LINK11

WHITEPAPER

It's a fact: NIS-2 kommt

Stand Oktober 2024

www.link11.com

In Kooperation mit:

SCHALAST
LAW | TAX

Liebe Leserinnen und Leser,

Die NIS-2-Richtlinie („The Network and Information Security (NIS) Directive“) stellt Unternehmen in der EU vor eine neue Herausforderung: die umfassende Stärkung ihrer Cybersecurity. Während das Bewusstsein für die Bedeutung von Cybersicherheit gewachsen ist, zeigen aktuelle Umfragen, dass viele Unternehmen noch nicht ausreichend vorbereitet sind, um die neuen Anforderungen zu erfüllen.

NIS-2 geht über bisherige Vorschriften hinaus. Sie betrifft eine größere Anzahl von Unternehmen und Sektoren und stellt höhere Anforderungen an die Risikobewertung, das Incident Management und die Lieferketten-Sicherheit. Unternehmen, die nicht konform sind, müssen mit empfindlichen Bußgeldern rechnen.

Ziel der Richtlinie ist es, die Widerstandsfähigkeit gegen Cyberangriffe zu erhöhen und EU-weit ein höheres Maß an Cybersicherheit zu gewährleisten. Für Unternehmen bedeutet dies nicht nur erhöhte Compliance-Kosten, sondern auch eine steigende Komplexität der IT-Landschaften. Gleichzeitig eröffnet die NIS-2 neue Chancen, sich von Wettbewerbern zu differenzieren und das Vertrauen von Kunden und Geschäftspartnern zu stärken.

Die Umsetzung von NIS-2 gestaltet sich jedoch als komplex. Dieses Whitepaper bietet Ihnen einen umfassenden Überblick über NIS-2 und zeigt Ihnen, wie Sie die neuen Anforderungen erfolgreich umsetzen können. Wir gehen auf die wichtigsten Aspekte ein, wie beispielsweise die konkreten Maßnahmen, die Sie ergreifen müssen, um NIS-2-konform zu werden, und welche Technologien Sie dabei unterstützen können.

Lassen Sie uns gemeinsam dafür sorgen, dass Ihre Organisation für die Zukunft der Cybersecurity gerüstet ist.

Wir wünschen Ihnen eine informative Lektüre.

Herzliche Grüße

Jens-Philipp Jung
Link11
CEO

Janka Schwaibold
Schalast LAW | TAX
Rechtsanwältin, Partnerin

Inhalt

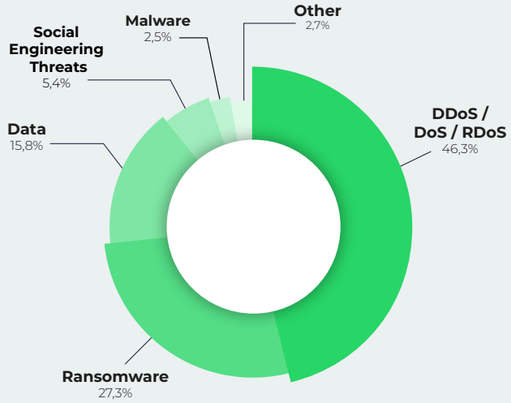
Überblick über aktuelle Cyber-Bedrohungen in Europa

Die Cyber-Bedrohungslandschaft: Ein Minenfeld für Unternehmen
Der digitale Wandel hat unser Leben grundlegend verändert. Gleichzeitig hat er auch die Angriffsfläche für Cyberkriminelle exponentiell vergrößert. Die aktuelle Bedrohungslage ist komplex und dynamisch und stellt Unternehmen jeder Größe vor immense Herausforderungen.

Laut dem aktuellen X-Force Threat Intelligence Index von IBM[1] **verzeichnete Europa im Jahr 2023 mit 32 % aller Vorfälle weltweit die meisten Cyberangriffe.** Besonders betroffen waren Großbritannien (27 %), Deutschland (15 %) und Dänemark (14 %). **Der Bericht zeigt auch, dass 74 % der Cyberangriffe in der Europäischen Union auf kritische Infrastrukturen abzielten.** Ein alarmierender Anstieg, der die Verwundbarkeit dieses Sektors verdeutlicht.

Diese Bedrohung wird durch die zunehmende Nutzung gestohlener Zugangsdaten verschärft, die einen einfachen Zugang zu Netzwerken ermöglichen. Der Missbrauch gültiger Konten durch Cyberkriminelle stieg 2023 um 66 %.

Cybercrime-as-a-Service: Cyberkriminalität für jedermann
Ransomware-Angriffe stellen nach wie vor eine der größten Bedrohungen dar. Laut dem Internet Crime Report (IC3) 2023[2] des FBI wurden mehr als 2.825 Ransomware-Vorfälle gemeldet – ein Anstieg von 18 % gegenüber dem Vorjahr. **Gleichwohl sind fast die Hälfte der Cyberangriffe in der Europäischen Union Distributed-Denial-of-Service-Angriffe (DDoS).** Die Europäische Agentur für Cybersicherheit (ENISA) hat einen „signifikanten Anstieg" von Cybersicherheitsvorfällen in der EU festgestellt. Von Juli 2023 bis Juni 2024 waren laut der aktuellen „Threat Landscape 2024"[3] die größten Bedrohungen Angriffe gegen die Verfügbarkeit (DDoS) gefolgt von Ransomware. Die Entwicklung von Cybercrime-as-a-Service-Modellen hat die Schwelle für die Durchführung von Cyberattacken gesenkt. Auch technisch weniger versierte Angreifer können nun auf diese Tools zurückgreifen.



Quelle: ENISA Threat Landscape 2024

Die Kluft zwischen Groß und Klein
Besonders problematisch ist die wachsende Kluft bei der Cyber-Resilienz. Während große Organisationen ihre Sicherheitsmaßnahmen verbessern, geraten kleine und mittlere Unternehmen (KMU) zunehmend ins Hintertreffen. Laut dem Global Cybersecurity Outlook 2024[4] des Weltwirtschaftsforums erfüllen 30 % weniger Organisationen als im Vorjahr die Mindeststandards für Cyber-Resilienz. Diese Entwicklung ist besorgniserregend, da KMU in vielen Ländern den Großteil der Wirtschaft ausmachen, von dieser Diskrepanz aber überproportional betroffen sind. Mehr als doppelt so viele KMU wie Großunternehmen geben an, dass sie nicht über ausreichend Cyber-Resilienz verfügen, um ihre kritischen Geschäftsanforderungen zu erfüllen.

Ein weiteres großes Problem ist der Mangel an qualifiziertem Personal. Viele kleine Unternehmen geben an, dass sie nicht über die notwendigen Fähigkeiten verfügen, um ihre Cyberziele zu erreichen.

1 https://www.ibm.com/reports/threat-intelligence
2 https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
3 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
4 https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Die Lieferkette als Einfallstor
Die digitale Vernetzung von Unternehmen über Lieferketten hinweg bietet Cyberkriminellen zahlreiche Möglichkeiten, in Unternehmen einzudringen. **Schwachstellen in der Lieferkette können dazu genutzt werden, um vertrauenswürdige Software mit Schadcode zu infizieren oder an sensible Daten zu gelangen.** Mehr als die Hälfte der Unternehmen gibt an, in diesem Bereich Nachholbedarf zu haben.

Darüber hinaus schaffen das Internet der Dinge (IoT) und die zunehmende Nutzung von Cloud-Diensten neue Angriffsvektoren. Die Vielzahl vernetzter Geräte und die Speicherung sensibler Daten in der Cloud machen Unternehmen anfälliger für Cyberangriffe.

Auch staatlich finanzierte Cyberangriffe stellen eine wachsende Bedrohung dar. Diese Angriffe können sich gezielt gegen kritische Infrastrukturen oder politische Gegner richten. Angesichts dieser Herausforderungen ist eine verstärkte Zusammenarbeit zwischen staatlichen Stellen und dem Privatsektor von entscheidender Bedeutung, um den Bedrohungen wirksam zu begegnen.

Die Cyber-Bedrohungslandschaft ist dynamisch und komplex. Unternehmen müssen proaktive Maßnahmen ergreifen, um ihre digitale Widerstandsfähigkeit zu stärken. Dazu gehören Investitionen in moderne Sicherheitstechnologien, die Schulung von Mitarbeitenden und die enge Zusammenarbeit mit externen Experten. So können Unternehmen den wachsenden Cyberrisiken begegnen und ihre digitalen Assets schützen.

Risikoanalyse und -bewertung im Rahmen der NIS-2-Richtlinie

Die NIS-2-Richtlinie stellt einen Meilenstein in der europäischen Cybersicherheitslandschaft dar. Sie verpflichtet Unternehmen, die kritische Infrastrukturen betreiben, zu einer umfassenden Risikoanalyse und -bewertung. Diese ist unerlässlich, um Schwachstellen zu identifizieren und gezielte Schutzmaßnahmen zu ergreifen.

