Deutscher Bundestag **Drucksache 20/[…]**

20. Wahlperiode [Datum]

Antrag

der Fraktion der CDU/CSU

Cyberresilienz von KRITIS-Betreibern stärken – NIS-2 umsetzen

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Ganz gleich, ob Krankenhäuser, IT-Dienstleister oder Flughäfen: Die Anzahl folgenreicher Cybersicherheitsvorfälle häuft sich. Das Dominikus-Krankenhaus in Berlin-Reinickendorf musste zum Beispiel kürzlich die Notfallversorgung einstellen, weil Kriminelle die internen IT-Systeme mit Ransomware verschlüsselt hatten und Lösegeld forderten. Ein Angriff auf den Dienstleister Südwestfalen-IT legte mehrere Kommunen lahm. Eine sog. DDoS-Attacke sorgte Anfang 2023 dafür, dass Websites zahlreicher deutscher Flughäfen wegen Überlastung nicht erreichbar waren.

In Deutschland ist nach einer Auswertung des Bitkom fast jedes Unternehmen bereits mindestens einmal von Cyberkriminalität betroffen gewesen: 84 Prozent aller Unternehmen wurden 2022 erwiesenermaßen Opfer einer Cyberattacke, weitere neun Prozent gehen von einem Angriff aus. Das BSI weist in seinem Lagebericht für 2023 ähnliche und zum Teil noch besorgniserregendere Zahlen auf. So lag beispielsweise die tägliche Zunahme an neuen Schadprogramm-Varianten zwischen Juni 2022 und Juni 2023 bei circa 250.000. Der finanzielle Schaden von Cyberattacken soll sich dabei auf ca. 200 Mrd. Euro pro Jahr belaufen.

Die seit dem 16. Januar 2023 in Kraft getretene sog. NIS-2-Richtlinie (RL (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022) ist die konsequente Reaktion auf die zunehmende Bedrohungslage. Der bestehende Rechtsrahmen soll modernisiert werden, um mit der zunehmenden Digitalisierung und einer sich verschärfenden Cyberbedrohungslage Schritt zu halten. Die Mitgliedsstaaten sind verpflichtet, die NIS-2-Richtlinie bis zum 17. Oktober 2024 in nationales Recht umzusetzen – spätestens dann müssen Unternehmen auch entsprechende Maßnahmen ergriffen haben.

Nach Medieninformationen ist jedoch bereits absehbar, dass die Bundesregierung die von der EU gesetzte Umsetzungsfrist zum 17. Oktober 2024 nicht einhalten wird. Entsprechend hatte sich auch der Parlamentarische Staatssekretär Saathoff in der Innenausschusssitzung am 15. Mai 2024 eingelassen.

Diese in der alleinigen Verantwortung der Bundesregierung liegende Verzögerung ist eine zusätzliche Belastung für die Betreiber kritischer Infrastrukturen und setzt die deutsche Infrastruktur unkalkulierbaren Sicherheitsrisiken aus. Bis heute ist weder absehbar, welche Unternehmen bzw. Betreiber überhaupt dem sachlichen Anwendungsbereich unterfallen, noch ist klar, wie die inhaltlichen Anforderungen konkret ausgestaltet sein werden. Insbesondere kleine und mittelständische sowie kommunale Unternehmen müssen aufgrund noch unklarer Vorgaben

und dem ohnehin bestehenden Fachkräftemangel im IT-Sektor mit übermäßigen Herausforderungen und Risiken für die Geschäftspraxis rechnen.

Das Vorgehen der Bundesregierung bei der Umsetzung der NIS-2-Richtlinie ist gerade mit Blick auf die grundlegend geänderte Sicherheitslage seit dem völkerrechtswidrigen russischen Angriff auf die Ukraine am 24. Februar 2022 völlig unverständlich und geradezu fahrlässig. Längst richtet sich die hybride Kriegsführung Russlands im analogen wie auch im Cyberraum auch gegen Deutschland und hier ansässige Unternehmen. Umso dringlicher ist es, durch eine konsequente, transparente und verständliche Implementierung von Cybersicherheitsanforderungen das Cybersicherheitsniveau des Industrie- und Innovationsstandorts Deutschland erheblich zu steigern. Deutschland würde dadurch insgesamt deutlich an Resilienz gewinnen – ein dringend notwendiger Schritt.

Wir werden dieses Ziel aber nur dann erreichen, wenn die Verpflichtungen praxisnah, vollkommen digital und möglichst unbürokratisch umgesetzt werden können. Mithin dürfen keine Doppelstrukturen der Behörden entstehen, welche die KRITIS-Betreiber mit überbordender Bürokratie zusätzlich belastet. In Anbetracht der sehr knappen Umsetzungsfrist bis Oktober 2024 und des Mangels an IT-Fachkräften ist es daher essenziell, dass die Bundesregierung schnellstmöglich den notwendigen regierungsintern abgestimmten Gesetzentwurf vorlegt. Damit würden auch die Rechtsunsicherheiten mit Blick auf eine mögliche unmittelbare Anwendbarkeit der Richtlinie nach Ablauf der Umsetzungsfrist reduziert.

