iX
MAGAZIN FÜR PROFESSIONELLE IT
3
MÄRZ
2024

Chaos bei VMware
Folgen der Übernahme

9,90 €
Österreich 10,90 €
Schweiz 15.90 CHF
restl. Europa 11,60 €
www.ix.de

EU-Regulierung für mehr Cybersicherheit

NIS2 erzwingt IT-Security

Wer betroffen ist • Was Sie tun müssen • Sonderfall IT-Branche
DORA: Cyberresilienz für den Finanzsektor

Beutezug durch Windows-Domänen
BloodHound CE durchleuchtet Active Directory und Entra ID

Coroot: Die Zukunft von Observability
eBPF erlaubt Überwachung ohne Instrumentierung

Fullstack-Frameworks fürs Web
Acht Pakete von Next.js bis Astro

Schutz vor SQL-Injections
Drei freie SQL-Firewalls im Test

PLUS: SBOMs für Cloud-Dienste
Rechtlicher Ärger mit KI-Codeassistenten
Perle IDS-108HP: PoE-Switch im Test
C# 12.0: Die wichtigen Neuerungen im Detail
Explorative Datenanalyse und -visualisierung mit LLMs

Zugriffskontrolle in Azure
Mit Role Engineering zu sicheren RBAC-Modellen

NIS2 – und jetzt?

Mit der Umsetzung von NIS2 in deutsches Recht wächst im Oktober die Anzahl der als kritisch eingestuften Unternehmen auf 30 000. Erstmals nimmt das Gesetz auch Unternehmen in der Lieferkette in die Pflicht. iX erklärt, was Unternehmen jetzt wissen müssen.

Von Ulrich Plate

Die Uhr läuft: Bis zum 17. Oktober 2024 muss der deutsche Gesetzgeber die europäischen Cybersicherheits- und Resilienzrichtlinien NIS2 (Network and Information Security) und CER (Critical Entities Resilience Directive) in den hiesigen Rechtsrahmen eingebunden haben. Seit Januar 2023 sind die beiden Richtlinien in der EU in Kraft, die sicherstellen sollen, dass als kritisch eingestufte Einrichtungen die Bevölkerung in den Mitgliedsstaaten mit lebenswichtigen Gütern und Diensten versorgen können. CER reguliert den physischen Schutz vor Sabotage und anderen Angriffen. Die Sicherheit der Informations- und Kommunikationstechnik ist Gegenstand der Richtlinie NIS2.

Der Anwendungsbereich beider Richtlinien umfasst insgesamt achtzehn Industriesektoren von Wasser bis Weltraum (Abbildung 1), an die sie umfassende Anforderungen an das Risikomanagement und die Cybersicherheit stellen. Will Deutschland kein Vertragsverletzungsverfahren mit der EU riskieren, müssen spätestens am Stichtag im Oktober Gesetze in Kraft treten, die die Richtlinien in nationales Recht umsetzen. Die Entwürfe für das KRITIS-Dachgesetz (KRITIS-DachG, siehe ix.de/z316) zur CER-Umsetzung und das etwas sperrig betitelte NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) befinden sich in unterschiedlichen Stadien des Gesetzgebungsverfahrens (siehe Kasten „Stand der Gesetzgebung“).

Bei potenziell Betroffenen der Regulierungsreform zur Cybersicherheit und Resilienz kritischer Einrichtungen haben die vorgestellten gesetzlichen Regelungen eine ähnliche Nervosität ausgelöst, wie sie zuletzt 2018 bei der Einführung der Datenschutz-Grundverordnung (DSGVO) zu beobachten war. Dabei ist es nicht ganz einfach, die eigene Betroffenheit überhaupt zu ermitteln. Viele Industrieverbände sind bereits dabei, ihren Mitgliedsunternehmen entsprechende Hilfestellungen beim Identifizieren der Rechtslage zu geben. Einige Beratungsunternehmen bieten interaktive NIS2-Checker, die anhand eines Fragenkatalogs abklopfen, ob Sektorzugehörigkeit und Charakter des Unternehmens den Schluss nahelegen, dass man dazugehören könnte. Schwierig zu beantworten ist die Frage aber auch für die Aufsichtsbehörden, die laut Richtlinie im April 2025 erstmals und dann alle zwei Jahre wieder die Anzahl der regulierten Einrichtungen nach Brüssel melden müssen.

