General Report

Praxisleitfaden zur Umsetzung von NIS2

Prof. Dr. Dennis-Kenji Kipker

November 2023

Praxisleitfaden zur Umsetzung von NIS2

01

Was ist NIS2 und warum ist NIS2 wichtig für Ihr Unternehmen?

1. Was ist NIS2 und warum ist NIS2 wichtig für Ihr Unternehmen?

NIS2 steht für „Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union“ und ist eine **EU-weite Gesetzgebung zur Cybersicherheit**, die zur Verbesserung und Vereinheitlichung des Gesamtniveaus europäischer Cybersecurity beitragen soll. Inhaltlich basiert NIS2 (Richtlinie 2022/2555) auf der europäischen NIS-1-Richtlinie aus 2016, die vornehmlich die IT-sicherheitsrechtliche Regulierung von „Kritischen Infrastrukturen“ und digitalen Diensten zum Gegenstand hatte. Seither aber hat sich nicht nur die Cyber-Bedrohungslage erheblich verschärft, sondern auch die Vernetzung und Verwendung von Cloud-Technologie hat erheblich zugenommen. Diese deutlich veränderte Interessenlage, aber auch das Erfordernis zu einer verbesserten unionsweiten Zusammenarbeit in der Cybersicherheit adressiert NIS2, die NIS-1 ablösen wird. Neben einer Anpassung der rechtlich vorauszusetzenden Cybersicherheitsmaßnahmen wird mit NIS2 auch der **Adressatenkreis des neuen europäischen Rechtsakts erheblich erweitert**. Grundsätzlich betroffen sind Unternehmen und Einrichtungen in den nachfolgend aufgeführten Sektoren:

Energie	**Verkehr**	**Bankwesen**
Finanzmarkt-infrastrukturen	**Gesundheitswesen**	**Trinkwasser**
Abwasser	**Digitale Infrastruktur**	**Verwaltung von IKT-Diensten (Business-to-Business)**
Öffentliche Verwaltung	**Weltraum**	**Post- und Kurierdienste**
Abfallbewirtschaftung	**Produktion, Herstellung und Handel mit chemischen Stoffen**	**Produktion, Verarbeitung und Vertrieb von Lebensmitteln**
Verarbeitendes Gewerbe/ Herstellung von Waren	**Anbieter digitaler Dienste**	**Forschung**

Da es sich bei NIS2 genau wie bei der Vorgängerregelung um eine **EU-Richtlinie** handelt, muss diese zu ihrer Wirksamkeit gegenüber den Unternehmen zunächst grundsätzlich in das nationale Recht umgesetzt werden. Hierbei gilt ein straffer Zeitplan, denn NIS2 sieht vor, dass diese Umsetzung in das Recht der EU-Mitgliedstaaten bis zum 17.10.2024 stattgefunden haben muss. NIS-1 wird sodann mit Wirkung zum 18.10.2024 aufgehoben – somit ist **Mitte Oktober 2024 der Stichtag** für die neuen EU Cybersecurity-Vorgaben. Der deutsche Gesetzgeber realisiert die Umsetzung der EU-Richtlinie mit dem sogenannten „Gesetz zur Umsetzung der NIS2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" **(NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuG)**, das die wesentlichen Vorgaben aus dem europäischen Recht übernimmt und darüber hinaus zusätzlich verschiedene nationale Besonderheiten regelt. Zu beachten ist im Hinblick auf die Cybersecurity Compliance von Unternehmen, dass NIS2 **nicht der einzige europäische Rechtsakt** ist, der sich mit dem Thema befasst. Cybersicherheit kann viele Facetten und Anwendungsszenarien haben. Zwar erfasst NIS2 somit in der Breite viele Unternehmen unterschiedlichster Bereiche, darüber hinaus existieren jedoch auch **bereichsspezifische Rechtsakte**. Speziell im Finanzsektor zu nennen ist an dieser Stelle der „Digital Operational Resilience Act" **(Verordnung 2022/2554, DORA)**, der bereichsspezifische Vorgaben zum Cyberschutz enthält. Für die zahlreichen Unternehmen, die personenbezogene Daten verarbeiten, müssen außerdem die Vorgaben zur **Datensicherheit aus der DS-GVO** beachtet werden, da NIS2 im Kern die Aufrechterhaltung der Funktionsfähigkeit eines Unternehmens adressiert, das sich vernetzter informationstechnischer Prozesse bedient. Für vorwiegend analoge Gefahren, die sich jedoch auch mit digitalen Bedrohungslagen überschneiden können, wird in Zukunft auf nationaler Ebene spiegelbildlich das **„KRITIS-Dachgesetz"** für hybride Sicherheit sorgen. Perspektivisch sei an dieser Stelle noch auf einen weiteren europäischen Rechtsakt hingewiesen: Der im September 2022 durch die EU-Kommission vorgelegte Entwurf eines **„Cyber Resilience Act" (CRA)** wird in den kommenden Jahren voraussichtlich weitere Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen enthalten. Damit stellt NIS2 in der Gesamtbetrachtung nur einen – wenn auch gewichtigen – Baustein der neuen europäischen Cybersecurity Compliance-Architektur dar.