Zentrale Rolle der Risikoanalyse in NIS-2
Die Risikoanalyse ist das Herzstück der NIS-2-Richtlinie. Sie verpflichtet Unternehmen dazu, ihre IT-Landschaft systematisch zu untersuchen und mögliche Risiken zu identifizieren. Dabei geht es nicht nur um technische Aspekte, sondern auch um organisatorische und menschliche Faktoren.

Diese umfassende Beurteilung von Bedrohungspotenzialen und Schwachstellen ist nicht nur eine gesetzliche Forderung, sondern auch eine unverzichtbare Grundlage für effektive Schutzmaßnahmen.

Ziele der Risikoanalyse gemäß NIS-2:

- **Identifikation von Schwachstellen:** Sowohl technische als auch organisatorische Schwachstellen sollen aufgedeckt werden.
- **Abschätzung der Eintrittswahrscheinlichkeit und der möglichen Auswirkungen:** Die Analyse soll die Wahrscheinlichkeit eines erfolgreichen Angriffs und den daraus resultierenden Schaden abschätzen.
- **Entwicklung von Schutzmaßnahmen:** Auf Basis der Risikobewertung können gezielte Schutzmaßnahmen ergriffen werden.
- **Kontinuierliche Verbesserung:** Die Risikoanalyse ist kein einmaliger Vorgang, sondern muss regelmäßig wiederholt werden, um auf Veränderungen in der IT-Landschaft und der Bedrohungslage reagieren zu können.

Die Umsetzung der NIS-2-Richtlinie ist jedoch mit zahlreichen Herausforderungen verbunden. Die Komplexität moderner IT-Landschaften, der Mangel an qualifiziertem Personal und die sich ständig ändernde Bedrohungslage erschweren eine umfassende Risikoanalyse. Zudem ist die Frage nach der richtigen Methodik – qualitative oder quantitative Ansätze oder eine Kombination aus beiden – oft umstritten.

Vor diesem Hintergrund stellt sich die Frage, wie Unternehmen die Anforderungen der NIS-2-Richtlinie erfolgreich umsetzen können. Welche konkreten Maßnahmen sind notwendig, um eine effektive Risikoanalyse durchzuführen? Wie wird die Lieferkette der Unternehmen eingebunden und welche Auswirkungen hat das? Wie wirken sich Konzernstrukturen auf die Umsetzung von NIS-2 aus? Diese und weitere Fragen haben wir mit Sophia Zimmer, Senior Consultant, bei der VICCON GmbH geklärt.

Sophia Zimmer
Senior Consultant,
VICCON GmbH

Sophia Zimmer ist Beraterin mit umfangreichen Erfahrungen im Bereich Informationssicherheitsmanagement (ISMS) bei VICCON. Sie verfügt über fundierte Kenntnisse in den Bereichen ISMS-Auditing, Projektleitung und Risikomanagement. Sophia hat erfolgreich den ISMS-Aufbau verantwortet und unterstützt Unternehmen dabei, die Einhaltung der gängigen Standards zu gewährleisten

NIS-2 & Risikomanagement

Sophia, ich würde gerne von dir wissen, welche konkreten Herausforderungen du bei der praktischen Umsetzung der NIS-2-Richtlinie in Bezug auf die Risikoanalyse siehst.

Grundsätzlich fordert die NIS-2 hinsichtlich des Risikomanagements folgende Punkte: Es muss ein Konzept zur Risikoermittlung, Bewertung der Risikomanagementmaßnahmen und die Beurteilung kritischer Lieferantenrisiken unter Berücksichtigung des All-Hazard-Prinzips (Allgefahrenansatz) vorliegen.

Insbesondere GmbHs und AGs sind gesetzlich bereits zur fortlaufenden Überwachung von Gefährdungen verpflichtet (gem. AktG, StaRUG), d.h. es existiert ein Risikomanagement. Die Herausforderung sehe ich darin, dass verschiedene Akteure (und damit auch sehr unterschiedliche Blickwinkel und Interessen) zusammenkommen, um die IT- und Informationssicherheits-Risiken zu bewerten. Das halte ich aber zugleich auch für den entscheidenden Erfolgsfaktor.

Letztlich macht die NIS-2-Richtlinie deutlich: IT-Risiken müssen als Unternehmensrisiken betrachtet werden. Ziel sollte sein, die Methoden des vorhandenen Risikomanagements zu nutzen, sodass alle relevanten Personen ein gemeinsames Verständnis entwickeln und Risiken effizient transparent berichtet sowie gemanaged werden können. Eine wesentliche Herausforderung im Risikomanagement ist für mich: Risiken transparent darstellen, um Entscheider konkret zu unterstützen sowie alle relevanten Personen ins Boot zu holen.

Wer bereits ein wirksames ISMS implementiert hat, wird zunächst nicht auf neue Herausforderungen stoßen. Allerdings wird sich die Risikoanalyse hinsichtlich der Betrachtung der Lieferketten erweitern müssen, da die NIS-2 sehr deutlich macht, dass vernetzte Risiken und Abhängigkeiten von Dienstleistern und Lieferanten konkret erfasst und bewertet werden müssen.

Da kommt einiges auf die Unternehmen zu, mitunter auch knifflige Situationen. Wie wirkt sich die Einbindung der gesamten Lieferkette auf die Risikoanalyse nach den NIS-2-Anforderungen aus, und warum ist eine sorgfältige Dokumentation der Entscheidungen hierbei besonders wichtig?

Die größte Herausforderung liegt darin, dass sicherheitsbezogene Aspekte zwischen den einzelnen Anbietern und deren unmittelbaren Dienstleistern erfasst werden müssen. Es kann auch hinsichtlich der Risikomanagementmaßnahmen knifflig werden, da Redundanzen nicht in allen Fällen verhältnismäßig sind. Von den zukünftig betroffenen Unternehmen wird nicht direkt ein perfektes Risk Assessment erwartet; alle Maßnahmen müssen hinsichtlich ihrer Verhältnismäßigkeit bewertet werden, abhängig von Unternehmensgröße, Schwere von Vorfällen und gesellschaftlichen und wirtschaftlichen Folgen. Die NIS-2 betrachtet IT- und Informationssicherheitsrisikenals reguläre Unternehmensrisiken, die transparent transportiert werden müssen. Entscheidet man sich gegen bestimmte Maßnahmen, sollte das dokumentiert und begründet werden, um im Nachhinein keine Fahrlässigkeit zu unterstellen.

Wie können Unternehmen die Risiken ihrer Lieferketten im Rahmen von NIS-2 effektiv managen, insbesondere bei komplexen globalen Wertschöpfungsketten?

Die größte Herausforderung liegt in der Risikoanalyse der Lieferkette. Es gilt, kritische Lieferanten zu identifizieren und detailliert zu bewerten. Unternehmen müssen Risiken in der Lieferkette erfassen, Ausfallsituationen durchdenken und sicherstellen, dass ihre Lieferanten Cybersicherheit gewährleisten.

Drei Dinge müssen in diesem Zusammenhang konkret betrachtet werden: Nachdem ich alle für mich kritischen Dienstleister identifiziert habe, muss ich 1) deren Informations- und IT-Sicherheit bewerten (insbesondere, wenn eine Netzwerk-Anbindung besteht oder Dateien in hohem Maße ausgetauscht werden)
2) deren BCM hinsichtlich dessen bewerten, welche Folgen ein Ausfall des Lieferanten für meine Betriebsfähigkeit haben kann (z.B. nach einer Ransomware-Attacke --> welchen Einfluss hat das auf meine Produktion/Prozesse/Dienstleistungen) und wie bereitet sich mein Lieferant sowie das eigene Unternehmen darauf vor? 3) Wie ist der Meldeweg definiert und sind außer Mail andere Kommunikationswege festgelegt, um im Falle einer Cyber-Attacke diese zu melden

Welche Schritte sollten Unternehmen einhalten, um die Informationssicherheit in ihrer Lieferkette zu gewährleisten, insbesondere wenn sie auf zahlreiche Lieferanten und Dienstleister angewiesen sind?

Unternehmen sollten unabhängig von der Länge ihrer Lieferantenliste folgende Schritte durchlaufen: Lieferanten listen und hinsichtlich relevanter Faktoren bewerten. Im nächsten Schritt müssen die kritischen Geschäftspartner innerhalb einer Risikoanalyse detaillierter betrachtet und bewertet werden. Zuletzt sollte man sich Gedanken machen, von welchem Lieferanten/Dienstleister welche Nachweise nützlich sind, um die IT- und Informationssicherheit in der Lieferkette sicherzustellen. Dabei ist es wichtig, die vertraglichen Verpflichtungen klar zu definieren, wie etwa Anforderungen an das Patch-Management, Back-up-Management, Notfallübungen und Incident Management.

