exeon

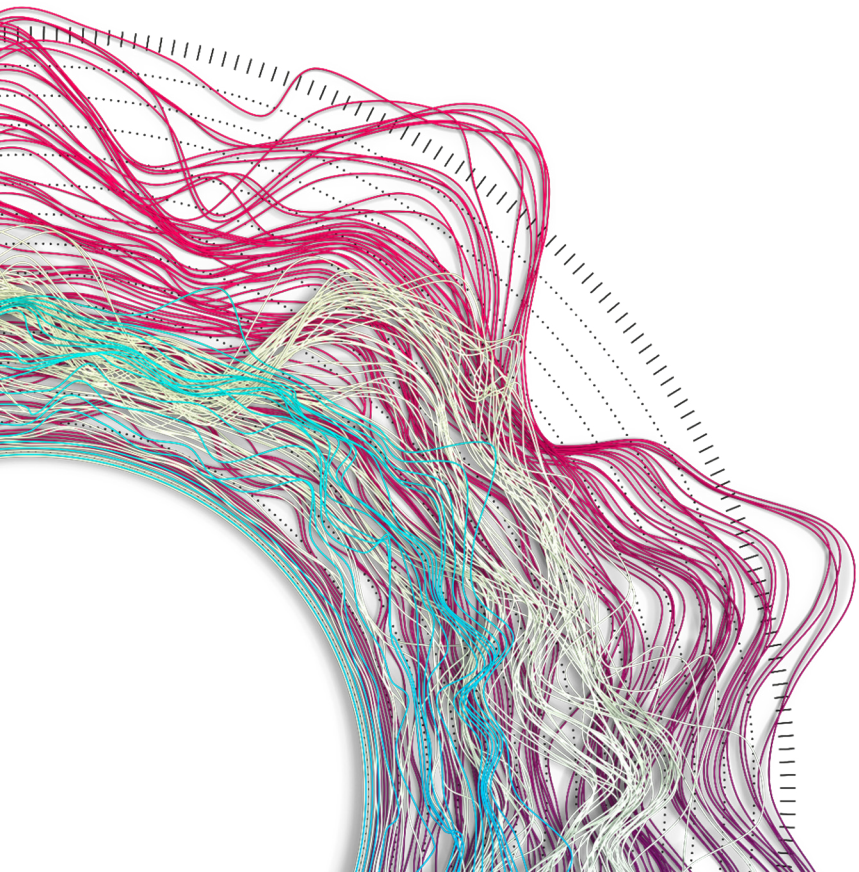
Smart Cyber Security.

WHITEPAPER

NIS2 Compliance Checkliste: Gewährleistung der Netzwerk- und Informationssicherheit

APRIL 2024

NIS2 Compliance Checkliste: Gewährleistung der Netzwerk- und Informationssicherheit



Da der Übergang von der ursprünglichen NIS-Richtlinie zu NIS2 durch mehrere wichtige Änderungen und Auswirkungen gekennzeichnet ist, die Unternehmen beachten müssen, soll die folgende Checkliste Sie durch alle Überlegungen und Tools führen, die NIS2 erfordert.

1. DEN UMFANG ZU VERSTEHEN

Finden Sie heraus, ob Ihre Organisation in den (erweiterten) Anwendungsbereich von NIS2 fällt.
NIS2 gilt für alle Unternehmen mit mehr als 50 Mitarbeitern und einem Jahresumsatz von mehr als 10 Millionen Euro sowie für alle Unternehmen, die bereits unter die ursprüngliche NIS-Richtlinie fielen.

Mit der aktualisierten Richtlinie wird der Anwendungsbereich auf folgende, neuen Sektoren ausgedehnt:

- Energie
- Transportwesen
- Bankwesen
- Finanzmarktinfrastruktur
- Gesundheit
- Trinkwasserversorgung
- Digitale Infrastruktur
- Öffentliche Verwaltung.