Künftig werden nach Schätzungen des Statistischen Bundesamts zehnmal mehr Unternehmen als bisher gesetzlich zur Einhaltung der Vorschriften aus den Richtlinien verpflichtet sein. Bislang sind in Deutschland rund 800 Betreiber kritischer Infrastrukturen (KRITIS) mit etwa doppelt so vielen Anlagen beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registriert, dazu kommen noch etwa zwei- bis dreitausend „Unternehmen im besonderen öffentlichen Interesse“ (kurz UBI) vor allem aus dem Chemie- und Rüstungssektor. Diese sind auch bereits reguliert, jedoch nicht in derselben Tiefe und Härte wie die KRITIS. Der Grund für den Aufschrei in vielen Bran-

iX-TRACT

- Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) soll im Oktober in Kraft treten. Die Richtlinie stellt umfassende Anforderungen an das Risikomanagement und die Cybersicherheit von Unternehmen in 18 Sektoren.
- Die neue Richtlinie bringt drei fundamentale Neuerungen: Sie stuft mehr als doppelt so viele Sektoren als kritisch ein, verschärft den Bußgeldkatalog erheblich und nimmt Geschäftsleiter in die Verantwortung.
- In den Zielsektoren betroffen sind Unternehmen mit mehr als 50 Mitarbeitern oder 10 Millionen Euro Jahresumsatz. Besonderes im ITK-Bereich können aber auch schon kleinere Anbieter unter die Richtlinie fallen.
- Die Richtlinie verlangt Risikoanalysen, Risikomanagement und Maßnahmen zur Informationssicherheit, inklusive Krisenmanagement beim Sicherheitsvorfall. Die Orientierung an bestehenden Maßnahmen bereits regulierter Sektoren kann hier eine große Hilfe sein.

Achtzehn Sektoren fallen in den Geltungsbereich der Richtlinien CER und NIS2, da sie EU-Bürger mit lebenswichtigen Gütern und Diensten versorgen (Abb. 1).

chen und Verbänden: Nach der Umsetzung von NIS2 und CER in Deutschland erfasst die Regulierung rund 30 000 Einrichtungen.

Sinnvoll und unstrittig

Obwohl die Folgen für viele Unternehmen erheblichen finanziellen und organisatorischen Aufwand verursachen werden, formiert sich kein fundamentaler Widerstand gegen eine staatliche Verpflichtung zur Anwendung von Cybersicherheitsmaßnahmen. Das liegt zum Teil daran, dass die künftig Betroffenen angesichts der Bedrohungslage nicht undankbar sind, wenn ihnen gesetzliche Vorschriften Instrumente zum Absichern ihres Geschäfts an die Hand geben. Viele IT-Abteilungen dürften sich sogar darüber freuen, dass ihre Budgets im Interesse der Sicherheit üppiger ausfallen könnten: Die unternehmerische Entscheidung, in diesen Bereich zu investieren, fällt leichter, wenn man dazu verpflichtet ist.

Es geht dabei auch um gesellschaftliche Verantwortung, die von den meisten Institutionen im Prinzip nicht infrage gestellt wird. Grob vereinfacht: Auch wer nicht unmittelbar im öffentlichen Auftrag handelt, den kann der Staat zum Einhalten von Sicherheitsvorschriften in die Pflicht nehmen. Die Rechtsform der Institution spielt dabei keine Rolle. Für privatwirtschaftliche Unternehmen, kommunale Betriebe und auch Vereine oder Genossenschaften gilt: Sie sind dazu verpflichtet, eine unterbrechungsfreie Versorgung der Bevölkerung mit lebenswichtigen Gütern und Leistungen sicherzustellen. Dieser Anspruch auf Resilienz der Daseinsvorsorge ist aus dem Sozialstaatsprinzip des Grundgesetzes abgeleitet.

Für Ausflüchte gibt es hier wenig Spielraum. Auch nicht staatliche Einrichtungen müssen gesellschaftlich unentbehrliche Dienste ohne Unterbrechung aufrechterhalten. Das ist die Kehrseite des Privilegs, mit Versorgungsleistungen Geld verdienen zu können, die früher meist der öffentlichen Hand oblagen. Wasser- und Energieanbieter, Telekommunikationsnetzbetreiber oder Krankenhäuser sind seit vierzig Jahren schrittweise privatisiert worden, aber die sozialstaatliche Verpflichtung zum Aufrechterhalten kritischer Infrastrukturen ist noch dieselbe.