Auch die hohe Dunkelziffer bei Cyberangriffen auf KRITIS-Betreiber muss praxisorientiert angegangen werden. Die Bundesregierung muss das Bundesamt für Sicherheit in der Informationstechnik (BSI) dazu in die Lage versetzen, ein tagesaktuelles Lagebild zur Cybersicherheit erstellen zu können. Dies könnte KRITIS-Betreiber mit relevanten Informationen zu Sicherheitsvorfällen versorgen. Ein solches Lagebild wäre für die Betreiber ein echter Mehrwert und lieferte einen Anreiz, selbst mögliche Vorfälle zu melden.

Für alle, die potenziell unter den Anwendungsbereich von NIS-2 fallen, ist es unerlässlich, sich damit endlich konkret und auf verlässlicher gesetzlicher Basis auseinandersetzen zu können. Diese Verlässlichkeit ist umso wichtiger, da im Zuge der NIS-2-Umsetzung auf viele Unternehmen zusätzliche Kosten zukommen werden.

II. Der Deutsche Bundestag fordert die Bundesregierung daher im Rahmen der zur Verfügung stehenden Haushaltsmittel auf:

1. Unverzüglich einen innerhalb der gesamten Bundesregierung abgestimmten Gesetzentwurf zur Umsetzung der NIS-2-Richtlinie vorzulegen, damit das Gesetzgebungsverfahren bis zur Umsetzungsfrist am 17. Oktober 2024 abgeschlossen werden kann und KRITIS-Betreiber Planungssicherheit erhalten;

2. gezielte Schulungen, Beratungen und Übungen für die betroffenen KRITIS-Betreiber zur Verfügung zu stellen sowie unverzüglich eine Anlaufstelle für Umsetzungsfragen einzurichten;

3. dem BSI die Ressourcen zur Erstellung eines tagesaktuellen Cybersicherheitslagebilds zur Verfügung zu stellen, welches die Betreiber von KRITIS tagesaktuell und als Mehrwert für den eigenen Meldeaufwand mit Informationen zu Cybersicherheitsvorfällen versorgt;

4. bei der Umsetzung der NIS-2-Richtlinie eine Kohärenz mit dem KRITIS-Dachgesetz zu schaffen und insbesondere beim Meldewesen Doppelstrukturen der Behörden (BSI, BBK und andere Aufsichtsbehörden wie BaFin, BNetzA, etc.) zu vermeiden;

5. KRITIS-Betreibern die Möglichkeit zu geben, ihren Melde- und Registrierungspflichten vollkommen digital nachkommen zu können;

6. beim NIS-2 Umsetzungsgesetz eine grundlegende Harmonisierung mit weiteren Sicherheitsgesetzen (bspw. Bundes-Immissionsschutzgesetz (BImSchG), Gesetz über überwachungsbedürftige Anlagen (ÜAnlG), Energiewirtschaftsgesetz (EnWG), DVOs in der Luftsicherheit) herbeizuführen, um Doppelzuständigkeiten und überbordende Bürokratie für KRITIS-Betreiber zu vermeiden;
7. im Rahmen der Umsetzung der NIS-2-Richtlinie auch den Aspekt der personellen Sicherheit gleichwertig zu berücksichtigen und hierfür die Möglichkeit zur Schaffung einer freiwilligen Zuverlässigkeits-/Vertrauenswürdigkeitsüberprüfung von Mitarbeitern in KRITIS-Bereichen analog der Geheimschutz-Überprüfung zu implementieren;
8. Ressourcen für regelmäßige gemeinsame länderübergreifende Übungen - auch mit kleinen und wechselnden KRITIS-Betreibern - im Hinblick auf den Schutz vor Cybersicherheitsvorfällen zur Verfügung zu stellen;
9. schnellstmöglich in Gespräche mit den betroffenen Verbänden darüber einzutreten, wie die Cybersicherheit von KRITIS-Betreibern in all ihren Aspekten und vor allem mit vorhandenen Mitteln und Fachkräften gewährleistet werden kann; über das Ergebnis dieser Gespräche soll der Deutsche Bundestag unverzüglich informiert werden;
10. den Digitalcheck um das Prinzip der Cyberresilienz von Regelungsvorhaben zu erweitern;
11. umgehend in Gespräche mit den Bundesländern darüber einzutreten, wie die Kompetenzen zwischen Bundes- und Landesbehörden bei der Umsetzung der NIS-2 Richtlinie überlappungsfrei zu regeln und zu überprüfen sind;
12. in Abstimmung mit den Bundesländern und Kommunen eine verbindliche zeitliche Regelung zu treffen, wann auch die vom Umsetzungsgesetz ausgenommenen Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene die Regeln und Standards der NIS-2 Richtlinie erfüllen und umsetzen müssen;
13. die NIS-2 Richtlinie eins zu eins in nationales Recht auf eine einheitliche Rechtsanwendung innerhalb der EU hinzuwirken;
14. den Erfüllungsaufwand für international agierende KRITIS-Betreiber zu reduzieren indem - ohne die Cyberresilienz zu schwächen - auf international anerkannte Standards gesetzt und auf nationale Anforderungen verzichtet wird, die nicht EU-weit anerkannt werden und über ein hinreichendes Mindestschutz-Niveau hinausgehen;
15. in Abstimmung mit den weiteren EU-Mitgliedsstaaten sicherzustellen, dass europaweit agierende Unternehmen nur in einem Mitgliedsstaat gebündelt für die gesamte EU ihren Nachweis-, Melde- und Registrierungspflichten nachkommen müssen.

Berlin, den […]

Friedrich Merz, Alexander Dobrindt und Fraktion