SOPHOS

NIS2-Richtlinie

Anforderungen – Auswirkungen – Eckdaten

Dieses Whitepaper wurde in Zusammenarbeit mit Rechtsanwalt Dr. David Bomhard von Noerr Partnerschaftsgesellschaft mbB erstellt.

Als Reaktion auf die erhöhte Bedrohungslage im Hinblick auf Cyberangriffe und die damit verbundene Erhöhung der (auch technischen) Anforderungen an die Abwehr solcher Vorfälle hat der europäische Gesetzgeber im Dezember 2022 die Network-and-Information-Security-Richtlinie 2.0 (Richtlinie (EU) 2022/2555, „NIS2-RL“) verabschiedet. Dadurch wurden die Anforderungen an die IT-Sicherheit in allen EU-Mitgliedstaaten erweitert und inhaltlich überarbeitet. Nicht zuletzt soll die IT-Sicherheitsgesetzgebung in der EU „zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft“ beitragen (vgl. Erwägungsgrund 1 NIS2-RL).

In diesem Whitepaper erfahren Sie, welche neuen und erweiterten Anforderungen die NIS2-RL für auf dem europäischen Markt tätige Unternehmen und andere Einrichtungen mit sich bringt und wie Sophos-Lösungen Sie bei der Implementierung der neuen Anforderungen unterstützen können.

Sophos-Whitepaper, April 2023

A. Hintergrund und wesentliche Inhalte der NIS2-RL

I. Roadmap: Von NIS1 über IT-SiG 2.0 zu NIS2

Mit der Network-and-Information-Security-Richtlinie (Richtlinie (EU) 2016/1148, „**NIS1-RL**") fanden ab 2016 auf EU-Ebene erste Vereinheitlichungsbestrebungen im Bereich der Cybersicherheit Eingang in die Rechtsordnungen der EU-Mitgliedstaaten. Diese hatte der deutsche Gesetzgeber 2017 vor allem durch das IT-Sicherheitsgesetz („**IT-SiG**") umgesetzt, soweit die Anforderungen nicht ohnehin bereits geltendes (nationales) Recht waren. 2021 hatte der deutsche Gesetzgeber losgelöst von europarechtlichen Vorgaben nachgelegt und mit dem IT-Sicherheitsgesetz 2.0 („**IT-SiG 2.0**") den Adressatenkreis betroffener Einrichtungen wesentlich erweitert.

Im Dezember 2022 haben der Rat und das Europäische Parlament die NIS2-RL verabschiedet und damit die Anforderungen an die Cybersicherheit in der gesamten EU überarbeitet und erweitert. Da es sich bei der NIS2-RL wiederum um eine Richtlinie handelt, ist sie (im Unterschied zur Verordnung) nicht unmittelbar in den Mitgliedstaaten anwendbar, sondern bedarf zunächst einer Transformation in nationales Recht. Der deutsche Gesetzgeber ist daher gehalten, die nationalen IT-Sicherheitsgesetze (insbesondere das BSIG) anzupassen. Der europäische Gesetzgeber gewährte den Mitgliedstaaten hierfür eine Umsetzungsfrist bis zum 17.10.2024.

Selbst wenn der deutsche Gesetzgeber diese Frist nicht ausreizen sollte, müssen Unternehmen und andere Einrichtungen sich erst ab dem 18.10.2024 auf eine Geltung der neuen Bestimmungen einstellen. Dennoch ist Unternehmen dringend zu empfehlen, bereits jetzt die neuen Anforderungen der NIS2-RL und ihre etwaigen Auswirkungen auf die jeweilige Einrichtung zu prüfen.

> Beispiel:
> *Durch die Erweiterung des Anwendungsbereichs der NIS2-RL gegenüber der bisherigen Rechtslage kann es passieren, dass ein bisher nicht den Anforderungen des IT-Sicherheitsrechts unterfallendes Unternehmen (oder eine Behörde) nunmehr doch im Bereich der Cybersecurity reguliert wird. Einem solchen Unternehmen bzw. einer solchen Behörde wäre dringend zu raten, zeitnah Implementierungsmaßnahmen und Auswirkungen auf Geschäftsprozesse bzw. Verwaltungsabläufe zu prüfen.*

II. Cybersicherheit als Managementaufgabe

Mit der NIS2-RL machte der europäische Gesetzgeber deutlich, dass er die Gewährleistung von Cybersicherheit und die Prävention von IT-Sicherheitsvorfällen als Aufgabe des obersten Managements jedes Unternehmens begreift. Gemäß Art. 20 Abs. 1 NIS2-RL müssen die „Leitungsorgane" die Einhaltung von Risikomanagementmaßnahmen (dazu unten IV.) überwachen und – noch bedeutender – können für Verstöße in diesem Bereich (persönlich) verantwortlich gemacht werden.

