LINK11

KRITIS im Kreuzfeuer von verschärften EU-Regularien und verstärkten Cyberangriffen

Was Sie jetzt beachten sollten

SCHALAST
LAW | TAX

www.link11.com

Inhalt

Bedrohung kritischer Infrastrukturen durch Sabotage und Cyberattacken wächst	03
Potenzielles Angriffsziel: KRITIS	05
Rechtliche Grundlagen gewährleisten Sicherheit der kritischen Infrastrukturen	08
Risikovermeidung nicht nur für KRITIS	13
Deep Dive Banking: Umfassende Regulierung sorgt für höheren Cyberschutz	14
Nachholbedarf bei KRITIS: Wer muss noch am meisten tun?	16
Sinnvolle IT-Sicherheitsstrategie erforderlich	17
Effektive IT-Schutzlösungen für die Zukunft	19

Bedrohung kritischer Infrastrukturen durch Sabotage und Cyberattacken wächst

Die Anschläge auf die Nord-Stream-Pipelines[1] im September 2022 und kurz darauf der Ausfall des Bahnbetriebsfunks[2] im Oktober sowie die jüngsten Angriffe auf Webseiten etlicher Behörden und der Polizei[3] im April 2023 hat die Verwundbarkeit kritischer Infrastrukturen in Deutschland in die öffentliche Debatte gebracht. Die EU-Kommission hat bereits im Jahr 2020 zwei zentrale Rechtsakte vorgeschlagen, die darauf abzielen, die Widerstandsfähigkeit kritischer europäischer Infrastrukturen zu stärken. Die Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) konzentriert sich auf physische Gefahren, während die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie) die Cybersicherheit kritischer Infrastrukturen betrifft.

Neben diesen physischen Sabotageakten hat für Betreiber kritischer Infrastrukturen ebenso die Gefahr durch Cyberattacken zugenommen. Zum einen gab es in den vergangenen Jahren rasante technologische Fortschritte und zum anderen kam eine deutlich gestiegene Anzahl dezentral vernetzter Systeme hinzu. Dadurch hat die Angriffsfläche für Cyberattacken zugenommen. Den Experten des Weltwirtschaftsforums zufolge zieht ein regelrechter „Cyber-Sturm“ auf. Aus dem aktuellen „Global Cybersecurity Outlook“ geht zudem hervor, dass 91 % der befragten Führungskräfte von weitreichenden und katastrophalen Cybervorfällen in den kommenden Jahren ausgehen.

Der Schaden allein für die deutsche Wirtschaft liegt laut einer im Sommer 2022 veröffentlichten Studie bei 203 Milliarden Euro. Zudem erwarten die befragten Unternehmen eine weitere Zunahme von Cyberattacken. 51 % der Betreiber kritischer Infrastrukturen rechnen mit einem starken Anstieg von Cyberangriffen.

Während der Corona-Pandemie stieg die Anzahl der DDoS-Angriffe weltweit an, da Cyberkriminelle die digitale Verwundbarkeit der Unternehmen und der remote arbeitenden Bevölkerung ausnutzen wollten. Dabei folgte die Mehrheit der Angreifer finanziellen Motiven. Demgegenüber haben im Jahr 2022 politisch motivierte DDoS-Angriffe deutlich zugenommen. Ziel solcher Angriffe ist die Moral der der Bevölkerung zu schwächen und größtmöglichen Schaden anzurichten, wie auch Microsoft im Report „Defending Ukraine: Early Lessons from the Cyber War“ festgestellt hat.

Die prorussische Hackergruppe „Killnet“ hat mehreren Ländern, darunter auch Deutschland, den Cyberkrieg erklärt.[4] In Deutschland, Italien, Litauen, Norwegen und Polen waren die Folgen dieser Erklärung bereits zu spüren.[5] Es verging kaum ein Monat, in dem es keinen Cyberangriff auf NATO-Staaten, deren öffentlichen Institutionen, Banken oder kritische Infrastrukturen gab. Das BSI konstatiert im aktuellen Lagebericht, die Bedrohungslage sei „so hoch wie nie“.

Die im Link11-Netzwerk abgewehrten DDoS-Attacken waren im Jahr 2022 im Durchschnitt zwar etwas weniger und kürzer, dabei aber intensiver und anspruchsvoller. Eine Analyse der im Link11-Netzwerk registrierten Attacken zeigt, dass die kritische Last bei den DDoS-Angriffen im Jahr 2022 im Durchschnitt bereits 55 Sekunden nach Beginn der Attacke erreicht wurde. Im Vergleich dazu benötigten Angriffe im Jahr 2021 durchschnittlich 184 Sekunden, um ihren Höhepunkt zu erreichen.

Diese „Turboangriffe“ können das Netzwerk bereits lahmlegen, bevor die Verteidigungsmaßnahmen greifen. Zudem verändern sich diese Attacken und die angewandten Methoden ständig. Statt willkürlich in der Hoffnung auf Erfolg die Unternehmen zu attackieren, kommen nun sehr gezielt fortgeschrittene und ausgeklügelte DDoS-Attacken zum Einsatz.

„Die Wandlungsfähigkeit der DDoS-Attacken ist enorm. Umso wichtiger ist die Analyse des Datenverkehrs in Echtzeit mit smarten, schnellen und sicheren Methoden.“

Jens Rieser, Account Executive, Link11

Wichtige Prozesse werden zu selten geprobt, sodass im Ernstfall die Erkennung eines DDoS-Angriffes und der Schwenk der Datenleitung viel zu lange dauern. In einem solchen Fall geht kostbare Zeit verloren und die Betriebsunterbrechung nimmt ihren Lauf. Liefermodelle und Betriebskonzepte sind heute in vielen Fällen nicht mehr zeitgemäß.

Wichtig in diesem Zusammenhang sind Service Level Agreements (SLAs), die dem neuesten Stand entsprechen. Denn nicht nur die Anzahl der DDoS-Attacken steigt, es verändert sich auch zunehmend deren DNA. Die Komplexität der Angriffe ist in den vergangenen Jahren kontinuierlich gestiegen. Deshalb rückt bei fortschrittlichen SLAs die Zeit für die erfolgte Abwehr (TTM) anstelle der Erkennung in den Mittelpunkt. Statt auf Marketingversprechen kommt es vor allem auf die vertragliche Absicherung an, die aufgrund der gestiegenen Anforderungen im Hinblick auf die IT-Verfügbarkeit stärker in den Fokus rückt.

Hierbei sollen rechtliche Rahmenbedingungen eine gewisse Cybersicherheit der KRITIS gewährleisten. Andererseits müssen Unternehmen regelmäßig die Bedingungen überprüfen, um Fehlannahmen zu widerlegen und sich nicht in falscher Sicherheit zu wähnen.

Potenzielles Angriffsziel: KRITIS

Kritische Infrastrukturen sind Einrichtungen und Systeme, die für das Funktionieren der Gesellschaft und der Wirtschaft von wesentlicher Bedeutung sind. Dazu gehören Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit, Informationstechnik und Telekommunikation, Medien und Kultur, Siedlungsabfallentsorgung, Staat und Verwaltung, Transport und Verkehr, Wasser.[6]

Diese Systeme sind besonders anfällig für Cyberangriffe aus mehreren Gründen

Hohe Abhängigkeit von Informationstechnologie (IT): Kritische Infrastrukturen sind stark von der IT abhängig, um effektiv zu funktionieren. Dies bedeutet, dass ein erfolgreicher Cyberangriff auf die IT-Systeme dieser Infrastrukturen ihre Funktionsfähigkeit erheblich beeinträchtigen oder sogar komplett lahmlegen kann.

Komplexe Systeme: Kritische Infrastrukturen sind oft sehr komplexe Systeme, die aus vielen verschiedenen Komponenten und Subsystemen bestehen. Dies erhöht die Anzahl der potenziellen Schwachstellen, die von einem Angreifer ausgenutzt werden können.

Veraltete Systeme: Viele kritische Infrastrukturen wurden vor Jahren oder sogar Jahrzehnten gebaut und sind möglicherweise nicht auf dem neuesten Stand der Technik. Einige dieser Systeme können veraltete oder unsichere Technologien verwenden, die anfällig für Angriffe sind.

