DIE NIS-2-RICHTLINIE

Ein ausführlicher Leitfaden zu den EU-Anforderungen an die Cybersicherheit

Die verbindliche EU-Richtlinie zur Cybersicherheit (NIS-2) trat im Oktober 2024 in Kraft und betraf eine Vielzahl von Branchen. Unternehmen waren ab diesem Zeitpunkt verpflichtet, wirkungsvolle Cybersicherheitsmaßnahmen zu ergreifen und kritische Vorfälle zu melden. Die EU-Mitgliedstaaten mussten die NIS-2-Richtlinie in nationales Recht umsetzen.

Während die Richtlinie ein Grundniveau für die Cybersicherheit festlegt, wird Deutschland noch strengere Anforderungen beschließen („Mindestharmonisierung"). Das NIS2UmsuCG befindet sich derzeit im parlamentarischen Verfahren und wird aktuell im Bundestag beraten. Die Umsetzung der NIS-2-Richtlinie bleibt weiterhin vordringlich. Ab Inkrafttreten müssen betroffene Unternehmen die Vorgaben ohne Übergangsfrist erfüllen. Erfahren Sie, inwiefern Ihr Unternehmen betroffen ist und wie octoplant Sie bei der Compliance unterstützen kann.

Die NIS-2-Richtlinie revolutioniert die Cybersicherheitslandschaft. Hier ein Überblick über ihre wichtigsten Merkmale.

Erweiterter Anwendungsbereich

Der Anwendungsbereich der Cybersicherheitsanforderungen wird über die Betreiber kritischer Infrastrukturen (KRITIS) in Sektoren wie Energie, IT, Gesundheit und Finanzen hinaus ausgeweitet. Mit der Einführung der NIS-2-Richtlinie und des NIS2UmsuCG fallen nun neue Sektoren wie die Chemieproduktion, der Lebensmittelvertrieb und verschiedene Fertigungsindustrien unter die Regelungen. Dazu gehören auch Teilsektoren wie die Herstellung von Datenverarbeitungsanlagen, elektrischen Geräten und Kraftfahrzeugen. Auch kleine und mittlere Unternehmen (KMU) mit mehr als 50 Beschäftigten oder mehr als 10 Mio. Euro Umsatz können nun betroffen sein. Schätzungsweise 25.000 Unternehmen müssen daher erstmals Cybersicherheitsanforderungen erfüllen.

Gefahrenübergreifendes Risikomanagement

Ein umfassender gefahrenübergreifender Risikomanagementansatz gemäß Artikel 21 der NIS-2-Richtlinie bzw. § 30 des BSIG-E ist essenziell für den Schutz vor diversen Bedrohungen. Dazu gehören Konzepte in Bezug auf die Risikoanalyse, die Sicherheit für Informationssysteme, die Bewältigung von Sicherheitsvorfällen, die Aufrechterhaltung des Betriebs (wie Backup-Management und Wiederherstellung nach einem Notfall) sowie das Gewährleisten der Sicherheit der Lieferkette durch vertragliche Vereinbarungen, die Bewältigung von Sicherheitsvorfällen und Patch-Management.

Auswirkungen auf die Lieferkette

Lieferanten und Diensteanbieter werden vertraglich zur Einhaltung NIS-2-konformer Cybersicherheitsstandards verpflichtet, auch wenn sie nicht direkt von NIS-2 betroffen sind. Das stellt sicher, dass die Cybersicherheitsziele entlang der gesamten Lieferkette erfüllt werden, und fördert Prinzipien wie „Sicherheit durch Technikgestaltung" und „Sicherheit durch datenschutzfreundliche Voreinstellungen".

Strengere Vorgaben für Betreiber kritischer Einrichtungen

Diese Einrichtungen müssen strengere Vorgaben einhalten, etwa durch den Einsatz von Angriffserkennungssystemen (octoplant selbst ist zwar kein Angriffserkennungssystem, trägt aber durch Softwareversionsanalyse zu einer besseren Erkennung und Rückverfolgung von Angriffsmustern bei).