> Beispiel:
> *Dem Management eines Automobilkonzerns ist zu raten, die Implementierung von Maßnahmen zur Cybersicherheit nicht pauschal zu delegieren, sondern selbst die Umsetzung der gesetzlichen Anforderungen zu betreuen und zu überwachen. Denn eine Haftung für Verstöße gegen diese Vorgaben durch die jeweilige Einrichtung kann letztlich die Leitungspersonen selbst treffen.*

Nach Art. 32 Abs. 6 NIS2-RL gilt diese Konsequenz auch für die öffentliche Verwaltung, unbeschadet etwaiger nationaler Vorschriften über die Haftung von öffentlichen Bediensteten oder anderen Amtsträgern. Insoweit bleibt abzuwarten, wie die Mitgliedstaaten die Haftung der Leitungspersonen im Einzelnen umsetzen und ausgestalten werden.

Weitere Informationen zum Thema "Managementhaftung" erhalten Sie im Sophos-Whitepaper: Geschäftsführerhaftung bei Cyber-Angriffen

[1] NIS2UmsuCG = NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

III. Neuer erweiterter Anwendungsbereich der NIS2-RL

1. Erweiterung der regulierten Sektoren

Die NIS2-RL weitet den bisherigen Anwendungsbereich deutlich aus und erstreckt sich nun auf 18 Sektoren, sowohl im öffentlichen als auch im privaten Bereich.

> Beispiel:
> *Durch die NIS2-RL werden die erfassten Sektoren beispielsweise um die Luft- und Raumfahrt sowie auf kritische Dienste der öffentlichen Verwaltung ausgeweitet.*

Als europäische Richtlinie ist für die Anwendbarkeit der NIS2-RL ein gewisser Bezug zur EU erforderlich. Daher gilt die Richtlinie für Einrichtungen, die ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben. Unternehmen, die lediglich zuliefernde Tätigkeiten für ein europäisches Unternehmen erbringen, selbst aber keine Dienste in der EU erbringen oder Tätigkeiten in der EU ausüben, sind durch die NIS2-RL allenfalls mittelbar über konkrete Risikomanagementmaßnahmen betroffen (dazu s.u. IV.2.).

Die folgenden 18 Sektoren sind von der NIS2-RL erfasst:

SEKTOREN MIT HOHER KRITIKALITÄT (ANHANG I DER NIS2-RL):	SONSTIGE KRITISCHE SEKTOREN (ANHANG II DER NIS2-RL):
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschung
Digitale Infrastruktur	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

Durch die umfassendere Definition des Anwendungsbereichs obliegt die Festlegung relevanter Sektoren nicht mehr den Mitgliedstaaten, die Schwellenwerte der deutschen BSI-Kritisverordnung dürften daher bald Geschichte sein.

Die folgende Tabelle verdeutlicht die Erweiterung der Sektoren durch die NIS2-RL gegenüber der bisherigen Rechtslage:

NIS1-RL/BSI-KRITISVERORDNUNG	NIS2-RL
Energie	Energie
Wasser	Trinkwasser, Abwasser
Ernährung	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Informationstechnik und Telekommunikation	Digitale Infrastruktur
Gesundheit	Gesundheitswesen
Finanz- und Versicherungswesen	Bankwesen, Finanzmarktinfrastrukturen
Transport/Verkehr	Verkehr, Weltraum (teilweise), Post- und Kurierdienste,
Entsorgung	Abfallbewirtschaftung
	Verwaltung von IKT-Diensten (B2B)
	Öffentliche Verwaltung
	Produktion, Herstellung und Handel mit chemischen Stoffen
	Verarbeitendes Gewerbe/Herstellung von Waren
	Anbieter digitaler Dienste
	Forschung

Die NIS2-RL ist zunächst auf jede Einrichtung der in den Anhängen I und II der NIS2-RL genannten Sektoren anwendbar, die nach der Terminologie des Europarechts die Schwellenwerte für mittlere Unternehmen überschreitet. Das ist grundsätzlich dann der Fall, wenn die Einrichtung mindestens 50 Beschäftigte hat oder einen Jahresumsatz bzw. eine Jahresbilanzsumme von mehr als 10 Mio. EUR erzielt.

Unabhängig von ihrer Größe unterwirft Art. 2 Abs. 2–5 NIS2-RL bestimmte Einrichtungen explizit dem Anwendungsbereich der Richtlinie. Dazu gehören unter anderem Anbieter von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen Kommunikationsdiensten, außerdem bestimmte Einrichtungen der öffentlichen Verwaltung. Die Zahl der Beschäftigten sowie der Umsatz und die Bilanzsumme spielen insofern keine Rolle.

