Gaia-X
FEDERATION SERVICES
GXFS

WHITEPAPER

Informationssicherheit kritischer Infrastrukturen

Recht und Regulierung für Gaia-X und die Gaia-X Föderationsdienste

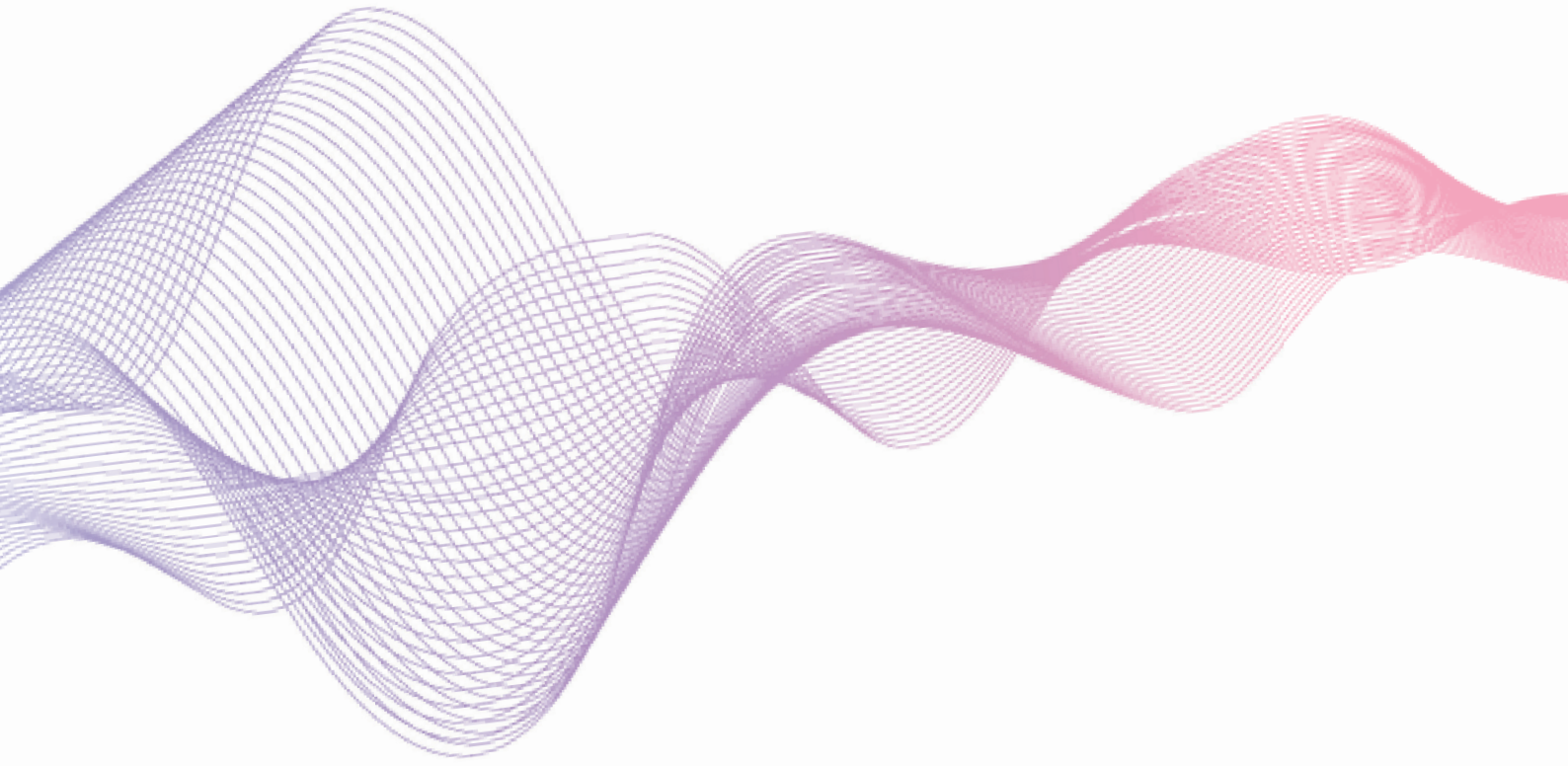
Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

www.gxfs.de

Inhalt



Informationssicherheit kritischer Infrastrukturen: Recht und Regulierung für Gaia-X und die Gaia-X Föderationsdienste

Einleitung

Legalitätspflicht digitaler Dienstleister

Für alle Akteure der Bereitstellung von öffentlichen oder privaten Dienstleistungen ist es selbstverständlich, sich innerhalb der Grenzen von Recht und Gesetz zu bewegen. Im Rechtsstaat ist Verwaltungshandeln stets an Verfassungsgrundsätzen und Gesetzmäßigkeit ausgerichtet, während die Privatwirtschaft durch die einschlägigen Leitungs- und Sorgfaltspflichten des Aktien- oder GmbH-Gesetzes gebunden ist, an die sich Vorstände und Geschäftsführung halten müssen. Aber der Rechtsrahmen, an dem sie alle sich orientieren, ist ständigen Änderungen unterworfen. Für digitale Angebote unter Stichworten wie Cloud-Computing, Rechenzentrumsleistungen und digitaler Kommunikation im allerweitesten Sinne hat sich die Rechtslage nicht nur inhaltlich fundamental gewandelt: Vor allem der Geltungsbereich der Regulierung wurde erheblich ausgeweitet, so dass heute schon – und in Zukunft noch viel mehr – Unternehmen und andere Institutionen spezifischen Verpflichtungen unterliegen, die in der Vergangenheit noch ohne solche formalen Regeln funktionierten.

Geänderter Rechtsrahmen führt zu mehr Regulierung in erweitertem Geltungsbereich

Sind wir "kritische Infrastruktur", und wenn ja, was sind die Konsequenzen?

Dieses Whitepaper versucht, einen blinden Fleck auszuleuchten, der in weiten Teilen der digitalen Wirtschaft existiert und auch im Gaia-X-Umfeld und seinen Föderationsdiensten bislang noch leicht übersehen werden konnte: Sind die Betriebsgrundlagen der eigenen Plattform und ihrer Dienstleistungen als sogenannte „kritische Infrastruktur" einzustufen und damit einer staatlichen Regulierung unterworfen? Welche Kriterien und Maßstäbe werden angelegt, um zu einer solchen Einstufung zu gelangen? Welche gesetzlichen Pflichten und regulatorischen Maßnahmen resultieren daraus, wenn der Betrieb einer Dienstleistung als „kritisch" gilt? Welche technischen und organisatorischen Standards in Bezug auf die Informationssicherheit sind dann einzuhalten?

Fortwährende Änderungen der Gesetzgebung

Um diese Kernfragen der kritischen Infrastrukturen - sowohl ihres Betriebs als auch der Regulierung, der sie unterliegen - angemessen zu beantworten, sind ein breites Verständnis und vertiefte Kenntnisse notwendig. Man muss sich zunächst damit vertraut machen, dass die Rahmenbedingungen laufend aktualisiert und verändert werden. Mit den aktuellen Entwicklungen der gesetzlichen Grundlagen und der daraus entstehenden Verordnungen zu ihrer Umsetzung wird sowohl der Kreis der Adressaten weiter als bisher gezogen als auch die Anzahl der innerhalb der betroffenen Sektoren tätigen Unternehmen um ein Vielfaches vergrößert. Dieses Whitepaper ist auf dem Stand der Gesetzgebung von Anfang März 2023 verfasst, bietet also bereits einen verlässlichen Überblick über die in Kraft befindlichen deutschen und europäischen Rechtsrahmensetzungen zu diesem Zeitpunkt.

Aktueller Stand März 2023

Fall 1: Gaia-X ist kritische Infrastruktur

Fall 2: Gaia-X-Kunden sind kritische Infrastruktur

Bei der Analyse der Regelwerke und der Evaluierung ihrer Anwendbarkeit auf die Akteure im Gaia-X-Kontext dürfen zwei Blickwinkel nicht aus den Augen verloren werden: Erstens, kann durchaus selbst als Betreiber kritischer Infrastruktur (in Deutschland gern auch als „KRITIS" abgekürzt) eingestuft werden, wer innerhalb der Gaia-X-Umgebung als Anbieter - oder "Föderator" - auftritt. Zweitens, muss die Problematik eines Dienstleisters, dessen Kunden ihrerseits Betreiber kritischer Infrastruktur sind, getrennt gewürdigt werden. Auch wenn im Einzelfall vielleicht keine Einstufung des Dienstleisters als KRITIS-Unternehmen erfolgt, müssen ge-

gebenenfalls Nachweise erbracht werden, die im Rahmen der Nachweis-, Berichts- und Meldepflichten sowie der Einhaltung spezifischer Anforderungen dieser Kunden erforderlich sind. Als Outsourcing-Partner eines KRITIS-Betreibers muss man sich gegebenenfalls also Regeln unterwerfen, die ohne einen solchen Kunden, nur aus der eigenen Geschäftstätigkeit, nicht unbedingt resultierten.

Exkurs: Finanzmarktaufsicht

Doppelte Regulierung

Drittdienstleister unterliegen auch der Aufsicht

Ein Beispiel: Sektorspezifisch regulierte Unternehmen wie Kreditinstitute und Versicherungen unterliegen der Kontrolle durch unterschiedliche Aufsichtsstellen, sofern sie als kritische Infrastrukturen eingestuft sind. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) weist darauf hin, dass eine Mehrbelastung der Institute durch die doppelte Aufsichtsfunktion "bestmöglich reduziert" werden soll. Trotzdem gilt für die etwa 90 Unternehmen im Finanzsektor, die derzeit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Betreiber kritischer Infrastruktur registriert sind, dass sie weiterhin den gesetzlichen Anforderungen der Finanzmarktregulierung nach Kreditwesengesetz (KWG), Zahlungsdiensteaufsichtsgesetz (ZAG) bzw. Versicherungsaufsichtsgesetz (VAG) und der damit verbundenen Aufsicht durch die BaFin (und die größten unter ihnen auch dem einheitlichen europäischen Bankenaufsichtsmechanismus) unterworfen sind, aber zusätzlich auch die gesetzlichen Anforderungen an Betreiber kritischer Infrastrukturen nach der KRITIS-Verordnung (KritisV) des BSI erfüllen müssen. Den Dienstleistern, die für Finanzunternehmen Teile ihrer kritischen Infrastruktur betreiben, kann deshalb auferlegt sein, dass die BaFin unmittelbar bei ihnen zu Prüfungen und Anordnungen berechtigt ist, sofern für die Banken wesentliche Aktivitäten an sie ausgelagert werden.

Ähnliche Verflechtungen von Anforderungen und behördlicher Aufsicht gibt es etwa im Energiesektor und für Telekommunikationsbetreiber - für sie wären die beiden relevanten Aufsichtsbehörden die Bundesnetzagentur (BNetzA) und das BSI. Die Mechanismen der mehrseitigen Kontrolle skizzieren wir später, aber wichtig ist vor allem: Jede Institution, die zur Aufsicht über Betreiber kritischer Infrastrukturen befugt ist, greift im Zweifel auch auf diejenigen durch, die lediglich als Drittdienstleister für die regulierten Sektoren tätig sind.

Gaia-X ist kritische Infrastruktur?

Zu untersuchen ist auch, wie sich der regulatorische bzw. gesetzliche Rahmen auf Gaia-X als Betreiber einer kritischen Infrastruktur selbst auswirkt. Ob es sich bei Gaia-X oder den Akteuren der Plattform überhaupt um KRITIS-Unternehmen handeln kann, ist immerhin zu diskutieren. Spätestens unter der Maßgabe der Anfang des Jahres 2023 in Kraft befindlichen europäischen Gesetzgebung ist aber davon auszugehen, dass weite Teile der Gaia-X-Umgebung und der Föderationsdienste zumindest potenziell als kritische Infrastruktur einstufbar sind.

Pflichten für KRITIS-Betreiber, die externe Dienste nutzen

Mitbehandelt werden schließlich die Maßgaben für Betreiber kritischer Infrastrukturen, wenn sie zum Beispiel Gaia-X-Dienste in Anspruch nehmen. In allen Mitgliedstaaten der Europäischen Union gelten hier einheitliche Verpflichtungen, wie externe Dienstleister in das Risikomanagement der KRITIS-Betreiber zu integrieren sind, um den Anforderungen an die Informationssicherheit ihrer kritischen Infrastruktur zu genügen. Solchen Pflichten müssen vertragliche Grundlagen und Kontrollbefugnisse Geltung verschaffen, deren Durchgriffstiefe über die üblichen Service Level Agreements zwischen Dienstleistern und Kunden deutlich hinausgehen.

Voraussetzungen, Rechtsgrundlagen und Branchenstandards

Dieses Whitepaper kann keine vollständige Matrix von sektorspezifischen Sicherheitsstandards, Berichts- und Meldepflichten zusammenstellen, die für Unternehmen in den jeweiligen Bereichen maßgeblich sind. Es entfaltet aber einen breiten Überblick über die wesentlichen Voraussetzungen für einen regulierungskonformen Betrieb kritischer Infrastrukturen. Wir beschränken uns dabei auf eine Darstellung der Rechtsgrundlagen und einschlägiger Branchenstandards, die im jeweiligen Kontext zur Anwendung kommen. Einen Ausblick geben wir zu konkreten Vorschlägen, die in einer Einzelfallbewertung entstehen und zur Umsetzung empfohlen werden könnten. Ohne eingehende Betrachtung des Kontexts ist der richtige Anspruch an die Dienste und die Umsetzung der Anforderungen an ihre Informationssicherheit kaum eindeutig zu formulieren. Auch dies gilt

auf beiden Seiten, sowohl der Föderatoren und der Gaia-X-Infrastruktur als auch der Anwender, die als Betreiber kritischer Infrastruktur auf die Einhaltung ihrer eigenen Vorgaben achten. Notwendig ist hier zunächst nur die Einsicht, dass zur Konformität mit Gesetzen und Regulierungen für kritische Infrastrukturen konkrete Maßnahmen auch im Gaia-X-Umfeld unverzichtbar sind.

Kontextualisierung für das Gaia-X-Umfeldt

Kritische Infrastrukturen in der deutschen Gesetzgebung und Regulierung

Kritische Infrastrukturen sind Einrichtungen der Daseinsvorsorge, die von besonderer Bedeutung für das öffentliche Leben sind, und deren Störung oder Ausfall die elementaren Bedürfnisse der Menschen erheblich beeinträchtigen könnte oder sogar katastrophale Folgen hätte. Der abstrakte Begriff bezeichnet die Gesamtheit aller technischen und organisatorischen Systeme, ohne deren Funktionieren der Fortbestand der Gesellschaft gefährdet wäre. Im Vordergrund stehen dabei die Energieversorgung, Transport und Verkehr, Staat und Verwaltung, Ernährung, Wasser, Gesundheit, auch Medien und Kultur, und nicht zuletzt die digitale Infrastruktur: Informationstechnik und Telekommunikation.