Die wichtigsten Neuerungen der NIS2

Drei fundamentale Änderungen kommen durch die NIS2 auf die Betroffenen zu: Erstens sollen künftig mehr als doppelt so viele Sektoren kritisch eingestuft sein, als bisher im Anwendungsbereich der Regulierung lagen. Zweitens werden Verstöße gegen die Vorgaben der NIS2 nach einem erheblich verschärften Bußgeldkatalog geahndet, der nach oben nur noch durch prozentuale Anteile vom weltweiten Jahresumsatz gedeckelt ist – ähnlich wie 2018 bei der Einführung der Datenschutz-Grundverordnung. Und drittens, vielleicht das schärfste Schwert: Die NIS2 führt eine Geschäftsleiterverantwortung ein. Chefs haften also künftig persönlich, wenn sie ihre Pflichten verletzen – inklusive Schadensersatzforderungen, die aus dem eigenen Vermögen zu leisten wären.

Auch die bisher schon bestehende Meldepflicht bei Sicherheitsvorfällen regelt das NIS2UmsuCG neu. Sie ist in Zukunft dreistufig: Bereits binnen 24 Stunden muss eine vorläufige Meldung erfolgen, wenn eine kritische Dienstleistung ausfällt – auch wenn noch keine präzise Kenntnis vorliegt, was genau passiert ist. Spätestens nach 72 Stunden erwarten die Aufsichtsbehörden eine qualifizierte Meldung über den Vorfall und seine Bekämpfung.

Kernstück der Reform ist aber zunächst eine völlige Neusortierung der Zielgruppe. Im bisherigen Verständnis kritischer Infrastrukturen war die Bestimmung ihrer Kritikalität in der KRITIS-Verordnung (KritisVO) geregelt. Ein dreistufiges Verfahren legt darin die Sektorenzugehörigkeit, bestimmte Anlagenkategorien und vor allem Schwellenwerte fest, deren Überschreitung einen Betreiber zu KRITIS im Sinne der Verordnung werden ließ. Virtueller Maßstab dieser Schwellenwerte ist bei allen Anlagen immer eine Zahl von 500 000 Menschen, die von einem Ausfall der kritischen Infrastruktur betroffen wären.

Stand der Gesetzgebung

Während bei der Umsetzung des gleichzeitig anstehenden KRITIS-Dachgesetzes neben der Ressortabstimmung bereits die Länder- und Verbändeanhörungen für den zweiten Referentenentwurf abgeschlossen sind, gibt es beim NIS2UmsuCG kaum Fortschritte. Ein erster Referentenentwurf kursierte inoffiziell bereits im Sommer 2023, das federführende Bundesministerium des Innern und für Heimat veröffentlichte jedoch keine offizielle Version. Um wenigstens etwas Transparenz zu schaffen, lud man im Herbst Verbände und Organisationen der Zivilgesellschaft ein, ein Diskussionspapier zu wirtschaftsrelevanten Aspekten des NIS2UmsuCG zu kommentieren (siehe ix.de/z316).

Über die Ursachen der Verzögerung lässt sich nur spekulieren. Möglich ist, dass die Ressortabstimmung auf erheblichen Widerstand einzelner Bundesministerien gestoßen ist. Im weiteren Verlauf wäre dann eine Anhörung der Länder sowie der Verbände und der Zivilgesellschaft der nächste Schritt – ob und wann es dazu kommen wird, ist derzeit unklar. Der Zeitplan, den Gesetzentwurf durchs Kabinett und das anschließende parlamentarische Verfahren zu bringen, ist mittlerweile äußerst eng – und eine Fristüberschreitung des Startdatums 18. Oktober 2024 nicht mehr unwahrscheinlich.

