NIS2 –
Was steckt konkret dahinter?

Network & Information Security 2 – Richtlinien

Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union

Network & Information Security 2 - Richtlinie

- Verschärfung der EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau
- Digitalisierung, Industrie 4.0 und IoT führen zu einer größeren Angriffsfläche
- Häufigkeit und Tragweite von Cyberangriffen hat rasant zugenommen

Gefahr eines Betriebsausfalls steigt

Ab wann gilt NIS2?

Für wen gilt NIS2?

Kleine Unternehmen / Gesellschaften *

1–49 Mitarbeiter

0,5–10 Mio. € Umsatz

>10 Mio. € Bilanzsumme

Mittelgroße Unternehmen / Gesellschaften

50–249 Mitarbeiter

10 –50 Mio. € Umsatz

<43 Mio. € Bilanzsumme

Große Unternehmen / Gesellschaften

ab 250 Mitarbeitern

ab 50 Mio. € Umsatz

>43 Mio. € Bilanzsumme

Wen betrifft diese Regelung?

Wesentliche Einrichtungen

Energie
(Elektrizität, Fernwärme, Erdöl, Erdgas, Wasserstoff)

Verkehr
(Luft, Schiene, Schiff, Strasse)

Bankwesen
(Banken und Kreditinstitute)

Finanzmärkte
(Handelsplätze)

Gesundheit
(Dienstleister, Hersteller, Labore, R&D)

Trinkwasser
(Lieferanten u. Versorger)

Abwasser
(Entsorgung industriell, kommunal,häuslich)

Digitale Infrastruktur
(Betreiber von Internetknoten, Cloudcomputing, Rechenzentren, Kommunikationsnetzen)

IKT Dienste
(Anbieterverwalteter Dienste und Sicherheitsdienste)

Öffentliche Verwaltung
(Zentrale und regionale Einrichtungen)

Weltraum
(Bodeninfrastruktur und Erbringung weltraumgestützter Dienste)

Wen betrifft diese Regelung?

Wichtige Einrichtungen

Post und Kurier
(Anbieter dieser Dienste)

Abfallwirtschaft
(Unternehmen der Abfallbewirtschaftung)

Chemie
(Produktion, Herstellung und Handel)

Lebensmittel
(Produktion, Verarbeitung und Vertrieb)

Digitale Dienste
(Anbietern von Online Marktplätzen, Suchmaschinen, Sozialen Netzwerken)

Forschung
(Forschungseinrichtungen)

Verarbeitendes Gewerbe/Herstellung von Waren
(Medizinprodukte, DV (Computer), Elektronik, Optik, Elektrische Ausrüstung, Herstellung von Kraftwagen und Teilen, Maschinenbau, Sonstiger Fahrzeugbau)

Mehrstufiges Meldungswesen

1. 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Frühwarnung
2. Innerhalb von 72 Stunden eine Meldung über den Sicherheitsvorfall und eine erste Bewertung
3. Spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls ein Abschlussbericht

Ebenfalls müssen Einrichtungen ggf. ihre **Kunden und Partner über die erhebliche Cyberbedrohung** an sich **informieren**, dass sie potenziell davon betroffen sein können und gleichzeitig alle Maßnahmen oder Abhilfemaßnahmen mitteilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können.

Prüfen Behörden?

1. Regelmäßige aber auch Ad-hoc-Vor-Ort-Kontrollen sowie Stichprobenkontrollen
2. Durchführung von Sicherheitsscans
3. Anforderung der Ergebnisse von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden

Strafen und Geldbußen

Was droht bei Nichteinhaltung?

