Cybersicherheit: Wie Wirtschaft und Staat jetzt handeln müssen

Wettbewerbsfähig und handlungsfähig durch starke Cyberresilienz

Cybersicherheit ist längst keine technische Detailfrage mehr. Sie ist zu einer strategischen Herausforderung für die wirtschaftliche Stabilität, die staatliche Handlungsfähigkeit und den gesellschaftlichen Zusammenhalt geworden. Die Bedrohungslage ist dramatisch: In Deutschland verursachen Cyberangriffe jährlich Schäden in Höhe von rund 290 Milliarden Euro. Betroffen sind längst nicht mehr nur große Konzerne oder sicherheitsrelevante Einrichtungen. Immer häufiger geraten kleine und mittlere Unternehmen, Kommunen und gemeinnützige Organisationen ins Visier. Mehr als zwei erfolgreiche digitale Angriffe auf deutsche Kommunen werden jeden Monat verzeichnet. Die Frage ist längst nicht mehr, ob Cyberangriffe stattfinden, sondern wie wir sie erfolgreich abwehren können.

Die Risiken reichen weit: Fällt in Kommunen die IT aus, können Bau- und Betriebsgenehmigungen nicht erteilt und öffentliche Ausschreibungen nicht durchgeführt werden. Dadurch verzögern sich Investitionen, Unternehmen verlieren Planungssicherheit und die wirtschaftliche Entwicklung einer ganzen Region gerät ins Stocken. Ein Datenleck in einem kleinen Zulieferbetrieb kann hochsensible Verteidigungsprojekte gefährden und globale Folgen auslösen. Und ein Angriff auf Energie- oder Abfallwirtschaft bedroht unmittelbar die öffentliche Versorgung. Deutschland und Europa stehen damit vor einem Paradigmenwechsel: Cybersicherheit muss als Grundpfeiler der Daseinsvorsorge begriffen werden – gleichrangig mit Energie- oder Gesundheitsversorgung.

EXECUTIVE SUMMARY

Cyberangriffe verursachen in Deutschland jedes Jahr Schäden von über 200 Milliarden Euro. Sie legen nicht nur Unternehmen lahm, sondern treffen auch Universitäten und Kommunen – mit gravierenden Folgen für die Wirtschaft: Genehmigungen können nicht erteilt, Investitionen nicht umgesetzt und Projekte nicht gestartet werden. Deutschland hat die Umsetzungsfrist der NIS-2-Richtlinie verpasst und riskiert mit nationalen Sonderwegen zusätzliche Unsicherheiten. Entscheidend ist eine schnelle und einheitliche Umsetzung, die auch die öffentliche Verwaltung einschließt.

Aus Sicht der Unternehmen sind insbesondere folgende Maßnahmen entscheidend:

- Cybersicherheit als Teil der Daseinsvorsorge mit Mindeststandards und Förderung verankern.
- Das BSI zu einer echten Zentralstelle für IT-Sicherheit ausbauen.
- NIS-2 und CER ohne nationale Sonderwege umsetzen – auch für Behörden.
- Regulierungen harmonisieren, um Doppelbelastungen zu vermeiden.
- Lieferketten besser absichern und verteidigungsrelevante Daten besonders schützen.
- Europäische digitale Souveränität stärken und neue Schwachstellen verhindern.

HERAUSFORDERUNG

Die ökonomische Schadensbilanz ist gravierend. Cyberangriffe führen nicht nur zu direkten finanziellen Verlusten, sondern auch zu gestohlenem geistigem Eigentum, blockierten Produktionsprozessen und nachhaltigen Reputationsschäden. Mit jährlich über 200 Milliarden Euro Schaden gehören Cyberangriffe zu den größten gesamtwirtschaftlichen Bedrohungen unserer Zeit.