> Beispiel:
> *Auch im Gesundheitssektor werden durch die NIS2-RL fortan viel mehr Einrichtungen durch das EU-Cybersicherheitsrecht reguliert. Im Unterschied zur bisherigen Rechtslage werden sämtliche Hersteller medizinischer Geräte im Sinne der europäischen Medizinprodukte-Verordnung (EU) 2017/745 von den Vorgaben der NIS2-RL erfasst und nicht mehr nur Hersteller bestimmter Medizinprodukte, die bestimmte Schwellenwerte überschreiten.*
>
> *Demzufolge müssen zukünftig beispielsweise auch Hersteller von Wearables wie z.B. Fitness-Trackern die Vorgaben des EU-Cybersicherheitsrechts beachten.*

2. Wesentliche und wichtige Einrichtungen

Der Anwendungsbereich der NIS2-RL erstreckt sich im Grundsatz nur auf Einrichtungen, die folgende Schwellenwerte überschreiten: Mindestens 50 Beschäftigte oder über 10 Mio. EUR Jahresumsatz bzw. Jahresbilanzsumme. In bestimmten Fällen (z.B. bei Anbietern von öffentlich zugänglichen elektronischen Kommunikationsdiensten) greift die NIS2-Richtlinie auch unabhängig von der Größe.

Ihre Verpflichtungen knüpft die NIS2-RL überwiegend an die Klassifizierung eines Betreibers als „wesentliche" oder „wichtige" Einrichtung.

„Wesentliche Einrichtungen" sind:

- Unternehmen der Sektoren in Anhang I, die folgende Schwellenwerte überschreiten: mind. 250 Beschäftigte oder über 50 Mio. EUR Jahresumsatz und über 43 Mio. EUR Jahresbilanzsumme;
- qualifizierte Vertrauensdiensteanbieter und Domänennamenregister der Domäne oberster Stufe sowie DNS-Diensteanbieter, unabhängig von ihrer Größe;
- Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste, die folgende Schwellenwerte überschreiten: mindestens 50 Beschäftigte oder über 10 Mio. EUR Jahresumsatz oder Jahresbilanzsumme;
- Einrichtungen der Zentralregierungen;
- Unternehmen, die vom Mitgliedstaat als „wesentliche Einrichtungen" eingestuft werden;
- Einrichtungen, die gemäß der CER-Richtlinie (2022/2557) als kritische Einrichtungen eingestuft werden;
- sofern der Mitgliedstaat das vorsieht: Einrichtungen, die von den Mitgliedstaaten nach der NIS1-RL oder nach nationalem Recht als Betreiber wesentlicher Dienste eingestuft wurden.

„Wichtige Einrichtungen" sind:

- Einrichtungen der Sektoren in Anhang I oder II, die nicht bereits als wesentliche Einrichtung gelten;
- Einrichtungen, die vom Mitgliedstaat als „wichtige Einrichtungen" eingestuft werden.

WESENTLICHE EINRICHTUNG	WICHTIGE EINRICHTUNG
Sektor in Anhang I + mind. 250 Beschäftigte oder über 50 Mio. EUR Jahresumsatz bzw. über 43 Mio. EUR Jahresbilanzsumme	**Sektoren in Anhang I u. II +** mind. 50 Beschäftigte oder über 10 Mio. EUR Jahresumsatz bzw. Jahresbilanzsumme (soweit nicht bereits wesentliche Einrichtungen)
bestimmte Sonderfälle, z.B. Zentralregierung, DNS-Diensteanbieter oder staatliche Einstufung als wesentliche Einrichtung	bestimmte größenunabhängige Sonderfälle, z.B. staatliche Einstufung als wichtige Einrichtung

IV. Zentrale Verpflichtung: Ergreifen von Risikomanagementmaßnahmen

Die NIS2-RL verpflichtet wesentliche und wichtige Einrichtungen zum Ergreifen von geeigneten und verhältnismäßigen technischen, operativen und organisatorischen Maßnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten (Art. 21 Abs. 1 UAbs. 1 NIS2-RL).

Unter die NIS2-RL fallende Unternehmen bzw. Behörden sollten dazu in einem ersten Schritt die für ihren Bereich im Einzelfall erforderlichen Maßnahmen ermitteln und diese in einem zweiten Schritt implementieren.

1. Erforderliche Maßnahmen ermitteln (Art. 21 Abs. 1) → **2. Geeignete Maßnahmen ergreifen** (Art. 21 Abs. 1+2)

Schritt 1: Ermitteln der erforderlichen Maßnahmen

Ausgangspunkt der Beurteilung, welche Maßnahmen im Einzelfall zu ergreifen sind, ist eine systemische Analyse der Umstände des Einzelfalls unter Berücksichtigung des menschlichen Faktors und des Grads der Abhängigkeit von Netz- und Informationssystemen. Die Verhältnismäßigkeit der zu ergreifenden Maßnahmen bestimmt sich nach den potentiellen gesellschaftlichen und wirtschaftlichen Auswirkungen eines etwaigen Cybervorfalls. Je gravierender die Auswirkungen sein können, desto größere Anstrengungen sind dem Betreiber beim Ergreifen von Risikomanagementmaßnahmen zuzumuten. Gerade bei wesentlichen Einrichtungen dürfte vor diesem Hintergrund ein erheblicher Begründungsaufwand erforderlich sein, um bestimmte Risikomanagementmaßnahmen aus Kostengründen zu unterlassen.

