf vertrauenswürdige Hersteller zu setzen.

4. Welche Maßnahmen werden allgemein ergriffen, um die IT-Sicherheitsinfrastruktur der Bundesbehörden gegen Angriffe zu schützen, und welche Bundesbehörden lassen nach Kenntnis der Bundesregierung ihre IT-Sicherheitsinfrastruktur im Speziellen mittels Penetrationstests überprüfen (bitte jeweils nach Behörden aufschlüsseln)?

Um die IT-Sicherheitsinfrastruktur der Bundesbehörden gegen Angriffe zu schützen, werden verschiedene Maßnahmen ergriffen. Hierzu zählt die Umsetzung des BSI IT-Grundschutzes mit beratender Unterstützung durch das BSI. Darüber hinaus stellt das BSI Arbeitshilfen bereit, um ein standardisiertes, hohes Sicherheitsniveau von IT-Schutz über alle Bundesbehörden hinweg zu ermöglichen. Ein fester Bestandteil der Empfehlungen ist die Durchführung von Penetrationstests. Diese werden durch die Behörden veranlasst und die Ergebnisse sowie das weitere Vorgehen vertraulich mit dem BSI abgestimmt. Außerdem hat das BSI die Umsetzungsberatung für die Bundesbehörden intensiviert und gewährleistet hierdurch schnelle Anpassungen an die aktuelle Lage der Cybersicherheit.

Zur Erkennung und Abwehr von Cyberangriffen insbesondere durch hochqualifizierte Akteure wird im BSI das Bundes-Security Operation Center (BSOC) als Dienstleistung für die Bundesverwaltung angeboten.

Weiterhin stellt das BSI der Bundesverwaltung verschiedene IT-Sicherheitsprodukte durch spezifische Rahmenverträge zur Verfügung.

Die Bundesregierung unterhält u. a. ein dediziertes ressortübergreifendes Kommunikationsnetz (derzeit Netze des Bundes), welches für den Austausch von Informationen bis zum Einstufungsgrad „VS-Nur für den Dienstgebrauch“ und für die Handlungsfähigkeit der Bundesregierung in besonderen Lagen dient. Derzeit werden vielfältige Sicherheitsmaßnahmen zum Schutz der ressortübergreifenden Kommunikationsnetze getroffen, wobei der Verteidigungsfall als Gefährdung hiervon nicht eingeschlossen ist. Die bestehende Absicherung der Vertraulichkeit und Integrität beginnt auf der Ebene der Infrastruktur (bspw. Zutritt für sicherheitsüberprüftes Personal) und reicht bis zur Produktauswahl (bspw. BSI-geprüfte Produkte) und wird derzeit durch einen Freigabe- und Abnahmeprozess des BSI besonders bewertet. Die Härtung bzw. Sicherstellung der Verfügbarkeit wird ebenfalls durch umfangreiche Maßnahmen (bspw. nationales Routing und dedizierte Glasfaserverbindungen) gesichert. Zur Absicherung der zentralen Schutzmechanismen werden seitens BSI auch die angeschlossenen Behörden mittels des Mindeststandards Nutzerpflichten Netze des Bundes (NdB) zur Mitwirkung verpflichtet. Des Weiteren gibt es für Bundesbehörden grundsätzliche Anforderungen (insbesondere IT-Grundschutz und Mindeststandards), aus denen konkrete Maßnahmen zum Schutz physischer Infrastrukturbereiche und somit auch der IT-Sicherheitsinfrastruktur abgeleitet werden. Teilweise werden diese Aspekte auch geprüft.

Folgende Bundesbehörden haben an Penetrationstests teilgenommen:

Bundesinstitut für Arzneimittel und Medizinprodukte

Bundeskanzleramt

Bundeszentralamt für Steuern

Bundesamt für Sicherheit in der Informationstechnik

Bundesverwaltungsamt

Informationstechnikzentrum Bund

Bundesministerium für Digitales und Verkehr

Bundesministerium des Innern und für Heimat

Auswärtiges Amt

Bundeskriminalamt

Bundesstelle für Flugunfalluntersuchung

Bundeskartellamt

Bundesministerium für Arbeit und Soziales

Bundesministerium für Ernährung und Landwirtschaft

Bundesanstalt für Geowissenschaften und Rohstoffe

Bundespresseamt

Beschaffungsamt des Bundesministeriums des Innern

Kraftfahrt-Bundesamt

Bundesministerium der Justiz

Bundesamt für Familie und zivilgesellschaftliche Aufgaben (BAFzA)

Bundesnetzagentur

Bundesamt für Justiz

Bundesamt für Seeschifffahrt und Hydrographie

Bundeszentrale für politische Bildung

Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)

Bundesamt für Verbraucherschutz und Lebensmittelsicherheit (BVL)

Umweltbundesamt

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)

Statistisches Bundesamt

Generalzolldirektion

Eisenbahn-Bundesamt

Bundesamt für Naturschutz

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

In Summe sind es 99 Penetrationstests bei Bundesbehörden gewesen.