Menschliches Versagen: Kritische Infrastrukturen werden von Menschen betrieben und verwaltet. Hier können sich Fehler und Nachlässigkeit einschleichen. Schon ein einfacher Fehler kann zu einem Sicherheitsrisiko führen und einem Angreifer den Zugriff auf das System erleichtern.

Aufgrund ihrer Bedeutung für die Gesellschaft und die Wirtschaft stehen kritische Infrastrukturen im Fadenkreuz von Cyberkriminellen. Durch deren Zugriff auf die Systeme können Daten gestohlen, Geld erpresst oder sogar physische Schäden verursacht werden. Ein erfolgreicher Angriff auf kritische Infrastrukturen kann weitreichende Auswirkungen auf die Gesellschaft haben und daher von großem Interesse für Cyberkriminelle sein.

Angegriffen werden alle: Konzerne, kleine und mittelständische Unternehmen sowie die öffentliche Verwaltung und die Zivilgesellschaft. Besonders gefährdet sind alle Bereiche, die zur kritischen Infrastruktur (KRITIS) gehören – wie Einrichtungen, Organisationen, Anlagen und Systeme, die für das staatliche Gemeinwesen wichtig sind.[7] Kommt es zu Störungen oder gar Ausfällen, hat das gravierende Folgen für die Gesellschaft und die staatliche Ordnung.

Die kritischen Infrastrukturen unterteilen sich in Deutschland in folgende Sektoren:

Welche Unternehmen zur kritischen Infrastruktur gezählt werden, muss im Einzelfall unter Beachtung mehrerer Faktoren geprüft werden. Zentrale Frage ist, ob eine Dienstleistung kritisch ist oder nicht. In einem regulierten Sektor wie etwa dem Gesundheitswesen ist die Bewertung relativ einfach: Bei Krankenhäusern wird der Schwellenwert auf Basis der „vollstationären Fälle“ geprüft und eindeutig definiert. Die Schwellenwerte variieren je nach Branche. So hat der Gesetzgeber u. a. folgende Schwellenwerte festgesetzt:

- Produktionsmenge,
- Transportvolumen,
- produzierte Energie.

Dabei ist das typische Messkriterium die Versorgung von 500.000 Menschen. Das heißt, dass Betriebe und Unternehmen, die 500.000 Menschen versorgen können, zur kritischen Infrastruktur gehören.

Ein gut definierter Schwellenwert erleichtert oftmals die Entscheidung, denn Unternehmen und Gesetzgeber beziffern die Dienstleistung oder die Waren häufig unterschiedlich. Während im Logistikbereich international in Twenty-foot Equivalent Units (TEU) gerechnet wird, betrachtet der Gesetzgeber die Menge in Tonnen. Neben der Frage nach der kritischen Dienstleistung und den entsprechenden Schwellenwerten spielt eine vernetzte IT-Infrastruktur ebenfalls eine Rolle, ob ein Unternehmen zur kritischen Infrastruktur gehört. Je zentraler und vernetzter die IT-Systeme auch bei unterschiedlichen Standorten sind, desto wahrscheinlicher gehört das Unternehmen dazu.

KRITIS-Verständnis im Rahmen neuer EU-Richtlinien

Grundsätzlich wird zwischen systemischer und konsequenzbasierter Kritikalität unterschieden. Systemische Kritikalität bezieht sich auf die Bedeutung für die infrastrukturelle Versorgung, während konsequenzbasierte Kritikalität die gesellschaftliche Relevanz betont.

Die Definition kritischer Infrastrukturen nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz/BSIG) und der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (BSI-KritisV) geht konsequenzbasiert vor und legt den Fokus auf die Bedeutung für das Funktionieren des Gemeinwesens.

Die seit Januar 2023 in Kraft getretene Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie) etabliert nun die Begriffe der „wesentlichen Einrichtungen“ (Essential Entities) und der „wichtigen Einrichtungen“ (Important Entities), um kritische Infrastrukturen zu definieren.

Die wesentlichen Einrichtungen umfassen große Betreiber aus elf Sektoren sowie bestimmte Betreiber und Branchen, die unabhängig von ihrer Größe als Essential Entity reguliert werden. Die wichtigen Einrichtungen umfassen große Betreiber aus sieben Sektoren und mittlere Betreiber aus allen achtzehn Sektoren.

Die Regulierung erfolgt nach der Größe des Unternehmens. Der Unterschied zwischen den beiden Definitionen bezieht sich vor allem auf den Umfang der staatlichen Aufsicht und Sanktionsmöglichkeiten. Staaten können bestimmte Betreiber als wesentliche oder wichtige Einrichtungen festlegen, wenn sie eine spezielle nationale oder regionale Bedeutung haben oder ein signifikantes systemisches Risiko für Sektoren und grenzüberschreitende Abhängigkeiten darstellen.

Darüber hinaus identifiziert die seit Januar 2023 in Kraft getretene Richtlinie über die Resilienz kritischer Einrichtungen betroffene KRITIS-Betreiber (EU RCE Directive oder CER-Richtlinie) im Hinblick auf nationale Risiko-Analysen. Zudem wird der disruptive Effekt im Falle eines Ausfalls berücksichtigt. Diese Regelungen gelten für elf Sektoren, die sich weitgehend mit den KRITIS-Sektoren decken.

Überlbick der Definitionen der NIS2 und CER Richtlinie

Rechtliche Grundlagen gewährleisten Sicherheit der kritischen Infrastrukturen

Die Sicherheit der KRITIS gewährleistet ein ausgeprägter und sich stets entwickelnder Regulierungsrahmen. So sehen sowohl der deutsche als auch der europäische Gesetzgeber verpflichtende Maßnahmen für ein einheitliches Sicherheitsniveau der Netz- und Informationssysteme von KRITIS vor, wobei im Zweifel das europäische Recht vorgeht.

