WHITEPAPER

NIS2 - Der Countdown läuft:

Wie Sie das Bewusstsein und die Umsetzung bei Führungskräften fördern

Phil MUNCASTER



MADE IN EU

ESET Cybersecurity Progress. Protected.

EVERSHEDS SUTHERLAND

Inhaltsverzeichnis

Wo ist der Unterschied zwischen NIS & NIS2? 3

Einführung 4

Was ist neu in NIS2? 6

Wie man mit dem Management über NIS2 spricht 7

Planung eines NIS2-Compliance-Programms 11

Diese 3 Konzepte sind der Schlüssel zum Erfolg 12

Fazit: Zeit zum Handeln 12

Angriffe minimieren und NIS2 einhalten 13

Wo ist der Unterschied zwischen NIS & NIS2?

	NIS	NIS2
ANWENDUNGSBEREICH	Begrenzter Kreis an Betreibern wesentlicher Dienste (OES) und Anbietern digitaler Dienste (DSP). Zu OES gehören: Verkehr, Banken, Finanzmärkte, Trinkwasser, digitale Infrastruktur, Energie, Gesundheit.	Breiteres Spektrum an Sektoren, die zusätzlich erfasst werden: Post/Kurierdienst, verarbeitendes Gewerbe, Abwasser/Verwaltung, öffentliche Verwaltung, Raumfahrt, Forschung, digitale Dienstleistungen, Lebensmittelherstellung/-vertrieb, Anbieter elektronischer Kommunikationsdienste, Chemie, breiteres Spektrum an regulierten Themen.
SECURITY / REPORTING	Vage Anforderungen an OES und DSPs, "angemessene" Sicherheitsmaßnahmen anzuwenden und Vorfälle zu melden, die den Geschäftsbetrieb "erheblich beeinträchtigen". Es gilt, die Regulierungsbehörde innerhalb von 72 Stunden zu benachrichtigen.	10 vorgeschriebene Basissicherheitsmaßnahmen (siehe Seite 6). Plus Meldepflicht, die Aufsichtsbehörde "unverzüglich" oder innerhalb von 24 Stunden über einen Vorfall zu informieren und innerhalb von 72 Stunden einen offiziellen Bericht zu erstellen. Organisationen haben auch Prüfungspflichten.
DURCHSETZUNG	Die Mitgliedstaaten können ihre eigenen Schwellenwerte für finanzielle Strafmaßnahmen festlegen.	Vereinheitlichte Durchsetzungsvorschriften. Geldbußen für wichtige Unternehmen von bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist). Geldbußen für wichtige Unternehmen von bis zu 7 Mio. EUR oder 1,4 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist).
RECHENSCHAFTSPFLICHT	Leitende Angestellte werden nicht direkt für Vorfälle verantwortlich gemacht.	Bei grober Fahrlässigkeit können Führungskräfte persönlich für die Nichteinhaltung der Vorschriften haftbar gemacht werden.

Einführung

Nach Angaben der Europäischen Kommission werden die jährlichen Kosten der Cyberkriminalität für die Weltwirtschaft bis Ende 2020 auf 5,5 Billionen Euro geschätzt, und bis 2025 wird sich dieser Betrag voraussichtlich verdoppeln. Wäre dies das Bruttoinlandseinkommen eines Landes, wäre es reicher als alle anderen Länder außer den USA und China.

Viele dieser Angriffsziele sind Anbieter kritischer nationaler Infrastrukturen (CNI) sowie deren Partner und Zulieferer. Als Reaktion auf die Attacken und die zunehmende Bedrohungslage für Nationalstaaten hat die Europäische Kommission eine neue Version ihrer **EU-Richtlinie zur Netz- und Informationssicherheit (NIS)** vorgelegt.

Die Frist für Mitgliedsstaaten, die NIS2-Anforderungen in nationales Recht umzusetzen, ist der 17. Oktober 2024. Da es sich um eine EU-Richtlinie (und nicht um eine Verordnung) handelt, werden die einzelnen Länder die Regeln leicht unterschiedlich definieren. Unternehmen, die die Vorschriften einhalten wollen, werden warten müssen, bis die in ihrem eigenen Land umgesetzten Versionen der NIS2 veröffentlicht werden. Erst dann werden Firmenlenker wissen, welche Compliance-Anforderungen und Zeitpläne gelten. Unabhängig davon können Organisationen schon heute einiges tun, um sich auf die neue Richtlinie vorzubereiten.

Ziel der NIS2-Richtlinie ist es, die Cyber-Resilienz in weitaus mehr Unternehmen zu verbessern, die in der EU wesentliche oder wichtige Funktionen erfüllen. Außerdem ist die Richtlinie darauf ausgelegt, Unstimmigkeiten bei den erwarteten Standardmaßnahmen zum Cyber-Risikomanagement in den EU-Mitgliedstaaten zu verringern.

