WHITE PAPER

EINFÜHRUNG UMFASSENDER ANFORDERUNGEN AN INFORMATIONS- UND CYBERSICHERHEIT FÜR WESENTLICHE ODER WICHTIGE UNTERNEHMEN IM EUROPÄISCHEN RAUM

NETWORK AND INFORMATION SECURITY DIRECTIVE 2 (NIS-2)

Die Überarbeitung der NIS-Direktive durch die Europäische Kommission und die Ausweitung des Anwendungsbereichs auf eine Vielzahl neuer Sektoren soll das Cybersicherheitsniveau für den gesamten europäischen Raum steigern und durch nationale Gesetze mit gemeinsamen Mindestanforderungen zusammenbringen. Für viele deutsche Unternehmen stellt dies die erste regulatorische Anforderung im Bereich Informationssicherheit dar.

Foto: iStock

protiviti®
Global Business Consulting

WHITE PAPER

EINFÜHRUNG UMFASSENDER ANFORDERUNGEN AN INFORMATIONS- UND CYBERSICHERHEIT FÜR WESENTLICHE ODER WICHTIGE UNTERNEHMEN IM EUROPÄISCHEN RAUM

NETWORK AND INFORMATION SECURITY DIRECTIVE 2 (NIS-2)

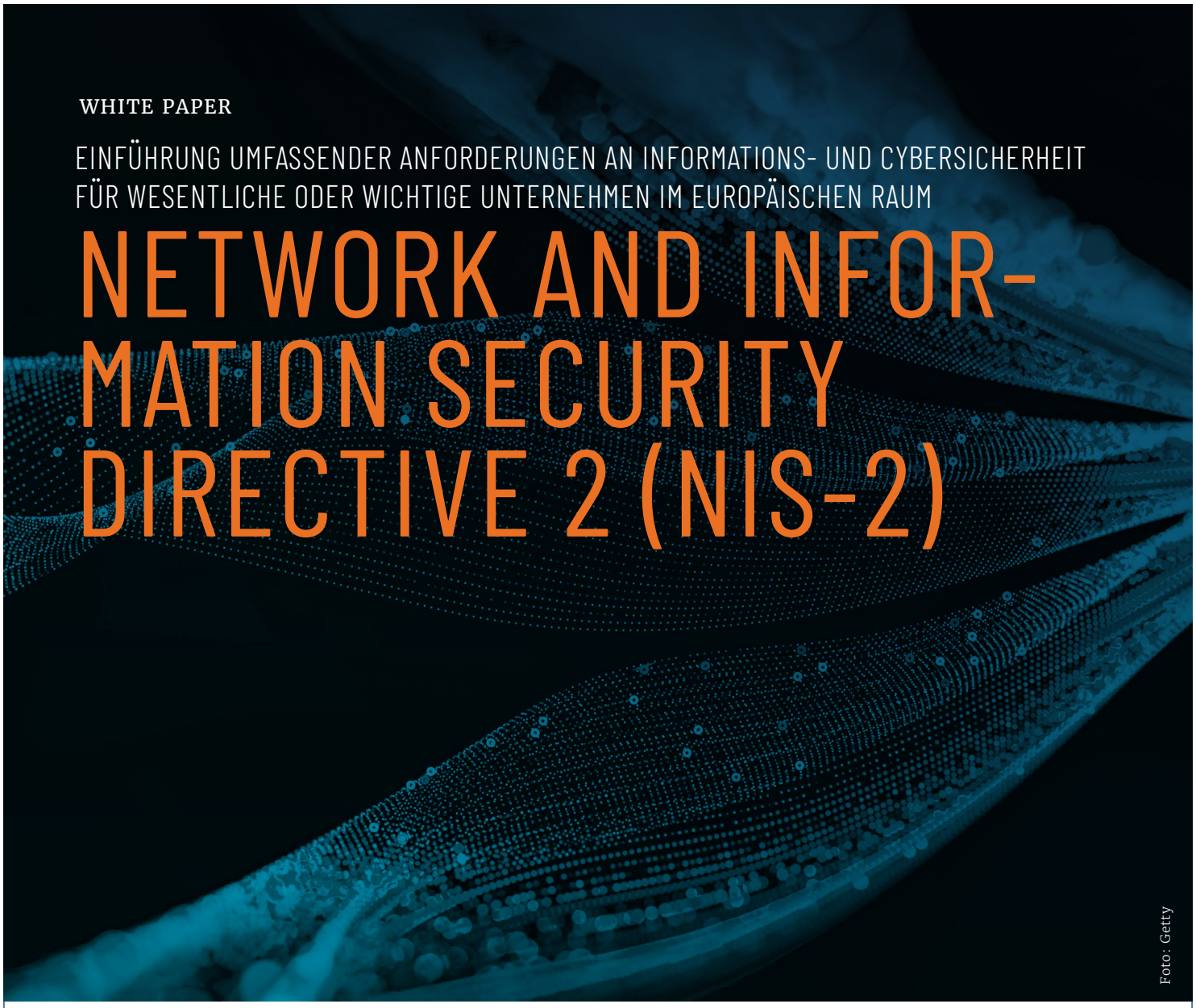


Foto: Getty

INHALTSVERZEICHNIS

EINLEITUNG

In ihrem Bestreben nach einem sicheren Europäischen Wirtschaftsraum ist die Europäische Kommission ermächtigt, regulatorische Vorgaben zu erlassen und die Mitgliedstaaten zur Umsetzung zu verpflichten. Diese Vorgaben sind häufig von neu entstandenen oder zunehmend auftretenden Bedrohungen motiviert, die als Gefahr für die Mitglieder der EU angesehen werden. Hierzu zählen insbesondere die über die letzten Jahre zunehmenden Angriffe auf die IT-Infrastruktur von Netz- und Informationssystemen. Die EU kategorisiert die Möglichkeit der Angriffe als „Cyberbedrohung" und definiert diesen Begriff als „einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte". Diese Cyberbedrohungen, welche weltweit entstehen und grenzübergreifend wirken können, sind durch eine zunehmend vernetzte Wirtschaft und Gesellschaft relevanter als je zuvor und die Tendenz für sich daraus ergebende Schäden dürfte mit zunehmender Digitalisierung noch weiter steigen.

Für die EU-Kommission sind Cyberbedrohungen kein neues Phänomen, sondern bereits seit Jahren ein ernstzunehmender Faktor, welcher negativen Einfluss auf die Stabilität der Wirtschaft haben kann. Bereits 2016 ist die „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" erschienen, welche aufgrund ihres Fokus auf Netz- und Informationssysteme auch als NIS-Richtlinie bekannt ist. Diese Richtlinie ist durch die EU-Kommission überarbeitet und Ende 2022 als „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)" veröffentlicht worden, wobei diese Direktive auch als NIS-2-Richtlinie abgekürzt wird. Ziel ist die Schaffung eines gesetzlichen Rahmens für ein einheitliches Mindestniveau in Bezug auf Cyberresilienz im EU-Raum. Obwohl der Inhalt der NIS-2-Richtlinie von den Mitgliedstaaten der EU bis zum 17. Oktober 2024 in nationales Gesetz überführt wird, sind in Deutschland bereits Zweifel aufgekommen, ob dieser Termin eingehalten werden kann.