NIS-2 & Risikomanagement

- **Erforderlich:** Konzept zur Risikoermittlung, Bewertung der Maßnahmen, und Analyse kritischer Lieferantenrisiken.
- **Ziel:** IT- und Informationssicherheitsrisiken als Unternehmensrisiken behandeln, einheitliche Methoden und Berichte für das Management erstellen.
- **Schwerpunkt:** Berücksichtigung der gesamten Lieferkette und vernetzte Risiken erfassen. Transparentes Risikomanagement zur Unterstützung von Entscheidern etablieren.

NIS-2 & Konzernstrukturen

Wie stellen Konzerne sicher, dass die NIS-2-Anforderungen in allen Konzernunternehmen einheitlich umgesetzt werden? Das ist besonders für Unternehmen relevant, die in verschiedenen Ländern tätig sind und den jeweiligen Landesvorschriften unterworfen sein könnten.

Grundsätzlich gilt: Übt ein Unternehmen in einem der in den Anlagen genannten Sektoren eine Tätigkeit aus, so unterliegt es mit Übertreten der definierten Schwellwerte den Anforderungen der NIS-2-Umsetzung. Ob der gesamte Konzern oder nur ein Tochterunternehmen von den Anforderungen betroffen ist, hängt von der Eigenständigkeit der jeweiligen Unternehmensteile ab. Kann die Unabhängigkeit eines Unternehmens vom Konzern nachgewiesen werden, so sind die Zahlen des Tochterunternehmens maßgeblich. Hier sind dann entsprechend die Vorschriften des EU-Landes relevant, in dem das Tochterunternehmen seinen Hauptsitz hat. Man unterstellt, dass dort die Entscheidungen zu Maßnahmen im Cybersicherheitsrisikomanagement getroffen werden. Gelten die jeweiligen Vorschriften eines anderen EU-Mitgliedsstaates, so sind diese gesondert zu überprüfen, da sie wegen des Mindestharmonisierungsprinzips schärfer gefasst sein können als die Vorgaben der NIS-2 selbst.

Um also sicherzustellen, dass sich die tatsächlich betroffenen Unternehmensbereiche bei der jeweils zuständigen Stelle melden und registrieren, muss zuerst deren Betroffenheit und die Verbundenheit überprüft werden, um dann nach dem Gesetz die jeweilige Zuständigkeit zu ermitteln. Darauf basierend kann man dann analysieren, welche Vorgaben welches EU-Landes für welche Unternehmensteile relevant sind.

Welche Rolle spielen die einzelnen Unternehmensbereiche (z. B. IT, Rechtsabteilung) bei der Erfüllung der NIS-2-Anforderungen in einem Konzern?

Generell zielt die ganzheitliche Unternehmensbetrachtung darauf ab, dass die Relevanz aller Unternehmensbereiche deutlich gemacht wird. Der Scope kann nicht mehr auf die IT, die für eine bestimmte Dienstleistung oder Leistung genutzt wird, beschränkt werden. Vielmehr sind sämtliche IT-Prozesse, die das Unternehmen nutzt, in die Umsetzung der Anforderungen einzubinden.

Damit meint der Gesetzgeber konkret alle Aktivitäten, die ein Unternehmen unternimmt, um seine Dienste zu erbringen. Das ist eine große regulatorische Veränderung. Viele Unternehmen stehen damit vor der Herausforderung, entweder ein bereits bestehendes ISMS nun unternehmensweit auszurollen oder aber ein ISMS über das gesamte Unternehmen hindurch neu zu etablieren.

Das Thema BCM (Business Continuity Management) ist entscheidend, wobei alle relevanten Stakeholder zur BIA (Business Impact Analyse) beitragen müssen. Verantwortliche für BCM, IT-Sicherheit, ISMS und (IT-)Risikomanagement müssen zusammenarbeiten, um die Unternehmensrisiken einheitlich abzubilden. Eine wichtige Rolle spielen auch Compliance-Beauftragte und der Einkauf, der für den Incident Management Prozess geschult werden muss. Meiner Meinung nach liegt genau in diesem Umstand der große Erfolgsfaktor der NIS-2: Gefordert wird ein unternehmensweites einheitliches Verständnis, eine einheitliche Awareness, um den aktuellen und künftigen Bedrohungen in der Cyberwelt begegnen zu können. Das Einfallstor für eine Bedrohung kann sowohl in der IT als auch in der OT (Operative Technologie bzw. Betriebstechnologie) liegen. Wo der Vorfall auftritt, ist so betrachtet nicht relevant – getroffen ist getroffen.

Welche Rolle spielt das „Einfallstor“ Rechenzentrum?

Mit dem „Einfallstor“ ist gemeint, dass oft vergessen wird, dass eigens betriebene Rechenzentren, unter die in Anlage 1 genannte wirtschaftliche Tätigkeit fallen. Unternehmen, die ein eigenes Rechenzentrum ausschließlich für ihre eigene IT betreiben, sind von diesen Vorschriften ausgenommen. Die Unabhängigkeit des Rechenzentrums muss jedoch genau überprüft werden.

Damit soll verhindert werden, dass Unternehmen ihre Rechenzentren in Tochterunternehmen ausgliedern. Existiert in einem Konzern eine Tochtergesellschaft, die ein Rechenzentrum für die anderen Gesellschaften desselben Konzerns betreibt, so greift die Ausnahmeregelung nicht mehr. Denn in diesem Fall liegt ein verbundenes Unternehmen vor und das ausgegliederte Unternehmen gilt als Betreiber eines Rechenzentrums und ist damit betroffen.

Was hat es mit der NIS-2-Anwendbarkeit und Nebentätigkeiten auf sich?

Maßgeblich für die Betroffenheit ist nicht das Kerngeschäft, sondern alle wirtschaftlichen Tätigkeiten eines Unternehmens. Fällt ein Unternehmensbereich unter die in der NIS-2 genannten Tätigkeiten, so gilt das gesamte Unternehmen als betroffen. Deshalb sollte eine Betroffenheitsanalyse besser nicht anhand eines Standard-Formulars durchgeführt werden. Denn es ist wichtig, wirklich genau hinzusehen und einer strukturierten Analyse zu folgen.

NIS-2 & Konzernstrukturen

- **Zuständigkeit:** Hängt von der Eigenständigkeit der Unternehmensteile ab; Vorschriften des EU-Landes, in dem der Hauptsitz oder die Entscheidungsstelle liegt.
- **Ganzheitlicher Ansatz:** Einbindung aller Unternehmensbereiche (IT, Rechtsabteilung, Management) in die Umsetzung der Anforderungen.
- **Wichtig:** Unabhängigkeit von Tochtergesellschaften muss nachgewiesen werden, um verschiedene regulatorische Vorgaben zu beachten.

NIS-2 & Outsourcing

Wie wirkt sich Outsourcing auf die Erfüllung der NIS-2-Anforderungen aus?

Outsourcing im Sinne von „ich gründe ein eigenes Unternehmen und habe so kleinere Werte und Zahlen, die ich zur Bewertung heranziehen muss und kann so Unternehmensteile von der Erfüllung der Anforderungen umgehen“ wird nicht funktionieren. Die NIS-2 zielt genau darauf ab, das zu unterbinden. Beim tatsächlichen Outsourcing kommt die differenzierte Supply-Chain-Security ins Spiel. Unternehmen müssen analysieren, welche Tätigkeiten ausgelagert sind, wie relevant und kritisch diese für ihre Betriebsfähigkeit sind und eine Risikoanalyse durchführen. Die Ergebnisse sollten in Anforderungen übersetzt werden, die regelmäßig überprüft und vertraglich festgehalten werden.

NIS-2 & Outsourcing

- **Vermeidung von Umgehung:** Outsourcing zur Umgehung der NIS-2-Anforderungen ist nicht zulässig.
- **Supply-Chain-Security:** Detaillierte Analyse der ausgelagerten Tätigkeiten und deren Kritikalität für die Betriebsfähigkeit.
- **Maßnahmen:** Ergebnisbasierte Anforderungen formulieren und regelmäßig überprüfen, um Compliance sicherzustellen.

VICCON begleitet Unternehmen, öffentliche Einrichtungen und KRITIS-Betreiber seit 25 Jahren bei der Umsetzung von Informations- und Cybersicherheit. Durch maßgeschneiderte Lösungen optimiert VICCON Geschäftsprozesse, stärkt die Resilienz und ermöglichen Compliance für regulatorische Anforderungen. Mehr Informationen unter www.viccon.de

VICCON CONSULTING

Was verbirgt sich hinter der NIS-2 Richtlinie?

Die NIS-2-Richtlinie, kurz für „Network and Information System Security“, ist ein wichtiger Schritt der Europäischen Union zur Stärkung der Cybersicherheit in ihren Mitgliedstaaten. Sie ersetzt ihre Vorgängerin, die NIS-Richtlinie, und führt eine Reihe neuer und verschärfter Anforderungen ein.