Begriffsdefinition "kritische Infrastruktur": Einrichtungen der Daseinsvorsorge

Solche Infrastrukturen waren bis in die 1990er Jahre ganz überwiegend staatlich betrieben. Ihre Privatisierung hat den Staat aber nicht aus der Infrastrukturverantwortung entlassen, die sich in Deutschland aus dem Grundgesetz ergibt (Art. 20 Abs. 1 GG). Das Sozialstaatsprinzip, das dort verankert ist, ist die Grundlage der Regulierungsverantwortung überall dort, wo die öffentliche Hand sich aus der eigentlichen Leistung der Daseinsvorsorge zurückgezogen hat. Für die kritischen Infrastrukturen resultiert aus dieser Verantwortung die regulatorische Aufgabe, Mindestanforderungen an die Betreiber nun meist privatwirtschaftlich organisierter Dienste zu stellen, um die Versorgungssicherheit auch dort zu gewährleisten, wo der Staat nicht unmittelbar selbst handelt

Verantwortung des Staates für die Regulierung kritischer Infrastrukturen

Selbstregulierung der Betreiber kritischer Infrastrukturen

Seit von kritischer Infrastruktur die Rede ist, wird die Frage der Zugehörigkeit von Versorgungsunternehmen oder Institutionen der öffentlichen Hand zu dieser Gruppe von besonderer Bedeutsamkeit für das öffentliche Leben immer wieder neu und häufig anders beantwortet. Ob ein Unternehmen oder eine Behörde kritische Infrastruktur bereitstellt, ist dabei genauso schwierig zu bestimmen wie die Bewertung, welchen Grad der Bedeutsamkeit für die Aufrechterhaltung des öffentlichen Lebens die Institution hat. Der erste Ansatz nach Einführung des Begriffs der kritischen Infrastruktur in die Debatte über Gefahren und Risiken für die Öffentlichkeit in Deutschland bestand zunächst darin, beide Fragen durch die Betreiber einer mutmaßlich kritischen Infrastruktur selbst beantworten zu lassen: Sowohl der Stellenwert einer Dienstleistung für die Versorgungssicherheit als auch das Ausmaß ihrer Kritikalität wurden von den Institutionen selbst eingeschätzt.

Selbsteinschätzung der Betreiber ist Basis der Einstufung als "kritische Infrastruktur"

Abgelöst wurde diese frei zu vereinbarende Evaluierung der Kritikalität mit der Einführung einer Dachstrategie für die Informationssicherheit durch die Bundesregierung, unter Federführung des Innenressorts und fachlich begleitet durch das BSI. Der sogenannte "Umsetzungsplan für die Kritischen Infrastrukturen" (UP KRITIS) resultierte aus dieser 2005 veröffentlichten nationalen Informationssicherheitsstrategie unter dem Titel "Nationaler Plan zum Schutz der Informationsinfrastrukturen" (NPSI). Obwohl der NPSI bereits 2011 durch eine stärker vernetzte Cybersicherheitsstrategie der Bundesregierung abgelöst wurde, besteht der UP KRITIS als öffentlich-private Partnerschaft zur Selbstregulierung mit heute über 800 teilnehmenden Organisationen fort. Auch der gleichzeitig ins Leben gerufene "Umsetzungsplan für die Bundesverwaltung" (UP Bund) ist

Umsetzungsplan KRITIS

ÖPP zur Selbstregulierung

weiterhin in Anwendung und wird laufend aktualisiert. Der UP Bund regelt zum Beispiel die Voraussetzungen für den Einsatz von Informationstechnik, die Anschlüsse an die Netze des Bundes und andere technische Rahmenbedingungen für den Datenverkehr von Verwaltungen, verlangt in erster Linie aber formale und organisatorische Grundlagen wie die Einführung von Informationssicherheitsmanagementsystemen (ISMS) in allen Institutionen des Bundes, Meldepflichten und anderes mehr.

Umsetzungsplan Bund

Unabhängig von den inzwischen etablierten gesetzlichen Grundlagen der Einstufung als Betreiber kritischer Infrastrukturen und den verpflichtenden Regelwerken wird die Gremienarbeit der Mitgliedsinstitutionen in UP KRITIS und UP Bund fortgeführt. So unterhält der UP KRITIS eine Reihe von Branchen- und Themenarbeitskreisen, deren Mitglieder gemeinsam Konzepte und Handlungsempfehlungen für die Informationssicherheit bei KRITIS-Betreibern entwickeln und vereinbaren. Arbeitskreise für die KRITIS-Sektoren von Energie bis Telekommunikation und Internet stehen neben solchen für Themen wie die gesetzlich vorgeschriebenen Audits und Standards oder gemeinsame Übungen für Krisensituationen. Ein eigener Branchenarbeitskreis für Datacenter und Hosting wurde ebenfalls etabliert. Für die Mitgliedsunternehmen entstehen im UP KRITIS zum Beispiel Musterverträge - Service Level Agreements - für Lieferanten von Hard- und Software zur Verwendung in kritischen Infrastrukturen, um ein hohes Sicherheitsniveau bei den verwendeten Komponenten verbindlich zu verankern. Da es keine gesetzliche Vorgabe für den Mindeststandard bei solchen Komponenten gibt, ist die vertragliche Vereinbarung die einzige Möglichkeit, die Lieferanten auf den Anforderungskatalog und die Best Practices der Informationssicherheit festzulegen. Der UP KRITIS ist darüber hinaus als Vertretung der Unternehmen im Nationalen Cyber-Sicherheitsrat der Bundesregierung tätig und damit aktiver Teilnehmer an strategischen Weichenstellungen zum Schutz der Informationssicherheit für Staat und Gesellschaft.

Gemeinsame Entwicklung von Handlungsempfehlungen und Konzepten

Vertragliche Grundlagen schaffen verbindliches Sicherheitsniveau

Gesetzgebung mit Relevanz für kritische Infrastrukturen

Die gesetzlichen Rahmenbedingungen für die Betreiber kritischer Infrastrukturen sind in einer Reihe von Einzelgesetzen und Verordnungen festgelegt, die in den letzten zwanzig Jahren entwickelt, ständig erweitert, präzisiert und aktualisiert wurden. Dabei steht vor allem der Aspekt des Schutzes der Netzwerke und Informationssysteme im Fokus, die für die Aufrechterhaltung des Betriebs kritischer Infrastrukturen benötigt werden. Zeitlich sehr eng beieinander liegend ist in Deutschland und in der Europäischen Union eine verbindliche Festlegung von Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus in der Informationstechnik und den Netzwerken erfolgt, die dem Betrieb kritischer Infrastrukturen dienen.

Gesetzgeberische Festlegungen in Deutschland und Europäischer Union im gleichen Zeitraum

Der aktuell in Deutschland gültige Rechtsrahmen für die Betreiber der kritischen Infrastruktur wird gebildet aus folgenden Einzelgesetzen:

Deutscher Rechtsrahmen

- BSI-Gesetz (BSIG)
- Telekommunikationsgesetz (TKG) und Telemediengesetz (TMG)
- Energiewirtschaftsgesetz (EnWG) und Atomgesetz (AtG)
- Fünftes Buch Sozialgesetzbuch (SGB V)

Wichtigste Verordnung, die aus dem BSIG abgeleitet wurde, ist die KRITIS-Verordnung (BSI-KritisV von 2016, geändert 2017 und 2021). Sie ist maßgeblich für die Einstufung von Betreibern kritischer Infrastrukturen oberhalb definierter Schwellenwerte, und setzt den Rahmen für die Umsetzung der Anforderungen des Gesetzes.

KRITIS-Verordnung

Die Bezeichnung "IT-Sicherheitsgesetz" (IT-SiG), die in der öffentlichen Diskussion häufig wie ein Markenname verwendet wird ("IT-SiG", "IT-SiG 2.0"), referenziert Artikelgesetze, die eine Sammlung von neuen oder geän-

IT-SiG

derten Paragraphen mehrerer Gesetze beinhalten - ein eigenständiges Fachgesetz für die Informationssicherheit gibt es unter diesem Titel nicht.

Europäischer Rechtsrahmen

Die deutsche Gesetzgebung ist eng mit dem europäischen Rechtsrahmen verwoben, der vor allem aus zwei Richtliniendokumenten besteht:

- NIS - Network and Information Security (NIS 1 2016, NIS 2 2022)
- CER - Critical Entities Resilience (2022; löst die Vorgängerrichtlinie ECI - European Critical Infrastructures von 2008 ab)

Zu den weiteren rechtlich bindenden Vorgaben der Europäischen Union gehören Richtlinien und Verordnungen, die sektorspezifische oder andere Belange der Informationssicherheit berühren.

- DORA - Digital Operational Resilience Act (Richtlinie und Verordnung 2022 in Kraft getreten; regeln die digitale Betriebsstabilität im Finanzsektor)
- CRA - Cyber Resilience Act (noch im Verfahren, Verabschiedung voraussichtlich 2023; regelt Anforderungen zur Informationssicherheit von IT-Produkten, ohne digitale Dienste)

Chronologie der Rechtsrahmen in Deutschland und Europa

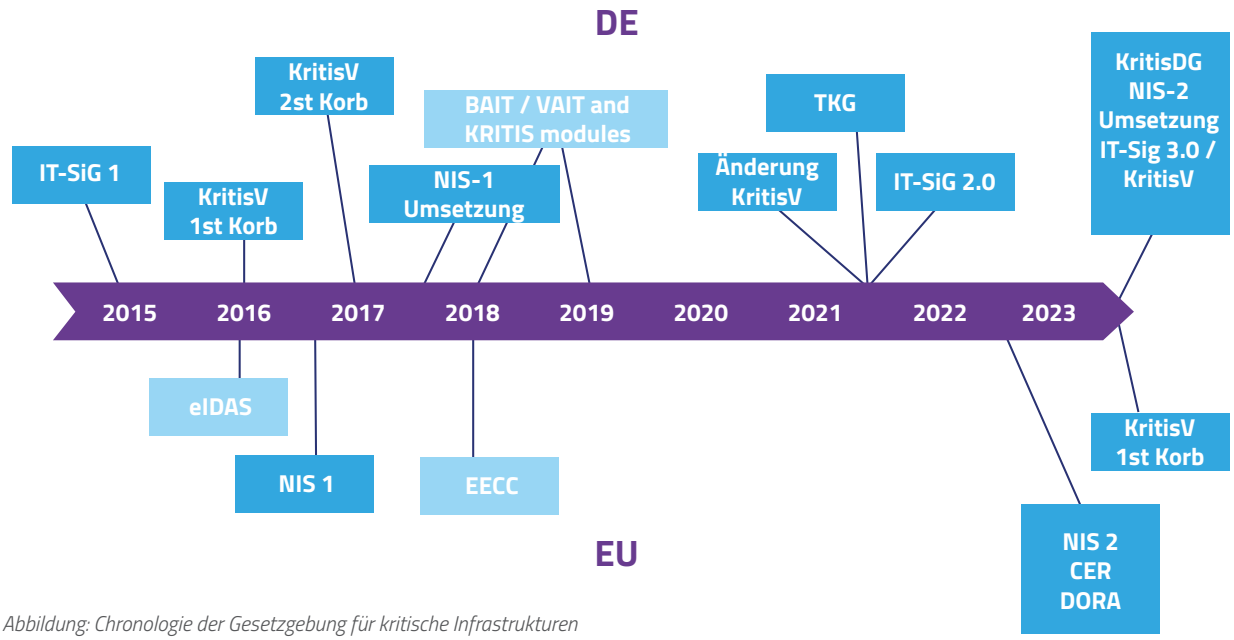


Abbildung: Chronologie der Gesetzgebung für kritische Infrastrukturen

BSI-Gesetz und KRITIS-Verordnung (KritisV)

Maßgeblich für die Informationssicherheit kritischer Infrastrukturen ist innerhalb des deutschen Rechtsrahmens in erster Linie das BSI-Gesetz. In den Eckpunkten zu einem künftigen "KRITIS-Dachgesetz" (KritisDG), die im Dezember 2022 im Kabinett verabschiedet wurden, wird darauf hingewiesen, dass es noch kein "sektoren- und gefahrenübergreifendes" Gesetz gibt, das die uneinheitliche oder fehlende Regelung des physischen Schutzes von kritischer Infrastruktur aufgreift. Während also mit dem angekündigten KritisDG erstmals auf das Gesamtsystem abgezielt wird, ist die Cybersicherheit kritischer Infrastrukturen bereits umfassend im BSIG geregelt.

§§ 8a und 8b BSIG

Gesetzliche Anforderungen: Stand der Technik und Nachweispflicht

Wer als Betreiber kritischer Infrastruktur identifiziert wird, muss nach dem BSIG erstens angemessene Sicherheitsvorkehrungen nach dem Stand der Technik bereithalten (§ 8a Abs. 1 BSIG) und zweitens regelmäßige Nachweispflichten erfüllen (gemäß § 8a Abs. 3 BSIG). Wie beim Datenschutz in Art. 32 der DSGVO bzw. dem Bundesdatenschutzgesetz (BDSG, § 71) wird auch im BSIG darauf verzichtet, eine Konkretisierung vorzunehmen, was genau unter dem jeweils zu berücksichtigenden Stand der Technik zu verstehen ist. Den Maßstab für die Einhaltung technischer Anforderungen in dieser Weise offen zu lassen, erlaubt laufende Anpassungen an die Entwicklung von Risiken und ihrer Behandlung, die durch Vorgaben konkreter Maßnahmen eher eingeschränkt würden. "Stand der Technik" ist als unbestimmter Rechtsbegriff jahrzehntelang eingeführt und wird auch vom Bundesverfassungsgericht schon seit 1978 akzeptiert. Gemeint ist, dass eine vollständige Sicherheit nicht möglich sei, deshalb aber nicht auf die Anwendung von Technologien insgesamt verzichtet werden könne: Sofern dem "Stand der Technik" angemessene Maßnahmen zur Sicherung der Informationstechnik ergriffen werden, sind die Folgen trotz angemessener Maßnahmen entstehender Vorfälle "unentrinnbar und insofern als sozialadäquate Lasten" zu tragen.

Risikobehandlung wird laufend angepasst

Auch wenn sich die dynamische Ausrichtung am Stand der Technik also bewährt hat und als Richtschnur den Regelfall für Nachweise angemessener Sicherheitsvorkehrungen dient, lässt das BSIG zu, dass in Form von Branchenstandards konkrete Maßnahmen formuliert werden. Die Einhaltung dieser Maßnahmenkataloge gilt für Branchen, die über solche Standards verfügen, automatisch als dem Stand der Technik entsprechend.

Zusätzlich konkrete Maßnahmen in Branchenstandards

Die Pflicht zum Einsatz eines Systems zur Angriffserkennung ist im Zuge des IT-SiG 2.0 nachträglich ins BSIG und ins EnWG aufgenommen worden (§ 8a Abs. 1a BSIG, § 11 Abs. 1f EnWG). Sie gilt ab dem 1.5.2023 für alle Betreiber kritischer Infrastrukturen, und ihre Umsetzung muss im Rahmen der alle zwei Jahre erfolgenden Prüfungen nach § 8a nachgewiesen werden.

Angriffserkennung als neue Pflicht

Alle Betreiber kritischer Infrastrukturen sind verpflichtet, eine Kontaktstelle zu benennen, über die sie jederzeit erreichbar sein müssen. Die Meldung von Sicherheitsvorfällen an das BSI ist nach § 8b Abs. 4 BSIG verpflichtend. Es wird unterschieden zwischen "gewöhnlichen" und "erheblichen" Störungen, die im ersteren Fall meldepflichtig sind, wenn sie einem Ausfall oder eine erhebliche Beeinträchtigung der kritischen Infrastruktur verursacht haben. Eine als "erheblich" geltende Störung muss dagegen noch gar keine Auswirkungen haben: Die Meldepflicht gilt schon dann, wenn auch nur die Möglichkeit besteht, dass die Funktionsfähigkeit einer erbrachten kritischen Dienstleistung bedroht ist. Hier unterscheidet sich das BSIG von der NIS-Richtlinie, die nur bereits erfolgte Ausfälle als meldepflichtige Störung betrachtet.