Praxistipp: Abgrenzung NIS2 von anderen Rechtsakten

Obwohl NIS2 eine Kernregelung europäischer Cybersecurity Compliance darstellt, ist stets zu prüfen, ob nicht gegebenenfalls bereichsspezifische Rechtsakte den Vorrang genießen. Zu Beginn der jeweiligen Regelungen finden sich im Anwendungsbereich wichtige Hinweise darauf, für welche Einrichtung welche Rechtsvorschrift gilt. Insbesondere ist die inhaltliche Abgrenzung zwischen NIS2 und CRA deutlich: NIS2 ist eine unternehmensbezogene Richtlinie, wohingegen der CRA eine produktbezogene Verordnung darstellt.

02

Welche konkreten Anforderungen gibt NIS2 zur Verbesserung der Cybersicherheit in der Praxis vor?

2. Welche konkreten Anforderungen gibt NIS2 zur Verbesserung der Cybersicherheit in der Praxis vor?

Bereits **NIS-1 stellt in Art. 14 Anforderungen** an die Sicherheit von Netz- und Informationssystemen auf. So wird die Vorgabe gemacht, dass die Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen müssen, um „die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen". Zusätzlich wird die Vorgabe gemacht, dass diese Maßnahmen unter „Berücksichtigung des Stands der Technik" ein Sicherheitsniveau gewährleisten müssen, das dem bestehenden Risiko angemessen ist. Nach NIS-1 ist den Auswirkungen von Sicherheitsvorfällen, welche die Dienstebereitstellung beeinträchtigen, vorzubeugen bzw. die Auswirkungen sind im Sinne der Diensteverfügbarkeit so gering wie möglich zu halten.

Da **NIS2 inhaltlich auf den Vorgaben aus NIS-1 aufbaut**, orientieren sich die neuen europäischen Cybersicherheitsanforderungen ebenfalls an einem risikobasierten Ansatz, der nunmehr in Art. 21 vorzufinden ist, wobei inhaltlich verschiedene Konkretisierungen und Erweiterungen vorgenommen werden: So haben die betroffenen Einrichtungen geeignete und verhältnismäßige **technische, operative und organisatorische Maßnahmen** zu ergreifen, um die Risiken für die Sicherheit der für den Betrieb bzw. die Diensteerbringung genutzten IT-Systeme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Diensteempfänger oder andere Dienste zu verhindern oder möglichst gering zu halten. Bezug nimmt NIS2 dabei nicht nur auf den **„Stand der Technik"**, sondern auch auf die einschlägigen europäischen und internationalen Normen.

Praxistipp: Zur Bestimmung des „Stand der Technik"

Der vielzitierte „Stand der Technik" ist eine auslegungsbedürftige rechtliche Generalklausel und definitorisch in die Begriffstrias zwischen „allgemein anerkannten Regeln der Technik" und dem „Stand von Wissenschaft und Technik" einzuordnen. Die Bestimmung des konkreten Stands der Technik, der erforderlich ist, um eine gesetzliche Anforderung zu erfüllen, kann daher nicht abstrakt oder allgemein bestimmt werden, sondern ist beispielsweise von der konkreten Risikoexposition eines Unternehmens abhängig. In den vergangenen Jahren wurden jedoch verschiedene Handreichungen mit Instrumenten zur Bestimmung des Stands der Technik in der Cybersicherheit publiziert, die grundsätzlich auch für NIS2 herangezogen werden können.