Darüber hinaus soll der Informationsaustausch zwischen den zuständigen Behörden verbessert und sollen klare Regeln für die Reaktion auf Vorfälle im Falle einer großen Krise und für die Meldung im Allgemeinen aufgestellt werden.

Eine einzige Datenschutzverletzung kostet heute schätzungsweise durchschnittlich 4,5 Mio. Dollar (4,1 Mio. €) und damit so viel wie nie zuvor. Bei einem schwerwiegenden Ransomware-Angriff, der auch kritische Dienste außer Betrieb setzt, könnte diese Summe sogar um ein Vielfaches steigen. Das europäische Beratungsunternehmen Sopra Steria gab zu, dass der Ransomware-Angriff im Jahr 2020 das Unternehmen wahrscheinlich bis zu 50 Millionen Euro gekostet hätte.

Bei der Einhaltung der NIS2-Richtlinie geht es um die Verbesserung der Resilienz von Organisationen, Versorgungssicherheit der Gesellschaft sowie eine Zusammenarbeit bei der IT-Sicherheit in Europa. Aber auch Geschäftsführer und Vorstände rücken in den Fokus. Sie können nun persönlich für die Nichteinhaltung der Vorschriften haftbar gemacht werden, wenn ihnen nachgewiesen werden kann, dass der Vorfall durch schwere Fahrlässigkeit verursacht wurde.

All dies sind überzeugende Gründe, warum CISOs die Chefetage zur Einhaltung von NIS2 drängen sollten. Dabei sollten sie den Prozess nicht nur als Risikominderung bewerten, sondern auch bewusst machen, dass die Einhaltung der Vorschriften das Geschäft fördert. Wer die damit verbundenen Herausforderungen als Vorteil begreift, kann die richtigen Voraussetzungen schaffen, um eine erfolgreiche digitale Transformation und ein nachhaltiges Wachstum im Unternehmen voranzutreiben.

In diesem Whitepaper erfahren Sie, wie CISOs und die Führungsebene diese Ziele erreichen.

Türöffner statt Bremsklotz:
Mit Einhaltung der NIS2-Richtlinie kann die Führungsebene zum einen verhindern, dass sie persönlich haftbar gemacht wird, sollte grobe Fahrlässigkeit bei einem Vorfall vorliegen, zum anderen kann die Erfüllung der Vorschriften auch das Geschäft fördern.

Wenn Unternehmen die damit verbundenen Herausforderungen als Chance begreifen, können sie den richtigen Rahmen für eine erfolgreiche digitale Transformation und nachhaltiges Wachstum schaffen.

Was ist neu in NIS2?

Die NIS2 enthält mehrere wesentliche Änderungen gegenüber der ursprünglichen Richtlinie. Die wichtigsten davon sind:

EIN BREITERER ANWENDUNGSBEREICH

NIS2 wird Organisationen in den Sektoren betreffen, die als Anbieter „wesentlicher" oder „wichtiger" Dienstleistungen gelten. In Deutschland spricht man hier von "wichtigen" und "besonders wichtigen Einrichtungen", sowie Betreibern kritischer Anlagen. Zu den ersteren gehören große Unternehmen aus sehr kritischen Sektoren wie dem Energiesektor und dem Gesundheitswesen sowie einige Sonderfälle. Zu letzteren gehören große Betreiber aus anderen kritischen Sektoren, wie Anbieter digitaler Dienste und Hersteller sowie mittlere Betreiber.

HÖHERE STRAFEN

Die NIS2-Regulierungsbehörden können gegen einige Unternehmen Geldstrafen in Höhe von bis zu 2 % des Jahresumsatzes bzw. 10 Mio. EUR für schwerwiegende Verstöße verhängen. Und einige Strafen können fortlaufend verhängt werden.

PERSÖNLICHE HAFTUNGSRISIKEN

Geschäftsführer und Vorstände werden direkt für den Cyber-Schutz in ihrem Unternehmen verantwortlich gemacht. Führungskräfte oder leitende gesetzliche Vertreter können bei Fahrlässigkeit, die zu einer schwerwiegenden Sicherheitsverletzung führt, können sie sogar zeitweilig vom Dienst freigestellt werden. Sie müssen Cybersicherheitsschulungen erhalten und regelmäßige Risikobewertungen durchführen.

SICHERHEIT DER LIEFERKETTE

Unternehmen müssen das Risiko Dritter durch „geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen" bewerten und steuern. Dies muss mit einer koordinierten Risikobewertung beginnen.

