Deutscher Bundestag **Drucksache 21/8046**

21. Wahlperiode 16.09.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Ruben Rupp, Robin Jünger, Alexander Arpaschi, weiterer Abgeordneter und der Fraktion der AfD – Drucksache 21/7844 –

Zu existenzbedrohenden Cyberangriffen auf deutsche Unternehmen

Vorbemerkung der Fragesteller

Die Bedrohungslage für die deutsche Wirtschaft, speziell den Mittelstand, durch Cyberangriffe hat offenbar eine neue existenzbedrohende Qualität erreicht. Wie aktuelle Medienberichte belegen, musste das Traditionsunternehmen ZEGO Textilveredelungszentrum aus Aschaffenburg Insolvenz anmelden, nachdem ein Cyberangriff Ende März 2026 die Produktion für fast sechs Wochen vollständig lahmgelegt hatte (vgl. www.t-online.de/finanzen/aktuelles/wirtschaft/id_101335202/insolvenz-textil-firma-aus-deutschland-wegen-eines-cyberangriff-insolvent.html). Dieser Fall ist beileibe kein Einzelfall; auch der Mittelständler Fasana, ein Serviettenhersteller aus Euskirchen, geriet infolge massiver Hackerattacken in eine schwere finanzielle Schieflage (ebd.).

Laut den Daten des Branchenverbands Bitkom von 2024 sind acht von zehn Unternehmen in Deutschland von Cyberangriffen betroffen, wobei der jährliche Gesamtschaden für die deutsche Wirtschaft auf rund 267 Mrd. Euro geschätzt wird (vgl. www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf). Besonders Ransomware-Attacken und DDoS-Angriffe (DDoS = Distributed Denial-of-Service) führen immer häufiger zu langwierigen Betriebsausfällen, die gerade für den kapitalgebundenen Mittelstand oft nur schwer zu kompensieren sind (ebd.).

Aus Sicht der Fragesteller ist es von großer Bedeutung, ob in Ergänzung der unternehmensinternen Mechanismen der IT-Sicherheit staatliche Schutzmechanismen zur Unterstützung angeboten werden, um das Rückgrat der deutschen Wirtschaft – den Mittelstand – wirksam vor den Folgen der digitalisierten Kriminalität zu schützen, Umsätze zu halten und Arbeitsplätze dauerhaft zu sichern. Dabei geht es den Fragestellern zum einen um ein möglichst detailliertes Lagebild, zum anderen um administrative Unterstützungsleistungen in einer zunehmend vernetzten und damit verwundbaren digitalen Wirtschaftswelt.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 16. September 2026 übermittelt.

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

1. Wie viele Cyberangriffe auf Unternehmen in Deutschland sind der Bundesregierung beziehungsweise den zuständigen Behörden (etwa dem Bundesamt für Sicherheit in der Informationstechnik [BSI] und dem Bundeskriminalamt [BKA]) seit 2022 zur Kenntnis gelangt (bitte nach Jahren und Unternehmensgröße aufschlüsseln)?

Die Polizeiliche Kriminalstatistik weist für die Jahre 2022 bis 2025 folgende Fallzahlen für Cybercrime-Delikte aus, bei denen der Handlungsort der Täter im Inland liegt:

2025:	136.034 Fälle
2024:	131.391 Fälle
2023:	134.407 Fälle
2022:	136.865 Fälle

Seit 2024 werden erstmals absolute Zahlen zu Fällen ausgewiesen, bei denen der Aufenthaltsort der Täter unbekannt ist oder diese sich nicht in Deutschland aufhalten, aber ein Schaden/Taterfolg in Deutschland eingetreten ist (sog. Auslandstaten). Für 2024 wurden hier 201.877 Fälle erfasst, sowie 207.888 Fälle für 2025. Eine dezidierte Aufschlüsselung dieser Fallzahlen nach Art des Geschädigten nach Unternehmen und Unternehmensgröße ist nicht möglich.

Da jedoch nicht alle Angriffe bei den zuständigen Behörden angezeigt werden, liegt die Dunkelziffer sehr wahrscheinlich deutlich höher.