In der Bundesverwaltung ist von allen Bundesbehörden ein Informationssicherheitsmanagement nach BSI-Standards und IT-Grundschutz verpflichtend umzusetzen. Hierzu gehören auch regelmäßige Informationssicherheits-Revisionen (bei Bedarf einschließlich der Durchführung von Penetrationstests). Die Rah-

menbedingungen für die Bundesverwaltung ergeben sich insbesondere aus dem Kabinettbeschluss UP Bund (Informationssicherheitsleitlinie für die Bundesverwaltung) sowie aus dem BSI-Gesetz (das derzeit im Rahmen der Umsetzung der europäischen NIS2-Richtlinie eine Aktualisierung erfährt).

Zudem werden die Mitarbeitenden der Bundesbehörden geschult und für den Arbeitsalltag sensibilisiert, die Sicherheitsprodukte der IT-Sicherheitsinfrastruktur nach den Vorgaben einzusetzen.

5. Wie viele Cyberangriffe wurden dem BSI seitens Akteuren der Privatwirtschaft innerhalb der letzten zwölf Monate gemeldet (bitte nach Art und Umfang des Angriffs, betroffenen Wirtschaftszweig, Schadenshöhe und getroffenen Gegenmaßnahmen aufschlüsseln)?

362 gesamt.

Eine spezifische Auswertung über alle Meldestellen aus der Wirtschaft ist aufgrund unterschiedlicher Meldeformulare nicht möglich. Daher ist eine Aufschlüsselung nach Art und Umfang des Angriffs nicht meldestellenübergreifend möglich. Es existiert meldeübergreifend keine einheitliche Kategorisierung in Wirtschaftszweige. Eine Schadenshöhe liegt dem BSI nicht vor. Die getroffenen Gegenmaßnahmen seitens der Betroffenen liegen dem BSI nur teilweise vor. Eine statische Auswertung der Gegenmaßnahmen erfolgt nicht.

6. Ist der Bundesregierung bekannt, ob dem BSI bekannte Schwachstellen nicht an die betroffenen Akteure kommuniziert wurden, und wenn ja, wie viele solcher Fälle sind der Bundesregierung bekannt, um welche Schwachstellen handelt es sich, werden diese auch von Sicherheitsbehörden genutzt, sieht die Bundesregierung insoweit einen Wertungswiderspruch?

Dem BSI gemäß der Clean-Vehicles Directive-Richtlinie (CVD-Richtlinie) gemeldete Schwachstellen (www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html) werden immer an die betroffenen Hersteller/Akteure kommuniziert.

7. Welche Förderprogramme und Beratungsangebote vonseiten des Bundes gibt es für Unternehmen und Forschungseinrichtungen, um Innovationen im Bereich Cybersicherheit zu fördern, welche Förderprogramme und Beratungsangebote vonseiten des Bundes gibt es speziell für Einrichtungen der kritischen Infrastruktur, und in welchem Umfang werden die Förderbudgets hier jeweils ausgeschöpft?

Das deutsche Nationale Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung (NKCS) berät zu Themen der Cybersicherheitsforschung und -entwicklung inklusive Projektvorhaben mit einer europäischen Perspektive und platziert deutsche Interessen in EU-Forschungsprogrammen. Der Lenkungskreis des NKCS setzt sich zusammen aus BMI, Bundesministerium für Wirtschaft und Klimaschutz (BMWK), BMBF und Bundesministerium der Verteidigung (BMVg), durchgeführt wird das Projekt NKCS vom BSI, dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) Projektträger (DLR-PT) und dem Forschungsinstitut CODE der Universität der Bundeswehr München (FI CODE). Als die Cybersicherheitsbehörde des Bundes fungiert das BSI dabei als Kopfstelle und „Single Point of Contact“ (SPoC) und wurde am 10. Dezember 2021 vom BMI gegenüber der EU-Kommission offiziell als solches notifiziert.

