

Network and Information Security (NIS2)

Was die neue EU-Richtlinie für die Cybersicherheit von Unternehmen bedeutet

Einleitung

Die [NIS2-Richtlinie](#) (Network and Information Security) ist eine Richtlinie, die das kollektive Cybersicherheitsniveau aller EU-Mitgliedstaaten verbessern soll. Sie trat im Januar 2023 in Kraft und verpflichtet alle relevanten Organisationen und Unternehmen, die neuen Anforderungen bis zum **18. Oktober 2024** zu erfüllen.

Die NIS2-Richtlinie ersetzt die [NIS-Richtlinie von 2016](#), die als erste **EU-weite Richtlinie für Cybersicherheit** galt. Sie stärkt Sicherheitsanforderungen, adressiert Sicherheit von Lieferketten, vereinheitlicht die Meldepflichten und führt strengere Aufsichtsmaßnahmen sowie härtere Durchsetzungsanforderungen, einschließlich harmonisierter Sanktionen in der gesamten EU, ein.



NIS2 bezieht mehr Industriesektoren ein

NIS2 erweitert auch den Anwendungsbereich und verpflichtet nun mehr Einrichtungen und Sektoren, Maßnahmen zu ergreifen. Dazu gehören Anbieter von wesentlichen und wichtigen Diensten, digitale Dienstleister, öffentliche Verwaltungen, Hersteller von Verbraucher-IoT-Geräten und Anbieter von Cybersicherheitsdiensten.

Unternehmen, die die NIS2-Vorgaben erfüllen müssen:

Sectors of High Criticality	
Energy	Electricity, oil, gas, hydrogen, heating and cooling
Transport	Road, rail, air and water
Banking	Banks, stock markets, financial institutions
Healthcare	Hospitals, labs, research centers, pharmacies and medical devices
Water	Wastewater and drinking water
Digital infrastructure	Telco, Data centers, cloud computing, DNS providers etc.
ICT services	Managed services and managed security services
Public administration	Central and regional government entities
Space	Operators of ground infrastructure

Other Critical Sectors	
Post and couriers	Mail and package shipping
Waste management	Waste collection, processing and recycling
Chemicals	Production and distribution of chemicals
Food	Production, processing and distribution of foodstuffs
Manufacturing	Manufacturers of medical devices, machinery, vehicles and electric/electronic devices
Digital services	Search engines, online marketplaces and social networks
Research	Research organisations

NIS2 und die neuen Anforderungen für Cybersicherheit

Im Zuge von NIS2 müssen betroffene Unternehmen einer Reihe neuer Verpflichtungen gerecht werden:

- **Risikomanagement**

Organisationen müssen Maßnahmen zur Minimierung von Cyberrisiken überwachen. Dazu gehören die Meldung und das Management von Zwischenfällen, die Ausfallsicherheit der Lieferkette, verbesserte Netzwerksicherheit sowie die Zugangskontrolle und Verschlüsselung.

- **Verantwortlichkeit des Managements**

Die Unternehmensleitung muss die Maßnahmen zur Cybersicherheit überwachen, genehmigen und die Belegschaft im Umgang mit Cyberrisiken schulen. Verstöße ziehen Geldstrafen für die Unternehmensleitung nach sich, einschließlich der Haftung und eines möglichen vorübergehenden Ausschlusses von Führungsaufgaben.

- **Meldepflichten**

Kritische Stellen müssen über Verfahren zur raschen Meldung von Sicherheitsvorfällen verfügen, die ihren operativen Betrieb erheblich beeinträchtigen könnten. Dabei legt NIS2 bestimmte Meldefristen fest: innerhalb von 24 Stunden muss eine Erstmeldung zusammen mit einem ersten Bericht übermittelt werden, ein vollständiger Bericht ist dann innerhalb von 72 Stunden vorzulegen. Final muss innerhalb eines Monats nach der initialen Meldung des Vorfalls ein Abschlussbericht eingereicht werden, der eine detaillierte Beschreibung des Vorfalls beinhalten muss.

- **Geschäftskontinuität**

Organisationen müssen so aufgestellt sein, dass die Geschäftskontinuität im Falle größerer Cyber-Vorfälle sichergestellt ist. Zudem müssen klare Vorgehensweisen zur Systemwiederherstellung, zu Notfallverfahren und zur Einrichtung eines Krisenreaktionsteams definiert sein.

