Fallstricke, Stolpersteine, Mythen und Legenden

Was bedeutet die EU-weite NIS2-Umsetzung für direkt und indirekt betroffene Unternehmen?

Digital Security
Progress. Protected.

Maik Wetzel

Strategic Business Development Director DACH
- ESET Deutschland GmbH -

Digital Security
Progress. Protected.

Über ESET

- #1 EU-Hersteller IT-Security
- unabhängig, inhabergeführt
- 1992 gegründet
- HQ in Bratislava, weltweite Präsenz (21 Niederlassungen, 13 R&D Zentren)
- 195+ Länder und Regionen
- ca. 110 Mitarbeiter in Deutschland (Jena/München)

- ca. 2.500 Mitarbeiter global
- ca. 6.500 qualifizierte Reseller (IT-Dienstleister) in Deutschland
- breite Installations- und Kundenbasis
- 110.000.000+ Anwender
- 400.000+ Business Kunden
- 1.300.000.000+ geschützte Internetnutzer

Trust Seal
www.teletrust.de/itsmie

Warum NIS2??

Digital Security
Progress. Protected.

Bedrohungslage

- hybride Bedrohungslage
- Lage ist kritisch
- Zeitenwende
- Cybercrime as a Service
- Staatliche Akteure

Bestehende Mindeststandards (Regulierung)

- BSI-Gesetz / IT-SIG 2.0
- BSI-KritisV
- 10 Sektoren
- Hohe Schwellenwerte

Selbstregulierung des Marktes

- Unzureichend!
- Stand der Technik?
- IT-Sec = Chefsache?
- …

Gesellschaftliche Stabilität und Versorgungssicherheit

Ziele von NIS 2.0

Digital Security
Progress. Protected.

Ziele von NIS 2.0

Verbesserung der Resilienz / Cybersicherheit

Harmonisierung – EU-weite Standards

Verbesserung der Zusammenarbeit

Wer ist von NIS 2.0 betroffen?

Digital Security
Progress. Protected.

Sektoren nach Anhang I	Sektoren nach Anhang II
Energie	Post- und Kurierdienste
Verkehr und Transport	Abfallwirtschaft
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmärkte	Produktion, Verarbeitung und Handel von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschungseinrichtungen
Digitale Infrastruktur	
ICT* Service Management (Managed Service Provider - MSP)	
Öffentliche Verwaltung	
Weltraum	

A Besonders wichtige Einrichtungen

Große Betreiber aus 11 Sektoren (Anhang I) und Sonderfälle

B Wichtige Einrichtungen

Große/Mittlere Betreiber aus allen 18 Sektoren und Sonderfälle, soweit nicht von besonders wichtigen Einrichtungen erfasst

Mittlere Unternehmen

- Mindestens 50 Beschäftigte
- Jahresumsatz/Jahresbilanz > 10 Mio. EUR

Große Unternehmen

- Mindestens 250 Beschäftigte
- Umsatz > 50 Mio. EUR
- Bilanz > 43 Mio. EUR

Unabhängig von Unternehmensgröße

Qualifizierende Faktoren, z.B.:

- Kritische Tätigkeit
- Auswirkung auf öffentliche Ordnung
- Systemrisiken
- Grenzüberschreitende Auswirkungen

NIS2- Was ist neu?

Digital Security
Progress. Protected.

Basics

- Definition von **Mindeststandards für Cybersicherheit**
- **Technische und organisatorische Maßnahmen** (gefahrenübergreifender, risikobasierter Ansatz, Stand der Technik)
- gilt grundsätzlich **für öffentliche und private Organisationen**, die ihre Dienste in der EU erbringen oder ihre Tätigkeit dort ausüben
- Anwendung bei betroffenen Unternehmen **für die gesamte Lieferkette**
- Unterscheidung **wichtige und besonders wichtige Einrichtungen**
- Sub-Kategorie: **Betreiber kritischer Anlagen**
- Massive **Ausweitung des Scope** (18 Sektoren, auch kleine/mittlere Unternehmen erfasst)

Und dann ist da noch…

Registrierungspflicht	• Registrierung beim BSI • Spätestens 3 Monate nach Inkrafttreten NIS2UmsuCG
Nachweispflicht	• Nur für Betreiber kritischer Anlagen (Auditberichte, Zertifikate, Mängelberichte, 3 Jahre nach Inkrafttreten) • Wichtige und besonders wichtige Einrichtungen keine Nachweispflicht (aber Dokumentationspflicht)
Unterrichtspflicht	• Generell bei erheblichen Sicherheitsvorfällen • Information aller Empfänger der Dienste der Einrichtung (Kunden) über Vorfall und Abhilfemaßnahmen
Meldepflicht	• Frühwarnung nach 24 Stunden (ab Kenntnisnahme) • innerhalb von 72 Stunden eine Folgemeldung (mit IoCs!) • Zwischenbericht auf Anfrage mit Status-Update (ohne Zeitangabe) • Abschlussbericht nach spätestes einem Monat