Diese Ausweitung ist eine Reaktion auf die zunehmende Interdependenz dieser Sektoren und die potenziellen Kaskadeneffekte von Cybersicherheitsvorfällen.
Alle 27 EU-Mitgliedstaaten müssen die NIS2-Richtlinie bis Oktober 2024 in nationales Recht umsetzen.

Wenn Sie sich zu diesem Zeitpunkt im Geltungsbereich befinden, müssen Sie Ihre Kontaktdaten angeben:

- Teilen Sie der ENISA den Namen Ihres Unternehmens sowie die Adressen der Hauptniederlassung und anderer rechtlicher Niederlassungen in der EU mit.
- Stellen Sie aktuelle Kontaktdaten, einschliesslich E-Mail-Adressen und Telefonnummern, innerhalb von 12 Monaten zur Verfügung.
- Ausländische Unternehmen, die nicht in der EU ansässig sind, aber Dienstleistungen erbringen (z. B. Anbieter von Datenzentren und Inhalten), müssen einen repräsentativen Ansprechpartner vor Ort benennen.
- Aktualisierung innerhalb von 3 Monaten, wenn eine Änderung (der Adresse oder des Vertreters) wirksam wird.

Auch wenn Sie nicht in den Geltungsbereich fallen, können Sie sich beteiligen und wichtige Vorfälle oder Cyber-Bedrohungen auf freiwilliger Basis melden.

Tabelle 1: Von NIS2 betroffene Branchen

FRÜHERE NIS-SEKTOREN	ZUSÄTZLICHE NIS-SEKTOREN
• Gesundheitswesen • Transport • Wasserversorgung • Energie • Virtuelle Infrastruktur • Anbieter digitaler Dienste • Bankwesen • Infrastruktur der Finanzmärkte	• Anbieter von öffentlichen elektronischen Kommunikationsnetzen oder -diensten • Abwasser • Chemikalien • Gesundheitswesen (Pharmazie, Forschung und Entwicklung, kritische medizinische Geräte) • Lebensmittelhersteller, -verarbeiter und -vertreiber • Hersteller kritischer Produkte (medizinische Geräte, Computer, Elektronik, Automobile) • Digitale Anbieter (Plattformen sozialer Netzwerke, Suchmaschinen, Online-Marktplätze) • Luft- und Raumfahrt • Post- und Kurierdienste • Öffentliche Verwaltung

2. ÜBERSICHT ÜBER DIE WICHTIGSTEN ÄNDERUNGEN UND AUSWIRKUNGEN VON NIS2

2.1. Machen Sie sich mit dem Übergang von der ursprünglichen NIS-Richtlinie zu NIS2 und den damit verbundenen Auswirkungen auf Ihre Organisation vertraut.

Im Rahmen der neuen Richtlinie wird gefordert:

- Meldung eines bedeutenden Sicherheitsvorfall innerhalb von 24 Stunden nach seiner Entdeckung.
- Übermittlung einer ersten Bewertung innerhalb von 72 Stunden nach der Entdeckung des Vorfalls.
- Vorlage eines ausführlichen Abschlussberichts innerhalb eines Monats nach der Entdeckung.

"Cyber-Hygiene" gemäss NIS2 Artikel 21

Cyberhygienerichtlinien bilden die Grundlage für den Schutz von Netzwerk- und Informationssysteminfrastrukturen, Hardware, Software und Online-Anwendungssicherheit sowie von Geschäfts- und Endbenutzerdaten, auf die sich Unternehmen verlassen. Cyber-Hygienerichtlinien, die eine Reihe gemeinsamer Praktiken umfassen - darunter Software- und Hardware-Updates, Passwortänderungen, die Verwaltung neuer Installationen, die Einschränkung von Zugangskonten auf Administratorebene und die Sicherung von Daten - ermöglichen einen proaktiven Rahmen für die Bereitschaft und allgemeine Sicherheit im Falle eines Vorfalls oder einer Cyber-Bedrohung.

