EU-Vorschriften zur Cyber-Sicherheit zum Schutz kritischer Infrastrukturen und zur Sicherstellung der Compliance

Drei Frameworks, eine Mission: Resilienz. NIS2. DORA. KRITIS.

Whitepaper

exeon

Inhaltsverzeichnis

1.Einführung

Die EU und ihre Mitgliedstaaten haben Vorschriften wie NIS2 und DORA eingeführt, um die Cyber-Sicherheit und -Widerstandsfähigkeit von Organisationen in der Region zu stärken. Diese Frameworks wirken sich insbesondere auf Finanzdienstleister, Energieversorger und andere kritische Infrastruktursektoren aus, in denen Cyberangriffe schwere wirtschaftliche Verluste und erhebliche Betriebsunterbrechungen verursachen können.

Ransomware, Datendiebstahl und gezielte Angriffe nehmen zu

Im Jahr 2024 etwa legte ein Ransomware-Angriff 25 Krankenhäuser in Rumänien lahm und stoppte wichtige Dienste, und die deutsche CDU wurde durch einen Angriff, der mit staatlichen Akteuren in Verbindung gebracht wurde, vom Netz genommen. Zwei von - leider - vielen Beispielen. Diese Vorfälle unterstreichen die anhaltende Anfälligkeit kritischer Systeme. Der Finanzsektor ist hierbei besonders gefährdet.

68%
der Banken meldeten in den letzten zwei Jahren schwere Cyberangriffe.

Mit den jetzt in Kraft getretenen Vorschriften drohen den Unternehmen nicht nur die Kosten eines Cyberangriffs, sondern auch erhebliche Geldstrafen bei Nichteinhaltung. Für Unternehmen ist es an der Zeit, ihre Sicherheitslage neu zu bewerten, sich an den neuen gesetzlichen Anforderungen auszurichten und die Abwehrkräfte proaktiv zu stärken.

2. Gemeinsamkeiten und Unterschiede

2.1. Gemeinsame Ziele

Die Verordnungen zielen darauf ab:

- Die Widerstandsfähigkeit der Cyber-Sicherheit zu stärken, indem Firmen und Behörden dazu verpflichtet werden, robuste Verteidigungsmassnahmen und wirksame Risikomanagement-Praktiken zu implementieren,
- Bedrohungen schnell zu erkennen und darauf zu reagieren,
- Die obligatorische Meldung von Vorfällen und regelmässige Sicherheitsaudits einzuführen, um eine kontinuierliche Überwachung zu gewährleisten.

2.2. Ein Blick in die Gesetze

Feature	NIS2	DORA	KRITIS/SzA
Ziel-gruppe	Unternehmen in Bereichen wie **Energie, Verkehr, Gesundheit, Wasser und öffentliche Verwaltung**	**Finanzinstitute, Banken, Versicherer,** IT- und Cloud-Anbieter sowie Zahlungsdienste	Mit dem IT Sicherheitsgesetz 2.0 wurden die kritischen Infrastrukturen (gemäss BSI-KritisV) **um das Gesundheitswesen, Medien und die Abfallwirtschaft erweitert**
Schwer-punkt	Cyber-Sicherheit, Risikomanagement, Berichtswesen und **Sicherheit der Lieferkette**	**Operative Widerstandsfähig-keit,** IT-Risiko- und IKT-Bedrohungs-management, BCM und digitale Wider-standsfähigkeit	**Absicherung kritischer Infrastrukturen** durch verpflichtende IT-Audits, Sicherheitsstandards und Berichterstattung an das BSI
Melde-pflichten	**Erstmeldung innerhalb von 24 Stunden**, Aktua-lisierung in 72h, Abschlussbericht in einem Monat an Cybersicherheits-behörden (z. B. BSI)	Unverzügliche Meldung erforderlich. Erstbericht **innerhalb von 4 Stunden**	Nach dem IT-Sicherheitsgesetz müssen Unternehmen erhebliche IT-Vorfälle **innerhalb von 72 Stunden an das BSI melden**
Strafen	Bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes	Bis zu 2 % des gesamten Jahresumsatzes	Sanktionen durch das BSI mit **Bussgeldern** und verpflichtenden Kor-rekturmassnahmen

