softline

NIS2 leicht gemacht

Ein umfassender Leitfaden zur Umsetzung

Cybersecurity-Webinarreihe | Teil 2

Ablauf

- Einstieg: Überblick zu NIS2
- Bedeutung von NIS2 für betroffene Unternehmen
- Stufenplan zur Umsetzung von NIS2
- Organisatorische und technische Hilfsmittel
- Offene Fragen und Diskussion

Was steckt hinter der NIS2-Richtlinie?

Die NIS2-Richtlinie zielt darauf ab, die Cyber- und Informationssicherheit in der EU zu stärken, indem sie erweiterte Anforderungen an Unternehmen und Institutionen stellt.

Sie ist seit 16.01.2023 und muss in den Mitgliedsstaaten bis zum 17. Oktober 2024 in nationales Recht umgesetzt sein.

Es geht nicht nur darum, Regularien zu erfüllen,

sondern um die Sicherheit Ihres Unternehmens.

Überblick zur NIS2-Richtlinie

- Erweiterter Anwendungsbereich, insb. in kritischen Sektoren wie Energie
- Mindestsicherheitsanforderungen und Meldepflichten:
  - Fokus auf Cyber-Risikomanagement, Umgang mit Zwischenfällen und Geschäftskontinuität
  - Ergreifen von technisch-organisatorischen Maßnahmen (TOMs).
- Verschärfte Aufsichtsmaßnahmen und Haftungsregeln:
  - Betonung der Sicherheit der Lieferkette und des Risikomanagements.
  - Strengere Haftungsregeln für Geschäftsleitungen
  - Einführung eines Single Point of Contact (SPoC): Sicherstellung der grenzüberschreitenden Zusammenarbeit der Behörden der Mitgliedstaaten.

Wann fallen Unternehmen unter NIS2?

1. Unternehmensgröße

Unternehmen mit

- mindestens **50 Mitarbeitenden** und
- mindestens **10 Mio. Euro Jahresumsatz**

können unter den Anwendungsbereich der NIS2-Richtlinie fallen, wenn auch das zweite Kriterium erfüllt ist.

2. Unternehmenssektor

11 besonders wichtige Einrichtungen

Energie, Luft-, Schienen-, Straßen- und Schiffsverkehr, Bankwesen/Finanzwesen, Raumfahrt, Gesundheit, Wasser, Digitale Infrastruktur und IT-Dienste, Öffentliche Verwaltung

7 wichtige Einrichtungen:

Anbieter von Post- und Kurierdiensten, Abfallwirtschaft, Chemische Erzeugnisse, Lebensmittel, Hersteller, Digitale Anbieter, Forschungseinrichtungen

Was bedeutet NIS2 für Unternehmen?

Anforderungen von NIS2 – Auszug aus Artikel 21:

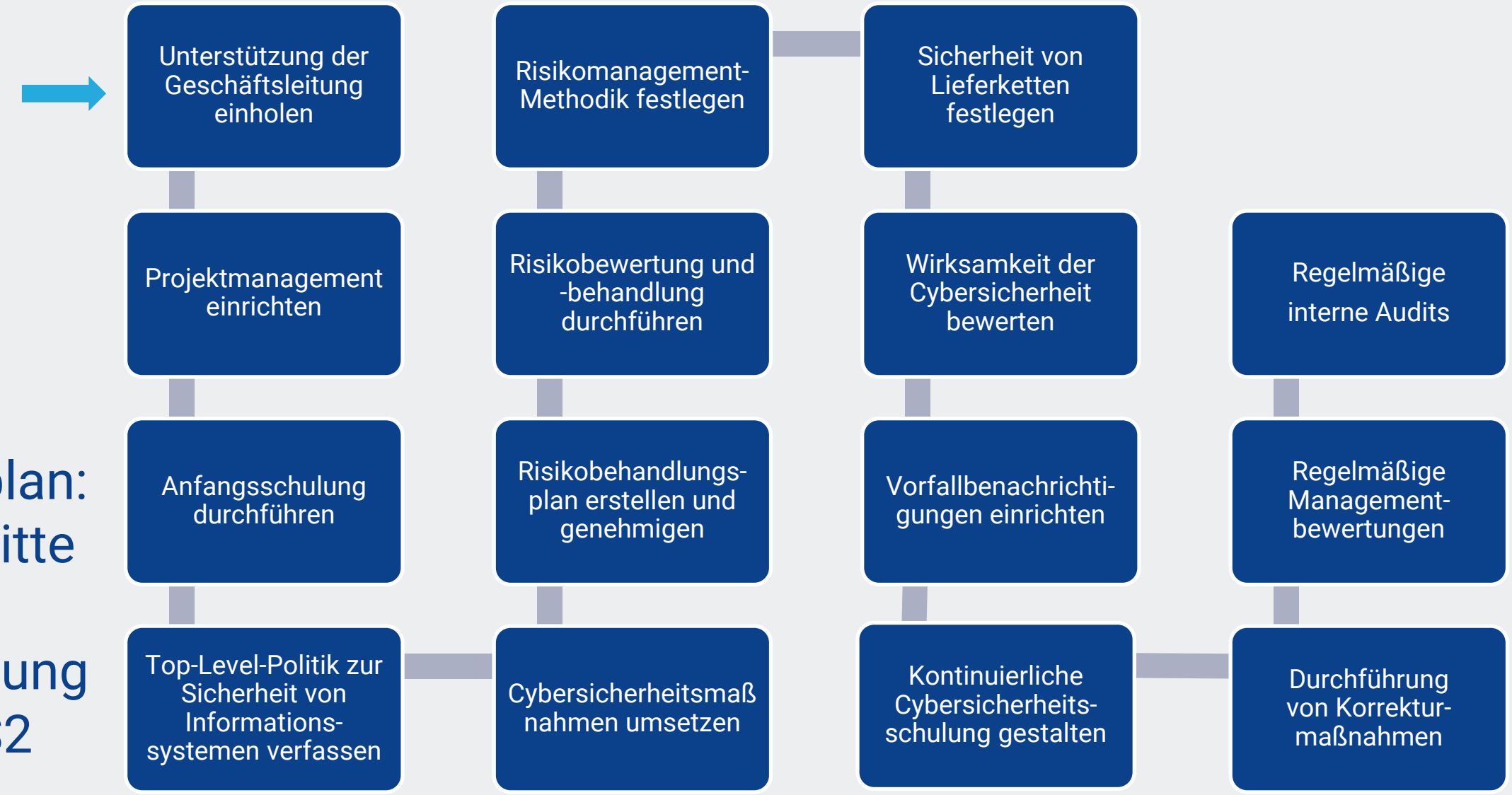
- Konzepte in Bezug auf Risikoanalyse und Sicherheit für Informationssysteme;
- Bewältigung von Sicherheitsvorfällen;
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

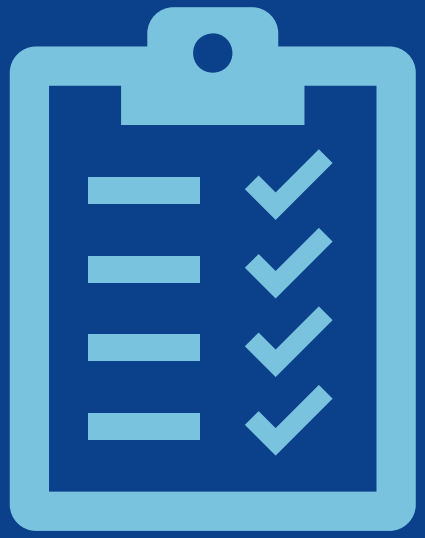
Was bedeutet NIS2 für Unternehmen?

Anforderungen von NIS2 – Auszug aus Artikel 21:

- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

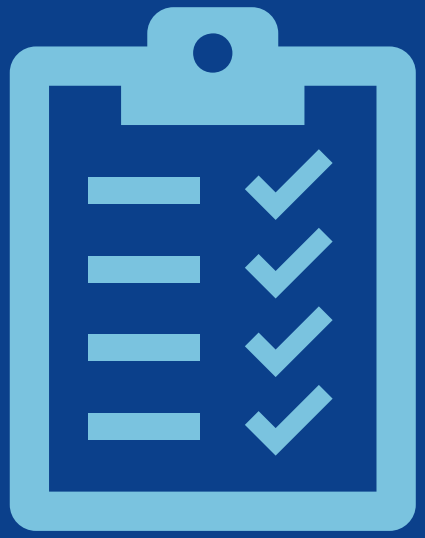
Stufenplan: 15 Schritte bis zur Umsetzung von NIS2





Organisatorische Hilfsmittel zur Umsetzung

- ✓ Aufbau eines „mini-ISMS“ Regelungen zur Informations- und Cybersicherheit sowie Datenschutzthemen als Regelprozess (NIS2 greift bereits bestehende Anforderungen der ISO 27001 auf)
- ✓ Bewältigung von Sicherheitsvorfällen: Incident Response Plan, Notfallplan, Backup- und Restoreplan, BCM sowie Krisenmanagement
- ✓ Meldepflichten und -wege etablieren
- ✓ Sicherheit der Lieferkette: Tools zur Überwachung der Lieferkette können dabei helfen, Risiken, die von Drittanbietern ausgehen, zu minimieren.