Die wichtigsten NIS2-Direktiven und ihre Bedeutung

Die NIS2-Richtlinie soll dazu beitragen, das Cybersicherheitsniveau in Europa langfristig zu erhöhen und einen einheitlichen Binnenmarkt für Cybersicherheit zu schaffen. Sie soll auch das Vertrauen der Bürger und Unternehmen in digitale Dienste stärken und die Widerstandsfähigkeit gegenüber Cyberbedrohungen erhöhen.

Die **Meldung und das Management von Zwischenfällen** bei NIS2 sind von immenser Wichtigkeit, weil dadurch die Sicherheit und Zuverlässigkeit der Netz- und Informationssysteme in der Europäischen Union signifikant verbessert werden sollen.

Durch die Meldung von Zwischenfällen können die zuständigen Behörden Risiken bewerten, angemessene Gegenmaßnahmen ergreifen und die Auswirkungen auf die Nutzer und die öffentliche Ordnung minimieren.

Das Management von Zwischenfällen ermöglicht Anbietern wesentlicher und digitaler Dienste, ihre Systeme zu schützen, zu überwachen und stetig zu verbessern, um künftige Zwischenfälle zu reduzieren oder gar zu vermeiden.

Die **Ausfallsicherheit der Lieferkette** ist essenziell für die Sicherheit und Zuverlässigkeit der kritischen Infrastrukturen in der EU.

Die Richtlinie verpflichtet Betreiber von wichtigen Diensten, angemessene technische und organisatorische Maßnahmen zu ergreifen, um die Risiken von Cyberangriffen auf ihre Softwarelieferkette zu reduzieren und die Widerstandsfähigkeit ihrer Systeme zu erhöhen.

Eine gestörte oder kompromittierte Lieferkette kann zu schwerwiegenden Folgen für die öffentliche Sicherheit, die Wirtschaft, das Gesundheitswesen und die Umwelt führen.

Daher ist es wichtig, dass die Betreiber von wesentlichen und wichtigen Diensten die Ausfallsicherheit ihrer Lieferkette sicherstellen, indem sie die Herkunft, Integrität und Vertrauenswürdigkeit ihrer Lieferanten überprüfen, Sicherheitsanforderungen in ihre Verträge aufnehmen und regelmäßige Audits durchführen.

Zugangskontrolle ist ein wesentlicher Bestandteil der NIS2-Direktive. Damit soll die Sicherheit von Netz- und Informationssystemen in der EU deutlich verbessert werden.

Zugangskontrolle bedeutet, dass nur autorisierte Personen oder Geräte auf die Daten oder Ressourcen zugreifen können, die sie benötigen, und dass unbefugte Zugriffe verhindert oder erkannt werden. Dies schützt die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und der darin enthaltenen Informationen. Zugangskontrolle ist von daher maßgeblich, um das Risiko von Cyberangriffen, Datenverlusten oder Diebstählen zu verringern und das Vertrauen von Nutzenden zu stärken.

Datenverschlüsselung gewährleistet die Sicherheit und Vertraulichkeit von kritischen Informationen.

Die Richtlinie zielt darauf ab, die Widerstandsfähigkeit und das Vertrauen in die digitale Infrastruktur innerhalb der EU zu erhöhen, indem sie Anforderungen an die Anbieter wesentlicher und wichtiger Dienste sowie an die digitalen Dienstleister stellt. Datenverschlüsselung ist eine der Maßnahmen, die ergriffen werden muss, um Systeme vor Cyberangriffen zu schützen und Kundendaten zu respektieren.

NIS2-Anwendungsfälle

- **Threat Intelligence und Incident Response**

Die Implementierung einer Echtzeit-Bedrohungsintelligenz-Plattform, die potenzielle Bedrohungen und Anomalien kontinuierlich überwacht, hilft Unternehmen, Vorfälle schnell zu erkennen und darauf zu reagieren. In diesem Zusammenhang sind klar definierte Reaktionspläne und Tools erforderlich, um die Auswirkungen von Cyberangriffen wirksam abzumildern.

- **Data Security Anywhere**

Mit der Nutzung hybrider Infrastrukturen, also On-Premises kombiniert mit Cloud-Lösungen, wird Data Security immer wichtiger. Empfehlenswerte Maßnahmen sind dabei, eine hochautomatisierte Data Governance-Lösung sowie die End-to-End-Verschlüsselung von sensiblen Daten zu implementieren, um Datenverluste zu verhindern und mögliche hohe Geldstrafen zu vermeiden.

- **Supply Chain Cyber Resilience**

Unternehmen sind angehalten, für eine angemessene Cyber-Resilienz innerhalb ihrer gesamten Softwarelieferkette zu sorgen. Das heißt, dass sie auch die Cyberrisiken der einzelnen Software-Komponenten innerhalb der Lieferkette bewerten und entsprechende Maßnahmen ergreifen müssen.

