SOPHOS

Umsetzung der NIS2-Richtlinie in Deutschland

Grundlage voraussichtliches NIS2-Umsetzungsgesetz.

Dieses Whitepaper wurde in Zusammenarbeit mit Rechtsanwalt Andreas Daum und Rechtsanwalt Dr. Paul Vogel 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. Der deutsche Gesetzgeber wird die NIS2-RL mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz („NIS2UmsuCG") in nationales Recht umsetzen. Dieses Gesetz sieht eine grundlegende Überarbeitung des bisherigen BSI-Gesetzes vor (die Neufassung im Folgenden: „BSIG n.F."), welches bereits heute die IT-sicherheitsrechtlichen Anforderungen an die Betreiber kritischer Infrastrukturen regelt.[1]

In diesem Whitepaper erfahren Sie, welche neuen und erweiterten Anforderungen die NIS2-RL und das neue BSIG Unternehmen und andere Einrichtungen, die auf dem europäischen Markt tätig sind, mit sich bringen und wie Sophos-Lösungen Sie bei der Implementierung der neuen Anforderungen unterstützen können.

Sophos-Whitepaper, Oktober 2024

Hintergrund und wesentliche Inhalte des neuen BSIG

I. Roadmap: Von NIS1 über IT-SiG 2.0 zu NIS2 und NIS2UmsuCG

Im Jahr 2016 zeigte der europäischen Gesetzgeber mit der Network-and-Information-Security-Richtlinie (Richtlinie (EU) 2016/1148, **„NIS1-RL"**) erste Bestrebungen zur rechtlichen Vereinheitlichung im Bereich der Cybersicherheit. Der deutsche Gesetzgeber ging über diese Vorgaben hinaus und erhöhte im Jahr 2021 mit dem IT-Sicherheitsgesetz 2.0 (**„IT-SiG 2.0"**) das allgemeine Schutzniveau und erweiterte den Adressatenkreis der betroffenen Einrichtungen .

Der europäische Gesetzgeber zog schnell nach verabschiedete im Dezember 2022 die NIS2-RL, welche die Anforderungen an die Cybersicherheit in der gesamten EU gegenüber der NIS1-RL und dem IT-SiG 2.0 noch einmal verschärft. Da es sich bei der NIS2-RL um eine Richtlinie handelt, ist sie (im Unterschied zu einer Verordnung) aber nicht unmittelbar in den Mitgliedstaaten anwendbar, sondern bedarf zunächst einer Transformation in nationales Recht. Der deutsche Gesetzgeber ist daher gehalten, die nationalen IT-Sicherheitsgesetze anzupassen. Die EU gewährte den Mitgliedstaaten hierfür eine Umsetzungsfrist bis zum 17.10.2024.

Seit Verabschiedung der NIS2-RL hat der deutsche Gesetzgeber bereits mehrere Entwürfe eines deutschen NIS2-Umsetzungsgesetzes vorgelegt. Im Juli 2024 beschloss das Bundeskabinett schließlich einen Regierungsentwurf des sog. NIS2UmsuCG. Da der Entwurf zunächst noch Bundestag und Bundesrat passieren muss, ist mit Stand September 2024 fraglich, ob der deutsche Gesetzgeber die Umsetzungsfrist einhalten können wird. Da das NIS2UmsuCG keine Übergangsfrist vorsieht, ist Unternehmen dringend zu empfehlen, bereits jetzt die neuen Anforderungen der NIS2-RL bzw. seiner Umsetzung und ihre etwaigen Auswirkungen auf die jeweilige Einrichtung zu prüfen. Die neuen Vorgaben werden jedenfalls erst mit Inkrafttreten des BSIG n.F. anwendbar sein, selbst wenn dies erst nach dem 17.10.2024 erfolgen sollte.

II. Cybersicherheit als Managementaufgabe

Mit der NIS2-RL macht der europäische Gesetzgeber deutlich, dass er die Gewährleistung von Cybersicherheit und die Prävention von IT-Sicherheitsvorfällen als Aufgabe des obersten Managements begreift. Dieses Verständnis spiegelt sich auch im NIS2UmsuCG wider.

Nach § 38 Abs. 1 BSIG n.F. muss die Geschäftsleitung einer regulierten Einrichtung Risikomanagementmaßnahmen (dazu unten IV.) umsetzen und ihre Umsetzung überwachen. Für Verstöße in diesem Bereich können Geschäftsleiter (persönlich) verantwortlich gemacht werden.

