Deutscher Bundestag **Drucksache 21/7844**

21. Wahlperiode 04.09.2026

Kleine Anfrage

der Abgeordneten Ruben Rupp, Robin Jünger, Alexander Arpaschi, Sebastian Maack, Tobias Ebenberger, Lars Haise, Edgar Naujok, Steffen Janich, Dr. Michael Kaufmann, Micha Fehre, Beatrix von Storch, Thomas Ladzinski, Ronald Gläser, Peter Bohnhof und der Fraktion der AfD

Zu existenzbedrohenden Cyberangriffen auf deutsche Unternehmen

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.

Wir fragen die Bundesregierung:

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)?

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?
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?
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?
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)?
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)?
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)?
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?
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?
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?
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)?
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?
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)?

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

Berlin, den 24. August 2026

Dr. Alice Weidel, Tino Chrupalla und Fraktion

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