Alles in allem liegt den Anforderungen an das Risikomanagement ein gefahrenübergreifender Ansatz zugrunde: Nicht nur „digitale" Gefahren sind in die Erwägungen einzubeziehen, sondern auch physische.

> Beispiel:
> *Ein Technologiekonzern sollte beim Ermitteln der erforderlichen Risikomanagementmaßnahmen nicht nur die Gefahr von Phishing- oder Hacking-Szenarien einbeziehen, sondern auch Beeinträchtigungen wie Diebstahl, Feuer (z.B. Brand im Rechenzentrum) oder Stromausfälle berücksichtigen.*

Schritt 2: Ergreifen geeigneter Maßnahmen

Im Einzelnen verlangt die NIS2-RL unter anderem folgende Maßnahmen als Teil des aktiven Risikomanagements:

- **Policies:** Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
- **Business Continuity:** Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- **Incident Management:** Bewältigung von Sicherheitsvorfällen
- **Einkauf:** Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- **Schulungen:** grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- **Verschlüsselung:** Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- **Supply Chain:** Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
- **Effektivität:** Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- **Weitere organisatorische Maßnahmen:** Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

Weitere technische Maßnahmen: Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, gesicherte Kommunikation, gegebenenfalls gesicherte Notfallkommunikationssysteme

Durch die Verpflichtung zur Gewährleistung der Sicherheit auch in der Lieferkette können mittelbar sogar solche Unternehmen von der NIS2-RL berührt sein, die an sich überhaupt nicht ihrem Anwendungsbereich unterfallen. Die Weitergabe von Cybersecurity-Maßnahmen durch die Lieferkette hinweg seitens der unmittelbar verpflichteten Einrichtung wirkt sich damit potentiell auch auf außereuropäische Unternehmen aus.

> Beispiel:
> *Ein Automobilhersteller ist nach Art. 21 Abs. 2 NIS2-RL verpflichtet, die Cybersicherheit auch in der Lieferkette zu gewährleisten. Er wird daher unter Umständen an seine Zulieferer herantreten und – beispielsweise vertraglich – bestimmte Cybersecurity-Maßnahmen auf Seiten der Zulieferer durchsetzen, um seine eigene Verpflichtung zum Ergreifen von Risikomanagementmaßnahmen nach der NIS2-RL zu erfüllen.*

V. Standardisierung und Zertifizierung

Die NIS2-RL ermöglicht den Mitgliedstaaten eine Regelung, wesentliche und wichtige Einrichtungen zur Verwendung von EU-Cybersecurity-Zertifizierungen und/oder von zertifizierten Produkten zu verpflichten. Perspektivisch werden damit zertifizierte technische Lösungen für die Betreiber ein erwägungswürdiger Weg sein, um die Einhaltung der Vorgaben der NIS2-RL zeit- und kosteneffizient nachzuweisen. Die Zertifizierung derartiger Produkte richtet sich nach europäischen Schemata für die Cybersicherheitszertifizierung nach dem EU-Cybersecurity-Act (Verordnung (EU) 2019/881).

Daneben gibt die NIS2-RL auch der Europäischen Kommission die Befugnis, per delegierten Rechtsakten bestimmte Kategorien wesentlicher und wichtiger Einrichtungen zur Nutzung bestimmter zertifizierter technischer Lösungen zu verpflichten oder ein entsprechendes Zertifikat zu erlangen. Der Erlass solcher delegierter Rechtsakte setzt jedoch voraus, dass die Kommission zuvor ein unzureichendes Cybersecurity-Niveau identifiziert und eine Umsetzungsfrist gesetzt hat.

Es ist davon auszugehen, dass perspektivisch zumindest die Mitgliedstaaten entsprechende Verpflichtungen etablieren werden. Unternehmen und andere Einrichtungen sollten daher die Umsetzung dieser Ermächtigung durch das jeweilige nationale Gesetz genau verfolgen, um rechtzeitig die geforderten Zertifizierungen bzw. zertifizierten Produkte implementieren zu können.

Die Mitgliedstaaten sind darüber hinaus durch die NIS2-RL angehalten, die Anwendung europäischer und internationaler Normen und technischer Spezifikationen für die Sicherheit von Netz- und Informationssystemen zu fördern (z.B. ISO/IEC 27001). Derartigen Standards wird daher unter Geltung der NIS2-RL eine noch größere Bedeutung zukommen.

