infinigate
spark your growth

ma't

NIS2 kommt
Was Sie wissen sollten

NIS2 kommt – Warum Sie jetzt handeln sollten

NIS2 – die Richtlinie zur Netz- und Informationssicherheit – ist eine Überarbeitung der NIS-Richtlinie, die bereits 2016 in Kraft gesetzt wurde, mit dem Ziel, die EU-weite Cybersicherheitsresilienz zu stärken.

Mit der Neufassung werden Meldepflichten verschärft sowie strengere Aufsichtsmaßnahmen und Durchsetzungsvorschriften eingeführt. Bis zum 17. Oktober 2024 muss die NIS2-Richtlinie in allen EU-Mitgliedsstaaten umgesetzt werden. Doch so sehr die Zeit drängt – es stellen sich für viele Unternehmen noch unterschiedliche Fragen.

Distributoren wie Infinigate können als Schnittstelle zwischen Resellern und Vendoren durch ein breites Portfolio und zielgerichtete Services in der Umsetzung von NIS2 effektiv unterstützen.

Anforderungen der NIS-2-Richtlinien für Unternehmen

Erweiterter Anwendungsbereich

- 7 wesentliche Sektoren
- 11 wichtige Sektoren
- Schwellenwert: über 50 Beschäftigte & Jahresumsatz von über 10 Mio. EU

Risikomanagementmaßnahmen

- Risikoanalyse- und Sicherheitskonzepte
- Bewältigung von Sicherheitsvorfällen
- Backup- und Krisenmanagement
- Gewährleistung der Sicherheit in der Lieferkette

Pflichten für Leitungsorgane

- Genehmigung & Überwachung der Risikomanagement-maßnahmen
- Teilnahme an Cybersicherheits-Schulungen

Meldepflichten

- Frühwarnung 24 Stunden nach Bekanntwerden eines Vorfalls
- Abschlussbericht spätestens nach einem Monat