2. Werden im Nationalen Cyber-Abwehrzentrum (vgl. www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum_node.html) versuchte und im Sinne des Angreifers erfolgreiche Cyberattacken auf deutsche Unternehmen seit 2022 dokumentiert und evaluiert, wenn ja, mit welchen Ergebnissen und welchen Konsequenzen, und wenn nein, warum nicht?

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) ist eine Kooperations-, Kommunikations- und Koordinationsplattform von deutschen (Sicherheits-)Behörden und weiteren Einrichtungen unterschiedlicher Ressorts, welche sich insbesondere mit Cybersachverhalten gesamtstaatlicher Relevanz befasst.

Das Cyber-AZ ist keine eigene Behörde. Zur Bewältigung von Sachverhalten mit (potenziell) gesamtstaatlicher Tragweite werden zwischen den Teilnehmern am Cyber-AZ die individuellen Behördenaktivitäten abgestimmt und koordiniert. Deren Umsetzung verbleibt weiterhin in der Zuständigkeit der jeweiligen Behörde bzw. Einrichtungen. Sollte zu der Umsetzung der Behördenaktivitäten auch gehören, dass Cyberattacken (z. B. auf deutsche Unternehmen) dokumentiert und evaluiert werden, so würde dies bei den jeweils zuständigen Behörden stattfinden.

3. Mit welchen Maßnahmen zum Schutz durch Aufklärung und Prävention tritt das BSI seit 2022 an Unternehmen heran, um deren bestehende Aktivitäten zur Cybersicherheit zu prüfen, zu bewerten und gegebenenfalls zu verstärken?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet vielfältige Informationsmaterialien zur Aufklärung und Prävention für Unternehmen an. Diese reichen von Broschüren, Vorträgen bei Branchenverbänden, Industrie- und Handelskammern und Handwerkskammern über Webinare bis hin zu Expertenkreisen, in denen sehr spezifische Fachthemen thematisiert werden.

Mit der Allianz für Cybersicherheit (ACS) organisiert und betreibt das BSI im Rahmen einer Public-Privat-Partnership die größte Cybersicherheitsinitiative Europas.

Im BSI kümmert sich ein eigenes Referat ausschließlich um die Belange kleiner und mittlerer Unternehmen (KMU). Um KMU zu unterstützen, wurde in Kooperation mit Partnern aus der Wirtschaft, Verbänden und dem Deutschen Institut für Normung (DIN) die DIN SPEC 27076 „IT-Sicherheitsberatung für kleine und Kleinstunternehmen“ und der darauf basierende CyberRisikoCheck entwickelt. Durch diesen können KMU bei IT-Dienstleistern eine standardisierte Beratung erhalten, die speziell auf ihre Bedürfnisse angepasst ist. In der DIN SPEC wurden auch die Handlungsempfehlungen für KMU standardisiert. Dadurch wissen sowohl Auftraggeber als auch Auftragnehmer, welche Leistung zu erwarten bzw. zu erbringen ist (siehe auch: www.cyberrisikocheck.de).

Um von NIS-2 betroffene Unternehmen bestmöglich zu unterstützen, bietet das BSI zahlreiche Informationspakete zu den einzelnen Pflichten und den Risikomanagementmaßnahmen an. Diese finden sich vereinfacht unter dem Hashtag #nis2know. Darüber hinaus werden gerade Angebote für die Positionsbestimmung des eigenen Unternehmens im Rahmen der Erreichung der NIS-2-Anforderungen sowie zur Nachweiserbringung in NIS-2-Verfahren erarbeitet.

4. Mit welchen Maßnahmen zum Schutz durch Aufklärung und Prävention tritt das BKA seit 2022 an Unternehmen heran, um deren bestehende Aktivitäten zur Cybersicherheit zu prüfen, zu bewerten und gegebenenfalls zu verstärken?