Dienste	große Unternehmen	mittlere Unternehmen	Kleinst- und Kleinunternehmen
DNS			
TLD-Registry			
qualifizierte Vertrauensdienste			
öffentliche Kommunikationsnetze/-dienste			
Internet Exchange Point			
Cloud-Computing-Dienste			
Rechenzentren			
Inhaltszustellnetze (CDN)			
nicht qualifizierte Vertrauensdienste			

Im ITK-Bereich weicht die Richtlinie von einer reinen Zuordnung nach Unternehmensgröße ab. Hier spielt besonders die Art des Dienstes eine Rolle für die Zuteilung: Orange sind „besonders wichtige Einrichtungen", hellblau „wichtige"; lila markierte sind nicht betroffen (Abb. 2).

Ähnlich wie Frankreich, wo man ebenfalls die bisherigen Einstufungen neben den neuen Kriterien beibehalten will, gibt auch Deutschland die Methodik der KritisVO nicht völlig auf. Wer bisher schon Betreiber einer kritischen Infrastruktur nach der KritisVO ist, bleibt dies auch nach der Reform. Um richtlinienkonform zu bleiben, müssen die Umsetzungsgesetze die neue Systematik der NIS2 und der CER in Deutschland einführen. Mit den umfangreichen Schwellenwertfestlegungen der KritisVO weist sie keine Ähnlichkeiten auf. Nach langem Hin und Her hatte man sich in den Verhandlungen zu den beiden EU-Richtlinien darauf verständigt, die Einstufung kritischer Einrichtungen europaweit nach Unternehmensgröße und Umsatzzahlen vorzunehmen.

Diese Unternehmen sind betroffen

Mit einigen Ausnahmen, aber in den allermeisten Fällen gilt künftig ein leicht zu merkendes Mengengerüst: Unternehmen aus einem der achtzehn Sektoren (siehe Abbildung 1) mit mehr als 50 Mitarbeitern oder 10 Millionen Euro Jahresumsatz sind „wichtige Einrichtungen", „important entities" in der EU-Richtlinie. Ab mehr als 250 Mitarbeitern oder 50 Millionen Euro Umsatz im Jahr fallen Unternehmen unter die wesentlichen Einrichtungen – so heißen die „essential entities" gemäß der offiziellen deutschen Übersetzung des EU-Sprachendienstes immerhin in Österreich, während das Bundesinnenministerium beschlossen hat, sie in Deutschland „besonders wichtige Einrichtungen" zu nennen.

Der Unterschied zwischen „wichtig" und „besonders wichtig" besteht vor allem darin, dass nur letztere Einrichtungen einer sogenannten Ex-ante-Regulierung unterliegen. Besonders wichtige Einrichtungen sind demnach – wie schon die bisherigen KRITIS-Betreiber – zum aktiven Nachweis des Einhaltens der Regeln verpflichtet. Für die wichtigen Einrichtungen gelten die Anforderungen der NIS2 ohne Abstriche auch, ohne jedoch einer regelmäßigen Nachweispflicht zu unterliegen. Bei einem Vorfall oder begründeten Verdacht können die Aufsichtsbehörden aber jederzeit Nachweise einfordern.

Von der einfachen „size cap rule", also dem Einteilen der kritischen Einrichtungen nach Unternehmensgröße, gibt es natürlich Ausnahmen. Die haben es in sich, insbesondere im ITK-Bereich: Für Einrichtungen wie Domain-Name-Services oder Vertrauensdienste mit qualifiziertem Signaturmanagement, die nach der NIS2 sozusagen als superkritisch gelten, spielt die Unternehmensgröße keine Rolle. Auch kleine oder Kleinstunternehmen, die solche Dienste anbieten, gelten als besonders wichtige Einrichtungen – mit allen Pflichten, die daraus resultieren. Auch deshalb lohnt es sich, die Betroffenheit des eigenen Unternehmens genau zu ermitteln.

Diese Maßnahmen verlangt die Richtlinie

Die europäische NIS2 enthält einen umfangreichen Katalog von Maßnahmen, die alle betroffenen Institutionen als Grundvoraussetzung umsetzen müssen. Diese zehn Punkte übernimmt das deutsche Umsetzungsgesetz vollständig. Die Maßnahmenliste bleibt relativ abstrakt (siehe Kasten „NIS2-Anforderungen"). Sie ent-

NIS2-Anforderungen

Die Richtlinie verlangt in Artikel 21 die Einhaltung von zehn Risikomanagementmaßnahmen im Bereich der Cybersicherheit:

- 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 das 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.