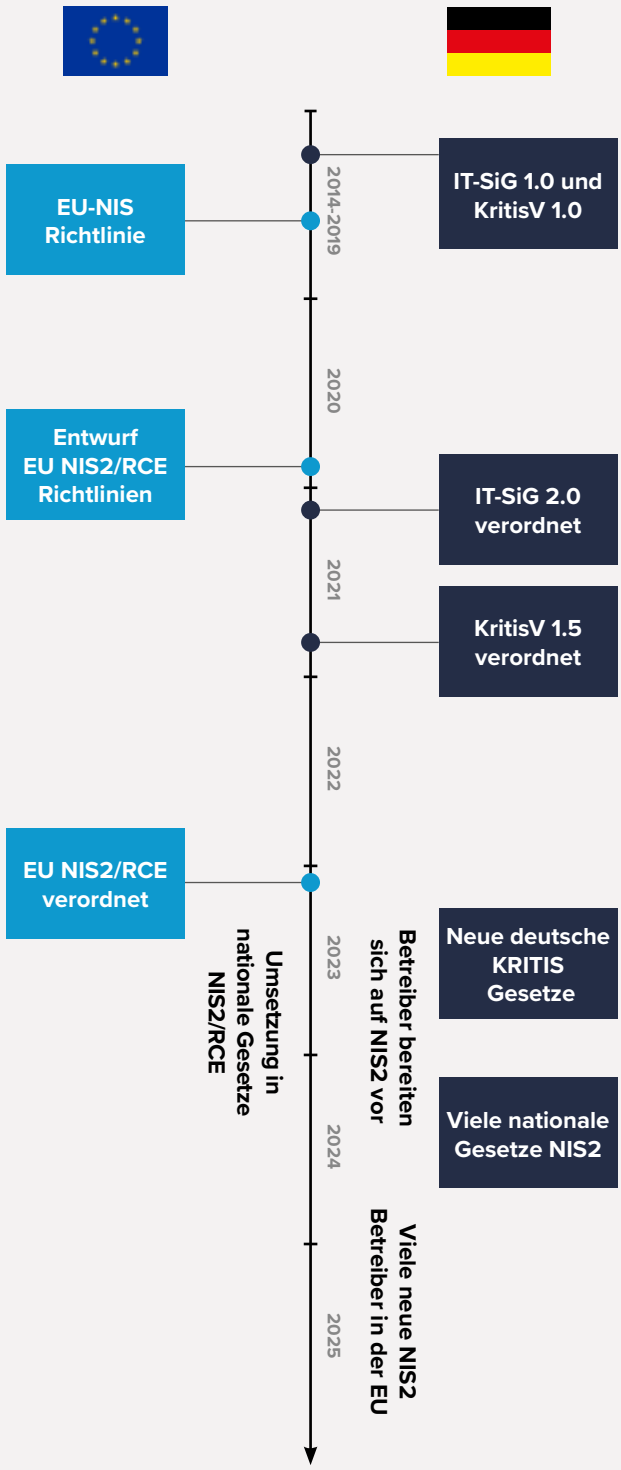
Überblick über die Rechtsgrundlagen

Auf nationaler Ebene bildet das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (sog. BSI-Gesetz/BSIG) die Rechtsgrundlage für die Regulierung von KRITIS und deren Betreiber. Konkretisiert wird die Definition der kritischen Infrastrukturen in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (sog. BSI-KritisV). In ihr finden sich nähere Beschreibungen zu den einzelnen Sektoren sowie Schwellenwerte zur Bestimmung kritischer Infrastruktur. Aktuell gilt die Dritte Verordnung zur Änderung der BSI-Kritisverordnung vom 1. März 2023.[8] Daneben bestehen sektorspezifisch einzelgesetzliche Regelungen. So sind zum Beispiel für den Sektor Energie Regelungen des Energiewirtschaftsgesetzes (EnWG) und für die Telekommunikation das Telekommunikationsgesetz (TKG) vorrangig zu beachten, da sie spezifischer auf die Belange des jeweiligen Sektors abzielen. In anderen Sektoren finden sich Spezialregelungen in allgemeineren Gesetzen, zum Beispiel für den Gesundheitssektor u. a. im SGB V. Im Rahmen der zwei IT-Sicherheitsgesetze (2015 und 2021), die jeweils als Mantelgesetze verschiedene Gesetze im Kontext IT-Sicherheit betrafen, wurden das BSIG sowie andere einschlägige Gesetze wie das EnWG, das Atomgesetz oder das TKG erweitert.

Auf europäischer Ebene trat 2016 die EU-Richtlinie zur Netzwerk- und Informationssicherheit (sog. NIS-Richtlinie) in Kraft, die über das zweite IT-Sicherheitsgesetz in deutsches Recht umgesetzt wurde. Am 16. Januar 2023 sind zwei neue Richtlinien, die die Sicherheit kritischer Infrastrukturen verbessern sollen, in Kraft getreten[9]:

- Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie)[10]
- Richtlinie über die Resilienz kritischer Einrichtungen (EU RCE Directive oder CER-Richtlinie)[11]

Rechtsgrundlagen im Zeitverlauf



NIS2 stärkt die Cybersicherheit kritischer Infrastrukturen in der EU

Die NIS2-Richtlinie ersetzt die EU-Richtlinie zur Netzwerk- und Informationssicherheit von 2016 (NIS1) und schafft einen einheitlichen Rahmen für den Aufbau nationaler Kapazitäten für Cybersicherheit in der EU. Die Richtlinie enthält Mindestsicherheitsanforderungen und Meldepflichten für Betreiber von kritischen Infrastrukturen und bestimmten Anbietern digitaler Dienste und muss innerhalb von 21 Monaten in deutsches Recht umgesetzt werden.

Die kommende EU-Regulierung geht teilweise über die bisherigen deutschen Anforderungen hinaus und beinhaltet konkrete Schutzmaßnahmen sowie erweiterte Betreiberpflichten und staatliche Governance. Neue Themen wie die koordinierte Offenlegung von Schwachstellen und eine europäische Schwachstellendatenbank werden ebenfalls in europäische Kooperationsformate überführt. Eine Regelung für das Cybersicherheitskrisenmanagement wurde auch geschaffen.

Nach der Prüfung der NIS1-Richtlinie wurde zudem deutlich, dass es Abweichungen bei der Identifizierung von Einrichtungen und der Anzahl von Meldefällen gab. NIS2 enthält daher umfangreiche Änderungen wie die Aufnahme zusätzlicher Sektoren und die Einbeziehung von Einrichtungen der öffentlichen Verwaltung. Die Sicherheitsanforderungen werden national anhand einer Verhältnismäßigkeitseinschätzung abgestuft angewandt und die Meldepflichten werden in ein dreistufiges Melderegime mit festen Fristen umgewandelt.

NIS2 definiert betroffene Unternehmen und Organisationen in kritischen Sektoren nach Größe und Umsatz. Es ist noch offen, ob die deutsche Methodik beibehalten oder durch die NIS2-Methodik ergänzt wird. Möglicherweise wird ein mehrstufiges System implementiert, das bestehende KRITIS-Sektoren, darüberhinausgehende Sektoren und Unternehmen sowie Unternehmen im besonderen öffentlichen Interesse reguliert.

Die NIS2-Richtlinie definiert achtzehn Sektoren, die sich mit den deutschen KRITIS-Sektoren und den Unternehmen im besonderen öffentlichen Interesse teils überschneiden, teils aber auch darüber hinausgehen. Möglicherweise werden die fehlenden Sektoren im IT-Sicherheitsgesetz 3.0 oder neuen Rechtsverordnungen geregelt.

CER-Richtlinie festigt Widerstandsfähigkeit kritischer Infrastrukturen

Das bedeutet, es gibt noch ausstehende Änderungen an der KRITIS-Verordnung, insbesondere im Bereich der Siedlungsabfallentsorgung und der Unternehmen im besonderen öffentlichen Interesse (UBI). Parallel zur NIS2 wurde beispielsweise auch die Richtlinie über die EU RCE Directive (CER-Richtlinie) verhandelt, die ein überarbeitetes Konzept für die Widerstandsfähigkeit kritischer Infrastrukturen enthält. Dabei werden Maßnahmen bei Unternehmen und der staatlichen Aufsicht ergriffen, um Ausfallsicherheit bei kritischen Dienstleistungen von Betreibern (Critical Entities) zu fordern.

Diese Maßnahmen ergänzen die Cybersecurity-Regulierungen von NIS2. Die EU RCE Directive löst die ECI European Critical Infrastructures Directive von 2008 ab und wurde Ende 2022 zusammen mit NIS2 in der EU verabschiedet. Während die CER-Richtlinie bereits im kommenden KRITIS-Dachgesetz behandelt wird, muss NIS2 bis Oktober 2024 in nationale Gesetzgebung überführt werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) setzt sich aktiv dafür ein, dass die neue Richtlinie NIS2 auch in Deutschland zu einer deutlichen Erweiterung der erfassten Einrichtungen führt. Dabei betont das BSI, dass auch die nationalen Vorgaben der BSI-Kritisverordnung (BSI-KritisV) berücksichtigt werden sollten. Insbesondere im Bereich der Aufsicht und Durchsetzung werden die Befugnisse und Handlungsmöglichkeiten der national zuständigen Behörden erweitert.

Mehr Einheitlichkeit durch das KRITIS-Dachgesetz

Darüber hinaus arbeitet das deutsche Innenministerium an einem Dachgesetz[12] zur Regulierung von kritischen Infrastrukturen (KRITIS), das ab 2023 in Kraft treten soll. Hintergrund sind aktuelle Vorfälle wie die Anschläge auf die Nord-Stream-Pipeline oder die Deutsche Bahn sowie die politische Lage im Jahr 2022. Das Gesetz soll Anforderungen an die physische Sicherheit und Resilienz von KRITIS-Betreibern konkretisieren und Teile der kommenden EU-Regulierungen vorwegnehmen.

Seit Ende 2022 wird das Dachgesetz öffentlich[13] diskutiert und soll die Sicherheit von KRITIS-Betreibern stärken. Im Dezember 2022 hat das Innenministerium ein Eckpunkte-Papier[14] veröffentlicht und will bis zur Sommerpause 2023 einen Gesetzesentwurf vorlegen. Dabei greift das Dachgesetz teilweise der CER-Richtlinie vor. Vorrangiges Ziel des KRITIS-Dachgesetzes ist die Stärkung der Resilienz durch einheitliche Mindestvorgaben. Dazu gehören unter anderem die Ergänzung der bestehenden KRITIS-Definition, einheitliche Risikobewertungen und die Schaffung eines institutionellen Rahmens.