2.3. Überblick: Vergleich der Cybersicherheitsvorschriften in der EU und D-A-CH

Feature	EU: NIS2, DORA	KRITIS/SzA	Aktueller Stand
Rechtsgrundlage	NIS2 für kritische Unternehmen, DORA für den Finanzsektor	**IT-Sicherheitsgesetz, KRITIS**-Verordnung (KritisV), sektorspezifische Anforderungen (SzA)	**Informationssicherheitsgesetz (ISG), Datenschutzgesetz (DSG)** und (geplante) verpflichtende **Vorfallsmeldung** für kritische Infrastrukturen
Zielgruppe	**Kritische und wesentliche Sektoren**, Finanzinstitute, IT-Dienstleister	Kritische Infrastrukturen: **Energie, Gesundheit, Wasser, Verkehr, Regierung**	**Bundesbehörden und Betreiber kritischer Infrastrukturen** (private Regulierung noch begrenzt)
Schwerpunkt	**Cybersicherheit, Netzwerksicherheit,** digitale Resilienz, Vorfallsmeldung	**Schutz kritischer Infrastrukturen,** Mindestanforderungen an IT-Sicherheit, Meldepflichten	**Schutz öffentlicher Daten**, freiwillige Sicherheitsmassnahmen für Unternehmen, mit weiterer Regulierung in Zukunft
Vorfallsmeldung	Verpflichtend für alle **betroffenen Unternehmen** (24 h Erstmeldung, 72 h Update, 1 Monat Abschlussbericht)	**Verpflichtend für KRITIS-**Unternehmen, Meldung an das BSI (Frist: 72 h)	Derzeit **freiwillig, verpflichtend für Bundesbehörden;** verpflichtende Meldung für KRITIS-Unternehmen geplant (über NCSC)
Sanktionen	Bis zu **10 Mio. € oder 2 % des weltweiten Jahresumsatzes (NIS2), bis zu 2 % des Umsatzes** für Finanzinstitute (DORA)	Sanktionen und Auflagen durch das BSI, Bussgelder für **KRITIS-Unternehmen**	Keine spezifischen Bussgelder für Privatunternehmen oder potenzielle Sanktionen für Bundesbehörden

3. Herausforderungen/Chancen

3.1. Die wichtigsten Auswirkungen auf die Sicherheit von Unternehmen und Behörden

Es wird erwartet, dass die NIS2-Richtlinie allein in Deutschland etwa **29.500 zusätzliche Unternehmen betreffen wird**, was den Anwendungsbereich über die bisher regulierten Betreiber kritischer Infrastrukturen hinaus erweitert.

Die DORA-Richtlinie gilt für ein breites Spektrum von Finanzunternehmen in der gesamten EU und umfasst etwa **22.000 Finanzunternehmen und IKT-Dienstleister**. Folglich werden diese Cybersicherheitsvorschriften erhebliche Auswirkungen auf eine wachsende Zahl von Organisationen in ganz Europa haben.

Viele Unternehmen unterliegen mehreren Vorschriften gleichzeitig, was zu komplexen **Anforderungen an die Netzwerksicherheit, die Meldung von Vorfällen und das Risikomanagemen**t führt.

Die folgenden zehn Schlüsselbereiche veranschaulichen die sich überschneidenden Anforderungen und organisatorischen Herausforderungen.

1. Erweiterte Cyber-Sicherheitsanforderungen und Resilienzverpflichtungen

Nach dem IT-Sicherheitsgesetz und der BSI-KritisV müssen Unternehmen ihre Netze sichern, Notfallpläne erstellen und Meldevorschriften einhalten.

DORA verlangt von den Finanzinstituten, die betriebliche Widerstandsfähigkeit sicherzustellen und IKT-Risiken zu managen.

NIS2 und KRITIS verlangen eine doppelte Authentifizierung, eine Planung der Geschäftskontinuität und einen breiteren Schutzumfang.

2. Strengere Meldepflichten bei Vorfällen

DORA: Erste Benachrichtigung innerhalb **von 4 Stunden bei grösseren Vorfällen.**

NIS2: Erstbericht in 24 Stunden, Aktualisierung in 72 Stunden, Abschluss-bericht in 30 Tagen.

KRITIS: Meldung an das BSI innerhalb von 72 Stunden.

3. Sichere Nutzung der Cloud und von Drittanbietern

DORA: Strenge Kontrollen der IKT-Anbieter für Finanzunternehmen.

NIS2: Verlangt Sicherheit in der Lieferkette. Unternehmen brauchen hybride Cloud-Strategien mit robusten Kontrollen.

KRITIS: Schränkt die Verlagerung kritischer Systeme in die Cloud ohne angemessene Sicherheits-vorkehrungen ein.