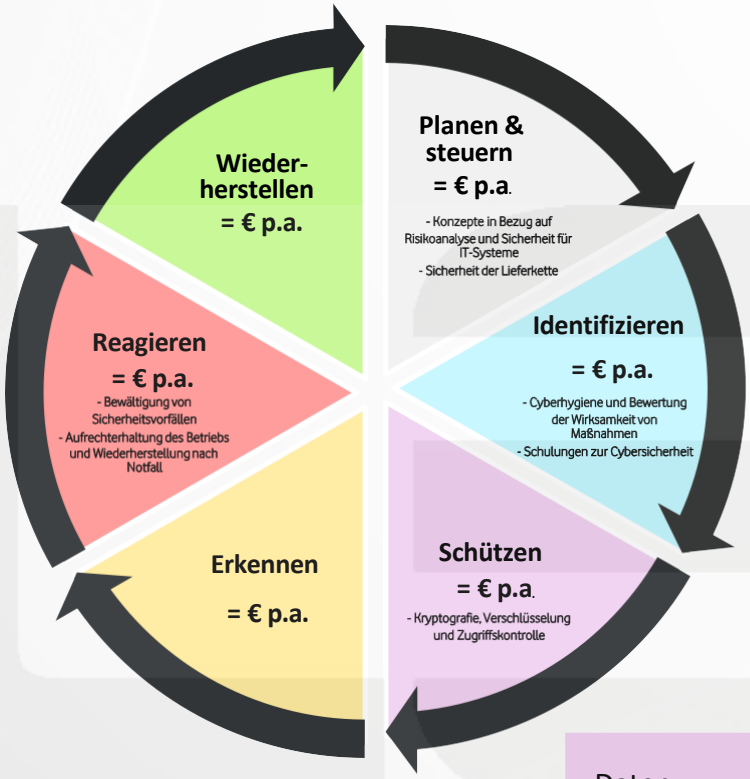
1. **Aussetzung** von **Zertifizierungen oder Genehmigungen**
2. **Geschäftsführungs-**bzw. Vorstandsebene **untersagen**, **Leitungsaufgaben wahrzunehmen**
3. **Bußgelder**
    1. Wesentliche Einrichtungen: **min. 10 Mio EUR oder 2%** des gesamten weltweiten **Umsatzes**, je nachdem welcher Betrag höher ist
    2. Wichtige Einrichtungen: **min. 7 Mio EUR oder 1,4%** des gesamten weltweiten **Umsatzes**, je nachdem welcher Betrag höher ist

Was kommt auf uns zu?

Risikomanagementmaßnahmen

- Konzepte in Bezug auf Risikoanalyse und Sicherheit für IT-Systeme Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs und Wiederherstellung nach Notfall Sicherheit der Lieferkette
- Cyberhygiene und Bewertung der Wirksamkeit von Maßnahmen Schulungen zur Cybersicherheit
- Kryptografie, Verschlüsselung und Zugriffskontrolle

- Backups
- Public Relations
- Disaster Recovery
- Lessons Learned
- IT-Notfallplan
- IT-Forensik
- BCM-Strategie
- Incident Response
- Notfall-kommunikation
- Mitigation / Remediation
- SOC / MDR
- IDS
- EDR, NDR, XDR
- SIEM
- Interne Audits



- Daten-speicherung
- Kommunikation / Datenaustausch
- Netzwerk-sicherheit

- Risiko-& Sicherheits-strategie
- IT-Sicherheits-konzept
- Rollen & Verant-wortlichkeiten
- Dokumenten-management
- Asset-/ & Risiko-management
- Penetration Test
- Schwachstellen-Scan
- Phishing-Simulation
- Awareness Trainings
- Antivirus, Anti-Spam, -Ransom- und Malware
- Remote Access
- Firewall/DDOS, DNS Security
- Endgeräte-management
- Zugriffs-management

C2 Genel

Unsere Leistungen – 6 Punkte Plan

1. Infrastrukturerhebung und Bewertung für Asset- und Risikomanagement

- **Asset- und Risikomanagement:** Umfassende Analyse zur Identifikation und Bewertung von Risiken ihrer IT-Infrastruktur.
- **Penetrationstests:** Simulierte Angriffe auf Netzwerke, Anwendungen und Endpunkte, um proaktiv Schwachstellen zu identifizieren und Maßnahmen zur Risikominderung zu entwickeln.
- **Schwachstellenscans:** Scan zur frühzeitigen Erkennung und schnellen Behebung potenzieller Sicherheitslücken.
- **Phishing-Simulationen:** Gezielte Tests zur Erkennung des Sicherheitsbewusstseins der Mitarbeitenden gegen Phishing-Bedrohungen.

