Whitepaper zur NIS-2-Richtlinie

Stand Oktober 2023

„Die Zukunft kann man
am besten voraussagen,
indem man sie selbst gestaltet!“
- Alan Kay –

Contents

ÜBER PASSION4IT

Wir haben die Berge im Blut und die Leidenschaft für IT bereits im Namen. Diese Kombination zeichnet unsere Arbeitsweise aus: Die Freude, unsere Kunden aus dem Mittelstand auf ein neues Level zu begleiten. Sie mit pragmatischen Digitalisierungs-Lösungen fit für die Zukunft und die Herausforderungen von morgen zu machen.

Bei den gemeinsamen Projekten nehmen wir dabei die Rolle der digitalen Bergführer ein. Wir analysieren den Leistungsstand deines Teams, zeigen Routen auf und planen gemeinsam den Aufstieg und das notwendige Equipment. Genauso wichtig ist uns dabei aber immer deine Crew. Wir sind kein Helikopter-Shuttle, das deine Crew absetzt und wieder verschwindet, sondern verfolgen die Philosophie einer aktiven, eingespielten Seilschaft am Berg. In der jedes Teammitglied die Besteigung aus eigener Kraft bewältigen muss.

Das ist manchmal gewiss unbequem, es sichert den Erfolg jedoch nachhaltig ab. Und: Die gemeinsame Freude am Gipfel, das Leuchten in den Augen der Teilnehmer über den Ausblick, vor allem aber über die eigene Leistung, ist durch nichts zu ersetzen!

Wenn du eine Expedition planst, trommle die Leute nicht zusammen, um Aufgaben zu verteilen, Ausrüstung zu sammeln und Routen zu planen, sondern lehre sie die Sehnsucht nach den erhabenen Gipfeln und dem endlosen Himmel.

www.passion4it.de

EINLEITUNG

Die Digitalisierung ist ein Schlüssel zur Steigerung von Effizienz und Flexibilität in der modernen Arbeitswelt. Mit der wachsenden Bedeutung von Technologien steigt jedoch auch die Abhängigkeit und die Gefahr durch Cyberkriminalität.

Die bevorstehende NIS2-Richtlinie der EU ist eine zentrale Vorschrift, die Unternehmen beachten müssen, um Strafen zu vermeiden und Sicherheit zu gewährleisten.

NIS-2-RICHTLINIE IM ÜBERBLICK

Die NIS2-Richtlinie ist eine überarbeitete Version der NIS1-Richtlinie von 2016 und stellt strengere Anforderungen an die Cybersecurity für ein breiteres Spektrum von Unternehmen. Bei Verstößen drohen Strafen von bis zu 10 Millionen Euro. Die Richtlinie betrifft "wesentliche Sektoren" wie Energie, Gesundheit, Transport und Bankwesen sowie "wichtige Sektoren" wie Post, Abfallwirtschaft, Chemie und digitale Dienste.

WAS IST DIE NIS-2 RICHTLINIE?

- NIS steht für Netz- und Informationssystemsicherheit.
- Ziel: Ein hohes, einheitliches Cybersicherheitsniveau in der EU.
- Es werden Mindeststandards vorgegeben; Länder können jedoch strengere Vorschriften erlassen.

AB WANN GILT NIS-2?

Das NIS-Umsetzungsgesetz soll im März 2024 verkündet werden und wie geplant ab Oktober 2024 in Kraft treten. Mit der NIS-2-Richtlinie (EU) 2022/2555 gelten ab Oktober 2024 für viele Unternehmen und Organisationen in 18 Sektoren verpflichtende Sicherheitsmaßnahmen und Meldepflichten – auch für viele, die bisher nicht betroffen waren.

- Seit Anfang 2023 auf EU-Ebene in Kraft.
- Bis zum 17. Oktober 2024 in nationales Recht umzusetzen.
- Das deutsche NIS2-Umsetzungsgesetz liegt als Referentenentwurf vor.

WEN BETRIFFT NIS-2?

Unternehmen mit mindestens 50 Mitarbeitern und einem Jahresumsatz oder einer Jahresbilanz von über 10 Mio. Euro könnten unter den Anwendungsbereich der NIS-2-Richtlinie fallen, sofern sie in den betroffenen Sektoren tätig sind.