Mehr zu den einschlägigen Rechtsgrundlagen finden Sie hier.

Regulierungsbehörden

KRITIS-Betreiber unterliegen der behördlichen Aufsicht. Das Innenministerium ist als federführendes Ressort auf Bundesebene für den Schutz kritischer Infrastrukturen und die damit verbundene Gesetzgebung und Regulierung verantwortlich.

Als Cybersicherheitsbehörde ist das Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI) die zentrale Stelle. Insgesamt wird ein **strikter Maßnahmenstandard** angelegt. So hat das BSI Befugnisse, bei Nichteinhaltung gegebenenfalls selbst vorzugehen, kann **Mindeststandards** an Sicherheitssysteme und einzelne Komponenten festlegen, **Portscans** in Bereichen von IP-Adressen durchführen und hat auch eine Befugnis zur **Bestandsdatenauskunft.**

Neben dem BSI gibt es sektorenspezifische Zuständigkeiten weiterer Behörden wie die Bundesnetzagentur (BNetzA) oder die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Für Energieanlagen und -netze (und den Bereich Telekommunikation) definiert beispielsweise die BNetzA gemeinsam mit dem BSI die Mindeststandards, um die individuellen Gegebenheiten des Energiesektors besonders berücksichtigen zu können. Ferner beschäftigt sich das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zum Beispiel mit der Bearbeitung von KRITIS-Strategien, Schutzkonzepten und Risikomanagement.[15]

Man sieht: Das KRITIS-Netz ist vielseitig und sektoren- sowie aufgabenabhängig. Wichtigste Anlaufstelle bleibt jedoch das BSI.

Pflichten für KRITIS-Betreiber (nicht abschließend)

Grundsätzlich bestehen für Betreiber zwei Hauptpflichten: Technische und organisatorische Sicherheitsvorkehrungen zur Sicherung ihrer Netz- und Informationssysteme zu treffen und eine Meldepflicht bei bestimmten Störungen der informationstechnischen Systeme.

Pflicht	Beschreibung
Registrierungspflicht	• Pflicht zur Registrierung als Betreiber beim BSI & Benennung der Kontaktstelle, sobald vorgeschriebene Schwellwerte überschritten. • Erforderlich für authentifizierbare Meldungen von Angriffen & Empfang von Lage- und Warninformationen des BSI. • Je nach Sektor kann Einrichten einer Kontaktstelle unabhängig vom Stellenwert einer KRITIS sinnvoll oder inzident verpflichtend sein, zum Beispiel im Bereich Energie eine inzidente Registrierungserfordernis aus der Meldepflicht (s. u.) für alle Energieversorgungsnetze. • Zusätzlich ggf. Registrierungspflicht bei anderen Behörden, zum Beispiel je nach Anlage und Dienst in den Sektoren Energie und Telekommunikation auch bei der BnetzA.
Meldepflicht	• Unverzügliche Meldepflicht bei IT-Störungen / erheblichen Beeinträchtigungen inkl. Herausgabepflicht von Informationen (bezieht sich auf alle zur Bewältigung der Störung notwendigen Informationen).
Pflicht zum Einsatz von „Systemen zur Angriffserkennung“	• IT-Sicherheit muss auf dem „Stand der Technik“ umgesetzt werden. • Dazu gehört neben technischen Anforderungen aber auch die Vermeidung der noch immer häufigen Ursache „menschlicher Einfallstore“. • Genaueres ist in „branchenspezifischen Sicherheitsstandards“ (B3S) festgelegt, in denen Anforderungen zum Stand der Technik konkretisiert werden.
Nachweispflicht	• Dass die IT-Sicherheit tatsächlich auf dem Stand der Technik ist, muss alle zwei Jahre gegenüber dem BSI nachgewiesen werden.

Das weitere Prozedere nach pflichtgemäßer Abgabe der Meldung von IT-Störungen hängt vom Einzelfall ab. Betreiber können die Störung entweder allein beseitigen oder selbst entscheiden, ob sie weitere Behörden und eine mögliche Strafverfolgung einbinden. In speziellen Fällen kann das BSI auch von Amts wegen weitere Aufsichts- oder Sicherheitsbehörden wie das Bundeskriminalamt oder das Bundesamt für Verfassungsschutz einbinden oder bei der Störungsbewältigung unterstützen.

Unabhängig vom Einzelfall kann sich eine Anzeige wohl immer bewähren: Zum einen hilft es den Ermittlungsbehörden, die Brisanz und das Ausmaß einer Gruppierung einzuordnen, wenn mehr Fälle bekannt sind. Zum anderen kann, wenn Täter ermittelt wurden, zur Strafbemessung nur herangezogen werden, was aktenkundig ist. Um KRITIS-Betreibern die Erfüllung dieser Pflichten zu erleichtern, bietet das BSI konkrete Informationen zur Umsetzung der genannten Punkte[16] wie auch sektorspezifische Informationen.[17]

Spezialgesetzliche Pflichten sind ebenso zu beachten (Auszug): So regelt zum Beispiel § 11 EnWG zentral die Sicherungs- und Meldepflichten[18] für **Betreiber von Energieanlagen** und -netzen und verpflichtet **alle** Netzbetreiber (auch unterhalb der Schwellenwerte!) dazu, einen angemessenen Schutz gegen Bedrohungen solcher (IT-)Systeme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Die BNetzA hat für diese Informationssicherheitsmanagementsysteme (ISMS) in ihrem IT-Sicherheitskatalog[19] entsprechende Mindeststandards festgelegt, die umgesetzt, dokumentiert und (ab Mai 2023) alle zwei Jahre gegenüber dem BSI nachgewiesen werden müssen. Auch müssen spätestens **ab Mai 2023** Systeme zur Angriffserkennung eingesetzt werden.

Netzbetreiber sind verpflichtet, die Konformität ihrer ISMS mit den Anforderungen des IT-Sicherheitskatalogs durch Zertifikate zu belegen.[20] Ebenso müssen eingesetzte Systeme und damit verbundene Maßnahmen kontinuierlich auf ihre Wirksamkeit überprüft und ggf. angepasst werden.[21]

Im Finanzsektor müssen sich bspw. **Zahlungsdienstleister** an spezialgesetzliche Bestimmungen[22] halten und angemessene Risikominderungsmaßnahmen und Kontrollmechanismen einrichten, aufrechterhalten und anwenden.

Auch **Krankenhäuser** (Sektor Gesundheit) müssen seit 01.01.2022 angemessene Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme treffen, § 75c SGB V.[23]

Aktuell gewinnt daneben die Anzeigepflicht für die Verwendung kritischer Komponenten an Bedeutung. Hierbei handelt es sich um IT-Produkte, die in KRITIS eingesetzt werden, und deren Störungen zu erheblichen Beeinträchtigungen, Gefährdungen oder einem Ausfall führen können.[24] Hintergrund dieser Pflicht ist die zunehmende Gefahr, dass ausländische Regierungen indirekt Kontrolle über besonders bedeutsame Infrastrukturen erlangen könnten. Komponenten, die ab 31. Dezember 2025 verbaut werden, müssen von einer anerkannten Zertifizierungsstelle zertifiziert und von einer anerkannten IT-Überprüfungsstelle überprüft worden sein. Vorher eingesetzte Komponenten müssen spätestens bis dahin ersetzt werden, wenn sie keine Zertifizierung erhalten.