Hinzu kommt ein strukturelles Problem: Kompetenzen sind in Deutschland zwar vorhanden, aber auf zahlreiche Institutionen verteilt. Der Informationsaustausch funktioniert unzureichend, insbesondere zwischen Bund, Ländern und Kommunen. Gerade die kommunale Ebene ist trotz hoher Angriffswahrscheinlichkeit institutionell kaum eingebunden und hat bisher weder die Ressourcen noch die Ansprechpartner, die im Ernstfall nötig wären. Ein weiteres Problemfeld sind die Lieferketten. Nahezu jedes Unternehmen ist Teil komplexer globaler Wertschöpfungsnetze. Schwachstellen an einem einzigen Glied können ganze Branchen gefährden. Lücken in der Informationsweitergabe erhöhen die Risiken für die gesamte Wirtschaft.

Auch die politische Umsetzung von Sicherheitsvorgaben ist unzureichend. Die NIS-2-Richtlinie soll europaweit ein hohes Sicherheitsniveau schaffen, doch Deutschland hat die Frist verschlafen und läuft nun Gefahr, mit einem unambitionierten und kurzsichtigen Gesetz den eigentlichen Zweck zu unterlaufen. Dass die öffentliche Verwaltung weitestgehend von den Vorgaben ausgenommen wird, ist angesichts der Bedrohungslage nicht akzeptabel. Gerade Behörden sollten Vorreiter sein.

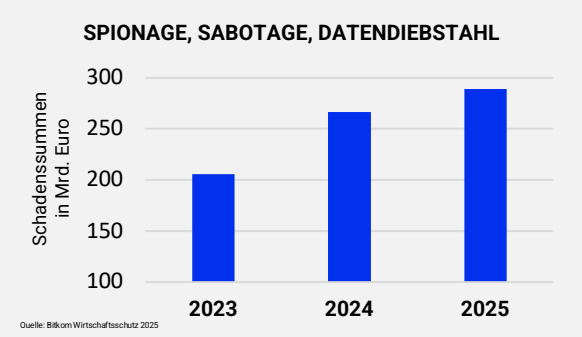
Neben der Umsetzung europäischer Vorgaben stellt sich die grundsätzliche Frage der digitalen Souveränität. Heute stützt sich ein erheblicher Teil kritischer Dienste auf US-amerikanische Cloud- und Sicherheitsanbieter. Diese Lösungen sind technologisch oft führend und gewährleisten ein hohes Schutzniveau. Gleichzeitig können dadurch Abhängigkeiten entstehen, die in geopolitischen Krisen zu erheblichen Risiken führen können. Für Europa bedeutet das eine doppelte Aufgabe: Zum einen müssen eigene, leistungsfähige Lösungen für besonders sensible Bereiche genutzt werden – etwa für Daten der inneren und äußeren Sicherheit oder andere „strategic assets“. Hier ist es strategisch notwendig, die Daten im europäischen Rechtsraum zu halten und eigene Fähigkeiten zu stärken. Zum anderen darf die Nutzung internationaler Systeme nicht grundsätzlich in Frage gestellt werden. Für den Großteil der Daten – rund 95 Prozent – sind internationale Anbieter unproblematisch und können durch Partnerschaftliche Modelle und Air-Gap-Architekturen sogar besonders hohe Sicherheit bieten.

Wichtig ist daher eine Balance: Europa muss Abhängigkeiten durch gezielte Diversifizierung reduzieren und Schlüsselbereiche absichern, ohne sich durch ein „Europe Only“-Denken von der globalen technologischen Entwicklung abzuschneiden. Cybersicherheit ist nicht national oder rein europäisch möglich. Angriffe sind global vernetzt, und effektive Abwehr gelingt nur in enger internationaler Kooperation. Die Erfahrungen mit Palantir oder Huawei verdeutlichen, dass Europa technologische Leistungsfähigkeit und strategische Souveränität nicht als Gegensätze begreifen darf, sondern als komplementäre Ziele einer resilienten Digitalpolitik: Eigenständigkeit in hochsensiblen Bereichen, Offenheit für sichere internationale Lösungen.

