Wo gesetzliche Regelungen aktuell unsere Resilienz schwächen

EWE-Kampagne „Resilienz“
Frühjahr 2026
Informationspapier Nummer 2

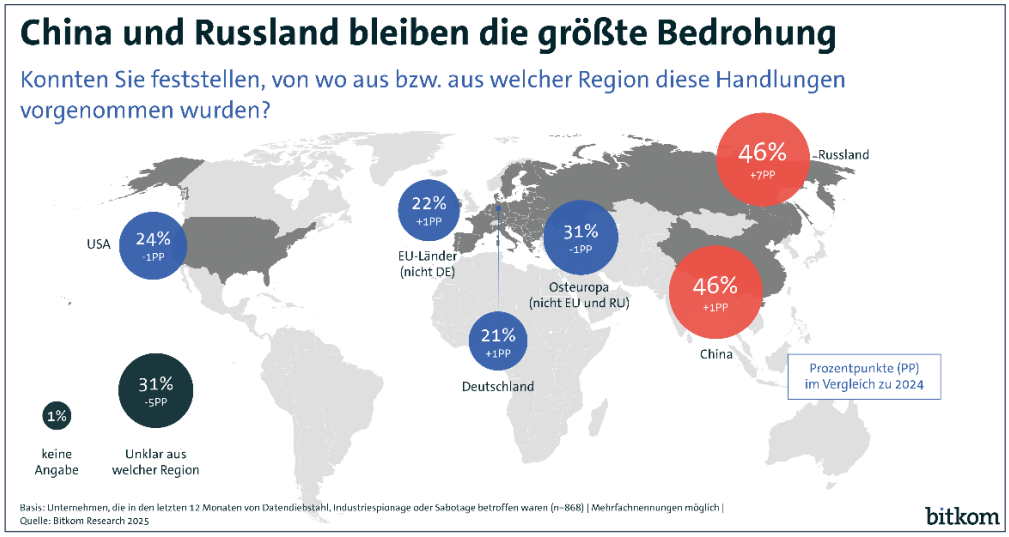
Oldenburg, 21. April 2026

Wo gesetzliche Regelungen aktuell unsere Resilienz schwächen

ALLGEMEIN

Cyberangriffe Überblick 2025

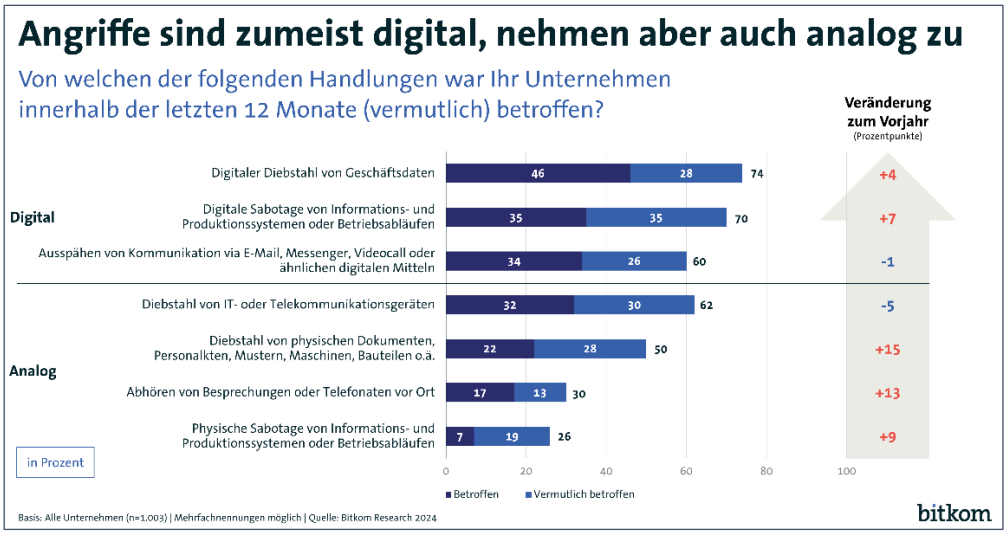
Deutschlands Sicherheitsdienste warnen: Cyberattacken auf deutsche Unternehmen, Einrichtungen und staatliche Stellen haben in den vergangenen Jahren massiv zugenommen. In ihrer im September 2025 vorgestellten Studie „Wirtschaftsschutz 2025“ gaben das Bundesamt für Verfassungsschutz (BfV) und der Branchenverband Bitkom einen Überblick.[1] Der Schaden durch Datendiebstahl, Industriespionage und Sabotage stieg auf 289 Milliarden Euro. Dabei führt die Spur immer öfter nach Osten – und zu ausländischen Geheimdiensten.