Das BSI ist als zentrale Cybersicherheitsbehörde des Bundes für die Sicherheit der Informationstechnik auch für den Bereich der Wirtschaft zuständig. Die Aufgabe der Prävention liegt demzufolge dort, wenngleich auch die Zentrale Ansprechstelle Cybercrime (ZAC) des BKA für Unternehmen der kritischen Infrastruktur (KRITIS) als Ansprechpartner zum Thema Cybercrime fungiert. Durch die ZAC werden Beratungsgespräche angeboten und Fachvorträge gehalten, um Unternehmen zu dem Thema Cybercrime zu informieren, mögliche Notfallpläne zu besprechen und Kontakte auszutauschen.

Die Initiative Wirtschaftsschutz ist ein vom Bundesministerium des Innern (BMI) koordinierter Zusammenschluss von Sicherheitsbehörden mit Spitzenwirtschafts- und Sicherheitsverbänden. Das BKA ist Teil dieser Initiative und beteiligt sich maßgeblich an den dort stattfindenden Präventionsmaßnahmen, wie dem regelmäßig stattfindenden Sicherheitsbriefings, dessen Schwerpunkt zuletzt auch Cybersicherheit war.

5. Liegen der Bundesregierung differenzierende Informationen zur Art der genannten Cyberangriffe – etwa DDoS-Attacken, Verschlüsselung der Daten in erpresserischer Absicht, Diebstahl sensibler Informationen, Identitätsdiebstahl oder Sabotage – vor (bitte ausführen)?

Differenzierende Informationen zur Art der Cyberangriffe liegen nur eingeschränkt vor. Die Deutsche Telekom AG konnte 2025 in ihren Netzen ca. 37.000 DDoS-Angriffe feststellen. Bezüglich der Verschlüsselung der Daten in erpresserischer Absicht (sog. Ransomware-Fälle) wurden dem Bundeskriminalamt 1.041 Fälle für 2025 gemeldet. Darüber hinaus weist die Polizeiliche Kriminalstatistik 2.292 Fälle für 2025 von Datenveränderung und Computersabotage aus, sowie 9.403 Fälle zum Tatbestand des Ausspähens von Daten.

6. In wie vielen Fällen führten die dokumentierten Angriffe nach Kenntnis der Bundesregierung zu einer zeitweisen Einstellung des Geschäftsbetriebs von mindestens einer Woche (bitte ausführen)?

Diese Informationen werden ausschließlich im Bereich der KRITIS-Meldungen strukturiert und damit auswertbar erfasst. Die diversen KRITIS-Unternehmen müssen aufgrund der Bedeutung ihrer Dienstleistung vielfältige Schutzvorkehrungen treffen. Dies wurde im Jahr 2016 mit dem IT-Sicherheitsgesetz insbesondere auch für die kommunalen Querverbunds-Unternehmen gesetzlich geregelt. Im genannten Zeitraum waren die diversen seitens des BSI und der Unternehmen ergriffenen Maßnahmen bereits wirksam und erfolgreich. Aufgrund der vielfältigen Maßnahmen kam es in keinem dieser Fälle zu einer entsprechend langen Einstellung des Geschäftsbetriebs.

7. Wie viele Fälle von Insolvenzen, bei denen seitens der betroffenen Unternehmen ein Cyberangriff als (Mit-)Ursache für die Zahlungsunfähigkeit angegeben wurde, sind der Bundesregierung seit 2022 bekannt geworden (bitte nach Branchen aufschlüsseln)?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

8. Mit welcher Summe beziffert die Bundesregierung den durch Cyberkriminalität entstandenen direkten wirtschaftlichen Schaden (etwa durch Lösegeldzahlungen oder Reparaturkosten) sowie den indirekten Schaden (etwa durch Produktionsausfall oder Reputationsverlust) speziell für den deutschen Mittelstand seit 2022?

Offizielle Studien (Bitkom e. V.) und der jährliche Wirtschaftsschutzbericht (BKA) beziffern die Gesamtschäden aufgrund von Cyberangriffen auf Basis verschiedener mess- und schätzbaren Faktoren. Eine Unterscheidung in indirekte/direkte Kosten erfolgt nicht.