MINDESTSICHERHEITSANFORDERUNGEN

Mit NIS2 wird ein Standard an Maßnahmen eingeführt, die alle Organisationen einhalten müssen. Dazu gehören:

- Risikoanalyse und Informationssicherheitspolitik
- Vorfallmanagement zur Vorbeugung, Aufdeckung und Reaktion auf Vorfälle
- Geschäftskontinuität und Krisenmanagement, einschließlich Notfallwiederherstellung
- Sicherheit der Lieferkette
- Sicherung der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Schwachstellenmanagement
- Testen und Prüfen von Maßnahmen des Cyber-Risikomanagements
- Grundlegende Cyber-Hygiene, einschließlich Cybersicherheitsschulungen
- Richtlinien und Verfahren in Bezug auf die Verwendung von Kryptografie und Verschlüsselung
- HR-Sicherheit, einschließlich Zugangskontrollrichtlinien und Vermögensverwaltung
- Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung; sichere Sprach-, Video- und Textkommunikation und sichere Notfallkommunikationssysteme

Wie man mit dem Management über NIS2 spricht

Die Bedeutung der Cybersicherheit für den Unternehmenserfolg rückt immer mehr in das Bewusstsein der Managementebene. In einer Studie des Weltwirtschaftsforums (WEF) aus dem Jahr 2023 heißt es, dass "die globale geopolitische Instabilität dazu beigetragen hat, die Wahrnehmungslücke zwischen den Ansichten von Unternehmens- und Cyber-Führungskräften über die Bedeutung des Cyber-Risikomanagements zu schließen".

Trotz dieser Entwicklung hält sich nach wie vor der alte Glaube, dass Cybersicherheit eine rein operative IT-Angelegenheit und keine strategische Geschäftsfunktion ist. Eine PwC-Umfrage aus dem Jahr 2022 zeigt, dass nur zwei Fünftel (41 %) der Direktoren glauben, dass ihr Management Sicherheitsrisiken "sehr gut" verstehen. Weitere Daten zeigen, dass nur 5 % der europäischen Führungskräfte über Erfahrungen im Bereich Cybersicherheit verfügen.

Das macht die Herausforderungen für CISOs noch größer, wenn sie versuchen, den Geschäftsführern die Bedeutung der NIS2-Compliance zu vermitteln. Gartner® erkennt 8 "häufige Fehler bei der Präsentation bei der Führungsetage":

Was oft präsentiert wird		Was das Management braucht
zu lang	≠	eine klare Botschaft, warum die Chefetage die Informationen erhält
zu technisch		Prägnanz
zu operativ ausgerichtet		Keine oder begrenzte technische Fachsprache
auf Vergangenheit statt Zukunft gerichtet		zukunftsweisende Botschaften mit Fokus auf Wertsteigerung
Keine bestimmte Bitte von oben		Relevanter, vertretbarer Beweis zur Stärkung der Position
zu viele (und überflüssige) Informationen		Direkte Bezüge zu Vorstandsinteressen (Umsatz, Kosten, Risiko)
keinen Bezug zu den Interessen der Führungsetage (Umsatz, Kosten, Risiko)		Klare, pragmatische Empfehlungen zur Unterstützung der Entscheidung
Zeigt keinen klaren Weg nach vorn		

zu berücksichtigende Faktoren beim Reporting ans Management

- Art des Managements
- Gesetzeslandschaft
- Thema der Präsentation
- Industriezweig
- Art der Organisation
- Profil der Zielgruppe und deren Rolle
- Cyber-Wissensstand der Zuhörer
- Häufigkeit des Reporting
- Geografische Lage

Quelle: Gartner®, CISO Foundations: Comprehensive Resource List for Presenting Cybersecurity to the Board of Directors, Ursprünglich veröffentlicht am 8. August 2022. Aktualisiert am 26. September 2023. GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seinen Tochtergesellschaften in den USA und international und wird hier mit Genehmigung verwendet. Alle Rechte vorbehalten.

Abbildung 1: Häufige Fehler bei Präsentationen bei der Führungsetage vs. was das Leitungsgremium sucht

Bei der Vermittlung von der Tragweite des Themas sollten CISOs Folgendes sicherstellen:

SPRECHEN SIE DIE RICHTIGE SPRACHE UND HALTEN SIE SICH KURZ

Der erste Schritt auf dem Weg zu einer engeren Abstimmung zwischen Cybersicherheit und Unternehmen bei der Einhaltung von NIS2 ist es, verstanden zu werden. Das bedeutet, dass man die Sprache der unternehmerischen Risiken spricht und nicht die Sprache der Bits, Bytes und der komplexen technischen Details, die sich in der Tiefe abspielen. CISOs sollten auf den Fachjargon verzichten und ihre Sprache einfach, klar und verständlich gestalten. Anekdotische Geschichten aus dem Unternehmen oder von Mitbewerbern können ebenfalls dazu beitragen, einen Punkt zu verdeutlichen. Mit konkreten Beispielen zu erklären, was einem Unternehmen passiert, wenn es IT-Sicherheitsregeln nicht einhält, kann ein überzeugendes Mittel sein, um die Meinung der Vorstandsetage zu beeinflussen.

Unabhängig vom Inhalt sollten sich CISOs auch bewusst sein, dass ihre Zuhörer eine begrenzte Aufmerksamkeitsspanne haben. Sie sollten sich also auf die wichtigsten Punkte konzentrieren, die Zahl ihrer Folien auf eine Handvoll beschränken und sicherstellen, dass die Präsentation kurz und ansprechend ist.