Leitungsorgane

Risikomanagement in wesentlichen und wichtigen Einrichtungen

- Verantwortlichkeit liegt bei den Leitungsorganen
  - Risikomanagementmaßnahmen zu initiieren, genehmigen („billigen“) und überwachen
- Leitungsorgane sollen für Verstöße der Einrichtungen persönlich verantwortlich gemacht werden können (!!)
- Schulungen werden für Leitungsorgane verpflichtend
  - für alle anderen Mitarbeiter dieser Einrichtungen sollen regelmäßige Schulungen angeboten werden

Sanktionen

Sanktionen (Grundsatz: wirksam, verhältnismäßig und abschreckend)

- Wesentliche Einrichtungen: Strafen bis zu einem Maximum von 10 Mio. EUR oder 2% des weltweiten Umsatzes
- Wichtige Einrichtungen: Strafen bis zu einem Maximum von 7 Mio. EUR oder 1,4% des weltweiten Umsatzes
- Persönliche Haftung der Leitungsorgane bei Pflichtverletzungen (?)

Nationale Umsetzung

Digital Security
Progress. Protected.

Zeitplanung	NIS2UmsuCG Zeitplan
Referentenentwurf	24.06.2024
Kabinettbeschluss über Regierungsentwurf	24.07.2024
Zuleitung Bundesrat	16.08.2024
Bundesrat 1. Durchgang	27.09.2024
Kabinettbeschluss über Gesetzänderung	02.10.2024 mit Nachmeldung
Zuleitung Bundestag	
Bundestag 1. Lesung	11.10.2024
Ausschüsse, Anhörung	Beschluss Anhörung 16.10.2024 Anhörung: 04.11.2024 Abschluss IA: 13.11.2024
Bundestag 2./3. Lesung	05./06.12.2024
Bundesrat 2. Durchgang	14.02.2025
Inkrafttreten	**März 2025**

Stand der Technik und Zero-Trust

Digital Security
Progress. Protected.