Erneut zugenommen haben Taten, die nach Russland und China zurückverfolgt werden konnten. Von den betroffenen Unternehmen haben 46 Prozent mindestens einen Angriff aus Russland (2024: 39 Prozent) festgestellt, ebenso viele aus China (2024: 45 Prozent). Mit deutlichem Abstand folgen Attacken aus Osteuropa außerhalb der EU (31 Prozent, 2024: 32 Prozent), aus den USA (24 Prozent, 2024: 25 Prozent), aus EU-Ländern (22 Prozent, 2024: 21 Prozent) sowie Deutschland (21 Prozent, 2024: 20 Prozent). Dabei nehmen ausländische Geheimdienste die deutsche Wirtschaft verstärkt ins Visier.

73 Prozent aller deutschen Unternehmen waren von digitaler Sabotage betroffen oder vermutlich betroffen. Bei 62 Prozent wurde digitale Kommunikation wie E-Mails oder Videokonferenzen sicher oder vermutlich ausgespäht. Zwei Dritteln (66 Prozent) wurden Geschäftsdaten gestohlen oder sie vermuten das. Den davon betroffenen Unternehmen entwendeten die Täter vor allem Kommunikationsdaten (69 Prozent), Kundendaten (57

[1] https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2025/2025-09-18-studie-bitkom.html



Prozent) sowie Finanzdaten (39 Prozent). Geistiges Eigentum wie Patente oder Informationen aus Forschung und Entwicklung flossen bei 29 Prozent der betroffenen Unternehmen ab, gefolgt von Zugangsdaten und Passwörtern (27 Prozent) sowie Daten von Beschäftigten (24 Prozent).

Beispiel 1 Rheinmetall

Hier zwei prominente Beispiele aus der jüngsten Vergangenheit: Am 4. April 2025 wird bekannt, dass eine mutmaßlich Russland nahestehende Hackergruppe Zugriff auf insgesamt 750 Gigabyte interne Daten des deutschen Rüstungskonzerns Rheinmetall erlangt hat.[2] Sie veröffentlichte dazu einen Link zum Download von 1400 Dokumenten und versicherte, im Besitz zahlreicher weiterer Dokumente zu sein. Bei den geleakten Dokumenten geht es um Panzer wie den Puma, Motoren, Computer und um mechanische Eigenschaften von Materialien. Dabei sind auch Lieferscheine und weitere Dokumente, mit denen Zulieferfirmen gegenüber Rheinmetall die Qualität ihrer Produkte attestieren.

Beispiel 2 Deutsche Bahn

Am 17. Februar 2026 legte ein Cyberangriff sämtliche Auskunfts- und Buchungssysteme der Deutschen Bahn lahm.[3] Zwei Tage später war der Angriff überwunden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) teilte später mit, bei dem Cyberangriff habe es sich um eine digitale Überlastungsattacke (DDoS-Attacke) gehandelt. Bei dem Angriff sei es nicht um Kundendaten gegangen. Vermutlich habe diese öffentlichkeitswirksame DDoS-Attacke Propagandazwecken gedient.