Schließlich gibt es ein kulturelles Defizit. Cybersicherheit wird häufig als Kostenblock betrachtet, nicht als Investition in Stabilität und Wettbewerbsfähigkeit. Zudem fürchten viele Unternehmen Reputationsschäden und berichten daher nicht offen über Angriffe oder Schwachstellen. Diese Kultur der Kurzsichtigkeit und Verschwiegenheit verhindert das Lernen aus Vorfällen und schwächt die kollektive Resilienz.

PRAXIS BLICK

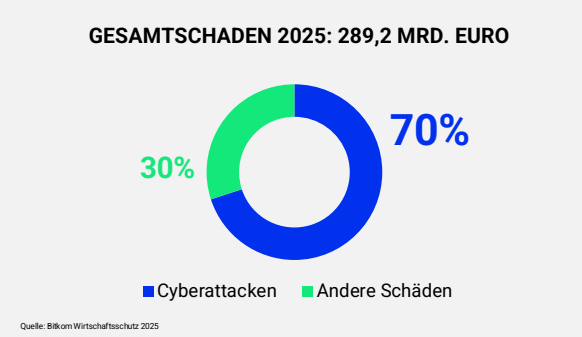
Die Realität zeigt, wie breit das Spektrum der Betroffenen ist – von Verteidigungsunternehmen über die öffentliche Verwaltung bis hin zur Industrieproduktion. So wurde Rheinmetall im April 2025 von einem massiven Datenleck getroffen, das militärisch hochsensible Informationen an die Öffentlichkeit brachte. Die Ursache lag mutmaßlich nicht im Konzern selbst, sondern bei einem Zulieferer – ein warnendes Beispiel für die Verwundbarkeit der nationalen Sicherheit durch globale Lieferketten.



Wie sehr diese Verwundbarkeit auch zentrale Infrastrukturen betrifft, zeigte sich kurz darauf bei einem Angriff auf den US-Systemanbieter Collins Aerospace. Durch eine Ransomware-Attacke kam es europaweit an mehreren großen Flughäfen zu erheblichen Störungen – betroffen waren unter anderem der BER, Brüssel, Dublin und London-Heathrow. Der Vorfall verdeutlichte nicht nur die Anfälligkeit globaler IT-Strukturen, sondern auch die wirtschaftlichen Risiken, die daraus entstehen können. Zugleich zeigte der Flughafen Münster/Osnabrück, wie erfolgreiche Cyberabwehr funktionieren kann: Dort reagierten die Verantwortlichen innerhalb von 30 Minuten, trennten den betroffenen Server vom Netz und stellten reibungslos auf einen autarken Betrieb um – klare Zuständigkeiten und Entscheidungswege verhinderten jegliche Auswirkungen auf den Flugbetrieb.

Dass Cybersicherheit längst kein „Nice-to-have“ mehr ist und ganze Branchen existenziell bedrohen kann, macht das Beispiel Jaguar Land Rover deutlich: Seit September steht die komplette Produktion still – verursacht durch eine Cyberattacke. Der Schaden wird auf rund 58 Millionen Euro pro Woche geschätzt und könnte sich insgesamt auf über eine Milliarde Euro summieren. Ohne Cyberversicherung muss das Unternehmen den Verlust selbst tragen und sah sich daher gezwungen mit staatlicher Unterstützung Kredite in Milliardenhöhe aufzunehmen. In akuter Gefahr ist auch das Zulieferernetzwerk mit rund 200.000 Beschäftigten, das nun ebenfalls staatliche Unterstützung fordert.

Es gibt jedoch auch positive Signale: viele Unternehmen verdeutlichen mit der Einrichtung einer CISO-Position als Stabsstelle der Unternehmensleitung, dass Cyber-Sicherheit Chefsache ist – ein Modell, das Schule machen sollte. Mit den Mittelstand-Digital-Zentren existieren zudem Anlaufstellen, die gerade kleinen und mittleren Unternehmen praxisnah zeigen, wie sich Risiken erkennen und abwehren lassen.