Die Nationale Kontaktstelle Digitale und Industrielle Technologien – NKS DIT – ist eine Beratungs- und Serviceeinrichtung zur europäischen Forschungsförderung; sie arbeitet im Auftrag BMBF. Forschung und Innovation im „Cluster 3: Civil Security for Society“ im Themenfeld „Cybersecurity“ sollen dazu beitragen, den Einsatz innovativer digitaler Technologien, wie z. B. künstliche Intelligenz, Kryptographie oder Quantentechnologien, zu fördern, um Datensicherheit und Cybersicherheit zu erhöhen. Darüber hinaus sollen Europas industrielle Kapazitäten im Bereich Cybersicherheit gestärkt und die technologische Souveränität gesteigert werden.

Das Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ (Laufzeit von 2021 bis 2026) bündelt die Förderaktivitäten zur Cybersicherheitsforschung und fördert Innovationen an Universitäten, Hochschulen, Forschungseinrichtungen und Unternehmen. Das Programm sieht Mittel von über 350 Mio. Euro für den Förderzeitraum vor. Bewilligungen konnten in dieser Höhe bereits gewährt werden.

Die Bundesregierung bietet eine zentrale Stelle, die Förderberatung „Forschung und Innovation“ des Bundes an, um Interessierten den Weg in die Forschungs- und Innovationsförderung zu ebnen. Im Bereich der Cybersicherheitsforschung bietet der zuständige Projektträger VDI/VDE-IT GmbH Informationsveranstaltungen zu den Förderrichtlinien und Beratung von Förderinteressenten und -beteiligten zu Programm, Förderrichtlinien und -verfahren an. Eine Beratung zu Gründungen innerhalb der Fördermaßnahme StartUpSecure erhalten Interessierte in den Gründungsinkubatoren, angesiedelt an den Forschungszentren CISPA in Saarbrücken, ATHENE in Darmstadt und KASTEL in Karlsruhe sowie an der Ruhr-Universität Bochum.

Das BMWK bietet z. B. mit dem Zentralen Innovationsprogramm Mittelstand (ZIM) verschiedenen Beratungsangebote und Fördermöglichkeiten, um Innovationen im Bereich Cybersicherheit bei Unternehmen zu fördern.

Die Transferstelle Cybersicherheit im Mittelstand der Initiative IT Sicherheit in der Wirtschaft KMU unterstützt über Informations- und Qualifikationsformate, zahlreiche Veranstaltungen, eine Detektions- und Reaktionsplattform für Cyberangriffe und ein breites Netzwerk an Partnern das Cybersicherheitsniveau im Mittelstand und hilft Unternehmen resilienter zu machen.

Das BSI kann gemäß § 3 Absatz 3 BSIG Betreiber Kritischer Infrastrukturen (KRITIS) auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen. Die Beratung durch das BSI erfolgt vertraulich und herstellerneutral. Das BSI ist verpflichtet, den KRITIS-Betreibern die entstandenen Kosten gemäß BMI-Kostenverordnung in Rechnung zu stellen.

8. Welche Maßnahmen des Aktionsplans Wirtschaftsschutz 2024+ wurden bereits umgesetzt oder werden zurzeit umgesetzt, und gibt es bereits Ergebnisse, welche Bedarfe und Maßnahmen bei kleineren und mittleren Unternehmen sind aus Sicht der Bundesregierung erforderlich?

Die Maßnahmen des Aktionsplanes Wirtschaftsschutz 2024+ befinden sich zum überwiegenden Teil in der Umsetzung. Das betrifft insbesondere auch die Ermittlung des benötigten Unterstützungsbedarfs von KMUs und Start-ups, die notwendige Verzahnung mit bereits bestehenden staatlichen Initiativen im Bereich der Cybersicherheit und die Weiterentwicklung des Wirtschaftsgrundschutzes.

Zum jetzigen Zeitpunkt ist aus Sicht der Bundesregierung für kleine und mittlere Unternehmen vor allem erforderlich, sich selbst besser vor Angriffen aus dem Realraum und dem Cyberraum zu schützen und die Widerstandskraft ihrer

eigenen Organisation erhöhen zu können. Die Maßnahmen aus dem Aktionsplan 2024+ sollen dazu ihren Beitrag leisten, indem insbesondere Informationswege und Best-Practice-Austausche optimiert und initiiert werden.