Organisatorische Hilfsmittel zur Umsetzung

- ✓ Sicherheit in der Entwicklung, Beschaffung und Wartung: Tools wie Static Code Analysis oder Software Composition Analysis können die Sicherheit von Anwendungen verbessern.
- ✓ Integraler Bestandteil muss das Risikomanagement sein:
  - ✓ Bestimmung von Werten, schützenswerten Gütern oder Prozessen
  - ✓ Risikoanalyse zur Bewertung und Umgang mit den Risiken
  - ✓ Definition von Maßnahmen zur Minimierung, Akzeptanz, Transfer und Versicherung
- ✓ Auditierung und Prüfungsprozess etablieren
- ✓ Schulungen für Cybersicherheit etablieren und Awareness schaffen

Technische Hilfsmittel

- **Sicherheitsinformationen- und Ereignismanagement (SIEM):** SIEM-Tools wie Wazuh oder Splunk können dabei helfen, Sicherheitsereignisse zu überwachen und zu analysieren.
- **Firewalls und Network Detection Response (NDR):** Hersteller wie Fortinet, Checkpoint etc. bieten robuste Firewalls mit Angriffserkennung, NDR Systeme wie z.B. von Darktrace können dabei helfen, unerwünschten internen Datenverkehr zu erkennen und zu blockieren.
- **Schwachstellenmanagement und Penetration Testing Werkzeuge:** Tools wie Greenbone, Nessus oder Metasploit können dabei helfen, Schwachstellen zu identifizieren und zu testen.

Technische Hilfsmittel

- **Identity and Access Management (IAM):** IAM-Tools wie Microsoft Entra ID, Okta oder Keycloak können dabei helfen, den Zugriff auf Ressourcen zu verwalten und in Abhängigkeit des Risikos zu verwehren.
- **Client Datenanalyse:** tiefe Inhaltsanalyse in E-Mails und im Webtraffic, EDR am Endpoint lassen Schadcode, Phishing und Co wenig Chancen.
- **Backup und Disaster Recovery:** Tools wie z.B. Veeam können dabei helfen, Daten frei von Ransomware und unveränderlich zu sichern und im Falle eines Datenverlusts sicher wiederherzustellen.
- **Compliance Management:** Tools wie Microsoft Purview Compliance Manager oder IBM OpenPages können dabei helfen, den Überblick über Compliance-Anforderungen zu behalten.

Unser Fazit

- NIS2 ist ein positiver Impuls aus der Politik
- Konkreter Mehrwert fürs Unternehmen, erhöht die Sicherheit und minimiert die Risiken
- NIS2 sichert die Zukunft von Unternehmen und sollte als unumgängliche Investition gesehen werden

Ergebnis der Umsetzung der NIS2-Maßnahmen:
Umfassendes Sicherheitskonzept für das Unternehmen
und seine kritischen IT-Systeme

So kann Softline bei der Umsetzung unterstützen

NIS2 Assessment

1. Softline Reifegradermittlungen für die Themen **Informationssicherheit** (nach ISO 27001 und ISO 27002) und **IT-Security**
2. GAP-Analyse erstellen
3. Handlungsempfehlungen

SIEM – Tooling und der Betrieb in Form eines Security Operation Centers

1. Managed Detection
2. Managed Intelligence
3. Managed Response
4. Managed Risk

Sie haben noch Fragen?

Melden Sie sich gerne direkt bei mir!

Ronald Kuntz | ronald.kuntz@softline.de | +49 (341) 24051-201

Die Webinarreihe geht im Herbst weiter.

Teil 3

Vorfallreaktion und Forensik:
Praxisbeispiele für das Navigieren durch Cybersicherheitsvorfälle

Teil 4

SOC as a Service:
Ein umfassender Einblick in Managed Security Services