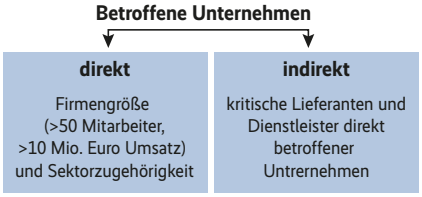
hält eher Kapitelüberschriften als konkrete Einzelanforderungen, aber das Ziel ist unmissverständlich: Maß aller Dinge ist ein funktionierendes Risikomanagement, aus dem betroffene Einrichtungen Sicherheitsvorkehrungen zum Eindämmen der Risiken ableiten. Gemäß beider Richtlinien, CER und NIS2, ist das systematische Management technischer und organisatorischer Risiken unabdingbare Voraussetzung, um im Sinne der Richtlinie rechtskonform zu handeln.

Die Richtlinie verlangt, dass Konzepte und Verfahren zu Risikoanalyse vorhanden sind und dass das Unternehmen bewerten kann, wie wirksam seine Maßnahmen des Risikomanagements und zur Stärkung der Informationssicherheit sind. Außerdem müssen Unternehmen konkrete Maßnahmen zur Bewältigung von Sicherheitsvorfällen und zur Aufrechterhaltung beziehungsweise Wiederherstellung des Betriebs nach einem Ausfall vorweisen, Krisenmanagement inklusive. Erstmals wird auch explizit die Sicherheit der Lieferkette einbezogen. Beschaffung, Entwicklung und Wartung von IT- und Netzwerktechnik sind ins Risikomanagement einzubeziehen. Das NIS2UmsuCG fordert außerdem Maßnahmen zur Cyberhygiene (kein Mehrfachverwenden von Passwörtern und Ähnliches) und Schulungen zur Cybersicherheit, Regeln für den Einsatz von Kryptografie, die Sicherheit des Personals, Zugriffskontrolle und Anlagenmanagement, Multi-Faktor- oder kontinuierliche Authentifizierung und gesicherte Kommunikation auch im Notfall. Die Grundlagen des Schwachstellenmanagements [1] und hilfreiche Werkzeuge [2] finden sich in iX 12/2023.

Mit anderen Worten: Wer im Geschäft bleiben möchte, kommt um das Umsetzen der Anforderungen nicht herum. Jenseits des bürokratischen Erfüllungsaufwands schätzt der inoffizielle Referentenentwurf des BMI die Kosten für die gesamte Privatwirtschaft auf über anderthalb Milliarden Euro jährlich. Das allerdings berücksichtigt nur die voraussichtlichen Aufwände bei den unmittelbar betroffenen Unternehmen: Weil das Risikomanagement eines nach der NIS2 regulierten Anbieters auch alle Dritten beurteilen muss, deren Leistungen oder Produkte für die kritischen Dienste unverzichtbar sind, müssen solche kritischen Lieferanten ebenfalls Cybersicherheitsmaßnahmen einführen oder verschärfen. Auch wenn eine seriöse Prognose kaum möglich ist: Die tatsächlichen Kosten der NIS2-Einführung werden jedenfalls weit über den Schätzungen des Ministeriums liegen.

Handlungsanweisungen für frisch Regulierte

Für diejenigen, die sich in der Vergangenheit auch ohne explizite Verpflichtung schon um die Sicherheit von IT- und Netzwerktechnik bemüht haben, steht in den künftig einzuhaltenden Anforderungen kaum radikal Neues. Der Maßnahmenkatalog nach NIS2 und die auch schon nach den bisherigen IT-Sicherheitsgesetzen üblichen Regeln des Informationssicherheitsmanagements sind vielen Unternehmen längst vertraut. Die Motivation für



NIS2 bezieht erstmals auch explizit die Sicherheit der Lieferkette ein. Unternehmen und Einrichtungen können also auch mittelbar betroffen sein und müssen dann ebenfalls die Sicherheitsanforderungen erfüllen (Abb. 3).

eine freiwillige Umsetzung ist jedoch nicht unbedingt bei allen dieselbe.

