

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Steffen Janich, Dr. Bernd Baumann, Erhard Brucker, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/3209 –**

Lagebericht 2025 des Bundesamtes für Sicherheit in der Informationstechnik

Vorbemerkung der Fragesteller

Der aktuelle jährliche Bericht zur Lage der IT-Sicherheit in Deutschland wurde vom Bundesminister des Innern, Alexander Dobrindt, und der Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik (BSI) am 11. November 2025 in der Bundespressekonferenz vorgestellt (www.youtube.com/watch?v=WbVwPTbFZGY). Der Bericht bezieht sich auf den Zeitraum von 1. Juli 2024 bis 30. Juni 2025 (<https://medien.bsi.bund.de/lagebericht/de/>).

Bei seiner Ansprache kündigte der Bundesinnenminister über den Inhalt des Berichts hinaus an, „für die Sicherheitsbehörden neue Befugnisse zur Cyberabwehr zu schaffen, die es zukünftig auch ermöglichen, die digitale Infrastruktur von Angreifern vom Netz zu nehmen, zu attackieren, zu stören, auch zu zerstören. Dies wird auch dann möglich sein, wenn sich die Angreifer mit ihrer Infrastruktur außerhalb der Bundesrepublik Deutschland befinden. [...] Das ist allerdings kein Hackback. [...] Uns geht es darum, die rechtlichen Grundlagen zu schaffen, dass wir die digitalen Systeme der Angreifer, die Server und die Software, stören und zerstören können, um Gefahren abzuwehren. Bisher sind die rechtlichen Grundlagen dafür nicht ausreichend. Wir werden diese rechtlichen Grundlagen schaffen“ (vgl. Link YouTube a. a. O., Minute 7:50 bis 9:35).

Wie schon im Bericht 2024 wird die IT-Sicherheitslage anhand der fünf Kriterien Bedrohungen, Angriffsfläche, Gefährdungen, Schadwirkungen und Resilienz beschrieben. Die Anzahl der Diagramme und Tabellen soll sich nach eigenen Angaben mit über 70 mehr als verdoppelt haben, während die Texte „prägnanter“ gehalten sein sollen (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2025_Achtseiter.pdf, S. 2). Nach Auffassung der Fragesteller soll hierdurch jedoch lediglich eine empirische Evidenz des Berichts suggeriert werden, die es aufgrund der Interpretierbarkeit deskriptiver Statistik und des hohen Dunkelfeldes jedoch nicht geben kann.

Nach Auffassung der Fragesteller ist ferner auffällig, dass trotz des Berichtstitels „IT-Sicherheit“ in dem Handout durchgängig von „Cybersicherheit“ die Rede und auch der Volltext diesbezüglich nicht hinreichend trennscharf formuliert ist.

Der Bericht ist im Gegensatz zu seinen Vorgängerberichten nicht als ein vollumfängliches PDF-Dokument verfügbar, sondern ist lediglich als Onlineversion einsehbar, ergänzt um ein siebenseitiges PDF-„Handout“, das „ausgewählte statistische Diagramme, Daten und Fakten“ enthält (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2025_Achtseiter.pdf).

So führt laut Bericht die sich weiter zuspitzende geopolitische Lage zu einer unverändert angespannten IT-Sicherheitslage (<https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/>). Insbesondere Web-Angriffsflächen würden nach wie vor einen besorgniserregenden Zustand zeigen. Der Bericht beschreibt einen Trend weg von großen, aufwendigen Angriffen hin zu vielen kleinen, einfach durchzuführenden Angriffen, die sich gegen kleine und mittlere Unternehmen (KMU) richten und 80 Prozent der angezeigten Angriffe ausmachen würden (ebd.). Bei Datenleaks wurden die durchschnittlich höchsten Lösegelder seit Beginn der Aufzeichnungen festgestellt (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2025_Achtseiter.pdf, S. 3). Gleichzeitig stellt der Bericht die These auf, dass die Summe der insgesamt gezahlten Lösegelder zurückgegangen sei, da Cyberangreifer mehr und mehr auch mittlere, kleine und Kleinstunternehmen mit schwach geschützten Angriffsflächen angreifen, auch wenn diese je Fall weniger Lösegeld erwarten lassen würden (<https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/>).

