SOPHOS

Die NIS-2-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 NIS-2-Richtlinie ersetzt. Diese sieht strengere Aufsichtsmaßnahmen für nationale Behörden und strengere Durchsetzungsvorschriften vor und soll die Sanktionsregelungen zwischen den Mitgliedstaaten harmonisieren. Die NIS-2-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 NIS-2-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 NIS 2 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. NIS 2 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 NIS-2-Richtlinie, Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit, unterstützen und ihnen bei der Einhaltung der NIS-2-Richtlinie helfen.

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.
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.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
	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.
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.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
	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.
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.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
	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.
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 reagieren.
	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
	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 Bereich der Cybersicherheit;	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 korrigieren.
	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 Verwaltungskontrollen, Multi-Faktor-Authentifizierung und granulare Zugriffskontrollen sind ebenfalls enthalten.
	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.
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 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. Zum Regeln des Zugriffs sind zudem granulare Zugriffskontrollen in die Sophos Firewall integriert.
	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.

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
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.
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.

2024-08-26 (WP-NP)

SOPHOS