2.2. Strengere Sicherheitsanforderungen, einschliesslich Risikomanagementverfahren und regelmässiger Sicherheitsbewertungen.

Gemäss Artikel 21 der NIS2 sollten die Mitgliedstaaten sicherstellen, dass bedeutende und wichtige Einrichtungen robuste Systeme, Strategien und bewährte Verfahren für das Risikomanagement einführen, die eine Vielzahl von Massnahmen und Disziplinen im Bereich der Cybersicherheit abdecken, einschliesslich:

- Risikoanalyse und Sicherheit von Informationssystemen
- Bearbeitung von Zwischenfällen und Berichterstattung
- Business-Kontinuität, z. B. Backup-Management und Notfallwiederherstellung
- Krisenmanagement
- Sicherheit der Lieferkette
- Sicherheit bei der Beschaffung, Entwicklung und Wartung von Systemen
- Grundlegende Praktiken der Cyberhygiene (siehe Definition unten) und Schulungen zur Cybersicherheit
- Kryptographie und Verschlüsselungstechnologien
- Personelle Sicherheit, Zugangskontrollen und Asset-Management
- Zero-Trust-Zugang (Multi-Faktor-Authentifizierung, kontinuierliche Authentifizierung)
- Seien Sie sich bewusst, dass die Zusammenarbeit, der Informationsaustausch und die Meldung von Vorfällen an die Behörden immer wichtiger werden.

3. BEWERTUNG IHRES NETZES UND IHRER INFORMATIONSSYSTEME

3.1. Durchführung einer umfassenden Bewertung des Netzwerks und der Informationssysteme Ihres Unternehmens, um potenzielle Bedrohungen und Schwachstellen zu ermitteln.

• **Bewerten Sie Ihre Sicherheitslage:** Eine Sicherheitsbewertung kann dazu beitragen, Schwachstellen wie nicht verwaltete Passwörter oder falsch konfigurierte oder ruhende Konten zu ermitteln, die anfällig für den Diebstahl von Anmeldedaten sind.
• **Analysieren Sie Ihren aktuellen Ransomware-Schutz:** Ist Ihr Unternehmensnetzwerk-vollständig gesichert? Kostspielige und lähmende Ransomware-Angriffe zu vermeiden sind ein Hauptanliegen der EU-Regulierungsbehörden und einer der Hauptgründe für die NIS2-Richtlinie. Implementierung von Sicherheitslösungen und bewährten Verfahren zum proaktiven Schutz vor Ransomware.



• **Überprüfen Sie Ihre Software-Lieferkette:** Angriffe auf die Lieferkette sind ein wichtiges Anliegen der EU-Regulierungsbehörden und ein Hauptgrund für die NIS2-Richtlinie. Werfen Sie einen neuen Blick auf Ihre Software-Lieferkette und erwägen Sie die Implementierung einer Secrets Management-Lösung, um die Risiken zu mindern.

3.2. Bewerten Sie die Wirksamkeit Ihrer derzeitigen Sicherheitsmassnahmen und stellen Sie fest, ob sie die Anforderungen von NIS2 erfüllen.

Eines der Sicherheitsziele von NIS2 besteht darin, dass elektronisch gespeicherte oder übermittelte Daten vor Aktionen wie unbefugtem Zugriff, Änderung oder Löschung geschützt werden, die zu einer Unterbrechung wesentlicher Dienste führen können. Wie effektiv ist Ihre Organisation in dieser Hinsicht?

Darüber hinaus muss die Organisation den Sicherheitsstatus der Netze und Systeme überwachen, die die Bereitstellung wichtiger Dienste unterstützen, um potenzielle Sicherheitsprobleme zu erkennen und die laufende Wirksamkeit von Sicherheitsschutzmassnahmen zu verfolgen.

Bei einer auf IT-Sicherheit ausgerichteten Governance, die IT und OT umfasst, muss sichergestellt werden, dass die operative Seite von Anfang an einbezogen wird und mit ihr zusammenarbeitet.