ZEIGEN SIE DEN WERT FÜRS GESCHÄFT

CISOs sollten darauf gefasst sein, dass der Vorstand verlangt, die Einhaltung der NIS2-Richtlinie mit ihrem bestehenden Budget zu erreichen. Wer vorlegt, was durch Compliance eingespart werden kann, hat gute Chancen, den CFO und Vorstand auf seine Seite zu bringen.

MACHEN SIE DAS THEMA FÜR DIE ZUHÖRER RELEVANT

Relevanz ist alles. Man sollte nicht nur Kennzahlen und Geschäftsrisiken veranschaulichen, sondern auch welche möglichen Folgen bei NIS2-Compliance-Verstößen auf sie zukommen. Denn in der neuen Richtlinie können CEO und Vorstand bei grober Fahrlässigkeit persönlich in die Verantwortung und Haftung genommen werden.

CISOs sollten allerdings auch die potenziellen Auswirkungen aufzeigen, wie den finanziellen Schaden oder den Reputationsverlust, die bei Nichteinhaltung der NIS2-Vorgaben durch schwerwiegende Sicherheitsverletzungen entstehen könnte. Mögliche Folgen sind:

- Reaktion nach einem Sicherheitsverstoß, einschließlich Geldstrafen und Anwaltskosten
- Forderungen nach Audit- und Compliance-Nachweisen, die bei Nichteinhaltung zu Geldbußen seitens der Aufsichtsbehörden führen können
- Geschäftseinbußen, darunter unmittelbare Unterbrechungen des Betriebs/der Produktion, verlorene Kunden und die Unfähigkeit, neue Kunden zu werben

Im Rahmen dieser Diskussion kann es sinnvoll sein, die Beteiligten auch zu informieren, wie die Aufsichtsbehörden die neue Richtlinie durchsetzen werden. Bei beiden Arten von Unternehmen (wesentlich und wichtig) werden die zuständigen Stellen befugt sein, Inspektionen vor Ort und nachträgliche Kontrollen außerhalb des Unternehmens sowie Ad-hoc-Sicherheitsprüfungen, Sicherheits-Scans und Anfrage auf Datenzugriff durchzuführen. Letzteres könnte auch die Forderung von Nachweisen für die Umsetzung von Cybersicherheitsrichtlinien beinhalten, wie z. B. die Ergebnisse von Sicherheitsaudits durch Dritte.

Bußgelder für wesentliche Organisationen bis zu

10 Mio. €

oder 2% des globalen Jahresumsatzes

Bußgelder für wichtige Organisationen bis maximal

7 Mio. €

oder mind. 1,4% des globales Jahresumsatzes (je nachdem, welcher Betrag höher ist.)

EXISTENZIELLE RISIKEN AUFZEIGEN

Die NIS2-Richtlinie wurde entwickelt, um die Cybersicherheit in der EU zu stärken und Unternehmen dazu zu verpflichten, angemessene Sicherheitsmaßnahmen zu ergreifen, um ihre Netzwerke und Informationssysteme zu schützen. Beispiele für Schäden durch Cyberangriffe gibt es zuhauf und belegen die Wichtigkeit einheitlicher Standards. Gerade eine umfassende Risikoanalyse und -bewertung aller Geschäftsprozesse muss stattfinden und kann Schwachstellen aufzeigen. Einen Ausfall der IT-Systeme kann sich keine Organisation erlauben. Schlimmstenfalls bedeutet eine Unterbrechung den wirtschaftlichen Ruin.

NENNEN SIE GUTE GRÜNDE FÜR COMPLIANCE

CISOs sollten die Einhaltung von NIS2 nicht nur als Risikovermeidung sehen. Es gibt auch ein starkes Argument für die Erschließung neuer Geschäftspotenziale. Konkret hieße das:

- Senkung der Betriebskosten durch Vermeidung oder Minimierung von Ausfallzeiten, Bußgeldern und anderen oben genannten Kosten für Sicherheitsverletzungen.
- Steigerung des Umsatzes, indem Sie das Unternehmen dabei unterstützen, sich abzuheben und Kunden anzusprechen, die Wert auf IT-Sicherheit und Datenschutz legen. Etwa 87% der Verbraucher geben an dass sie ihre Geschäfte woanders tätigen, wenn sie nicht darauf vertrauen können, dass ein Unternehmen verantwortungsvoll mit ihren Daten umgeht. Ein wichtiges Unterscheidungsmerkmal im Wettbewerb sind freiwillige Zertifizierungen wie die ENISA-Zertifizierung der EU oder Zertifizierungen und Prüfberichte, die für bestimmte Branchen relevant sind.
- Differenzierung und Akquise von Geschäftspartnern, denen Sicherheit wichtig ist. Die meisten Organisationen, an die Sie liefern oder mit denen Sie Business machen, werden eine vollständige NIS2-Konformität verlangen, so dass Sie sie abdecken sollten. Und das Gleiche sollten Sie auch von Ihren Lieferanten fordern.
- Verbesserung der internen Effizienz durch optimierte Prozesse und weniger Fehler.
- Förderung des innovationsgetriebenen Wachstums, indem Sie eine stabile und sichere Grundlage für die digitale Transformation schaffen.

