Prevention First

Cybersicherheit stärken: Die Umsetzung der NIS2-Richtlinie

Thorsten Urbanski

Director of Marketing
Leiter TeleTrust Initiative IT Security Made in EU

INTERNATIONAL CENTERS
BRATISLAVA (HQ)
SAN DIEGO
BUENOS AIRES
SINGAPORE

OFFICES
PRAGUE
JENA (DACH HQ)
MUNICH
BOURNEMOUTH
MILAN
TORONTO
MEXICO CITY
SAO PAULO
SYDNEY
MELBOURNE
TOKYO

RESEARCH AND DEVELOPMENT CENTERS
BRATISLAVA
KOSICE
ZILINA
PRAGUE
BRNO
JABLONEC NAD NISOU
KRAKOW
IAȘI
TAUNTON
MONTREAL
BUENOS AIRES
SINGAPORE

NR. 1 IN DER EU

35+ JAHRE CYBERSECURITY

MITARBEITENDE

2200+

NIEDERLASSUNGEN

23

FORSCHUNGS- & ENTWICKLUNGS- ZENTREN

12

“

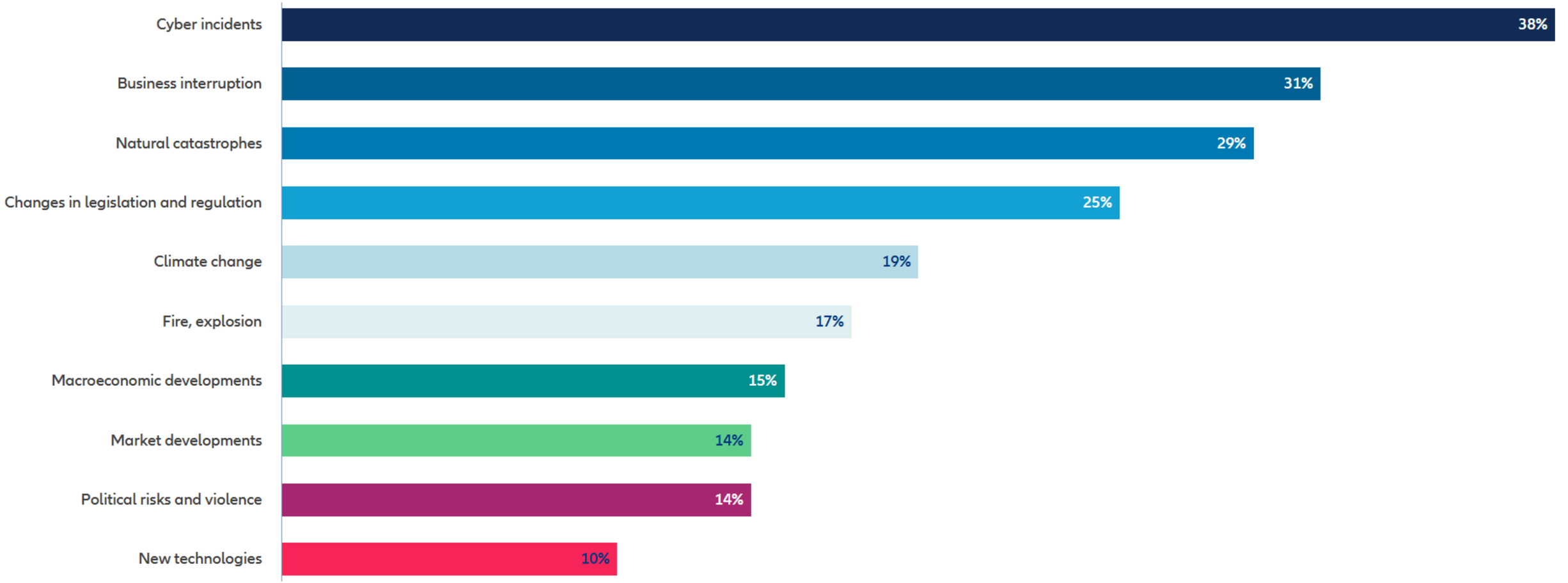
Deutschen Unternehmen ist durch Sabotage, Spionage und Datendiebstahl ein jährlicher Schaden von 267 Milliarden Euro entstanden

Bitkom-Wirtschaftsstudie 2024

The most important business risks in 2025: global

Allianz Risk Barometer 2025

Figures represent the number of risks selected as a percentage of all survey responses from 3,778 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.