Ohne OT-Unterstützung wird die Cybersicherheitsinitiative nicht wirksam sein. Da Organisationen verpflichtet sind, alle bedeutenden Cybervorfälle, die sich auf die Sicherheit ihres Netzes und ihrer Informationssysteme auswirken, den von ihnen benannten nationalen Behörden zu melden, sollte der Meldeprozess zeitnah erfolgen und ausreichende Informationen enthalten, damit die Behörden den Vorfall bewerten und gegebenenfalls Unterstützung leisten können.

4. ANWENDUNG VON RISIKOMANAGEMENTVERFAHREN

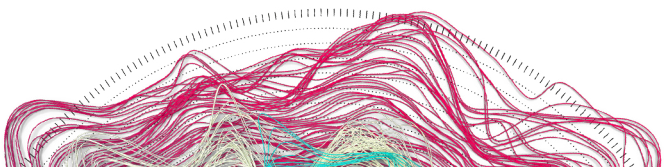
4.1. Anwendung eines risikobasierten Ansatzes für die Netz- und Informationssicherheit.

Ermöglichen eines Maximums an Transparenz im Netzwerk, einschliesslich Schwachstellenkartierung, Risikobewertung und Reporting-Tools?

4.2. Identifizierung potenzieller Bedrohungen, Bewertung ihrer Auswirkungen und Umsetzung geeigneter Massnahmen um Risiken abzumildern.

Für Budget- und Risikoabschätzungen kann der ENISA NIS-Investitionsbericht von grossem Nutzen sein: Betrachten Sie die Ausfallkosten und den Produktionsverlust, addieren Sie die Wiederherstellung und den Aufwand, der nötig ist, um den normalen Betrieb wiederherzustellen. Dann werden die geschätzten NIS2-Strafkosten und der Schaden für die angeschlossenen Unternehmen aufgezeigt.

4.3. Überprüfen und aktualisieren Sie regelmässig Ihre Risikomanagementpraktiken, um den sich entwickelnden Bedrohungslandschaft.



5. EIN VERFAHREN ZUR MELDUNG VON ZWISCHENFÄLLEN ENTWICKELN

5.1. Schaffung eines Verfahrens für die Meldung wichtiger Cyber-Vorfälle, die die Sicherheit Ihres Netzwerks und Ihrer Informationssysteme beeinträchtigen.

Da NIS2 auch die Meldung von Vorfällen umfasst, sollten Sie sicherstellen, dass der Prozess aus diesen Schritten besteht:

- Ein Vorfall oder eine Bedrohung wird identifiziert
- Die erste Meldung wird von einer Einrichtung innerhalb von 24 Stunden übermittelt
- Die Behörden übermittelten innerhalb von 24 Stunden eine erste Antwort und gaben Hinweise zu Abhilfemassnahmen
- Zwischenbericht über relevante Statusaktualisierungen, die von der Einrichtung auf Anfrage der Behörden übermittelt werden
- Ein abschliessender Bericht über den Vorfall wird von einer Einrichtung übermittelt (innerhalb eines Monats nach der Meldung)

5.2. Sicherstellen, dass die Berichterstattung rechtzeitig erfolgt und ausreichende Informationen enthält, damit die benannten nationalen Behörden eine Bewertung vornehmen und bei Bedarf Unterstützung leisten können.

6. GEWÄHRLEISTUNG DER EINHALTUNG UND DURCHSETZUNG

6.1. Machen Sie sich mit dem von der NIS2 geschaffenen Rahmen für die Einhaltung und Durchsetzung der Vorschriften vertraut.

Wer und wann ist zu benachrichtigen?