Ukraine-Krieg

Die Bedeutung von Cybersicherheit in Deutschland ist spätestens mit Beginn des Ukraine-Kriegs noch stärker in den Fokus der Öffentlichkeit gerückt, mahnt das Bundeskriminalamt (BKA).[4] Aufgrund seiner Rolle als NATO-Mitglied, EU-Schlüsselstaat sowie maßgeblicher finanzieller und materieller Unterstützer der Ukraine stehe Deutschland neben Angriffen durch finanziell motivierte Cyberakteure zunehmend auch „im Zielspektrum

[2] https://www.tagesschau.de/wirtschaft/digitales/cybersecurity-deutsche-unternehmen-gehackt-100.html
[3] https://www.tagesschau.de/inland/gesellschaft/bahn-cyberangriff-bsi-100.html
[4] https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html?nn=29746

aggressiver, hybrider Angriffskampagnen, die u.a. die Schwächung und Destabilisierung von Staat, Gesellschaft und Wirtschaft zum Ziel“ hätten, schreibt das BKA in seinem im Juni 2025 veröffentlichten „Bundeslagebild Cybercrime 2024“.

Energiesektor im Visier

Das BfV warnte indessen in seinem „Sicherheitshinweis für die Wirtschaft“ vom 26. März 2026 jüngst davor, dass der Energiesektor verstärkt ins Visier geraten sei.[5] Es sei davon auszugehen, dass ausländische Nachrichtendienste und Cybergruppierungen Kritische Infrastrukturen in Deutschland (KRITIS) gezielt auskundschafteten, um Einfallstore für Angriffe zu identifizieren und vorzubereiten. Russland besitze die Fähigkeiten und den Willen, entsprechende Aktivitäten gegen EU-Mitgliedsstaaten und NATO-Bündnispartner zu richten. 2025 seien vereinzelt niedrigschwellige Angriffsversuche von dort zu verzeichnen gewesen, darunter auch Aufklärungsaktivitäten der dem russischen Inlandsgeheimdienst FSB zugeordneten Cyber-Spionagegruppe „Berserk Bear“. Aktuell lägen keine Erkenntnisse zu konkreten Kampagnen vor. Im Falle einer weiteren Lageverschärfung sei jedoch mit einer erhöhten Gefährdung auch für deutsche KRITIS zu rechnen.

„Hase und Igel“

Es ist also nicht die Frage, ob man als KRITIS-Betreiber ins Visier von Cyberkriminellen gerät, sondern lediglich wann. Und Sicherheitsexperten warnen auch davor, dass eine dauerhafte vollständige IT-Sicherheit nicht zu erreichen sei. Der Prozess gleiche eher einem stetigen Hase-und-Igel-Spiel. Das BSI stellt klar: „Informationssicherheit ist kein Zustand, der einmal erreicht wird und dann fortbesteht, sondern ein Prozess, der kontinuierlich angepasst werden muss. Geänderte Verfahren und Prozesse in einer Institution, der Wandel in den gesetzlichen Rahmenbedingungen, neue Technik, aber auch bislang unbekannte Schwachstellen und daraus erwachsende Gefährdungen stellen immer wieder neue Anforderungen, so dass die nachhaltige Angemessenheit und Wirksamkeit nicht automatisch gewährleistet sind.“[6]

Vor diesem Hintergrund ist es lohnend, sich bestehende und geplante gesetzliche Regelungen genauer anzuschauen. Die von den Sicherheitsbehörden festgestellte, latent steigende Bedrohungs- und Gefährdungslage kann es ratsam erscheinen lassen, einzelne regulatorische Maßnahmen noch einmal neu zu beleuchten. Im Zentrum sollte dabei die Frage stehen: Wo machen wir es potenziellen Angreifern unnötig einfach, auf sensible Daten und KRITIS-Strukturen zuzugreifen? Oder: Wo rollen wir ihnen vielleicht sogar den sprichwörtlichen „roten Teppich“ aus?