Im Hinblick auf Resilienz stellt der Bericht fest, dass die meldepflichtigen KRITIS (kritische Infrastrukturen)-Betreiber stetig Fortschritte erzielen, wirksame Maßnahmen, insbesondere bei politiknahen Institutionen oder Verbrauchern jedoch überwiegend noch ausbleiben (<https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/>).

Mit der weiteren Aussage „Kleine und mittlere Unternehmen: Alle sind gefährdet“ (ebd.) zeigt der Bericht nach Auffassung der Fragesteller eine weitere gravierende Unschärfe in den Begrifflichkeiten, da eine „Gefährdung“ nach der BSI-eigenen Systematik erst dann entsteht, wenn „eine Bedrohung, beispielsweise ein Schadprogramm, auf eine Angriffsfläche, zum Beispiel einen Webserver trifft“, wenn also ein tatsächlich stattfindender Angriff, „je nach Resilienz eine Schädigung zur Folge haben kann“ (<https://medien.bsi.bund.de/lagebericht/de/systematik-der-lagebewertung/>). Auf Basis der BSI-eigenen Systematik wäre nach Auffassung der Fragesteller vielmehr die Aussage „Alle sind bedroht“ zutreffend.

Nach Auffassung der Fragesteller benennt der Bericht trotz seines statistischen Darstellungsaufwandes bei Weitem nicht hinreichend differenziert genug, welche Arten von kleinen und mittleren Unternehmen sich im Fokus von Cyberangriffen befinden. So sind nach Angaben des Statistischen Bundesamtes (www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/aktuell-beschaeftigte.html#:~:text=Mit%203%20im%20Jahr%202023%20600%20000%20Unternehmen%20als%20KMU%20im%20engeren%20Sinne%20einzuordnen%2C%20w%C3%A4hrend%202%2C6%20Millionen%20Unternehmen%20als%20Kleinstunternehmen%20gelten%2C%20Letztere%20verf%C3%BCgen%20lediglich%20%C3%BCber%20maximal%20neun%20Besch%C3%A4ftigte%20und%20maximal%202%20Mio.%20Euro%20Jahresumsatz%2C%20w%C3%A4hrend%20es%20bei%20KMU%20im%20engeren%20Sinne%20bis%20zu%20249%20Besch%C3%A4ftigte%20und%2050%20Mio.%20Euro%20Jahresumsatz%20sind) im Jahr 2023 600 000 Unternehmen als KMU im engeren Sinne einzuordnen, während 2,6 Millionen Unternehmen als Kleinstunternehmen gelten. Letztere verfügen lediglich über maximal neun Beschäftigte und maximal 2 Mio. Euro Jahresumsatz, während es bei KMU im engeren Sinne bis zu 249 Beschäftigte und 50 Mio. Euro Jahresumsatz sind (www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/Glossar/kmu.html). Auf welche KMU-Gruppierung sich der Bericht bezieht, bleibt nach Auffassung der Fragesteller größtenteils offen.

Neben der fehlenden Betrachtung dieser Größenunterschiede von KMU bleibt nach Auffassung der Fragesteller ebenfalls unbeleuchtet und damit für die Ableitung effizienter und effektiver Sicherheitsmaßnahmen ungenügend, wie die Lage in den sehr unterschiedlichen KMU-Branchen ist, z. B. im Verarbeiten oder im Gastgewerbe, in der Wasserversorgung, im Handel oder in sonstigen Dienstleistungsbranchen wie Kunst und Unterhaltung.

Nach Auffassung der Fragesteller besteht durch eine solch undifferenzierte Berichterstattung die Gefahr von Fehlanreizen für ein Kosten-Nutzen subopti-

males Zuviel an zahlungswirksamen IT-Sicherheitsmaßnahmen, gerade bei der weit überwiegenden Anzahl an Kleinstunternehmen.

Als eine Schlussfolgerung sieht der Bericht für das Jahr 2026 den Schutz der Angriffsflächen als entscheidendes Element für die Verbesserung der Cybersicherheit (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2025_Achtseiter.pdf, S. 3).

Vorgaben für die Cyberresilienz der Institutionen, die die politische Willensbildung in Deutschland tragen, seien bislang noch nicht gesetzlich geregelt, was dringend nachgeholt werden sollte (<https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/>).

1. Steht die Aussage des Berichts, dass die sich weiter zuspitzende geopolitische Lage zu einer unverändert angespannten IT-Sicherheitslage führt (vgl. Vorbemerkung der Fragesteller), in Zusammenhang mit dem Säulendiagramm „APT-Gruppen 2025 nach Zielland (Top 10)“ (<https://medien.bsi.bund.de/lagebericht/de/apt-gruppen/>), und wenn ja, in welchem?