Hintergrund und Ziele:
Die zunehmende Digitalisierung und die wachsende Abhängigkeit von digitalen Technologien haben die Bedrohung durch Cyberangriffe deutlich erhöht. Kritische Infrastrukturen wie Energieversorgung, Verkehr, Gesundheitswesen und Finanzdienstleistungen sind besonders gefährdet. **Die NIS-2-Richtlinie wurde entwickelt, um**

- **ein höheres Maß an Cybersicherheit zu gewährleisten:** Durch die Einführung strengerer Anforderungen sollen Unternehmen und Organisationen besser gegen Cyberangriffe geschützt werden.
- **ein einheitliches Sicherheitsniveau in der EU zu schaffen:** Die Richtlinie soll dazu beitragen, dass alle EU-Mitgliedstaaten vergleichbare Cybersicherheitsstandards umsetzen.
- **die Zusammenarbeit zwischen den Mitgliedstaaten zu verbessern:** Durch einen verstärkten Informationsaustausch und eine bessere Koordination sollen die Mitgliedstaaten gemeinsam gegen Cyberbedrohungen vorgehen.

Kernpunkte der NIS-2-Richtlinie:

- **Erweiterter Anwendungsbereich:** Die NIS-2-Richtlinie deckt eine größere Anzahl von Sektoren und Unternehmen ab als ihre Vorgängerin.
- **Verschärfte Anforderungen:** Unternehmen müssen umfassende Risikoanalysen durchführen, Vorfallmanagementpläne erstellen und ihre IT-Systeme regelmäßig überprüfen.
- **Meldepflicht:** Unternehmen sind verpflichtet, bestimmte Cyberangriffe den zuständigen Behörden zu melden.
- **Zusammenarbeit mit Behörden:** Unternehmen müssen bei der Bekämpfung von Cyberangriffen eng mit den zuständigen Behörden zusammenarbeiten.
- **Verschärfte Sanktionen:** Unternehmen, die gegen die NIS-2-Richtlinie verstoßen, müssen mit hohen Geldstrafen rechnen.

Warum ist die NIS-2-Richtlinie wichtig?

- **Schutz kritischer Infrastrukturen:** Durch die NIS-2-Richtlinie werden kritische Infrastrukturen besser geschützt und die Widerstandsfähigkeit der EU gegen Cyberangriffe erhöht.
- **Stärkung der Wirtschaft:** Eine sichere digitale Infrastruktur ist eine Voraussetzung für eine funktionierende Wirtschaft.
- **Schutz der Bürger:** Durch die NIS-2-Richtlinie werden die persönlichen Daten der Bürger besser geschützt.

Die NIS-2-Richtlinie ist ein wichtiger Schritt zur Stärkung der Cybersicherheit in Europa. Sie stellt Unternehmen und Organisationen vor neue Herausforderungen und bietet ihnen gleichzeitig die Chance, ihre Widerstandsfähigkeit gegen Cyberangriffe zu erhöhen.

Strategische Bedeutung für die Unternehmenssicherheit

Die NIS-2-Richtlinie stellt für Unternehmen einen wichtigen strategischen Meilenstein in der Cybersicherheit dar. Sie fordert Unternehmen auf, ihre Cybersicherheitsstrategien grundlegend zu überdenken und proaktive Maßnahmen zu ergreifen. Neben der gesetzlichen Verpflichtung bringt NIS-2 entscheidende Vorteile für die Unternehmenssicherheit mit sich, die weit über die Erfüllung von Vorschriften hinausgehen.

Die strategische Bedeutung von NIS-2 liegt im Reputationsmanagement. Ein erfolgreicher Cyberangriff kann den Ruf eines Unternehmens massiv schädigen und das Vertrauen der Kunden zerstören. NIS-2 verpflichtet Unternehmen dazu, proaktive Maßnahmen zu ergreifen, um solche Risiken zu minimieren und ihr Image zu schützen. Die Richtlinie fördert eine umfassende Risikoanalyse und einen robusten Vorfallmanagementplan, die für den Schutz der Unternehmensreputation von entscheidender Bedeutung sind.

Die NIS-2-Richtlinie hat auch weitreichende Auswirkungen auf die Geschäftskontinuität. Durch die Umsetzung der Richtlinie können Unternehmen ihre Widerstandsfähigkeit gegenüber Cyberangriffen deutlich erhöhen und ihre Geschäftsprozesse

vor möglichen Störungen schützen. Dies ist besonders wichtig in einer Zeit, in der Cyberbedrohungen immer komplexer und gefährlicher werden. Regelmäßige Updates, Backups und ein strukturierter Notfallplan sind daher unverzichtbare Bestandteile der Cybersicherheitsstrategie.

Darüber hinaus kann NIS-2 als Katalysator für Innovationen im Bereich der Cybersicherheit dienen. Unternehmen, die sich intensiv mit den Anforderungen der Richtlinie auseinandersetzen, können neue Technologien und Sicherheitslösungen nutzen, um ihre Systeme zu stärken. Diese proaktive Haltung verschafft ihnen nicht nur einen Wettbewerbsvorteil, sondern trägt auch zur kontinuierlichen Verbesserung der Sicherheitsstandards bei. Die Einhaltung von NIS-2 wird somit zu einem strategischen Vorteil, der Unternehmen nicht nur schützt, sondern auch ihre Marktposition stärkt.

„Kritische Infrastrukturen stehen besonders im Fokus, denn die Bedrohungslage ist real. Unternehmen, die ihre Risiken jetzt nicht umfassend managen, setzen nicht nur ihre Daten, sondern auch ihre Geschäftsfähigkeit aufs Spiel. Es geht nicht nur um Compliance – es geht um den Schutz unserer Wirtschaft und unserer Bürger.“

Florian Frisse, Partner und Rechtsanwalt, Schalast

Wichtige Neuerungen im Vergleich zur bisherigen NIS-Richtlinie

Die NIS-2-Richtlinie stellt eine Weiterentwicklung der ursprünglichen NIS-Richtlinie dar und bringt wesentliche Änderungen sowie neue Anforderungen mit sich. Im Vergleich zur bisherigen NIS-Richtlinie sind dies wichtige Neuerungen. Beide Richtlinien haben das klare Ziel, die Cybersicherheit in der Europäischen Union zu stärken und Unternehmen sowie Organisationen vor Cyberangriffen zu schützen.

Die digitale Transformation schreitet rasant voran und damit auch die Komplexität von Cyberbedrohungen. Wir müssen handeln, um unsere Systeme und Daten zu schützen. Um diesen Risiken entgegenzuwirken und kritische Dienste, sensible Informationen sowie das Wohl der Menschen und der Wirtschaft zu schützen, wurde die NIS-Richtlinie eingeführt.

Seit ihrer Einführung im Jahr 2018 wurde jedoch deutlich, dass die NIS-Richtlinie nicht einheitlich in den Mitgliedstaaten umgesetzt wurde. Dies führte zu einem ineffizienten, fragmentierten System. Die daraus resultierenden Unzulänglichkeiten machten eine Überarbeitung notwendig, um aktuelle Anforderungen des Marktes zu berücksichtigen und eine detailliertere, verbesserte Rechtsvorschrift zu schaffen.

Die neue NIS-2-Richtlinie erweitert den Anwendungsbereich und **enthält strengere Meldepflichten sowie erhöhte Sanktionen. Sie fordert umfassendere Maßnahmen zur Cybersicherheit und stärkt die persönliche Haftung der Geschäftsleitung. Zusätzlich etabliert sie neue Mechanismen zur Koordinierung und Zusammenarbeit auf europäischer Ebene.** Die Umsetzung der NIS-2-Richtlinie wird nicht ausschließlich im BSIG vollzogen. Beispielsweise wird auch das TKG eine Novellierung erfahren. So werden sich u. a. der zu ergreifende Maßnahmenkatalog in § 165 TKG-E und das Meldeverfahren in § 168 TKG-E wiederfinden.