Registrierung und Meldepflicht

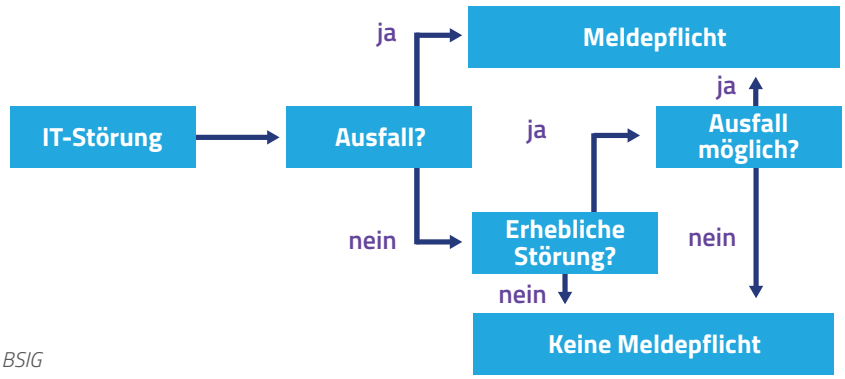


Abbildung: Meldung nach § 8b Abs. 4 BSIG

Ablauf einer Meldung bei Sicherheitsvorfällen

Eine Frist ist für die Meldung nach § 8b Abs. 4 nicht festgelegt, aber sie soll "unverzüglich" erfolgen, also sobald der meldepflichtige Betreiber der kritischen Infrastruktur ein ausreichend klares Bild von der Lage hat, um eine sinnvolle Meldung zu machen.

§ 8c: Besondere Anforderungen für Anbieter digitaler Dienste

Für "geschäftsmäßig angebotene Telemedien" war bereits 2015 durch das erste IT-SiG im Telemediengesetz (TMG alt bis 2021, § 13 Abs. 7) die Verpflichtung verankert worden, durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf Systeme möglich ist und sie gegen Datenschutzverletzungen und Störungen durch äußere Angriffe gesichert sind.

Pflichten der Anbieter digitaler Dienste

Mit der Umsetzung der NIS-Richtlinie von 2016 in nationales Recht wurde eine Änderung des BSIG erforderlich, die mit der Einfügung eines neuen § 8c besondere Anforderungen für "Digital Services Providers", also die Anbieter digitaler Dienste (ADD) festschreibt. Diese Erweiterung umfasst nach § 2 Abs. 11 BSIG ausschließlich Unternehmen, die

Sonderformen der Regulierung für Suchmaschinen, Clouds und Handelsplattformen

- Online-Suchmaschinen
- Cloud-Computing-Dienste
- Online-Marktplätze

betreiben. Die ADD unterliegen allerdings keiner ex-ante-Regulierung wie die KRITIS-Einrichtungen, müssen also keine regelmäßigen Berichte über den Status ihrer Sicherheitsmaßnahmen an das BSI liefern. Auch eine Registrierung ist nicht erforderlich. ADD sind aber verpflichtet, Sicherheitsvorfälle mit erheblichen Auswirkungen dem BSI zu melden – die Kriterien, wann dieser Fall eintritt, sind nach der Dauer von Ausfällen, der Anzahl der Betroffenen und dem für sie entstehenden individuellen Schaden in der NIS definiert.

Unternehmen in besonderem öffentlichen Interesse (UBI)

Nicht zu KRITIS im engeren Sinne zählen die in § 2 Abs. 14 BSIG definierten "Unternehmen in besonderem öffentlichen Interesse" (UBI), die den "wichtigen Einrichtungen" der NIS-2-Richtlinie entsprechen. Sie sind in drei Kategorien unterteilt:

"UBI": zusätzliche Branchen und besondere Unternehmen in der Regulierung

UBI-Kategorie	Betroffene Unternehmen
UBI 1 (AWV-UBI)	(Rüstungs-)Unternehmen nach § 60 Außenwirtschaftsverordnung (AWV), also Hersteller von Waffen, Munition und anderen Rüstungsgütern, aber auch IT-Sicherheitsprodukten "zur Verarbeitung staatlicher Verschlusssachen".
UBI 2 (Wertschöpfungs-UBI)	Die zu den größten in Deutschland zählenden Unternehmen und die für sie wesentlichen Zulieferer.
UBI 3 (Störfall-UBI)	Betreiber, die unter die Störfallverordnung (StöV) nach dem Bundes-Immissionsschutzgesetz fallen, bei denen gefährliche Stoffe in Mengen oberhalb eines dort festgelegten Schwellenwerts vorhanden sind.

Für die Registrierung als UBI, ihre Meldepflichten und das Verfahren der Selbsterklärungen zur IT-Sicherheit nach § 8f BSIG Abs. 1 gelten unterschiedliche Fristen je nach Kategorie: Unternehmen der Kategorie UBI 1 müssen sich ab 1.5.2023 beim BSI registrieren und danach alle zwei Jahre eine "Selbsterklärung" abgeben, in der nicht nur Kontaktdaten und Ansprechpartner abgefragt werden: Alle im Zeitraum der letzten zwei Jahre erworbenen Zertifizierungen und durchgeführten Audits sind anzugeben, und sie müssen erklären, wie sie

Anderer Umfang und Tiefe der Regulierung gegenüber KRITIS

einen angemessenen Schutz ihrer IT-Systeme und Komponenten und der besonders zu schützenden Prozesse sicherstellen. Für die Störfall-UBI der Kategorie UBI 3 besteht keine Registrierungspflicht, aber sie dürfen sich freiwillig beim BSI registrieren. Die Meldepflicht für Sicherheitsvorfälle resultiert bei ihnen aus der Störfall-Verordnung und gilt bereits seit 1.11.2021. Bei den Unternehmen der Kategorie UBI 2 gelten die Pflichten zur Registrierung und Selbsterklärung erst zwei Jahre nach Inkrafttreten der Rechtsverordnung, die ihre Zugehörigkeit zu den größten Unternehmen in Deutschland feststellt. Sie wird dem sogenannten Top-100-Panel der Monopolkommission vergleichbar erstellt, muss darüber hinaus die Kriterien für die Zuerkennung einer Wesentlichkeit bei den Zulieferern der größten Unternehmen festlegen und liegt derzeit noch nicht vor.

Mindeststandards für die Bundesverwaltung und andere öffentliche Stellen

Mindeststandards für öffentliche Einrichtungen

Die Festlegung, welche Maßnahmen für die Informationssicherheit von Stellen des Bundes, öffentlichen Körperschaften und Stiftungen oder öffentlicher Unternehmen als Betreiber kritischer Infrastrukturen anzuwenden sind, geschieht über Mindeststandards. Ihre Einhaltung wird im Rahmen der Prüfungen nach § 8a nachgewiesen. Mindeststandards sind vom BSI veröffentlichte Handreichungen für diejenigen Institutionen, denen das BSI nach § 8 Abs. 1 BSIG selbst Vorgaben erteilen kann, an denen sich aber auch betroffene Unternehmen oder andere Behörden orientieren können.

Nachweis- und Meldepflicht

Ergänzende oder abweichende Pflichten für Nachweise und Meldungen

Zur Vervollständigung der Nachweis- und Meldepflichten, die abweichend von der Systematik nach § 8a (Nachweis) und § 8b (Meldung) geregelt sind, dient diese Übersicht:

Sektor	Nachweispflicht	Meldepflicht
Energie	Zertifizierung nach IT-Sicherheitskatalog gemäß § 11 Absatz 1b EnWG und regelmäßige Überprüfungen durch die BNetzA (Anlagen nach § 7 AtG sind anders geregelt)	Meldung von Sicherheitsvorfällen an das BSI, das "unverzüglich" an die BNetzA (bzw. bei kerntechnischen Anlagen an eine Meldekette für Reaktorsicherheit) weitermelden muss.
Telekommunikation	Sicherheitskonzept gemäß § 166 TKG und regelmäßige Überprüfungen durch die BNetzA	Sicherheitsvorfälle mussten früher nur der BNetzA, seit NIS-Umsetzung aber sowohl dem BSI als auch der BNetzA gemeldet werden.
Sektor	Nachweispflicht	Meldepflicht
Gesundheit	Sicherheitsgutachten über Komponenten und Dienste wird von den Betreibern der Telematik-Infrastruktur dem BSI zur Prüfung vorgelegt.	Betreiber melden Sicherheitsvorfälle an die gematik, die ihrerseits an das BSI weitermeldet.
Finanz	Jahresabschlussprüfung dient gleichzeitig als Nachweis nach § 8a Abs. 3	Meldung an die BaFin (Meldekette europäische Aufsicht) und an das BSI
ADD	Keine, aber ex-post-Aufsicht durch das BSI	Meldung von Sicherheitsvorfällen an das BSI

KritisV zur Umsetzung der Methodik und Festlegungen zur Identifizierung

Dreistufige Methodik zur Bestimmung kritischer Infrastrukturen in der KRITIS-Verordnung

Zur Bestimmung der Kritikalität einer Infrastruktur wird im § 10 Abs. 1 BSIG eine Methodik vorgegeben, die auf drei Verfahrensschritten begründet ist. Die Anwendung dieser Methodik ist Gegenstand der KritisV, die 2015 erstmals und 2021 in einer stark erweiterten Fassung in Kraft getreten ist. Bei der Erstellung der Festlegungen hat das BSI eine "umfassende Beteiligung" der Ressorts des Bundes und Vertretern der betroffenen Branchen über den normalen Rahmen von öffentlichen und Verbändeanhörungen hinaus praktiziert, um einen der Komplexität der Bestimmungen angemessenen "kooperativen Ansatz" zu verfolgen. Die KritisV konkretisiert die Vorgaben des BSIG, indem sie die Schwellenwerte und die Anlagen für die einzelnen KRITIS-Sektoren definiert, auf deren Basis Anlagenbetreiber als kritische Infrastruktur im Sinne der Rechtsdefinition identifiziert werden können. Mit der Änderung der KritisV von 2021 sind sowohl Schwellenwerte abgesenkt als auch Anlagenkategorien hinzugefügt worden, was den Kreis der identifizierten Betreiber kritischer Infrastrukturen erweitert hat.

IT-Sicherheitsgesetz (IT-SiG 2.0)

IT-Sicherheitsgesetz und NIS-Richtlinie als erste konkrete gesetzliche Grundlagen

Das 2015 in Kraft getretene erste IT-SiG war ein Artikelgesetz, mit dem erstmals für den deutschen Rechtsraum die Kernziele der Informationssicherheit und des Schutzes von IT-Systemen und Diensten auf eine konkrete gesetzliche Grundlage gestellt wurden. Der Zeitpunkt der Gesetzgebung ist insofern bemerkenswert, als die Bundesregierung damals nicht abgewartet hat, bis die erste NIS-Richtlinie der Europäischen Union verabschiedet wurde, sondern die im Entwurf zur NIS enthaltenen verbindlichen Maßnahmen im Vorgriff umgesetzt. Lücken zur abschließenden Inkraftsetzung der NIS wurden 2017 geschlossen. Insbesondere die neue Kategorie der ADD gehörte zu den Änderungen, die im Umsetzungsgesetz zur NIS berücksichtigt wurden.

IT-SiG 2.0: Mehr Pflichten für mehr Unternehmen, verschärfte Anforderungen, mehr Aufsichtsbefugnisse

Durch das "Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-SiG 2.0), das seit Mai 2021 in Kraft ist, wurde die bisherige Regulierung der KRITIS-Betreiber auf noch einmal deutlich breitere Grundlage gestellt. Das Artikelgesetz enthält Änderungen im BSIG, EnWG, TKG, der AWV und dem SGB X, die zusammenfassend einem größeren Kreis betroffener Unternehmen mehr Pflichten auferlegen, gleichzeitig die Anforderungen an ihre Informationssicherheit deutlich erhöhen und den Aufsichtsbehörden mehr Befugnisse einräumen. Im Vorgriff auf Änderungen in den europäischen Richtlinien NIS 2 und CER sind Maßnahmen nun Vorschrift, die ab Mai 2023 verbindlich eingefordert werden können: Systeme zur Angriffserkennung und ihre Auswertung, Organisation und Steuerung für Sicherheitsvorfälle, regelmäßige Penetrationstests und Schwachstellenmanagement.

Sektorenerweiterung und neue UBI-Kategorien

Neben der bereits im Abschnitt zum BSIG erläuterten, neu eingeführten Kategorie in § 2 Abs. 14 S. 1 Nr. 2 BSIG, den UBI, ist im IT-SiG 2.0 vor allem die Erweiterung der KRITIS-Sektoren um die Siedlungsabfallentsorgung hinzugefügt worden. Während die gesetzlichen Änderungen vollzogen sind, warten die betroffenen Branchen noch auf die konkreten Vorgaben, die im Rahmen einer geplanten KritisV-Novelle und weiteren Rechtsverordnungen getroffen werden sollen.

Weitere Gesetze

TKG

Telekommunikationsnetze und -dienste unterliegen eigener gesetzlicher Festlegung außerhalb des BSIG

Für die Betreiber öffentlicher Telekommunikationsnetze oder -dienste gelten die besonderen Sicherheitsanforderungen und die Nachweispflichten nach § 8a Abs. 1 BSIG ausnahmsweise nicht, auch wenn sie als kritische Infrastrukturen eingestuft sind. Telekommunikationsnetz- und -dienstbetreiber unterliegen dem TKG, soweit Anlagen dem Betrieb von Telekommunikationsnetzen oder der Erbringung von Telekommunikationsdiensten dienen. Aber nicht jede KRITIS-Anlage, die sie betreiben, fällt unter diese Ausnahmeregelung: Hosting-Dienste, die ein Telekommunikationsunternehmen ebenfalls anbietet, wären weiterhin nach § 8a Abs. 1 BSIG zu behandeln.

Die Vorschriften des TKG zur Einhaltung der Anforderungen an die Informationssicherheit sind oftmals schärfer und vor allem eindeutiger festgelegt. Wir beschreiben weiter unten die Sicherheitsanforderungen im Detail, hier deshalb nur kursorisch zu erwähnen: Im TKG sind explizite Vorschriften zum Informationssicherheitsmanagement und technische Vorgaben bis hin zur Zertifizierung kritischer Komponenten enthalten.

Schärfere und eindeutig festgelegte Vorgaben

EnWG

§ 11 Abs. 1a EnWG verlangt "angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind." Dazu wird von der Bundesnetzagentur im Benehmen mit dem BSI ein Katalog von Sicherheitsanforderungen erstellt. Der Unterschied zu den Anforderungen an andere KRITIS-Sektoren, die gemäß § 8a Abs. 1 S. 2 BSIG zur Einhaltung des "Stands der Technik" verpflichtet sind, sind die konkreten Maßnahmen, die der Katalog vorschreibt: Werden sie umgesetzt und nachgewiesen, gilt der Schutz als angemessen.

Energieversorger mit konkretem Sicherheitskatalog

SGB V

Für den Sektor Gesundheit ist das Fünfte Buch des Sozialgesetzbuchs (SGB V) maßgeblich. Seit 1.1.2022 sind nach § 75c SGB V alle Krankenhäuser - nicht nur diejenigen, die zur kritischen Infrastruktur zählen - dazu verpflichtet, "nach dem Stand der Technik angemessene Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind." Weil der Stand der Technik sich laufend ändert, legt das Gesetz auch fest, dass die eingesetzten Systeme "spätestens alle zwei Jahre" anzupassen sind. Die Krankenhäuser sollen sich dabei an den branchenspezifischen Sicherheitsstandards (B3S) orientieren, die vom BSI freigegeben werden. Für das Gesundheitswesen gibt es zwei solcher B3S, neben dem für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus einen weiteren für die Arzneimittelhersteller.

Branchenspezifische Sicherheitsstandards für Krankenhäuser

Für den Bereich der kritischen Infrastruktur für Netzwerkdienstleistungen im Gesundheitssektor regelt § 291b des SGB V die Melde- und Nachweispflichten der sogenannten Telematik-Infrastruktur, die durch die Gesellschaft für Telematik (gematik) betrieben wird.

Abweichende gesetzliche Grundlage für Gesundheits-Telematik

Europäischer Rechtsrahmen

NIS 2

Mit der Richtlinie zur Netz- und Informationssicherheit (NIS) hatte die Europäische Union erstmals 2016 die Sicherheitspflichten für Betreiber kritischer Infrastrukturen europaweit festgelegt. Vor allem das Verfahren zur Identifizierung von kritischer Infrastruktur in Deutschland, das im Rahmen der KritisV und seinen konkreten Schwellenwerten für die Kritikalität der Dienste etabliert wurde, wurde von der Systematik der NIS geprägt.