4. Hohe Strafen bei Nichteinhaltung

Die Verordnungen sehen schwere Strafen von bis zu 10 Millionen Euro oder 2 % des weltweiten Umsatzes vor. KRITIS ergänzt die Durchsetzung durch BSI-Audits und obligatorische Massnahmen. Unternehmen brauchen ein integriertes Compliance-Management, um Geldstrafen und Reputationsschäden zu vermeiden.

5. Wachsende Bedrohungen durch neue Technologien

DORA erfordert detaillierte IKT-Risikobewertungen für Mobile Banking, APIs und Cloud-Plattformen.

NIS2 betont die Netzwerksicherheit besonders. Kritische Infrastrukturen im Finanzwesen müssen die IT-Sicherheit über alle digitalen Kanäle aufeinander abstimmen.

6. Auf geopolitische Risiken reagieren

Die zunehmenden globalen Spannungen erhöhen das Risiko für Verwaltung, Banken, Energie und andere. NIS2 und KRITIS erfordern proaktive Notfallpläne und eine starke Cyberabwehr. Widerstandsfähige IT-Architekturen sind jetzt für die betriebliche Stabilität unerlässlich.

7. Digitale Vermögenswerte und Kryptowährungen sichern

DORA: Verstärkt die IT-Risikokontrollen zum Schutz von Kryptowährungen und Zahlungssystemen.

NIS2: Betont die Integrität digitaler Transaktionen, die eine integrierte End-to-End-Sicherheit erfordern.

8. KI als Chance und Risiko

KI-gesteuerte Bedrohungserkennung trägt dazu bei, die Anforderungen von NIS2 und DORA zu erfüllen, indem sie schnellere, automatisierte Reaktionen auf Vorfälle ermöglicht. Gleichzeitig schreiben NIS2 und KRITIS den **Schutz vor KI-basierten Cyberangriffen vor, insbesondere bei der Betrugserkennung und dem Identitätsschutz**. Daher muss KI sowohl Teil der Verteidigungsstrategie als auch des Bedrohungsmodells sein.

9. Gleichgewicht zwischen Isolierung und Sichtbarkeit

DORA: Echtzeitüberwachung und integrierte IT-Umgebungen.

NIS2: Regelmässige IT-Sicherheitsprüfungen, für ein Gleichgewicht zwischen Systemisolierung und operativer Transparenz.

KRITIS: Unternehmen sollten auf on-premises und air-gapped Systeme zur Sicherung kritischer Infrastrukturen setzen.

10.Bedarf an einheitlichem Cyber-Risikomanagement

Viele Organisationen fallen unter mehrere Regularien, die jeweils unterschiedliche, aber sich überschneidende Anforderungen haben.

DORA: Ausfallsicherheit für Finanzgeschäfte bei Angriffen.

NIS2: Ständige Bedrohungsanalyse und Früherkennung.

KRITIS: Obligatorische IT-Audits/vorgeschriebene Verbesserungen.

3.2. Defizite bei der Cybersicherheit in kritischen Sektoren

Im Bereich der IT- und Cybersicherheit wurden in entscheidenden Sektoren erhebliche Lücken festgestellt:

- **Unvollständige Risikoanalyse und unzureichende Sicherheitsmassnahmen:** Fehlende Bedrohungsmodelle, fehlende segmentierte Netzwerke, unzureichender Schutz sensibler Daten.
- **Mängel im Identitäts- und Zugangsmanagement:** Unzureichende Multi-Faktor-Authentifizierung, übermässige Berechtigungen, fehlende Überwachung des privilegierten Zugangs.
- **Schwächen bei der Erkennung und Meldung von Sicherheitsvorfällen:** Fehlende oder unzureichende Sicherheitsüberwachung, unvollständige SIEM, IDS/IPS Integration, unklare Meldewege und -fristen.
- **Defizite bei der Reaktion auf Cyberangriffe (Incident Response):** Fehlende IR-Pläne und Mitarbeiterschulungen für Notfallszenarien.
- **Probleme bei der Umsetzung von Resilienzmassnahmen:** Unzureichende Redundanzkonzepte, ungeprüfte Notfallpläne, fehlende Backups oder unzureichend gesicherte Backup-Systeme.
- **Unvollständige IT-Assetübersichten und Sicherheitsklassifizierungen**: Fehlende Dokumentation und Priorisierung kritischer Systeme.
- **Schwachstellen in der physischen und digitalen Sicherheitsarchitektur:** Lücken in der Zugangskontrolle, der physischen Sicherheit und der Segmentierung sensibler Bereiche.
- **Fehlende Cyber-Abwehrmechanismen:** Fehlende oder unzureichende Bedrohungsanalysen, verzögerte Sicherheitsupdates, schwacher Endpunktschutz.
- **Defizite bei Notfall- und Krisenmanagementplänen:** Dazu gehören unklare Zuständigkeiten, mangelnde Abstimmung mit Behörden und fehlende Tests von Krisenszenarien.
- **Probleme bei der Erfüllung gesetzlicher Vorschriften:** Unzureichende Umsetzung von Meldepflichten, fehlende Dokumentation von Sicherheitsvorfällen und Massnahmen.