Die Aussage steht nicht in Zusammenhang mit der Säulengrafik.

- a) Inwieweit steht die Erläuterung zum Säulendiagramm, dass es sich bei Deutschland und Großbritannien um zwei westeuropäische Länder handle, in Zusammenhang mit einer sich weiter zuspitzenden geopolitischen Lage, warum weist nach Kenntnis der Bundesregierung Großbritannien einen 20 Prozent geringeren Wert als Deutschland auf, und warum weist Frankreich nach Kenntnis der Bundesregierung einen offenbar nochmals deutlich geringeren Wert als Deutschland auf, da es sich nicht in den Top Ten befindet?

Über die im Bericht angeführten allgemeinen Hintergründe hinaus liegen keine Erkenntnisse vor.

- b) Steht die Anzahl der in einem Zielland operierenden APT (Advanced Persistent Threats)-Gruppen mit dem Ausmaß zwischenstaatlicher Spannungen des Ziellandes in Zusammenhang, und wenn ja, wie ist es nach Kenntnis der Bundesregierung zu interpretieren, dass Japan einen höheren Wert als Deutschland aufweist?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt keine Analyse der strategischen Bedrohungslage von Japan durch und hat daher hierzu keine Erkenntnisse.

- c) Aus welchen Gründen beinhaltet der Bericht an dieser Stelle lediglich die Anzahl der APT-Gruppen in einem Zielland, nicht jedoch der Anzahl von APT-Angriffskampagnen auf ein Zielland?
- d) Inwieweit schmälert eine mögliche Inaktivität von APT-Gruppen oder die Möglichkeit des Outsourcings von APT-Angriffskampagnen an kommerzielle Dienstleister die Aussagekraft dieses Säulendiagramms?

Die Fragen 1c und 1d werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die aktuelle Datenlage bzgl. der Anzahl der APT-Angriffskampagnen (Advanced Persistent Threats) wird als zu wenig belastbar eingeschätzt. Zudem sind die Kenntnisse über Aktivitäten von APT-Gruppen aufgrund ausgeprägter klandestiner Vorgehensweisen grundsätzlich mit einer gewissen Unschärfe behaftet. Die Sicherheitsbehörden arbeiten stetig daran, ihr Wissen über die APT-Gruppen, ihre Aktivitäten sowie konkreten Vorgehensweisen zu verbessern.

- e) Sind an der Erstellung des Lageberichts ausschließlich IT-Experten oder auch Politik- und Wirtschaftswissenschaftlicher beteiligt?

An der Erstellung des Lageberichts sind Personen mit diversem fachlichen (auch nicht-technischem) Hintergrund beteiligt, um die vielfältigen Aspekte der IT-Sicherheitslage kompetent zu bewerten.

- f) Welche konkreten geopolitischen Initiativen oder Positionierungen der Bundesregierung führen nach Erkenntnissen des BSI zu der beschriebenen angespannten IT-Sicherheitslage in Deutschland?

Die Antwort auf diese Frage ist nicht von den gesetzlichen Aufgaben des BSI umfasst.

2. Bis wann soll das im Bericht formulierte Ziel des BSI erreicht werden, die Schwachstellen in veralteten, nicht aktualisierten Systemen der Web-Angriffsfläche der Bundesverwaltung strukturiert abzuarbeiten und ein wirkungsvolles Angriffsflächenmanagement in Form einer robusten Cybersicherheits-Governance-Struktur umzusetzen (<https://medien.bsi.bund.de/lagebericht/de/web-angriffsflaechen-der-bundesverwaltung/>)?
- a) Wird dieses Vorhaben mit einer spezifischen Projektstruktur verfolgt, und wenn ja, sind dieser bereits die notwendigen Ressourcen zugeordnet?
- b) Haben Maßnahmen zur Zielerreichung bereits begonnen, wenn ja, wann, und mit welchem Ergebnis, und wenn nein, warum nicht?

