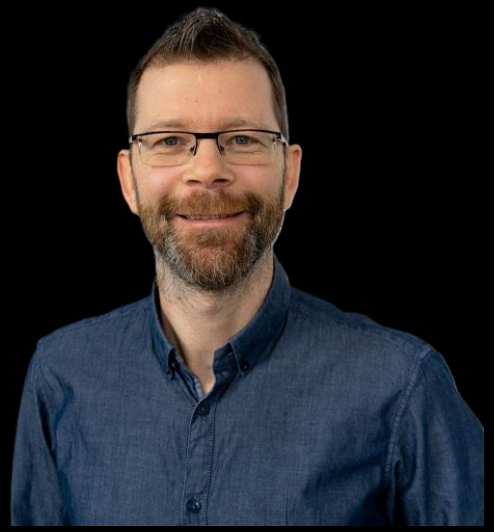

base it

DIE ANTWORT AUF NIS 2 IN DER MICROSOFT PLATTFORM

PETER FORSTER

Lead Architect

2024-03-08

professional.
fast.
secure.

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

Agenda

- **NIS 2 – eine Übersicht**
  - Allgemeine Informationen zur NIS 2
  - Welche Einrichtungen sind betroffen?
- **Die Umsetzung**
  - Maßnahmen erkennen und umsetzen
  - Nachweise zur erfolgreichen Umsetzung
  - Laufende Kontrolle

NIS 2 – EINE ÜBERSICHT

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

- Umsetzung bis 17. Oktober 2024 als nationales Gesetz
- Risikomanagementmaßnahmen umsetzen
- Meldepflichten
- Betroffen: kleine, mittlere und große Unternehmen
- Betroffen: Digitale Infrastruktur
- indirekt betroffen: Lieferkette

NIS 2.0

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

base it

Umsetzung bis 17. Oktober 2024 als nationales Gesetz

- Gültig ab 18. Oktober 2024
- Richtline muss in nationales Gesetz umgewandelt werden
- Gesetz wird sich voraussichtlich nicht wesentlich von der Richtlinie unterscheiden
  - Mit der Umsetzung nicht auf das Gesetz warten

- NIS 2 Directive zum Nachlesen
- https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555&qid=1704363865349

Risikomanagementmaßnahmen erkennen

- Maßnahme für Risikobewertung und Informationssicherheit
- Handhabung von Sicherheitsereignissen
- Betriebskontinuität und Krisenbewältigung
- Sicherheitsvorkehrungen bei Kauf/Entwicklung/Wartung von IKT-Systemen
- Methoden und Prozesse zur Beurteilung der Effektivität von Risikosteuerungsmaßnahmen

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

base it

Risikomanagementmaßnahmen erkennen

- Cyberhygiene und Fortbildungen im Bereich Cybersicherheit
- Verschlüsselungstechniken und ggf. Verschlüsselung
- Personalsicherheit, Zugriffskontrollstrategien
- Authentifizierung mit mehreren Faktoren
- Sicherheit der Lieferkette muss gewährleistet sein

- **Zusammengefasst: Umsetzung eines Informationssicherheits & Management-System (ISMS)**

Risikomanagementmaßnahmen erkennen

- ISO/IEC 27001:2022 schreibt viele dieser organisatorischen Maßnahmen bereits vor

- Geschäftsführung bzw. Vorstand persönlich in der Verantwortung

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

Meldepflichten

- https://nis.cert.at/
  - maximal 24h nach Kenntnis muss der Vorfall gemeldet werden
  - Nach maximal 72h muss eine Meldung über die erste Bewertung durchgefürht werden
  - Abschlussmeldung bis maximal 1 Monat nach der initialen Meldung

Dauert der Vorfall länger als 1 Monat muss eine Zwischenmeldung jedes Monat durchgeführt werden

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

betroffen: mittlere und große Unternehmen

Unternehmensklasse	Beschäftigte (VZÄ*)	Jahresumsatz	Jahresbilanzsumme
Kleines Unternehmen **Achtung: Sonderfälle!**	< 50 und	< 10 Mio. Euro oder	≤ 10 Mio. Euro
Mittleres Unternehmen	< 250 und	≤ 50 Mio. Euro oder	≤ 43 Mio. Euro
Großes Unternehmen	≥ 250	< 50 Mio. Euro und	> 43 Mio. Euro

*VZÄ = Vollzeitäquivalente. zB gelten zwei Teilzeitbeschäftige als ein Beschäftigter

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

betroffen: mittlere und große Unternehmen

- Bei komplexen Unternehmensstrukturen ist eine Einzelfallprüfung notwendig
- zB Tochtergesellschaft in einem Konzern