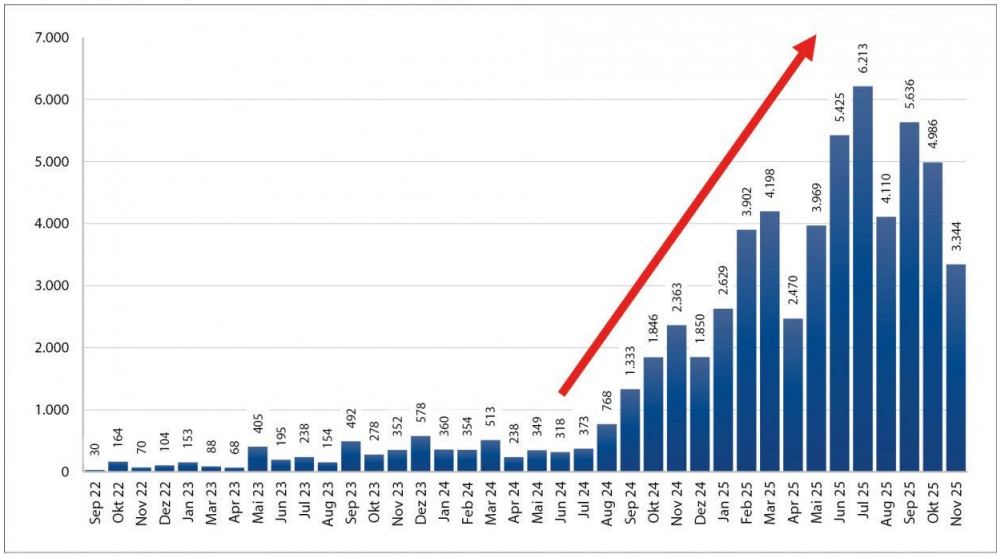
[5] https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/praevention_wirtschafts-und_wissenschaftsschutz/2026-01-sicherheitshinweis-fuer-die-wirtschaft.pdf?__blob=publicationFile&v=9

[6] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/Lektion_2_01/Lektion_2_01_node.html

RESILIENZ

Eine Lehre aus dem seit 2022 tobenden Ukraine-Krieg ist, dass vom Aggressor bewusst Einrichtungen der Strom-, Wärme- und Wasserversorgung als strategische Ziele angegriffen werden, um das Durchhaltevermögen von Staat und Bevölkerung zu schwächen. In der Ukraine erfolgten die Angriffe zumeist über autonome Angriffsdrohnen und Raketen, die mit den entsprechenden Zielkoordinaten gefüttert wurden.[7] Bei den größten Angriffen wurden z. B. am 7. September 2025 mehr als 800 Angriffsdrohnen eingesetzt und am 8. November 2025 mehr als 450 Drohnen und 45 Raketen.

Grafik 1: **Gemeldete monatliche Angriffe mit Shahed 131/136- und Geran-2-Kamikazedrohnen, September 2002 – November 2025**



Quelle: Rochan Consulting

Transparenz als Problem

Wie erfährt ein möglicher Angreifer, welche Ziele sich in seinem Sinne „lohnen“ und auf welchen Koordinaten sie zu finden sind? Provokant ausgedrückt, reicht in Deutschland ein Blick ins Internet. Durch diverse Melde- und Veröffentlichungspflichten sind sehr viele Leistungsdaten der deutschen Energiewirtschaft online abrufbar. Es ist ein Leichtes, entsprechende Angaben mit online vorliegenden Geodaten zu kombinieren, um so eine Karte kritischer Infrastruktur-Knotenpunkte zu erstellen.

Mit den verfügbaren Plattformen und Tools lassen sich mit wenig Aufwand direkte Zuordnungen von Bildquellen, Geokoordinaten und kritischen Infrastrukturen herstellen, die für die Programmierung autonomer Angriffsdrohnen benötigt werden.

Es stellt sich also die Frage, ob Deutschland an der Praxis festhalten sollte, über bestehende Webangebote von Behörden oder von Open-Source-Quellen systematisch Leistungs- bzw. Geodaten von KRITIS-Einrichtungen der weltweiten Öffentlichkeit bereitzustellen.