Systematisch ähnlich der Rechtsgrundlage in Deutschland

Grob vereinfacht betrachtet gibt es eine Entsprechung der "essential entities" (wesentliche Einrichtungen) der NIS 2 und den deutschen KRITIS-Einstufungen, während die "important entities" (wichtige Einrichtungen) mit den deutschen UBI korrelieren. ADD gehen zukünftig wie UBI mindestens in den Betreibern wichtiger Dienste auf, sie werden nicht mehr getrennt betrachtet.

Neuer Maßstab: wesentliche und wichtige Einrichtungen

In der Vorbereitung der Umsetzung in deutsches Recht, die bis spätestens 17. Oktober 2024 erfolgen muss, fällt ein wesentlicher Unterschied zur KritisV sofort auf: Nach der neu eingeführten "Size-Cap-Rule" werden künftig alle Betreiber ab der Größe eines mittleren Unternehmens eingestuft, gemessen allein an der Zahl der Beschäftigten (mehr als 50) und Umsatz (größer als 10 Mio. Euro Jahresumsatz/-bilanzsumme) und damit

Unternehmensgröße entscheidendes Kriterium

nicht mehr anhand von Schwellenwerten, wie sie in der KRITIS-Verordnung angelegt sind. Das Statistische Bundesamt schätzt, dass die Anzahl der "essential entities" gegenüber den nach der bisherigen NIS-Richtlinie erfassten Einrichtungen etwa versechsfacht wird.

Bisherige KRITIS-Einstufungen sollen fortgeführt werden

Obwohl es nach dem Buchstaben der NIS 2 nicht mehr vorgegeben ist, einen Identifizierungsprozess wie nach NIS 1 und BSIG bzw. KritisV durchzuführen, will Deutschland nach jetzigem Stand für besonders schützenswerte Unternehmen an der bisherigen risikobasierten Einstufung der Betreiber kritischer Infrastruktur festhalten. Bleibt es dabei, ändern sich die Kategorien der Einrichtungen nach dem BSIG:

Kategorie	Charakterisierung
KRITIS	Betreiber kritischer Infrastrukturen, identifiziert nach der bisherigen Methodik der KritisV.
Bundesverwaltung	Stellen und öffentliche Einrichtungen des Bundes
Wesentliche Einrichtungen	Deckungsgleich mit den KRITIS-Sektoren nach deutscher Lesart, einige davon in verschiedene Teilsektoren aufgeteilt, plus einige zusätzliche wie Bodeninfrastruktur für weltraumgestützte Dienste. Identifiziert werden sie ausschließlich nach Unternehmensgröße.
Wichtige Einrichtungen	Post- und Kurierdienste, Produktion diverser Güter, die teilweise auch in der KritisV bereits berücksichtigt sind. UBI und ADD gehen in dieser Kategorie auf.

Empfindlich verschärfter Bußgeldkatalog

In Anlehnung an die Datenschutzgrundverordnung (DSGVO) wird der Bußgeldrahmen für Informationssicherheit nicht mehr nur in absoluten Beträgen festgelegt, sondern abhängig vom Umsatz des Unternehmens, das den Regeln zuwiderhandelt. Anders als im Datenschutz wird für Bußgelder für Verstöße gegen die Anforderungen der NIS 2 aber eine Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen gemacht: Erstere werden mit höchstens zehn Millionen oder zwei Prozent des weltweiten Jahresumsatzes sanktioniert, letztere mit sieben Millionen respektive 1,4 Prozent. Das ist mit den Höchstbeträgen nach IT-SiG 2.0 zwar vergleichbar (bisher können schon Bußgelder bis 20 Millionen Euro verhängt werden, wenn Unternehmen sich der Umsetzung einer vom BSI angeordneten Abstellung eines Sicherheitsmangels verweigern), aber für große Unternehmen kann die umsatzbezogene Festlegung von Bußgeldern erheblich höhere Summen als bisher erreichen. Die in der Richtlinie erstmals verfügte Geschäftsleiterverantwortlichkeit bedingt außerdem, dass diese für Versäumnisse bei gesetzlich vorgeschriebenen Sicherheitsmaßnahmen persönlich haftbar gemacht werden können. Das Sanktionsregime für Verstöße gegen die Regeln der Informationssicherheit schlägt damit eine Richtung ein, die in europäischen Unternehmen eine ähnlich dynamische Umsetzung der Regulierungsanforderungen verspricht, wie es 2018 bei der Anwendung der DSGVO der Fall war.

Persönliche Haftung von Geschäftsleitern

Aufsicht und Durchsetzung

Neues Meldeverfahren

Neu gegenüber der NIS 1 ist ein nunmehr dreistufiges Meldeverfahren: Eine Frühwarnung über einen Vorfall soll binnen 24 Stunden an die zuständigen Aufsichtsbehörden gemeldet werden, die umfassende Sicherheitsmeldung soll - innerhalb einer analog zu Datenschutzvorfällen nach der DSGVO gewählten Frist - vor Ablauf von 72 Stunden abgegeben werden, und der Bericht zu Vorfall und Behebung spätestens einen Monat nach dieser Meldung.

Auch nach der Neustrukturierung des Anwendungsbereichs werden die Anforderungen an "wichtige Einrichtungen" weniger streng als für tatsächliche KRITIS-Betreiber oder die "wesentlichen Einrichtungen" sein. Wesentliche Einrichtungen werden von der zuständigen Behörde (in Deutschland in der Regel das BSI) nach der NIS 2 laufend geprüft (durch Anforderung von Informationen, Vor-Ort-Kontrollen, regelmäßige oder anlassbezogene Überprüfungen), bei wichtigen Einrichtungen findet dies nur aufgrund eines begründeten Verdachts statt.

Abgestufte Anforderungen und Prüfverfahren

Der Katalog der Mindestsicherheitsanforderungen nach Art. 21 Abs. 1 der NIS 2 wird künftig ins BSIG übernommen, aber nach Kategorien differenziert. NIS 2 hat unter anderem die Sicherheitsanforderungen des europäischen Kodex für die elektronische Kommunikation (EECC-Richtlinie) übernommen, deren eigene Umsetzung in nationales Recht bereits 2020 erfolgen sollte, aber verspätet ist. Auch die eIDAS-Verordnung wurde in die NIS 2 überführt. EECC und eIDAS werden in diesem Papier deshalb nicht separat referenziert, aber dort erwähnt, wo sie als Einflussfaktoren weiterhin von Bedeutung sind.

Harmonisierung mit bisherigen EU-Richtlinien

Richtlinie zur Resilienz kritischer Infrastrukturen: Critical Entities Resilience (CER) Directive

Die Vorgängerrichtlinie "European Critical Infrastructures" (ECI) war bei Inkrafttreten 2008 die allererste europaweit verbindliche Regulierung im Feld der kritischen Infrastrukturen, die bis dahin ausschließlich nationalen Regeln unterworfen oder gar nicht reguliert waren. Zwei interessante Änderungen gegenüber der ECI sind in der CER festzustellen: Es ist nicht mehr die Rede von "kritischer Infrastruktur", sondern "critical entities", also "kritischen Einrichtungen", und es geht nicht mehr um ihren Schutz ("protection"), sondern die Ausfallsicherheit ("resilience"). Dahinter steht mehr als nur eine veränderte Wortwahl: Die Aufrechterhaltung des Betriebs (im Sinne eines "Business Continuity Management", dem nach ISO 22301 standardisierten BCM) verfolgt eine andere Zielsetzung als der traditionelle Ansatz, Störfälle zu vermeiden. Der Fokus bewegt sich also weg von einer Störfallverordnung, die sich mit den Folgen von Ausfällen auseinandersetzen muss, zu einer systematischen Betrachtung regulärer Geschäftsprozesse und wie sie auch unter Bedrohungsszenarien kontinuierlich weitergeführt werden können.

Ausfallsicherheit als Kriterium für kritische Infrastrukturen

Fortführung von Geschäftsprozessen statt Störfallbetrachtung

Alle nach den Kriterien der CER identifizierten Betreiber kritischer Infrastruktur fallen automatisch auch unter die "wesentlichen Einrichtungen" der NIS 2. In Deutschland soll diese Identifizierung sowohl für den physischen wie den digitalen Schutz kritischer Infrastrukturen im KRITIS-Dachgesetz zusammenfallen, das sich in Vorbereitung befindet.

Nach CER klassifizierte Einrichtungen automatisch höchste KRITIS-Stufe

Die Umsetzung der Richtlinie in nationales Recht erfolgt in Deutschland im Rahmen des geplanten KritisDG.

DORA

In Ergänzung der NIS 2 wurde parallel eine Verordnung zur Stärkung der Informationssicherheit bei Finanzdienstleistungen verabschiedet, die "Verordnung über die digitale operationale Resilienz im Finanzsektor", englisch kurz: Digital Operational Resilience Act (DORA). Sie trat am 16.1.2023 in Kraft und wird nach einer zweijährigen Übergangsfrist ab 17.1.2025 angewendet. Bis dahin erstellen die europäischen Aufsichtsbehörden Leitlinien und technische Regulierungs- und Durchführungsstandards (Regulatory Technical Standards, RTS, und Implementing Technical Standards, ITS). Die in der DORA spezifizierten Anforderungen gelten für die gesamte Finanzbranche, von Versicherungen über Kredit- und Zahlungsinstitute bis zu Ratingagenturen, Kryptowährungsplattformen oder Spezialdiensten wie Transaktionsregistern. In der Frage, welche dieser Pflichten abhängig von der Unternehmensgröße relevant sein werden, setzt DORA tiefer an als NIS 2, denn auch für kleine Unternehmen (2 bis 10 Millionen Euro Jahresumsatz/Bilanzsumme, 10-50 Mitarbeiter) gelten dieselben Regeln wie für mittlere, nur für Kleinstunternehmen unterhalb dieser Grenzen nicht.

Spezialverordnung für die Finanzbranche

Geltungsbereich umfasst auch kleinere Unternehmen

DORA-Anforderungen gelten auch für alle Drittdienstleister der digitalen Infrastruktur, die für diese Finanzunternehmen tätig sind: Rechenzentren, IT- und Telekommunikationsinfrastruktur, Cloudbetreiber und weitere Anbieter von Informations- und Kommunikationstechnik für die Branche. Den Finanzunternehmen wird durch die Verordnung auferlegt, diese Dritten in ihr Risikomanagement zu integrieren und dafür zu sorgen, dass vertragliche Vereinbarungen mit ihnen auf der Grundlage einer "Strategie für das IKT-Drittparteienrisiko" die entsprechenden Anforderungen an Informationssicherheit erfüllen. Dazu gehören in jedem Fall aber auch Zugangs-, Inspektions- und Auditrechte bei den Dritten.

Drittdienstleister explizit mitgeregelt

Definiert sind die "IKT-Drittdienstleister" als "digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden" (Art. 3 S. 1 Nr. 21): Die Anbieter der Föderationsdienste innerhalb GXFS gehören damit zum Kreis der Verpflichteten nach dieser Verordnung, wenn sie Dienste für Finanzunternehmen erbringen. Die weitreichenden Überwachungs- und Integrationspflichten der Drittanbieter nach DORA sollen bis zur Anwendung 2025 noch weiter spezifiziert werden.

GXFS damit im Geltungsbereich, wenn sie durch Finanzbranche genutzt werden

Cyber Resilience Act (CRA)

Der Cyber Resilience Act führt für "Produkte mit digitalen Bestandteilen" - IT-Produkte - Regeln ein, die einzuhalten sind, um die Sicherheit von Hard- und Software zu gewährleisten. Er richtet sich an Hersteller von Geräten und Anwendungen, die nur solche Produkte produzieren und in Verkehr bringen dürfen, deren Umsetzung der Anforderungen des CRA nachweisbar ist. Zur Bestätigung dieser Konformität werden sie mit einer CE-Kennzeichnung des Europäischen Komitees für elektrotechnische Normung (CENELEC) versehen.

Zulassungsregeln für IT-Produkte

Für die Bewertung von IT-Produkten werden drei Sicherheitskategorien eingeführt (Standard, kritische Klasse I und II), die nach Kriterien wie Funktionalität, beabsichtigte Verwendung und möglichen Auswirkungen von Sicherheitsproblemen zugeordnet sind:

Sicherheitskategorien abhängig vom Verwendungszweck

Sicherheitskategorie	Produktbeispiele
Standard	Text- und Bildverarbeitungssoftware, intelligente Lautsprecher, Festplatten, Spiele
Kritische Klasse I	Browser, Identitäts- und Passwortmanager, Virenschutzprogramme, Netzschnittstellen, Firewalls und Intrusion Detection, Mikrocontroller wie CNC-Steuerungen, SCADA etc.
Kritische Klasse II	Betriebssysteme für Server, Desktops und mobile Geräte; Virtualisierung; CPUs; Public Key Infrastructure, dazu einige Produkte aus der kritischen Klasse I, aber zur industriellen Anwendung (Router/Switches, Firewall/Intrusion Detection, Mikrocontroller.

Bewertung der Konformität in der Regel durch die Hersteller

Wie sie die Sicherheit ihrer Produkte nachweisen, bleibt bis auf Ausnahmen den Herstellern überlassen. Konformitätsbewertungsverfahren, die im CRA je nach Sicherheitskategorien verlangt werden, reichen von der Selbstbewertung durch die Hersteller bis zur Prüfung durch Dritte. Eine verpflichtende Konformitätsbewertung durch unabhängige Dritte gibt es im CRA nur für die oberste kritische Klasse II.

Die formelle Abstimmung im Trilog zwischen Europäischer Kommission, Rat und Parlament und die Finalisierung des Gesetzgebungsverfahren für den CRA wird im Laufe des Jahres 2023 erwartet.

In Vorbereitung: KRITIS-Dachgesetz (KritisDG)

Physischer Schutz bislang kaum oder nur in Einzelregelunge etabliert

Zum physischen Schutz kritischer Infrastrukturen gibt es eine Vielzahl von Einzelbestimmungen in Fachgesetzen, in denen Vorgaben für Betreiber oder Befugnisse der Behörden bereits geregelt sind. Diese bisherigen Einzelregelungen, ergänzt durch mittelbar wirksame Vorschriften zur Verwendung und Einhaltung von Normen und Standards (z. B. in der Bautechnik), nehmen explizit auf kritische Infrastruktur Bezug. Weil hier aber Verflechtungen und gegenseitige Abhängigkeiten unterschiedlicher Sektoren in den Einzelregelungen nicht ausreichend berücksichtigt werden, soll der Bereich des physischen Schutzes nun eine Konsolidierung und Erweiterung in einem ressort- und sektorenübergreifenden Gesetz erfahren. Konkret soll analog zur europäischen Initiative der Critical Entities Resilience Directive eine Klammer über alle Anforderungen gezogen werden, die nicht unmittelbar mit Cybersicherheit zu tun haben, für die Versorgungssicherheit der kritischen Infrastrukturen insgesamt aber unabdingbar sind.