BEGREIFEN SIE NIS2-COMPLIANCE ALS SECURITY-BOOSTER

Die Einhaltung von NIS2 ist kein Nice-to-have. Sie ist das Gesetz. Sie sollten Führungskräften raten, auf die national umgesetzten NIS2-Vorschriften zu achten, wenn sie im Oktober 2024 gelten. Sie werden dann genauer wissen, wo noch Lücken bei der Compliance bestehen und welche Investitionen noch erforderlich sind.

CISOs sollten die Chance ergreifen, größere Investitionen in Sicherheitsinitiativen seitens der Geschäftsleitung zu tätigen. Dies könnte der richtige Zeitpunkt sein, um zum Beispiel die Notwendigkeit eines langfristigen Best-Practice-Zero-Trust-Programms zu fördern.

Wie immer können Messwerte helfen, die Argumente zu untermauern. Laut der EU-Sicherheitsagentur ENISA sind 62 % der Betreiber wesentlicher Dienste und Anbieter digitaler Dienste in der EU der Ansicht, dass die Umsetzung der ersten NIS-Richtlinie direkte und positive Auswirkungen auf die Erkennung von Bedrohungen hatte. Und ein Fünftel (21 %) sagt dasselbe über ihre Fähigkeit, sich schnell von einem Vorfall zu erholen.

62%

der Dienstleistungsbetreiber und Anbieter digitaler Dienste in der EU sind der Meinung, dass sich die NIS-Richtlinie positiv auf die Erkennung von Bedrohungen ausgewirkt hat.

Quelle: *ENISA, NIS Investments, November 2022*.

21%

sagen das Gleiche über ihre Fähigkeit, sich schnell von einem Vorfall zu erholen.

Quelle: *ENISA, NIS Investments, November 2022*.

Planung eines NIS2-Compliance-Programms

Sobald die Führungsetage der Finanzierung eines NIS2-Compliance-Programms zugestimmt hat, ist es an der Zeit, den Grundstein für den Start des Projekts zu legen. Der erste Schritt besteht darin, festzustellen, ob das Unternehmen eine wesentliche oder wichtige Einrichtung ist. Davon hängt ab, welche Regeln sie befolgen muss und welche Strafen bei Nichteinhaltung drohen.

Als Nächstes sollten Sie Folgendes berücksichtigen :

1. **Umfang ermitteln:** Was sind die regulierten Dienstleistungen? Wie kann die Organisation sie in Bezug auf Vermögenswerte, Organisationseinheiten gestalten/formulieren?

2. **GAP-Analyse durchführen:** Bewertung der bestehenden Sicherheitslage und Analyse von Bereichen, in denen die NIS2 nicht eingehalten wird, sowie andere Schwachstellen. Die Ergebnisse sollten umsetzbare Empfehlungen zur Verbesserung der Sicherheitskontrollen, Verwaltung und anderer kritischer Bereiche liefern.

3. **Compliance-Programm planen:** Darin sollten Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter und Management im Einklang mit den neuen Anforderungen von NIS2 enthalten sein.

4. **Staatliche Beihilfen prüfen:** Zur Finanzierung der NIS2-Compliance-Maßnahmen hat die Europäische Kommission einen großen Topf mit Mitteln bereitgestellt, um speziell KMU zu helfen.

5. **Plan ausführen**

6. **Audits/ Vorprüfungen durchführen:** Kontrolle, inwieweit die Vorschriften eingehalten werden.

7. **Plan anpassen:** Fahren Sie ggf. mit Punkt 3 fort, bis die Anforderungen erfüllt sind.

Diese 3 Konzepte sind der Schlüssel zum Erfolg

Zehntausende von Unternehmen in der EU werden in den Anwendungsbereich der neuen NIS2-Richtlinie fallen. Einige werden in der Lage sein, die Einhaltung intern zu bewältigen. Viele kleinere Unternehmen werden sich allerdings externes Fachwissen und möglicherweise auch Finanzmittel beschaffen müssen, um die Umsetzung vor dem Stichtag im Oktober 2024 voranzutreiben.

Im Zuge dieses Prozesses sollten CISOs drei Schlüsselkonzepte im Auge behalten: Kommunikation, Bewusstsein und kollektive Resilienz. Kommunikation und Bewusstseinsbildung sind auf Führungsebene von entscheidender Bedeutung, um zum einen die notwendige Finanzierung zu sichern. Zum anderen auch dafür zu sorgen, dass die Chefetage über das richtige Maß an Wissen und Engagement verfügt, um wichtige Risikomanagemententscheidungen zu treffen. Vor allem aber geht es darum, umfassende, europaweite kollektive Verteidigungsstrategien gegen Cyber-Bedrohungen aufzubauen.

