

Cybersicherheit | 07.10.2026 | Nr. 319/26

Uta Wentzel: TOP 13: Aus Cyberangriffen lernen und den Schutz verbessern

Es gilt das gesprochene Wort!

Sehr geehrte Frau Präsidentin, sehr geehrte Damen und Herren,

ein schwerer Cyberangriff ist nicht vorbei, nur weil die Systeme wieder laufen. Wenn Server wieder erreichbar sind, Daten hoffentlich wiederhergestellt werden konnten und der unmittelbare Schaden begrenzt wurde, beginnt eine zweite, ebenso wichtige Aufgabe: Wir müssen verstehen, warum der Angriff erfolgreich war – und was wir daraus für die Zukunft lernen, um unsere Systeme besser zu schützen.

Genau darum geht es in unserem gemeinsamen Antrag. Denn die Bedrohung durch Cybercrime in Deutschland bleibt auf hohem Niveau. Deutschland zählt als drittgrößte Volkswirtschaft der Welt weiterhin zu den wichtigsten Angriffszielen im Cyberraum. Besonders schwere Cyberdelikte sowie Angriffe auf Unternehmen, Behörden und kritische Infrastrukturen nehmen weiter zu.

Das geschätzte Schadensvolumen für die deutsche Wirtschaft liegt laut des Bundeskriminalamtes bei 202,4 Milliarden Euro jährlich und entspricht damit rund 4,5 Prozent des Bruttoinlandsprodukts.

Bitkom addierte in der Wirtschaftsschutz-Studie 2025 analoge Schäden hinzu und kommt sogar auf ein Schadensvolumen von 289,2 Milliarden Euro. Das deutsche Cybercrime-Lagebild 2025 erreichte ein neues Rekord-Niveau. 2025 wurden rund 335.000 Fälle von Cybercrime im engeren Sinne registriert. Etwa zwei Drittel der Taten wurden aus dem Ausland oder von unbekannten Tatorten aus begangen. Die tatsächliche Bedrohung dürfte allerdings aufgrund eines erheblichen Dunkelfeldes deutlich höher liegen. KI senkt die Einstiegshürden für Täter dramatisch. Die meisten Angriffe kommen weiterhin aus Russland und China. Es gilt also, unser Land besser zu schützen gegen diese Angriffe und Schaden von unserer Volkswirtschaft abzuwenden.

Deutschland verfügt bereits über starke Strukturen der Cybersicherheit: das BSI, CERT-Bund, das Nationale Cyber-Abwehrzentrum, Sicherheits- und Strafverfolgungsbehörden und die entsprechenden Strukturen der Länder. Auch Schleswig-Holstein stärkt seine Resilienz konsequent – mit dem IT-Sicherheitsschirm, dem Ausbau von CERT Nord zum CSIRT und einer noch engeren Zusammenarbeit mit dem BSI.

Aber diese Strukturen haben vor allem die Aufgabe, Gefahren zu erkennen, Angriffe abzuwehren, Schäden zu begrenzen und Täter zu verfolgen.

Eine andere Frage stand bislang nicht genug im Fokus: Wie werten wir besonders schwerwiegende Cybervorfälle unabhängig und systematisch aus? Wie identifizieren wir nicht nur die konkrete Schwachstelle, sondern auch strukturelle Ursachen und Wirkzusammenhänge? Und vor allem: Wie sorgen wir dafür, dass die daraus gewonnenen Erkenntnisse allen zugutekommen?

Andere sicherheitsrelevante Bereiche zeigen uns seit langem, welchen Wert eine solche Lernkultur hat. Nach schweren Ereignissen in der Luftfahrt, im Schienenverkehr oder in der Schifffahrt wird unabhängig untersucht – nicht, um vorschnell Schuldige zu benennen, sondern um das Gesamtsystem sicherer zu machen.

Australien hat diesen Gedanken inzwischen auf die Cybersicherheit übertragen. Ein unabhängiges Cyber Incident Review Board führt dort sogenannte No-Fault-Reviews bedeutender Cybervorfälle durch und entwickelt daraus konkrete Empfehlungen für Staat und Wirtschaft.

Wir wollen prüfen, wie ein solcher Ansatz auch Deutschland stärker machen kann – eingebettet in die bestehende Sicherheitsarchitektur und im Kontext des geplanten Cyberdomes. Es geht ausdrücklich nicht darum, eine weitere operative Behörde neben bestehende Strukturen zu setzen. Es geht darum, eine Lücke zu schließen: zwischen akuter Gefahrenabwehr und langfristigem, institutionellem Lernen.

Dabei müssen klare Voraussetzungen gelten: Unabhängigkeit, der Schutz sensibler und klassifizierter Informationen, die Einbindung von Wissenschaft, Wirtschaft, Verwaltung und Sicherheitsbehörden – und ein klarer Mehrwert gegenüber bestehenden Strukturen.

Schleswig-Holstein kann dazu etwas beitragen. Wir verfügen im Land über kurze Wege und vernetzte Kompetenzen in Verwaltung, Wissenschaft, Wirtschaft und Cybersicherheit. Diese Expertise sollten wir in einen nationalen Lernprozess einbringen. Denn Cyberangriffe halten sich weder an Ressortgrenzen noch an föderale Zuständigkeiten. Gerade deshalb müssen Bund und Länder ihre Erkenntnisse zusammenführen.

Auch Europa geht diesen Weg. Der Cyber Solidarity Act sieht bereits einen europäischen Mechanismus zur nachgelagerten Analyse bedeutender Cybervorfälle und zur Ableitung von Lessons Learned vor.

Liebe Kolleginnen und Kollegen, Cyberresilienz bedeutet deshalb mehr, als den nächsten Angriff abzuwehren. Ein handlungsfähiger Staat sollte aus jedem schweren Vorfall lernen und dieses Wissen konsequent in besseren Schutz übersetzen. Genau diese Lernfähigkeit wollen wir stärken.