Jedoch bleibt auch die öffentliche Verwaltung nicht verschont: Anfang Oktober legte ein prorussisches Hacker-Kollektiv das zentrale Vergabeportal des Bundes über mehrere Tage lahm. Betroffen war damit eine der wichtigsten Schnittstellen zwischen Staat und Wirtschaft – täglich werden hier 30.000 öffentliche Aufträge veröffentlicht. Der Angriff führte zu einer erheblichen Störung laufender Vergabeverfahren. Der Vorfall zeigt, dass Cybersicherheit im öffentlichen Sektor nicht nur eine Frage staatlicher, sondern auch wirtschaftlicher Handlungsfähigkeit ist.

WAS TUN?

1. Cybersicherheit als Daseinsvorsorge verankern

Cybersicherheit muss als Teil der öffentlichen Daseinsvorsorge verstanden werden – ebenso unverzichtbar wie Energie- oder Wasserversorgung. Ihre wirksame Gewährleistung setzt eine enge Zusammenarbeit zwischen Privatwirtschaft und öffentlicher Verwaltung voraus. Dafür sind verbindliche Mindeststandards sowie eine gezielte Förderung notwendig, insbesondere für Kommunen und kleine Unternehmen. Der aktuelle Gesetzesentwurf der Bundesregierung greift jedoch deutlich zu kurz: Er überträgt die Verantwortung nahezu ausschließlich den Unternehmen, während der öffentliche Sektor infolge kurzsichtiger Sparmaßnahmen weitgehend außen vor bleibt.

2. Das BSI zur Zentralstelle ausbauen

Das Bundesamt für Sicherheit in der Informationstechnik sollte zur echten Zentralstelle für IT-Sicherheit weiterentwickelt werden. Der eingeschlagene Weg sollte hier konsequent weitgegangen werden. Es braucht klare Kompetenzen, bessere Ausstattung und die Fähigkeit, föderale Strukturen zu koordinieren und Angriffe zentral abzuwehren.

3. Öffentliche Verwaltung einbeziehen

Die öffentliche Verwaltung darf dabei nicht von strengeren Vorgaben ausgenommen werden, sondern muss Vorreiter sein. Daher sollten nicht nur Behörden des Bundes, sondern auch der Länder und Kommunen Risikomanagementmaßnahmen verpflichtend umsetzen müssen.

4. Lieferketten absichern

Unternehmen sind zunehmend über ihre Zulieferer angreifbar. Damit Sicherheitsrisiken frühzeitig erkannt werden können, braucht es klare Informations- und Meldepflichten entlang der Lieferkette. Nur wenn Zulieferer transparent über Schwachstellen und Vorfälle berichten, können Unternehmen rechtzeitig reagieren und ihre eigene Sicherheit gewährleisten.

5. Sicherheitsrelevante Daten besonders schützen

Die sensibelsten Informationen – etwa aus den Bereichen innere Sicherheit, Verteidigung und kritische Infrastruktur – müssen im europäischen Rechtsraum verbleiben. Hier gilt es, eigene technologische Fähigkeiten auszubauen und langfristig zu sichern. Europa muss strategisch in Cloud- und Sicherheitslösungen investieren, um Abhängigkeiten von Drittstaaten zu verringern. Dabei geht es nicht um Abschottung, sondern um gezielte Eigenständigkeit in Schlüsselbereichen – kombiniert mit internationaler Zusammenarbeit, wo sie die Sicherheit verbessert. Der Staat sollte dabei als Ankerkunde europäische Systeme frühzeitig beschaffen und so Markteintrittsbarrieren senken.