Es gibt Institutionen, die in Kenntnis der Sicherheitslage bereits für sich beschlossen haben, ihre Widerstandsfähigkeit gegen Cyberattacken zu verbessern – besonders die, die schon einmal Opfer von Angriffen waren. Wer darüber hinaus Sicherheitszertifizierungen nach BSI-IT-Grundschutz oder der nativen ISO 27001 vorgenommen hat, tat dies oftmals aber, um wichtige Kunden nicht zu verlieren. Insbesondere bei Ausschreibungen von Behörden und Verwaltungen kommen häufig nur noch Anbieter zum Zuge, die auch im Hinblick auf Cybersicherheit entsprechende Nachweise erbringen. Das Einhalten der Regeln des IT-Grundschutzes gehört bei öffentlichen Auftraggebern regelmäßig zu den Eignungskriterien für Bieter im Angebotsverfahren.

Die im Zuge von NIS2 erstmals oder als Lieferanten mittelbar betroffenen Unternehmen sind mit erheblichen Ansprüchen aus der Regulierung konfrontiert, um die Voraussetzungen für Informa-

tionssicherheit und Resilienz zu schaffen. Wer nicht ohnehin schon in der Vergangenheit seine Cybersicherheit auf den Stand der Technik gebracht hat, dessen IT-Architektur und Organisation stehen vor fundamentalen Änderungen. Auch wenn die Übergangsfristen relativ großzügig sind und mit Sanktionen überhaupt erst in drei Jahren zu rechnen ist, sollten diese Unternehmen die Einführung von Sicherheitsmaßnahmen nicht zu gemächlich angehen. Das Implementieren eines professionellen Informationssicherheitsmanagementsystems inklusive aller firmeninternen Richtlinien, Arbeitsanweisungen und technisch-organisatorischen Maßnahmen dauert selbst bei kleineren Firmen mindestens ein bis zwei Jahre. Kommt es in der Übergangszeit zu einem Sicherheitsvorfall, könnten die Behörden auch einen kritischen Blick auf die Umsetzungsbemühungen werfen.

Vorhandene Sicherheitskataloge und Standards nutzen

Die klassischen Anbieter kritischer Dienstleistungen treffen die gesetzlichen Rahmenbedingungen für Cybersicherheit nicht unvorbereitet. Die Betreiber, die bereits nach der bisherigen Rechtslage als KRITIS im Sinne der KritisVO galten, und insbesondere auf der Basis eigener Fachgesetze regulierte Branchen wie Kreditwesen oder Telekommunikation (TK) sind spätestens seit Einführung der ersten IT-Sicherheitsgesetze vor immerhin neun Jahren reguliert. Nicht alles ist dabei einheitlich geregelt, weil Sicherheitsanforderungen zum Beispiel zwischen TK- und Energienetzbetreibern stark voneinander abweichen können. Die Systematik ist ihnen jedoch vertraut: Die Unternehmen, die kritische Infrastrukturen betreiben, sind zur Einhaltung des „Stands der Technik“ bei der Sicherung ihrer IT-Systeme und Netzwerke verpflichtet. Diese Formulierung ist deckungsgleich mit den Kriterien, die der Gesetzgeber an die technisch-organisatorischen Maßnahmen des Datenschutzes anlegt.

Für die meisten Branchen existieren bereits konkrete Hinweise, welche Anforderungen umzusetzen sind. Hier können auch neu verpflichtete Unternehmen von den Grundlagen für die bisherigen KRITIS-Betreiber profitieren. Die Bundesnetzagentur etwa, als Aufsichtsbehörde unter anderem für Telekommunikations- und Stromnetzbetreiber, bietet eigene Sicherheitskataloge an, die mit einer Mischung aus internationalen Normen der ISO-27000-Familie und branchenspezifischen Einzelvorgaben für Informationssicherheit ein klar umrissenes Muster vorgeben. Auch die Art des Nachweises, ob und wie diese Vorgaben eingehalten werden, ist Teil der branchenspezifischen Pflichten. Für TK-Anbieter gilt, dass sie alle zwei Jahre ein Sicherheitskonzept bei der Bundesnetzagentur abgeben müssen, das das Einhalten der Anforderungen belegt und das von der Behörde geprüft wird. Die Energiewirtschaft muss ebenfalls regelmäßig berichten, aber die Prüfung ihrer Sicherheitsmaßnahmen erfolgt im Rahmen unabhängiger Zertifizierungen, die Unternehmen der Bundesnetzagentur nur noch nachweisen müssen.