Source: Allianz Commercial

Digitale Zeitenwende

Digital Security
Progress. Protected.

17. Dezember 2016

Angriffsziel:
KRITIS; Stromversorgung in Kiew

Auswirkungen:
Blackout

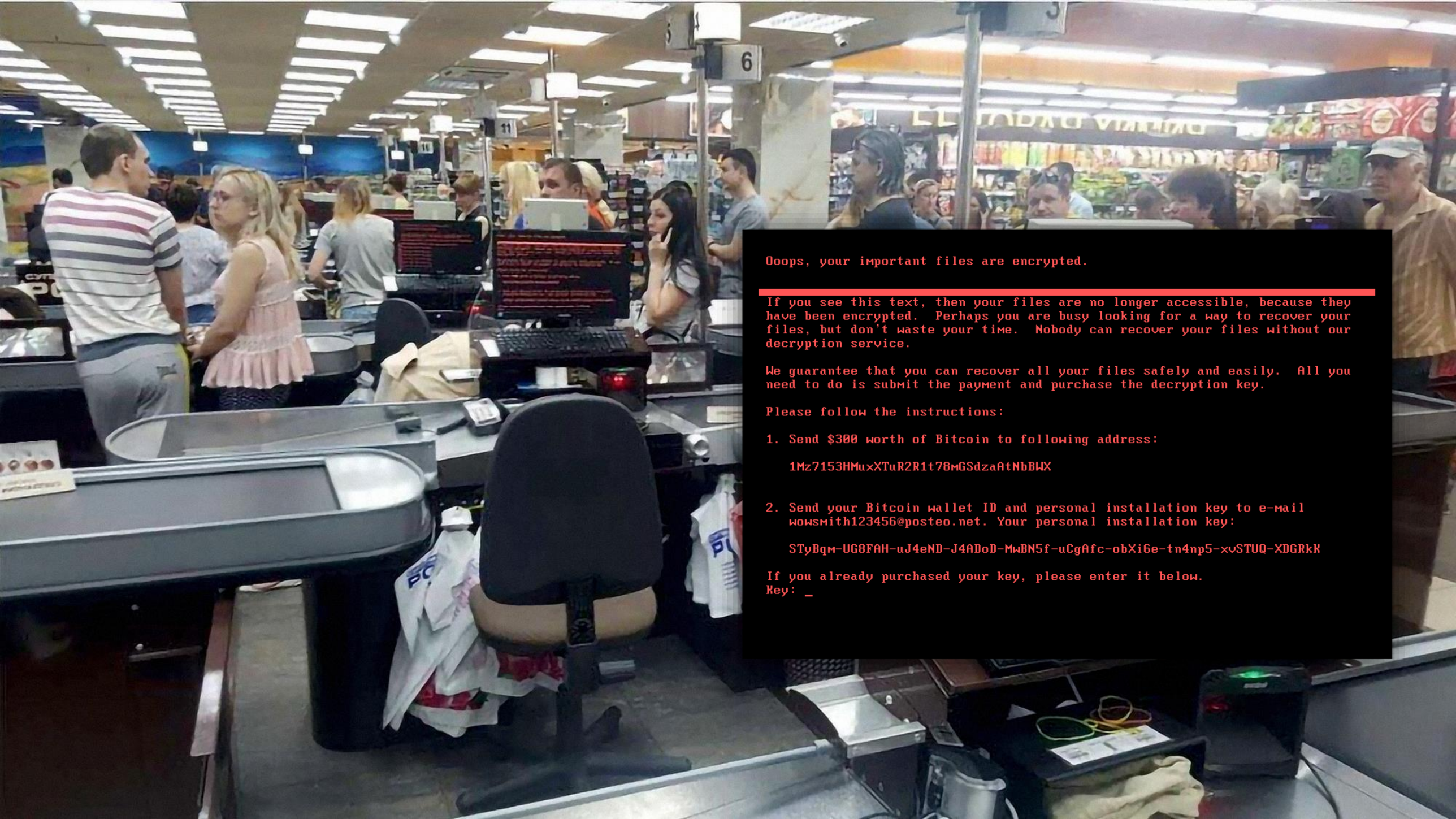
INDUSTROYER

WAS IST SO BESONDERS AN INDUSTROYER?

INDUSTROYER

2017 NotPetya (erste Kollateralschäden)

Digital Security
Progress. Protected.


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
STyBqm-UG8FAH-uJ4eND-J4ADoD-MwBN5f-uCgAfc-obXi6e-tn4np5-xvSTUQ-XDGRkK
If you already purchased your key, please enter it below.
Key: _

SCHADEN DURCH NOTPETYA

10 Milliarden USD

Die Täter

Digital Security
Progress. Protected.

Buhtrap

InvisiMole

Energetic Bear

Sandworm

Telebots
/Voodoo Bear

The Dukes

Cozy Bear/APT29

Turla

Gamaredon

Sednit

Fancy
Bear/APT28

FSB

SVR

GRU

Sources:

FBI

National Cyber Security Centre

Militaire Inlichtingen en Veiligheidsdienst

SECURITY SERVICE OF UKRAINE

Microsoft

Relation Cyber-Incidents zu KRITIS-Meldungen

DE

136.865

BKA/BSI Daten

davon KRITIS
200+ (0,15 %)

AT

17.000

CERT.at

davon KRITIS
85-170 (5-10%)

CH

34.000

Swiss NCSC

davon KRITIS
340-510 (10-15%)

Investitionswachstum in IT-Sicherheit

+ 17,3 %

Software

5,8 Milliarden Euro

+ 11,4 %

Services

4,4 Milliarden Euro

+ 5,2 %

Hardware

970 Millionen Euro

Quellen: IDC &Bitkom

NIS 2: Status Quo

Digital Security
Progress. Protected.

Der Zweck von NIS 2

Bedrohungslage

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

