NIS-2 in Informational- & Operational Technology

Die NIS-2-Richtlinie: Stärkung der Cybersecurity für kritische Infrastrukturen

Die NIS-2-Richtlinie in Kürze

Die digitale Welt bietet viele Vorteile, aber sie birgt auch Risiken für kritische Sektoren, wie Verkehr, Energie, Gesundheit und Finanzen durch Cyberbedrohungen. Die NIS-2-Richtlinie der EU stärkt den Schutz dieser Infrastrukturen mit klaren Sicherheitsstandards für Netzwerke und Informationssysteme, um Gesellschaft und Bevölkerung zu schützen.

Einführung der NIS-2 Richtlinie zur Stärkung der Cybersecurity in kritischen Sektoren.

Ersetzt die bisherige NIS-Richtlinie und erweitert den Adressatenkreis.

Unternehmen in kritischen Sektoren mit mehr als 50 Mitarbeitern und 10 Mio. Euro Jahresumsatz.

NIS-2-Richtlinie: Nicht warten, handeln

Die NIS-2-Richtlinie wurde am 27. Dezember 2022 im EU-Amtsblatt veröffentlicht und ist seit dem 16. Januar 2023 in Kraft. Die Umsetzung in nationales Recht muss bis September 2024 erfolgen.[1] Die NIS-2-Richtlinie beinhaltet die folgenden Vorgaben:

- Zusammenarbeit von KRITIS-Betreibern mit Aufsichtsbehörden und Dienstleistern in der EU
- Sicherstellung von Cyber-Ressourcen und Fachkenntnissen, um Meldepflicht zu erfüllen
- Einrichtung eines Meldverfahrens zur Meldung größerer Vorfälle an die Behörden

Da die Zahl der KRITIS-Unternehmen mit der neuen Richtlinie stark ansteigt, müssen sich viele Unternehmen, die bisher nicht unter die Anforderungen der NIS-Richtlinie fielen, innerhalb kurzer Zeit mit strengen Cybersecurity-Standards und Meldepflichten auseinandersetzen.

Daher empfiehlt es sich, eine Expertenberatung in Anspruch zu nehmen, um eine optimale Anpassung an die Anforderungen der NIS-2-Richtlinie, Artikel 21, für die IT- / OT-Umgebung zu gewährleisten und Änderungen in der Infrastruktur zeitnah umzusetzen.

NIS-2-Bußgelder: Schützen Sie Ihre Infrastruktur

Betroffene Unternehmen und Organisationen müssen verschiedene Maßnahmen ergreifen, um den Anforderungen der NIS-2-Richtlinie gerecht zu werden. Dazu gehören Cyber-Risikomanagement, Sicherheit in der Lieferkette, Business Continuity Management, Penetrationstests, Reaktion auf Vorfälle sowie Berichterstattung an die Behörde und Abhilfemaßnahmen. Bei Verstoß drohen empfindliche Strafen.[1]

VORKEHRUNGEN

Vorkehrungen zur Cybersicherheit nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen.

Wichtige Einrichtungen:
7 Mio. EUR oder 1,4% des Umsatzes

Kritische Einrichtungen:
10 Mio. EUR oder 2% des Umsatzes

NACHWEIS

Nachweise über Erfüllung der Anforderungen von NIS-2 nicht oder nicht rechtzeitig erbracht.

Wichtige Einrichtungen:
500.000 EUR

Kritische Einrichtungen:
10 Mio. EUR oder 2% des Umsatzes

MELDUNG

Meldungen eines Vorfalls an BSI erfolgen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig.

Wichtige Einrichtungen:
7 Mio. EUR oder 1,4% des Umsatzes

Kritische Einrichtungen:
10 Mio. EUR oder 2% des Umsatzes

UNTERNEHMENS-REGISTRIERUNG

Eigenständige Registrierung & Nachweis über Erfüllung der NIS-2-Anforderungen nicht oder nicht rechtzeitig erbracht.

Wichtige Einrichtungen:
500.000 EUR

Kritische Einrichtungen:
500.000 EUR

Laut dem Entwurf des Bundesinnenministeriums haften die Leitungsorgane von Unternehmen für die Einhaltung des Risikomanagements mit ihrem Privatvermögen.