2025:	202 Mrd. Euro
2024:	179 Mrd. Euro
2023:	148 Mrd. Euro
2022	203 Mrd. Euro

9. Welche konkreten Schutzlücken identifiziert die Bundesregierung derzeit bei Start-ups sowie bei kleinen und mittleren Unternehmen (KMU) im Vergleich zu besonders beobachteten Betreibern kritischer Infrastrukturen (KRITIS), und welche Maßnahmen werden durch welche Akteure ergriffen, um diese Lücken zu schließen?

Kleine und mittlere Unternehmen (KMU) als Innovationstreiber, „Hidden Champions“ und wichtige Teile der Lieferketten von KRITIS-Unternehmen verfügen häufig über nur unzureichende Ressourcen (Zeit, Geld, Personal) und haben daher meist keinen direkten Kontakt zu Sicherheitsbehörden und deren Leistungen. Daher weiten die Sicherheitsbehörden ihre Angebote – insbesondere zur Ansprache von gefährdeten KMU – in allen Bereichen aus.

Das BMI plant ein Modellprojekt zur Information und Beratung in sozialen Medien. Damit sollen die herkömmlichen Wege, wie Zusammenarbeit mit Verbänden, Nutzung bestehender Medien (Websites, Broschüren etc.) mit neuen, digitalen Zugangswegen mittels sozialer Medien (z. B. Xing, LinkedIn u. a.), KI-Chatbots oder (Online-)Veranstaltungen erprobt, analysiert und kombiniert

werden. Ziel ist es, auch solche Unternehmen zu erreichen, die noch keine Berührungspunkte mit Sicherheitsthemen haben und diese für den Wirtschaftsschutz zu sensibilisieren und in ihren Kompetenzen zu stärken.

Auch das BSI kennt die grundsätzlichen Bedarfe des Deutschen Mittelstandes. Wie bereits unter Frage 3 ausgeführt, wurden seitens des BSI explizite Angebote für KMU entwickelt, um das Thema Informationssicherheit ganzheitlich anzugehen.

Für diese Unternehmen braucht es verständliche Orientierung in einfacher Sprache und geeignete Sensibilisierung, um mehr in den Bereich der Informationssicherheit zu investieren. Das BSI verfügt hierzu über ein breites Angebot (www.bsi.bund.de/kmu).

10. In welchem Umfang nehmen Unternehmen nach Kenntnis der Bundesregierung bei einem laufenden Angriff die Hilfe staatlicher Stellen (etwa besonderer Einheiten des BSI) in Anspruch, und wie bewertet die Bundesregierung die Kapazitäten dieser Teams im Verhältnis zur Anzahl der Angriffe?

Das Bundesamt für Verfassungsschutz (BfV) befindet sich im Rahmen der Präventionsarbeit und Detektionsarbeit zu staatlich gesteuerten Cyberangriffen im vertrauensvollen Austausch mit verschiedenen Unternehmen, sowohl bilateral als auch im Rahmen von Formaten, an denen mehrere Unternehmen beteiligt sind. Die auf diese Weise etablierten Kontakte und die vertrauensvolle Zusammenarbeit führen auch zur Meldung von Cybervorfällen seitens der Unternehmen an das BfV. Die Unterstützung des BfV reicht dabei von beratender Tätigkeit bis hin zur Übermittlung von technischen Informationen, die zur Aufklärung und Mitigation von Angriffsaktivitäten geeignet sind. Diese Zusammenarbeit hat sich in den letzten Jahren verstetigt. Diesbezüglich wird auch auf die Ergebnisse der Studie „Wirtschaftsschutz 2026“ des Digitalverbandes Bitkom e. V. hingewiesen, die diese Entwicklung in der aktuellen Studie besonders hervorhebt.

Das BSI unterstützt betroffene Unternehmen bei der Abwehr von Cyberangriffen in herausgehobenen Fällen. Eine solche weitergehende Unterstützung wird aus Sicht der Bundesregierung regelmäßig nachgefragt. Die konkrete operative Unterstützung richtet sich dabei neben dem Bedarf des Betroffenen ebenso nach den zur Verfügung stehenden personellen Kapazitäten im entsprechenden Einsatzteam.