4. Netzwerkspezifische Artikel der Regulierungen

4.1 NIS2, DORA und KRITIS

- **Erkennung & Reaktion auf Bedrohungen in Echtzeit**
  - NIS2 Art. 21
  - DORA Art. 5
  - KRITIS/BSI IT-Sicherheitsgesetz §8a
- Zero Trust **Architektur für Netzwerksicherheit**
  - NIS2 Art. 20
  - DORA Art. 6
  - SzA nach BSI
- **Kontinuierliches Monitoring & Logging für Transparenz**
  - NIS2 Art. 22
  - DORA Art. 11
  - KRITIS-Anforderungen
- **Regelmässige digitale Resilienztests,** inkl. TLPT
  - DORA Art. 11
- **Angriffserkennungspflicht für KRITIS-Betreiber**
  - BSI IT-Sicherheitsgesetz §8a

4.2. Artikel zur Netzwerksicherheit

- DORA Art. 5 - **Verpflichtung zu belastbaren IT-Systemen** mit Risikomanagementmechanismen.
- DORA Art. 11 - **Regelmässige Tests der digitalen Widerstandsfähigkeit,** einschliesslich TLPT (Penetrationstests).
- DORA Art. 15 - **Erkennung und Meldung** von IKT-bezogenen Vorfällen.
- NIS2 Art. 21 - **Verpflichtung zur Umsetzung** von Massnahmen zur Cyber-Sicherheit des Netzes.
- NIS2 Art. 11 - Anforderungen an CSIRTs für **Bedrohungserkennung und Schwachstellenmanagement.**
- NIS2 Art. 29 - Förderung des **Austauschs von Bedrohungsinformationen**.
- BSI IT-Sicherheitsgesetz §8a - Verpflichtung der KRITIS-Betreiber zur **Erkennung von Angriffen.**

5. Netzwerkerkennung und -Reaktion (NDR) als Schlüssel zur Umsetzung

5.1. Vorteile von NDR Lösungen

- Automatische Erkennung von Anomalien durch KI-gestützte Algorithmen.
- Erkennung von Anomalien, z.B. Lateral-Movements, um Angreifer innerhalb des Netzwerks frühzeitig zu stoppen.
- Weniger Fehlalarme durch risikobasierte Alarmierung.
- Agentenlose Integration in bestehende IT- und Sicherheitsinfrastrukturen.

Mit Exeon.NDR, erhalten Unternehmen einen vollständigen Einblick in ihre Netzwerke, erkennen Bedrohungen in Echtzeit und erfüllen gleichzeitig die Anforderungen verschiedener Vorschriften ohne komplexe und schwerfällige Sicherheitsarchitekturen.

5.2. So funktioniert es in der Praxis

Exeon.NDR ermöglicht die effiziente Umsetzung der meisten Cybersicherheits-anforderungen von NIS2, DORA und KRITIS durch eine Kombination aus KI-gestützter Analyse, kontinuierlicher Überwachung und einfacher Integration in bestehende IT-Landschaften. Mit einem ganzheitlichen Ansatz unterstützt es Unternehmen bei der Einhaltung der Regularien, stärkt proaktiv ihre Sicherheitsstrategie und wehrt Cyber-Angriffe effektiv ab.