Die folgende Tabelle bietet einen detaillierten Vergleich der wichtigsten Neuerungen der NIS-2-Richtlinie im Vergleich zur ursprünglichen NIS-Richtlinie:

	NIS-Richtlinie	NIS-2-Richtlinie
Anwendungsbereich	Betreiber wesentlicher Dienste, Anbieter digitaler Dienste	Erweiterung auf zusätzliche Sektoren wie chemische Industrie, medizinische Geräte, Lebensmittelverarbeitung, soziale Netzwerke. Neue Begriffe: „wesentliche Einrichtungen“ und „wichtige Einrichtungen“
Cybersecurity-Maßnahmen	Grundlegende Maßnahmen zur Sicherstellung der Cybersicherheit	Erweiterte Maßnahmen einschließlich Risikomanagement, Business Continuity, Sicherheit der Lieferkette, Cyberhygiene, Kryptografie und mehr
Meldepflichten	Signifikante Vorfälle melden, zeitliche Vorgaben nicht spezifiziert	Strengere Meldepflichten: Erstmeldung innerhalb 24 Stunden, detaillierte Meldung innerhalb 72 Stunden, Abschlussmeldung innerhalb eines Monats
Sanktionen	Nationale Sanktionen, keine einheitlichen Vorgaben	Höhere Geldstrafen: bis zu 10 Millionen Euro oder 2 % des weltweiten Umsatzes für wesentliche Einrichtungen; bis zu 7 Millionen Euro oder 1,4 % des weltweiten Umsatzes für wichtige Einrichtungen
Haftung	Keine spezifischen Regelungen zur Haftung der Geschäftsleitung	Persönliche Haftung der Geschäftsleitung für die Umsetzung von Cybersicherheitsmaßnahmen
Zertifizierungen	Keine expliziten Vorgaben, teilweise nationale Regelungen	Zunehmende Bedeutung von Audits und Zertifizierungen, Nachweispflicht für Betreiber kritischer Infrastrukturen und wesentlicher Einrichtungen gegenüber dem BSI alle drei Jahre
Sicherheit der Lieferkette	Keine spezifischen Anforderungen	Umfassende Anforderungen an die Sicherheit der Lieferkette, Einbeziehung der Sicherheitsaspekte der Beziehungen zu Lieferanten und Dienstanbietern
EU-CyCLONe	Nicht vorhanden	Einrichtung eines Europäischen Netzwerks für die Koordinierung von Cyberkrisen (EU-CyCLONe), Unterstützung der Länder bei der Bewältigung von Cyber-Sicherheitsvorfällen großen Ausmaßes
Peer Reviews	Nicht vorhanden	Einführung von freiwilligen Peer Reviews zur Verbesserung der Cybersicherheit und zum Austausch bewährter Verfahren zwischen den Mitgliedstaaten
Cyberhygiene	Keine spezifischen Regelungen	Einführung von Maßnahmen zur Cyberhygiene, einschließlich regelmäßiger Software-Updates, Passwortänderungen, Netzwerksegmentierung und Schulungen für Mitarbeiter

Die NIS-2-Richtlinie ist ein wichtiger Schritt zur Stärkung der Cybersicherheit in der EU. Sie setzt neue Maßstäbe und fördert gleichzeitig die Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten. Unternehmen, insbesondere die KMUs, müssen sich auf höhere Anforderungen und mögliche Anpassungsbedarfe einstellen, um den neuen Vorgaben gerecht zu werden.

Umsetzung in nationales Recht

Am 7. Mai 2024 wurde in Deutschland der Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Stärkung der IT-Sicherheit in der Bundesverwaltung veröffentlicht. Das Bundeskabinett hat am 24. Juli 2024 den Entwurf eines Gesetzes zur Stärkung der IT-Sicherheit in Deutschland beschlossen. Der Gesetzesentwurf wurde seitens der Bundesregierung am 16. August 2024 dem Bundesrat zugeleitet. Die Umsetzung der NIS-2-Richtlinie soll insbesondere die Novellierung des bereits bestehenden BSIG erfolgen. Es ist unklar, ob das Gesetzgebungsverfahren bis zum Stichtag im Oktober 2024 abgeschlossen sein wird. Der BMI-Zeitplan sieht ein Inkrafttreten im März 2025 vor. In der deutschen Version der NIS2-Richtlinie ist von "wesentlichen Einrichtungen" und "wichtigen Einrichtungen" die Rede.Im deutschen Regierungsentwurf wird der Begriff der "wesentlichen Einrichtungen" durch den der "besonders wichtigen Einrichtungen" ersetzt.

Die Debatten in Deutschland machen deutlich, dass die Umsetzung der NIS-2-Richtlinie in nationales Recht ein komplexer und zeitaufwendiger Prozess ist. Einige EU-Mitgliedstaaten sind bereits deutlich weiter als Deutschland.

Der Regierungsentwurf eines Gesetzes der Bundesregierung zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz; Drs. 380/24) enthält eine Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG) sowie Änderungen einer Vielzahl weiterer Bundesgesetze (u. a. des BND-Gesetzes, des Telekommunikationsgesetzes, des Hinweisgeberschutzgesetzes, des Energiewirtschaftsgesetzes, Teile des Sozialgesetzbuchs, der Außenwirtschaftsverordnung u. v. m.).

Die nachfolgenden Ausführungen enthalten ausschließlich die (für Unternehmen relevantesten) im BSI-Gesetzentwurf (BSIG-E) enthaltenen Regelungen (aus Teil 3, Kapitel 1 und 2):

Zuständige Behörde und zentrale Meldestelle
§ 3 BSIG-E regelt umfassend die Aufgaben des **Bundesamtes für Sicherheit in der Informationstechnik (BSI), das nach § 4 BSIG-E die zentrale Meldestelle für die Zusammenarbeit der Einrichtungen** der Bundesverwaltung in Angelegenheiten der Sicherheit in der Informationstechnik darstellt und nach § 5 BSIG-E als zentrale Stelle für Meldungen von Dritten Informationen über Sicherheitsrisiken in der Informationstechnik entgegennimmt und diese Informationen auswertet.

Nach § 40 Absatz 1 BSIG-E ist das BSI zudem nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für die Aufsicht für besonders wichtige sowie wichtige Einrichtungen.

Sektoren besonders wichtiger und wichtiger Einrichtungen
In den Anlagen 1 und 2 zum BSIG-E werden die **Sektoren besonders wichtiger und wichtiger Einrichtungen** (Anlage 1) **sowie (nur) wichtiger Einrichtungen** (Anlage 2) **unter Unterteilung in Branchen und Einrichtungsarten geregelt,** wobei der Entwurf die in der NIS-2-Richtlinie genannten Sektoren-Begriffe teilweise konsolidiert. In Anlage 1 werden die Sektoren Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, Digitale Infrastruktur und Weltraum verortet, in Anlage 2 die Sektoren Transport und Verkehr, Abfallbewirtschaftung, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Verarbeitendes Gewerbe/Herstellung von Waren, Anbieter digitaler Dienste und Forschung.

„NIS-2 bringt mehr als nur Pflichten – sie ist eine Chance für Unternehmen, ihre Cyber-Resilienz zu stärken und Vertrauen bei Kunden sowie Partnern langfristig zu sichern.“

Micheal Scheffler, VP Sales, Link11

Wichtige und besonders wichtige Einrichtungen
Die von der NIS-2-Richtlinie geforderte sog. **„Size-Cap-Rule“**, nach der einheitliche Identifikationskriterien auf Grundlage der Unternehmensgröße für alle EU-Mitgliedstaaten definiert werden, **soll folgendermaßen umgesetzt werden**:

In § 28 BSIG-E werden wichtige und besonders wichtige Einrichtungen wie folgt definiert

Gemäß § 28 Abs. 1 Satz 1 BSIG-E gelten als besonders wichtige Einrichtung

1. Betreiber kritischer Anlagen,
2. qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter,
3. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die a) mindestens 50 Mitarbeiter beschäftigen oder b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen,
4. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind und die a) mindestens 250 Mitarbeiter beschäftigen oder Drucksache 380/24 - 32 - b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.

Als wichtige Einrichtungen gelten gem. § 28 Abs. 1 Satz 1 BSIG-E

Gemäß § 28 Abs. 1 Satz 1 BSIG-E gelten als besonders wichtige Einrichtung

1. Vertrauensdiensteanbieter,
2. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die a) weniger als 50 Mitarbeiter beschäftigen und b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen,
3. natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen sind und die a) mindestens 50 Mitarbeiter beschäftigen oder b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.

13

Die folgende Grafik zeigt Ihnen auf einen Blick, welche Gruppen betroffen sind, und welche Kriterien gelten:

Verpflichtendes Risikomanagement
Der BSIG-Entwurf sieht ein umfassendes, verpflichtendes Risikomanagement vor, wobei die Systeme grundsätzlich den Stand der Technik einzuhalten haben.

Besonders wichtige Einrichtungen und wichtige Einrichtungen sind gemäß § 30 Abs. 1 Satz 1 BSIG-E **verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.** § 30 Abs. 2 BSIG-E konkretisiert Mindeststandards, u. a. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik (Nr. 1), die Bewältigung von Sicherheitsvorfällen (Nr. 2) und die Sicherheit der Lieferkette (Nr. 4).

Für Betreiber kritischer Anlagen gelten nach § 31 Absatz 1 BSIG-E **besondere Anforderungen an die Risikomanagementmaßnahmen.** So soll für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, im Vergleich zu anderen informationstechnischen Systemen, Komponenten und Prozessen besonders wichtiger Einrichtungen ein noch höheres Schutzniveau gelten, dessen Aufwand auch in der Verhältnismäßigkeit strenger zu bewerten sein wird.