- Schnellanalyse der WKO: https://ratgeber.wko.at/NIS2/

base-IT kann keine akkreditierte Auskunft über die Pflicht zur NIS 2 geben

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

betroffen: mittlere und große Unternehmen bestimmter Sektoren

- Unterscheidung zwischen wesentlich und wichtig

Sektoren der wesentlichen Unternehmen:

Energie / Verkehr / Bankwesen / Finanzmarkt / Gesundheit / Trinkwasser / Abwasser / Digitale Infrastruktur / Verwaltung von IKT-Diensten / Weltraum / öffentliche Verwaltung

Wesentliche Einrichtungen müssen regelmäßige Audits durchführen

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

base it

betroffen: mittlere und große Unternehmen bestimmter Sektoren

Sektoren der wichtigen Unternehmen:

Post und Kurierdienste / Abfallbewirtschaftung / Chemie / Lebensmittelproduktion- und Handel / verarbeitendes und herstellendes Gewerbe / Anbieter digitaler Dienste / Forschung

Wichtige Einrichtungen werden nur bei begründetem Verdacht überprüft

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

base it

betroffen: mittlere und große Unternehmen bestimmter Sektoren

Die Direktive Liste in Anhang I und Anhang II konkret die Sektoren auf, welche betroffen sind. Auszug:

ANHANG II

SONSTIGE KRITISCHE SEKTOREN

Sektor	Teilsektor	Art der Einrichtung
1. Post- und Kurierdienste		Anbieter von Postdiensten im Sinne des Artikels 2 Nummer 1a der Richtlinie 97/67/EG, einschließlich Anbieter von Kurierdiensten
2. Abfallbewirtschaftung		Unternehmen der Abfallbewirtschaftung im Sinne des Artikels 3 Nummer 9 der Richtlinie 2008/98/EG des Europäischen Parlaments und des Rates ([1]), ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist
3. Produktion, Herstellung und Handel mit chemischen Stoffen		Unternehmen im Sinne des Artikels 3 Nummern 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates ([2]), die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse im Sinne des Artikels 3 Nummer 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln		Lebensmittelunternehmen im Sinne des Artikels 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates ([3]), die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

basg it

Immer betroffen: Digitale Infrastruktur

- Unabhängig von der Unternehmensgröße
- Bestimmte digitale Dienste
  - 2 Personen, welche einen öffentlichen DNS-Service anbieten fallen unabhängig vom Umsatz und der Unternehmensgröße unter die Richtlinie als wichtiges Unternehmen

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

base it

indirekt betroffen: Lieferkette

- Kunde wird an den Lieferanten/Geschäftspartner die NIS 2 Pflichten vertraglich übertragen
- Kunde wird einen Nachweis über die Maßnahmen verlangen

- Indirekt betroffen bedeutet nicht, dass die NIS 2 vollumfänglich umgesetzt werden muss

Sicherheit hat noch nie geschadet!

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

indirekt betroffen: Lieferkette

- Nachweis kann erfolgen durch:
  - ÖISHB: Zusammenarbeit mit Externen (6.2), Evaluierung von Zertifizierungen (14.2), Lieferantenbeziehungen (15)
  - ISO/IEC 27001: Information security in supplier relationships
  - IEC 62443 2-1: Supply chain security
  - CIS CSC v8.0: Service Provider Management
  - KSÖ Cyber Risk Rating: Anforderungen für A bzw. B Rating
    - Demo-Assessment: https://demo.cyberrisk-rating.at/

ÖISHB: österreichisches Informationssicherheitshandbuch
CIS CSC: Center for internet security - Critical security controls
KSÖ: Kompetenzzentrum sicheres Österreich

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

Registrierungspflicht

- Unternehmen werden sich registrieren müssen
- Möglich sind Verwaltungsstrafen bei einer nicht erfolgten Registrierung

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

Haftung (Auszug der WKO)

Die Leitungsorgane (Geschäftsführung bei GmbH, Vorstand und Aufsichtsrat bei Aktiengesellschaften) betroffener Einrichtungen müssen die Einhaltung der Risikomanagementmaßnahmen sicherstellen und beaufsichtigen. Sie haften schadenersatzrechtlich, wenn dem Unternehmen durch die Nichteinhaltung ein schuldhaft verursachter Schaden entstanden ist. Die Leitungsorgane müssen sich die notwendigen Fähigkeiten im Bereich Cybersicherheit in Schulungen aneignen und auch den Mitarbeiter:innen entsprechende Schulungen anbieten.