VI. Sanktionen bei Verstößen

Die NIS2-RL erlegt den EU-Mitgliedstaaten die Pflicht auf, Bußgeldtatbestände für Verstöße gegen Art. 21 (Risikomanagementmaßnahmen, s.o.) und Art. 23 NIS2-RL (Berichtspflichten über erhebliche Sicherheitsvorfälle) zu schaffen. Gleichzeitig legt die NIS2-RL bereits einen Mindestwert für die obere Grenze des Bußgeldrahmens fest:

WESENTLICHE EINRICHTUNGEN	WICHTIGE EINRICHTUNGEN
Geldbuße bis zu: **10 Mio. EUR** oder **2 % des gesamten weltweiten Vorjahresumsatzes des Unternehmens, dem die Einrichtung angehört**	Geldbuße bis zu: **7 Mio. EUR** oder **1,4 % des gesamten weltweiten Vorjahresumsatzes des Unternehmens, dem die Einrichtung angehört**

Ein etwaiges Bußgeld tritt dabei neben weitere Aufsichts- und Durchsetzungsmaßnahmen, die eine zuständige Behörde im Falle eines (potentiellen) Verstoßes verhängen kann.

Beispiel:
Nach Art. 32 Abs. 5 NIS2-RL sollen die Mitgliedstaaten in Umsetzung der Richtlinie eine Befugnis der für die Durchsetzung der NIS2-RL zuständigen Behörden regeln, die gewissermaßen als „ultima ratio" verstanden werden kann: Bei Nichtbefolgung von Aufsichtsmaßnahmen soll die für die Durchsetzung der NIS2-RL zuständige Behörde von anderen zuständigen Behörden bzw. Gerichten verlangen können, den Angehörigen des Managements vorübergehend zu untersagen, Leitungsaufgaben in der jeweiligen Einrichtung wahrzunehmen. Damit verdeutlicht der europäische Gesetzgeber den Grundsatz „Cybersecurity ist Chefsache" (dazu s.o.).

Ähnliches gilt für den öffentlichen Sektor: Zwar sind bestimmte Durchsetzungsmaßnahmen ausdrücklich nicht auf Einrichtungen der öffentlichen Verwaltung (z.B. Behörden) anwendbar. Jedoch gelten die jeweiligen Haftungsregelungen des Mitgliedstaats für öffentliche Bedienstete und Amtsträger (Amtshaftung). In Deutschland haftet demnach zunächst typischerweise der Staat auf Ersatz der Schäden, die ein Amtsträger in Ausübung eines ihm übertragenen öffentlichen Amtes verursacht. Auch den einzelnen Amtsträger können persönliche Konsequenzen treffen. Zum einen droht ein Regressanspruch des Dienstherrn. Zum anderen sind disziplinarrechtliche Konsequenzen möglich, die von einem bloßen Verweis über Bezügekürzungen bis hin zur Entfernung aus dem Beamten- oder Dienstverhältnis führen können.

Die Leitungsebenen wesentlicher und wichtiger Einrichtungen sind daher gut beraten, die Pflicht zum Ergreifen von Risikomanagementmaßnahmen frühzeitig und sorgfältig anzugehen, um Geldbußen wegen Verstößen in empfindlicher Höhe zu vermeiden.

Ob auch die nunmehr in den Anwendungsbereich der NIS2-RL fallenden Einrichtungen der öffentlichen Verwaltung (etwa Behörden) Bußgelder befürchten müssen, bleibt abzuwarten: Nach Art. 34 Abs. 7 NIS2-RL ist es den Mitgliedstaaten individuell vorbehalten, ob und in welchem Umfang gegen Einrichtungen der öffentlichen Verwaltung Geldbußen verhängt werden können.

Auf den folgenden Seiten finden Sie eine Übersicht, welche Sophos-Lösungen Ihnen dabei helfen können, konkrete Anforderungen der NIS2-RL zu erfüllen.