> Beispiel:
>
> *Das Management eines Automobilkonzerns darf die Implementierung von Maßnahmen zur Cybersicherheit nicht pauschal delegieren, sondern muss die Umsetzung dieser Maßnahmen selbst betreuen und überwachen. Bei einem Verstoß gegen diese Vorgabe kann es zu einer persönlichen Haftung des Managements für etwaige Schäden kommen.*

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

III. Neuer erweiterter Anwendungsbereich

1. Erweiterung der regulierten Sektoren

Das BSIG n.F. weist gegenüber der aktuellen Rechtslage einen deutlich breiteren Anwendungsbereich auf. Das Gesetz erstreckt sich nun auf 14 Sektoren, sowohl im öffentlichen als auch im privaten Bereich.

> Beispiel:
>
> *Das BSIG n.F. erfasst nun beispielsweise auch die Luft- und Raumfahrt oder das verarbeitende Gewerbe. Daneben werden zudem auch kritische Dienste der öffentlichen Verwaltung (auf Bundesebene) reguliert.*

Die folgenden 14 Sektoren werden vom BSIG n.F. erfasst:

SEKTOREN BESONDERS WICHTIGER UND WICHTIGER EINRICHTUNGEN (ANLAGE 1 DES BSIG N.F.):	SEKTOREN WICHTIGER EINRICHTUNGEN (ANLAGE 2 DES BSIG N.F.):
Energie	Transport und Verkehr (Post- und Kurierdienste)
Transport und Verkehr (Luft-, Schienen-, Straßenverkehr, Schifffahrt)	Abfallbewirtschaftung
Finanzwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Gesundheit	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Wasser	Verarbeitendes Gewerbe/Herstellung von Waren
Digitale Infrastruktur	Anbieter digitaler Dienste
Weltraum	Forschung

Durch die umfassendere Definition des Anwendungsbereichs obliegt die Festlegung relevanter Sektoren nicht mehr den Mitgliedstaaten.

Die folgende Tabelle verdeutlicht die Erweiterung der Sektoren durch die NIS2-RL bzw. das BSIG n.F. gegenüber der bisherigen Rechtslage:

NIS1-RL/BSIG a.F.	NIS2-RL/BSIG n.F.
Energie	Energie
Wasser (Trinkwasser, Abwasser)	Wasser (Trinkwasser, Abwasser)
Ernährung (Lebensmittelherstellung, -behandlung und -handel)	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Informationstechnik und Telekommunikation	Digitale Infrastruktur
Gesundheit	Gesundheit
Finanz- und Versicherungswesen	Finanzwesen (Bankwesen, Finanzmarktinfrastrukturen)
Transport/Verkehr	Transport und Verkehr
Entsorgung	Abfallbewirtschaftung
	Post- und Kurierdienste
	Weltraum
	Produktion, Herstellung und Handel mit chemischen Stoffen
	Verarbeitendes Gewerbe/Herstellung von Waren
	Anbieter digitaler Dienste
	Forschung

Das BSIG n.F. ist zunächst auf jede Einrichtung der genannten Sektoren anwendbar, die nach der KMU-Definition der Europäischen Kommission die Schwellenwerte für mittlere Unternehmen erfüllt oder überschreitet. Dies ist der Fall, wenn die Einrichtung mindestens 50 Beschäftigte hat oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils mehr als EUR 10 Mio. erzielt. Alle Einrichtungen, die diese Schwellenwerte nicht erreichen (und folglich als kleine oder Kleinstunternehmen im Sinne der europäischen Definition gelten), können jedoch mittelbar über die Lieferkette von Vorschriften des BSIG n.F. betroffen sein (hierzu unten IV.).

Daneben unterwirft das BSIG n.F. bestimmte Einrichtungen unabhängig von ihrer Größe explizit dem Anwendungsbereich des Gesetzes. Dazu gehören unter anderem Anbieter öffentlich zugänglicher Telekommunikationsdienste sowie Betreiber öffentlicher Telekommunikationsnetze, außerdem bestimmte Einrichtungen der Bundesverwaltung. Die Zahl der Beschäftigten sowie der Umsatz und die Bilanzsumme spielen insofern keine Rolle.