> »Das unternehmensweite ISMS sollte zeitnah auf die NIS-2-Anforderungen geprüft und die Behebung von Lücken strukturiert geplant werden.«
>
> ANDREJ GREINDL,
> MANAGING DIRECTOR

Für Deutschland erfolgt die Überführung der NIS-2-Richtlinie in geltendes Recht durch das „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes" (NIS2UmsuCG). Als zuständige Aufsichtsbehörde für die Einhaltung der Vorgaben fungiert das Bundesamt für Sicherheit in der Informationstechnik (BSI), das bereits dieselbe Funktion bezüglich geltenden Rechts für Betreiber kritischer Infrastrukturen (KRITIS) innehat. Das NIS2UmsuCG ist dabei ein Änderungsgesetz, welches für viele Sektoren in Deutschland neu ist. Ein Gesetz mit Fokus auf Cyber- und Informationssicherheit in Deutschland, das derart viele Unternehmen in unterschiedlichen Bereichen betrifft, existierte bisher nicht. Insbesondere für bisher nicht oder geringfügig regulierte Unternehmen stellt der Weg

»Ein Gesetz mit Fokus auf Cyber- und Informationssicherheit in Deutschland, welches derart viele Unternehmen in unterschiedlichen Bereichen betrifft, existierte bisher nicht.«

CHRISTOPHER CHASSÉE,
DIRECTOR

zur NIS-2-Compliance eine Herausforderung dar, da neben einer Eigenmotivation zur Umsetzung von Maßnahmen im Bereich Sicherheit in der Informationstechnik nun auch die Besonderheiten von regulatorischen Anforderungen zu berücksichtigen sind. Wer genau von NIS-2 betroffen ist, wird dabei durch die Kriterien des NIS2UmsuCG definiert. Im Folgenden konzentriert sich das Whitepaper hauptsächlich darauf, die von NIS-2 betroffenen Unternehmen zu identifizieren, die Kerninhalte und -anforderungen von NIS-2 zu erläutern, den daraus resultierenden Handlungsbedarf sowie empfohlene Maßnahmen aufzuzeigen.

BETROFFENE UNTERNEHMEN & EINTEILUNG IN SEKTOREN

Die Anforderungen nach NIS-2 sind nicht für jedes Unternehmen in Deutschland verbindlich, sondern nur für Unternehmen, die für die Wirtschaft oder das Allgemeinwohl einen relevanten Beitrag leisten. Dazu sind im NIS2UmsuCG klare Kriterien definiert, wann ein Unternehmen unter NIS-2 als relevant erachtet wird. Im Wesentlichen existieren zwei unterschiedliche Arten von Unternehmen, die zur Einhaltung des NIS2UmsuCG verpflichtet sind: „besonders wichtige“ Einrichtungen (im Englischen: Essential Entities), zu denen auch KRITIS-Betreiber gehören, und „wichtige“ Einrichtungen (im Englischen: Important Entities).
Eine Einrichtung zählt zu den „besonders wichtigen“ Einrichtungen, wenn mindestens eines der folgenden Kriterien zutrifft (davon ausgenommen sind Einrichtungen der Bundesverwaltung, insofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind):

