Die NIS2-Richtlinie

Die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS) war der erste EU-weite Rechtsakt zur Cybersicherheit und trat 2016 in Kraft. Um die innerhalb des derzeitigen Rahmenwerks festgestellten Einschränkungen zu adressieren und auf die zunehmenden Cybersecurity-Bedrohungen in der EU infolge der Digitalisierung und der COVID-19-Pandemie zu reagieren, hat die Europäische Kommission die NIS-Richtlinie durch die NIS2-Richtlinie ersetzt. Diese sieht strengere Aufsichtsmaßnahmen für nationale Behörden und strengere Durchsetzungsvorschriften vor und soll die Sanktionsregelungen zwischen den Mitgliedstaaten harmonisieren. Die NIS2-Richtlinie ist am 16. Januar 2023 in Kraft getreten und die Mitgliedstaaten haben 21 Monate Zeit, um die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umzusetzen.

Die NIS2-Richtlinie soll die Sicherheitsanforderungen in der EU erhöhen, indem ihr Anwendungsbereich auf weitere Sektoren und Einrichtungen ausgeweitet wird; dabei werden Maßnahmen wie Risikoanalyse und Sicherheitsrichtlinien für Informationssysteme, Bewältigung von Sicherheitsvorfällen und die Sicherheit von Lieferketten berücksichtigt und unter anderem die Berichtspflichten gestrafft. Bei Nichterfüllung der Pflichten müssen die Mitgliedstaaten gemäß NIS2 hohe Geldbußen auferlegen: 10 Mio. € oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist) für wesentliche Einrichtungen und 7 Mio. € oder 1,4 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist) für wichtige Einrichtungen. NIS2 verpflichtet die Leitungsorgane unmittelbar zur Umsetzung und Überwachung der Einhaltung der Rechtsvorschriften durch ihre Organisation. Bei Verstößen gegen diese Richtlinie kann die Ausübung von Leitungsaufgaben auf Geschäftsführungs- bzw. Vorstandsebene der Einrichtung vorübergehend untersagt werden.

In diesem Dokument wird erläutert, wie Sophos-Lösungen Unternehmen und Einrichtungen bei der Umsetzung von Kapitel IV der NIS2-Richtlinie, **Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit**, unterstützen und ihnen bei der Einhaltung der NIS2-Richtlinie helfen.

NIS2-Richtlinie – Kapitel IV, Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit

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.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

2023-03-15 RC-DE (PS)

SOPHOS