Fazit: Zeit zum Handeln

Laut der WEF-Umfrage sind die meisten Geschäfts- und Cybersicherheitsführer der Meinung, dass geopolitische Spannungen in den nächsten zwei Jahren „mäßig" (93 %) oder „sehr wahrscheinlich" (86 %) zu einem verheerenden Cyber-Vorfall führen werden. Es stehen viele Dinge auf dem Spiel. Aus diesem Grund wurde die NIS2-Richtlinie entwickelt - nicht nur, um die Cyber-Resilienz in der gesamten EU zu verbessern, sondern auch, um sie zu einem Thema auf Führungsebene der wichtigsten Dienstleister zu machen. Wenn, wie die frühere IBM-Chefin Ginni Rometty behauptet, der CEO von heute auch der Chief Risk Officer seines Unternehmens sein muss, dann muss das Thema Cybersecurity im Mittelpunkt aller Überlegungen stehen, die er zur künftigen Ausrichtung des Unternehmens anstellt. Nichtsdestotrotz ist es den meisten (72 %) immer noch unangenehm, sicherheitsrelevante Entscheidungen zu treffen. Das muss sich ändern, und NIS2 wird diesen Wandel herbeiführen.

Eine große Verantwortung lastet auf den Schultern des CISO. Er muss die Führungsriege und den CEO von der Tragweite der NIS2-Compliance überzeugen – zum einen, um Geschäftsrisiken zu vermeiden. Zum anderen muss er dafür sorgen, dass das Unternehmen wachsen und die digital Transformation umsetzen kann. Und sie sind es, die den Kurs bestimmen, damit die Vorschriften auch eingehalten werden, einschließlich wichtiger Schulungen und der Sensibilisierung von Führungskräften. Dies wird nicht einfach sein, aber die CISOs, die erfolgreich sind, können ihre eigene Rolle und ihre Karriereaussichten verbessern.

Der Arbeitsaufwand hängt davon ab, wie ausgereift die bestehenden Sicherheitsvorkehrungen und -prozesse des Unternehmens sind und wie stark das Engagement der oberen Führungsebene ist. Doch wie jedes Compliance-Programm ist auch NIS2 eine kontinuierliche Reise und kein Ziel. Sicher ist nur, dass die Reise jetzt beginnen muss.

ANGRIFFE MINIMIEREN UND NIS2 EINHALTEN

VULNERABILITY & PATCH MANAGEMENT

Die Lösung identifiziert Schwachstellen in Betriebssystemen sowie gängigen Anwendungen, einschließlich automatischer Patches für alle Endgeräte über ESET PROTECT.

MANAGED DETECTION & RESPONSE

ESET Service zur Vermeidung, Erkennung, Analyse und Behebung von Bedrohungen, ohne dass dabei eigene Personal-, Hardware- oder Softwareressourcen von Nöten sind.

EXTENDED DETECTION & RESPONSE (XDR)

Die EDR-Lösung von ESET dient zur Vorbeugung, Erkennung und Behebung von Sicherheitsvorfällen, inklusive forensischen Einblicken.

ESET THREAT INTELLIGENCE (ETI)

Bietet globales Wissen über gezielte Angriffe, Advanced Persistent Threats (APTs), Zero Days und Botnet-Aktivitäten, das von ESET Experten gesammelt wird.

ESET ENDPOINT ENCRYPTION

Verschlüsselung ermöglicht einen optimalen Schutz u.a. für bestimmte Dateien, Ordner, virtuelle Festplatten oder Archive und hilft bei der Einhaltung von Richtlinien wie DSGVO.

ESET PROTECT PLATFORM

ESET PROTECT bietet ein vollständiges Security Management mit Funktionen zur Prävention, Erkennung und Reaktion, ergänzt durch ESET Managed & Professional Services.

Rundum-Schutz mit 24/7 MDR Service
Erfahren Sie mehr zu **ESET PROTECT MDR**

JETZT INFORMIEREN

ESET Lösungen für NIS2-Compliance

In Deutschland wurde mit dem NIS-2-Umsetzungsgesetz, das im Dezember 2025 in Kraft trat, unter anderem das BSI-Gesetz (BSIG) grundlegend überarbeitet und erweitert. Von besonderer Bedeutung für viele Unternehmen sind die neu hinzugekommenen Paragraphen zu Risikomanagement (§ 30) und Meldepflichten (§ 32), die nun für deutlich mehr Sektoren und Einrichtungen gelten (siehe § 28). Die folgende Übersicht zeigt unseren Ansatz für eine mögliche Umsetzung der geforderten IT-Sicherheitsmaßnahmen unter Einsatz von ESET Lösungen.

In Österreich wurde das NIS-2-Umsetzungsgesetz im Dezember 2025 veröffentlicht und tritt im Oktober 2026 in Kraft. Weitere Informationen finden Sie ↗hier.