03

Kosten-Nutzen-Analyse in der Cybersicherheit

3. Kosten-Nutzen-Analyse in der Cybersicherheit

Ebenfalls in die Risikobewertung einzubeziehen sind die durch die Umsetzungsmaßnahmen entstehenden Kosten in Relation zu den Risiken bzw. den durch eine Maßnahme erzielten Nutzen als **Angemessenheitskriterium**, da auch dem europäischen Gesetzgeber bewusst ist, dass trotz aller Bemühungen hierum **keine hundertprozentige Cybersicherheit** erreicht werden kann. Außerdem ist im Rahmen der durch NIS2 regulierten Cybersicherheitsmaßnahmen das **Meldewesen für Sicherheitsvorfälle** zu berücksichtigen, das zwar bereits durch NIS-1 vorgegeben ist, aber durch NIS2 basierend auf den Erfahrungen der vergangenen Jahre weiter optimiert wurde. Gerade auch das Meldewesen setzt voraus, dass betroffene Unternehmen nicht nur reaktionär auf Cybersicherheitsvorfälle tätig werden, sondern Maßnahmen im Sinne eines präventiven Managementsystems ergreifen, wozu auch Dokumentation und Nachweis getroffener Maßnahmen gehören können.

Praxistipp: Die „Angemessenheit" der im Rahmen von NIS2 zu ergreifenden Cybersicherheitsmaßnahmen

Maßnahmen zur Cybersicherheit müssen verhältnismäßig und wirtschaftlich sein – auch NIS2 verlangt keine „Cybersecurity um jeden Preis" und damit keine unverhältnismäßige finanzielle und administrative Belastung für betroffene Einrichtungen. Generell gilt jedoch, dass ein Cybersicherheitsniveau zu realisieren ist, das dem bestehenden Risiko angemessen ist. Bei der Bewertung dieser Verhältnismäßigkeit sind nachfolgende Eigenschaften gebührend zu berücksichtigen:

- Ausmaß der Risikoexposition der Einrichtung
- Größe der Einrichtung
- Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen
- Schwere der Sicherheitsvorfälle einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen (beispielsweise auch im Hinblick auf die Versorgungssicherheit)
- Technischer Standard und Umsetzungskosten

Die Angemessenheitsbeurteilung setzt somit eine sorgfältige Analyse von Komponenten, Systemen und Prozessen sowie den damit verbundenen Risiken voraus. Aus der durchgeführten Analyse können sodann entsprechende Maßnahmen zur Mitigation abgeleitet werden. Anhand dieser Kriterien zur Risikoanalyse wird aber ebenso deutlich, dass es keinen einheitlichen Maßstab zur Risikoabwägung gibt, sondern die Risiken in erheblichem Maße auch von den Sektoren und Branchen abhängig sein können, in denen eine Einrichtung bzw. ein Unternehmen tätig ist bzw. ob es gesellschaftskritische Dienste erbringt. Ebenfalls deutlich wird, dass sich die Auswirkungen von Cybersicherheitsvorfällen gerade in den versorgungsrelevanten Branchen auch weit über die durch NIS2 betroffene Einrichtung hinaus erstrecken können. Folgende Fragestellungen können daher bei einer Bestimmung des Cybersicherheitsniveaus hilfreich sein:

- Welche Kritikalität besitzt eine Einrichtung?
- Inwieweit ist eine Einrichtung in ihrer Funktion von vernetzten IT-Systemen abhängig?
- Ist das Funktionieren der Einrichtung abhängig vom Funktionieren digitaler Lieferketten?
- Hat es bereits Vorfälle in der Vergangenheit gegeben bzw. ist anzunehmen, dass sich Angriffe in Zukunft häufen werden?
- Ist eine Einrichtung in der öffentlichen Wahrnehmung besonders exponiert?
- Was könnten potenzielle Angreifer infolge einer erfolgreichen Kompromittierung der Einrichtung erlangen?

Insgesamt gilt für das Ergebnis einer Risikoanalyse natürlich, dass die daraus abgeleiteten Maßnahmen geeignet sein müssen, Beeinträchtigungen der Cybersicherheit tatsächlich zu reduzieren und nicht allein nur die wirtschaftlichen Folgen eines erfolgreichen Cyberangriffs zu verringern oder zu vermeiden. Daher kann zum Beispiel auch der Abschluss einer Cyberpolice allein nicht ausreichend sein, um den Anforderungen nachzukommen.