Bestehende Mindeststandards (Regulierung)

- BSI-Gesetz / IT-SIG 2.0
- BSI-KritisV
- 10 Sektoren
- Hohe Schwellenwerte
- Ca. 3.000 Organisationen

Selbstregulierung des Marktes

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

Gesellschaftliche Stabilität und Versorgungssicherheit

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

Cyber Security Maßnahmen NIS 2.0

Maßnahmen und Mindeststandards

- Mindestanforderungen, deren Einhaltung die Geschäftsführung von Betreibern nach nationaler Gesetzgebung überwachen und dafür haftbar gemacht werden soll.
- Maßnahmen:
  - **Policies:** Richtlinien für Risiken und Informationssicherheit
  - **Incident Management:** Prävention, Detektion und Bewältigung von Cyber Incidents
  - **Business Continuity:** BCM mit Backup Management, DR, Krisen Management
  - **Supply Chain:** Sicherheit in der Lieferkette — bis zur sicheren Entwicklung bei Zulieferern
  - **Einkauf:** Sicherheit in der Beschaffung von IT und Netzwerk-Systemen
  - **Effektivität:** Vorgaben zur Messung von Cyber und Risiko Maßnahmen
  - **Training:** und Cyber Security Hygiene
  - **Kryptographie:** Vorgaben für Kryptographie und wo möglich Verschlüsselung
  - **Personal:** Human Resources Security
  - **Zugangskontrolle**
  - **Asset Management (ISMS)**
  - **Authentication:** Einsatz von Multi Factor Authentisierung
  - **Kommunikation:** Einsatz sicherer Sprach-, Video- und Text-Kommunikation
  - **Notfall-Kommunikation:** Einsatz gesicherter Notfall-Kommunikations-Systeme