B. Sophos-Produkte für Betreiber wesentlicher und wichtiger Einrichtungen

ANFORDERUNGEN DER NIS2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Kapitel IV, Artikel 20, Governance		
(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.	**Sophos-Trainings und -Zertifizierungen**	Trainingskurse und Zertifizierungen, die Partnern und Kunden dabei helfen, das Potenzial ihrer Sophos-Sicherheitsimplementierungen voll auszuschöpfen; Zugang zu neuestem Know-how und Expertise für Security Best Practices.
	Sophos Phish Threat	Bietet simulierte Phishing-Cyber-Angriffe und Security-Awareness-Trainings für die Endbenutzer von Unternehmen und Einrichtungen. Das Kursangebot deckt die Bereiche Phishing und Cybersecurity ab: Unsere Trainingsmodule behandeln Themen wie Verhinderung von Datenverlust, Passwort-Schutz und mehr.
Kapitel IV, Artikel 21, Risikomanagementmaßnahmen im Bereich der Cybersicherheit		
(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen… (2) Die in Absatz 1 genannten Maßnahmen müssen… zumindest Folgendes umfassen: a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;	**Sophos Intercept X** **Sophos Intercept X for Server**	Eine Kombination innovativer Technologien wie Deep Learning, Anti-Exploit, Active Adversary Protection und Malicious Traffic Detection mit Echtzeit-Bedrohungsdaten aus den SophosLabs, damit Sie Bedrohungen auf allen Geräten und Plattformen einfach abwehren, erkennen und beseitigen können.
	Sophos Firewall	Erkennt dank der branchenführenden Machine-Learning-Technologie von Sophos (unterstützt von SophosLabs Intelix) neueste Ransomware und unbekannte Bedrohungen bereits, bevor sie in Ihr Netzwerk gelangen. Bietet modernsten Schutz vor aktueller Drive-by- und gezielter Web-Malware, Filterung von URLs/ schädlichen Websites, Filterung von Webanwendungen und cloudbasierte Filterung für Offsite-Schutz.
	Sophos Cloud Optix	Sorgt für ein kontinuierliches Monitoring der Konfigurationsstandards, um Abweichungen zu erkennen. So können Sie versehentliche oder böswillige Änderungen in der Ressourcenkonfiguration verhindern, erkennen und automatisch korrigieren.
	Synchronized Security in Sophos-Produkten	Ermöglicht durch den Austausch von Telemetrie- und Statusdaten ein koordiniertes Erkennen, Isolieren und Beseitigen von Malware auf Servern, Endpoints und Firewalls. So können auch komplexe Angriffe gestoppt werden.
	Sophos Managed Detection and Response (MDR)	24/7 Threat Detection and Response erkennt und beseitigt komplexe Cyberangriffe, die Technologien allein nicht stoppen können.
	Sophos Network Detection and Response (NDR)	Überwacht kontinuierlich den Netzwerkverkehr innerhalb des Netzwerks, um Anomalien und verdächtige Aktivitäten zu erkennen. Mit NDR können u.a. fremde und ungeschützte Geräte sowie Datendiebstahl und Angriffe auf IoT- und OT-Systeme erkannt werden.
(2) b) Bewältigung von Sicherheitsvorfällen;	**Sophos Managed Detection and Response (MDR)**	Überwacht kontinuierlich Signale aus der gesamten Sicherheitsumgebung (u. a. von Netzwerk-, E-Mail-, Firewall-, Identity-, Endpoint- und Cloud-Technologien), damit wir potenzielle Cybersecurity-Vorfälle schnell und präzise erkennen und darauf reagieren können. Ein kompletter Incident Response Service ist standardmäßig enthalten und bietet 24/7-Betreuung durch Incident-Response-Experten. Umfasst eine komplette Ursachenanalyse und Reporting. Im Schnitt analysieren und beheben wir Vorfälle in nur 38 Minuten nach der Erkennung.
	Sophos Network Detection and Response (NDR)	Überwacht kontinuierlich den Netzwerkverkehr innerhalb des Netzwerks, um Anomalien und verdächtige Aktivitäten zu erkennen. Mit NDR können u.a. fremde und ungeschützte Geräte sowie Datendiebstahl und Angriffe auf IoT- und OT-Systeme erkannt werden.
	Sophos Rapid Response Service	Bietet blitzschnelle Soforthilfe durch ein Expertenteam beim Erkennen und Beseitigen aktiver Bedrohungen.
	Synchronized Security in Sophos-Produkten	Austausch von Telemetrie- und Statusdaten, koordiniertes Erkennen, Isolieren und Beseitigen von Malware auf Servern, Endpoints und Firewalls.