[7] https://www.bpb.de/themen/europa/ukraine-analysen/nr-327/575836/analyse-russische-angriffe-auf-die-ukrainische-energieinfrastruktur-trends-und-ausblick/

Regelungen

Um welche bestehenden Regelungen geht es konkret?

- §23c EnWG: Hier werden die Veröffentlichungspflichten von Netzbetreibern festgelegt. Der Paragraf verpflichtet Betreiber dazu jährlich bestimmte Strukturmerkmale und netzrelevante Daten online zu veröffentlichen.
- Geodatenzugangsgesetz (GeoZG): Es verpflichtet natürliche und juristische Personen dazu, gewisse geografische Daten und Metadaten in elektronischer Form für den Bund bereitzustellen. Letztlich können so Adressen von kritischen Liegenschaften digital eingesehen werden.
- Informationsfreiheitsgesetz (IFG), Umweltinformationsgesetz (UIG), Landesinformationsgesetz Landes-IFG: Sie sollen der Öffentlichkeit im Sinne der Transparenz Zugriff auf Behördeninformationen ermöglichen. Es sind Jedermannsrechte, die Bund und Länder zur Auskunft an Ihre Bürger verpflichten. So können Auskünfte über Akten, Pläne, Berichte, Fotos oder Karten, sofern sie „amtlichen Zwecken dienen“ verlangt werden.

Beispiel Berlin

Insbesondere die Offenlegung von Netzkontenpunkten kann dazu führen, dass diese für Sabotagezwecke missbraucht werden. Diese Erfahrung mussten Anfang dieses Jahres rund 100.000 Berlinerinnen und Berliner machen, als am 3. Januar ein Brandanschlag auf eine eher unscheinbare Kabelbrücke in Berlin-Lichterfelde/Zehlendorf verübt worden war.[8] 45.000 Haushalte und mehr als 2200 Betriebe sowie mehrere Krankenhäuser und Pflegeeinrichtungen waren tagelang ohne Strom und Heizung. Erst vier Tage später waren laut Medienberichten die Folgen weitgehend beseitigt.

Unsere Resilienz wird also bereits durch im Internet veröffentlichte Daten geschwächt. Wie sieht es aber mit vertraulichen Daten aus, die vermeintlich geschützt auf Servern liegen? Die Warnungen der Sicherheitsbehörden vor zunehmenden Cyberangriffen und elektronischen Ausspähversuchen sind aktuell. Ist es vor diesem Hintergrund sinnvoll, so etwas wie eine zentrale Schatzkammer anzulegen, in der alle kritischen und wertvollen Daten gesammelt vorliegen? Folgte man den Warnungen von BKA, BfV und BSI sollte man lieber davon Abstand nehmen.

„Infrastrukturatlas“

Gerade diese „Schatzkammer-Idee“ verfolgt hingegen das gerade in der parlamentarischen Beratung befindliche TKG-Änderungsgesetz 2026.[9] In den Paragrafen 78ff wird das Vorhaben eines Gigabit-Grundbuchs als „zentrale Informationsstelle des Bundes“ beschrieben. Der vorliegende Referentenentwurf sieht wie das geltende TKG eine zentrale Speicherung der Daten aller deutschen Versorgungsnetze im sogenannten Infrastrukturatlas bei der Bundesnetzagentur (BNetzA) vor. Darin sollen alle öffentlichen

[8] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2026/Presse2026/260127_Zeugenaufruf_Brandanschlag_Berlin.html
[9] https://bmds.bund.de/service/gesetzgebungsverfahren/tkg-aenderungsgesetz-2026

Versorgungsnetze (außer Frischwasser) aufgeführt werden, die dann Interessierten zugänglich gemacht werden sollen. Ziel dieser Regelung soll es sein, die Mitnutzung bestehender Infrastrukturen für den Ausbau von Glasfasernetzen zu ermöglichen, um die Baukosten zu senken.