Drei Schritte zur NIS-2-Compliance

Zum Schutz und zur Widerstandsfähigkeit kritischer Infrastrukturen hat die Europäische Union die NIS-2-Richtlinie verabschiedet. Diese Maßnahme setzt klare Standards für die Sicherheit von Netzwerk- und Informationssystemen, um potenzielle Gefahren zu minimieren. Dabei stellen wir Ihnen drei Schritte zur Verfügung, die essenziell für die NIS-2-Bewertung sind:

1. Selbstbewertung und Scoping

Klären ob Unternehmen unter NIS-2 fallen. Wenn NIS-2, dann Registrierung beim BSI verpflichtend.

Während IT-SiG lediglich kritische Netzwerke beleuchtet, ist NIS-2 auf das gesamte Unternehmen anzuwenden.

2. Umfassende Risikobewertung

Identifikation wichtiger Assets, Services und potenzieller Schwachstellen.

Erste Risikoanalyse durchführen. Segmentierung kritischer Bereiche und Assets für gezielte Maßnahmen.

3. Maßnahmen ergreifen

Vorbeugung, Protokollierung, Detektion, Reaktion und Mitigation der Risiken.

Überwinden von Hindernissen und Minimierung der Störanfälligkeit der Tools und Prozesse.

Werkzeuge für umfassenden Cybersicherheitsschutz

Um einen umfassenden Cybersicherheitsschutz zu gewährleisten, ist es sinnvoll, dass Organisationen in ihren IT- / OT-Umgebungen mehrschichtige Maßnahmen etablieren. Eine Kombination aus technischen Anpassungen (Tools) und organisatorischen Veränderungen (Prozesse) ist dabei essenziell.

Die wichtigsten Maßnahmen für eine mehrschichtige Abwehrstrategie sind:

Prozessanpassungen	Benötigte Tools	Fortinet Lösung
Policies	Encryption	NGFW
Incident Management	People Management	SIEM, ANALYZER, SOAR, EDR
Business Continutity	Access Management	NGFW, NAC, FAC, CLIENT, TOKEN, PROXY
Supply Chain	Asset Management	NGFW, NAC, SWITCH, WIFI, EDR
Purchasing	Authentication	NGFW, NAC, FAC, CLIENT, TOKEN, PROXY
Efficiency	Communication	NGFW, MANAGER, SIEM, ANALYZER
Training	All-Risk Approach	

Erweiterte Sicherheit für OT-Umgebungen mit Fortinet

Um die Anforderungen der NIS-2 an eine IT- / OT-Umgebung zu erfüllen, empfehlen wir die Zertifizierung nach IEC 62443 anzuwenden. Abhängig vom Sicherheitsebenenmodell können Sie dabei eine Vielzahl der Foundational-Requirements (FR) mit den Lösungen von Fortinet abbilden.

Ein Beispiel für FR-5: Die Netzwerksegmentierung und Mikrosegmentierung in Verbindung mit den erweiterten Bedrohungsschutzfunktionen der FortiGate Next-Generation Firewalls reduzieren die Anfälligkeit eines OT-Netzwerks gegenüber Cyberbedrohungen. Dabei zentralisieren FortiGates die Sichtbarkeit und Verwaltung der Sicherheitsarchitektur einer Organisation.

OT-Sicherheit

Spezialisierte Lösungen für die Herausforderungen in OT-Umgebungen.

OT-Experten

Erfahrene Experten unterstützen bei der Entwicklung maßgeschneiderter Sicherheitsstrategien.

OT-Hardware

Hardware gebaut für OT-Umgebungen, ausgelegt für extreme Temperaturen, elektromagnetische Störungen und Vibrationen.

OT-Protokolle

Umfangreiche branchenspezifische Protokolle und Signaturen mit täglichen Aktualisierungen. Einheitliche Benutzeroberfläche für maximale Visbilität und Verwaltung.

Wählen Sie Fortinet für Ihre Umsetzung von NIS-2!

Setzen Sie auf Fortinet, um eine Vielzahl der NIS-2 Anforderungen zu erfüllen!

Mit unserem breiten Produktportfolio bieten wir Ihnen nicht nur die passende Lösung für die jeweilige Situation, sondern auch einen klaren Weg zur erfolgreichen Implementierung.

Von FortiGate Next-Generation Firewalls bis hin zu komplexen Lösungen - wir bieten Sicherheit aus einer Hand, die IT- / OT-Umgebungen brauchen, um kritische Infrastrukturen zu schützen.

Nehmen Sie jetzt Kontakt mit Ihrem Channel Account Manager auf, um einen persönlichen Gesprächstermin zu vereinbaren.

[1] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022.