

Kleine Anfrage

der Abgeordneten Steffen Janich, Dr. Bernd Baumann, Erhard Brucker, Dr. Gottfried Curio, Christopher Drößler, Jochen Haug, Martin Hess, Sascha Lensing, Markus Matzerath, Arne Raue, Dr. Christian Wirth und der Fraktion der AfD

Lagebericht 2025 des Bundesamtes für Sicherheit in der Informationstechnik

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%2003%20Prozent%2020%20Millionen%20z%203%20Prozent%2014%20Millionen%20als%20Gro%C3%20Prozent%209%20Unternehmen%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%20) 2,6 Millionen 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 Verarbeitenden 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 suboptimales 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/>).

Wir fragen die Bundesregierung:

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?
 - a) Inwieweit steht die Erläuterung zum Säulendiagramm, dass es sich bei Deutschland und Großbritannien um zwei westeuropäische Länder handele, 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?
 - 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?
 - 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?
 - e) Sind an der Erstellung des Lageberichts ausschließlich IT-Experten oder auch Politik- und Wirtschaftswissenschaftlicher beteiligt?
 - f) Welche konkreten geopolitischen Initiativen oder Positionierungen der Bundesregierung führen nach Erkenntnissen des BSI zu der beschriebenen angespannten IT-Sicherheitslage in Deutschland?

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?
 - c) Aus welchen Gründen existieren im Jahr 2025 überhaupt noch veraltete, nicht aktualisierte Systeme der Web-Angriffsfläche der Bundesverwaltung?
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/gefahrdungslage-der-kleinen-und-mittleren-unternehmen/>)?
 - 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)?
 - b) Liegen der Bundesregierung Kenntnisse über die Branchenzugehörigkeiten dieser „KMU“ vor, und wenn ja, welche?
 - 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?
 - 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.)?
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?
 - a) Ist dieser Trend quantifizierbar, und wenn ja, aus welchen Gründen wurde kein entsprechendes Diagramm für diesen Zusammenhang erstellt?
 - 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/)?

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-oeffentlicher-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“?
 - b) Ist die Aussage des Berichts, bei DDoS-Angriffen handele es sich um ein „beliebtes“ Werkzeug für Cyberhactivismus 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 Cyberhaktivisten zurückzuführen?
 - c) Aus welchem Grund wird als einziges Beispiel für Cyberhactivismus die russische Gruppe NoName057(16) vorgestellt, und welchen Anteil haben nach Erkenntnis der Bundesregierung umwelt-, religiös- oder sozioökonomisch motivierte deutsche Haktivistengruppen an Cyberangriffen in Deutschland?
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?
7. Aus welchen Gründen wurde auf die Erstellung eines vollumfänglichen PDF-Formats zusätzlich zur Lageberichtwebsite verzichtet?
8. Wie hoch waren die Kosten für die Erstellung der Website zum Lagebericht 2025?
 - 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?
 - c) Wie hoch waren die Kosten für die Erstellung der Lageberichte der Jahre 2020 bis 2024, und welchen Umfang hatten diese Berichte jeweils?
9. Ist es geplant, den Berichtstext aufgrund des mit nur geringem Aufwand änderbaren Onlineformats dynamisch fortzuschreiben bis zur Erstellung des nächstjährigen Lageberichts?
10. Ist der Lagebericht 2025 für einen spezifischen Adressatenkreis formuliert, z. B. Wissenschaft, Wirtschaft, Verbraucher, und unterscheidet er sich darin von früheren BSI-Lageberichten?
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)?
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)?

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?

Berlin, den 8. Dezember 2025

Dr. Alice Weidel, Tino Chrupalla und Fraktion