Betreiber kritischer Anlagen sind außerdem nach § 31 Absatz 2 BSIG-E verpflichtet, Systeme zur Angriffserkennung einzusetzen, die geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten müssen. Die Systeme sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.

Die Umsetzung der Maßnahmen nach § 30 Absatz 1 Satz 1 in Verbindung mit § 31 Absatz 1 und 2 Satz 1 müssen Betreiber kritischer Anlagen dem Bundesamt nachweisen:

- zu einem vom Bundesamt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festgelegten Zeitpunkt, frühestens drei Jahre nachdem sie erstmals oder spätestens drei Jahre nachdem sie erneut als ein Betreiber einer kritischen Anlage gelten,
- und anschließend alle drei Jahre
- durch Sicherheitsaudits, Prüfungen oder Zertifizierungen gem. § 39 Abs. 1 Satz 1 BSIG-E.

Zeitkritische Melde- und Berichtspflichten sowie Unterrichtungspflichten

Besonders wichtige und wichtige Einrichtungen nach § 32 BSIG-E sind insbesondere verpflichtet,

- unverzüglich, spätestens jedoch **innerhalb von 24 Stunden nach Kenntniserlangung** von einem erheblichen Sicherheitsvorfall eine frühe Erstmeldung unter Abgabe einer Verdachtseinschätzung abzugeben,
- unverzüglich, spätestens jedoch **innerhalb von 72 Stunden** nach entsprechender Kenntniserlangung eine auf die Verdachtsmeldung bezogene **Meldung zur weiteren Bewertung** des erheblichen Sicherheitsvorfalls und
- spätestens **einen Monat nach Übermittlung** der Meldung des Sicherheitsvorfalls eine **Abschlussmeldung** abzugeben.
- Zudem muss auf Ersuchen des Bundesamtes eine Zwischenmeldung über relevante Statusaktualisierungen abgegeben werden.

§ 35 BSIG-E regelt Unterrichtungspflichten von besonders wichtigen und wichtigen Einrichtungen im Fall eines erheblichen Sicherheitsvorfalls gegenüber dem Bundesamt.

Selbsteinordnungspflicht und Registrierungspflicht
Nach § 33 BSIG-E sind besonders wichtige und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter verpflichtet, sich spätestens drei Monate, nachdem sie erstmals oder erneut als eine der vorgenannten Einrichtungen gelten oder Domain-Name-Registry-Dienste anbieten, dem Bundesamt über eine dafür eingerichtete Registrierungsmöglichkeit unter Selbsteinordnung in die entsprechenden Kategorien zu registrieren.

Bestimmte Einrichtungsarten (DNS-Diensteanbieter, Top Level Domain Name Registries, Domain-Name-Registry-Dienstleister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider sowie für Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke) **unterliegen nach § 34 BSIG-E einer besonderen Registrierungspflicht.**

Ausnahmemöglichkeiten
Nach § 37 Absatz 1 BSIG-E kann sich eine besonders wichtige Einrichtung oder eine wichtige Einrichtung von Verpflichtungen nach diesem Gesetz nach in Absatz 2 genannten Maßgaben teilweise befreien (einfacher Ausnahmebescheid) oder nach Maßgabe des Absatzes 3 insgesamt befreien lassen (erweiterter Ausnahmebescheid), sofern die Einrichtung Vorgaben einhält, die den Verpflichtungen nach diesem Gesetz gleichwertig sind.

Umfassende Pflichten und Haftung für Geschäftsleitungen
Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen sind nach § 38 Absatz 1 BSIG-E **persönlich verpflichtet,** die von diesen Einrichtungen nach § 30 zu ergreifenden Risiko**managementmaßnahmen umzusetzen** und ihre Umsetzung **zu überwachen.**

Geschäftsleitungen, die diese Pflichten verletzen, haften nach § 38 Absatz 2 BSIG-E ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts.

Geschäftsleitungen sind nach § 38 Absatz 3 BSIG-E zudem **verpflichtet, regelmäßig an Schulungen teilzunehmen.**

Bußgeldvorschriften
Die Bußgeldtatbestände des § 65 BSIG-E sehen Bußgelder bis zu 10 Millionen Euro oder 2% des weltweiten Umsatzes für besonders wichtige Einrichtungen und bis zu 7 Millionen Euro oder 1,4% des weltweiten Umsatzes für wichtige Einrichtungen vor.

Festlegung kritischer Anlagen durch Rechtsverordnung
Nach § 56 Absatz 4 i.V.m. § 2 Nr. 22 BSIG-E wird durch Rechtsverordnung festgelegt, welche Anlagen als kritische Anlagen gelten.

Haftungsrisiken und rechtliche Konsequenzen bei Nichteinhaltung

Die Nichteinhaltung von Pflichten aus der Umsetzung von NIS-2 hat weitreichende Konsequenzen.

Erhöhung der Bußgelder: Wesentliche Einrichtungen müssen bei Verstößen mit Bußgeldern bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes rechnen, es gilt der höhere Betrag. Für wichtige Einrichtungen können die Strafzahlungen bis zu 7 Millionen Euro oder 1,4 % des weltweiten Jahresumsatzes betragen, es gilt der höhere Betrag.

Haftung der Geschäftsleitung: Die ausdrücklichen Pflichten für Geschäftsleitungen in § 38 BSIG-E sollen nach dem Willen des Gesetzgebers auch zu einer entsprechenden Haftung bei Nichterfüllung führen. Das BSIG-E verweist auf die für die entsprechende Rechtsform der Einrichtung geltenden Regeln des Gesellschaftsrechtes. Besonders relevant kann hier die Haftung mit dem Privatvermögen gegenüber der Gesellschaft werden (z. B. nach § 43 GmbHG bzw. § 93 AktG).

Verweigert die Geschäftsleitung die Teilnahme an Schulungen trotz Fristsetzung, so kommt nach § 61 Abs. 9 BSIG-E sogar zeitweise eine behördliche Untersagung der Tätigkeitsausübung in Betracht.

Neue Compliance-Anforderungen und ihre Bedeutung

Die NIS-2-Richtlinie stellt neue Maßstäbe an die Compliance-Anforderungen der von ihr betroffenen Unternehmen. Hierbei werden sich insbesondere viele der KMU erstmalig mit Compliance-Anforderungen konfrontiert sehen. Um etwaige Bußgeldzahlungen, Aufsichtsmaßnahmen oder die private Haftung der Geschäftsführung zu vermeiden, ist die Implementierung einer hinreichend aufgestellten Compliance-Abteilung unabdingbar. Hierbei muss beispielsweise der vom Gesetzgeber vorgesehene Meldeprozess nach § 32 BSIG-E genaustens eingehalten werden. Damit die Meldung ordnungsgemäß gelingt, gerade in der belastenden Situation eines (erfolgreichen) Cyberangriffs, ist die genaue Planung und Implementierung der zu ergreifenden Maßnahmen erforderlich.

Best Practice – ein 5-Stufen-Plan zur Umsetzung

Die erforderlichen Handlungsschritte lassen sich in der Regel für die meisten Betroffenen zu diesen 5 Stufen zusammenfassen:

1. Frühzeitige Klärung der Rollen und Verantwortlichkeiten der einzelnen Stakeholder im Prüfungs- und Umsetzungsprozess unter frühzeitiger Einbindung der unternehmensintern Verantwortlichen für Informations-, IT- und Cybersicherheit,
2. Identifikation relevanter Regelungen und Schwellenwerte zur Selbsteinordnung des Unternehmens und der Tätigkeiten, sowie Durchführung der Registrierung
3. Einrichtung und regelmäßige Aktualisierung der erforderlichen Cybersecurity-Schutzmaßnahmen
4. Durchführung von Feuerproben zur praktischen Überprüfung der getroffenen Cybersecurity-Schutzmaßnahmen (an den Faktor Mensch denken)
5. Stetiges Überwachen und Vorantreiben des Prozesses durch die Geschäftsleitung

Bei der Implementierung des neuen Rechtsrahmens ist die Auswahl geeigneter Rechtsberater und externer Unterstützung von besonderer Bedeutung. Ist ein passendes Beraterteam gefunden, sollten diesem schnellstmöglich die angefragten Unterlagen und Daten zur Verfügung gestellt werden.

DORA und NIS-2: Was sind die Unterschiede?