- **Frühzeitige Erkennung von Angriffen:** Mithilfe von maschinellem Lernen analysiert NDR den Netzwerkverkehr in Echtzeit und erkennt verdächtige Muster, um Angriffe wie Ransomware, APTs (Advanced Persistent Threats), oder Insider-Bedrohungen frühzeitig zu erkennen.
- **Schnelle Reaktion auf Vorfälle:** Die automatisierte Korrelation von Bedrohungsindikatoren ermöglicht es dem Sicherheitsteam, effizient zu reagieren und Angreifer zu isolieren, bevor sie Schaden anrichten.
- **Optimierung der Compliance:** Unternehmen erfüllen die Anforderungen von NIS2, DORA und KRITIS, indem sie alle sicherheitsrelevanten Netzwerkaktivitäten lückenlos dokumentieren und Sicherheitsvorfälle gesetzeskonform melden können**.**
- **Nahtlose Integration und Skalierbarkeit**: Da Exeon.NDR agentenlos arbeitet, kann es problemlos in komplexe, hybride IT-Umgebungen integriert werden - sei es on-premises, in der Cloud oder in kritischen Infrastrukturen mit einer Air-Gapped-Umgebung.
- **Optimierung der Ressourcen:** Durch die Reduzierung von Fehlalarmen und die Priorisierung echter Bedrohungen wird sichergestellt, dass sich Sicherheitsanalysten auf die wichtigsten Vorfälle konzentrieren können, anstatt in irrelevanten Alarmen förmlich zu ertrinken.

6. Gesucht: Umsetzer für NIS2, DORA & Co!

Die Anforderungen von NIS2, DORA und KRITIS erfordern robuste Sicherheitsstrategien mit modernster Technologie. Exeon ermöglicht die effiziente Umsetzung dieser Anforderungen durch die Kombination von Netzwerksicherheit, Bedrohungserkennung und Compliance-erfordernissen. Unternehmen profitieren von einer höheren Ausfallsicherheit, weniger Fehlalarmen und einer schnelleren Reaktion auf Cyber-Bedrohungen (incident response).

- Schnelle und einfache Implementierung ohne zusätzliche Hardware.
- Vollständige Netzwerktransparenz durch Metadatenanalyse.
- Sicherstellung der Compliance mit NIS2, DORA und KRITIS durch automatisierte Berichterstattung.
- Effektive Bedrohungserkennung für Cloud-, On-Premises- und Hybrid-Umgebungen.
- Technische Implementierung mit Exeon: Maschinelles Lernen & KI zur Erkennung unbekannter Bedrohungen.
- Netzwerk-Forensik & Anomalie-Analyse zur Erkennung von Bedrohungen in Echtzeit.
- Log-Daten & Flow-Monitoring zur detaillierten Analyse des Datenverkehrs.
- API-Schnittstellen zur nahtlosen Integration mit SIEM, SOAR, und EDR.

SWISS

Christian Keller, CISO @ SWISS

“Für die Sicherheit der SWISS IT setzen wir Exeon als zentrales Cybersecurity-Tool ein, das vollständig von unserem langjährigen Partner Reist Telecom AG verwaltet wird. Eine perfekte Kombination und Lösung, um unser Netzwerk zu überwachen und Anomalien schnell zu erkennen.”

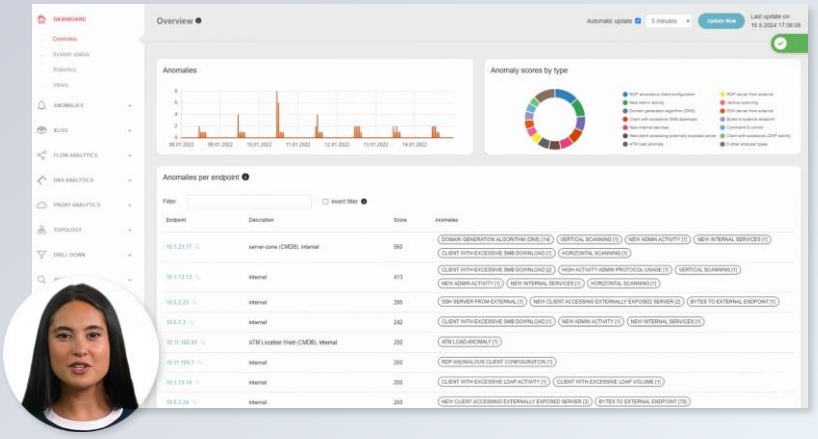
Was können Sie als nächstes tun?

Wir empfehlen folgende weitere Schritte::

- Beurteilen Sie, ob Sie Ihr Netzwerk so umfassend wie möglich auf Anomalien überwachen, Schwachstellen identifizieren und den Status quo bestimmen können.
- **Nehmen Sie sich 10 Minuten Zeit, um zu verstehen, wie Anomalien und APTs im NDR-Tool identifiziert, priorisiert und Gegenmassnahmen abgeleitet werden können, indem Sie sich das folgende Video ansehen.**

Video tour:

Erkennung von Advanced Persistent Threats in komplexen Infrastrukturen



Zum Video >