ÜBERSICHT DER 18 BETROFFENEN SEKTOREN

Energie (Elektrizität, Fernwärme, Erdöl, Erdgas, Wasserstoff)	Transport (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr)
Bankwesen (Kreditinstitute)	Finanzmarktinfrastruktur (Handelsplätze, Zentrale Gegenpartien)
Gesundheit (Gesundheitsdienstleister; EU Labore, Medizinforschung, Pharmazeutik, Medizingeräte)	Trinkwasser (Wasserversorgung)
Abwässer (Abwasserentsorgung)	Digitale Infrastruktur (Internet-Knoten (IXP), DNS (ohne Root), TLD Registries, Cloud Provider, Rechenzentren, CDNs, Vertrauensdienste (TSP), Elektronische Kommunikation)
IKT-Dienstleistungsmanagement (B2B) (Managed Service Providers, Managed Security Service Providers	Öffentliche Verwaltungen (Zentralregierung, regionale Regierung)
Weltraum (Bodeninfrastruktur)	Post- und Kurierdienste (Postdienste)
Abfallwirtschaft (Abfallbewirtschaftung)	Herstellung, Produktion und Vertrieb von Chemikalien (Unternehmen im besonderen öffentlichen Interesse)
Lebensmittelproduktion, -verarbeitung und -vertrieb	Produktion, Herstellung von Medizinprodukten, Maschinen, Fahrzeugen sowie elektrischen/elektronischen Geräten
Digitale Anbieter (Marktplätze, Suchmaschinen, soziale Netzwerke)	Forschung (Forschungsinstitute)

AUSNAHMEREGELUNGEN BEI DER KATEGORISIERUNG NACH NIS-2

Die Kategorisierung nach NIS-2 berücksichtigt nicht nur Größe und Umsatz eines Unternehmens. Es gibt spezielle Ausnahmen, etwa wenn ein Unternehmen essenzielle Funktionen ausführt, Einfluss auf die öffentliche Sicherheit hat oder wenn systemische Risiken und internationale Auswirkungen auftreten würden, sollte es ausfallen. Diese könnten im Geltungsbereich der NIS2 enthalten sein, selbst wenn sie weniger als 50 Mitarbeiter beschäftigen oder ihr Jahresumsatz unter 10 Millionen Euro liegt.

Beispielsweise könnten auch kleinere Firmen, die Lieferanten eines NIS-2 betroffenen Unternehmens sind, berücksichtigt werden (somit soll laut NIS-2 Cybersecurity auch in Lieferketten berücksichtigt sein):

- „Supply Chain: Sicherheit in der Lieferkette — bis zur sicheren Entwicklung bei Zulieferern“
- „Cyber Security: Die Anforderungen an Betreiber und Mitgliedstaaten steigen, Cyber Security muss auch in Lieferketten betrachtet werden“

Quelle: EU NIS-2 Direktive: Cybersecurity in Kritischen Infrastrukturen (openkritis.de)

- "Den größten Nachholbedarf gibt es bei den Anforderungen zur Kontrolle von Lieferanten, Dienstleistern und Dritten: Hier liegt der Umsetzungsstand bei 65 Prozent."

Quelle: Untersuchung der Wirksamkeit der IT-Sicherheitsgesetze unter Betreibern Kritischer Infrastrukturen (bund.de)

- Kunden könnten NIS2-Pflichten an ihre Lieferanten vertraglich übertragen.
- Kunden könnten aus Haftungsgründen einen Nachweis für Cybersecurity von ihrem Lieferanten verlangen.

WAS MÜSSEN BETROFFENE UNTERNEHMEN UND ORGANISATIONEN TUN?

Maßnahmen zum Risikomanagement für Cybersicherheit umsetzen:

- Konzepte für Risikoanalyse und Sicherheit für Informationssysteme.
- Prävention, Erkennung und Bewältigung von Sicherheitsvorfällen.
- Business Continuity (z.B. Backup-Management) und Krisenmanagement.
- Sicherheit in der Lieferkette.
- Sicherheit bei Einkauf, Entwicklung und Wartung der IT-Systeme.
- Bewertung der Wirksamkeit der Maßnahmen.
- Cyberhygiene (z.B. Updates) und Schulungen in Cybersecurity.
- Kryptografie und ggf. Verschlüsselung.
- Personalsicherheit, Zugriffskontrolle und Asset Management.
- Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung.