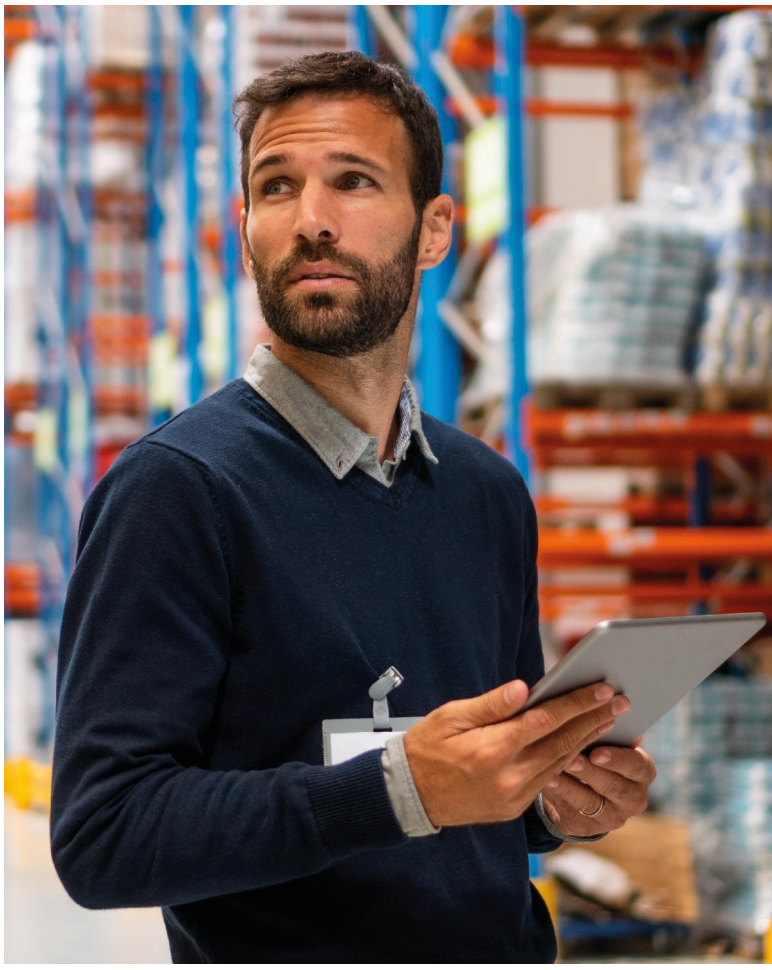
Strengere Kontrollen durch Behörden

- Regelmäßige Überprüfungen (auch vor Ort)
- Geldbußen bis zu 10. mio Euro oder 2% des weltweiten Jahresumsatzes

Weitere gesetzliche Vorgaben

- Cyber Resilience Act
- Delegierte Verordnung zur Funkanlagenrichtlinie (RED)

Wer ist betroffen?



Mit Inkrafttreten des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes - kurz NIS2UmsuCG - im Herbst 2024 sind Organisationen in 18 Sektoren ab 50 Mitarbeitern und 10 Millionen Euro Umsatz betroffen, die als „wesentlich“ und „wichtig“ eingestuft sind. Darüber hinaus sollen einige Einrichtungen unabhängig von ihrer Größe reguliert werden – insbesondere in den Bereichen digitale Infrastruktur und öffentliche Verwaltung.

Unter die Kategorie „wesentlich“ und „wichtig“ fallen kritische Infrastrukturen aus den folgenden Bereichen:

- Energie
- Transport
- Banken- und Finanzwesen
- Bildungswesen
- Wasserversorgung
- Digitale Infrastruktur
- ITK-Dienstleistungsmanagement
- Öffentliche Verwaltung,
- Weltraum
- Post- und Kurierdienste
- Abfallwirtschaft
- Herstellung, Produktion und Vertrieb von Chemikalien
- Lebensmittelproduktion, -verarbeitung und -vertrieb
- Industrie & Herstellung (Medizinprodukte und In-vitro, Datenverarbeitung, Elektronik, Optik, Elektrische Ausrüstung, Maschinenbau, Kraftwagen und Teile, Fahrzeugbau)
- Digitale Anbieter (Marktplätze, Suchmaschinen, Soziale Netzwerke)
- Forschungsinstitute

Aber: Die NIS2-Vorschriften gelten nicht nur für jene Unternehmen, die an vorderster Front stehen, sondern auch für deren Auftragnehmer.
Darüber hinaus gibt es auch Ausnahmeregelungen, sodass die NIS2-Direktive auch unabhängig von Unternehmensgröße und Umsatz greifen kann, beispielsweise wenn kritische Tätigkeiten ausgeübt oder Systemrisiken befürchtet werden müssen.

Nicht von NIS2 betroffen sind Unternehmen dann, wenn...

...sie Tätigkeiten in den Bereichen Verteidigung, nationale und öffentliche Sicherheit sowie Strafverfolgung ausüben. Im Gegensatz zu öffentlichen Verwaltungen auf zentraler und regionaler Ebene sind die Justiz, Parlamente und Zentralbanken vom Anwendungsbereich ausgenommen.

Gut zu wissen: Die „size-cap“-Regel

Die „size-cap“-Regel ist eine der Neuerungen, die mit NIS2 einhergehen, und soll ermöglichen, dass Ungleichheiten zwischen den betroffenen Unternehmen, die mit unterschiedlichen Bedürfnissen und Risiken, aber auch mit den unterschiedlichen Gegebenheiten in Bezug auf Budget, Ressourcen und Know-how einhergehen, beseitigen. Die Regelung soll somit Start-ups und mittelständischen Unternehmen ebenso wie Großkonzernen ermöglichen, die auf Grundlage von NIS2 geforderten Sicherheitsmaßnahmen durchführen zu können.