Die Fragen 2c bis 2b werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Beseitigung von Schwachstellen in Systemen der Bundesverwaltung ist ein permanent laufender Prozess. Um diese zeitnah zu erkennen, scannt das BSI u. a. regelmäßig die Web-Systeme der Bundesregierung und gibt Hinweise zu Problemen über die etablierten Kommunikationswege an die betroffenen Ressorts und Behörden/Einrichtungen. Mit der Novelle des BSI-Gesetzes (BSIG) erhält der CISO Bund (Chief Information Security Officer) eine stärker koordinierende Rolle und kann damit Maßnahmenprogramme zur messbaren Verbesserung der IT-Sicherheit der Bundesverwaltung festlegen. Die dafür notwendigen Ressourcen werden im Rahmen von Haushaltsaufstellungsverfahren beantragt.

- c) Aus welchen Gründen existieren im Jahr 2025 überhaupt noch veraltete, nicht aktualisierte Systeme der Web-Angriffsfläche der Bundesverwaltung?

Aufgrund der Vielschichtigkeit von Cybersicherheit im Allgemeinen und Schwachstellenmanagement bei Web-Anwendungen im Besonderen sind hierzu keine allgemeingültigen Aussagen möglich.

3. Wie ist die Aussage, dass die durchschnittlich 119 neuen Schwachstellen, die im aktuellen Berichtszeitraum durchschnittlich täglich weltweit bekannt wurden, gerade bei KMU „besonders häufig“ durchschlagen, zu quantifizieren (<https://medien.bsi.bund.de/lagebericht/de/gedaehrdungslage-der-kleinen-und-mittleren-unternehmen/>)?

Das BSI sieht eine Abnahme der Anzahl der erfolgreichen Angriffe auf große Unternehmen. Gleichzeitig steigt die Anzahl der Vorfälle bei kleineren und mittleren Unternehmen.

In der internationalen Entwicklung zeigen die regelmäßigen Berichte des IT-Dienstleisters Coveware den Trend zu Angriffen gegen kleine- und mittelständische Unternehmen (www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet). Diese Entwicklung beobachtet das BSI auch im Expertenaustausch mit Partnern aus der Wirtschaft und der IT-Sicherheitscommunity.

- a) Handelt es sich bei diesen „KMU“ um die ca. 600 000 KMU im engeren Sinne oder auch um die ca. 2,6 Millionen Kleinstunternehmen (vgl. Vorbemerkung der Fragesteller)?

Zugrunde liegt die Definition des Statistischen Bundesamtes. Diese sieht auch die Kleinstunternehmen als Teil der Gruppe der kleinen und mittleren Unternehmen (KMU).

Die Definition findet sich u. a. unter www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/_inhalt.html.

- b) Liegen der Bundesregierung Kenntnisse über die Branchenzugehörigkeiten dieser „KMU“ vor, und wenn ja, welche?

Der Bundesregierung liegen für den Lagebericht 2025 keine Erkenntnisse vor. Erst mit dem Lagebericht 2026 werden Daten zu umgesetzten Cyberrisikomanagementmaßnahmen und Betroffenen vorliegen (siehe Antwort zu Frage 3c).

- c) Handelt es sich bei der Aussage, „(a)uch im aktuellen Berichtszeitraum besitzen ‚viele‘ Unternehmen nach Erfahrung des BSI weder eine ausreichende Kenntnis über die allgemeine Cyberbedrohungslage noch über das eigene Risikoprofil“, um empirische Befunde oder um anekdotische Evidenz, und wie kann diese Aussage quantifiziert werden?

Die Aussage wird durch Studien und Auswertungen des BSI gestützt. Beispielsweise bewerten laut der „TÜV Cybersecurity Studie 2025“ 90 Prozent der mittleren und 91 Prozent der kleinen Unternehmen die Cybersicherheit ihres Unternehmens als „eher gut/sehr gut“. Gleichzeitig werden von den Unternehmen, die den CyberRisikoCheck auf Basis von DIN SPEC 27076 durchführen (in dem die absoluten Minimalanforderungen der Informationssicherheit abgeprüft werden), im Schnitt nur knapp 56 Prozent der Anforderungen erfüllt.

Um die Entwicklung in diesem Bereich zu verfolgen, werden kontinuierlich weitere Daten ausgewertet. So führt das BSI beispielsweise gemeinsam mit dem Deutschen Institut für Wirtschaftsforschung (DIW) und der Helmut-Schmidt-Universität der Bundeswehr aktuell ein Forschungsprojekt zur Cybersicherheit in KMU durch (www.uzbonn.de/blog/5034/forschungsprojekt-zur-cybersicherheit-in-kmu/), bei dem – ebenso wie beim CyberRisikoCheck – auch die Branchenzugehörigkeit abgefragt wird.