> Beispiel:
>
> *Im Gesundheitswesen sind durch das BSIG n.F. fortan deutlich mehr Einrichtungen betroffen. Im Unterschied zur bisherigen Rechtslage werden sämtliche Hersteller medizinischer Geräte im Sinne der europäischen Medizinprodukte-Verordnung (EU) 2017/745 von den Vorgaben des BSIG erfasst und nicht mehr nur solche Hersteller die Medizinprodukte herstellen und gewisse Schwellenwerte überschreiten.*
>
> *Demzufolge müssen zukünftig beispielsweise auch Hersteller von Wearables wie z.B. Fitness-Trackern die Vorgaben des BSIG n.F. beachten.*

Besonders wichtige und wichtige Einrichtungen

Die Zugehörigkeit einer Einrichtung zu einem der vorgenannten Sektoren bedeutet grundsätzlich noch nicht, dass diese Einrichtung die Vorgaben des BSIG n.F. implementieren muss. Vielmehr muss die Einrichtung, wie erwähnt, auch eine gewisse Größe aufweisen:

Die Pflichten knüpft das BSIG n.F. überwiegend an die Klassifizierung eines Betreibers als „besonders wichtige" oder „wichtige" Einrichtung.

„Besonders wichtige Einrichtungen" sind:

- Betreiber sogenannter „kritischer Anlagen" (siehe hierzu unten);
- Einrichtungen der Sektoren Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, Digitale Infrastruktur und Weltraum, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und folgende Schwellenwerte überschreiten: mind. 250 Beschäftigte oder über 50 Mio. EUR Jahresumsatz und über 43 Mio. EUR Jahresbilanzsumme;
- qualifizierte Vertrauensdiensteanbieter, Top Level Domain, Name Registries oder DNS-Diensteanbieter, jeweils unabhängig von ihrer Größe;
- Anbieter öffentlicher Telekommunikationsnetze oder öffentlich zugänglicher Telekommunikationsdienste, die folgende Schwellenwerte überschreiten: mindestens 50 Beschäftigte oder über 10 Mio. EUR Jahresumsatz und Jahresbilanzsumme.

Daneben sind auf bestimmte Einrichtungen der Bundesverwaltung (v.a. Bundesbehörden und öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung) im Wesentlichen die Vorschriften für besonders wichtige Einrichtungen anzuwenden.

„Wichtige Einrichtungen" sind:

Einrichtungen aller oben genannten Sektoren, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und folgende Schwellenwerte überschreiten: mind. 50 Beschäftigte oder über 10 Mio. EUR Jahresumsatz und Jahresbilanzsumme, sofern diese Einrichtungen nicht bereits als „besonders wichtige Einrichtungen" gelten;

- Vertrauensdiensteanbieter;
- Anbieter öffentlicher Telekommunikationsnetze oder öffentlich zugänglicher Telekommunikationsdienste, die weniger als 50 Beschäftigte haben und einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Mio. EUR oder weniger aufweisen.

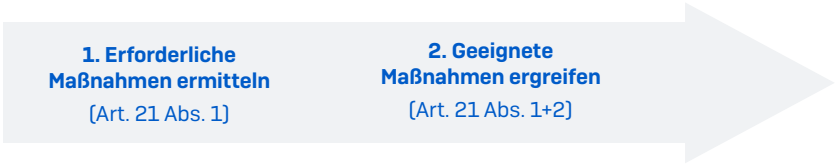
„Kritische Anlagen" sind Anlagen, die für die Erbringung einer kritischen Dienstleistung erheblich sind. Welche Anlagen hierzu zählen, wird der Gesetzgeber noch in einer gesonderten Rechtsverordnung niederlegen. Diese Rechtsverordnung wird die BSI-Kritisverordnung ablösen und voraussichtlich auf dieser aufbauen. Ein Entwurf dieser neuen Verordnung liegt gegenwärtig (September 2024) noch nicht vor.

BESONDERS WICHTIGE EINRICHTUNG	WICHTIGE EINRICHTUNG
Sektoren: Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, Digitale Infrastruktur und Weltraum **Größe:** mind. 250 Beschäftigte oder über 50 Mio. EUR Jahresumsatz und über 43 Mio. EUR Jahresbilanzsumme	**Sektoren: Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, Digitale Infrastruktur und Weltraum sowie Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Verarbeitendes Gewerbe/ Herstellung von Waren, Anbieter digitaler Dienste, Forschung** **Größe:** mind. 50 Beschäftigte oder über 10 Mio. EUR Jahresumsatz und Jahresbilanzsumme (soweit nicht bereits besonders wichtige Einrichtung)
Bestimmte größenunabhängige Sonderfälle, z.B. Betreiber kritischer Anlagen, DNS-Diensteanbieter oder qualifizierte Vertrauensdiensteanbieter	**Bestimmte größenunabhängige Sonderfälle,** z.B. Vertrauensdiensteanbieter

IV. Zentrale Verpflichtung: Umsetzung von Risikomanagementmaßnahmen

Das BSIG n.F. verpflichtet besonders wichtige und wichtige Einrichtungen zum Ergreifen von geeigneten, verhältnismäßigen und wirksamen technischen und organisatorischen Maßnahmen, 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. 1 BSIG n.F.).