Bitte beachten Sie, dass unsere Inhalte keine rechtliche Beratung ersetzen. Bitte wenden Sie sich für Ihren konkreten Fall an eine Rechtsanwältin oder einen Rechtsanwalt Ihres Vertrauens.

Übrigens: Das BSIG beinhaltet für die unter das Gesetz fallenden privaten und öffentlichen Einrichtungen **umfangreiche Berichtspflichten**. Dazu gehört, dass Einrichtungen laut § 32 Abs. 1 BSIG einen erheblichen Sicherheitsvorfall **innerhalb von 24 Stunden** der zuständigen Behörde melden müssen. **Innerhalb von 72 Stunden** sollen zudem **Kompromittierungsindikatoren** (IoCs) benannt werden und **nach einem Monat soll ein umfassender Abschlussbericht** vorgelegt werden. Bei der Bereitstellung solch umfangreicher Dokumentationen können Extended Detection & Response (XDR) Lösungen wie ESET Inspect unterstützen.

§ 30 Abs. 2 BSIG:

Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

BSIG im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,	Wir von ESET bzw. unsere Vertriebspartner unterstützen Sie bei der technischen Bewertung, Erstellung und Umsetzung von passenden IT-Sicherheitskonzepten entsprechend Ihrer Kundenumgebung.		Unter Umständen Bestandteil der Presales-Phase			
	Mit unserer Management-Konsole haben Sie dank Hard- und Software-Inventarisierung Ihre schützenswerten Assets im Blick und verfügen damit über eine zuverlässige Grundlage für die Risikoanalyse sowie die Erstellung Ihres Sicherheitskonzepts.	ESET PROTECT	✓	✓	✓	✓
2. Bewältigung von Sicherheitsvorfällen,	Unser Extended Detection & Response Tool ermöglicht eine umfassende Gefahrensuche und -abwehr. Ereignisse im Netzwerk werden protokolliert und zu Vorfällen zusammengefasst, sodass Sie einen Überblick darüber haben, was in Ihrer IT-Umgebung vor sich geht. So können Sie bei einem Sicherheitsvorfall schnell reagieren. Dank festgelegter Reaktionsmaßnahmen wird das Sicherheitsniveau zudem weiter gesteigert.	ESET Inspect (in Kombination mit ESET PROTECT)	✓	✓	✓	
	ESET Experten übernehmen den operativen Betrieb Ihrer ESET Inspect Instanz und damit die Überprüfung, Auswertung und Interpretation aller Daten sowie die Reaktion auf mögliche Sicherheitsvorfälle.	ESET MDR Ultimate	✓			
	Mit dem KI-gestützten Managed Detection & Response Service haben auch Unternehmen mit weniger finanziellen Ressourcen die Möglichkeit, von der Expertise der ESET Spezialisten zu profitieren. Durch die Anbindung an das ESET-eigene Security Information and Event Management (SIEM) Tool wird ESET Inspect mit den nötigen Daten versorgt, um automatisiert auf verdächtige Aktivitäten innerhalb der Unternehmensumgebung zu reagieren.	ESET MDR		✓		
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,	ESET bietet keine spezielle Backup-Management-Lösung.					
	ESET Experten übernehmen für Sie den operativen Betrieb Ihrer ESET Inspect Instanz – dazu gehört auch die Reaktion auf akute Vorfälle, einschließlich der Eindämmung und Isolierung einer Bedrohung – und unterstützen Sie so dabei, den Betrieb im Falle eines Vorfalls aufrecht zu erhalten.	ESET MDR Ultimate	✓			

BSIG im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,	Prävention ist unsere Expertise. ESET Sicherheitslösungen erkennen und wehren Bedrohungen wie Viren, Ransomware, Phishing oder Spam zuverlässig ab[1] und verhindern damit auch deren Ausbreitung auf andere Organisationen. Unsere Schutzlösungen für Clients, Mobilgeräte, Server und Cloud-Anwendungen bilden die Basis. Ergänzt werden sie durch unsere cloudbasierte Sandboxing-Lösung ESET LiveGuard® Advanced, die selbst Zero-Days zuverlässig erkennt.	ESET Endpoint Security | ESET Server Security | ESET Mail Security | ESET Security for Microsoft SharePoint Server ESET LiveGuard® Advanced	✓	✓	✓	✓
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,	Der Großteil unserer Produkte und Services ist nach ISO 27001 und ISO 9001 zertifiziert. Die Zertifizierung umfasst alle Unternehmensprozesse von der sicheren Programmierung bis hin zum Vertrieb. Damit gewährleisten wir ein hohes Maß an Produktqualität sowie Informationssicherheit im eigenen Haus.		✓	✓	✓	✓
	Unsere Schwachstellen- und Patch-Management-Lösung sorgt dafür, dass Sicherheitslücken auf Endgeräten und Servern umgehend erkannt und behoben werden.	ESET Vulnerability & Patch Management	✓	✓	✓	✓
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,	Dank regelmäßiger, automatisch generierbarer Reports mit relevanten Sicherheitsereignissen und Kennzahlen behalten Sie den Überblick über den Sicherheitsstatus in Ihrem Unternehmensnetzwerk. Hierdurch lässt sich zudem nachverfolgen und belegen, dass festgelegte Schutzmaßnahmen tatsächlich greifen. Darüber hinaus können Sie aus den Erkenntnissen der Reports Maßnahmen zur weiteren Verbesserung Ihres Schutzes ableiten und so Ihr Sicherheitsniveau kontinuierlich steigern.	ESET PROTECT + ESET Inspect	✓	✓	✓	✓*
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,	Unsere kostenlosen Trainings stärken das Bewusstsein für IT-Sicherheit bei allen Mitarbeitenden in Ihrem Unternehmen.	ESET Cybersecurity Awareness Trainings	✓	✓	✓	✓