1. Betreiber kritischer Anlagen.
2. Es handelt sich bei der Einrichtung um einen qualifizierten Vertrauensdienstanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter.
3. Es handelt sich um Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder öffentlicher Telekommunikationsnetzen, die entweder mindestens 50 Mitarbeiter beschäftigen oder deren Jahresumsatz und Jahresbilanzsumme jeweils über 10 Millionen Euro betragen.
4. Es werden Dienstleistungen oder Waren entgeltlich angeboten und das Unternehmen ist in einem laut NIS2UmsuCG besonders wichtigen Sektor angesiedelt (die Sektoren sind in Grafik 1 dargestellt). Eine Organisation muss zudem entweder mindestens 250 Mitarbeiter beschäftigen oder einen Jahresumsatz von über 50 Millionen Euro sowie eine Bilanzsumme von über 43 Millionen Euro erzielen.

Eine Einrichtung zählt hingegen zu den „wichtigen“ Einrichtungen, wenn keines der Kriterien für „besonders wichtige“ Einrichtung, jedoch mindestens einer der folgenden Punkte, zutrifft (davon ausgenommen sind Einrichtungen der Bundesverwaltung):

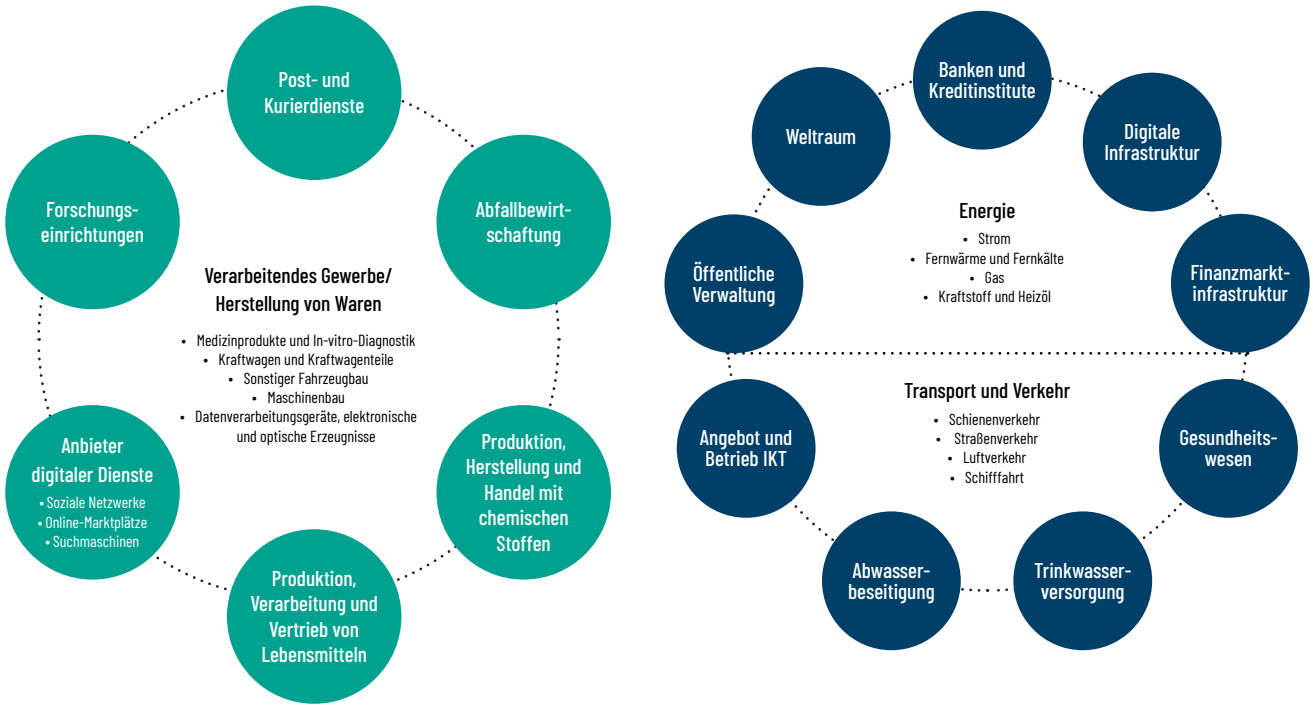
1 Das Unternehmen ist ein Vertrauensdienste-anbieter.

2 Es handelt sich um Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder öffentlicher Telekommunikationsnetze, die entweder weniger als 50 Mitarbeiter beschäftigen oder deren Jahresumsatz und Jahresbilanzsumme jeweils 10 Millionen Euro oder weniger betragen.

3 Es werden Dienstleistungen oder Waren entgeltlich angeboten und das Unternehmen ist in einem laut NIS2UmsuCG wichtigen Sektor angesiedelt (die Sektoren sind in Grafik 1 dargestellt). Zusätzlich muss eine Organisation entweder eine Mitarbeiterzahl von mindestens 50 Personen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.