- d) Handelt es sich bei der Aussage, dass IT-affine KMU „teils feststellen“, dass es in ihrer Region entweder zu wenig qualifizierte Dienstleister gibt oder nur solche, die nicht zu ihrer eigenen Unternehmensgröße passen, um empirische Befunde oder um anekdotische Evidenz, und wie kann diese Aussage quantifiziert werden (ebd.)?

Eine wichtige Säule zur Stärkung der Cyber-Resilienz von Unternehmen ist das Thema Prävention. In diesem Zusammenhang führt das BSI jährlich eine große Zahl von Vortragsveranstaltungen (beispielsweise bei Branchenverbänden, Industrie- und Handelskammern, Handwerkskammern oder Cybersicherheitsinitiativen von Ländern und Wirtschaft) und Webinaren durch. Regelmäßig werden dabei von Seiten des Publikums Probleme beim Finden eines geeigneten IT-/IT-Sicherheitsdienstleisters angeführt.

Tagessätze von 1 500 Euro sind bei großen IT-Dienstleistern keine Seltenheit. Dass solche Summen beispielsweise einen kleinen Handwerksbetrieb in der Regel finanziell überfordern, ist auch ohne explizite wissenschaftliche Studie evident.

4. Wie begründet die Bundesregierung die These des Berichts (vgl. Vorbemerkung der Fragesteller), dass Cyberangreifer mehr und mehr auch mittlere, kleine und Kleinstunternehmen mit schwach geschützten Angriffsflächen angreifen, auch wenn diese je Fall weniger Lösegeld erwarten lassen würden?

In der internationalen Entwicklung zeigen die regelmäßigen Berichte des IT-Dienstleisters Coveware den Trend zu Angriffen gegen kleine- und mittelständische Unternehmen (www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet). Diese Entwicklung beobachtet das BSI auch im Expertenaustausch mit Partnern aus der Wirtschaft und der IT-Sicherheitscommunity.

- a) Ist dieser Trend quantifizierbar, und wenn ja, aus welchen Gründen wurde kein entsprechendes Diagramm für diesen Zusammenhang erstellt?

Die Aussage stützt sich auf den Bundeslagebericht Cybercrime 2024 des Bundeskriminalamtes (BKA). Vergleichszahlen für die Vorjahre liegen im BSI nicht vor. Aus diesem Grund ließ sich kein Diagramm erstellen.

- b) Sieht die Bundesregierung diese These im Widerspruch zu der von ihr im Bericht zitierten Sicherheitsfirma Chainalysis, die in ihrem X-Tweet vom 30. Juli 2024 von dem immer deutlicher werdenden Trend zur Großwildjagd bei Cybererpressungen spricht, wonach „weniger Attacken auf größere Ziele mit tieferen Taschen“ zu verzeichnen sind (www.bleepingcomputer.com/news/security/dark-angels-ransomware-receives-record-breaking-75-million-ransom/)?

Nein.

In dem in der Antwort zu Frage 4 zitierten Artikel heißt es weiter „This is in stark contrast to most ransomware groups, which target victims indiscriminately and outsource most of the attack to affiliate networks of initial access brokers and penetration testing teams.“

Das BSI kommt in seinen Analysen zum aktuellen Berichtszeitraum zu anderen Ergebnissen als das Unternehmen Chainalysis in seinem Tweet vor 17 Monaten.

Der dem Tweet zugrundeliegende Vorfall ist ein Einzelfall mit überdurchschnittlich hoher Lösegeldforderung. Aktuellere Daten von Chainalysis aus dem Berichtszeitraum des BSI Jahreslageberichts zeigen eine Mehrheit der Lösegeldzahlungen zwischen 1 000 und 100 000 US-Dollar (www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/).

Dem ist unbenommen, dass Angreifer versuchen, größere Unternehmen zu erpressen. Jedoch beobachtet das BSI wie auch IT-Dienstleister wie Coveware (www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet) eine steigende Resilienz großer Unternehmen selbst im Falle eines Angriffs, sodass diese Geschädigten von einer Lösegeldzahlung verstärkt Abstand nehmen.