Die betroffenen Einrichtungen sollten in einem ersten Schritt die für ihren Bereich im Einzelfall erforderlichen Maßnahmen ermitteln und diese in einem zweiten Schritt implementieren.



Schritt 1: Ermitteln der erforderlichen Maßnahmen

Der Ausgangspunkt für die Beurteilung, welche Maßnahmen im Einzelfall zu ergreifen sind, ist eine systemische Analyse, bei der der menschliche Faktor berücksichtigt wird, um ein vollständiges Bild der Sicherheit des Netz- und Informationssystems zu erhalten. Die Verhältnismäßigkeit der Maßnahmen bestimmt sich nach den potentiellen gesellschaftlichen und wirtschaftlichen Auswirkungen eines etwaigen Cybervorfalls. Nach § 30 Abs. 1 BSIG n.F. sind für die Bewertung der Verhältnismäßigkeit das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen zu berücksichtigen.

Je gravierender die Auswirkungen sein können, desto größere Anstrengungen sind dem Betreiber zuzumuten. Gerade bei besonders wichtigen Einrichtungen dürfte vor diesem Hintergrund ein erhöhter 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 muss 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: Umsetzung geeigneter Maßnahmen

Im Einzelnen verlangt das BSIG n.F. unter anderem folgende Maßnahmen als Teil eines aktiven Risikomanagements:

- **Policies**: Konzepte in Bezug auf die Risikoanalyse und Sicherheit in der Informationstechnik
- **Incident Management:** Bewältigung von Sicherheitsvorfällen
- **Business Continuity:** Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- **Einkauf:** Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen
- **Schulungen:** grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik
- **Verschlüsselung:** Konzepte und Verfahren für den Einsatz von Kryptografie und 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 Sicherheit in der Informationstechnik
- **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

Die Pflicht zur Umsetzung von Maßnahmen zur Gewährleistung der Sicherheit in der Lieferkette kann dazu führen, dass mittelbar auch solche Unternehmen vom BSIG n.F. berührt sind, die eigentlich nicht dessen Anwendungsbereich unterfallen. Die Weitergabe von Cybersecurity-Maßnahmen über die Lieferkette hinweg wirkt sich damit potenziell auch auf kleine oder Kleinstunternehmen aus.

> Beispiel:
>
> *Ein Automobilhersteller, der dem Anwendungsbereich des BSIG n.F. unterfällt ist nach § 30 BSIG n.F. verpflichtet, die Cybersicherheit auch in der Lieferkette zu gewährleisten. Er wird daher unter Umständen an seine Zulieferer herantreten und – typischerweise vertraglich – bestimmte Cybersecurity-Maßnahmen durchsetzen, um seine eigene Verpflichtung zum Ergreifen von Risikomanagementmaßnahmen nach dem BSIG n.F. zu erfüllen.*

Um klarzustellen, welche Risikomanagementmaßnahmen regulierte Einrichtungen künftig umsetzen müssen, wird die Europäische Kommission durch eine Durchführungsverordnung zusätzliche Bestimmungen erlassen. Diese Verordnung gilt ausschließlich für Einrichtungen aus den Bereichen „Digitale Infrastruktur" und „Anbieter digitaler Dienste". Die Verabschiedung dieser Verordnung ist bis zum 17.10.2024 geplant.

V. Standardisierung und Zertifizierung

Nach § 30 Abs. 6 BSIG n.F. dürfen besonders wichtige und wichtige Einrichtungen bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine EU-Cybersecurity-Zertifizierungen verfügen. Welche Produkte, Dienste und Prozesse das sein werden, wird der deutsche Gesetzgeber noch mittels gesonderter Rechtsverordnung festlegen. 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 regulierter 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.