Unbeachtet der Merkmale gilt NIS-2 auch für alle durch VAG und KWG regulierten Unternehmen – also alle Finanzdienstleister. Dabei sind die NIS-2-Anforderungen als zusätzliche Vorgaben anzusehen, die jedoch nur geringfügig von den bereits umfangreichen regulatorischen Anforderungen der BaFin oder anderer Aufsichtsbehörden abweichen.
Eine Neuerung durch das NIS2UmsuCG ist die Etablierung von Sektoren, anhand derer die Bedeutung der jeweiligen Unternehmen für das Allgemeinwohl, und entsprechend das Ausmaß an regulatorischen Anforderungen an die betroffenen Unternehmen, festgelegt wird. Dieser Ansatz ist der gesetzlichen Grundlage für KRITIS-Betreiber entliehen und wird für NIS-2 erweitert. Mit der Erweiterung gibt es insgesamt 18 Sektoren, von denen elf (11) Sektoren als „besonders wichtig“ und sieben (7) Sektoren als „wichtig“ eingestuft werden. Die Sektoren unterteilen sich wie in der nachfolgenden Grafik 1 dargestellt:

Grafik 1: Sektorenübersicht in NIS-2



	Mitarbeiter	Umsatz	Bilanz	Organisation
Mittel	50 - 249	10 - 50 Mio. EUR &	< 43 Mio. EUR	W
Groß	≥ 250	≥ 50 Mio. EUR &	≥ 43 Mio. EUR	B oder W

»Eine Fokussierung auf die eigene Cyber- und Informationssicherheit, ohne Einbeziehung der Lieferkette des Unternehmens, kann der aktuellen Risikolage nicht mehr gerecht werden.«

CARSTEN SCHMELZEKOPF, MANAGER

Staatliche Institutionen der Bundesverwaltung und staatsnahe Einrichtungen, solange sie keine kritischen Anlagen betreiben, insbesondere aber das Auswärtige Amt, das Bundesministerium für Verteidigung sowie der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz werden vom NIS2UmsuCG ausgenommen. Welche organisatorischen und technischen Maßnahmen genau von den betroffenen Unternehmen gefordert werden wird, ist aufgrund des Entwurfsstatus des Gesetzes in Deutschland noch nicht vollständig gesichert. Durch Parallelen in anderen Gesetzgebungen und der bereits bekannten Anforderung, ein effektives Informationssicherheitsmanagementsystem (ISMS) zu betreiben, ist jedoch weitgehend absehbar, welche Anforderungen auf Unternehmen zukommen werden. Insbesondere die bisher nicht regulierten Unternehmen können sich zunächst am „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)“ und der zugehörigen „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ orientieren. Diese beinhalten die Anforderungen für KRITIS-Betreiber, welche voraussichtlich umfangreicher sind als die Maßnahmen, die sowohl durch „besonders wichtige“ als auch „wichtige“ Einrichtungen unter NIS2UmsuCG umzusetzen sind. Dennoch ist zu erwarten, dass die Anforderungen weitestgehend analog sein werden, da NIS-2 sowohl als eine Erweiterung von KRITIS-Betreibern auf weitere Bereiche mit Bedeutung für das Allgemeinwohl und die Wirtschaft agiert, als auch durch dieselbe Behörde, das BSI, überwacht wird. Sollten nicht regulierte Unternehmen bisher noch kein ISMS betreiben, ist die Einführung eines ISMS aus Selbstschutz nun nicht mehr nur sinnvoll, sondern aufgrund der regulatorischen Anforderung durch NIS-2 zwingend erforderlich. Bereits regulierte Unternehmen, etwa Finanzdienstleister, werden ihre Prozesse zum Umgang mit Cyberbedrohungen nach NIS-2 anpassen müssen, operieren aber bereits auf einer guten Grundlage. KRITIS-Betreiber hingegen können mit dem geringsten Anpassungsbedarf an ihren bisherigen Prozessen mit Bezug auf Cyberresilienz rechnen, wie zum Beispiel der Meldung des erstmaligen Einsatzes kritischer Komponenten an das Bundesministerium des Inneren und für Heimat.

(NEUE) ANFORDERUNGEN AN UNTERNEHMEN

Der Schutz vor Schäden aus Cyberbedrohungen sollte Unternehmen bereits vor NIS-2 ein Anliegen gewesen sein, da Reputationsverlust und monetäre Einbußen durch Cyberangriffe in der Vergangenheit stetig gewachsen sind. So belief sich bereits Ende 2020 der Verlust für die Weltwirtschaft durch Cyberangriffe auf fast 5,5 Billionen Euro. Durch das NIS2UmsuCG werden nun neue und umfangreichere regulatorische Anforderungen zur Bekämpfung von Cyberbedrohung in Deutschland geschaffen. Die Anforderungen fokussieren sich dabei für betroffene Unternehmen auf geeignete, verhältnismäßige und wirksam technische und organisatorische Risikomanagementmaßnahmen zum Schutz der Verfügbarkeit, Integrität und