HANDLUNGSBEDARF

Unternehmen sollten unverzüglich handeln, um die Richtlinie bis Oktober 2024 umzusetzen. Dies erfordert eine umfassende Überprüfung und Anpassung der internen Prozesse und IT-Sicherheitsmaßnahmen. Die Umsetzung kann in Schritten unterteilt werden, von der Identifikation kritischer Infrastrukturen bis zur kontinuierlichen Überprüfung der IT-Sicherheitsrichtlinien.

NIS-2 SCHNELLTEST

PWC: Qualtrics Survey | Qualtrics Experience Management (pwc.com)

WKO.AT: wko.at Online-Ratgeber - Cybersicherheitsrichtlinie - NIS2

HANDLUNGSEMPFEHLUNG (P4IT CYBER SECURITY CHECK)

- ✓ **Analyse und Bewertung:** Beginnen Sie umgehend mit der Identifikation und Prüfung Ihrer internen kritischen Infrastrukturen und Dienstleistungen, und ob Sie NIS-2 betroffen sind.

    - Um den besonderen Anforderungen von KMUs gerecht zu werden, haben wir einen zielgerichteten Fragenkatalog basierend auf der ISO-27001 und BSI-Standards entwickelt. Mithilfe von 126 Fragen aus 16 Prüfgruppen werden technische und organisatorische Schutzmaßnahmen Ihres Sicherheitsprozesses hinsichtlich Cybersecurity überprüft, wir sehen uns auch die notwendige IT-Dokumentation und Richtlinien genauer an.

    - Ein umfangreicher Abschlussbericht legt ihnen alle Ergebnisse zum IST-Zustand Ihrer IT-Sicherheit vor. Anschließend können wir gemeinsam über entsprechende Maßnahmen zur Beseitigung der aufgefundenen Mängel nachdenken. Kein System ist perfekt, wir sind uns also sicher, dass wir gemeinsam Verbesserungen erzielen können!

    - Die einzelnen Maßnahmenempfehlungen werden priorisiert und gleich Verantwortlichkeiten festgelegt, sodass ein konkreter Projektplan für die Umsetzung in Ihrem Unternehmen entsteht. Ihre Haftungsträger werden fortan eine ausgereifte Grundlage zur Planung des IT-Budgets vorliegen haben und können anhand dieser entsprechende Aufgaben auch ohne notwendiges Fachwissen delegieren.

- ✓ **Implementierung von Maßnahmen:** Setzen Sie umfassende Sicherheitsvorkehrungen um und integrieren Sie diese in Ihre Unternehmensstrategie und Prozesse und definieren Sie klare Verantwortlichkeiten.

- ✓ **Mitarbeiterschulung:** Sensibilisieren und schulen Sie Ihre Mitarbeiter bezüglich der Relevanz und Bedrohlichkeit von Cyberkriminalität (z.B. durch Anti-Phishing Kampagnen).

- ✓ **Überprüfung von Dienstleistern:** Stellen Sie sicher, dass auch Ihre Dienstleister die notwendigen Sicherheitsstandards einhalten (z.B. Cloudanbieter).

- ✓ **Kontinuierliche Überwachung:** Überprüfen Sie regelmäßig Ihre IT-Sicherheitsrichtlinien und passen Sie diese an die aktuelle Bedrohungslage an. PASSION4IT bietet dazu einen Managed Service an.

FAZIT

Die NIS2-Richtlinie stellt erhöhte Anforderungen an die Cybersecurity von Unternehmen. Mittelstand, Geschäftsführer und IT-Leiter sollten jetzt handeln, um die Compliance sicherzustellen und Strafen zu vermeiden. Zur Erfüllung der NIS-2-Richtlinie empfiehlt sich die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001.

BEITRAG VON PASSION4IT

PASSION4IT unterstützt Unternehmen dabei, die Anforderungen der NIS2-Richtlinie zu verstehen und umzusetzen. Wir bieten Beratung und Unterstützung bei der Identifikation kritischer Infrastrukturen, der Sensibilisierung von Mitarbeitern und der Überprüfung von Online-Dienstleistern.

KONTAKT

Für weitere Informationen und Unterstützung kontaktieren Sie Florian Laumer

Terminvereinbarung

Tel: +49 151 11676 502
E-Mail: florian.laumer@passion4it.de

- ITQ Auditor (Information Security)
- LEAD Digital Transformation Analyst (LEADing Practice)
- Certified SAFe 6 Agilist
- ICO ISMS Security Officer according to ISO/IEC 27001:2022