9. Wie plant die Bundesregierung zukünftig die Koordinierung der Zusammenarbeit mit der EU im Bereich Cybersicherheit?

Die Bundesregierung ist in der Horizontalen Gruppe „Fragen des Cyberraums“ des Rates der EU vertreten. Die horizontale Arbeitsplattform koordiniert die gemeinsame Cybersicherheitspolitik der Mitgliedstaaten und der Europäischen Union, auch indem sie einen engen Austausch mit anderen Arbeitsgruppen und Institutionen, wie bspw. der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) oder dem Europäischen Auswärtigen Dienst (EAD), pflegt. Die Bundesregierung setzt sich dort für ein einheitliches Vorgehen der EU und ihrer Mitgliedstaaten zu cyberpolitischen Fragen ein, dies gilt sowohl für Fragen der Cybersicherheit als auch der gemeinsamen Cyber-Außenpolitik.

10. Welche Schlussfolgerungen zieht die Bundesregierung aus dem ersten Bericht von ENISA (Europäische Agentur für Netz- und Informationssicherheit) über den Stand der Cybersicherheit in der Union?

Der im Dezember 2024 von der ENISA veröffentlichte Bericht zur Lage der Cybersicherheit in der EU 2024 stellt aus Sicht der Bundesregierung die bekanntermaßen hohe und wachsende Bedrohungslage für die europäische Cybersicherheit und zu den auf EU-Ebene verfügbaren Fähigkeiten zum Schutz des Cyberraums gut und zutreffend dar. Die dort dargelegten Erkenntnisse sind bereits jetzt Grundlage der nationalen und europäischen Maßnahmen zur Erhöhung der Cybersicherheit und zu deren Fortentwicklung. Insofern ergibt sich aus dem Bericht keine grundlegende Neubewertung der Cybersicherheitslage. Die von der ENISA abgeleiteten Handlungsempfehlungen sind aus Sicht der Bundesregierung nachvollziehbar begründet, wobei sichergestellt werden muss, dass sich die Aktivitäten von ENISA in diejenigen der Mitgliedstaaten kohärent einfügen.

11. Welche Rolle spielt Deutschland bei der NATO-Cyberabwehr (NATO Cooperative Cyber Defence Centre of Excellence), und an welchen Übungen mit bzw. für die NATO-Cyberabwehr hat die Bundeswehr konkret teilgenommen?

Die NATO-Cyberabwehr ist unabhängig vom NATO Cooperative Cyber Defence Centre of Excellence organisiert, das die NATO und ihre Mitgliedstaaten als unabhängige Forschungs- und Trainingsinstitution unterstützt.

Deutschland ist Gründungsmitglied des NATO Cooperative Cyber Defence Centre of Excellence und einer der größten Unterstützer des Centers. Deutschland besetzt drei Dienstposten des Centers.

Die Bundeswehr nimmt an den drei regelmäßig in der NATO stattfindenden Cyber-Übungen Locked Shields, Crossed Swords sowie Cyber Coalition teil.

12. Wie schätzt die Bundesregierung die Rolle künstlicher Intelligenz in Bezug auf die Cybersicherheitsmaßnahmen der Bundesbehörden ein, und ist geplant, diese einzusetzen, und wenn ja, wo soll künstliche Intelligenz eingesetzt werden?

Die Bundesregierung prüft derzeit die Möglichkeiten des KI-Einsatzes, um Cybersicherheitsmaßnahmen zu unterstützen.

Sofern bereits Softwarelösungen zur KI gezählt werden, werden bereits verschiedene Lösungen zur Absicherung eingesetzt bspw. Virenschutz, Firewall-Regeln, Intrusion Detektion und Monitoring von Systemzuständen.

13. Welche nationalen Forschungsprojekte zu Verschlüsselungstechnologien gibt es nach Kenntnis der Bundesregierung, gibt es Planungen und Vorbereitungen, Quantenkryptografie zu verwenden?

Im BMVg sind derzeit folgende nationale Forschungsprojekte zu Verschlüsselungstechnologien bekannt:

- F&T-Vorhaben „Kryptotransformation Bw“ des BAAINBw
- Projekt „MuQuaNet – Das Quanten-Internet im Großraum München“ des dtec.bw
- Projekt „Encrypted Computing“ der Cyberagentur

Das BSI hat gemeinsam mit europäischen Partnerbehörden aus Frankreich, den Niederlanden und Schweden ein Positionspapier zu Quanten Key Distribution (QKD) veröffentlicht. Zusätzlich hat das BSI eine Studie veröffentlicht, die den aktuellen Wissensstand zu Implementierungsangriffen auf QKD-Systeme darstellt. Darin wird auch aufgezeigt, welche weiteren Arbeiten in diesem Bereich notwendig sind, um Vertrauen in die Implementierungssicherheit von QKD-Systemen zu entwickeln. Das BSI hat in Zusammenarbeit mit dem europäischen Standardisierungsinstitut ETSI die Entwicklung des ersten Protection Profiles nach Common Criteria für „Prepare-and-Measure-QKD“ in Auftrag gegeben. Das Protection Profile wurde im Januar 2024 vom BSI zertifiziert.