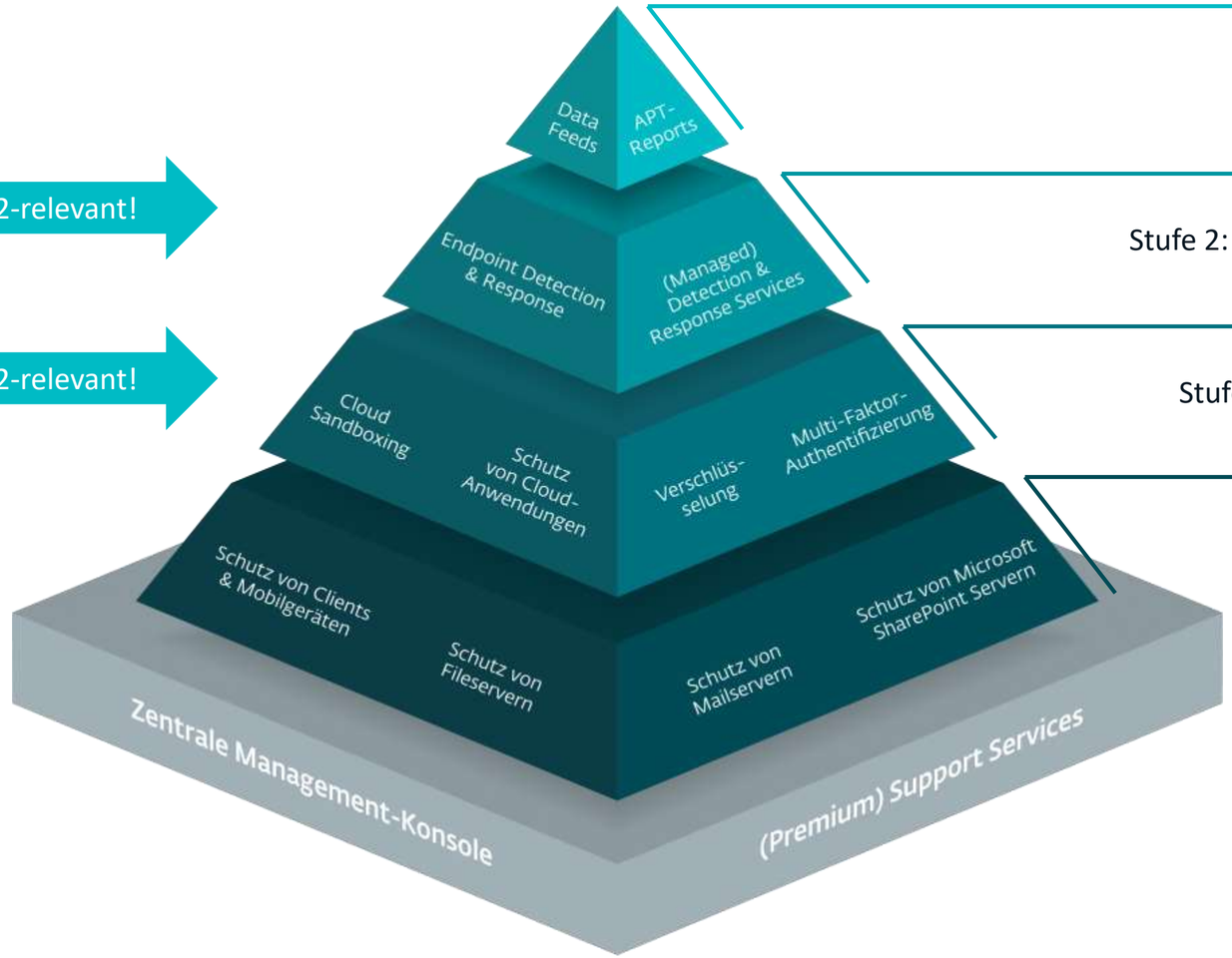
Zero Trust Security

EINSATZBEREICH

SCHUTZLEVEL

NIS2-relevant!

NIS2-relevant!



Ganzheitliches Lagebild – Außensicht

Stufe 3: Bietet tiefe Einblicke in die globale Bedrohungslandschaft als Grundlage für einen SOC-/SIEM-Betrieb

Gefahrensuche und Abwehr – Innensicht

Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalie-erkennung, Schwachstellenanalyse und Incident Management

Grundschutz Plus

Stufe 1: Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero-Days

Grundschutz Basis

Stufe 0: Mindestabsicherung für Endgeräte und Server

Digital Security
Progress. Protected.

Zero Trust Security

- passgenaue IT-Security für jeden Schutzbedarf
- Beschreibung aller Schutzlevel im Detail

Jetzt herunterladen

ESET 100% Made in EU IT-Security

Digital Security
Progress. Protected.

Handlungsempfehlung

Digital Security
Progress. Protected.

Ganz schön dickes Brett! Und nun?

Anfangen!!!!

Fragen beantworten: ist mein Unternehmen/mein Kunde betroffen? Verändert sich mein/sein Status?

Hilfe und Beratung suchen?

Zukünftige Verpflichtungen ableiten

Maßnahmen planen

Umsetzung beginnen

Anpassungen im Bereich von (vorhandenen) Versicherungen erfolgt / erforderlich?

⇒Pflichten identifizieren!

⇒Umsetzungsfristen beachten!

⇒Budgets planen

⇒Maßnahmen einleiten

Einige Fragen des gesunden Menschenverstandes…

1. Welche IT-Assets existieren in der Organisation (aktive Nutzung vs. Schatten-IT)?

2. Wie kritisch sind diese IT-Assets für den Geschäftsbetrieb? (Risikoanalyse, -bewertung, Wahrscheinlichkeit des Eintritts, anzunehm-ender Schaden bei Eintritt)

3. Wer betreibt diese IT-Assets und wo findet der Betrieb statt (on Prem, aaS, Cloud, eigene Infrastruktur)?

4. Mit welchen technisch-organisatorischen Maßnahmen kann ein dem festgestellten Risiko angemessener Schutz realisiert werden? (eventuell externe Beratung?)

5. Was ist Stand der Technik?

6. Wie können praktikable Notfallpläne und Wiederanlaufkonzepte aussehen? (regelmäßig üben!)

7. Müssen Verträge mit Lieferanten, Dienst-leistern oder Kunden angepasst werden? (Lieferkette!!)

8. …

Zielgruppe:
CISOs
Geschäftsführer
Vorstände / Beiräte
Security-Verantwortliche

Mehr Information:
www.eset.de/nis2

eset Digital Security
Progress. Protected.

Stand der Technik

Digital Security
Progress. Protected.

Herzlichen Dank für Ihre Aufmerksamkeit!

Fragen?

Maik Wetzel

Strategic Business Development Director DACH

ESET Deutschland GmbH
Spitzweidenweg 32
07743 Jena
Deutschland
Telefon: +49 3641 3114 211
Mobil: +49 151 401 037 04
maik.wetzel@eset.com
www.eset.de

Digital Security
Progress. Protected.