”

„Das regulatorische Umfeld ist nicht statisch, sondern dynamisch, die Erfüllung einer Schutzpflicht ist kein abgeschlossener Prozess.“

Janka Schwaibold, Rechtsanwältin und Partnerin,
Schalast LAW | TAX

Bußgelder & Haftungsfragen

Grundsätzlich sind die KRITIS-Strategien auf eine konstruktive Zusammenarbeit von Behörden und Betreibern ausgelegt und dienen auch den Interessen der betroffenen Unternehmen, um Schäden im Vorfeld zu vermeiden.[25] Verstößt der KRITIS-Betreiber jedoch gegen Pflichten, kann das BSI selbstständig tätig werden. So kann zum Beispiel die Registrierungspflicht auch gegen den Willen des Betreibers durchgesetzt werden.[26]

Die Nichterfüllung der Pflichten stellt außerdem eine Ordnungswidrigkeit dar und kann nach § 14 BSIG[27] mit unterschiedlichen Bußgeldern zwischen bis zu 100.000 und 2 Mio. EUR geahndet werden. Die fehlende Registrierung als KRITIS kann zum Beispiel ein Bußgeld von bis zu 500.000 Euro auslösen. Im Fall einer Datenpanne stellen Bußgelder ebenso ein Risiko dar, denn auch nach DSGVO[28] müssen technische und organisatorische Maßnahmen getroffen werden, um einen Grundschutz für die verarbeiteten Daten sicherzustellen. Da DDoS immer häufiger in Verbindung mit sog. Double oder Triple Extortion (samt Ransomware) auftaucht, laufen Unternehmen bei einem ungenügenden oder fehlenden DDoS-Schutz Gefahr, dass dies einen unzureichenden Schutz darstellt (denn das Risiko war offenkundig hinreichend bekannt) und damit einen Bußgeldtatbestand begründet.

Je nach Konstellation ist das wirtschaftliche Risiko beispielsweise durch einen Betriebsausfall[29] und durch zivilrechtliche Haftung deutlich größer. So ist fraglich, ob gesetzliche oder vertragliche Haftungsbeschränkungen greifen, wenn ein Unternehmen seiner Leistungspflicht gegenüber Kunden infolge einer Störung nicht nachkommen kann, obwohl die Störung durch entsprechende Maßnahmen hätte verhindert werden können und müssen. Tragische Beispiele zeigen Risiken über wirtschaftliche Einbußen und Reputationsschäden hinaus: Ein Hackerangriff legte 2020 eine Uniklinik lahm, wodurch Rettungswagen an weiter weg gelegene Kliniken umgeleitet werden mussten – rettende Minuten, die im Zweifelsfall fehlen.

Grundsätzlich besteht die Gefahr, in der Wachsamkeit nachzulassen, wenn man sich auf bekannte Risiken vorbereitet hat. Die KRITIS-Vorgaben stellen aber nur ein Mindestmaß an Sicherungsmaßnahmen dar. Die Erfüllung allein ist keine Garantie für eine vollständige Absicherung.

Risikovermeidung nicht nur für KRITIS

Insgesamt sind die Maßnahmen[30] des Regulierungsrahmens auf ein möglichst einheitliches Sicherheitsniveau ausgelegt. Sobald ein Unternehmen zu einem der schützenswerten Sektoren gehört, sind die genannten Pflichten zu erfüllen. Etwaige Pflichtverstöße werden auch ohne öffentlichkeitswirksame Schäden durch regelmäßige Nachweispflichten transparent. Daher braucht es eine kontinuierliche Auseinandersetzung mit dem Thema Cybersicherheit. Dies gilt auch für Unternehmen, die noch nicht die Schwellenwerte überschritten haben und somit per Definition noch nicht zur KRITIS gehören.

Denn auch **andere Unternehmen** im Kontext kritischer Infrastrukturen sind beliebte Angriffsziele für Cyberattacken. Es empfiehlt sich daher, einen höheren Sicherungsmaßstab zu prüfen, auch wenn die Schwellenwerte (noch) nicht überschritten sind. KRITIS-Betreiber müssen den Versorgungsgrad ihrer Anlage (Schwellenwerte!) für das zurückliegende Kalenderjahr bis zu einer bestimmten Frist, in der Regel 31. März, ermitteln.[31] Zumindest in Bereichen, in denen Schwankungen denkbar sind, muss sichergestellt sein, dass die Schwellenwerte regelmäßig überprüft werden. Betreiber, die sich den Schwellenwerten nähern, sollten sich an den vorgegebenen Fristen zur internen Überprüfung orientieren. Denn sobald diese erreicht sind, ist man unverzüglich meldepflichtig und setzt sich der Gefahr eines möglichen Bußgeldes aus.

Ebenso dient die regelmäßige Überprüfung dazu, mögliche Fehlannahmen zu widerlegen und sich nicht in falscher Sicherheit zu wähnen. Im Rahmen von „Feuerproben“ kann das Unternehmen sich und die Mitarbeitenden auf ausreichende Sicherheitsstandards überprüfen. Auch sollte man sich in dem Zusammenhang fragen, ob man sich auf etwaige Sicherheitsvorkehrungen seiner (möglicherweise zahlreichen) IT-Dienstleister verlassen darf, denn häufig kann dies nur im Innenverhältnis Ansprüche auslösen, im Außenverhältnis bleibt es ein Versäumnis des Auftraggebers. Zuletzt darf der Faktor Mensch nicht unterschätzt werden.[32] Auch um sich davor zu schützen, sollten Unternehmen geeignete technische Mittel einsetzen.

Die IT-Sicherheitsgesetze in Deutschland haben bereits einige der neuen Sektoren nach der NIS2-Richtlinie umgesetzt, aber es wird zu massiven Ausweitungen bei den IT-Sicherheitspflichten kommen. Die NIS2-Richtlinie wird dazu führen, dass die von Risikomanagementanforderungen und Meldungen betroffenen Sektoren ausgeweitet werden. Das aktuelle Vorhaben der Bundesregierung zur Schaffung eines KRITIS-Dachgesetzes bietet zudem die Chance, eindeutiger zu klären, was genau an kritischen Infrastrukturen kritisch ist und was nicht.

„Die Regulierung gibt nur einen Mindeststandard vor, das angemessene Schutzniveau muss jedes Unternehmen für sich selbst bestimmen.“

Janka Schwaibold, Rechtsanwältin und Partnerin,
Schalast LAW | TAX

Deep Dive Banking: Umfassende Regulierung sorgt für höheren Cyberschutz

Einige Bereiche innerhalb der kritischen Infrastrukturen erfüllen bereits einen hohen Cyberschutz aufgrund regulatorischer Vorgaben oder spezifischen Branchenstandards wie etwa der Finanzsektor. In Deutschland gibt es für die Finanzbranche verschiedene Regelungen.

Dazu gehört die Mindestanforderungen an das Risikomanagement (MaRisk) für Banken und andere Finanzdienstleister. Diese Anforderungen umfassen auch Vorgaben zum Cybersicherheitsmanagement und zur IT-Sicherheit, die von den betroffenen Unternehmen umgesetzt werden müssen. Die MaRisk setzen damit einen Standard für den Schutz der IT-Infrastruktur im Finanzsektor und stellen sicher, dass die Institute angemessene Sicherheitsmaßnahmen ergreifen, um sich vor Cyberangriffen zu schützen.

„Die MaRisk setzen einen Standard für den Schutz der IT-Infrastruktur im Finanzsektor und stellen sicher, dass die Institute angemessene Sicherheitsmaßnahmen ergreifen, um sich vor Cyberangriffen zu schützen."

Alexander Gebhard, Rechtsanwalt und Partner, Schalast LAW | TAX

Daneben sind die Bankaufsichtlichen Anforderungen an die IT (BAIT) sowie die Zahlungsdienstaufsichtlichen Anforderungen an die IT (ZAIT) Verordnungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), die sich auf die IT-Sicherheit im Finanzsektor konzentrieren. Die Verordnungen stellen Mindestanforderungen an die IT-Infrastruktur von Finanzinstituten und Zahlungsdienstleistern und legen fest, welche Schutzmaßnahmen gegen Cyberangriffe ergriffen werden müssen.