AMDT
PRODUCTION RESILIENCE DELIVERED

Weitere erforderliche Maßnahmen

- Sicherheit für Netz- und Informationssysteme bei Erwerb, Entwicklung und Wartung
- Management und Offenlegung von Schwachstellen
- Verfahren für die Cyberhygiene und regelmäßige Schulungen im Bereich der Cybersicherheit
- Konzepte für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- Konzepte für die Sicherheit des Personals, die Zugriffskontrolle und das Management von Anlagen
- Verwendung von Multi-Faktor-Authentifizierung, gesicherte Kommunikation sowie Notfallkommunikationssysteme

Verantwortlichkeit des Managements

Cybersicherheit ist nunmehr eine zentrale Aufgabe der Geschäftsführung. Leitungsorgane sind verpflichtet, aktiv Risikomanagementmaßnahmen zu treffen und zu überwachen, regelmäßig an Schulungen teilzunehmen und sich ausreichende Kenntnisse zur Erkennung und Bewertung von Risiken im Bereich der Informationssicherheit anzueignen. Eine passive Haltung ist nicht länger akzeptabel – Cybersicherheit bedarf aktiver Steuerung auf höchster Ebene.

Große Unternehmen oder Einrichtungen können bei Pflichtverstößen mit Geldbußen bis zu 10 Mio. Euro oder 2 Prozent des weltweiten Jahresumsatzes sanktioniert werden. Kommen wichtige Einrichtungen mit Cybersicherheitsmängeln den BSI-Vorgaben nicht fristgerecht nach, kann ihre Betriebsgenehmigung ganz oder teilweise ausgesetzt werden und ihrem Management die Ausübung von Leitungsaufgaben vorübergehend untersagt werden. Leitungsorgane haften bei Nichteinhaltung der Cybersicherheitsverpflichtungen für entstandene Schäden.

Strengere Meldepflichten bei Sicherheitsvorfällen unter NIS-2

Im Falle eines erheblichen Sicherheitsvorfalls müssen Einrichtungen einen strengen Meldeprozess an das Bundesamt für Sicherheit in der Informationstechnik (BSI) befolgen. Dieser umfasst:

- Frühwarnung: innerhalb von 24 Stunden nach Feststellung des Vorfalls
- Ausführliche Beschreibung des Vorfalls: innerhalb von 72 Stunden nach Kenntniserlangung
- Zwischenbericht: gegebenenfalls auf Anfrage im Zuge der Ermittlungen
- Abschlussbericht: innerhalb eines Monats, mit Angaben zu Bedrohung, zugrunde liegender Ursache und getroffenen oder geplanten Abhilfemaßnahmen

Die NIS-2-Richtlinie schützt IT- und OT-Systeme besser vor Cyberangriffen, indem sie die Systemresilienz stärkt. octoplant unterstützt Sie bei der notwendigen Compliance Ihrer IT- und OT-Infrastruktur.

Verbessertes Sicherheitsprofil

Octoplant ermöglicht ein proaktives Schwachstellen-management in der Produktion und reduziert die mit Produktionsausfällen, Datenschutzverletzungen und unerlaubtem Zugriff verbundenen Risiken.

Aufrechterhaltung des Betriebs

Mit octoplant können einzelne Geräte oder ganze Produktionsanlagen schnell auf einen gültigen Stand zurückgesetzt werden, wodurch sich Ausfälle und Störungen minimieren und Fehler oder Manipulationen rückgängig machen lassen.

CVE-Mapping und -Bewertung

Dank Zugriff auf Kritikalitätsbewertungen und detaillierte Asset-Informationen können Kunden risikoreiche Schwachstellen priorisieren und beseitigen – im Sinne einer gezielten und effektiven Cybersicherheitsstrategie.

Compliance Management

octoplant unterstützt Sie bei der Einhaltung von NIS-2, indem es durch Konfigurations- und Asset-Management die Transparenz in der Produktion erhöht, ein schnelles Recovery ermöglicht und Stillstandzeiten reduziert.

octoplant

Fragen Sie unser Team nach einer 30-Tage-Testversion oder vereinbaren Sie auf unserer Website eine Demo.