5. Ist die Aussage des Berichts, die öffentliche Verwaltung meldete vor allem DDoS-Angriffe mit „geringer“ technischer Schadwirkung näher quantifizierbar, wenn ja, wie hoch ist die Schadwirkung (<https://medien.bsi.bund.de/lagebericht/de/geschaedigte-in-gesellschaft-wirtschaft-und-oefentlicher-verwaltung/>)?
 - a) Ist die Aussage des Berichts, dass längerfristige Schäden durch DDoS (Distributed Denial of Service)-Angriffe allein „selten“ seien, näher quantifizierbar, und wenn ja, wie oft ist „selten“?

Die Fragen 5 und 5a werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

DDoS-Angriffe (Distributed Denial-of-Service) wirken auf das Schutzziel Verfügbarkeit. Sie wirken darauf so lange ein, wie die Angriffe anhalten. Es gibt wirksame Mitigationsmechanismen gegen entsprechende Angriffe.

Mittelbare Schäden entstehen durch den erforderlichen Ressourceneinsatz für die Kommunikation und Einordnung von DDoS-Angriffen, da insbesondere DDoS-Angriffe auf prominente Ziele erhebliche öffentliche Aufmerksamkeit erhalten.

Eine Quantifizierung der technischen Schadwirkung ist aus Sicht der Bundesregierung vor diesem Hintergrund weder möglich noch sinnvoll.

- b) Ist die Aussage des Berichts, bei DDoS-Angriffen handele es sich um ein „beliebtes“ Werkzeug für Cyberhacking näher quantifizierbar, und wenn ja, wie viele der im aktuellen Berichtszeitraum erfolgten 196 Meldungen und wie viele der davon als externer Angriff eingeschätzten 64 Vorfälle sind auf Cyberhacker zurückzuführen?

Es liegen der Bundesregierung keine Informationen im gewünschten Detaillierungsgrad vor.

- c) Aus welchem Grund wird als einziges Beispiel für Cyberhacking die russische Gruppe NoName057(16) vorgestellt, und welchen Anteil haben nach Erkenntnis der Bundesregierung umwelt-, religiös- oder sozioökonomisch motivierte deutsche Hacktivistengruppen an Cyberangriffen in Deutschland?

Da diese Gruppierung öffentlich sehr präsent ist, wurde sie namentlich genannt. Zum zweiten Teil der Frage liegen der Bundesregierung keine Informationen im gewünschten Detaillierungsgrad vor.

6. Betrachtet die Bundesregierung die Begriffe „IT-Sicherheit“ und „Cybersicherheit“ als synonym, wenn ja, wie begründet die Bundesregierung

ihre Auffassung, und wenn nein, worin bestehen nach Auffassung der Bundesregierung Unterschiede?

Die Begriffe werden im Bericht synonym verwendet.

7. Aus welchen Gründen wurde auf die Erstellung eines vollumfänglichen PDF-Formats zusätzlich zur Lageberichtwebsite verzichtet?

Ab dem Jahr 2025 erscheint die Vollversion des Lageberichtes im Sinne eines Digital-First-Ansatzes im neuen Online-Format als Webseite. Die Vollversion wird durch Abformate (z. B. Handout als pdf) ergänzt. Auf weitere Veröffentlichungsformate der Vollversion (wie etwa Druckfassung oder eine pdf-Datei der Vollversion) wurde im Jahr 2025 verzichtet.

8. Wie hoch waren die Kosten für die Erstellung der Website zum Lagebericht 2025?

Für externe Dienstleistungen zur Konzeption und Entwicklung des digitalen Lageberichtes (inkl. Entwicklung eines Content-Management-Systems (CMS)) sind Kosten i. H. v. 1,3 Mio. Euro entstanden.

- a) Wie viele Personentage wurden für die Erstellung des Lageberichts 2025 aufgebracht (bitte nach BSI, BMI und Dienstleistern aufschlüsseln)?
- b) Wie viele Personen waren hauptsächlich mit der Erstellung des Lageberichts 2025 beschäftigt?

Die Fragen 8a und 8b werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die genauen Personentage und damit verbunden Personalkosten sind nicht zu ermitteln, da die Mitwirkung am Lagebericht immer nur ein Teil der Aufgaben der jeweiligen Personen ist

Zusätzliche Kosten entstanden wie folgt:

- Kosten für Agenturleistungen 27 986,25 Euro,
- 1 071 Euro für die Erstellung der notwendigen barrierefreien pdf in Deutsch und Englisch (535,50 Euro je Version).