Die DORA-Verordnung (Digital Operational Resilience Act) und die NIS-2 haben auf den ersten Blick ähnliche Ziele – nämlich den Schutz vor Cyberrisiken und die Erhöhung der Resilienz gegenüber IT-Störungen. Doch unterscheiden sie sich deutlich in ihrem Anwendungsbereich und ihren Anforderungen. Während die **NIS-2 auf eine Vielzahl von Wirtschaftssektoren abzielt und sich mit der Cybersicherheit von Netz- und Informationssystemen beschäftigt, fokussiert sich die DORA ausschließlich auf den Finanzsektor und legt den Schwerpunkt auf die operative Widerstandsfähigkeit.**

Das Instrumentarium der DORA umfasst u. a. durchzuführende IT-Stresstests oder auch das Management von Drittanbietern. Zum regulierten Finanzsektor gehören beispielsweise: Banken, Versicherungen, Investmentgesellschaften, Zahlungsdienstleister und Finanzinfrastrukturen wie Börsen, Clearinghäuser und Finanzmarktinfrastrukturen. Die **DORA-Verordnung gilt zudem auch für IT-Dienstleister, die für Finanzinstitute arbeiten, einschließlich Cloud-Anbieter und IT-Sicherheitsdienstleister.** Ein wesentlicher Unterschied liegt darin, dass die **DORA als Verordnung unmittelbar rechtliche Wirkung in den einzelnen EU-Mitgliedsstaaten entfaltet.** Anders ist dies bei einer Richtlinie, wie NIS-2. Hier bedarf es eines nationalen Umsetzungsaktes, was häufig zu Verzögerungen in den einzelnen Mitgliedsstaaten führt.

Seitenblick auf andere EU-Staaten

Felder anklicken für mehr Informationen

NIS-2 ist in nationales Recht umgesetzt

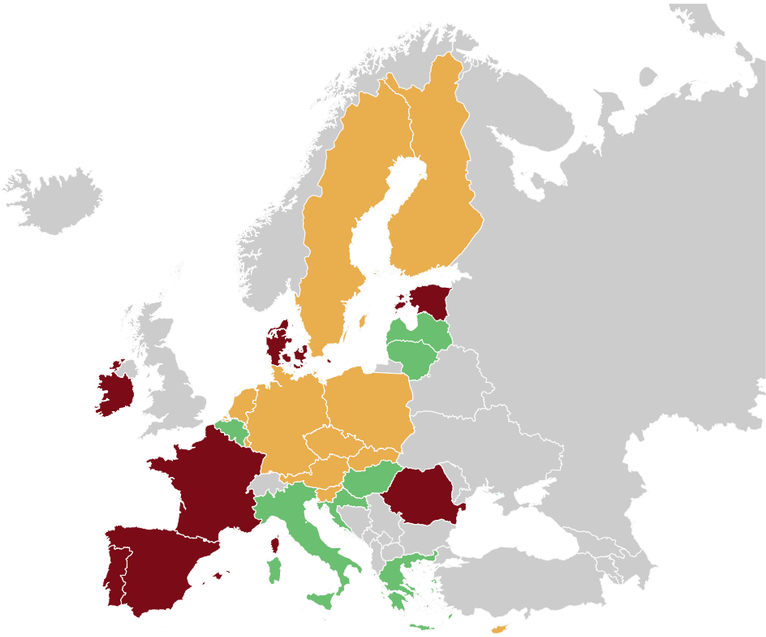
NIS-2 im Gesetzgebungsverfahren

NIS-2-Umsetzung: Erste Schritte und Verzögerungen

NIS-2 ist in nationales Recht umgesetzt

NIS-2 im Gesetzgebungsverfahren

NIS-2-Umsetzung: Erste Schritte und Verzögerungen



Hinweis: Diese Informationen basieren auf den zum Druckzeitpunkt zur Verfügung stehenden Daten und können sich inzwischen verändert haben.

Technische Maßnahmen und Sicherheitsstrategien

Eine erfolgreiche Cybersicherheitsstrategie beginnt zwingend mit einer gründlichen Risikobewertung. Unternehmen müssen ihre kritischen Assets, Prozesse und Systeme identifizieren und die potenziellen Risiken bewerten, denen sie ausgesetzt sind. Unternehmen müssen Angriffsszenarien entwickeln, um ihre Abwehrmaßnahmen zielgerichtet anpassen zu können.

Technische Kontrollmaßnahmen für umfassenden Schutz
Um die Risiken zu minimieren, sind technische Kontrollmaßnahmen unerlässlich.

- **Zugriffskontrolle:** Sensible Daten und Systeme dürfen ausschließlich autorisierten Personen zugänglich gemacht werden. Eine starke Multi-Faktor-Authentifizierung und eine regelmäßige Überprüfung von Zugriffsrechten sind unerlässlich.
- **Netzwerksicherheit hat höchste Priorität:** DDoS-Schutz, Firewalls, Intrusion Detection and Prevention Systems (IDS) sowie eine strikte Netzwerksegmentierung schützen vor unbefugtem Zugriff und Datenverlust.
- **Endgerätesicherheit:** Durch regelmäßiges Patchen, den Einsatz von Virenschutzsoftware und Mobile Device Management (MDM) stellen wir sicher, dass die Sicherheit von Endgeräten gewährleistet ist.
- **Cloud-Sicherheit:** Die Migration in die Cloud erfordert besondere Aufmerksamkeit. Unternehmen müssen vertrauenswürdige Cloud-Anbieter auswählen und strenge Sicherheitsmaßnahmen für ihre Daten in der Cloud implementieren.
- **Sicherheitsbewusstsein:** Ein wichtiger Faktor für die Cybersicherheit ist ein geschultes Personal. Mitarbeitende müssen regelmäßig geschult und durch Phishing-Simulationen für die häufigsten Bedrohungen sensibilisiert werden.

Incident Response: Schnell und effektiv reagieren
Ein umfassender Incident-Response-Plan ist für den Ernstfall unerlässlich. Damit können Sie auf Cyberangriffe schnell und effektiv reagieren. Dieser Plan muss klare Verantwortlichkeiten, Eskalationswege und Wiederherstellungsprozesse definieren. Regelmäßige Simulationen sind unerlässlich, um die Effektivität des Plans zu überprüfen.

Unternehmen müssen über die eigenen Grenzen hinausdenken: Lieferketten und Mitarbeitende sind zentrale Faktoren.
Neben der Implementierung von Sicherheitskontrollen wie Netzwerksegmentierung, Multi-Faktor-Authentifizierung und Endpoint Detection and Response **müssen Unternehmen auch ihre Lieferketten sichern. Unternehmen müssen potenzielle Schwachstellen in ihren Lieferketten identifizieren und minimieren, indem sie strenge Sicherheitsanforderungen in Verträge mit Drittanbietern einbinden und regelmäßige Risikobewertungen durchführen.** Hierbei dürfte die Aufnahme einer undetaillierten Klausel, wonach der Vertragspartner auf die Einhaltung definierter Standards verpflichtet wird, nicht ausreichend sein, um sich einer Haftung zu entziehen. Gleiches dürfte für vertragliche Regelungen gelten, wonach der Vertragspartner lediglich zum Nachweis von Zertifikaten oder der Abgabe von Erklärungen über die Einhaltung der Vorschriften, ohne jede Prüfung und Überwachung, verpflichtet wird.

Compliance-Management: Kontinuierliche Verbesserung: Ein effektives Compliance-Management ist erforderlich, um die Compliance mit der NIS-2-Richtlinie sicherzustellen. **Unternehmen müssen ihre Sicherheitsmaßnahmen lückenlos dokumentieren, regelmäßig Audits durchführen und kontinuierlich an der Verbesserung ihrer Sicherheitsprozesse arbeiten.**

„Indem Unternehmen die NIS-2-Richtlinie als Chance zur Stärkung ihrer Cybersicherheit betrachten, können sie nicht nur gesetzliche Anforderungen erfüllen, sondern auch ihren Wettbewerbsvorteil sichern.“

Jens-Philipp Jung, CEO, Link11

Die Einhaltung der Datenschutz-Grundverordnung (DSGVO) ist von entscheidender Bedeutung, da sie eng mit der NIS-2-Richtlinie verzahnt ist. Unternehmen können die Anforderungen der NIS-2 und der DSGVO gleichermaßen erfüllen, indem sie technische Maßnahmen zur Gewährleistung des Datenschutzes umsetzen.

Cybersicherheit 4.0
Die Rolle von KI und Automatisierung: Unternehmen sollten in Technologien wie Künstlicher Intelligenz (KI) und Machine Learning (ML) investieren, um ihre Resilienz gegen Cyberangriffe zu erhöhen. Diese Technologien erkennen Anomalien und automatisieren Sicherheitsaufgaben. KI und ML bieten neue Möglichkeiten, um die Cybersicherheit entscheidend zu verbessern. KI-basierte Systeme erkennen Anomalien im Netzwerkverkehr und melden verdächtige Aktivitäten automatisch.

Die Cybersicherheitslandschaft entwickelt sich rasant weiter. Unternehmen müssen daher zwingend ihre Sicherheitsmaßnahmen kontinuierlich überprüfen und anpassen. Die Umsetzung der NIS-2-Richtlinie erfordert eine ganzheitliche Sicherheitsstrategie – ohne Wenn und Aber. **Unternehmen können ihre Widerstandsfähigkeit gegen Cyberangriffe deutlich erhöhen und die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten und Systeme gewährleisten – und zwar durch die Kombination von Technik, Organisation und einem starken Sicherheitsbewusstsein.** So sichern sie sich einen entscheidenden Wettbewerbsvorteil.