Vertraulichkeit der informationstechnischen Systeme, Komponenten sowie Prozesse. Analog zu den Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) gilt das Proportionalitätsprinzip. Dies bedeutet, dass die Maßnahmen im Verhältnis zu den geschützten Werten stehen sollen. Das gilt sowohl bei der Konzeptionierung der Maßnahmen (besonders schützenswerte Daten erfordern den Einsatz von fortgeschritteneren Sicherheitstechnologien und -mechanismen im Vergleich zu Daten, die als unkritisch eingestuft werden), als auch bei der Finanzierung (z. B. müssen keine Millionenbeträge investiert werden, wenn ein möglicher Schaden keine tausend Euro betragen würde).
Das nach NIS2UmsuCG geforderte Risikomanagement gegen Cyberbedrohungen konkretisiert dabei zehn Mindestanforderungen, die durch jede betroffene Einrichtung zu erfüllen und zu dokumentieren sind:

1 Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationstechnik;

2 Bewältigung von Sicherheitsvorfällen;

3 Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

4 Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

5 Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen einschließlich Management und Offenlegung von Schwachstellen;

6 Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik;

7 grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik;

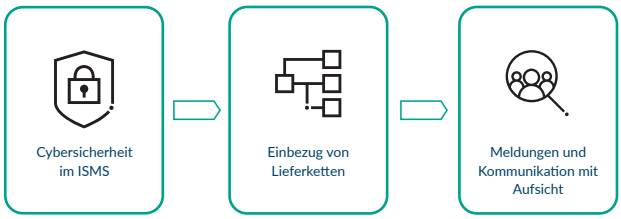
8 Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung;

9 Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

10 Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Diese Mindestanforderungen sowie die weiteren Vorgaben zu NIS-2 können in drei Primärbereiche unterteilt werden, auf die sich Unternehmen zunächst konzentrieren sollten. Diese Primärbereiche sind ein funktionsfähiges ISMS mit Abdeckung der Sicherheit in der Informationstechnik, die Steuerung von Risiken bei Dienstleistern durch Einbezug der Lieferkette in die Informationssicherheit und die Meldefähigkeit an die Aufsichtsbehörden zur Kommunikation von Sicherheitsvorfällen.

Grafik 2: Primärbereiche NIS-2



Anforderung 1: Cybersicherheit im ISMS

Ein ISMS ist ein systematischer und kontinuierlicher Managementansatz zum Schutz der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Informationswerten durch Methoden, Prozessen, Maßnahmen und Richtlinien. Als Teil der Informationssicherheit muss auch die Sicherheit in der Informationstechnik in einem ISMS sichergestellt sein, wobei durch NIS-2 der Umgang mit Cyberbedrohungen und die Stärkung von Cyberresilienz einen höheren Stellenwert einnimmt als es bisher in der regulatorischen Landschaft der Fall war. Gerade die Sicherheit von Netzsystemen und die operative Informationssicherheit sind häufig nicht auf einem ausreichenden Stand, entweder aufgrund fehlender qualifizierter Personen im Unternehmen für diese Aufgaben oder der fehlerhaften Risikoeinschätzung und damit einhergehender Vernachlässigung dieser Aspekte.
Um den NIS-2-Anforderungen nachzukommen, müssen „besonders wichtige“ und „wichtige“

Einrichtungen im Rahmen ihres Risikomanagements Risikoanalysen und -bewertungen für ihren Geltungsbereich durchführen. Aus den Ergebnissen sind technische und organisatorische Maßnahmen abzuleiten, die die potenziellen Bedrohungen und Schwachstellen adressieren, sodass potenzielle Schäden möglichst gering ausfallen oder vollständig vermieden werden. Zu solchen Maßnahmen gehören beispielsweise die Einführung von Zugriffskontrollen, Verschlüsselungstechnologien, Incident-Response-Verfahren und regelmäßige Schulung für Mitarbeiter zur Steigerung der Awareness im Bereich Sicherheit in der Informationstechnik. Hiervon ist auch die Geschäftsleitung betroffen, da deren Einbindung in Form von Billigung, Überwachung und regelmäßiger Teilnahme an Schulungen zu Risikomanagementpraktiken für Cybersicherheit durch das NIS2UmsuCG explizit gefordert ist.

Cybersicherheit und operative Informationssicherheit im Rahmen eines ISMS sind stark auf technische Maßnahmen fokussiert, da Schwachstellen und externe Bedrohungen direkt die IT-Infrastruktur betreffen. Die eingesetzten Sicherheitstechnologien müssen dem Stand der Technik angemessen und auf Bedrohungen abgestimmt sein, dürfen aber nicht die spezifischen Unternehmenseigenschaften außer Acht lassen. So kann je nach Unternehmensgröße und Anzahl an Cyberangriffen die Einrichtung eines Security Operation Centers unabdingbar sein, während Kleinstunternehmen dies durch interne Prozesse und Fachwissen in verringertem Umfang bewältigen können.

Unerlässlich bleiben jedoch die sichere Verwaltung und Konfiguration von Netzwerken, sowohl bei externen Schnittstellen als auch bei ausschließlich internen Bereichen. Die Segmentierung und Zonierung des Netzwerks, die Härtung von IT-Systemen, Verschlüsselungsverfahren für Daten im Ruhezustand (data at rest), in der Verarbeitung (data in processing) sowie im Transport (data in transit), der Einsatz von Virenschutzprogrammen, Firewalls sowie Anti-Schadsoftware und regelbasierte Prüfungen von Dateien im Netzwerk sind ein zu erbringendes Mindestmaß für den Umgang mit Cyberbedrohungen. Zudem muss die Effektivität der Maßnahmen durch regelmäßige Schwachstellenscans, Penetrationstests und der Simulation von Angriffen kontrolliert und im Unternehmenskontext im Rahmen des Business Continuity Management als wesentlicher Punkt berücksichtigt werden. Das Business Continuity Management ist dabei nicht nur als Teil des eigenen Unternehmens zu verstehen, sondern betrifft ebenso geschäftskritische Dienstleister und Lieferanten, die dieses ebenfalls beachten oder umsetzen müssen.