Die Aktivitäten des BSI in diesem Kontext werden auf der zugehörigen Website www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Quantenkryptografie/quantenkryptografie_node.html aufgelistet und aktualisiert.

Im Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ (Laufzeit von 2021 bis 2026) fördert das BMBF folgende 67 Projekte zur Quanten- und Post-Quanten-Kryptographie mit dem Ziel, diese Technologien zu einem anwendungstauglichen Reifegrad zu bringen:

Projekte der Quantenkommunikation	Projekte der Post-Quanten-Kryptographie
QuNET-beta	PQDrive
QR.X	Quoryptan
QSAMIS	PoQ-KIKI
NEQSIS	QUDIS
QPIS	PQ-CCA
DIQTOK	EASEPROFIT
QTOK	PARFAIT
Q-ToRX	POST
HybridQToken	
DE-QOR	

Projekte der Quantenkommunikation	Projekte der Post-Quanten-Kryptographie
DemoQuanDT	
QuNet+RECONNAITRE	
QuNET+ML	
QUBE II	
QuantumHiFi	
QuaPhySI	
QuKuK	
InQuRe	
QD-E-QKD	
tubLAN	
QD-CamNetz	
QUIET	
QECHQS	
QuINSiDa	
QuAtuLo	
Quant-ID	
SQuaD	
6G-QuaS	
QuNET+ISQKMS	
Q-Fiber	
QuNET+ProQuake	
QuNET+DECODE	
QuNET+LORELAY	
QuNET+FuNK	
QuNET+SKALE	
QuNET+MOBIXHAP	
Q-net-Q	
MIHQU	
MiQuE	
MultiCoreSPS	
PoLiSiQ	
VOMBAT	
SINNER	
MultiQomm	
CBQD	
NetiQueT	
QuNET+ICLink	
QuNET+OptiRoute	
QuNET+BlueCert	
QuNET-gamma	
QUARKS	
MANTIS	
MEEDGARD	
EQSOTIC	
COMPHORT	
SEQUIN	
SeQuRe	
SQuIRRL	
QR.N	

Insbesondere sind die Projekte QuNET und SQadD unter Einbeziehung des BSI und der Physikalisch-Technischen Bundesanstalt (PTB) zu nennen. Außerdem begleitet die Bundesregierung unter Beteiligung des BSI zusammen mit

weiteren nationalen Sicherheitsbehörden das von der EU-Kommission vorangetriebene Projekt EuroQCI, in dessen Rahmen eine Quantenkommunikationsinfrastruktur in Europa aufgebaut werden soll.

14. Welche neuen Bedrohungsszenarien im Cyberraum erwartet die Bundesregierung in den nächsten fünf Jahren?

Die derzeit gültige Cybersicherheitsstrategie der Bundesregierung ist öffentlich abrufbar unter: www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cybersicherheitspolitik/cybersicherheitspolitik-node.html#doc18751090bodyText2.

Ergänzend sind Informationen des BSI zu aktuellen bzw. gängigen Bedrohungsarten im Cyber-Raum öffentlich abrufbar unter: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/empfehlungen-nach-gefaehrdungen_node.html

15. Wie wird die Informationssicherheit auf Bundesebene derzeit koordiniert, in welchen Formaten tauschen sich Bundesbehörden über Cyberangriffe und getroffene Maßnahmen aus, gibt es einen ressortübergreifenden Maßnahmenplan zum Umgang mit Cyberangriffen?

Im Bereich der Informationssicherheit, insbesondere hinsichtlich Cybersachverhalten gesamtstaatlicher Relevanz, besteht ein ständiger und intensiver Austausch zwischen den zuständigen Behörden auf verschiedenen Ebenen. Das Nationale Cyber-Abwehrzentrum, eine Kooperations-, Kommunikations- und Koordinationsplattform von deutschen (Sicherheits-)Behörden und weiteren Einrichtungen unterschiedlicher Ressorts, dient in diesem Zusammenhang als Plattform, auf der die beteiligten Behörden Informationen im Rahmen ihrer jeweiligen gesetzlichen Befugnisse schnell austauschen und gegebenenfalls Schutz-, Gefahrenabwehr- oder Strafverfolgungsmaßnahmen koordinieren können.

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.bundesanzeiger-verlag.de
ISSN 0722-8333