Haftung (Auszug aus der Direktive)

*Die Mitgliedstaaten stellen sicher, dass die **Mitglieder der Leitungsorgane wesentlicher** und wichtiger **Einrichtungen** an **Schulungen teilnehmen müssen**, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben*

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

Strafrahmen

- Wesentliche Einrichtungen: 10.000.000 EUR bzw. 2% des Umsatzes
- Wichtige Einrichtungen: 7.000.000 EUR bzw. 1,4% des Umsatzes

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

Operative Umsetzung

- Unterliegt man der NIS 2? → Kunde
  - Lieferkette? → Kunde
- Ressourcen bereitstellen → Kunde/base-IT
- Sicherheitslandkarte mit Assets erstellen → Kunde/base-IT
- Risikoanalyse erstellen → Kunde/base-IT
- Maßnahmen ermitteln → Kunde/base-IT
- Maßnahmen umsetzen → Kunde/base-IT
- Laufende Kontrolle → Kunde/base-IT

NIS 2 UND MICROSOFT

NIS 2 UND MICROSOFT

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

NIS 2 BEREICHE

Verwalten des Sicherheitsrisikos	Schutz vor Cyberattacken	Erkennen von Cyberattacken	Die Auswirkungen von Cybersicherheitsvorfällen minimieren

NIS 2 Prinzipien

A1: Governance	A2: Risiko-management	B1: Schutz-richtlinien und -verfahren für Dienste	B2: Identitäts- und Zugrifss-verwaltung	C1: Aktives Monitoring von Sicherheits-vorfällen	C2: Proaktive Erkennung von Sicherheits-vorfällen	D1: Planung für Reaktion und Wieder-herstellung	D2: Lessons Learned
A3: Asset Verwaltung	A4: Supply Chain	B3: Datensicherheit	B4: System-sicherheit				
		B5: Ausfallsichere Systeme	B6: Anwender-schulungen				

NIS 2 UND MICROSOFT

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

NIS-Prinzipen	Microsoft Lösung
Governance	Defender CSPM, Entra
Risikomanagement	Defender XDR & Purview Compliance Manager
Assetverwaltung	Defender CSPM, Defender for Endpoint
Identity und Zugriff	Entra
Datensicherheit	Purview Information Protection
Systemsicherheit	Defender for Endpoint, Defender for IoT & Intune
Ausfallsichere Systeme	Azure, M365 Services
Anwenderschulungen	Defender Attack Simulator & Trainings
Sicherheitsüberwachung	Microsoft Sentinel
Proaktive Sicherheit	Defender XDR
Reaktion und Recovery	Defender XDR, Azure Backup & Recovery

OPERATIVE UMSETZUNG

Operative Umsetzung mit base-IT

- Im Wesentlichen bedeutet dies:
- Zero Trust Grundsätze → Conditional Access (MFA), Defender XDR
- Software-Updates → SCCM, Intune bzw. 3rd Party Patch-management
- Netzwerksegmentierung
- Identity Management mit Entra ID Plan 2
- Schulungen der AnwenderInnen wie zB Attack-Simulator
- Defender for Identity

Operative Umsetzung mit base-IT

- Sammeln von Log-Files der Systeme
- Erkennen von notwendigen Alarmierungen
- Microsoft Sentinel inkl. Anbindung an ITSM-Systeme

NIS 2

Network and Information Systems - Sicherheit von Netz- und Informationssystemen

Operative Umsetzung mit base-IT

- Für die vollständige Umsetzung der NIS 2 Richtlinie ist eine Microsoft 365 E5 Lizenz notwendig (bzw. Microsoft 365 E5 + E5 Security) oder Microsoft 365 Business Premium (limitiert)

- Mit Hilfe des Compliance Managers können auch organisatorische Maßnahmen dokumentiert und umgesetzt werden

Operative Umsetzung mit base-IT

- Wir begleiten Sie am Weg zu NIS 2 in folgenden Punkten
- Bestandsanalyse
  - Welche Maßnahmen wurden bereits ohne NIS 2 umgesetzt
- Projektscope definieren
  - Welche Maßnahmen müssen noch umgesetzt werden, um der NIS 2 zu entsprechen
- Umsetzen der Maßnahmen
  - Mit unseren Consultants setzen wir die Maßnahmen in Ihrer Umgebung um

Operative Umsetzung mit base-IT

- Laufende Kontrolle
  - Durch regelmäßige Kontrolle wird die Einhaltung der Maßnahmen sichergestellt

Nutzen Sie hier unser Angebot für Managed Service Security und dem 24x7 Security Operations Center (SOC) über die Bereitschaft. Schnelles Handeln ist ein wesentlicher Vorteil, bei einem Security-Incident

Fragen und Antworten

KI-generiertes Bild wurde mit DALL E3 erstellt

base it

Ansfelden | Salzburg | Wien | Hall in Tirol

+43 7229 87800 - 0 | office@baseit.at | www.baseit.at

Unsere digitale Unternehmensbroschüre