Die betroffenen Einrichtungen sollten die Umsetzung dieser Ermächtigungen 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 die Pflicht zur Ergreifung von Risikomanagementmaßnahmen sowie gegen Berichtspflichten über erhebliche Sicherheitsvorfälle zu schaffen. Der deutsche Gesetzgeber sieht in § 65 BSIG n.F. für die betroffenen Einrichtungen folgende Bußgeldrahmen vor:

BESONDERS WICHTIGE 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 das Bundesamt für Sicherheit in der Informationstechnik („**BSI**“) oder andere zuständige Behörden im Falle eines (potenziellen) Verstoßes verhängen kann.

> Beispiel:
>
> *Die zuständige Aufsichtsbehörde hat nach § 61 Abs. 9 Nr. 2 BSIG n.F. die Befugnis Geschäftsleitungen von besonders wichtigen Einrichtungen die Ausübung ihrer Tätigkeit vorübergehend zu untersagen, wenn sie den Anordnungen der Behörde nicht rechtzeitig nachkommen. Damit verdeutlicht der 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 allgemeinen Amtshaftungsregeln. 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 besonders wichtiger und wichtiger Einrichtungen sind daher gut beraten, die Pflicht zum Ergreifen von Risikomanagementmaßnahmen frühzeitig und sorgfältig anzugehen, um Geldbußen wegen Verstößen in empfindlicher Höhe und potenziell eine persönliche Haftung zu vermeiden.

Auf den folgenden Seiten finden Sie eine Übersicht, welche Sophos-Lösungen Ihnen dabei helfen können, konkrete Anforderungen des BSIG n.F. zu erfüllen.

B. Sophos-Produkte für Betreiber besonders wichtiger und wichtiger Einrichtungen

NIS-2-Richtlinie – Kapitel IV, Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit

ANFORDERUNGEN DER NIS-2-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 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.
	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.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Kapitel IV, Artikel 21, Risikomanagementmaßnahmen im Bereich der Cybersicherheit		
2. 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 Endpoint	Bietet modernsten Schutz vor Ransomware und komplexen Angriffen. Innovative Schutzfunktionen, darunter KI-basiertes Deep Learning, Anti-Exploit, lückenloser Ransomware-Schutz mit automatischem Rollback und adaptive Abwehrmechanismen, die automatisch auf Angreifer reagieren und selbst hochkomplexe Angriffe stoppen.
	Sophos Firewall	Bietet branchenführenden Netzwerkschutz, optimiert für das moderne verschlüsselte Internet und verteilte Benutzergruppen. Umfassende SD-WAN-Funktionen binden verteilte Büros und Standorte sicher an, während das integrierte ZTNA einen sicheren, benutzerbasierten Zugriff von jedem Standort ermöglicht. In Kombination mit Sophos Endpoint, Sophos ZTNA, Sophos Switches und Wireless Access Points sowie Sophos XDR und Sophos MDR kann die Sophos Firewall automatisch auf Bedrohungen reagieren und Angriffe stoppen, bevor sie sich ausbreiten. Kompromittierte Hosts werden automatisch isoliert. So werden laterale Bewegungen und externe Kommunikationen unterbunden, bis eine Bedrohung analysiert und beseitigt wird.
	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. Das proaktive Threat Hunting erkennt Bedrohungen, bevor sie das Unternehmen oder die Organisation beeinträchtigen.
	Sophos Network Detection and Response (NDR)	Analysiert Datenverkehr kontinuierlich auf verdächtige Muster. In Kombination mit Sophos-verwalteten Endpoints und Firewalls überwacht Sophos NDR Netzwerkaktivitäten und erkennt verdächtige und schädliche Muster. Sophos NDR erkennt ungewöhnliche Datenverkehrsflüsse von nicht verwalteten Systemen und IoT-Geräten, nicht autorisierte Assets, interne Bedrohungen, bisher unbekannte Zero-Day-Angriffe und ungewöhnliche Muster tief im Netzwerk.
	Sophos Cloud Optix	Ermöglicht Unternehmen und Organisationen, Public-Cloud-Umgebungen nach Best Practices-Sicherheitsstandards von Amazon Web Services, Microsoft Azure und Google Cloud Platform einzurichten und zu verwalten. Sophos Cloud Optix sorgt für ein kontinuierliches Monitoring der Konfigurationsstandards, um Abweichungen zu erkennen. So können Sie versehentliche oder mutwillige Manipulationen 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 Bedrohungen auf Servern, Endpoints und Firewalls. So können auch komplexe Angriffe gestoppt werden.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
2. b) Bewältigung von Sicherheitsvorfällen;	Sophos Endpoint	Erkennt und blockiert automatisch 99,98 % aller Angriffe. Forensikbasierte Bereinigungsfunktionen entfernen sowohl den Schadcode als auch die von der Malware erstellten Registry-Schlüssel-Änderungen.
	Sophos Firewall	Die umfangreichen On-Box- und cloudbasierten Protokollierungs- und Reporting-Tools bieten direkt in Handlungen umsetzbare Erkenntnisse, um die Reaktion auf Vorfälle zu steuern und zu beschleunigen, einschließlich umfassender Informationen zu Netzwerkaktivitäten und einfachem Protokollzugriff für forensische Analysen. Die automatisierte Reaktion auf Bedrohungen (in Zusammenarbeit mit anderen Sophos-Produkten) reduziert die Reaktionszeit von Minuten auf Sekunden und stoppt Angriffe, bevor sie sich ausbreiten können.
	Sophos Managed Detection and Response (MDR) Complete	Umfasst standardmäßig eine unbegrenzte umfassende Vorfallsreaktion durch rund um die Uhr aktive 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)	Wenn Sophos NDR einen Indicator of Compromise, eine aktive Bedrohung oder einen Angreifer erkennt, werden die Analysten sofort benachrichtigt. So können sie direkt einen Bedrohungsfeed an die Sophos Firewall senden, um automatische Reaktionsmaßnahmen zum Isolieren des kompromittierten Hosts einzuleiten.
	Sophos XDR	Ermöglicht Analysten, Vorfälle auf allen wichtigen Angriffsflächen mithilfe vorhandener Sicherheitslösungen (von Sophos oder anderen Anbietern) eines Unternehmens/einer Organisation zu erkennen, zu analysieren und darauf zu reagieren. Sophos XDR speichert Sicherheitstelemetrie 90 Tage lang im Sophos Data Lake, um die Vorfallsbearbeitung zu erleichtern. Gleichzeitig beschleunigen optimierte Workflows und KI-basierte Funktionen die Vorfallsanalyse und -reaktion.