- Die zuständige nationale Behörde oder CSIRTs
- Die Empfänger der Dienstleistungen (alle Vorfälle und potenziellen Vorfälle)
- Sie müssen die Parteien unverzüglich innerhalb von 24 Stunden, nachdem Sie von dem Vorfall erfahren haben, benachrichtigen
- Ein endgültiger Bericht über den Vorfall muss einen Monat nach Einreichung der Meldung übermittelt werden.

Der Incident Report muss mindestens folgende Angaben enthalten:

- Eine detaillierte Beschreibung des Vorfalls, seiner Schwere und seiner Auswirkungen
- Die Art der Bedrohung oder die Ursache, die wahrscheinlich den Vorfall ausgelöst hat
- Die angewandten und laufenden Minderungsmassnahmen
- Ob der Vorfall durch unrechtmässige oder böswillige Handlungen verursacht wurde
- Ein Nachweis, dass die Massnahmen zum Management der Cybersicherheitsrisiken definiert und umgesetzt sind
- Die Massnahmen sollen von Verwaltuvngsorganen genehmigt werden, die auch für Folgendes verantwortlich sind Nichteinhaltung
- Spezifische Ausbildung zum Erkennen von Sicherheitsrisiken und deren Auswirkungen auf den Betrieb

- Wird eine Nichteinhaltung festgestellt, sollten unverzüglich die erforderlichen Abhilfemassnahmen ergriffen werden, um die Einhaltung der Vorschriften durch den betreffenden Dienst zu gewährleisten.

6.2. Möglichen Sanktionen und Strafen bei Nichteinhaltung.

Die Mitgliedstaaten der EU können bei bestimmten Verstössen Geldbussen von bis zu 10 Mio. EUR oder 2 % des Jahresumsatzes (Einnahmen) verhängen. Darüber hinaus können kritische Leitungsorgane (d. h. Managementteams) für Verstösse persönlich haftbar gemacht werden.

6.3. Bereiten Sie sich auf Audits und Inspektionen durch nationale Behörden vor, um sicherzustellen, dass Sie Ihren Verpflichtungen nachkommen.

7. ZIEHEN SIE NETZERKENNUNGS- UND REAKTIONSLÖSUNGEN (NDR) IN BETRACHT

7.1. Bewertung der Vorteile der Implementierung von NDR-Lösungen für eine effektive Netzwerküberwachung und -sicherheit.

Um die Herausforderungen der NIS2 zu bewältigen und die Sicherheit und Widerstandsfähigkeit der Netze und Informationssysteme zu gewährleisten, sind Network Detection and Response (NDR)-Lösungen für Betreiber kritischer Infrastrukturen unerlässlich.

NDR bietet eine Reihe von Vorteilen für Organisationen, die NIS2 einhalten müssen, darunter:

- **Sichtbarkeit:** NDR-Lösungen bieten einen umfassenden Einblick in den Netzwerkverkehr und ermöglichen es Unternehmen, potenzielle Bedrohungen und Schwachstellen zu erkennen, bevor sie ausgenutzt werden können.
- **Erkennung:** Durch die kontinuierliche Überwachung des Netzwerkverkehrs können NDR-Lösungen verdächtige Aktivitäten, wie z. B. unbefugte Zugriffsversuche oder Datenabfluss, erkennen und Unternehmen darauf hinweisen.
- **Reaktion:** NDR-Lösungen ermöglichen es Unternehmen, schnell und effektiv auf potenzielle Bedrohungen zu reagieren, indem sie Verfahren zur Reaktion auf Vorfälle auslösen.
- **Einhaltung der Vorschriften:** NDR-Lösungen können Unternehmen dabei helfen, die Berichtspflichten gemäss NIS2 zu erfüllen, indem sie detaillierte Protokolle und Berichte über Netzwerkaktivitäten und Vorfälle bereitstellen.

Insgesamt ist die NDR ein wichtiges Instrument für Betreiber kritischer Infrastrukturen, um die aktualisierte NIS-Richtlinie einzuhalten und die Sicherheit und Widerstandsfähigkeit ihrer Netz- und Informationssysteme zu gewährleisten.