6. Stresstests einführen

Was im Finanzsektor längst Standard ist, muss auch auf kritische Bereiche der Realwirtschaft ausgeweitet werden. In besonders exponierten oder systemrelevanten Branchen sollten regelmäßige Penetrationstests nachweisen, dass die Cybersicherheitsabläufe im Falle eines Angriffs zuverlässig funktionieren.

7. Internationale Kooperation ausbauen

Cyberangriffe sind global vernetzt. Entsprechend müssen auch Abwehrstrategien international abgestimmt sein. Deutschland und Europa sollten deshalb stärker in internationale Kooperation investieren – von gemeinsamen Standards bis zu operativen Abwehrmechanismen.

8. Harmonisiert umsetzen

Die EU-Richtlinien sollten eins-zu-eins und ohne nationale Sonderwege umgesetzt werden, um europaweit einheitliche Rahmenbedingungen zu schaffen. NIS-2, CER, CRA und das KRITIS-Dachgesetz müssen dabei inhaltlich eng aufeinander abgestimmt werden, damit Unternehmen nicht mit widersprüchlichen Vorgaben oder mehrfachen Berichtspflichten belastet werden. Identische Definitionen zentraler Begrifflichkeiten sind entscheidend, um eine einheitliche Regulierung gewährleisten zu können. Ein kohärenter Ansatz reduziert Bürokratie, schafft Rechtssicherheit und ermöglicht es, Ressourcen auf tatsächliche Sicherheitsmaßnahmen, statt auf redundante Compliance-Prozesse zu konzentrieren.

9. Übergangsfristen für kritische Komponenten gewährleisten

Für Betreiber kritischer Infrastrukturen sind Übergangsfristen im Umgang mit kritischen Komponenten erforderlich, anstelle rückwirkender Verbote bereits verbauter Teile. Gleichzeitig braucht es klare und einheitliche Definitionen auf europäischer Ebene. Anstelle der vorgesehenen Einzelfallprüfungen sollte ein zentrales Register beim BMI eingerichtet werden, das vertrauenswürdige und nicht vertrauenswürdige Hersteller ausweist. Gerade für Branchen wie die Energiewirtschaft würde die Einzelfallprüfung einen unverhältnismäßigen bürokratischen Aufwand bedeuten.

10. Kulturwandel auch im Mittelstand etablieren

Eine gezielte Bewusstseinsbildung und eine neue Fehlerkultur sind zentral für effektive Cybersicherheit. Das BSI sollte daher eine breit angelegte Informationskampagne zu Cybergefahren starten, insbesondere für den Mittelstand. Ergänzend sollten die Mittelstand-Digital-Zentren weiter ausgebaut werden, um Unternehmen und Behörden praxisnah zu schulen. Ziel ist die Förderung einer Sicherheitskultur, in der über Vorfälle offen berichtet wird, damit Organisationen aus Erfahrungen lernen und präventiv handeln können.

WEITERFÜHRENDE INFOS

- Bitkom-Studie Wirtschaftsschutz 2025: https://www.bitkom.org/sites/main/files/2025-09/bitkom-pressekonferenz-wirtschaftsschutz-cybercrime.pdf

In den Kompetenzclustern entwickeln die Mitglieder der Wirtschaftsvereinigung aus den Unternehmen im Austausch mit der Politik in Themenfeldern fachliche Perspektiven.

KOMMEN SIE JEDERZEIT GERN AUF UNS ZU

Aus der Wirtschaft, mit der Politik: In den Kompetenzclustern entwickeln die Mitglieder der Wirtschaftsvereinigung der Grünen Perspektiven und Impulse. Diese müssen nicht in jedem einzelnen Fall mit den Positionen jedes einzelnen Mitglieds übereinstimmen. Mehr dazu hier.

Die Wirtschaftsvereinigung der Grünen e.V.
Dorotheenstr. 3, 10117 Berlin
Hauptgeschäftsführung:
Martin Kaul, Katharina Krüger (stellv.)

Referenten Innovation & Digitalisierung:
Christoph Busch, Leander Hérault, Alisa Gropper