Um die jetzt anstehenden Maßnahmen umzusetzen, muss also niemand das Rad neu erfinden. Die Cybersicherheitsanforderungen aus dem Kompendium der NIS2-Richtlinie sind leicht zu erfüllen, wenn man auf dem vorhandenen Maß an Informationssicherheit weiter aufbauen kann und ein umfassendes Risikomanagement betreibt. Für die künftig regulierten Unternehmen wird das sicher aufwendig, aber nicht dramatisch sein. Vielfach sollte genügen, sich an bisher schon verfolgten Best Practices und Normen zu orientieren und sie in eine Form zu bringen, die gegebenenfalls auch als Nachweis dienen kann, dass die Anforderungen erfüllt sind.

Welche Folgen die NIS2-Einführung für Unternehmen haben kann, die lediglich als Lieferanten tätig sind, also nicht direkt der Regulierung unterliegen, zeigt besonders deutlich der Finanzsektor. Banken und Versicherungen hatten schon immer besonders strenge Regeln, und die Vorschriften der „bankenaufsichtlichen Anforderungen an die Informationstechnik“ (BAIT) sind fester Bestandteil ihres Risikomanagements. Für Drittdienstleister kann das bedeuten, dass ein Auftraggeber ihre Cybersicherheit bewerten muss und das Ergebnis in den von Wirtschaftsprüfungsgesellschaften erstellten Jahresabschluss aufnimmt. Das heißt: IT-Dienstleister und andere Zulieferer müssen damit rechnen, Lieferantenaudits unterzogen zu werden, in denen die Robustheit ihrer Informationstechnik geprüft wird. De facto wird das bedeuten, dass in der Lieferkette dieselben Anforderungen zu erfüllen sind, die auch für die regulierten Auftraggeber gelten (siehe Abbildung 3).

Rechtssicherheit schrittweise verbessern

Abzuwarten ist, wie die KRITIS-Gepflogenheiten – zum Beispiel die alle zwei Jahre fälligen Berichte nach § 8a BSI-Gesetz – auch im neuen Rechtsrahmen beibehalten werden. Und auch wie die Nachweispflicht für die neuen besonders wichtigen Einrichtungen aussehen soll, ist noch nicht geklärt. Man wird sich Zeit lassen mit der Folgeverordnung zur KritisVO, vor 2026 ist nicht mit einer vollständigen Neubearbeitung zu rechnen. Bis dahin sind dann aber auch die Durchführungsrechtsakte erlassen, die die EU für einzelne Sektoren und Branchen noch nachliefern will.

Fest steht allerdings, dass die NIS2 in ihrer Umsetzung im deutschen Rechtsrahmen am 18. Oktober 2024 implementiert und scharf geschaltet sein muss. Mit den Mechanismen zum Durchsetzen der Aufsicht müssen die jeweiligen Behörden sich selbst erst vertraut machen – das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) wird nach KRITIS-Dachgesetz die Rolle einer übergeordneten Aufsichtsbehörde einnehmen, die es mit BSI und Bundesnetzagentur koordinieren muss.

Wenn NIS2 dann auch in Deutschland in Kraft tritt, dürfte die Richtlinie aber eigentlich schon niemanden mehr schrecken. Vor den sinnvollen Maßnahmen, die sie für verbindlich erklärt, muss jedenfalls niemand Angst haben: Vieles ist bereits betriebliche Praxis, anderes schnell nachzurüsten. Schließlich ist der Schutz des eigenen Unternehmens und seiner Informationssicherheit ein hohes Gut, das nicht nur für die von der Regulierung direkt Betroffenen von Bedeutung ist. (pst@ix.de)

Quellen

[1] Leonard Frank, Mirko Casper; Schwachstellenmanagement: mehr als Scannen und Finden; iX 12/2023, S. 50

[2] Leonard Frank, Mirko Casper; Werkzeuge für das Schwachstellenmanagement; iX 12/2023, S. 58

[3] Links zur NIS2-Richtlinine, der KritisVO, dem kommenden KRITIS-Dachgesetz und zum aktuellen Stand des NIS2UmsuCG finden sich unter ix.de/z316.

ULRICH PLATE

ist Berater für Informationssicherheit bei der nGENn GmbH und Leiter der Kompetenzgruppe Kritische Infrastruktur des Verbands der Internetwirtschaft eco e. V.