	Sophos Cloud Optix	Scannt Cloud-Ressourcen auf falsche Sicherheitskonfigurationen, erstellt ein Profiling aller Warnmeldungen nach Risikostufe, damit sich Teams auf die Prioritätsbereiche konzentrieren können, und bietet detaillierte Anweisungen zur Problembehebung.
	Sophos Rapid Response Service	Bietet unmittelbare 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 Bedrohungen auf Servern, Endpoints und Firewalls.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
2. c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;	Sophos Endpoint	Verwendet innovative und adaptive Sicherheitstechnologien, um Geschäftsunterbrechungen zu verhindern, einschließlich KI-basiertem Deep Learning, Anti-Exploit-Technologie und lückenlosem Ransomware-Schutz mit automatischem Rollback.
	Sophos Firewall	Die Plug-&-Play-Hochverfügbarkeits(HA)-Cluster der Sophos Firewall bieten Ausfallsicherheit bei Betriebsunterbrechungen. Mit Aktiv/Passiv-Redundanz müssen Kunden nur Lizenzen für das aktive Gerät erwerben und können so Kosten sparen. Für maximale Ausfallsicherheit unterstützt die Sophos Firewall auch mehrere Internetverbindungen mit Zero Impact Failover und Load Balancing über Wireless LTE, Kabel, DSL und Glasfaser. Umfassende Protokollierungen sowie On-Box- und cloudbasiertes Reporting liefern aussagekräftige Telemetriedaten, die die Notfallwiederherstellung erleichtern.
	Sophos Managed Detection and Response (MDR)	Minimiert das Risiko von Geschäftsunterbrechungen mit 24/7 Detection and Response. Im Falle eines Vorfalls wird ein kompletter Incident Response Service bereitgestellt. Durch die Integration mit Anbietern von Backup- und Recovery-Lösungen können Analysten erkennen, wenn Angreifer Backups ins Visier nehmen, sodass sie schnell eingreifen und den Angriff beseitigen können. Der Service speichert Sicherheitstelemetrie bis zu ein Jahr lang im Sophos Data Lake und erleichtert so die Notfallwiederherstellung.
	Sophos XDR	Speichert Sicherheitstelemetrie 90 Tage lang im Sophos Data Lake, was die Notfallwiederherstellung erleichtert. Durch die Integration mit Anbietern von Backup- und Recovery-Lösungen können Analysten erkennen, wenn Angreifer Backups ins Visier nehmen, sodass sie schnell eingreifen und den Angriff beseitigen können.
	Sophos Cloud Optix	Ermittelt, für welche Public-Cloud-Konten keine Backups angefertigt werden, und fordert das Sicherheitsteam innerhalb der Cloud-Optix-Konsole dazu auf, Maßnahmen zu ergreifen.
	Sophos Rapid Response Service	Bietet unmittelbare Soforthilfe durch ein Expertenteam beim Erkennen und Beseitigen aktiver Bedrohungen.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
2. d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;	Sophos Endpoint	Bietet umfassenden Schutz vor Bedrohungen, die über Drittanbieter in Ihre Umgebung gelangen. Schutzfunktionen, darunter KI-basiertes Deep Learning, Anti-Exploit, lückenloser Ransomware-Schutz mit automatischem Rollback und adaptive Abwehrmechanismen, die automatisch auf Bedrohungsaktivitäten
	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. Dank unternehmens-/organisationsübergreifender Integrationen mit Sicherheits- und Geschäftslösungen (einschließlich Microsoft und Google) können Bedrohungen in Ihrer Technologie-Lieferkette erkannt und abgewehrt werden.
	Sophos XDR	Ermöglicht Analysten, verdächtige Aktivitäten in ihrer Umgebung zu erkennen, zu analysieren und darauf zu reagieren, sodass sie Supply-Chain-Angriffe erkennen und stoppen können. Sophos NDR (ein Add-on zu Sophos XDR) ist tief im Netzwerk verankert und überwacht den gesamten Netzwerkverkehr, um Bedrohungen zu erkennen, die andere Lösungen übersehen – auch von Lieferkettenpartnern.
	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 Firewall	Die Sophos Firewall ist „Secure by Design" und wir arbeiten kontinuierlich daran, sie unantastbar für Hacker zu machen. Die Sophos Firewall bietet u. a.: › Integrierte Best Practices zur Optimierung der Kundensicherheit › Schutz vor Angriffen durch sicheres Remote-Management, Containerisierung, strenge Zugriffsverwaltung, MFA und vieles mehr › Automatisches Einspielen von Hotfixes zur Behebung dringender Sicherheitsprobleme › Proaktive Überwachung der globalen Firewall-Installationsbasis › Robustes und transparentes Programm zum Offenlegen von Schwachstellen mit marktführenden Bug-Bounty-Programmen