Unsere Leistungen – 6 Punkte Plan

2. Schwachstellenmanagement, Neuanschaffungen und Implementierungen (Teil 1)

- **Awareness-Schulungen:** Sensibilisierung Ihrer Mitarbeitenden durch regelmäßige Schulungen, die das Bewusstsein für Cyber-Bedrohungen wie Phishing und Social Engineering schärfen.
- **Antivir-, Anti-Spam-, Anti-Malware- und Anti-Ransomware-Lösungen:** Modernste Schutzlösungen gegen Schadsoftware, um Ihre Endgeräte und Netzwerke umfassend abzusichern.
- **Firewall- und DDoS-Schutz:** Leistungsfähige Firewalls und DDoS-Abwehrsysteme, um Ihre Infrastruktur gegen gezielte Angriffe und Überlastungsversuche zu schützen.
- **DNS Security und Remote Access:** Schutz der DNS Abfragen zur Abwehr von Manipulationen und sichere Remote-Access-Lösungen für die Arbeit im Homeoffice und unterwegs.

Unsere Leistungen – 6 Punkte Plan

2. Schwachstellenmanagement, Neuanschaffungen und Implementierungen (Teil 2)

- **Netzwerksicherheit und Endgerätemanagement:** Integrierte Netzwerksicherheitsstrategien und zentrale Verwaltung der Endgeräte, um Sicherheitsrichtlinien effektiv umzusetzen.
- **Neuanschaffungen von Hardware:** Beratung und Beschaffung moderner Hardware-Komponenten wie leistungsfähige Server, hochsichere Endgeräte und Netzwerkinfrastruktur, die neuesten Sicherheitsstandards entsprechen und ideal in die bestehende IT-Landschaft integriert werden können.
- **Zugriffsmanagement und Datenspeicherung:** Effizientes Zugriffsmanagement mit rollenbasierten Zugriffsrechten und sichere, DSGVO-konforme Datenspeicherlösungen zur Sicherstellung der Datenintegrität.

Unsere Leistungen – 6 Punkte Plan

3. IT-Sicherheitsvorfälle frühzeitig zu erkennen und abzuwehren (Teil1)

- **Interne Audits:** Regelmäßige Überprüfungen und Bewertungen der Sicherheitsinfrastruktur zur frühzeitigen Erkennung potenzieller Schwachstellen und Optimierung der Sicherheitsmaßnahmen.

- **SIEM (Security Information and Event Management):** Zentrale Lösung zur Sammlung und Analyse sicherheitsrelevanter Ereignisdaten aus allen IT-Systemen. SIEM ermöglicht eine Echtzeiterkennung von Anomalien und bietet eine solide Basis für die rasche Reaktion auf Bedrohungen.

- **XDR (Extended Detection and Response):** Erweiterte Erkennungs- und Reaktionslösungen, die Bedrohungen über mehrere Sicherheitsebenen hinweg korrelieren und umfassend abwehren.

- **EDR (Endpoint Detection and Response):** Effiziente Überwachung und Abwehr von Bedrohungen auf Endgeräten, um potenzielle Angriffe bereits auf der Endgeräte-Ebene zu stoppen.

Unsere Leistungen – 6 Punkte Plan

3. IT-Sicherheitsvorfälle frühzeitig zu erkennen und abzuwehren (Teil 2)

- **NDR (Network Detection and Response)**: Netzwerkbasierte Überwachungslösungen zur Erkennung ungewöhnlicher Aktivitäten und Angriffsversuche im Netzwerkverkehr, mit Fokus auf die Netzwerkebene

- **SOC/MDR (Security Operations Center/Managed Detection and Response):** Unser Security Operations Center bietet rund um die Uhr Überwachung und Bedrohungsabwehr, unterstützt durch spezialisierte Experten, die in Echtzeit auf Sicherheitsvorfälle reagieren.