Anforderung 2: Einbezug von Lieferketten

NIS-2 trägt der zunehmenden Vernetzung und Zusammenarbeit von Unternehmen Rechnung, sowohl innerhalb eines Landes als auch grenzübergreifend. Bei der Herstellung eines Produktes oder der Erbringung einer Dienstleistung ist nur noch in seltenen Fällen ein einziges Unternehmen involviert. Stattdessen fokussieren sich Unternehmen auf die Ausführung ihrer Kernprozesse, lagern Hilfsprozesse aus und beziehen Teilprodukte und Hilfsdienstleistungen von Zulieferern und Dienstleistern. Für „besonders wichtige“ und „wichtige“ Einrichtungen bedeutet dies, dass auch ihre Lieferkette abgesichert sein muss. Ein nach NIS-2 reguliertes Unternehmen muss bei der Planung und Umsetzung von Maßnahmen zur Sicherheit in der Informationstechnik auch Cyberangriffe auf seine Zulieferer berücksichtigen, wenn durch deren Ausfall die eigenen Betriebsabläufe beeinträchtigt oder sogar zum Stillstand gebracht werden können. Die Cybersicherheitspraktiken müssen gestärkt und die Risiken in der Lieferkette aktiv gesteuert werden.

Im Dienstleistungssteuerungsprozess muss bereits bei der Auswahl neuer Dienstleister darauf geachtet werden, dass potenzielle Lieferanten ein Bewusstsein für Cyberbedrohungen besitzen und Risiken im Kontext der Informationssicherheit proaktiv behandeln. Ein Indikator dafür kann zum Beispiel eine Zertifizierung der Cyber- und IT-Sicherheit sein, die nach Inkrafttreten des NIS2UmsuCG durch das BSI ausgestellt werden kann. Auch bereits etablierte Zertifikate nach Informationssicherheitsrahmenwerken wie ISO 27001 oder BSI IT-Grundschutz können als Indikatoren in der Dienstleisterauswahl genutzt werden.

Neue sowie bestehende Verträge sollten durch das dienstleistungsbeziehende Unternehmen hinsichtlich Maßnahmen zur Sicherheit in der Informationstechnik, Risikomanagement und Behandlung von Sicherheitsvorfällen geprüft werden. Nur vertraglich vereinbarte Anforderungen sind durch Lieferanten zu erbringen und können dementsprechend im Risikomanagement zuverlässig berücksichtigt werden. Darüber hinaus sollten die vertraglichen Regelungen bezüglich Cybersicherheit in regelmäßigen Abständen und anlassbezogen auditiert werden, weswegen die Vereinbarung eines Auditrechts unerlässlich ist.

Je nach Größe, Auditaufwand und Marktmacht des Lieferanten kann eine Prüfung eigenständig erfolgen, durch einen weiteren Dienstleister oder mit anderen Unternehmen zusammen in einer Prüfgemeinschaft.
Abgesehen von Kontrollen und Nachweisen ist auch ein gemeinschaftlicher Sicherheitsprozess zwischen Unternehmen und Lieferanten zielführend, etwa in Form eines gemeinsamen ISMS oder der Einbindung von Lieferanten in einen bestehenden Sicherheitsprozess. Ein abgestimmter Prozess, welcher auch in regelmäßigen Abständen verprobt wird, hilft bei der effektiven Bewältigung von Cyberbedrohungen. Ein solcher Prozess muss zudem sicherstellen, dass Sicherheitsvorfälle bei Lieferanten unverzüglich nach Eintreten weitergeleitet werden, damit die Meldepflichten bezüglich erheblicher Sicherheitsvorfälle gemäß NIS2UmsuCG durch die Einrichtungen eingehalten werden können.