Kritik

Alle Angaben über Netze (Strom, Gas, Telekommunikation) mit detaillierten Verläufen und vertraulichsten Angaben inklusive sämtlicher KRITIS-Knotenpunkte auf einem Server? Ein lohnendes Ziel für Hacker.

Nach Ansicht von Branchenkennern verschließen die Entwurfsverfasser mit diesem Ansatz die Augen vor den Risiken, die durch die Datenhaltung an einer einzigen Stelle entstehen: Sollte die IT-Sicherheit der BNetzA auch nur ein einziges Mal überwunden werden, ist die exakte geographische Lage aller Kommunikationsnetze, aller Energieversorgungsnetze und aller weiteren öffentlichen Versorgungsnetze in der Bundesrepublik für Angreifer verfügbar – und zwar für Jahrzehnte, denn diese Lage ändert sich in absehbarer Zeit nicht.

FORDERUNG

Unter Resilienzgesichtspunkten ist die geschilderte Situation mehr als mangelhaft. Will Deutschland seine Netze im Krisenfall einigermaßen schützen, muss das freiwillige Veröffentlichen beziehungsweise der gedankenlose Umgang mit sensiblen Daten enden.

Nun haben die verschiedenen Transparenzregeln zweifellos ihre Berechtigung. Niemand wünscht sich einen Staat, der seinen Bürgerinnen und Bürgern misstraut. Demokratische Teilhabe verlangt nach informierten Bürgern. Die Frage ist aber, muss man von sich aus anlasslos sensible Daten veröffentlichen? Es gilt hier, genau abzuwägen.

Registrierung

Im KRITIS-Bereich erscheint es sinnvoll, von der nahezu bedingungslosen Offenlegung abzuweichen. Um Personen etwa weiterhin Einsicht auf Netzpläne zu gewähren, könnte ein Verfahren gewählt werden, das zumindest eine Registrierung des Nachfragenden vorsieht, sodass festgestellt werden kann, wer Zugriff auf die Daten hatte und ob diese Person auch berechtigt ist die Daten abzufragen.

Ortungsdienste

Nachzudenken ist auch, ob sensible Liegenschaften von KRITIS-Betreibern nicht ebenso behandelt werden sollten wie Bundeswehreinrichtungen, indem sie aus Ortungsdiensten entfernt werden.

Dachgesetz

Das am 17. März 2026 in Kraft getretene KRITIS-Dachgesetz weist schon den richtigen Weg, weil es allzu offenherzige Tranzparenzregelungen vor dem Hintergrund der besonderen Schutzbedürftigkeit kritischer Infrastrukturen infragestellt. Zu begrüßen ist, dass es gleich in Paragraf 1 die Bundesregierung dazu verpflichtet, eine KRITIS-Resilienzstrategie vorzulegen.[10]

[10] https://www.gesetze-im-internet.de/kritisdachg/KRITISDachG.pdf

Dezentraler Atlas

Bezüglich des TKG-Änderungsgesetzes bietet sich eine dezentrale Speicherung der Daten an. Statt eines einzigen riesigen Datenschatzes wird mit einem „dezentralen Infrastrukturatlas“ gearbeitet. Kernpunkt: Die Daten bleiben beim Netzbetreiber und Anfragen werden von der BNetzA lediglich vermittelt. Dadurch wird das Risiko eines großen Datendiebstahls reduziert. Einen entsprechenden Vorstoß hat der Bundesverband Breitbankkommunikation (BREKO) bereits im Januar 2024 vorgelegt.[11]

Kontakt:
EWE AG
Markus Hümpfer
Konzernbeauftragter Bundespolitik
Pariser Platz 6a
10117 Berlin
Mobil: +49 162 2980912
E-Mail: markus.huempfer@ewe.de

[11] https://brekoverband.de/wp-content/uploads/2025/03/breko_strategiepapier_disa.pdf