In der Benennung konkreter Anforderungen der technischen, operativen und organisatorischen Maßnahmen **geht NIS2 über den Regelungsgehalt von NIS-1 hinaus**. Insbesondere wird das **Konzept eines „gefahrenübergreifenden Ansatzes"** verfolgt, der nicht nur auf den Schutz der Netz- und Informationssysteme selbst, sondern auch auf die physische Umwelt dieser Systeme abzielt. Damit wird auch der Bezug zur gegenwärtig verstärkt bestehenden **hybriden Bedrohungslage** deutlich.

Praxistipp: Die hybride Bedrohungslage und ihr Einfluss auf die Cybersicherheit

Mit NIS2 rückt ergänzend zu klassischen Cybersicherheitsmaßnahmen der „gefahrenübergreifende Ansatz" in den Fokus. Dieser zielt darauf ab, vernetzte IT-Systeme und ihr physisches Umfeld vor Ereignissen wie

- Diebstahl,
- Feuer,
- Überschwemmungen,
- Telekommunikations- oder Stromausfällen,
- unbefugtem physischen Zugang zu Informationen und Datenverarbeitungsanlagen und der Schädigung dieser Informationen und Anlagen und den entsprechenden Eingriffen zu schützen.

Gegenmaßnahmen in diesem Bereich können die Zugangskontrolle, den Schutz vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen und natürlichen Phänomenen umfassen.

Auch spiegelt sich der erweiterte Regelungsgehalt von NIS2 in den entsprechenden nationalen Vorschlägen für die Umsetzungsgesetze wider, indem es teils nicht mehr nur darum geht, dass Störungen in den IT-Systemen und -Prozessen vermieden werden sollen, die für die Funktionsfähigkeit der betriebenen Infrastruktur maßgeblich sind, sondern vielmehr alle Störungen in den IT-Systemen und -Prozessen zu vermeiden sind, die die Einrichtungen zur Erbringung ihrer Dienste nutzen. Hiermit dürften perspektivisch somit auch Anpassungen auf das Risikomanagement jener Unternehmen zukommen, die beispielsweise bereits von NIS-1 betroffen sind.

04

Leitlinien für effektive Risikobewertung und Maßnahmenumsetzung

4. Leitlinien für effektive Risikobewertung und Maßnahmenumsetzung

Die Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten den Grad der Abhängigkeit der durch NIS2 betroffenen Einrichtung von Netz- und Informationssystemen berücksichtigen und auch Maßnahmen zur Ermittlung jeder Gefahr eines Sicherheitsvorfalls, zur Verhinderung, und Aufdeckung von Sicherheitsvorfällen, zur Reaktion darauf und zur Wiederherstellung danach sowie der Minderung ihrer Folgen umfassen. Die Sicherheit von Netz- und Informationssystemen sollte sich auch auf gespeicherte, übermittelte und verarbeitete Daten erstrecken. Die Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten eine systemische Analyse vorsehen, bei der der menschliche Faktor berücksichtigt wird, um ein vollständiges Bild der Sicherheit des Netz- und Informationssystems zu erhalten. Die Maßnahmen gelten unabhängig davon, ob IT-Systeme intern gewartet werden oder ihre Wartung ausgelagert wird. Nach Vorschlag von NIS2 soll zukünftig außerdem die Möglichkeit bestehen, auch aus der Wirtschaft koordinierte Risikobewertungen von kritischen Lieferketten durchzuführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln.

Insgesamt ist es die Pflicht der europäischen Mitgliedstaaten, sicherzustellen, dass die durch NIS2 betroffenen Einrichtungen unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Maßnahmen zur Cybersicherheit ergreifen. Bei der Umsetzung der Maßnahmen stehen durch NIS2 insbesondere auch die Leitungsorgane in der Pflicht, Maßnahmen zu genehmigen und deren Umsetzung zu überwachen.