Zu den Anforderungen gehören unter anderem die Implementierung von Informationssicherheitsmanagement-Systemen, regelmäßige Sicherheitsüberprüfungen und Risikoanalysen sowie die Einrichtung von Krisenmanagement-Plänen. Wesentlicher Bestandteil sind zudem detaillierte Vorgaben zur sogenannten operativen Informationssicherheit. Deren Ziel ist es, dass die Banken sicherheitsrelevante Ereignisse noch zuverlässiger erkennen, zielgerichteter analysieren und regelmäßig die Wirksamkeit ihrer Informationssicherheitsmaßnahmen überprüfen. Zudem ist ein zentrales Meldesystem für kritische Sicherheitsvorfälle eingerichtet.

Der Digital Operational Resilience Act (DORA)[33] der Europäischen Kommission, der ebenfalls am 16. Januar 2023 in Kraft getreten ist, vereint bestehende Regulierungen zur Cybersicherheit und ergänzt sie. Die DORA-Verordnung schafft einen Rechtsrahmen für die digitale Betriebsstabilität, indem sie einheitliche Anforderungen für die Sicherheit der Netz- und Informationssysteme von Finanzunternehmen und Organisationen sowie kritischen Dritten, die im Bereich der Informations- und Kommunikationstechnologien (IKT) tätig sind, festlegt.

Um sicherzustellen, dass die Unternehmen Bedrohungen im Zusammenhang mit ihrer IKT standhalten, müssen zum Beispiel bedrohungsorientierte Penetrationstests durchgeführt werden. Die eigentliche Anwendung der Verordnung beginnt zwar erst im Januar 2025, gleichzeitig wird die Umsetzung der neuen Anforderungen die Banken im Betriebsalltag enorm fordern, um mit robusten IT-Systemen den zunehmenden Cybergefahren zu trotzen.

Die Einhaltung von regulatorischen Vorgaben und branchenspezifischen Auflagen ist für Finanzdienstleister unerlässlich. Die aktuelle Studie „Cybersicherheit in Zahlen"[34] zeigt, dass Angestellte in Banken und Versicherungen ein ausgeprägtes Sicherheitsbewusstsein haben, das in den meisten Fällen überdurchschnittlich ist. 68 Prozent der Befragten dieser Branche stimmen der Aussage zu, dass gesetzliche Regeln im Bereich IT-Sicherheit sinnvoll sind und dass sich die Unternehmen daran halten, auch wenn die Umsetzung sehr komplex ist.

Laut der Lünendonk-Studie 2022[35] sind nur ein Drittel der untersuchten Finanzdienstleister gut gegen Cyberangriffe geschützt, obwohl 97 Prozent der Befragten im Falle eines Angriffs schwer-

wiegende Schäden für ihr Unternehmen erwarten. Insbesondere der Verlust von Kundendaten und Reputationsschäden werden befürchtet. Obwohl 55 Prozent der Befragten das Risiko von DDoS-Angriffen als hoch einstufen, überprüfen nur sechs von zehn Finanzdienstleistern ihre IT-Systeme regelmäßig auf Schwachstellen.

Obwohl Banken und Versicherungen im Bereich IT-Sicherheit anderen Branchen voraus sind, dürfen sie in ihren Bemühungen nicht nachlassen. Auch die BaFin hat bereits Risiken aus Cyberattacken mit gravierenden Auswirkungen als eines der Fokusrisiken für das Jahr 2023 identifiziert.[36] Ein ausschlaggebender Hebel für mehr IT-Sicherheit ist das Sicherheitsbewusstsein der Mitarbeitenden. Ihr Wissen und ihre Reaktionsfähigkeit sind von entscheidender Bedeutung, um Cyberattacken frühzeitig zu unterbinden.

Allerdings dürfen Cyberrisiken im Finanzsektor nicht nur in den Instituten selbst überwacht werden, denn sie können auch durch ihre Kooperationen mit Dienstleistern betroffen sein. Finanzdienstleister lagern eine Vielzahl von Prozessen und Daten an Dritte aus, dadurch gibt es mehr angreifbare Schnittstellen. Dementsprechend müssen die Dienstleister ebenfalls angemessen gesteuert und kontrolliert werden.

Die BaFin überwacht daher ausgewählte IT-Mehrmandantendienstleister und ordnet Prüfungen an, um deren Risikomanagement in den Blick zu nehmen. Auf Grundlage des Finanzmarktintegritätsstärkungsgesetzes (FISG) kann die Aufsicht seit 2022 unmittelbar auf Auslagerungsunternehmen zugreifen, auch wenn diese nicht unmittelbar ihrer Aufsicht unterstehen. Damit soll indirekt die operative Resilienz vieler Unternehmen innerhalb des Finanzsektors gestärkt werden.

Insgesamt ist es wichtig, dass es spezifische Vorgaben und Standards gibt, um den Cyberschutz zu erhöhen. Die Umsetzung von Standards kann jedoch nur ein Teil eines umfassenden Cybersicherheitsmanagements sein. Alle Betreiber kritischer Infrastrukturen müssen zusätzlich eigene Schutzmaßnahmen ergreifen, um ihre Systeme und Daten vor Cyberangriffen zu schützen.

”

„Trotz hoher Sensibilisierung ist nur ein Drittel der Finanzinstitute gut gegen Cyberangriffe geschützt. Ein ausschlaggebender Hebel für mehr IT-Sicherheit ist das Sicherheitsbewusstsein.“

Jürgen Schreiner, Account Executive, Link11

Nachholbedarf bei KRITIS: Wer muss noch am meisten tun?

Im Gegensatz zum stark regulierten Finanzbereich gibt es mehrere kritische Infrastrukturen, die hinsichtlich ihrer Cybersicherheit noch Nachholbedarf haben.

Hier sind einige Beispiele:

Energieversorgung: Die Energieversorgung ist von zentraler Bedeutung für das Funktionieren von Gesellschaft und Wirtschaft. Die zunehmende Vernetzung von Stromnetzen und die Verwendung von Smart-Grid-Technologien schaffen jedoch neue Angriffsvektoren für Cyberkriminelle. Ein erfolgreicher Cyberangriff auf die Energieversorgung kann zu erheblichen Störungen im Stromnetz führen und im schlimmsten Fall zu einem landesweiten Stromausfall wie etwa 2015 in der Ukraine.[37]

Verkehr: Vernetzte Verkehrssysteme und künftig autonome Fahrzeuge können von Hackern manipuliert werden, um Verkehrschaos und sogar Unfälle zu verursachen. Darüber hinaus sind Flughäfen und Bahnhöfe anfällig für Cyberangriffe, da sie zunehmend auf digitale Systeme zur Steuerung von Flug- und Zugbewegungen angewiesen sind. Erst kürzlich kam es zu einem schwerwiegenden Ausfall am Frankfurter Flughafen.[38]

Gesundheitswesen: Krankenhäuser, Arztpraxen und andere medizinische Einrichtungen speichern sensible Patientendaten, die von Hackern gestohlen werden können. Ein Cyberangriff auf das Gesundheitswesen kann auch dazu führen, dass medizinische Geräte und Systeme manipuliert werden, was zu einer Gefahr für die Gesundheit von Patienten führen kann. Diese Erfahrung musste im März 2023 eines der wichtigsten Krankenhäuser in Barcelona machen.[39]

Ein genauer Blick auf den Bereich Energieversorgung offenbart den großen Nachholbedarf an unterschiedlichen Stellen. Ein wichtiger Aspekt ist dort die Lieferkette. Viele Energieversorger beziehen wichtige Komponenten und Dienstleistungen von Drittanbietern wie Software- und Hardwareanbieter, Ingenieurdienstleister oder Subunternehmer. Dies kann dazu führen, dass Schwachstellen in der Lieferkette ausgenutzt werden, um in das System einzudringen.

Ein weiterer Faktor ist die zunehmende Digitalisierung und Vernetzung der Energieversorgungssysteme, insbesondere im Zusammenhang mit der Einführung von Smart-Grid-Technologien. Darüber hinaus spielen veraltete IT-Systeme und unzureichende Cyber-Awareness bei Mitarbeitenden eine Rolle.

Insgesamt braucht es eine klare Definition von kritischen Infrastrukturen und eine kontinuierliche Verbesserung ihrer Cybersicherheitsmaßnahmen mit genauem Blick auf die Lieferketten. Nur so kann sichergestellt werden, dass sie gegen potenzielle Cyberangriffe ausreichend geschützt sind.