11. Welche Informationen liegen der Bundesregierung zur aktuellen Kooperation zwischen den Landeskriminalämtern, dem BKA und privaten IT-Sicherheitsdienstleistern im Falle von Erpressungsversuchen durch Ransomware vor (bitte ausführen)?

Der Bundesregierung liegen keine Informationen im Sinne der Fragestellung vor.

12. Existieren aktuell präventive Förderprogramme des Bundes spezifisch für Start-ups und KMU zur Härtung ihrer IT-Infrastruktur, und wenn ja, wie hoch waren die Abrufquoten dieser Mittel seit 2022?

Die Bundesregierung prüft regelmäßig, welche Maßnahmen notwendig und umsetzbar sind, um die Cybersicherheit in Deutschland insgesamt weiter zu verbessern. Aktuell erfolgt keine Direktförderung einzelner Unternehmen (sie-

he hierzu auch: www.mittelstand-digital.de/MD/Navigation/DE/Ueber-uns/foerderung/wie-wir-foerdern.html).

13. Plant die Bundesregierung steuerliche Anreize oder Sonderabschreibungsmöglichkeiten für Investitionen von Unternehmen in die Cyberresilienz, um die wirtschaftliche Belastung durch notwendige IT-Aufrüstungen abzufedern (bitte ausführen)?

Derzeit sind keine derartigen zusätzlichen steuerlichen Anreize oder Sonderabschreibungsmöglichkeiten für Investitionen von Unternehmen in die Cyber-Resilienz geplant. Die Bundesregierung hat jedoch mit der im Rahmen des Gesetzes für ein steuerliches Investitionssofortprogramm zur Stärkung des Wirtschaftsstandorts Deutschland vom 14. Juli 2025 (BGBl. I 2025, Nr. 161, S. 1–3) wiedereingeführten degressiven Abschreibung für bewegliche Wirtschaftsgüter bereits ein wirksames Instrument zur Förderung von Investitionen geschaffen. Die degressive Abschreibung kommt allen Unternehmen gleichermaßen zugute, ist unkompliziert in der Umsetzung und liefert damit eine Anreizwirkung in der Breite. Darüber hinaus bestehen durch den Investitionsabzugsbetrag und die Sonderabschreibung nach § 7g des Einkommensteuergesetzes weitere steuerliche Investitionsförderungen für kleine und mittlere Betriebe. Auch wurde der rasche technische Fortschritt bei der Bemessung der betriebsgewöhnlichen Nutzungsdauer für Computerhardware (einschließlich der dazu gehörenden Peripheriegeräte) sowie für die für die Dateneingabe und -verarbeitung erforderliche Betriebs- und Anwendersoftware bereits berücksichtigt (vgl. BMF-Schreiben vom 22. Februar 2022, BStBl I 2022, S. 187).

14. Sieht die Bundesregierung die Notwendigkeit, eine zentrale Meldestelle für Cyberangriffe zu schaffen, die über die reine Statistik hinaus eine Soforthilfe-Koordination für Unternehmen, die keine kritischen Infrastrukturen betreiben, leistet (bitte begründen)?

Die Bundesregierung sieht aktuell keinen Bedarf für die Einrichtung einer zentralen Meldestelle. Die in den vorhergehenden Antworten beschriebenen Maßnahmen sind derzeit aus Sicht der Bundesregierung ausreichend.

15. Liegen der Bundesregierung Erkenntnisse über konkrete Muster vor, nach denen Cyberkriminelle gegen Unternehmen vorgehen, differenziert etwa nach Branchen, Unternehmensgröße, langen Lieferketten und Umsatz (bitte ausführen)?

Cyberkriminelle verwenden eine große Vielzahl von Angriffsmethoden, die sich gegen verschiedene Branchen und Unternehmen richten. Das Nicht-Vorhandensein spezifischer Muster für einzelne Zielbranchen bedeutet hierbei, dass grundsätzlich jede Branche und jede Unternehmensgröße durch jeden Modus Operandi betroffen sein kann.