Was jetzt zu tun ist

Unternehmen sind verpflichtet, sich selbst in die Bereiche, unter die sie fallen könnten, einzuordnen und sich beim BSI (Bundesamt für Sicherheit in der Informationstechnik) innerhalb von drei Monaten nach der Identifikation zu registrieren.
Sicherheitsvorfälle müssen umgehend gemeldet werden.

Hier können Sie ermitteln, ob Ihr Unternehmen von der NIS-2 betroffen ist.

NIS-2 Schritt für Schritt umsetzen

Die strengen Sicherheitsanforderungen, die mit NIS2 einhergehen, machen die folgenden Schritte erforderlich:

Risikomanagement: Identifizieren, bewerten und Abhilfe schaffen

Betroffene Unternehmen sind gemäß der NIS2-Direktive verpflichtet, geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen zu ergreifen. Ein möglichst ganzheitlicher Ansatz soll sicherstellen, dass die Risiken für die Sicherheit von Netz- und Informationssystemen bewältigt werden können.

Sicherheitsbewertung: eine Selbstanalyse

Welche Schwachstellen gibt es im Unternehmen?
Wie steht es um die Cyberhygiene?
Welche Sicherheitspraktiken finden heute schon Anwendung?
Existieren falsch konfigurierte Konten, die anfällig für Datendiebstahl oder -manipulation sein könnten?
Eine Sicherheitsbewertung beantwortet alle diese Fragen.

Einfallstore schließen: Ransomware und Sicherheit in der Lieferkette

Eines der Hauptanliegen der NIS2-Direktive ist der proaktive Schutz vor Ransomware. Lösungen für die Endpunktsicherheit können hier Abhilfe schaffen. Auch Mitarbeiterschulungen helfen dabei, ein Bewusstsein für die Risiken zu schaffen und Cyberangriffe frühzeitig zu erkennen. Hier sollten Best Practices im Umgang mit sensiblen Daten und die sichere Nutzung von IT-Systemen im Fokus stehen.
Ein weiteres großes Problem sind Attacken auf Lieferketten. So gilt es für Unternehmen, die Sicherheitsmerkmale und -standards der Produkte und Dienstleistungen, die sie beziehen, sicherzustellen, sodass sie den aktuellen Sicherheitsanforderungen entsprechen.

Zugriffsmanagement: Schutz privilegierter Konten

Unternehmen, die unter die NIS2-Regelung fallen, sind angehalten, den Zugriff auf Konten auf Administratorebene zu beschränken und administrative Passwörter regelmäßig zu ändern. Ansonsten drohen Unterbrechungen des Geschäftsbetriebs und die Infiltrierung von Netzwerken und Systemen durch Cyberkriminelle.

Business Continuity: Gerüstet für den Ernstfall

Maßnahmen für das Business Continuity Management sind unumgänglich, wenn sichergestellt werden soll, dass kritische Systeme auch im Fall der Fälle aufrechterhalten werden können. Dazu gehören Backup Management, Disaster Recovery, Krisenmanagement und Notfallpläne.

Null-Toleranz-Strategie: Zugangskontrolle und Zero Trust

In einer Welt, in der die Unternehmensgrenzen aufgrund von Digitalisierung, Cloud-Infrastrukturen und dezentralen Arbeitsmodellen zunehmend verschwimmen, haben perimeterbasierte Architekturen ausgedient. Ein Zero-Trust-Konzept sieht mehrere Verteidigungslinien vor, setzt auf starke Authentifizierungsmethoden und Bedrohungsanalyse, um Zugriffsversuche zu validieren.

Sie haben Fragen zu NIS-2?

Christian Oelliger
+49 2104 494 17
christian.oelliger@mait.de

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar/München

T +49 89 89048-300
vertrieb@infinigate.de
www.infinigate.de

MAIT Germany GmbH
Berner Feld 10
78628 Rottweil

T +49 741 1752 – 0
hallo@mait.de
www.mait.de