Sinnvolle IT-Sicherheitsstrategie erforderlich

Es ist völlig unbestritten, dass Digitalisierung und Vernetzung auch innerhalb der kritischen Infrastrukturen weiter voranschreiten. In Zukunft nimmt der Einsatz künstlicher Intelligenz zu und immer mehr automatisierte Systeme werden digital miteinander kommunizieren. Umso stärker geraten Produzenten und Versorger im Energiebereich, Banken im Finanzsektor oder Krankenhäuser im Gesundheitswesen ins Visier von Angreifern. Aus den Cyberangriffen folgen millionenschwere Produktionsausfälle und Versorgungsengpässe, die in letzter Konsequenz sogar Menschenleben gefährden oder im schlimmsten Fall sogar kosten können.

Warum sich kritische Infrastrukturen gegen DDoS-Angriffe schützen sollten:

1. **Betriebsunterbrechung:** DDoS-Angriffe können dazu führen, dass kritische Infrastrukturen ihre Dienste nicht mehr ordnungsgemäß bereitstellen können. Diese Betriebsunterbrechung kann sich negativ auf die öffentliche Sicherheit und das Wohlergehen der Bevölkerung auswirken.

2. **Rufschädigung:** Sind kritische Infrastrukturen aufgrund von DDoS-Angriffen nicht verfügbar, kann dies zu einem Vertrauensverlust führen und längerfristige Auswirkungen haben.

3. **Datenverlust und -manipulation:** DDoS-Angriffe können als Ablenkungsmanöver eingesetzt werden, um gleichzeitig vertrauliche Daten zu stehlen oder zu manipulieren, die für die Funktionalität der Infrastrukturen unerlässlich sind.

4. **Cyberkriminelle Motivationen:** Cyberkriminelle oder staatliche Akteure können DDoS-Angriffe nutzen, um politischen Druck auf Regierungen auszuüben, kritische Infrastrukturen zu sabotieren oder Lösegeld zu erpressen.

Bereits Anfang Mai 2022 warnten u. a. das Bundesamt für Verfassungsschutz und das hessische Landeskriminalamt vor DDoS-Angriffen auf deutsche IT-Infrastrukturen von Behörden und Unternehmen durch prorussische Hacktivisten-Gruppierungen. Tatsächlich wurden in der Folge mehrere deutsche Behörden und Ministerien, darunter das Verteidigungsministerium, der Bundestag, die Bundespolizei sowie mehrere Landespolizeibehörden, Opfer eines groß angelegten DDoS-Angriffes.[40]

Die aktuellen Angriffe mögen zwar nicht besonders wirkungsvoll gewesen sein, aber sie zeigen, wie verwundbar die kritischen Infrastrukturen sind. Es stellt sich die Frage, ob diese wirklich ausreichend geschützt sind.

Die vielfältigen Beispiele im Link11-DDoS-Report 2022 zeigen, welche Auswirkungen DDoS-Angriffe auf Unternehmen und Organisationen der kritischen Infrastruktur haben können. Dazu gehören etwa die Angriffe auf politische Institutionen in Norwegen, Deutschland und anderen NATO-Staaten, die Attacke auf den Londoner Hafen sowie der Ausfall des Ticketsystems der Österreichischen Bundesbahn.

Vor dem Hintergrund der immer weiter steigenden Zahl von Cyberangriffen müssen sich Betreiber kritischer Infrastrukturen und Unternehmen intensiv mit dem Thema digitale Gefahren und den entsprechenden Schutzmechanismen auseinandersetzen. Denn sobald es um mehr geht als ein Lösegeld, können die Auswirkungen der Cyberangriffe nicht nur auf die Geschäftsfähigkeit abzielen, sondern gesamtgesellschaftliche Dimensionen annehmen.

Unternehmen sollten ihre IT-Systeme so strukturieren, dass ein Angriff nur minimale Auswirkungen hat und kritische Teile des

Netzwerks nicht erreicht werden. Neben den umfangreichen Regularien bietet das NIST Cybersecurity Framework[41] einen Leitfaden mit fünf Kernelementen, um die nötige Cyberresilienz zu erreichen und den Anforderungen von NIS2 gerecht zu werden. Besonders im Bereich KRITIS ist im Hinblick auf die nationale Sicherheit ein durchgängiges und integriertes IT-Sicherheitskonzept erforderlich, das den reibungslosen Betrieb gewährleistet.

Carrierbasierte Modelle oder der Einsatz lokaler Hardware sind nicht mehr zeitgemäß, da diese in der Regel die manuelle Erkennung und den reaktiven Schwenk des Datenverkehrs voraussetzen. Dieser Prozess ist in der Praxis häufig langatmig und fehleranfällig. Je nach Betriebsmodell des Unternehmens erfordert der ITIL-konforme IT-Betrieb Freigaben für die Durchführung eines Emergency Change und die manuelle Benachrichtigung des Providers. Es vergeht kostbare Zeit und die Betriebsunterbrechung ist nahezu gewiss. Ungeachtet der eingesetzten Technologie weist allein das Betriebskonzept systemische Schwächen auf und wirkt nicht mehr zeitgemäß.

Gleichzeitig kommt es in vielen Fällen zu menschlichem Versagen. Darüber hinaus sind die carrierbasierten Modelle zum Teil mit minimal ausgestatteten SLAs hinterlegt. Es fehlt in der Regel garantierte Schutzbandbreite oder eine vertraglich garantierte Time-to-mitigate (TTM) für alle Angriffsarten. Zu allem Überfluss behält sich der Carrier vor, den gesamten Datenverkehr für die Dauer des Angriffs zu verwerfen. Dieses sogenannte Null-Routen kann mitunter Stunden oder Tage lang andauern, wie im Jahr 2021 bei der neuseeländischen Börse geschehen.[42]

Checkliste – Was sollten KRITIS und andere Unternehmen tun?

	KRITIS	Unterhalb KRITIS
Identifikation relevanter Regelungen und Schwellenwerte	✓	✓
Bestimmung KRITIS	✓	**Regelmäßige Kontrolle**
Registrierung	✓	**Falls spezialgesetzliche Pflicht + Ggf. freiwillig zur Erleichterung von Informationsflüssen**
Abgleich Schutzstandard	✓	✓
Regelmäßige, umfassende Risikobetrachtungen	✓	✓
Kontinuierliche Prüfung der Cybersecurity-Schutzmaßnahmen	✓	✓
Feuerprobe	✓	✓
Integriertes IT-Sicherheitskonzept	✓	✓

Effektive IT-Schutzlösungen für die Zukunft

Link11 bietet effektive IT-Schutzlösungen, die Unternehmen vor Cyberbedrohungen umfassend schützen und ihre Cyberresilienz stärken. Durch den Einsatz künstlicher Intelligenz und maschinelles Lernen wird eine kontinuierliche Überwachung des Datenverkehrs gewährleistet. Der Datenverkehr wird in Echtzeit gefiltert, um Anomalien oder Angriffe schnell zu erkennen und darauf zu reagieren. Im Gegensatz zu traditionellen Lösungen bietet Link11 eine hochgradig skalierbare, automatisierte und präzise Abwehr von DDoS-Angriffen, die auch komplexe Angriffe stoppen kann.

On-Premise-Lösungen sind zumeist nicht in der Lage, komplexe Angriffe zu stoppen. So unterwandern beispielsweise Angriffe mit niedriger Bandbreite, sogenannte Carpet Bombing-Attacken, häufig das Radar und bringen das IT-Backend zum Kollabieren.

Wenn ein Angriff erst die IT-Systeme eines Unternehmens erreicht, ist es schon zu spät. Auf der anderen Seite können cloudbasierte Lösungen den Datenverkehr in Echtzeit filtern, analysieren und sogar blockieren, bevor dieser auch nur in die Nähe der IT-Systeme eines Unternehmens gelangt.