Praxistipp: „Mindestkatalog" für Cybersicherheitsmaßnahmen nach NIS2

Im Sinne eines Mindestkatalogs schreibt NIS2 folgende Maßgaben für die Cybersicherheit vor:

- 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

Bis zum 17.10.2024 erlässt die Europäische Kommission Durchführungsrechtsakte zur Festlegung der technischen und methodischen Anforderungen an die Risikomanagementmaßnahmen im Bereich der Cybersicherheit in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke sowie für Vertrauensdiensteanbieter. NIS2 enthält darüber hinaus die Möglichkeit für den Erlass weiterer Durchführungsrechtsakte zur Konkretisierung der Maßnahmen für die wesentlichen und wichtigen Einrichtungen. Die konkretisierenden Durchführungsrechtsakte entstehen aber nicht im „luftleeren Raum", sondern orientieren sich weitestgehend möglich an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen zur Cybersicherheit. Auch ansonsten verweist NIS2 zur Umsetzung auf europäische und internationale Normen und Standards in der Informationssicherheit, so zum Beispiel explizit auf die Reihe ISO/IEC 27000.

05

Anforderungen an das Cybersecurity-Management in NIS2 entschlüsseln

5. Anforderungen an das Cybersecurity-Management in NIS2 entschlüsseln

Nicht nur im konkreten Maßnahmenkatalog des Art. 21 NIS2, sondern auch an verschiedenen weiteren Stellen des EU-Rechtsakts finden sich an das Cybersecurity-Management anzulegende rechtliche Anforderungen und dieses **ergänzende hilfreiche Informationen**, die teils nicht immer unmittelbar aus dem Wortlaut der Vorschriften hervorgehen, was die Handhabe in der Praxis verkompliziert. Diese betreffen unter anderem folgende Fragestellungen und Maßgaben:

- **Kohärenz zwischen physischer Sicherheit und Cybersicherheit** und insbesondere die (behördliche) Abstimmung zu Fragen der Cybersicherheit und nicht cyberbezogenen Risiken,
- **Einsatz von Künstlicher Intelligenz** zur Aufdeckung und Verhütung von Cyberangriffen, denn gerade KI wird durch die EU als eine innovative Technologie gesehen, die dabei unterstützen kann, vorhandene Ressourcen wirksamer zur Abwehr von Cyberangriffen einzusetzen und Kapazitäten zu erhöhen,
- **Berücksichtigung auch von Datenschutzanforderungen** bei der Umsetzung von Cybersicherheit, denn es kann zur Umsetzung von NIS2 auch erforderlich sein, personenbezogene Daten zu verarbeiten, wobei die Datenschutzgrundsätze nach DS-GVO, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gelten,
- **Verwendung von Open-Source-Cybersicherheitswerkzeugen und -Anwendungen** können nicht nur zu einem höheren Maß an Offenheit beitragen, sondern sich auch positiv auf die Effizienz von industriellen Innovationen auswirken; offene Standards können zudem die Interoperabilität von Sicherheitstools erleichtern,
- **Fokus auf KMU-zentrierte Cybersicherheitsmaßnahmen** erleichtert es vor allem den Unternehmen mit begrenzten wirtschaftlichen und personellen Ressourcen, die Cybersicherheit zu verbessern, beispielsweise durch ein gestiegenes Cybersicherheitsbewusstsein, da Vorfälle in diesem Bereich auch Auswirkungen auf die (digitale) Lieferkette haben können,
- **Maßnahmen des aktiven Cyberschutzes** adressieren die Frage, welche Anforderungen geeignet sind, aktiv zur Verhütung, Erkennung, Überwachung, Analyse und Abschwächung von Sicherheitsverletzungen in einem Netzwerk beitragen zu können, insbesondere können darunter auch zu fassen sein Maßnahmen wie Verschlüsselung, Netzwerkkartografie und -Segmentierung, Kennzeichnung sowie Zugangsverwaltung,
- **Schwachstellenerkennung** ist ein zentraler Aspekt der Cybersicherheit, denn die Ausnutzung von Schwachstellen kann erhebliche Störungen und Schäden zur Folge haben, weshalb geeignete Verfahren zur Behandlung entdeckter Schwachstellen bestimmt werden und Verfahren eingeführt werden sollten, um Schwachstelleninformationen beispielsweise von Dritten entgegenzunehmen,
- **Abwehr von Wirtschaftsspionage und Schutz von Geschäftsgeheimnissen** bedeutet, dass sich Unternehmen insbesondere auch mit den Risiken befassen müssen, die sich aus ihren Interaktionen und Beziehungen zu Externen in einem weiter gefassten Ökosystem ergeben, das auch über die rein technische Cybersicherheit hinausgehen kann,
- **Cyberhygiene** umfasst grundlegende Praktiken wie Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugriffsmanagement, Sensibilisierung der Nutzer und Schulungen, Schaffung von Awareness zum Beispiel gegen Phishing und Social Engineering,