Empfehlungen für Entscheider:

Investitionen in Cybersecurity: Unternehmen dürfen nicht zögern, in Cybersicherheit zu investieren. Sie sollten ausreichend Ressourcen für den Aufbau und die Aufrechterhaltung einer robusten Cybersicherheit bereitstellen.

Kooperation: Eine enge Zusammenarbeit zwischen IT-Abteilung, Geschäftsführung und anderen relevanten Abteilungen ist entscheidend für den Erfolg von Cybersecurity-Initiativen.

Externe Expertise: Bei Bedarf sollten Unternehmen externe Experten hinzuziehen, um ihre Sicherheitsmaßnahmen zu bewerten und zu optimieren.

Fokus auf Risikobewusstsein: Risikobewusstsein fördern und kontinuierliche Verbesserungen in den Bereichen Cybersicherheit anstreben.

Langfristige Auswirkungen der NIS-2-Richtlinie

Die NIS-2-Richtlinie wird die europäische Cybersicherheit nachhaltig prägen. Sie führt zu einer Harmonisierung von Sicherheitsstandards in verschiedenen Branchen und fördert einen risikobasierten Ansatz, der Unternehmen dazu zwingt, ihre Sicherheitsmaßnahmen gezielter auf ihre spezifischen Bedrohungen auszurichten. **Die Förderung des Informationsaustausches und die Stärkung der Zusammenarbeit zwischen Unternehmen und Behörden werden dazu beitragen, dass die NIS-2 zu einer besseren gemeinsamen Lagebewertung und einer effizienteren Abwehr von Cyberbedrohungen führt.** Langfristig gesehen wird sie nicht nur die Sicherheit kritischer Infrastrukturen erhöhen, sondern auch das Vertrauen der Bürger in digitale Dienste stärken.

Die Umsetzung der NIS-2 stellt Unternehmen jedoch auch vor Herausforderungen. Eine effektive Sicherheitsstrategie umzusetzen, erfordert von Unternehmen eine langfristige Planung sowie die Bereitschaft, in entsprechende Maßnahmen zu investieren. Dabei spielen auch der Fachkräftemangel und die Notwendigkeit, sich an eine sich ständig verändernde Bedrohungslandschaft anzupassen, eine entscheidende Rolle. Unternehmen sehen sich zukünftig mit neuen Herausforderungen konfrontiert, beispielsweise mit der wachsenden Bedeutung von Cloud-Computing und der Entwicklung von Quantentechnologien. **Um diesen Herausforderungen zu begegnen, sind Investitionen in innovative Sicherheitslösungen sowie kontinuierliche Schulungen der Mitarbeitenden erforderlich.**

Die NIS-2-Richtlinie stellt einen Meilenstein in der europäischen Cybersicherheitslandschaft dar. Durch sich abzeichnende Veränderungen im Bereich der Cybersicherheit wird auch diese Richtlinie wieder an die sich ständig ändernde Bedrohungslage angepasst werden müssen. Zukünftige Anpassungen könnten folgende Aspekte umfassen:

- **Erweiterung des Anwendungsbereichs:** Die Richtlinie könnte auf weitere Sektoren ausgedehnt werden, die für kritische Infrastrukturen besonders relevant sind.
- **Verschärfung der Anforderungen an die Lieferkette:** Die Anforderungen an die Sicherheit der Lieferkette könnten verschärft werden, um Risiken durch Dritte zu minimieren.
- **Stärkerer Fokus auf Cloud-Sicherheit:** Angesichts der zunehmenden Bedeutung von Cloud-Diensten könnten die Anforderungen an die Cloud-Sicherheit erhöht werden.
- **Integration neuer Technologien:** Die Richtlinie sollte regelmäßig angepasst werden, um neue Technologien wie KI und Quantentechnologien angemessen zu berücksichtigen.

Cybersicherheit wird in Zukunft immer komplexer und dynamischer werden. Unternehmen müssen sich darauf einstellen, ihre Sicherheitskonzepte laufend anzupassen. Die NIS-2-Richtlinie bietet dafür einen wichtigen Rahmen, der künftig stärker dynamisiert werden dürfte. Doch auch sie wird an die neuen Herausforderungen angepasst werden müssen.

„Entscheider sollten die Cybersicherheit als strategische Investition betrachten und nicht nur als Kostenfaktor. Durch gezielte Investitionen in moderne Technologien, Schulungen und die Förderung einer starken Sicherheitskultur können Unternehmen ihre Widerstandsfähigkeit gegen Cyberangriffe signifikant erhöhen. Eine nachhaltige Cybersicherheit erfordert ein langfristiges Engagement auf allen Ebenen der Organisation.“

Janka Schwaibold, Rechtsanwältin & Partnerin, Schalast LAW | TAX

Fazit

Die NIS-2-Richtlinie stellt Unternehmen vor eine komplexe Herausforderung, bietet aber auch neue Chancen. **Sofern noch nicht geschehen, sollten Unternehmen umgehend prüfen, ob sie von der NIS-2-Richtlinie betroffen sind, indem sie ihre Zugehörigkeit zu den wesentlichen oder kritischen KRITIS-Sektoren überprüfen.** Dabei sind sowohl die spezifischen Sektor-Zuordnungen als auch die Schwellenwerte für die Unternehmensgröße zu beachten. **Darüber hinaus sollten Unternehmen ihre Lieferketten und Kundenbeziehungen evaluieren, da die Sicherheit der gesamten Lieferkette gemäß NIS-2 gewährleistet sein muss.**

Um die Anforderungen der Richtlinie zu erfüllen, müssen Unternehmen ihre Sicherheitsmaßnahmen grundlegend überdenken und anpassen. Der erste Schritt ist eine umfassende Risikoanalyse. Dabei gilt es, Schwachstellen in der IT-Infrastruktur, den Prozessen und der Lieferkette zu identifizieren und zu beheben. Die Implementierung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 kann dabei als Leitfaden dienen.

Die Umsetzung von NIS-2 erfordert die aktive Beteiligung des gesamten Unternehmens, insbesondere des Managements. Eine klare Kommunikation der Bedeutung von Cybersicherheit und die Bereitstellung der notwendigen Ressourcen sind entscheidend. Mitarbeitende müssen regelmäßig geschult werden, um das Sicherheitsbewusstsein zu stärken und menschliche Fehler zu minimieren.

Moderne Technologien wie Künstliche Intelligenz und maschinelles Lernen können Unternehmen bei der Umsetzung von NIS-2 unterstützen. Sie ermöglichen eine effizientere Erkennung von Bedrohungen und eine automatisierte Reaktion auf Sicherheitsvorfälle. Unternehmen sollten jedoch auch die mit neuen Technologien verbundenen Risiken im Auge behalten.

Die Zusammenarbeit mit externen Experten kann Unternehmen bei der Umsetzung von NIS-2 unterstützen. IT-Sicherheitsdienstleister und Anwaltskanzleien verfügen häufig über ein breites Fachwissen und Erfahrungen, die Unternehmen nicht immer intern vorhalten können.

Um die Anforderungen der NIS-2 zu erfüllen, sollten Unternehmen folgende Schritte unternehmen:

- **Risikobewertung:** Umfassende Analyse der eigenen IT-Landschaft und der Geschäftsprozesse.
- **ISMS einführen:** Ein ISMS nach ISO 27001 einführen oder an die Anforderungen von NIS-2 anpassen.
- **Mitarbeitende schulen:** Regelmäßige Cybersicherheitsschulungen durchführen.
- **Technologie nutzen:** Moderne Technologien wie KI und ML einsetzen.
- **Externe Experten hinzuziehen:** Unterstützung von IT-Sicherheitsdienstleistern und Beratern in Anspruch nehmen.
- **Kontinuierliche Verbesserung:** Regelmäßige Überprüfung und Anpassung der Sicherheitsmaßnahmen.

Die NIS-2-Richtlinie ist dynamisch. Unternehmen sollten sich darauf einstellen, dass sich die Anforderungen im Laufe der Zeit weiterentwickeln. Ein proaktiver und ganzheitlicher Ansatz ist daher unerlässlich, um die Cybersicherheit des Unternehmens langfristig zu gewährleisten und sich von der Konkurrenz abzuheben.

Kontakt

Michael Scheffler
Link11

m.scheffler@link11.com

Janka Schwaibold
Schalast LAW | TAX

janka.schwaibold@schalast.com

Florian Frisse
Schalast LAW | TAX

Florian.Frisse@schalast.com

Lorenz Haase
Schalast LAW | TAX

Lorenz.Haase@schalast.com

Sophia Zimmer
VICCON GmbH

s.zimmer@viccon.de

Hauptsitz

Link11
Lindleystr. 12
60314 Frankfurt