Neues Gesetz soll Lücke zwischen Cyber- und physischer Sicherheit schließen

Schutzstandards und Meldesystem

Mit dem KritisDG, das die Maßgaben der CER bereits integrieren soll, wird es erstmals verpflichtende Schutzstandards für die physische Sicherheit geben. Neu wird auch ein dafür einzuführendes Meldewesen sein, das in Bezug auf physische Sicherheitsvorfälle so noch nicht existiert. Viele der vorgesehenen Maßnahmen sind aber für die Betreiber keine neuen Anforderungen, weil sie unter Informationssicherheitsaspekten beispielsweise bereits seit langem darin geübt sind, ein eigenes Risikomanagement zu betreiben und Risikoanalysen und -bewertungen vorzunehmen. Wie die Anforderungen an technische und organisatorische Maßnahmen für die Einrichtungen in Bezug auf ihren physischen Schutz aussehen wird, ist noch nicht absehbar, aber auch hier wird eher präzisiert werden als vollkommen neue Standards zu setzen. Im Eckpunktepapier zum KRITIS-Dachgesetzentwurf werden zum Beispiel "die Errichtung von Zäunen und Sperren, der Einsatz von Detektionsgeräten, Zugangskontrollen, Sicherheitsüberprüfungen, aber auch das Vorhalten von Redundanzen und die Diversifizierung von Lieferketten" als geeignete Maßnahmen genannt. Welche Regelungstiefe und Mindeststandards hier einzuhalten sind, überwacht künftig das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das zu diesem Zweck erheblich ausgebaut wird und - auch das ist neu - als zentrale Meldestelle für Vorkommnisse mit Bezug zur physischen Sicherheit kritischer Infrastrukturen fungieren wird.

Aufsichtsbehörde wird das BBK

Der Referentenentwurf für das KritisDG und die Einbringung in des Gesetzgebungsverfahren wird im Laufe des Jahres 2023 erwartet.

Kriterien und Anforderungen an kritische Infrastrukturen

Begriffsdefinition

KRITIS sind Anlagen zur Erbringung kritischer Dienstleistungen

Die KritisV konkretisiert die Definition kritischer Infrastruktur im Hinblick auf die zu berücksichtigenden Komponenten: Unter "Anlagen" wird in der Verordnung alles verstanden, was Betriebsstätten, Maschinen, Geräte oder Software und Dienste sind, die "für die Erbringung einer kritischen Dienstleistung notwendig sind". "Kritische Dienstleistungen" sind alle Dienste, die zur Versorgung der Allgemeinheit notwendig sind, "deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde". Wichtig ist der Anlagenbegriff, weil nicht jeder Betreiber einer Regulierung unterfällt, sondern nur diejenigen, die für die Erbringung ihrer kritischen Dienstleistungen eine Anlage betreiben, die in der KritisV alle explizit genannt und mit Schwellenwerten versehen sind.

Kritisch oder systemrelevant?

Zur Abgrenzung vom Begriff der Systemrelevanz ist anzumerken, dass jeder Bestandteil des Gesamtsystems zur Sicherstellung der Versorgung der Bevölkerung mit lebenswichtigen Gütern und Dienstleistungen ein systemrelevanter Beitrag ist. Er kann als kritische Infrastruktur eingestuft sein, muss es aber nicht. Das BBK bringt es auf die Formel: "Demnach sind zwar alle kritischen Infrastrukturen gleichzeitig auch systemrelevant, aber nicht alle systemrelevanten Einrichtungen sind auch kritisch."

Methodik zur Identifizierung (nach § 10 Abs. 1 S. 1 BSIG)

Systematische Identifizierung

Die Identifizierung als Betreiber kritischer Infrastrukturen fußt immer noch bis zu einem gewissen Grad auf einer Selbsteinschätzung der Betreiber. Die KritisV überführt mit ihrer Präzisierung der Rahmenbedingungen und der konkreten Maßstäbe für die Einstufung dieses selbstregulierende Element in eine systematische Bewertung und Benennung kritischer Infrastrukturen.

1. Schritt: Sektorspezifische Kriterien

2. Schritt: Anlagenkategorien

3. Schritt: Versorgungsgrad

Die KritisV verfährt nach der Maßgabe des § 10 Abs. 1 S. 1 BSIG bei der Identifizierung der Betreiber kritischer Infrastrukturen nach einer dreistufigen Methodik. Ob ein Unternehmen sich der KRITIS-Regulierung zu unterwerfen hat, wird zunächst nach einem Kriterienkatalog bestimmt, der für die acht Sektoren jeweils festlegt, welche ihrer Dienste aufgrund ihrer Bedeutung als kritische Dienstleistungen einzustufen sind. Diese Feststellung ist die Voraussetzung, um im zweiten Schritt die betriebenen Anlagen zur Erbringung dieser Dienste wiederum sektorenspezifischen Anlagenkategorien zuzuordnen - sind die Anlagen nicht in den Kategorien im Anhang der KritisV enthalten, sind die Dienste nicht als kritische Infrastruktur einzustufen. Im letzten Schritt wird, sofern es sich um den Betrieb einer Anlage der kritischen Infrastruktur handelt, der Versorgungsgrad betrachtet: Der Regulierung unterworfen sind am Ende des Prozesses der Identifizierung nach dieser Methodik nur diejenigen Unternehmen, deren Anlagenbetrieb die in den Anhängen der KritisV definierten Schwellenwerte überschreitet.

Festlegung kritischer Dienstleistungen nach Bedeutung

Kritische Dienstleistungen

In den Paragraphen 2 bis 8 der KritisV wird für jeden Sektor eine Liste der wegen ihrer Bedeutung für die Daseinsvorsorge als kritisch anzusehenden Dienstleistungen aufgestellt.

Sektor	Kritische Dienstleistungen
Energie	Strom- und Gas-, Kraftstoff- und Heizöl- sowie Fernwärmeversorgung
Wasser	Trinkwasserversorgung und Abwasserbeseitigung
Ernährung	Lebensmittelversorgung inklusive -produktion, -verarbeitung und -handel
Informationstechnik und Telekommunikation	Sprach- und Datenübertragung sowie Datenspeicherung und -verarbeitung inklusive Housing, Hosting und Vertrauensdienste
Gesundheit	Stationäre medizinische Versorgung, Versorgung mit "unmittelbar lebenserhaltenden Medizinprodukten" und verschreibungspflichtigen Arzneimitteln, Blut- und Plasmakonzentraten, sowie Laboratoriumsdiagnostik
Finanz- und Versicherungswesen	Bargeldversorgung, Zahlungsverkehr (kartengestützt und konventionell), Verrechnung von Geschäften mit Wertpapieren und Derivaten, Versicherungsdienstleistungen (nur Erstversicherungen, keine Rückversicherer)
Transport und Verkehr	Personen- und Güterverkehr mit allen Verkehrsträgern (Luft, Schiene, Straße, Binnen- und Seeschifffahrt), aber ohne motorisierten Individualverkehr

Bestimmung von Anlagenkategorien zur Erbringung dieser Dienstleistungen

Anlagenkategorien mit Mindestgrößen

Für jeden der genannten Sektoren wird in der KritisV ein eigener Anhang angefügt, in dem die zur Erbringung der kritischen Dienstleistungen betriebenen Anlagenkategorien definiert werden. In bestimmten Kategorien ist bereits eine Aufgreifschwelle enthalten, die mindestens erreicht sein muss, um als "Anlage" im Sinne der Verordnung zu gelten. Für Rechenzentren heißt das zum Beispiel, dass mindestens ein geschlossener Raum mit mindestens zehn Racks vorhanden ist. Gibt es einen engen räumlichen oder betrieblichen Zusammenhang, können mehrere Anlagen als eine gemeinsame gewertet und die Gesamtanlage als kritische Infrastruktur eingestuft werden, wenn die einzelnen Anlagen in der Summe ihrer Leistungen einen kritischen Versorgungsgrad erreichen.

Sektorenspezifische Kriterien, Anlagenkategorien und Schwellenwerte

Kenngrößen für kritischen Versorgungsgrad als Kalkulationsgrundlage

Aus den Kategorien werden nach der Methodik der KritisV einzelne, als kritisch einzuschätzende Anlagen nach Versorgungsgrad und Bedeutsamkeit für die Allgemeinheit abgeleitet. Um aus den Anlagenkategorien aller Sektoren zu bestimmen, welche davon als kritisch einzuschätzen sind, werden Kenngrößen verwendet, mit denen über spezifische Berechnungsformeln je Sektor Schwellenwerte ermittelt werden. Überwiegend ist die Grundlage für die Kalkulation dabei die Annahme, dass ein kritischer Versorgungsgrad von Bedeutsamkeit für die Allgemeinheit dann erreicht ist, wenn die Versorgungssicherheit von 500.000 Menschen daran hängt. Für die einzelnen Anlagenkategorien muss das in Leistungskennzahlen umgerechnet werden, die für jeden Sektor genau definiert sind. Beispielhaft hier der Sektor Informationstechnik und Telekommunikation:

Anlagenkategorie	Schwellenwert (Leistung)
Zugangsnetz	100.000 Teilnehmeranschlüsse
Übertragungsnetz	100.000 Vertragspartner des jeweiligen Dienstes
Internet-Exchange-Knoten	100 angeschlossene Autonomous Systems (AS) im Jahresdurchschnitt
DNS-Resolver	100.000 Vertragspartner im Zugangsnetz, in dem er betrieben wird
Autoritative DNS-Server	250.000 Domains, für die er autoritativ ist oder die aus der Zone delegiert werden
Top-Level-Domain-Registry	250.000 verwaltete/betriebene Domains
Housing (Rechenzentrum)	3,5 MW
Hosting (Serverfarm)	10.000 physische oder 15.000 virtuelle Instanzen
Content Delivery Network	75 PB ausgeliefertes Datenvolumen pro Jahr
Vertrauensdienste	500.000 qualifizierte oder 10.000 Serverzertifikate

Anzuwendende Sicherheitsstandards und Regulierung

UP Bund 2017 und Mindeststandards des BSI

Mindeststandards Bund

Mit der "Leitlinie für die Informationssicherheit in der Bundesverwaltung", dem Umsetzungsplan Bund 2017, sind Mindestanforderungen für alle Ressorts und Bundesbehörden festgelegt worden, deren Einhaltung bereits verbindlich gemacht wurde. Die gesetzliche Grundlage folgte im IT-SiG 2.0, in dem der § 8 Abs. 1 S. 1 BSIG in einer Neufassung nun alle

- Stellen des Bundes,
- die Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihrer Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie
- öffentliche Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen

Beispiel: Cloud-Computing-Nutzung durch Bundesverwaltung

zur Umsetzung von sogenannten "Mindeststandards" verpflichtet, die das BSI als zuständige Behörde verfasst und veröffentlicht. Einer dieser Mindeststandards regelt die Sicherheitsanforderungen an die Nutzung von Cloud-Diensten durch die Institutionen des Bundes. Zu den Voraussetzungen, die der Cloud-Anbieter erfüllen muss, gehört die Vorlage eines Prüfberichts nach dem "Cloud Computing Compliance Criteria Catalogue" (C5) - keine obligatorische Zertifizierung wie nach dem IT-Grundschutz-Kompendium des BSI, aber immerhin ein Testat durch einen unabhängigen Wirtschaftsprüfer, das vorhanden sein muss. Ohne C5-Testat darf die Behörde den Anbieter bei der Beschaffung von Cloud-Dienstleistungen nicht berücksichtigen.

Kenngrößen für kritischen Versorgungsgrad als Kalkulationsgrundlage

Nach Art. 3 S. 1 (d) der NIS 2 werden Einrichtungen der "öffentlichen Verwaltung der Zentralregierung" oder - risikobasiert an der Bedeutung einer Störung für die Versorgungssicherheit gemessen - auch regionale Verwaltungseinrichtungen pauschal zu kritischen Infrastrukturen (bzw. wesentlichen Einrichtungen) erklärt. Damit gelten für sie auch die Anforderungen an die Informationssicherheit, die in der Richtlinie spezifiziert sind.

Sicherheitsanforderungen nach TKG

Eigener Sicherheitskatalog für die Betreiber von Telekommunikationsnetzen

Während in anderen Sektoren die gesetzliche Festlegung noch aussteht, hat das TKG für die Betreiber von Telekommunikationsnetzen bereits deutlich ausformulierte, spezifisch zum Beispiel auf die Zertifizierung von kritischen Komponenten ausgerichtete Bestimmungen. Der "Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG)" wird von der BNetzA im Benehmen mit dem BSI und dem BfDI erstellt und ist die Grundlage für das Sicherheitskonzept, das von jedem Telekommunikationsbetreiber erstellt werden muss. NB: Der Titel des Katalogs ist irreführend, weil seit der Änderung des TKG im IT-SiG 2.0 2021 die Verweise nicht mehr stimmen: Die im Sicherheitskatalog referenzierten Paragraphen des TKG beziehen sich noch auf die alte Version, weil er in seiner aktuell gültigen Fassung ein Jahr vor der TKG-Novelle verabschiedet wurde.

Das Sicherheitskonzept nach TKG

Der Nachweis über die Erfüllung der Anforderungen erfolgt mindestens alle zwei Jahre durch eine Überprüfung des Sicherheitskonzepts, die von der BNetzA selbst vorgenommen wird. Im Sicherheitskonzept ist nach § 166 TKG zu dokumentieren, "welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der (...) konkretisierten Verpflichtungen (...) getroffen oder geplant sind". Wo der Katalog von Sicherheitsanforderungen nur Ziele festlegt, muss das Sicherheitskonzept nachweisen, dass seine Maßnahmen diese Ziele auch erreicht.

Die erforderliche Zertifizierung von kritischen Komponenten vor ihrem erstmaligen Einsatz in kritischen Telekommunikations-Infrastrukturen ist in § 165 Abs. 4 TKG verankert. Sie wird explizit bisher nur auf öffentliche 5G-Mobilfunknetze angewendet, umfasst dort aber den gesamten Bereich der als kritisch identifizierten Funktionen und ist mit einer eigenen Technischen Richtlinie (BSI TR-03163) besonders eindeutig abgesteckt: Zertifizierungen von Kernnetzfunktionen, Management und Orchestrierung virtualisierter Netzwerke sowie Sicherheitsfunktionen des Management-Systems erfolgen nach den "Allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie" (Common Criteria, CC), Funktionen des eigentlichen Funkbetriebs und Netzmanagements im Radio-Access-Network (RAN) nach einem Zertifizierungsschema namens NESAS CCS-GI, und Sprach- und Datentransportfunktionen sowie IP-Netzwerkübergänge und -dienste außerhalb der eigenen Anlagen werden im Verfahren der Beschleunigten Sicherheitszertifizierung (BSZ) geprüft.

Kritische Komponenten müssen zertifiziert werden

In dieser Detailtiefe sind andere Sektoren noch nicht reguliert. Sie müssen bislang ihre kritischen Komponenten zwar auch schon registrieren und eine Garantieerklärung der Hersteller vorweisen, sind aber bislang nicht zur Zertifizierung der Komponenten gezwungen. Allerdings ist davon auszugehen, dass ähnliche Kriterienkataloge und die gesetzlichen Grundlagen auch für die übrigen KRITIS-Sektoren entwickelt und verabschiedet werden: § 2 Abs. 13 Nr. 3 BSIG ermöglicht für alle Sektoren, dass kritische Komponenten in einem Gesetz definiert werden.

Andere Sektoren noch nicht verpflichtet

Das TKG verlangt außerdem, im selben Paragraphen wie für das Sicherheitskonzept, dass jeder Netzbetreiber im Sektor Telekommunikation einen Sicherheitsbeauftragten bestimmen muss, der die Kontaktstelle zur Aufsichtsbehörde darstellt, und - für Anbieter außerhalb der Europäischen Union, die hier Netze betreiben - die Benennung eines verantwortlichen Ansprechpartners.

Sicherheitsbeauftragter nach § 166 TKG

IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG (BNetzA)

Der IT-Sicherheitskatalog verpflichtet Energieanlagenbetreiber zur Umsetzung IT-sicherheitstechnischer Mindeststandards. Kernforderung ist die Etablierung eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN EN ISO/IEC 27001 und dessen Zertifizierung. Diese Regelung ist 2021 noch einmal dahingehend verschärft worden, dass Energieversorger und Netzbetreiber im Falle einer Betriebsführung durch Dritte nicht mehr auf deren Zertifikate verweisen können, sondern selbst zertifiziert sein müssen. Eine Übergangsfrist erlaubt, diese Zertifizierung bis 31.3.2024 nachzuweisen.