Nicht zuletzt haben die Störungen der Lieferketten im Zuge der COVID-19-Pandemie deutlich aufgezeigt, wie vernetzt und anfällig unsere Informations-, Waren- und Zahlungsströme heute sind. Unternehmen müssen daher Vorkehrungen treffen, um die Wirkung und Dauer von DDoS-Angriffen auf technischer Ebene wirksam einzudämmen. Auf strategischer Ebene müssen Unternehmen die internen, aber auch die unternehmensübergreifenden Risiken in ihrer ganzen Breite und Tiefe identifizieren, bewerten und schließlich eindämmen. Im Bereich der KRITIS impliziert dies, seine Partner auch unter dem Gesichtspunkt der Resilienz gegenüber Cyberangriffen auszuwählen und die passenden Schutzmechanismen einzusetzen.

Traditionelle Schutzlösungen für Netzwerk- und Infrastruktursicherheit bauen allzu oft auf die manuelle Bewertung von Vorfällen und statische, musterbasierte Bewertung der Daten. Dieser zeit- und ressourcenintensive Ansatz hat angesichts der wachsenden Komplexität von IT-Sicherheit keine Zukunft. Neue Angriffstechniken unterlaufen das Radar, da sie dem Muster nicht entsprechen. Die vorhandene Automation greift nicht – es folgt der Schaden. Die notwendigen sinnvollen wie effektiven IT-Sicherheitsstrategien beinhalten permanentes Fragen und Simulieren des Ernstfalles sowie automatisierte Lösungen, um die Schwächen in den Betriebsmodellen sowie menschliches Versagen zu minimieren und den erforderlichen Schutz zu gewährleisten.

Für einen ganzheitlichen Schutz von IT-Infrastrukturen und kritischen Anwendungen und zur Stärkung der Cyberresilienz setzt Link11 mit seiner integrierten Cloud-Security-Plattform auf künstliche Intelligenz, maschinelles Lernen, Automatisierung und Echtzeit-Abwehr. Basierend auf diesen Schlüsseltechnologien schützt die Link11 Cloud-Security-Plattform Unternehmen auf Web- und Netzwerk-Ebene umfassend vor Cyberbedrohungen.

Wenn Sie Ihre Infrastruktur, Netzwerke und Applikationen gegen Cyberattacken schützen möchten, dann sprechen Sie mit den Cyberresilienz-Experten von Link11. Die integrierte Cloud-Security-Plattform von Link11 bietet eine ganzheitliche Lösung, die auf den neuesten Technologien basiert und Unternehmen vor wandlungsfähigen, komplexen und intensiven DDoS-Angriffen schützt.

Ansprechpartner

Jens Rieser
Account Executive
Link11

Jürgen Schreiner
Account Executive
Link11

Alexander Gebhard
Rechtsanwalt und Partner
Schalast LAW | TAX

Janka Schwaibold,
Rechtsanwältin und Partnerin
Schalast LAW | TAX

Nachweise

[1]https://de.wikipedia.org/wiki/Anschlag_auf_die_Nord-Stream-Pipelines

[2]https://de.wikipedia.org/wiki/Anschlag_auf_die_Deutsche_Bahn_am_8._Oktober_2022

[3]https://www.golem.de/news/webseiten-gestoert-cyberangriff-auf-polizei-und-behoerden-2304-173218.html

[4]https://www.emcrc.co.uk/post/killnet-declare-war-on-the-uk-and-nine-other-nations

[5]https://zero.bs/ddos-as-attackvector-for-state-sponsoredhacktivist-groups-in-times-of-crisis.html#evolution_of_killnet

[6]Einteilung gemäß Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
https://www.bbk.bund.de/SharedDocs/Downloads/DE/KRITIS/kritis-sektoren-brancheneinteilung.pdf?__blob=publicationFile&v=4

[7]https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html

[8]Durch die neue Verordnung wurden zwei neue Anlagenkategorien aufgenommen: LNG-Anlagen und Landstationen für Seekabel.

[9]https://digital-strategy.ec.europa.eu/de/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks

[10]https://eur-lex.europa.eu/eli/dir/2022/2555

[11]https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829

[12]https://netzpolitik.org/2022/kritis-dachgesetz-innenministerin-faeser-will-kritische-infrastruktur-physisch-besser-schuetzen/

[13]https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/12/kritis-eckpunkte.html

[14]https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2022/eckpunkte-kritis.pdf

[15]Informationsangebot: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html

[16]Informationsangebot: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Pflichten-fuer-KRITIS-Betreiber/Pflichten-fuer-KRITIS-Betreiber_node.html;jsessionid=C3E08B77C2927ACC6E0DF0551169C84F.internet482

[17]Sektorspezifische Informationen: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Sektorspezifische-Infos-fuer-KRITIS-Betreiber/sektorspezifische-infos-fuer-kritis-betreiber_node.html

[18]Vgl. § 11 Abs. 1c EnWG

[19]Gilt für Bereiche der öffentlichen Telekommunikation, Energienetze und bestimmte (nach KritisV).

[20]Vgl. IT-Sicherheitskatalog F.I. „Zertifizierung“: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=2

[21]Einhaltung kann von BNetzA überprüft werden, vgl. § 11 Abs. 1a EnWG.

[22]Vgl. § 53 ZAG „Beherrschung operationeller und sicherheitsrelevanter Risiken“

[23]Hier stellt die DKG ein Starterpaket zur Unterstützung zur Verfügung. https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/

[24]§ 2 Abs. 13 BSiG: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[25]Mitunter entstehen erhebliche Schäden durch Angriffe, z. B. bei ThyssenKrupp im Jahr 2016, als eine Cyberattacke nicht nur zu Datenverlusten sondern zu physischen Schäden an einem Hochofen führte.

[26]Dem BSI müssen die dafür nötigen Informationen bereitgestellt werden.

[27]https://www.gesetze-im-internet.de/bsig_2009/__14.html

[28]Vgl. Art. 24ff. DSGVO; für Bußgelder vgl. Art. 83 DSGVO.

[29]Beispiel USA: Pipeline im Mai 2021, Folge: vorrübergehende Engpässe an der gesamten Ostküste, Lösegeldzahlung von über 4 Mio. Dollar und Einstellung des Betriebs, um Angriff zu bewältigen.

[30]insbesondere die regelmäßigen Nachweispflichten

[31]Ergibt sich aus der BSI-KritisV; beispielhaft für den Sektor Energie, vgl. Anhang Energie Teil 1 Nr. 4: https://www.gesetze-im-internet.de/bsi-kritisv/anhang_1.html; BSI-KritisV: https://www.gesetze-im-internet.de/bsi-kritisv/index.html#BJNR095800016BJNE000301116

[32]Risikofaktor Mensch: Die häufigsten Angriffe auf KRITIS-Unternehmen sind Phishing-Attacken (56 %) – also eine Angriffsart, die Mitarbeitende dazu verleiten sollen, infizierte Anhänge oder Links zu öffnen; ZfK, 03.11.2021.

[33]https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

[34]https://www.gdata.de/cybersicherheit-in-zahlen

[35]https://www.luenendonk.de/produkte/studien-publikationen/luenendonk-studie-2022-von-cyber-security-zur-cyber-resilience-wie-finanzdienstleister-auf-die-neue-bedrohungslage-reagieren-it/

[36]https://www.bafin.de/SharedDocs/Downloads/DE/Fokusrisiken/2023_Fokusrisiken.html

[37]https://de.wikipedia.org/wiki/Hackerangriff_auf_die_ukrainische_Stromversorgung_2015

[38]https://www.hessenschau.de/wirtschaft/fehlendes-notfallsystem-sicherheitsexperte-wundert-sich-ueber-it-ausfall-bei-lufthansa-v1,lufthansa-it-ausfall-sicherheit-100.html

[39]https://apnews.com/article/barcelona-hospital-cyberattack-ransomware-37e0fee33798c56459e63866ca8b449f

[40]https://www.tagesschau.de/inland/cyberattacke-bundesregierung-ddos-101.html

[41]https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[42]https://www.handelsblatt.com/technik/thespark/new-zealand-exchange-cyber-angriffe-legen-boersenhandel-in-neuseeland-dritten-tag-in-folge-lahm/26132196.html?ticket=ST-11419945-KVHoCJJoP3gicc6rh3dp-ap5

Kontakt

Link11 GmbH
Lindleystr. 12
60314 Frankfurt