- **IoT & Operational Technology (OT) Security**

Im Zusammenhang mit IoT- und OT-Geräten beinhaltet Cyber-Resilienz die Sicherung des Zugangs zu Geräten, Netzwerk und Daten, um unbefugten Zugriff zu verhindern. Die Implementierung starker Authentifizierungsmechanismen und die Überwachung von ungewöhnlichem Geräteverhalten sollten Teil einer Resilienz-Strategie sein, um die NIS2-Richtlinie zu erfüllen.

Unser Ansatz

- **Threat Intelligence und Incident Response**

KI-gesteuerte Verhaltensanalyse (ohne erforderliche Schulung), intelligente Echtzeitkorrelation, Sicherheitsüberwachung, Erkennung von Bedrohungen und Reaktion auf Vorfälle sowie Out-of-the-Box-Erkennungen: All diese Funktionen unterstützen Sie bei der Einhaltung der NIS2-Richtlinien durch kontinuierliche Überwachung kritischer Dienste sowie intelligente und schnelle Reaktion auf potenzielle Bedrohungen.

Mehr erfahren:

<https://www.microfocus.com/en-us/cyberres/secops>

<https://cloudsecurity.cyberres.com/threat-intelligence/>

- **Data Security Anywhere**

Die Enterprise Security-Lösungen von OpenText bieten eine einzigartige Data Governance-Plattform, die Unternehmen unterstützt, sensible Daten zu erkennen, diese zu visualisieren, zu klassifizieren und zu schützen. Mit einer einzigartigen und anpassbaren Workflow-Automatisierung ist dies auch in hybriden Umgebungen möglich.

Unternehmen, die der NIS2-Compliance unterliegen, haben damit jederzeit die Kontrolle über ihre Daten und vermeiden die Nichteinhaltung von Vorschriften und das Risiko enormer Geldstrafen.

Mehr erfahren:

<https://www.microfocus.com/en-us/cyberres/data-privacy-protection>

- **Supply Chain Cyber Resilience**

Mit einem zentralisierten Identity & Access Management, Governance und erweiterter Zugriffsberechtigungsverwaltung mit intelligenten Überwachungsfunktionen helfen wir Unternehmen, den entsprechenden Stakeholdern die richtigen Berechtigungen für die richtigen Assets zu erteilen und so die Risiken einer Gefährdung kritischer Infrastrukturen und Daten zu reduzieren.

Des Weiteren können wir Sie auch unterstützen, intern entwickelte Software auf Sicherheitslücken zu prüfen, um eine zuverlässige Supply Chain-Resilienz gewährleisten zu können.

Mehr erfahren:

<https://www.microfocus.com/en-us/cyberres/identity-access-management>

<https://www.microfocus.com/en-us/cyberres/use-cases/securing-the-software-supply-chain>

- **IoT & Operational Technology (OT) Security**

NetIQ Advanced Authentication unterstützt eine Vielzahl von starken Authentifizierungsmethoden, wie Multi-Faktor-Authentifizierung (MFA) oder biometrische Authentifizierung. Diese robusten Authentifizierungsmechanismen bieten eine zusätzliche Sicherheitsebene und schützen sensible Infrastrukturen vor unberechtigtem Zugriff und Identitätsdiebstahl.

Mehr erfahren:

<https://www.microfocus.com/en-us/cyberres/identity-access-management/advanced-authentication>

Natürlich bieten wir auch Unterstützung für viele **andere NIS2-Anwendungsfälle**, die für Ihre Organisation oder Branche relevant sind. Sprechen Sie uns an!

Next Steps

Wir unterstützen Sie gerne, sich auf die NIS2-Richtlinie vorzubereiten und die neuen Anforderungen für Cybersicherheit bis Oktober 2024 zu erfüllen.

Wir helfen Ihnen, Risiken zu identifizieren und zu bewerten, NIS2-Pläne zu erstellen und Ihr Unternehmen vor Ransomware, Angriffen auf die Softwarelieferkette und anderen Bedrohungen zu schützen.

- **Erfahren** Sie mehr über unsere breit aufgestelltes [Cybersecurity-Portfolio](#), das die NIS2-Anforderungen umfassend abdecken kann.
- **Kontaktieren** Sie Ihren persönlichen Ansprechpartner oder unseren [Spezialisten](#), um weitere Informationen darüber zu erhalten, wie wir Sie bei der Vorbereitung auf NIS2 unterstützen können.