Erfolgreiche Angreifer passen ihren Angriff entweder spezifisch auf das Unternehmen und dessen Infrastruktur an oder aber greifen eine möglichst große Zahl von Unternehmen mit dem identischen Angriffsmuster an und bauen darauf, dass unter dieser hohen Menge hinreichend viele verwundbar sind. Cyberkriminelle gehen oftmals arbeitsteilig und kostenoptimiert vor. Je weniger Schutzmaßnahmen ein Unternehmen bereits umgesetzt hat, desto wahrscheinlicher wird es Opfer eines erfolgreichen Angriffs. Oftmals werden Einfallstore verwendet, die mit einfachen Mitteln hätten geschlossen werden können (z. B. nicht installierte Updates, schlechtes Passwortmanagement). Angreifer-Grup-

pen mit höherwertigen Fertigkeiten (APT-Gruppen) wählen teilweise den Weg über schlecht geschützte Unternehmen der Lieferkette, um Unternehmen mit einem hohen Cybersicherheitsniveau anzugreifen.

16. Kann die Bundesregierung Angaben zu möglichen Motiven hinter den dokumentierten Cyberattacken machen, und in wie vielen Fällen führten die Ermittlungen der Strafverfolgungsbehörden zur Identifizierung konkret Beschuldigter (bitte ausführen)?

Die Täter hinter den hier verzeichneten Cyberangriffen handeln vor allem aus finanziellen, politischen oder hacktivistischen / ideologischen Motiven. Die Polizeiliche Kriminalstatistik (siehe auch Antwort zu Frage 1) weist auch Informationen zu den ermittelten Tatverdächtigen aus. Im Bereich Cybercrime wurden 2025 30.153 Tatverdächtige ermittelt, bei denen der Handlungsort der Täter im Inland liegt. Bei den Fällen, in denen der Handlungsort der Tatverdächtigen nicht im Inland verortet werden kann, wurden 3.871 Tatverdächtige ermittelt.

17. Liegen der Bundesregierung Erkenntnisse über eine mögliche Dunkelziffer nicht zur Anzeige gebrachter Cyberangriffe auf deutsche Unternehmen vor (bitte ausführen)?

Im gesamten Deliktsbereich Cybercrime liegt ein hohes Dunkelfeld vor, das in einer Studie des Kriminologischen Forschungsinstituts Niedersachsen aus 2020 auf bis zu 91,5 Prozent geschätzt wird. Von einem hohen Dunkelfeld muss weiterhin auch bei betroffenen Unternehmen ausgegangen werden.

18. Liegen der Bundesregierung Erkenntnisse darüber vor, dass durch den Einsatz von Künstlicher Intelligenz (KI) Cyberattacken auf deutsche Unternehmen seit 2022 an Quantität und Qualität zugenommen haben (bitte ausführen)?

Der Einfluss Künstlicher Intelligenz (KI) nimmt in allen Lebensbereichen zu, auch bei Cyberangriffen. Ein Anstieg der Fallzahlen von Cyberangriffen aufgrund des unterstützenden Einsatzes von KI ist wahrscheinlich. Die Sicherheitsbehörden beobachten, dass Angreifer verstärkt KI adaptieren, um Cyberangriffe effektiver und damit gefährlicher zu machen. Cyberakteure lassen sich bei der Entwicklung von Malware und dem Entwerfen von Phishing-Material von KI unterstützen. Auch experimentieren Angreifer mit dem Einsatz von KI-Agenten zur Automatisierung von Angriffsschritten. Der Einsatz von KI erfordert Ressourcen, Rechenpower bzw. Tokens von KI-Betreibern, diese sind zu einem attraktiven Ziel für Cyberangreifer geworden und werden aktiv von cyberkriminellen Services gehandelt. Der Nachweis für den Einsatz von KI-Methoden bei Cyberangriffen ist grundsätzlich schwierig. Eine direkte Kausalität zwischen dieser steigenden Anzahl von Angriffen und der kriminellen Nutzung von KI liegt bislang allerdings nicht vor.

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