ANFORDERUNGEN DER NIS2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
(2) c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;	**Sophos Managed Detection and Response (MDR)**	Gewährleistet den Informationssicherheitsaspekt des Business Continuity Managements mit 24/7-Erkennung von und Reaktion auf Sicherheitsvorfälle in der gesamten IT-Umgebung, wobei menschliche Expertise, KI und modernste Technologien genutzt werden.
	Sophos Intercept X **Sophos Intercept X for Server**	Eine Kombination innovativer Technologien wie Deep Learning, Anti-Exploit, Active Adversary Protection und Malicious Traffic Detection mit Echtzeit-Bedrohungsdaten aus den SophosLabs, damit Sie Bedrohungen auf allen Geräten und Plattformen einfach abwehren, erkennen und beseitigen können. Nach einem Ransomware-Angriff oder Angriff auf den Master Boot Record werden alle Dateien in ihren Ursprungszustand zurückversetzt. Forensikbasierte Bereinigungsfunktionen entfernen sowohl den Schadcode als auch die von der Malware erstellten Registry-Schlüssel-Änderungen.
	Sophos Cloud Optix	Überwacht AWS-, Azure- und GCP-Konten auf Cloud-Speicherdienste ohne aktivierte Backup-Zeitpläne und bietet geführte Bereinigungsmaßnahmen.
(2) d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;	**Sophos Intercept X with XDR**	Bietet u. a. mit KI, Anti-Exploit-Technologie, Verhaltensschutz und Anti-Ransomware umfassenden Schutz vor Bedrohungen, die sich über Drittanbieter Zugriff verschaffen. Außerdem können Sie mit der leistungsstarken XDR-Funktionalität verdächtige Aktivitäten automatisch erkennen, Bedrohungsindikatoren priorisieren und Ihren gesamten Endpoint- und Server-Bestand schnell und einfach auf potenzielle Bedrohungen durchsuchen.
	Sophos Managed Detection and Response (MDR)	Bietet Threat Hunting durch ein Experten-Team und Bereinigung als Fully-Managed-Service. Sophos-Experten arbeiten rund um die Uhr daran, für Sie proaktiv potenzielle Bedrohungen und Sicherheitsvorfälle in der Lieferkette aufzuspüren, zu analysieren und Reaktionsmaßnahmen zu ergreifen.
	Sophos ZTNA	Schützt durch gezielte Zugriffssteuerung vor Angriffen auf die Lieferkette, die auf den Zugriff von Drittanbietern auf Ihre Systeme angewiesen sind. Diese Cloud-basierte Lösung überprüft die Benutzeridentität sowie den Gerätestatus und die Compliance, bevor Zugriff auf Ressourcen gewährt wird. Anfragen von vertrauenswürdigen Partnern werden unabhängig vom Standort authentifiziert.
(2) e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;	**Sophos Managed Detection and Response (MDR)**	Unsere Threat-Hunting-Experten überwachen und analysieren Warnmeldungen aus dem gesamten Netzwerk und nutzen Netzwerk-, Firewall-, Cloud-, E-Mail- und Endpoint-Security-Tools, um verdächtige Aktivitäten zu erkennen und zu untersuchen und personenbezogene Daten überall zu schützen. Sophos NDR erzeugt hochwertige, aussagekräftige Signale in der gesamten Netzwerkinfrastruktur und optimiert so die Cyberabwehr. Sophos MDR reagiert proaktiv auf vom Kunden gemeldete Schwachstellen. Nach entsprechender Benachrichtigung wird eine umfassende Untersuchung eingeleitet, bei der nach Anzeichen für eine Kompromittierung gesucht wird. Bei Bedarf behebt Sophos MDR den Vorfall und gibt Empfehlungen, wie die Umgebung vor künftigen Kompromittierungen geschützt werden kann. Abschließend wird ein vollständiger Experten-Bericht zur Untersuchung zur Verfügung gestellt.
(2) f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;	**Sophos Managed Detection and Response (MDR)**	Analysiert und bewertet potenzielle Sicherheitsrisiken in der gesamten Umgebung 24/7 und nutzt dabei die weltweit führende Threat Intelligence von Sophos X-Ops, um den Risikograd zu bestimmen und Maßnahmen zu priorisieren.
(2) g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;	**Sophos-Trainings und -Zertifizierungen**	Trainingskurse und Zertifizierungen, die Partnern und Kunden dabei helfen, das Potenzial ihrer Sophos-Sicherheitsimplementierungen voll auszuschöpfen; Zugang zu neuestem Know-how und Expertise für Security Best Practices.
	Sophos Phish Threat	Bietet simulierte Phishing-Cyber-Angriffe und Security-Awareness-Trainings für die Endbenutzer von Unternehmen und Einrichtungen. Das Kursangebot deckt die Bereiche Phishing und Cybersecurity ab: Unsere Trainingsmodule behandeln Themen wie Verhinderung von Datenverlust, Passwort-Schutz und mehr.
(2) h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;	**Sophos Central Device Encryption**	Schützt Geräte und Daten mit leistungsstarker Festplatten-Verschlüsselung für Windows und macOS. Überprüfen Sie den Verschlüsselungs-Status des Geräts und weisen Sie die Compliance nach.
	Sophos Email **Sophos Firewall**	Bietet TLS-Verschlüsselung und Unterstützung von SMTP/S sowie vollständige push-basierte und optionale pull-basierte Portalverschlüsselung.
	Sophos Mobile	Erzwingt Geräteverschlüsselung und überwacht die Compliance gemäß Verschlüsselungsrichtlinie.