[1] Aktueller Test: https://www.av-comparatives.org/tests/business-security-test-2025-august-november/

* ohne ESET Inspect

BSIG im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,	Unsere inhouse entwickelte und patentierte Festplattenverschlüsselung mit Pre-Boot-Authentifizierung bietet zuverlässigen Schutz für ruhende Daten. Selbst bei Verlust oder Diebstahl eines Geräts oder im Falle des Austritts eines Mitarbeiters werden unautorisierte Zugriffe auf die Daten verhindert und die Informationssicherheit gewährleistet.	ESET Full Disk Encryption	✓	✓	✓	✓
	Mit der Endpoint-Verschlüsselungslösung können Sie neben ruhenden Daten auch Daten in Bewegung zuverlässig absichern. Hierzu zählen neben E-Mails und Anhängen insbesondere externe Medien wie USB-Sticks. Diese Lösung ist perfekt zugeschnitten auf Organisationen mit besonderen Verschlüsselungsanforderungen sowie expliziten Richtlinien für den Einsatz gemeinsam genutzter Geräte.	ESET Endpoint Encryption	*	*	*	*
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,	Für alle Nutzer im Netzwerk können über dynamisch festlegbare Gerätegruppen ganz unkompliziert verschiedene Maßnahmen durchgesetzt werden, z.B. automatisierte Updates der Sicherheitssoftware auf den Endpoints oder die Installation bzw. Deinstallation von Drittanbieter-Software. Für alle Administratoren bzw. Nutzer der Management-Konsole lassen sich spezifische Rechte für den Zugriff und die Verwaltungsmöglichkeiten festlegen.	ESET PROTECT	✓	✓	✓	✓
	Mit unserer Endpoint-Verschlüsselungslösung können Sie Zugriffsrechte bis auf die Dateiebene festlegen. So verhindern Sie unbefugte Zugriffe auf besonders schützenswerte Daten wie z.B. Konstruktionspläne.	ESET Endpoint Encryption	*	*	*	*
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	Unsere unkomplizierte und einfach zu implementierende Multi-Faktor-Authentifizierung funktioniert mobilbasiert und schützt den Zugang zu gemeinsam genutzten Systemen (Windows & Server Logins, Microsoft-Dienste wie ADFS oder OWA sowie SAML, FIDO, VPNs und RADIUS-basierte Dienste). Auf Wunsch lassen sich mittels biometrischen FIDO-Sticks sogar beinahe passwortlose Umgebungen realisieren.	ESET Secure Authentication	✓	✓	✓	
	Mit unserer Schutzlösung für Mailserver sichern Unternehmen ihre E-Mail-Kommunikation zuverlässig ab. Die Lösung schützt den Host selbst und verhindert so, dass digitale Bedrohungen wie Spam oder Phishing die Posteingänge der Nutzer erreichen.	ESET Mail Security	✓	✓	✓	✓
	Sofern Sie Microsoft 365 oder Google Workspace Anwendungen nutzen, sollten Sie diese zusätzlich schützen. Die Kombination aus Spam-Filter, Malware-Scanner, Anti-Phishing und Cloud Sandboxing in unserer Lösung sichert Ihre Unternehmenskommunikation, Zusammenarbeit und den vorhandenen Cloud-Speicher nachhaltig ab.	ESET Cloud Office Security	✓	✓	✓	✓

* separat buchbar

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN

CHAMPION PARTNER

Seit 2019 ein starkes Team
auf dem Platz und digital

KLINIKUM LANDSHUT

Seit 2022 durch ESET geschützt
Mehr als 1.450 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Trust Seal
www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel
„IT Security made in EU" verliehen

Unsere Lösungen sind nach den
Qualitäts- und Informations-
sicherheitsstandards ISO 9001:2015 und
ISO/IEC 27001:2022 zertifiziert

In strategischer Partnerschaft

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

178
Länder & Regionen

500.000+
Geschützte Unternehmen

12
Forschungs- und Entwicklungszentren weltweit

ÜBER ESET

Als europäischer Hersteller mit mehr als 35 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Extended Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ESET BLOG

ESET Deutschland GmbH
Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH

Stand: 07/2026 | Druck: 07/2026 | Artikelnummer: M_PRINT2026_15