- **erhöhte Cybersecurity Governance auf Unternehmensleitungsebene** hat zur Folge, dass zukünftig auch die Leitungsorgane stärker in die NIS2-Umsetzung einbezogen werden und IT-Sicherheitsmaßnahmen nicht mehr beliebig delegierbar sind, indem eigenes Know-how und Managementpraktiken etabliert werden müssen,

- **Dokumentationspflichten** dienen dem Nachwies von Cybersicherheit gegenüber Aufsichtsbehörden und Geschäftspartnern, können aber auch im Zuge der Verbesserung des eigenen Prozessmanagements der Cybersecurity relevant sein,

- **Absicherung der Lieferkette** hat die Beziehung zu Lieferanten zum Gegenstand, so beispielsweise Anbieter von Datenspeicherungs- und -verarbeitungsdiensten, Anbieter von verwalteten Sicherheitsdiensten oder Softwarehersteller. Daher ist es wichtig, die Gesamtqualität und Widerstandsfähigkeit externer Produkte und Dienste als Bestandteil des Risikomanagements zu bewerten und zu berücksichtigen. Dies kann auch durch vertragliche Vereinbarungen geschehen.

- **Berücksichtigung und Vermeidung „nichttechnischer Risikofaktoren“** wie ungebührliche Einflussnahme eines Drittlandes auf Lieferanten und Diensteanbieter (mit der Folge von versteckten Schwachstellen oder Hintertüren sowie potenziellen systemischen Versorgungsunterbrechungen, auch im Hinblick auf die Abhängigkeit von bestimmten Technologien).

Praxistipp: Es gibt nicht „die eine“ Maßnahme zur rechtskonformen Umsetzung von NIS2

Bei Betrachtung der Risikomanagementmaßnahmen in der Cybersicherheit wird schnell deutlich, dass die NIS2-Richtlinie vor allem prozessbezogene Inhalte, jedoch nur sehr wenige konkrete technologiebezogene Elemente enthält. Diese „Unschärfe“ mag die Unternehmen zwar vor eine gewisse Rechtsunsicherheit in der Umsetzung stellen, ist aber durch den Gesetzgeber durchaus gewollt. Überdies findet sich eine ähnliche Herangehensweise auch in verschiedenen anderen Feldern der EU-Technikregulierung wieder, wie beispielsweise in der EU DS-GVO.

Dies hat vor allem zwei Hintergründe: Einerseits kann sich insbesondere der „Stand der Technik“ und damit die zu treffenden Maßnahmen in der Praxis schneller ändern, als dies durch den Gesetzgeber rechtlich abgebildet werden kann. Andererseits erfasst NIS2 im Anwendungsbereich eine Vielzahl nicht nur von unterschiedlichen Sektoren und Branchen, sondern auch von Unternehmensgrößen, sodass nicht sämtliche Fälle abschließend im Sinne einer Kasuistik rechtlich abgebildet werden können. Deshalb gibt es grundsätzlich durchaus mehrere und verschiedene Wege, um den Anforderungen aus NIS2 mittels Cybersecurity-Maßnahmen nachzukommen, da jedes Informationssicherheitsmanagement stets auf die individuellen betrieblichen Bedürfnisse zugeschnitten werden muss.

06

NIS2 Umsetzung: Ein ganzheitlicher Ansatz für rechtliche, technische und organisatorische Anforderungen

6. NIS2 Umsetzung: Ein ganzheitlicher Ansatz für rechtliche, technische und organisatorische Anforderungen

Die Vielfalt vorgenannter Umsetzungsanforderungen für NIS2 verdeutlicht, dass es zur effektiven und praxisorientierten Umsetzung der neuen rechtlichen Anforderungen mehr denn je und auch über NIS-1 hinausgehend eines **ganzheitlichen Ansatzes** bedarf, der im Kontext konkreter Anwendungsszenarien die Verwendung verschiedener Werkzeuge voraussetzt und neben der rein technischen Umsetzung stärker als bislang auch die **operative und organisatorische Komponente** in den Blick zu nehmen sein wird.