7.2. Bewertung der Fähigkeiten von NDR-Lösungen, wie z. B. umfassende Transparenz, Erkennung verdächtiger Aktivitäten, Unterstützung bei der Reaktion auf Vorfälle und Compliance-Berichterstattung.

Buchen Sie eine kostenlose Demo und erfahren Sie, wie ExeonTrace ML-Algorithmen nutzt, um Ihr Unternehmen widerstandsfähiger gegen Cyberangriffe und NIS2-konform zu machen - schnell, zuverlässig und völlig hardwarefrei.

8. WÄHLEN SIE EINEN GEEIGNETEN NDR-LÖSUNGSANBIETER

8.1. Wählen Sie einen seriösen NDR-Lösungsanbieter, der die spezifischen Anforderungen Ihres Unternehmens erfüllen kann.

Wir bei Exeon kennen die Herausforderungen, denen sich Betreiber kritischer Infrastrukturen bei der Einhaltung der aktualisierten NIS-Richtlinie (NIS2) gegenübersehen. Unsere Network Detection and Response (NDR)-Lösung bietet einen umfassenden Einblick in den Netzwerkverkehr, erkennt und warnt Unternehmen vor potenziellen Bedrohungen, ermöglicht eine effektive Reaktion und erleichtert die Einhaltung der Meldevorschriften. Erfahren Sie mehr darüber, wie wir Ihnen helfen können, die Sicherheit und Widerstandsfähigkeit Ihres Netzwerks und Ihrer Informationssysteme zu gewährleisten, unter exeon.com/de.

9. REGELMÄSSIGE ÜBERPRÜFUNG UND AKTUALISIERUNG IHRER SICHERHEITSMASSNAHMEN

9.1. Stellen Sie sicher, dass Ihr zuständiges Personal die Überwachung des Netzes fortlaufend beaufsichtigt und Sicherheitsmassnahmen.

9.2. Informieren Sie sich über neue Bedrohungen und technologische Fortschritte im Bereich der Cybersicherheit.

9.3. Aktualisieren Sie regelmässig Ihre Risikomanagementpraktiken und technischen Massnahmen, für neue Herausforderungen.

Denken Sie daran, dass diese Checkliste einen allgemeinen Überblick bietet und an die spezifischen Bedürfnisse und Anforderungen Ihrer Organisation angepasst werden sollte. Klicken Sie hier, um die vollständige, vom Europäischen Parlament veröffentlichte Gesetzgebung zu lesen.

NÄCHSTE SCHRITTE

Kontaktieren Sie uns für eine Beratung darüber, wie ExeonTrace grosse Unternehmensnetzwerke und kritische Infrastrukturen schützt. Unsere Cybersecurity-Experten und -Ingenieure zeigen Ihnen die vollständige Transparenz der Netzwerkdatenströme und die automatische Erkennung von verdächtigem Verhalten, die Ihr Sicherheitsteam bei der Reaktion auf ruhende und aktive Bedrohungen effizient unterstützt - bevor ein echter Schaden entsteht.

Laden Sie die KuppingerCole Executive View on NDR herunter, um ein tieferes Verständnis der Netzwerküberwachung als grundlegendes Element der Sicherheitsarchitektur zu erhalten.

Melden Sie sich für unseren Cybersecurity-Newsletter an, um die neuesten Informationen über NDR und Veranstaltungen in der DACH-Region zu erhalten.

Konzerne, die ExeonTrace vertrauen:

PostFinance SWISS PLANZER swisscom EnBW Cyber Security Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra

Exeon Analytics AG
Grubenstrasse 1 2
8045 Zürich, Schweiz

+41 44 500 77 21
contact@exeon.com
exeon.com/de

swiss made software

Gartner Peer Insights

Mit 4.8/5 bei Gartner bewertet -
lesen Sie die Bewertungen hier

LinkedIn https://exeon.pub/linkedin

YouTube https://exeon.pub/youtube