Anforderung 3: Meldungen und Kommunikation mit Aufsicht

Neben den Anforderungen, welche bei „besonders wichtigen“ und „wichtigen“ Einrichtungen intern oder gemeinsam mit Lieferanten umgesetzt werden müssen, gibt es durch NIS-2 auch die Verpflichtung zur Meldung von erheblichen Sicherheitsvorfällen an das BSI sowie die Kommunikation von generellen Informationen gemäß NIS2UmsuCG, wie beispielsweise Registrierungsdaten. Zu den Registrierungsdaten gehören etwa die Betroffenheit eines Unternehmens von NIS-2 inklusive des Namens der Einrichtung, der Rechtsform, Anschrift und Kontaktdaten mit öffentlichem IP-Adressbereich, den zutreffenden NIS-2-Sektoren und einer Auflistung der Mitgliedstaaten in der EU, in denen das Unternehmen tätig ist sowie die für die Tätigkeit zuständige Aufsichtsbehörde des Bundes und der Länder. Anhand dieser Registrierungsdaten führt das BSI ein Verzeichnis der NIS-2 relevanten Unternehmen, welches auch der Agentur der Europäischen Union für Cybersicherheit (ENISA) zur Verfügung gestellt wird.
Die Implementierung eines effektiven Berichtswesens stellt gleichfalls eine wesentliche Komponente dar. Für die Berichterstattung von Sicherheitsvorfällen gelten spezifische Fristen, etwa die Erstmeldung innerhalb von 24 Stunden nach Kenntnisnahme eines erheblichen Vorfalls, innerhalb von 72 Stunden die Bereitstellung einer detaillierten Bewertung des erheblichen Vorfalls sowie innerhalb eines Monats entweder die Meldung der abgeschlossenen Behandlung oder eine Fortschrittsmeldung mit aktuellem Status. Dazu müssen Mechanismen etabliert werden, die eine schnelle und genaue Erfassung sowie Meldung von Sicherheitsvorfällen gewährleisten. Dies erfordert nicht nur die Schaffung geeigneter interner sowie externe Kommunikationskanäle, sondern auch die Entwicklung eines zuverlässigen unternehmensinternen Systems zur Dokumentation, Analyse und Klassifikation von sicherheitsrelevanten Ereignissen und Sicherheitsvorfällen.
Die Meldung von Sicherheitsvorfällen ist jedoch kein einseitiges Unterfangen, da das BSI auch um Unterstützung bei der Behebung eines Sicherheitsvorfalls gebeten werden kann. Die Unterstützung kann dabei durch direkte Beratung, Empfehlung von Anlaufstellen oder einer situationsgemäßen Lösung erfolgen. Auch neben der Meldung von Sicherheitsvorfällen ist es allgemein ratsam, frühzeitig und kontinuierlich Kontakt mit dem BSI aufzunehmen und eine positive Beziehung zu pflegen. Neben dem direkten Austausch sind auch die Onlineplattform des BSI sowie die Informationen durch die ENISA hilfreiche Informationsquellen bei der Verbesserung der Unternehmensprozesse in den Bereichen Informationssicherheit und Cyberresilienz.

FAZIT: HANDLUNGSBEDARF FÜR BISHER NICHT REGULIERTE UNTERNEHMEN

Die Anforderungen von NIS-2, sowohl in den Primärbereichen als auch in anderen Bereichen, sind nicht einzeln, sondern als ineinandergreifende Pflichten zu betrachten, die das Niveau der Informations- und Cybersicherheit in der EU auf ein gutes Ausgangsmaß steigern sollen. Ein effektives ISMS ist unabhängig von regulatorischen Anforderungen zu konzipieren und stellt den Schutz der Unternehmensinformationen in den Mittelpunkt. Ein NIS-2-konformes ISMS erfüllt zudem spezifische Anforderungen, welche durch das NIS2UmsuCG gefordert werden, aber im ISMS eines unregulierten Unternehmens nicht zwingend vorkommen würden. Bisher nicht regulierte Unternehmen, welche nur ein rudimentäres oder gar kein ISMS besitzen, stehen daher neben der Herausforderung, in kürzester Zeit ein ISMS aufzubauen, auch vor der Problematik, die Besonderheiten von NIS-2 zu adressieren.
Die Anpassung des bereits bestehenden ISMS

eines Unternehmens hinsichtlich der Neuerungen ist zeitnah umzusetzen, da es keine Übergangsfrist des Gesetzes gibt, sodass bei Inkrafttreten des NIS2UmsuCG im Oktober 2024 keine Lücken bestehen dürfen oder andernfalls die Nichteinhaltung zu Bußgeldern führt. So drohen bei Nichterfüllung empfindliche Strafen mit persönlicher Haftung: für „wichtige“ Einrichtungen bis zu 7 Millionen Euro oder 1,4 % ab einem Jahresumsatz von 500 Mio. € sonst 7 Mio. € Strafe, bei „besonders wichtigen“ Einrichtungen sogar 2 % ab einem Jahresumsatz von 500 Mio. € sonst 10 Mio. € Strafe. Diese Strafen sollen das Bewusstsein für Cybersicherheit bei Entscheidungsträgern und verantwortlichen Personen in Unternehmen weiter stärken.

Neben der Stärkung des Bewusstseins von Unternehmen für Sicherheit in der Informationstechnik werden die Befugnisse der Aufsichtsbehörden erheblich ausgeweitet. Dazu gehören die Berechtigung für Inspektionen vor Ort, regelmäßige Sicherheitsaudits, Ad-hoc-Überprüfungen im Ernstfall und Durchführung von Sicherheitsscans sowie die Ausweitung von Strafen für Unternehmen außerhalb der nationalen Grenzen, in Kooperation mit anderen nationalen Aufsichten. Dies hat die ständige Überwachung und Anpassung der Sicherheitsmaßnahmen auf Seiten der Unternehmen zur Folge, um mit den sich permanent ändernden Bedrohungen und regulatorischen Anforderungen Schritt zu halten. Auch hier ist ein proaktives Handeln und der Aufbau einer guten Beziehung zum BSI, als deutscher Aufsichtsbehörde für NIS-2, und das Monitoring von Informationen der ENISA sowie anderen Interessensverbänden für Sicherheit in der Informationstechnik ratsam. Für Unternehmen, welche bisher noch keinen Kontakt zum BSI oder anderen Instituten für Informationssicherheit hatten, sollte die Auseinandersetzung mit dem Thema und dem Aufbau eines Kommunikationskanals als Teil ihres ISMS eine hohe Priorität einnehmen.