Praxistipp: Warum die Umsetzung von NIS2 für die betroffenen Unternehmen wichtig ist

Eindeutig wird durch NIS2 bestimmt, dass die Verantwortung für die Gewährleistung der Cybersicherheit in erheblichem Maße bei den betroffenen Einrichtungen liegt. Dies setzt voraus, dass die Einrichtungen eine Risikomanagementkultur fördern und entwickeln. Diese Risikomanagementkultur umfasst unter anderem die Risikobewertung und die Anwendung der bereits zuvor skizzierten Risikomanagementmaßnahmen im Bereich der Cybersicherheit. Doch nicht nur diese intrinsische Motivation spielt bei der Umsetzung von NIS2 eine Rolle. Unternehmen sollten sich stets bewusst sein, dass Cybersicherheitsvorfälle nicht nur Reputationsschäden und damit wirtschaftliche Schäden bedeuten können, sondern auch rechtliche Konsequenzen zur Folge haben können, die ebenso negative wirtschaftliche Folgen nach sich zu ziehen geeignet sind. Ebenso kann eine Verletzung der Cybersicherheit zugleich mit einer Datenschutzverletzung verbunden sein.

Eine Nichtbeachtung von Cybersicherheit kann zum Beispiel vertragliche oder deliktische Schadensersatzansprüche zur Folge haben, falls die Risikomanagementmaßnahmen nicht richtig, unzureichend oder schlimmstenfalls gar nicht implementiert wurden und dadurch die „im Verkehr erforderliche Sorgfalt“ außer Acht gelassen wurde.

Daneben sieht NIS2 umfassende behördliche Kontrollbefugnisse, Sanktionen und Bußgelder vor. Die Aufsichts- und Durchsetzungsmaßnahmen sollen laut dem europäischen Recht „wirksam, verhältnismäßig und abschreckend“ sein. Kehrseitig treffen die betroffenen Einrichtungen Mitwirkungspflichten, zum Beispiel zur Gewährung des Zugangs zu Daten, Datenverarbeitungsanlagen oder zur Erbringung von Nachweisen für die Umsetzung von Cybersicherheitskonzepten. Daraus resultierende behördliche Maßnahmen können unter anderem Folgendes umfassen:

- Warnungen über Verstöße
- Verbindliche Anweisungen zur Behebung eines Sicherheitsvorfalls
- Mitteilungen von Cyberbedrohungen an Diensteempfänger
- Anweisung zur öffentlichen Bekanntmachung von Verstößen
- Zwangsgelder
- Verhängung von Geldbußen

Bei der Ergreifung von Durchsetzungsmaßnahmen nach NIS2 werden verschiedene Aspekte in die Bewertung einbezogen:

- Schwere des Verstoßes
- Wichtigkeit der Bestimmungen, gegen die verstoßen wurde
- Wiederholung von Verstößen
- Nichtbehebung von Mängeln nach verbindlicher Anweisung
- Übermittlung falscher oder grob verfälschender Informationen in Bezug auf das Risikomanagement zur Cybersicherheit
- Dauer des Verstoßes
- Verursachte materielle oder immaterielle Schäden
- Vorsatz/Fahrlässigkeit
- Kooperation und Schadensminderungsmaßnahmen

Geldbußen können zusätzlich zu den weiteren behördlichen Maßnahmen nach NIS2 verhängt werden und bestimmen sich nach dem jeweiligen Einzelfall. Unterschieden wird dabei anhand der Schwere des Verstoßes und der betroffenen Einrichtung innerhalb von zwei Bußgeldbemessungsgrenzen:

- Geldbußen mit einem Höchstbetrag von mindestens 10.000.000 EUR oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens – je nachdem, welcher Betrag höher ist,
- Geldbußen mit einem Höchstbetrag von mindestens 7.000.000 EUR oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens – je nachdem, welcher Betrag höher ist.

Weitere Informationen zu NIS2

NIS2 kommt mit vielen Fragen daher: Für wen gilt NIS2? Welche Anforderungen stellt NIS2? Was müssen Kunden konkret unternehmen, um NIS2-Konformität zu erreichen? Finden Sie Antworten auf die wichtigsten Fragen auf den dedizierten NIS2-Webseiten von Trend Micro.

Für Kunden **Für Partner**

Hinweis: Die Inhalte auf diesen Webseiten sind auf die Gesetzeslage in Deutschland abgestimmt. Daher bitten wir um Prüfung der Relevanz der Inhalte in anderen Ländern.

Mehr unter **trendmicro.com**