ANFORDERUNGEN DER NIS2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
(2) i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;	**Sophos Managed Detection and Response (MDR)**	Threat-Hunting-Experten überwachen und korrelieren die Informationssystem-Aktivitäten in der gesamten IT-Sicherheitsumgebung und identifizieren und untersuchen verdächtige Aktivitäten, indem sie regelmäßig Aufzeichnungen der Informationssystem-Aktivitäten überprüfen, u. a. Audit-Protokolle, Zugriffsprotokolle, Zugriffsberichte und Berichte zur Nachverfolgung von Sicherheitsvorfällen.
	Sophos Firewall	Nutzersensibilisierung in allen Bereichen unserer Firewall bildet die Grundlage für alle Firewall-Richtlinien und Reports und ermöglicht benutzerbasierte Kontrollen über Anwendungen, Bandbreite und weitere Netzwerkressourcen.
	Sophos Central	Zugriffslisten und Informationen über Benutzerberechtigungen sind stets auf dem neuesten Stand. Kontrolle für Zugriffsrechte: Erfüllen Personen nicht mehr die Voraussetzungen für Zugriffsrechte, werden ihnen ihre Zugriffsrechte entzogen (z. B. weil sie die Stelle wechseln oder das Unternehmen verlassen).
	Sophos ZTNA	Ermöglicht höhere Sicherheit und mehr Agilität in sich schnell ändernden Umgebungen, da Benutzer und Geräte schnell und einfach registriert oder außer Betrieb genommen werden können. Überprüft kontinuierlich die Benutzeridentität, den Gerätestatus und die Compliance, bevor Zugriff auf Anwendungen und Daten gewährt wird.
	Sophos Cloud Optix	Inventory Management für mehrere Cloud-Anbieter mit kontinuierlichem Asset Monitoring sowie vollständiger Visualisierung der Netzwerktopologie und des Datenverkehrs.
(2) j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	**Sophos Firewall**	Unterstützt flexible Optionen zur mehrstufigen Authentifizierung, einschließlich Verzeichnisdiensten für den Zugriff auf wichtige Systembereiche.
	Sophos ZTNA	Überprüft kontinuierlich die Benutzeridentität, den Gerätestatus und die Compliance, bevor Zugriff auf Anwendungen und Daten gewährt wird.
	Sophos Central	Schützt privilegierte und Administrator-Konten dank erweiterter Zwei-Faktor-Authentifizierung:
	Sophos Cloud Optix	Überwacht AWS-/Azure-/GCP-Konten auf Root- und IAM-Benutzerzugriff ohne MFA, damit Sie Compliance sicherstellen können.
Kapitel IV, Artikel 23, Berichtspflichten		
(4) Die Mitgliedstaaten stellen sicher, dass die betreffenden Einrichtungen dem CSIRT oder gegebenenfalls der zuständigen Behörde für die Zwecke der Meldung nach Absatz 1 Folgendes übermitteln: d) spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Buchstabe b einen Abschlussbericht, der Folgendes enthält: ***(i) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;***	**Sophos Managed Detection and Response (MDR)**	Nach entsprechender Benachrichtigung wird eine umfassende Untersuchung eingeleitet, bei der nach Anzeichen für eine Kompromittierung gesucht wird. Bei Bedarf behebt Sophos MDR den Vorfall und gibt Empfehlungen, wie die Umgebung vor künftigen Kompromittierungen geschützt werden kann. Abschließend wird ein vollständiger Experten-Bericht zur Untersuchung zur Verfügung gestellt.
(4) Die Mitgliedstaaten stellen sicher, dass die betreffenden Einrichtungen dem CSIRT oder gegebenenfalls der zuständigen Behörde für die Zwecke der Meldung nach Absatz 1 Folgendes übermitteln: d) spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Buchstabe b einen Abschlussbericht, der Folgendes enthält: ***(ii) Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;***	**Sophos Managed Detection and Response (MDR)**	Sophos MDR analysiert und bewertet potenzielle Sicherheitsrisiken in der gesamten Umgebung 24/7 und nutzt dabei die weltweit führende Threat Intelligence von Sophos X-Ops. Außerdem stellt Sophos MDR eine komplette Ursachenanalyse zur Verfügung, auf deren Basis die Umgebung noch widerstandsfähiger gemacht und Reaktionspläne und -strategien den gewonnenen Erkenntnissen entsprechend aktualisiert werden können.
	Sophos XDR	Geht über die Endpoint-Ebene hinaus und berücksichtigt auch zahlreiche Netzwerk-, E-Mail-, Cloud- und mobile Datenquellen.So erhalten Sie ein noch umfassenderes Bild Ihrer Cybersicherheit und haben die Möglichkeit, bei Bedarf jederzeit Detailinformationen abzurufen. Da Daten von jedem Produkt in den Sophos Data Lake einfließen, können Sie schnell geschäftskritische Fragen beantworten, Ereignisse aus verschiedenen Datenquellen korrelieren und noch besser gezielte Maßnahmen ergreifen. Sie können beispielsweise Querverweise zu Netzwerk-Daten erstellen und sich so einen besseren Überblick über einen Vorfall und Ereignisse auf Geräten verschaffen, die bei einem Angriff außer Betrieb gesetzt wurden.

Die nächsten Schritte

Kontaktieren Sie uns. Wir unterstützen und beraten Sie gerne, welche unserer Lösungen sich für Ihre individuellen Bedürfnisse am besten eignen.

E-Mail: sales@sophos.de
Tel.Nr: 0611 5858-0

Wir empfehlen Ihnen einen unserer spezialisierten Vertriebspartner und stellen wenn gewünscht auch gerne den Kontakt her.

Ihr Vertriebspartner unterstützt und begleitet Sie bei der Umsetzung Ihres Vorhabens. Bei Fragen stehen selbstverständlich auch wir Ihnen weiterhin jederzeit zur Verfügung.

XAZER
IT-Systeme

E-Mail: info@xazer-it.de
Tel.Nr. 02778 598490-0

Dieses Whitepaper wurde in Zusammenarbeit mit Rechtsanwalt Dr. David Bomhard von Noerr Partnerschaftsgesellschaft mbB erstellt.

2023-04-28 EN-WP (NP)

SOPHOS