Sicherheitskatalog für Energieversorger

Anders als der Katalog für die Sicherheitsanforderungen für Telekommunikationsbetreiber basiert der IT-Sicherheitskatalog für Energieerzeuger und Netzbetreiber nach § 11a Abs. 1a EnWG auf den Normen der ISO-270XX-Familie: EN ISO/IEC 27001 für das Informationssicherheitsmanagementsystem (ISMS), die Umsetzungshinweise zum ISMS der EN ISO/IEC 27002 und die sie ergänzenden Informationssicherheitsmaßnahmen für die Energieversorgung aus EN ISO/IEC 27019.

Standardisiert nach ISO 270XX

MaRisk, BAIT und VAIT

Für den Finanzsektor, der unter der Aufsicht der BaFin steht, gibt es seit 2017 einen eigenen Katalog über die "Bankenaufsichtlichen Anforderungen an die IT" (BAIT), seit 2019 auch "Versicherungsrechtliche Anforderungen an die IT" (VAIT), die beide auf der Basis der "Mindestanforderungen an das Risikomanagement" (MaRisk), aber in noch größerer Detailtiefe die gesetzlichen Verpflichtungen nach dem KWG konkretisieren. Beispielsweise setzen die BAIT in einem eigenen Kapitel zum IT-Notfallmanagement detaillierte Anforderungen für die in der MaRisk abstrakt geforderten Notfall- und Geschäftsfortführungskonzepte und Wiederherstellungspläne.

Anforderungskataloge für Banken und Versicherungen

Weil § 25a Abs. 1 S. 3 Nr. 4-5 KWG "eine angemessene personelle und technisch-organisatorische Ausstattung des Instituts" und "die Festlegung eines angemessenen Notfallmanagements, insbesondere für IT-Systeme" verlangt, präzisiert die Aufsichtsbehörde die Ansprüche an die Informationssicherheit selbst, statt auf durch das BSI freigegebene branchenspezifische Sicherheitsstandards zu setzen, wie sie in anderen Sektoren Anwendung finden.

Abweichende gesetzliche Grundlage

Um die Institutionen der Banken- und Versicherungswirtschaft zu unterstützen, die zu den kritischen Infrastrukturen zählen und damit neben der BaFin-Aufsicht auch berichtspflichtig gegenüber dem BSI sind, wurden den BAIT 2018 und den VAIT 2019 jeweils KRITIS-Module hinzugefügt, die genau erklären, welche zusätzlichen Anforderungen nach § 8a BSIG zu erfüllen sind, die nicht mit denen der eigenen Aufsicht deckungsgleich sind. Der Vorteil dieser Vorgehensweise besteht darin, dass alle Sicherheitsanforderungen im Rahmen der für Kreditinstitute ohnehin obligatorischen Jahresabschlussprüfung nachgewiesen werden können - und dieser Nachweis dann auch dem BSI genügt.

Spezifische KRITIS-Regeln für IT in der Finanzbranche

BAIT und VAIT gehen außerdem weiter als vergleichbare Regelwerke: Die BAIT-Novelle von 2021 nimmt Aspekte der DORA-Richtlinie bereits vorweg, weil sie sich aus derselben Quelle speisen: sowohl in die BAIT als auch DORA sind die Leitlinien der European Banking Association (EBA) eingeflossen, die 2019 veröffentlicht wurden und den gesamten Bereich der Finanz-IT grundlegend definiert haben. Sogar Anforderungen zur Durchführung von Penetrationstests sind hier vorgesehen, von denen in anderen Sektoren gar keine Rede ist.

Verbindliche Pentests

Branchenspezifische Sicherheitsstandards (B3S) für diverse KRITIS-Sektoren

Branchenspezifische Sicherheitsstandards (B3S) sind als Prüfgrundlagen zugelassen, um alle zwei Jahre die für Betreiber kritischer Infrastrukturen die verpflichtenden Nachweisprüfungen nach § 8a BSIG durchzuführen. Sie sind in aller Regel von den Branchenverbänden selbst erstellt und werden auf Antrag durch das BSI freigegeben, wenn die Behörde feststellt, dass sie geeignet sind - die Eignung wird immer für einen Zeitraum von zwei Jahren bescheinigt. B3S dienen auch als Richtschnur für Unternehmen, die unterhalb der Schwellenwerte zur Einstufung als kritische Infrastruktur bleiben und zu ihrer Einhaltung nicht verpflichtet sind. Die Umsetzung der spezifischen Anforderungen für die eigene Branche stößt auf eine breite Akzeptanz und verbessert das Niveau der Informationssicherheit. Allerdings ist die Anwendung je nach Branche unterschiedlich: Während die Gesundheitswirtschaft sich sehr eng am B3S-Konzept orientiert, gibt es im Finanz- und im Telekommunikationssektor auch B3S, aber eher für Nischen, die durch die mächtigeren Instrumente BAIT/VAIT bzw. die Vorgaben nach TKG nicht schon umfassend abgedeckt sind. Im Finanzsektor wurde beispielsweise ein B3S aufgelegt, der speziell auf die Zahlungssysteme der gesetzlichen Krankenkassen und Pflegeversicherungen abstellt. Im Sektor IT und Telekommunikation wurden B3S für die Anlagenkategorien "Rechenzentrum", "Serverfarm" und "Content Delivery Netzwerk" geschaffen, die im TKG nicht berücksichtigt wurden.

Prüfgrundlagen werden von Branchenverbänden selbst entwickelt

Lückenschluss bei Vorgaben für spezielle Anlagenkategorien

Sektoren und Branchen in der erweiterten KRITIS-Regulierung

Aktueller Stand und absehbare Entwicklung

Das Bundesministeriums des Innern und für Heimat (BMI) geht davon aus, dass rund 29.000 Betreiber als wesentliche oder kritische Einrichtungen einzustufen sind, wenn alle unter KritisV, NIS 2 und CER fallende Anlagen zusammengezählt werden. Die heute rund 1.250 beim BSI registrierten KRITIS-Betreibern machen also von den zukünftig zu berücksichtigenden Einrichtungen nicht einmal fünf Prozent aus. Bei den UBI, die erst schrittweise unter die Regulierung fallen, sind die absoluten Zahlen noch völlig unklar, aber tendenziell wird eine ähnliche Größenordnung erreicht werden. Nimmt man die Kategorie UBI 3 als Beispiel, sind derzeit bereits etwa 3.000-4.000 Anlagenbetreiber nach der StöV meldepflichtig. Auf welche Zahl man sich bei den größten deutschen Unternehmen, der Kategorie UBI 2, einigen wird, ist nicht ganz gewiss (auch

Anzahl der Betreiber der kritischen Infrastruktur vervielfacht

Entwicklung bei UBI ähnlich

Wichtige Einrichtungen nach NIS 2 unbekannter Faktor

wenn es wahrscheinlich bei den hundert umsatzstärksten Unternehmen bleibt, die im Top-100-Panel der Monopolkommission erfasst sind) - und wie viele ihrer wesentlichen Zulieferer in denselben Kreis gehören, ebenfalls. Völlig ungeklärt ist dagegen die Frage, wie viele wichtige Einrichtungen nach NIS 2 am Ende der Regulierung unterworfen sein werden. Die grob als Obergrenze anzusetzenden 5.000 UBI sind sicher kein Maßstab mehr, wenn es zur Zählung der "important entities" kommt.

Erweiterung der Sektoren

Unterschiedliche Abdeckung bezüglich Sektoren zwischen EU-Richtlinien und

Mit dem IT-SiG 2.0 wurde bereits 2021 der Sektor der Siedlungsabfallentsorgung dem Geltungsbereich des BSIG hinzugefügt. Konkrete Angaben über die kritischen Dienstleistungen, die Anlagenkategorien und Schwellenwerte sind aber noch nicht in die KritisV übernommen. Sie werden in der anstehenden Novelle der KritisV (Referentenentwurf voraussichtlich im ersten Halbjahr 2023) dort als zusätzlicher Sektor aufgenommen. Mit den Richtlinien CER und NIS 2 hat sich aktuell die Anzahl der Sektoren, in denen kritische Infrastruktur betrieben wird, auf dann elf erhöht. Gegenüber KritisV und BSIG neu hinzu kommen vor allem die öffentliche Verwaltung, ICT Service Management, Weltraum und Forschung, neben einigen Sektoren, die derzeit in Deutschland nur teilweise oder anders erfasst sind.

Beispiel wesentliche Einrichtungen

Sektor	KRITIS	NIS 2	NIS 2	Anmerkungen
Energie	x	x	x	
Transport / Verkehr	x	x	x	In NIS 2 und CER getrennte Sektoren
Bankwesen / Finanzen	x	x	x	In NIS 2 und CER getrennte Sektoren
Gesundheit	x	x	x	
Trink-/Abwasser	x	x	x	In NIS 2 und CER getrennte Sektoren
Digitale Infrastruktur	x	x	x	In KRITIS als IT und Telekommunikation
ICT Service Management		x		
Öffentliche Verwaltung		x	x	
Weltraum	x	x	x	In KRITIS nur teilweise in Transport berücksichtigt
Ernährung	x	x	x	In NIS 2 nur als "important entity" Lebensmittel

Zu diesen kritischen Sektoren kommen für das vollständige Bild noch die neu hinzugetretenen "important entities" der NIS 2, die nur in KRITIS und UBI eine teilweise Entsprechung haben, in der CER dagegen gar nicht vorkommen:

Beispiel wichtiger Einrichtungen

Sektor	KRITIS / UBI	NIS 2	Anmerkungen
Post- und Kurierdienste	x	x	In KRITIS-Sektor Transport teilweise enthalten
Abfallwirtschaft	x	x	Als Siedlungsabfallentsorgung KRITIS-Sektor
Chemikalien	x	x	Kategorie UBI 3
Industrie	x	x	Kategorie UBI 2 deckt den Sektor nur teilweise ab
Digitale Dienste	x	x	In NIS 2 und CER getrennte Sektoren
Forschung		x	Keine UBI, aber nach TMG reguliert

Mit der Erweiterung der Sektoren sind zusätzliche Branchen in den Fokus geraten. Die Frage der Bestimmung von Unternehmensgrößen wurde mit der NIS 2 eigentlich abschließend geklärt: Grundsätzlich sind nur mittlere und große Unternehmen betroffen, also solche, die mehr als 50 Mitarbeiter und einen Jahresumsatz oder eine Bilanzsumme von mehr als 10 Millionen Euro im Jahr haben. Aber in Abhängigkeit von Bedeutung und Kritikalität für die Versorgungssicherheit gibt es in fast allen Sektoren und Branchen Ausnahmen, die auch kleine Unternehmen auf das Niveau einer wesentlichen Einrichtung anheben können. Wie viele Unternehmen von diesen Mechanismen betroffen sein werden, ist schwer einzuschätzen, insbesondere dann, wenn für Sonder-

Unternehmensgröße als bestimmender Faktor

Ausnahmen nach Kritikalität

behandlungen besonders kritischer Fälle staatliche Deklarationen außerhalb der Systematik erfolgen.

Entwicklung des Bezugsrahmens – starre Größen oder risikobasiert?

Bei der Absenkung der Schwellenwerte im KRITIS-Bezugsrahmen, die 2021 in der KritisV ihren Niederschlag gefunden hatte, waren bereits einige Unternehmen unterschiedlicher Branchen von den neuen Kriterien erfasst worden - die Begründung zur Novelle des IT-SiG enthielt bereits eine Schätzung der zusätzlichen KRITIS-Einrichtungen, die beispielsweise rund 130 Stromerzeuger, sieben Rechenzentren, drei IXPs usw. enthielt. Die Bedeutung dieser Schwellenwerte, auch wenn sie noch weiter abgesenkt würden, wird im Zusammenhang mit der NIS-2-typischen Bewertung nach Unternehmensgröße möglicherweise an Dynamik verlieren, weil der größere Teil der Unternehmen nicht mehr risikobasierten Einzelbewertungen unterliegen wird, sondern pauschal aufgrund seiner Wichtigkeit oder Wesentlichkeit identifiziert wird.

Kritische digitale Dienste

Digitale Infrastruktur und verbundene Dienstleistungen (nach KritisV und NIS 2)

Vier Kategorien digitaler Dienste sind immer wesentliche Einrichtungen

In der ersten NIS von 2016 waren bereits DNS, TLD, Cloud Computing, Vertrauensdienste und IXPs berücksichtigt. Gleichzeitig kannte die deutsche Gesetzgebung bereits Rechenzentren und Serverfarmen. Eine vollständige Übereinstimmung der Definitionen und Anwendungsbereiche ist auch nach NIS 2 und CER noch nicht erreicht. Die Kernbereiche der Regulierung sind aber klar benannt, was den Charakter der Dienstleistungen angeht, die erfasst sind. Es gibt eine Abstufung der Bedeutsamkeit bzw. Kritikalität, die einzelnen Dienstleistungen der digitalen Infrastruktur zugemessen wird, angefangen bei den vier wichtigsten, die immer zu den wesentlichen Einrichtungen gehören - ohne Rücksicht auf die Größe der Unternehmung. Diese Sonderregelung gilt für:

1. Domain Name Service (DNS)
2. Register der Top-Level-Domains (TLD)
3. Internet-Knoten (IXP)
4. Vertrauensdienste

Alle vier Kategorien sind also auch dann der kritischen Infrastruktur im Sinne wesentlicher Einrichtungen der NIS 2 zuzurechnen, wenn sie von Kleinstunternehmen betrieben werden.

DNS

DNS ohne Root-Server

Die rund 1600 Instanzen der Root-Zone, die das globale Rückgrat des DNS darstellen, sind nach kontroversen Verhandlungen mit der Europäischen Kommission explizit nicht in den Anwendungsbereich der NIS 2 aufgenommen worden. Von den 12 Root-Nameserver-Betreibern, die es weltweit gibt, befinden sich zehn außerhalb Europas, die allermeisten in den USA, darunter auch Regierungsinstitutionen: Vor Verabschiedung der Richtlinie setzte sich die Einsicht durch, keinen Anspruch darauf erheben zu können, etwa das amerikanische Verteidigungsministerium oder die NASA auditieren zu können.

TLD-Register

Nationale und europäische Register von Top-Level-Domains

Die von der Internet Corporation for Assigned Names and Numbers (ICANN) delegierten Aufgaben der Verwaltung von TLD (Ländercodes: ccTLD, generische: gTLD oder neue: nTLD) werden von unabhängigen Organisationen erbracht, den TLD-Registern, häufig auch Network Information Centers (NIC) genannt. Von den generischen TLD ist nur die .info an ein europäisches Register delegiert, in den anderen TLD sind es Dutzende eigenständiger NIC.

Internet-Knoten

Austauschknoten für Datenverkehr zwischen Providernetzen

Die Netzknoten des Internet, Internet Exchange Points (IXP), finden sich ebenfalls unabhängig von der Unternehmensgröße ihrer Betreiber im Geltungs- und Anwendungsbereich der NIS 2 wieder. Neben den 20 größten, typischerweise national bedeutenden Einrichtungen in den Mitgliedstaaten der EU gibt es eine Fülle regionaler Knotenbetreiber (zwei Dutzend etwa in Deutschland), die alle als Betreiber kritischer Infrastrukturen gelten. Insgesamt sind in Europa derzeit über 150 IXP aktiv, fast die Hälfte aller Knoten weltweit. Sie schaffen in ihren Rechenzentren Verbindungen zwischen den autonomen Systemen (AS) der am jeweiligen IXP angeschlossenen Anbieter von Internet-Infrastrukturdiensten, als Austauschplattform für den Datenverkehr zwischen den Netzbetreibern. Dazu gehören nicht nur die Zugangsnetze (in der Terminologie der NIS 2: öffentliche elektronische Kommunikationsnetze und öffentlich zugängliche elektronische Kommunikationsdienste), sondern auch die Inhaltszustellnetze (CDN).