- c) Wie hoch waren die Kosten für die Erstellung der Lageberichte der Jahre 2020 bis 2024, und welchen Umfang hatten diese Berichte jeweils?

Jahreslagebericht 2020: 88 Seiten; Kosten für Agenturleistungen: Layout, Satz, Lektorat: 39 915,60 Euro

- Jahreslagebericht 2021: 100 Seiten; Kosten für Agenturleistungen: Layout, Satz, Lektorat: 31 463,60 Euro,
- Jahreslagebericht 2022: 116 Seiten; Kosten für Agenturleistungen: Layout, Satz, Lektorat: 55 941,90 Euro,
- Jahreslagebericht 2023: 96 Seiten; Kosten für Agenturleistungen: Layout, Satz, Lektorat: 66 556,70 Euro,
- Jahreslagebericht 2024: 114 Seiten; Kosten für Agenturleistungen: Layout, Satz, Lektorat: 58 220,75 Euro.

9. Ist es geplant, den Berichtstext aufgrund des mit nur geringem Aufwand änderbaren Onlineformats dynamisch fortzuschreiben bis zur Erstellung des nächstjährigen Lageberichts?

Der „Bericht zur Lage der IT-Sicherheit in Deutschland“ ist ein Jahresbericht (vgl. § 58 Absatz 2 i. V. m. § 13 Absatz 2 BSIG) und somit ein abgeschlossenes Format.

10. Ist der Lagebericht 2025 für einen spezifischen Adressatenkreis formuliert, z. B. Wissenschaft, Wirtschaft, Verbraucher, und unterscheidet er sich darin von früheren BSI-Lageberichten?

Der Bericht dient gemäß § 58 Absatz 2 i. V. m. § 13 Absatz 2 BSIG zur Unterrichtung der Öffentlichkeit und ist nicht an einen spezifischen Adressatenkreis gerichtet.

11. Welche Initiativen werden von der Bundesregierung ergriffen oder sind in Planung, um der Einschätzung des Berichts nachzukommen, im Jahr 2026 sei der Schutz der Angriffsflächen das entscheidende Element für die Verbesserung der Cybersicherheit in Deutschland (vgl. Vorbemerkung der Fragesteller)?

Durch die zentrale Einführung eines „CISO Bund“ und das Aufsetzen entsprechender Prozesse erfolgt eine Stärkung der Cybersicherheit der Bundesverwaltung insgesamt. Dies wird sich auch positiv auf den Schutz der Angriffsflächen auswirken.

12. Welche Initiativen werden von der Bundesregierung ggf. ergriffen oder sind in Planung, um der Einschätzung des Berichts nachzukommen, Vorgaben für die Cyberresilienz der Institutionen, die die politische Willensbildung in Deutschland tragen, sollten dringend gesetzlich geregelt werden (vgl. Vorbemerkung der Fragesteller)?

Die Regelung von Vorgaben für die Cyberresilienz in Institutionen, die die politische Willensbildung in Deutschland tragen (wie etwa der Deutsche Bundestag), obliegt deren eigener Zuständigkeit.

13. Wie ist die Ankündigung des Bundesinnenministers zu verstehen, rechtliche Grundlagen dafür zu schaffen, digitale Infrastruktur von Angreifern auch außerhalb der Bundesrepublik Deutschland zerstören zu können, ohne dass es sich dabei um einen Hackback handele (vgl. Vorbemerkung der Fragesteller)?
 - a) Ist die Bezugnahme auf die Gefahrenabwehr als Ankündigung weiterer Befugnisse für Bundespolizei und BSI zu verstehen?
 - b) Werden die angekündigten gesetzlichen Grundlagen auch in das Grundgesetz eingreifen?
 - c) Wann ist mit einer entsprechenden parlamentarischen Initiative zu rechnen?

Die Fragen 13 bis 13c werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Das Bundesministerium des Innern erarbeitet derzeit einen Gesetzentwurf, um die Möglichkeiten der Sicherheitsbehörden des Bundes und des BSI zu stärken,

so dass schwerwiegende Angriffe besser erkannt und unterbunden werden können. Die konkreten Inhalte werden noch Gegenstand der Meinungsbildung der Bundesregierung sein. Die Willensbildung der Regierung gehört zum Kernbereich exekutiver Eigenverantwortung. Über das einleitend Gesagte hinaus nimmt die Bundesregierung daher zu dem laufenden Gesetzgebungsverfahren keine Stellung.