- **IDS (Intrusion Detection System):** Systeme zur Erkennung unautorisierter Zugriffe und verdächtiger Aktivitäten, die einen zusätzlichen Schutz vor Eindringlingen bieten.

Unsere Leistungen – 6 Punkte Plan

4. Reagieren: Schnelle und effiziente Maßnahmen im Ernstfall

- **IT-Notfallplan:** Erarbeiten eines detaillierten Planes, der alle Schritte und Verantwortlichkeiten im Falle eines IT-Notfalls definiert. So wird sichergestellt, dass alle Beteiligten schnell und gezielt reagieren können.
- **IT-Forensik:** Analyse und Aufklärung der Ursachen von Sicherheitsvorfällen, um die Schwachstellen und Angriffsmethoden zu identifizieren und zukünftige Vorfälle zu verhindern.
- **Notfallkommunikation:** Erstellen effektiver Kommunikationsstrategien, um alle betroffenen internen und externen Stakeholder zeitnah und transparent über den Vorfall zu informieren.
- **BCM-Strategie (Business Continuity Management):** Langfristige Strategien zur Aufrechterhaltung des Geschäftsbetriebs bei Störungen oder Ausfällen, um Geschäftsausfälle zu minimieren und eine rasche Wiederherstellung zu gewährleisten.
- **Mitigation und Remediation:** Sofortmaßnahmen zur Eindämmung des Vorfalls (Mitigation) sowie gezielte Schritte zur Behebung und nachhaltigen Sicherung des Systems (Remediation).

Unsere Leistungen – 6 Punkte Plan

5. Wiederherstellen: Effiziente Maßnahmen zur Wiederaufnahme des Geschäftsbetriebs

- **Backups:** Regelmäßige und gesicherte Datensicherungen ermöglichen die schnelle Wiederherstellung kritischer Daten und Systeme und minimieren die Auswirkungen von Datenverlusten.

- **Disaster Recovery**: Durch vordefinierte Disaster-Recovery-Pläne wird die Wiederherstellung der IT-Systeme im Ernstfall beschleunigt, sodass kritische Systeme schnell wieder verfügbar sind und Betriebsunterbrechungen minimiert werden.

- **Public Relations:** Eine klare Kommunikationsstrategie ist essenziell, um das Vertrauen von Kunden und Partnern zu erhalten. Transparente und zielgerichtete Kommunikation während und nach einem Vorfall hilft dabei, Reputationsschäden zu begrenzen.

- **Lessons Learned:** Nach jedem Vorfall analysieren wir die Ereignisse und bewerten die Wirksamkeit der getroffenen Maßnahmen. Diese Erkenntnisse fließen in zukünftige Sicherheitsstrategien ein und sorgen für kontinuierliche Verbesserungen im Umgang mit Krisen.

Unsere Leistungen – 6 Punkte Plan

6. Planen und Steuern: Strukturierte Sicherheitsplanung für nachhaltigen Schutz

- **Risiko- & Sicherheitsstrategie:** Entwicklung und Umsetzung einer umfassenden Strategie zur Identifizierung, Bewertung und Minderung potenzieller Risiken, abgestimmt auf die spezifischen Bedürfnisse Ihres Unternehmens.

- **IT-Sicherheitskonzept:** Ein maßgeschneidertes Konzept, das technische, organisatorische und personelle Maßnahmen zur Gewährleistung der IT-Sicherheit umfasst. Hierbei setzen wir auf bewährte Methoden und innovative Lösungen, die den Schutz Ihrer IT-Infrastruktur sicherstellen.

- **Rollen und Verantwortlichkeiten:** Klare Definition der Rollen und Verantwortlichkeiten aller Beteiligten, um eine reibungslose Zusammenarbeit und schnelle Reaktionsfähigkeit bei Sicherheitsvorfällen zu gewährleisten.

- **Dokumentenmanagement:** Ein systematisches Dokumentenmanagement, das alle sicherheitsrelevanten Dokumente organisiert und revisionssicher speichert. Dies gewährleistet eine stets aktuelle Übersicht und erleichtert Audits und Compliance-Prüfungen.