UNSERE EMPFEHLUNG FÜR DEN UMGANG MIT NIS-2 (BIS KONKRETISIERUNG)

Neben dem aufgezeigten Handlungsbedarf empfehlen wir Ihnen folgenden generalistischen Handlungsansatz zum Umgang mit dem bevorstehenden Inkrafttreten des NIS2UmsuCG, damit Ihr Unternehmen für NIS-2 vorbereitet ist und Sie auf einem guten Weg zur Stärkung Ihrer Sicherheit in der Informationstechnik sind:

1 **Prüfung NIS-2-Betroffenheit mit zugehöriger Kategorisierung**
NIS-2-Compliance beginnt mit der Bestimmung, ob Ihr Unternehmen in einem der dafür relevanten Sektoren arbeitet und die erforderliche Anzahl an Mitarbeitenden oder die Höhe des Jahresumsatzes plus Jahresbilanz aufweist, KRITIS-Betreiber ist oder aufgrund eines anderen Kriteriums als „besonders wichtige“ oder „wichtige“ Einrichtung gilt. Ist dies der Fall, ist NIS-2 für Sie relevant und es gilt die Anforderungen einzuhalten, allen voran die Meldung Ihrer Betroffenheit ab Oktober 2024 an das BSI.

2 **Ableitung der unternehmensspezifischen Anforderungen**
Aufbauend auf dem Ergebnis aus Schritt eins sind Ihre unternehmensspezifischen Anforderungen abzuleiten. Dazu gehört in erster Linie die Risikomanagementmaßnahmen für den Umgang mit Cyberbedrohungen für Netz- und Informationssysteme, welche in ihrem Umfang und Komplexität je nach unternehmenseigenen Bedingungen variieren können. Nicht variabel hingegen sind die zehn Mindestanforderungen, welche durch technische und organisatorische Maßnahmen zum Schutz der Unternehmensinformationen zwingend erfüllt werden müssen.

3 **Durchführung NIS-2-GAP-Assessment**
Anhand der für Sie zutreffenden Anforderungen empfehlen wir die Durchführung eines GAP-Assessments für Ihr Unternehmen, welches Ihre Kontrollframework mit den Anforderungen aus dem NIS2UmsuCG vergleicht. Unternehmen, die bereits reguliert sind und innerhalb eines gefestigten ISMS agieren, können sich auf die Neuerungen konzentrieren, die sich durch NIS-2 ergeben. Ziel des NIS-2-Gap-Assessments ist die Identifizierung von Lücken, damit diese entlang des Risikomanagementprozesses in Ihrem Unternehmen bewertet und angegangen werden können.

4 **Aufbau oder Anpassung des ISMS für NIS-2 durch kontinuierliche Verbesserung**
Die zuvor identifizierten Lücken sind als Teil des kontinuierlichen Verbesserungsprozesses Ihres ISMS zu schließen. Besteht noch kein ausgereiftes ISMS, muss der Aufbau dessen schnellstmöglich gestartet werden. Sowohl im Rahmen des kontinuierlichen Verbesserungsprozesses als auch beim Aufbau eines ISMS sollte der Fokus zunächst auf die drei Primärbereiche (Cybersicherheit im ISMS, Einbezug der Lieferkette in das Risikomanagement, Aufbau eines Meldeprozesses an und die Kommunikation mit der deutschen Aufsichtsbehörde BSI) gelegt werden.

5 **Monitoring von Änderungen am NIS2UmsuCG und Onlineplattformen der Aufsichtsbehörden**
Gesetze und Anforderungen ändern sich im Laufe der Zeit. NIS-2 selbst ist, als Erweiterung der NIS-Direktive von 2016, hierfür ein Beispiel. In einem fortlaufenden Prozess sollten Sie weitere Anpassungen im Bereich NIS-2 monitoren, damit Sie keine Änderungen verpassen oder in Verzug geraten. Neben dem Monitoring von Neuerungen am NIS2UmsuCG empfehlen wir sowohl das regelmäßige Besuchen der Onlineplattformen des BSI als auch der ENISA, damit Sie auf dem aktuellen Stand in Bezug auf Informations- und Cybersicherheit bleiben.

KONTAKT

ANDREJ GREINDL
Managing Director
+49 172 698 30 53
andrej.greindl@protiviti.de

CHRISTOPHER CHASSÉE
Director
+49 172 621 73 01
christopher.chassee@protiviti.de

CARSTEN SCHMELZEKOPF
Manager
+49 6996 376 81 96
carsten.schmelzekopf@protiviti.de

www.protiviti.de

© 2024 PROTIVITI GMBH

QUELLEN

[1] *Art. 2 Nr. 8 – gem. VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).*

[2] *Vgl. EU Agency y for Cybersecurity (data from July 2021 to July 2022): Infografik „Top Cyber Threats in the EU". Online verfügbar unter: Top Cyber Threats in the EU - Consilium (europa.eu).*