Vertrauensdienste

Zertifikatsbasierte elektronische Identifizierung und Authentifizierung

Von besonderem Interesse für die Bereitstellung von sicheren Werkzeugen für die Datenkommunikation sind die Lieferanten von Produkten und Dienstleistungen zur Erstellung, Überprüfung und Validierung von (qualifizierten oder unqualifizierten) elektronischen Signaturen sowie Zertifikaten für die Authentifizierung von Webseiten. Seit 2016 regelt eine eigene Verordnung, die "European Identification, Authentication and Trust Services Regulation" (eIDAS), den Bereich dieser Vertrauensdienste. Ursprünglich nur für echte Third-Party-Trust-Identitätsmodelle vorgesehen, ist für die eIDAS eine Öffnung in Richtung der sogenannten "selbst-souveränen Identitäten" (SSI) erfolgt, die im "European Self-Sovereign Identity Framework" (ESSIF) verankert ist. Vertrauensdiensteanbieter können seither in einem SSI-Netzwerk über eine SSI-eIDAS-Bridge integriert werden. Ob und wie auch der SSI-Broker als kritische Infrastruktur angesehen werden muss, ist derzeit unklar.

Cloud-Computing-Dienste

Transparente, dynamisch skalierbare Rechenleistungen und Speicheranwendungen

Mit Cloud-Computing ist allgemein die Bereitstellung von Ressourcen gemeint, die über ein geteiltes, meist externes, aber häufig in die internen IT-Systeme weitgehend integriertes Rechnernetz eingebunden werden. Charakteristisch für Cloud-Dienste ist ihre skalierbare, ohne weitere Vertragsänderungen elastisch mitwachsende oder schrumpfende Kapazität, die gemeinsam über mehrere Standorte verteilt liegen kann und transparent zur Verfügung gestellt wird. Cloud-Dienste können von Speicherplatz über Rechenleistung bis zur Nutzung von Software inklusive Fachanwendungen alle Formen der Datenverarbeitung anbieten. Der Verantwortungsbereich kann dabei zwischen Nutzer und Anbieter der Cloud-Dienste zur einen oder anderen Seite hin überwiegen: Infrastructure as a service (IaaS) bietet quasi einen virtualisierten Hardware-Rahmen, in dem die innerhalb der Cloud-Ressourcen stattfindende Datenverarbeitung und damit die Verantwortung für die Informationssicherheit der Anwendungen fast vollständig beim Kunden liegt, während Software as a service (SaaS) dazu genau entgegengesetzt eine annähernd hundertprozentige Betriebs- und Sicherheitsverantwortung beim Cloud-Anbieter sieht. Die vielen Betriebsmodelle der Cloud-Angebote bieten Lösungsvorschläge für fast alle IT-Problemstellungen, die Unternehmen oder andere Institutionen beschäftigen - wenn man sich vergegenwärtigt, dass dies immer unter der Prämisse stattfindet, die Verarbeitung der Daten außerhalb des eigenen Verantwortungsbereichs zu delegieren. Die daraus entstehenden Datenschutzfragen inklusive der Übermittlung in möglicherweise unzulässige Drittstaaten sind kein unmittelbarer Gegenstand der Einstufung als kritische Infrastruktur, aber sie müssen im Rahmen der Informationssicherheitsanforderungen natürlich mitbeantwortet werden.

Rechenzentrumsdienste

Rechenzentren als digitale Infrastruktur

Alle Betreiber von Rechenzentren sind Erbringer von Infrastrukturleistungen, die erstmals 2014 mit einem eigenen DIN-Standard (DIN EN 50600) eine umfassende Definition erfahren haben. Der Begriff des Rechenzentrums ist in der Norm weit gefasst, weil er auf die Funktionalität abhebt - im Prinzip kann nach DIN EN

50600 jeder Serverraum ein Rechenzentrum sein. Innerhalb des KRITIS-Sektors stellen Rechenzentren eine eigene Anlagenkategorie dar, die in Anhang 4 der KritisV mit einem Schwellenwert anhand der aufgenommenen Leistung versehen ist (früher 5 MW, nach Änderung 2021 nun 3,5 MW).

Online-Plattformen: Suchmaschinen, Marktplätze, Social Media

Separate Kategorien, gemeinsame Regulierung für Plattformbetreiber

Zu den 2018 eingeführten ADD gehören die Betreiber von Suchmaschinen neben anderen Diensten, die als Online-Plattformen definiert sind. Das BSI begründet die Aufnahme in den Katalog der verbundenen Dienstleistungen der ADD am Beispiel der Online-Marktplätze, die ihre Dienste gebündelt Dritten anbieten, um Waren an Käufer zu vermitteln: "Normzweck ist der Schutz der quasi-infrastrukturellen Bedeutung des Marktplatzes." Sie gehören mit der NIS 2 nicht zu den wesentlichen, aber den wichtigen Einrichtungen.

Inhaltszustellnetze

Datenmengen

Content Delivery Networks (CDN) sind Netze dezentraler Server zur Gewährleistung von hoher Verfügbarkeit, netztopologisch oder geografisch direktem Zugang und schnellem Abruf digitaler Inhalte oder Dienste aller Art: Die Palette reicht von Social-Media-Inhalten über Videostreaming bis zur verteilten Bereitstellung zum Beispiel von Software. Sie arbeiten im Auftrag von Anbietern, die im CDN an Brückenköpfen innerhalb oder an den Rändern der Netzwerke, in denen sich ihre Kunden befinden, ihre Angebote platzieren.

Öffentliche elektronische Kommunikationsnetze und öffentlich zugängliche elektronische Kommunikationsdienste

Elektronische Kommunikation (alles außer TK)

Die Definitionen für die öffentlichen elektronische Kommunikationsnetze und die öffentlich zugänglichen elektronischen Kommunikationsdienste stammen aus dem EECC, der in die NIS 2 überführt wurde: Ersteres ist ein elektronisches Kommunikationsnetz, das ganz oder überwiegend der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen. Letzteres umfasst "Internetzugangsdienste", interpersonelle Kommunikationsdienste (wie zum Beispiel E-Mail) und "Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden". Unter diese breite Definition fallen alle Internet-Provider und die meisten der in ihren Netzen angebotenen Dienste, aber auch die klassischen Fernsehkabelnetzbetreiber, soweit sie nicht sowieso als Internetzugangsdienst miterfasst sind.

Relevanz und Konsequenzen für Gaia-X und die Gaia-X Föderationsdienste

Betroffenheit prüfen – Verstöße gegen Regulierung vermeiden

Die Anwendung der KRITIS-Regulierung auf den Betrieb in und für die Gaia-X-Umgebung ist in mehrfacher Hinsicht möglich, nicht immer zwingend geboten, aber möglicherweise auch dann erforderlich, wenn sie nach formalen Kriterien vielleicht nicht unbedingt angezeigt zu sein scheint. Wichtig ist, die Entscheidung auf informierter Basis zu treffen, denn Verstöße gegen die Pflichten der Regulierung kritischer Infrastruktur können empfindliche Sanktionen nach sich ziehen, auch wenn sie möglicherweise unbeabsichtigt oder aus Unkenntnis über die Verpflichtung des eigenen Unternehmens und seiner Dienstleistung resultieren.

Anwendung bekannter Schwellenwerte

Zu den Faktoren, die dabei betrachtet werden müssen, ist auf der Ebene der Infrastruktur der Betrieb der Rechenzentren und ihrer Netzwerke im Vordergrund. Hier ist schon vor dem Hintergrund der Schwellenwerte für eine elektrische Leistung von 3,5 MW nach der aktuellen KritisV eindeutig der Bereich der kritischen Infrastruktur berührt, auch wenn die Plattform über mehrere Rechenzentren verteilt betrieben wird - die meisten Rechenzentren, in denen GXFS-Angebote verarbeitet werden, dürften oberhalb dieser Schwelle liegen. Im Portfolio der Föderationsdienste selbst ist, ohne eine Aussage zur Einhaltung oder Überschreitung der

Schwellenwerte zu machen, praktisch die gesamte Bandbreite der Dienstleistungen vertreten, die nach KritisV und NIS 2 zu den digitalen Diensten gehören. Welches Ausmaß hier im Einzelnen erreicht wird, ist zu prüfen.

Gaia-X Policy Rules zur umgebungsinternen Validierung

Der Aufnahme- und Validierungsprozess für Föderationsdienste umfasst bereits die Bestätigung von dokumentierten "Policy Rules" und anderen Regeln, die als "Rahmenwerk zur Regelkonformität" herangezogen werden, um die Einhaltung der Anforderungen zum Beispiel aus den Bereichen der Verschlüsselung, Datenschutzstandards und Interoperabilität sicherzustellen. Das ist für die Akkreditierung innerhalb des "Föderierten Katalogs" der Gaia-X-Umgebung verbindliche Voraussetzung, steht aber in keinem unmittelbaren Zusammenhang mit Sicherheitsanforderungen, die im Rahmen einer Einstufung als Betreiber kritischer Infrastruktur angelegt werden. Die Motivation ist eine andere: Nach der Validierung im Prozess der Akkreditierung als Anbieter von Föderationsdiensten verifizierbare Beglaubigungen ausgestellt, die Sicherheitsstufen dokumentieren und innerhalb des GXFS-Kontexts automatisch akzeptiert sind. Außerhalb des GXFS-Umfelds können diese Beglaubigungen einen Anhaltspunkt darstellen, dass die Einhaltung von Sicherheitsstandards ein wesentlicher Bestandteil des Föderationsdienstes ist, aber für die konkreten Vorgaben der KRITIS-Regulierung dienen sie nur als Indikator, nicht als regelkonformer Nachweis.

Möglicher Indikator für die Einhaltung von KRITIS-Vorgaben

Handreichung für die Bewertung des GXFS-Portfolios

Schematisierte Einstufung

Der Antwort auf die Frage, ob ein bestimmtes Angebot innerhalb des Portfolios der Föderationsdienste die Kriterien für die Einstufung als kritische Infrastruktur erfüllt, kann man sich nur iterativ nähern. Schematisch folgt die Entscheidung einem zumindest formal eindeutig klassifizierten Kriterienkatalog, der nach Dienst und Unternehmensgröße einordnet.

Dienste	Große Unternehmen	Mittlere Unternehmen	Kleinst- und Kleinunternehmen
DNS			
TLD registry			
Qualifizierte Vertrauensdienste			
Öffentliche Kommunikationsnetze/-dienste			
IXP			
Cloud-Computing-Dienste			
Rechenzentren			
Inhaltszustellnetze (CDN)			
Nichtqualifizierte Vertrauensdienste			

Wesentliche Einrichtungen
Wichtige Einrichtungen
weder wesentlich noch wichtig

Abbildung: Prüfschema für die Einstufung als Betreiber kritischer Infrastruktur

Ausnahmen sind die Regel

Der Haken an dieser noch überschaubaren Zuordnung: Sie stimmt nur solange, wie ein Dienst nicht aus anderen Gründen auf das nächsthöhere Niveau der Wichtig- oder sogar Wesentlichkeit aufgestuft wird. Gründe dafür, dass auch ein kleines Unternehmen mit weniger als 50 Mitarbeitern zu den wesentlichen Einrichtungen der kritischen Infrastruktur gehören kann, wären zum Beispiel vorhanden, wenn im betrachteten nationalen Umfeld niemand sonst diesen als kritisch einzustufenden Dienst erbringt. Ausnahmen von den Unternehmensgrößen als Maßstab der Einstufung gibt es nicht nur für die Anwendungsbereiche öffentlicher elektronischer Kommunikationsnetze und -dienste, für Vertrauensdiensteanbieter und die TLD-Register. Grundsätzlich kann jedes auch sehr kleine Unternehmen auf die Stufe der Wesentlichkeit gehoben werden, wenn ein Ausfall seiner Dienste zu wesentlichen Störungen der Daseinsvorsorge führt.

Föderationsdienste in der Selbsteinschätzung als kritische Infrastruktur

Konkretisierung der Anforderungen bis Herbst 2024

Bis zum 17. Oktober 2024 wird die Europäische Kommission Durchführungsrechtsakte erlassen, die die technischen und methodischen Anforderungen aller in Frage kommenden Dienste festlegen. Angekündigt sind diese Rechtsakte für Dienste mit hoher Kritikalität wie DNS, TLD-Register, Vertrauensdienste, Cloud Computing, Rechenzentren und CDN, zusätzlich aber auch für verwaltete IT- und Sicherheitsdienste, Online-Marktplätze und -Suchmaschinen sowie Plattformen für soziale Netzwerke. Auch mit einer solchen Festlegung der konkreten Vorgaben bleibt aber immer noch die Beurteilung der Frage, ob ein spezifischer Dienst aus dem eigenen Angebot zu den kritischen Dienstleistungen gehört - und nach Würdigung der schematisierten Prüfkriterien und individuellen Einschätzungen der Bedeutsamkeit nun tatsächlich unter die Regulierung der kritischen Infrastruktur fällt.

Selbsteinschätzung weiterhin maßgeblich

Die Entscheidung, ob man sich in dieser Weise eingestuft sieht, wird zunächst von den Betreibern der Dienste selbst getroffen. Keine Behörde wird zehntausende von Unternehmen systematisch auf ihre Kritikalität und Bedeutsamkeit überprüfen, aber die Selbsteinschätzung wird von der staatlichen Erwartungshaltung in der Regel nicht abweichen: Die Mechanismen der Risikoabschätzung sind grundsätzlich immer dieselben. Die Vorgehensweise für eine Bewertung der Föderationsdienste im Hinblick auf die Frage, ob sie selbst als kritische Infrastruktur zu betrachten sind oder immerhin für Betreiber kritischer Infrastrukturen als Drittdienstleistung angeboten werden, folgt den Prinzipien der Eintrittswahrscheinlichkeit von Ausfällen oder Störungen und dem zu erwartenden Schaden, der daraus entstünde. Einziger Unterschied zum Risikomanagement eines Unternehmens ist die Bewertung der Auswirkungen auf die Allgemeinheit. Für die Unternehmensziele stellt dies vielleicht keinen klassischen Risikofaktor dar, aber im Hinblick auf die staatliche Pflicht zur Daseinsvorsorge zwingt es die privaten Anbieter in die Regulierung.

Bewertungskriterien aus dem Risikomanagement – außer der Bedeutung für das Gemeinwohl

Vertrauensdienste fraglos betroffen

Einfach zu beantworten ist die Frage der Kritikalität und Bedeutsamkeit für die Versorgungssicherheit bei den Diensten, die auch nach der NIS 2 als wesentlich und damit unabdingbar nach den Maßstäben der KRITIS-Anforderungen bewertet werden müssen. Innerhalb der Föderationsdienste wären dies zum Beispiel die Vertrauensdienste, soweit sie als qualifizierte Dienste angeboten werden: das SSI-Framework deckt für sich genommen nicht alle Voraussetzungen dafür ab, weil es keinen qualifizierten Vertrauensdienst darstellt, aber in dem Moment, in dem "echte", also qualifizierte Identitäten über die eIDAS-SSI-Bridge betrieben werden, ist dieser Status erreicht, und die Einstufung als wesentliche Einrichtung greift unmittelbar.

Auch unkritische Dienste sind kritisch, wenn sie wesentlich an der Erbringung anderer kritischer Dienste mitwirken

Noch einfacher ist es, die Feststellung der Einstufung anhand der Frage vorzunehmen, ob und in welchem Grad der Bedeutsamkeit für den Betrieb der kritischen Infrastrukturen von Gaia-X-Anwendern Föderationsdienste genutzt werden. Auf eine einfache Formel gebracht: Auch eine für sich genommen unkritische Dienstleistung kann zur Erbringung von kritischen Diensten wesentlich sein. Zwar liegt die Verantwortung dafür, regulierungskonform zu handeln, in letzter Konsequenz bei den KRITIS-Betreibern selbst, nicht bei den Drittdienstleistern. Von diesen ist aber zu erwarten, dass sie selbst ihre Angebote so zur Verfügung stellen, dass ein regulierungskonformer Einsatz möglich ist, jederzeit nachgewiesen und auch vor Ort überprüfbar sein muss. Am radikalsten ist der Durchgriff der Aufsichtsbehörden auf Drittdienstleister sicher im Finanzsektor geregelt. Dort wäre es tatsächlich möglich, dass die BaFin Zugang zu den Einrichtungen der Drittdienstleister verlangt, wenn sie für Kreditinstitute oder Versicherungen tätig sind.