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
2. e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;	Sophos Managed Detection and Response (MDR)	Die Experten von Sophos MDR überwachen Warnmeldungen aus dem gesamten Netzwerk 24/7, analysieren verdächtige Aktivitäten und beseitigen Angriffe. Sophos NDR ist tief im Netzwerk verankert und überwacht den gesamten Netzwerkverkehr, um Bedrohungen zu erkennen, die andere Lösungen übersehen. 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. Sophos Managed Risk ist ein vollständig verwalteter Vulnerability Management Service, der Risiken identifiziert und risikobasierte Patching-Beratung bietet. Sophos Managed Risk arbeitet mit dem Sophos MDR-Service zusammen und ergänzt diesen. Sophos verpflichtet sich zu „Secure by Design“ Wir verfügen über ein robustes und transparentes Programm zum Offenlegen von Schwachstellen, einschließlich Safe-Harbor-Maßnahmen zur Unterstützung von Forschern und marktführenden Bug-Bounty-Programmen.
	Sophos XDR	Ermöglicht Analysten, Warnmeldungen aus dem gesamten Netzwerk rund um die Uhr zu überwachen, um verdächtige Aktivitäten zu analysieren und Angriffe zu beseitigen. Sophos NDR (ein Add-on zu Sophos XDR) ist tief im Netzwerk verankert und überwacht den gesamten Netzwerkverkehr, um Bedrohungen zu erkennen, die andere Lösungen übersehen.
	Sophos Cloud Optix	Scannt Cloud-Ressourcen auf falsche Sicherheitskonfigurationen, erstellt ein Profiling aller Warnmeldungen nach Risikostufe, damit sich Teams auf die Prioritätsbereiche konzentrieren können, und bietet detaillierte Anweisungen zur Problembehebung.
	Sophos Rapid Response Service	Bietet unmittelbare Soforthilfe durch ein Expertenteam beim Erkennen und Beseitigen aktiver Bedrohungen.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
2. f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im	Sophos Endpoint	Dank des integrierten Health Checks können Unternehmen und Organisationen Konfigurationsprobleme mit ihren Sophos-geschützten Geräten schnell erkennen und beheben. Sollte ein Problem erkannt werden, können Benutzer mit der Option „Automatisch beheben" unsichere Konfigurationen mit nur wenigen Klicks
	Sophos Firewall	Integrierte Statusreports ermöglichen Unternehmen und Organisationen, ihre Network-Security-Bereitstellung schnell zu bewerten und Optimierungsbereiche zu identifizieren.
	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 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.
	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.
2. h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;	Sophos Firewall	Ermöglicht MFA für VPN-Verbindungen, mit RADIUS/TACACS-Integration. Das in die Sophos Firewall-Systeme integrierte kryptographische Modul bietet FIPS 140-2-zertifizierte Kryptografie zum Schutz vertraulicher Informationen.
	Sophos Email	Bietet zur Sicherstellung von Compliance TLS-Verschlüsselung und Unterstützung von SMTP/S, PDF-Verschlüsselung von E-Mail Anhängen sowie Portalverschlüsselung.
	Sophos Wireless	Stellt dynamisch verschlüsselte WLAN-Verbindungen zum Schutz Ihrer Daten während der Übertragung in Netzwerken und auf Hotspots her, die von Sophos verwaltet werden.
	Sophos Central Device Encryption	Stellt die Durchsetzung von Festplatten-Verschlüsselung auf Windows und macOS Workstations sicher und ermöglicht dadurch die Überprüfung und Sicherstellung von Compliance.
	Sophos Mobile	Erzwingt Geräteverschlüsselung auf Mobilplattformen und ermöglicht dadurch die Überprüfung und Sicherstellung von Compliance.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
2. i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;	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. Das integrierte ZTNA bietet sicheren, benutzerbasierten Zugriff von jedem Standort. Rollenbasierte
	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, auch solche, die HR-Systeme, die Zugriffskontrolle und Gerätemanagement betreffen.
	Sophos XDR	Ermöglicht Analysten, Systemaktivitäten in der gesamten Sicherheitsumgebung zu überwachen und zu korrelieren, wodurch verdächtige Aktivitäten erkannt und analysiert werden können, auch solche, die HR-Systeme, die Zugriffskontrolle und Gerätemanagement betreffen.
	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 Cloud Optix	Unterstützt das Inventory Management für mehrere Cloud-Anbieter mit kontinuierlichem Asset Monitoring sowie vollständiger Visualisierung der Netzwerktopologie und des Datenverkehrs.
	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.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
2. j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung,	Sophos Firewall	Unterstützt flexible MFA-Authentifizierungsoptionen, einschließlich rollenbasierter Verwaltungskontrollen und Verzeichnisdiensten für den Zugriff auf wichtige Systembereiche. Das integrierte 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.
	Sophos ZTNA	Überprüft kontinuierlich die Benutzeridentität, den Gerätestatus und die Compliance, bevor Zugriff auf Anwendungen und Daten gewährt wird.
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)	Umfasst eine vollständige Reaktion auf Vorfälle und Ursachenanalyse. Sophos-Experten beheben den Vorfall und stellen einen vollständigen Experten-Bericht zur Verfügung. Dieser enthält eine detaillierte Analyse des Angriffsgeschehens und gibt Empfehlungen, wie die Umgebung vor künftigen Kompromittierungen geschützt werden kann.
	Sophos XDR	Ermöglicht Analysten, die gesamte Angriffskette zu identifizieren und Reports darüber zu generieren, einschließlich einer detaillierten Beschreibung des Vorfalls und der Angriffsursache.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
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)	Umfasst eine vollständige Reaktion auf Vorfälle und Ursachenanalyse. Sophos-Experten beheben den Vorfall und stellen einen vollständigen Experten-Bericht zur Verfügung. Dieser enthält eine detaillierte Analyse des Angriffsgeschehens und gibt Empfehlungen, wie die Umgebung vor künftigen Kompromittierungen geschützt werden kann.
	Sophos XDR	Ermöglicht Analysten, die gesamte Angriffskette zu identifizieren und Reports darüber zu generieren, einschließlich einer detaillierten Beschreibung des Vorfalls und der Angriffsursache.

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.

Dieses Whitepaper wurde in Zusammenarbeit mit Rechtsanwalt Andreas Daum und Rechtsanwalt Dr. Paul Vogel von Noerr Partnerschaftsgesellschaft mbB erstellt.

Endnoten

1 Die folgenden Verweise auf das BSIG n.F. beziehen sich auf das NIS2UmsuCG in der Fassung des Regierungsentwurfs vom 22.07.2024.

2024-10-17 DE-WP (MP)

SOPHOS