Folgenabschätzung

Aufwand durch KRITIS-Regulierung

Ob sich der Aufwand lohnt, die Maßgaben einer KRITIS-Regulierung zu erfüllen, auch wenn formal die Größe des Unternehmens dafür gar nicht ausreichend zu sein scheinen, ist Gegenstand einer Folgenabschätzung, die Dienstleister innerhalb einer Föderation für ihre Angebote vornehmen müssen.

Die Anbieter von Leistungen, die im Föderierten Katalog von Gaia-X registriert sind, müssen für sich selbst die Fragen beantworten, die im Zusammenhang mit der Inanspruchnahme ihrer Dienste durch Betreiber kritischer Infrastrukturen entstehen: Welche Vorkehrungen und Dokumentationspflichten entstehen zusätzlich für eine Dienstleistung, wenn sie im KRITIS-Zusammenhang genutzt werden soll? Was bedeuten Prüfungen durch Auftraggeber oder Aufsichtsbehörden, welche zusätzlichen Verpflichtungen geht man ein, wenn man sich von Kunden im Rahmen ihrer vertraglichen Mindestanforderungen auditieren lässt? Welcher Aufwand entsteht dadurch, und ist der Anbieter eines Föderationsdienstes dazu bereit und in der Lage, diesen Aufwand für die Aufrechterhaltung der Kundenbeziehung zu akzeptieren? Und wie groß ist dann noch der Unterschied, sich selbst sozusagen freiwillig als kritischen Betreiber einzustufen und so zu agieren, als sei man dazu verpflichtet?

Vorkehrungen, Verpflichtungen, Dokumentation

Aufwand durch Kundenanforderungen

Wer nicht potenziell als Anbieter von Leistungen von der Einstufung als kritische Infrastrukturen seiner Kunden mitbetroffen sein will, hat als denkbaren, aber wenig attraktiven Ausweg nur die Gestaltung von Geschäfts- und Vertragsbedingungen, die Betreiber kritischer Infrastrukturen grundsätzlich von der Inanspruchnahme der Dienste ausschließen, sofern sie als wesentlicher Teil des kritischen Dienstes gelten müssten.

Non-Compliance nur bei Ausschluss bestimmter Kunden

Risikomanagement für digitale Dienste im Rahmen von Gaia-X

Für eine individuelle Bewertung digitaler Dienste, deren Kritikalität eine entsprechende Berücksichtigung der Mindestanforderungen nach KritisV und NIS 2 erfordert, muss eine konkrete Evaluierung der Risikofaktoren stattfinden. Grundsätzlich sehen die Voraussetzungen für eine regulierungskonforme Integration der Dienste in das Risikomanagement der Betreiber kritischer Infrastrukturen eine Reihe umfassend definierter Maßnahmen vor, die nach Art. 21 Abs. 2 S. 1 NIS 2 einen "gefahrenübergreifenden Ansatz" verfolgen müssen und sich systematisch wie folgt einordnen lassen:

Gefahrenübergreifender Ansatz zur Integration in das eigene Risikomanagement

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Für die Erbringer von Dienstleistungen im GXFS-Umfeld stellt dieser Maßnahmenkatalog gleichsam eine Checkliste dar, mit der sie die Föderationsdienste auf Einhaltung der Vorgaben überprüfen können, wenn sie für den Betrieb kritischer Infrastrukturen eingesetzt werden sollen. Immer unter dieser Prämisse der Kritikalität der Dienstleistung gilt auch: Die Umsetzung der Maßnahmen aus Art. 21 sind Mindestanforderungen,

Checkliste zur Einhaltung der KRITIS-Vorgaben

deren Nichtbeachtung im Zusammenhang mit wesentlichen Störungen und Ausfällen der kritischen Dienste zu Sanktionen führen kann.

Dokumentation und Zertifizierung von KRITIS-Diensten im GXFS-Umfeld

Mehr als nur Indikatoren: Zertfizierungen nach einschlägigen Standards

Abgeleitet aus der Klassifizierung als ADD aus der NIS 1, die im Rahmen der NIS 2 in die Kategorie der wesentlichen oder wichtigen Einrichtungen fallen, ist davon auszugehen, dass alle Föderationsdienste, die als Cloud-Computing-Dienste zu betrachten sind, kritische Infrastruktur oder immerhin UBI sind. Sie unterliegen damit den Pflichten zum Nachweis der Einhaltung entsprechender Mindestanforderungen an die Informationssicherheit, die nicht nur den Aufsichtsbehörden bereitgestellt werden müssen. Im Beschaffungsprozess von Kunden, die ihrerseits als Betreiber kritischer Infrastruktur eingestuft sind, können die Nachweise auch dazu dienen, die nötigen Voraussetzungen als regulierungskonformer Drittdienstleister zu erfüllen. Ein Weg, diesen Nachweis zu vereinfachen, ist die beurkundete Zertifizierung nach einschlägigen Normen wie der EN ISO / IEC 27001, zum Beispiel auf Basis des BSI IT-Grundschutz-Kompendiums. Zu den Pflichten, die gegenüber den Vertragspartnern in jedem Fall einzuhalten sind, gehören zum Beispiel die Einräumung von Audit-Rechten und die Vorlage von Sicherheitsnachweisen - auch ohne Zertifikat sollte das leicht fallen, wenn solche Nachweise aus gegebenenfalls durchgeführten Überprüfungen nach § 8a BSIG vorhanden sind. Öffentliche Auftraggeber sind nach den Mindeststandards des BSI zudem in der Pflicht, vom Cloud-Dienstleister Prüfberichte und Testate nach dem C5-Katalog einzufordern.

Auditrechte für Kunden einräumen

Blickwinkel Zulieferkette: KRITIS-Betreiber muss Dienste immer erbringen können

Wenn Dienste nicht mehr verfügbar sind: KRITIS-Betreiber benötigen Exit-Strategie

KRITIS-Betreiber, die als Auftraggeber kritische Dienstleistungen in die Cloud eines Auftragnehmers auslagern, müssen sich gegen einen Ausfall dieser Dienstleistungen absichern. Sie müssen vor allem sicherstellen, dass die Verfügbarkeit ihrer kritischen Dienste auch dann gewährleistet bleibt, wenn der Clouddienst ausfällt. Wenn die Risikoanalyse ergibt, dass bestimmte Dienste nicht mehr benutzt werden dürfen - bestes Beispiel: Datenverarbeitung bei amerikanischen Cloudbetreibern, auch wenn die Daten europäische Rechenzentren nicht verlassen, nach Wegfall des Safe-Harbor-Abkommens zwischen der EU und den USA - muss eine Exit-Strategie vorliegen: der KRITIS-Betreiber muss nachweisen, dass er den gesamten Betrieb auch kurzfristig auf einen eigenen On-Premise-Server oder die Cloud eines DSGVO-konformen Anbieters verlegen kann.

KO-Kriterien Portabilität, Georedundanz, Resilienz

Für besonders innovative Dienste, die vielleicht sogar als Alleinstellungsmerkmal der GXFS-Umgebung gelten, kann das fatale Folgen haben: wenn der Dienst so exklusiv oder ausschließlich in einem bestimmten Umfeld möglich ist, läuft die vorgeschriebene Exit-Strategie der Auftraggeber ins Leere. Die Betreiber kritischer Infrastrukturen müssen jederzeit in der Lage sein, einen in Anspruch genommenen Dienst unterbrechungsfrei auf einer anderen Plattform weiterzubetreiben, um den an sie gestellten gesetzlichen Anforderungen zu genügen. Hier sind Konzepte gefragt, die das nötige Maß an Ausfallsicherheit im GXFS-Umfeld gewährleisten, entweder durch Georedundanz des Serverbetriebs und resiliente Netzwerkarchitektur innerhalb von Gaia-X, oder durch Unterstützungsleistungen bei der Portabilität von kritischen Diensten zu anderen Betreibern, privaten Clouds oder On-Premise-Plattformen.

Fazit und Empfehlungen

Maßnahmen schon vor Behördenentscheidung prüfen

Wer potenziell zu den Betreibern kritischer Infrastruktur in Deutschland und anderen Ländern Europas zählt, muss sich nach allen Seiten absichern, ob und in welcher Weise externe Berichts- und Meldepflichten und Regulierungen seines Informationssicherheitsmanagements und andere Vorschriften anzuwenden sind. Die Entscheidung obliegt im Zweifel den Aufsichtsbehörden, aber jedes Unternehmen ist gut beraten, vor einer offiziellen Feststellung der Zugehörigkeit zum Kreis der Betreiber kritischer Infrastruktur durch das BSI bereits entsprechende Maßnahmen zu prüfen, damit sie unverzüglich eingeleitet werden können, sobald die Verpflichtung eintritt. Dies gilt auch für Betreiber, deren Dienstleistungen im Umfeld kritischer Infrastrukturen sich noch in Planung oder Umsetzung befinden, weil der Aufwand zur Einhaltung der einschlägigen Vorschriften aus KritisV und branchenspezifischen Regulierungen bereits zu diesem Zeitpunkt eingeschätzt werden sollte, um die dafür benötigten Ressourcen zur Verfügung stellen zu können.

Notwendigkeit der Einhaltung von Mindestanforderungen unabhängig davon, ob nationale oder europäische Regulierung

Zertifizierung ist Hilfsmittel

Zertifizierungen sind ein sinnvolles Instrument zur Implementierung der Sicherheitsanforderungen, das den Betreibern kritischer Infrastrukturen an die Hand gegeben wird, aber in den seltensten Fällen vorgeschrieben: Sie sind hilfreich bei der Erfüllung der Nachweispflichten, aber sie schützen nicht vor Überprüfungen und Eingriffen der Aufsichtsbehörden.

Europaweite Weiterentwicklung im Blick behalten

Der sich laufend ändernde Rechtsrahmen muss in jedem Fall sorgfältig beobachtet werden. Welche spezifischen Umsetzungen in das jeweilige nationale Recht der EU-Mitgliedstaaten vor allem die beiden Richtlinien NIS 2 und CER erfahren werden, wird bis zur festgesetzten Umsetzungsfrist Ende 2024 nach und nach erkennbar sein. Dabei wird es beispielsweise mehr oder weniger starke Abweichungen geben, was die Rolle und Befugnisse der nationalen Aufsichtsbehörden betrifft. Die Verhältnisse in Deutschland sind von überwiegend absehbarer Tendenz, auch wenn es für die Umsetzungen im KritisDG und einem künftigen IT-SiG 3.0 noch keine Referentenentwürfe gibt. Für ein europaweit agierendes Konsortium wie die Betreiber der Gaia-X-Umgebung wird aber perspektivisch nicht nur die Regulierung kritischer Infrastrukturen im deutschen Markt relevant sein.

Abkürzungsverzeichnis

ADD	Anbieter digitaler Dienste
AS	Autonomous Systems, autonome Systeme
AtG	Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren („Atomgesetz“)
AWV	Außenwirtschaftsverordnung
B3S	Branchenspezifische Sicherheitsstandards
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAIT	Bankenaufsichtliche Anforderungen an die IT
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BDSG	Bundesdatenschutzgesetz
BImSchV, StöV	Zwölfte Verordnung zur Durchführung des Bundes- Immissionsschutzgesetzes (Störfall-Verordnung - 12. BImSchV)
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
BSZ	Beschleunigte Sicherheitszertifizierung
C5	Cloud Computing Compliance Criteria Catalogue
CC	Common Criteria („Common Criteria for Information Technology Security Evaluation“, allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie)
CDN	Content Delivery Networks, Inhaltszustellnetze
CE-Kennzeichen	Conformité Européenne (europäische Konformität), kennzeichnet Produkte, die den produktspezifisch geltenden europäischen Richtlinien entsprechen
CENELEC	Comité Européen de Normalisation Électrotechnique (Europäisches Komitee für elektrotechnische Normung)
CER(-Richtlinie)	Critical Entities Resilience Directive („Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates“)
CNC	Computerized Numerical Control, Verfahren zur Steuerung von Werkzeugmaschinen

CPU	Central Processing Unit, Hauptprozessor
CRA	Infrastructure as a Service
DIN	Deutsches Institut für Normung
DNS	Domain Name System
DORA	Digital Operational Resilience Act („Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011")
DSGVO	Datenschutz-Grundverordnung („Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG")
EBA	European Banking Association
ECI(-Richtlinie)	European Critical Infrastructure Directive („Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern")
EECC(-Richtlinie)	European Electronic Communication Codex („Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation")
EG	Europäische Gemeinschaft
eIDAS(-Verordnung)	Electronic Identification, Authentication and Trust Services („Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG")
EN	Internet Exchange Point, Internet-Austauschknoten
EnWG	Kritische Infrastrukturen
ESSIF	KRITIS-Dachgesetz (in Vorbereitung)
EU	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)
Gaia-X	Kreditwesengesetz
gematik	Mindestanforderungen an das Risikomanagement
GG	Megawatt
GXFS	Gaia-X Federated Services
IaaS	Infrastructure as a Service
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organisation for Standardization
IT	Informationstechnik
IT-SiG, IT-SiG 2.0	IT-Sicherheitsgesetz (Artikelgesetz)
ITS	Implementing Technical Standards
IXP	Internet Exchange Point, Internet-Austauschknoten

KRITIS	Kritische Infrastrukturen
KritisDG	KRITIS-Dachgesetz (in Vorbereitung)
KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)
KWG	Kreditwesengesetz
MaRisk	Mindestanforderungen an das Risikomanagement
MW	Megawatt
NESAS CCS-GI	NESAS (Network Equipment Security Assurance Scheme) Cybersecurity Certification Scheme - German Implementation
NIC	Network Information Center
NIS 2(-Richtlinie)	Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union („Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148", NIS-2-Richtlinie)
NIS(-Richtlinie)	Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit („Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union", NIS-Richtlinie)
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen
RAN	Radio Access Network
RTS	Regulatory Technical Standards
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition, System zur Überwachung und Steuerung technischer Prozesse
SGB V	Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung
SGB X	Sozialgesetzbuch (SGB) Zehntes Buch (X) - Sozialverwaltungsverfahren und Sozialdatenschutz
SSI	Self-Sovereign Identity
StöV	siehe BImSchV
TKG	Telekommunikationsgesetz
TLD, gTLD, ccTLD, nTLD	Top Level Domain, generic TLD, country TLD, new TLD
TMG	Telemediengesetz
TR	Technische Richtlinie
UBI	Unternehmen in besonderem öffentlichen Interesse
UP Bund	Umsetzungsplan für die Bundesverwaltung
UP KRITIS	Umsetzungsplan für die Kritischen Infrastrukturen
VAG	Versicherungsaufsichtsgesetz
VAIT	Versicherungsrechtliche Anforderungen an die IT
ZAG	Zahlungsdiensteaufsichtsgesetz

Herausgeber:
eco - Verband der Internetwirtschaft e.V.
Ansprechpartner: Emma Wehrwein, Vivien Witt, Lauresha Memeti - Projektteam GXFS-DE
E-Mail: pmo@gxfs.de
Adresse: Lichtstraße 43h, 50825 Köln

Beauftragter Studienersteller:
nGENn GmbH
Ansprechpartner: Ulrich Plate, Senior Information Security Consultant
E-Mail: plate@ngenn.net
Adresse: nGENn GmbH, Erdfunkstelle 1, 61250 Usingen