Fragestellungen und Maßnahmen

- Einführung eines Informationssicherheitsmanagementsystems (ISMS) z.B. nach ISO 27001 (viele der NIS2-Anforderungen sind Bestandteil von ISO 27001?)
- Welche IT-Assets und Prozesse gibt es?
- Welche Risiken verbinden sich mit diesen Assets für den Geschäftsbetrieb? (Risikoanalyse, Risikobewertung)
- Ableitung/Definition eines dem Risiko angemessenen Schutzniveaus
- Festlegung technischer und organisatorischer Schutzmaßnahmen (Stand der Technik!!)

Sicherheitsmaßnahmen umsetzen

- Notfallpläne und Wiederanlaufkonzepte erstellen
- Backup Konzepte erstellen und testen
- regelmäßige Schulungen und Trainings organisieren
- Beschaffung und Implementierung technischer Schutzlösungen
- Lieferketten einbeziehen
- Verträge mit Dienstleistern prüfen und gegebenenfalls anpassen

Kontinuierliche Messung der Wirksamkeit

Sicherheitsmaßnahmen sollten überwacht und kontinuierlich auf ihre Wirksamkeit überprüft werden

Stand der Technik ist ein Prozess!!

Bedrohungslage entwickelt sich

Regelmäßige Überprüfung und Anpassung

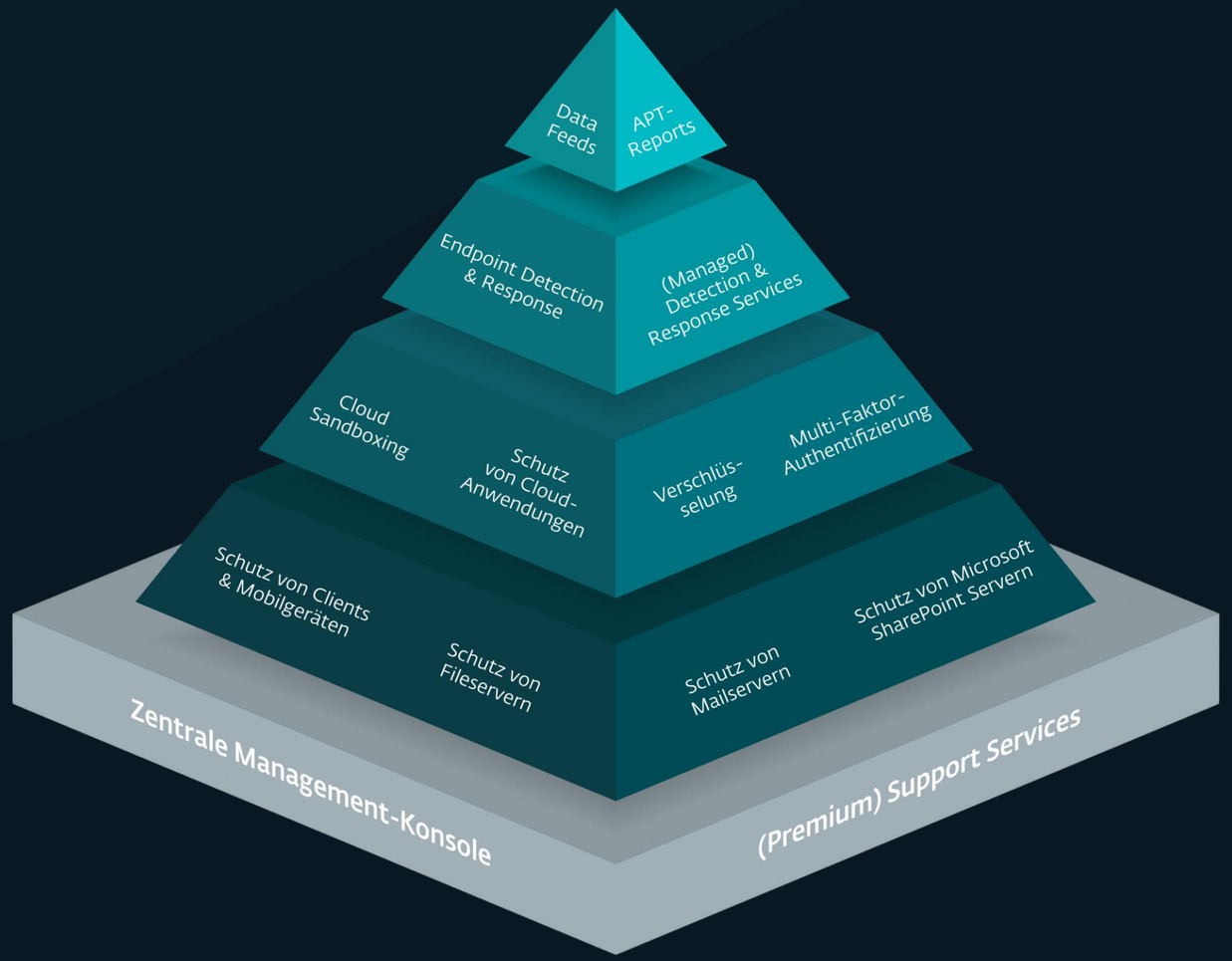
Technologische Anforderungen

Digital Security
Progress. Protected.

Must-Haves 2025

Digital Security
Progress. Protected.

Zero Trust Pyramide



Der Zero Trust Security-Ansatz von ESET besteht aus einem mehrstufigen, aufeinander aufbauenden Reifegradmodell. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer“.

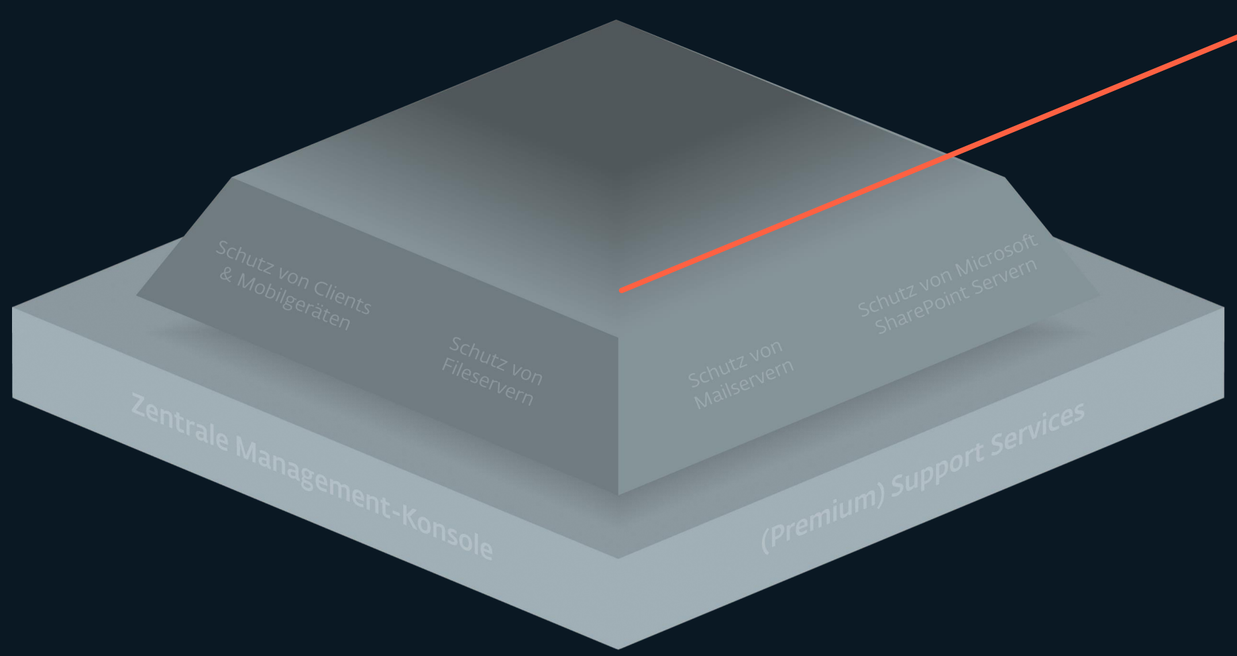
• GRUNDSCHUTZ BASIS

Reifegrad der IT-Organisation:

- Zentrales Management (Cloud oder On-Prem)
- Policies und Regeln für die Geräte- und Internetnutzung

• Unsere

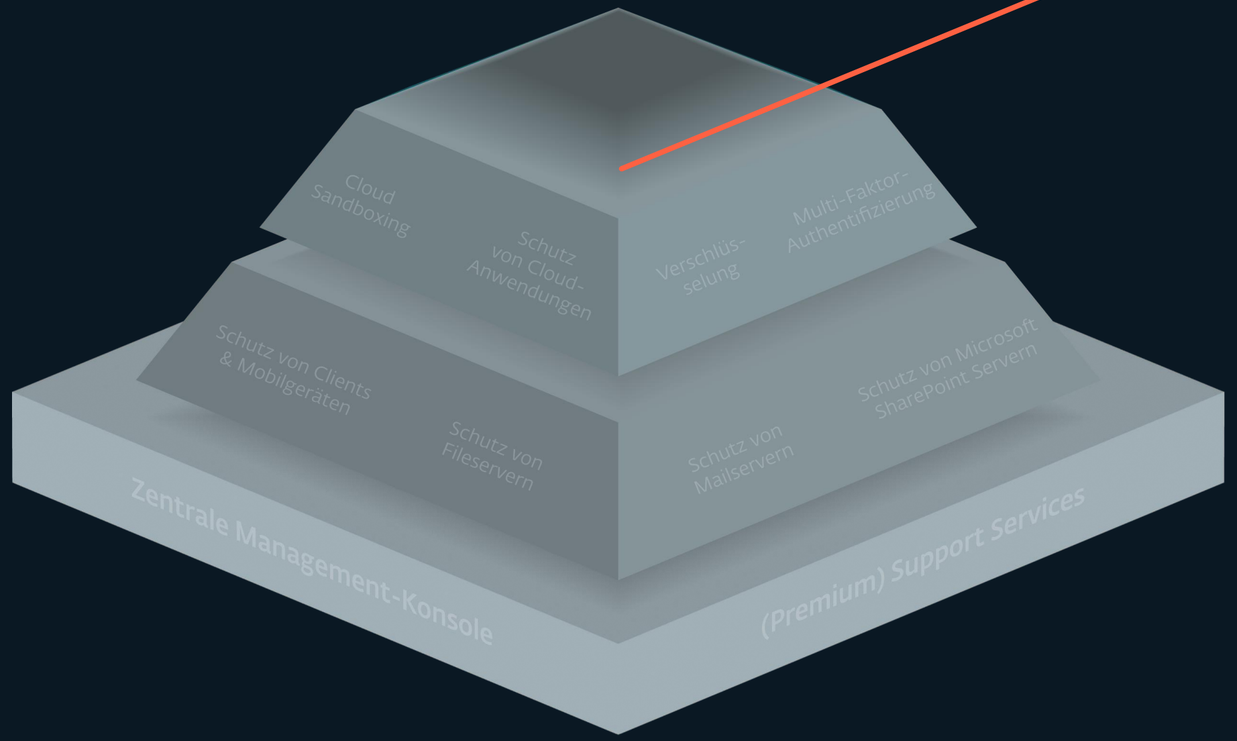
• GRUNDSCHUTZ PLUS



Reifegrad der IT-Organisation:

- Zentrales Management (Cloud oder On-Prem)
- Adaptive und skalierbare Policies, die auf dem Output der jeweiligen Lösung basieren

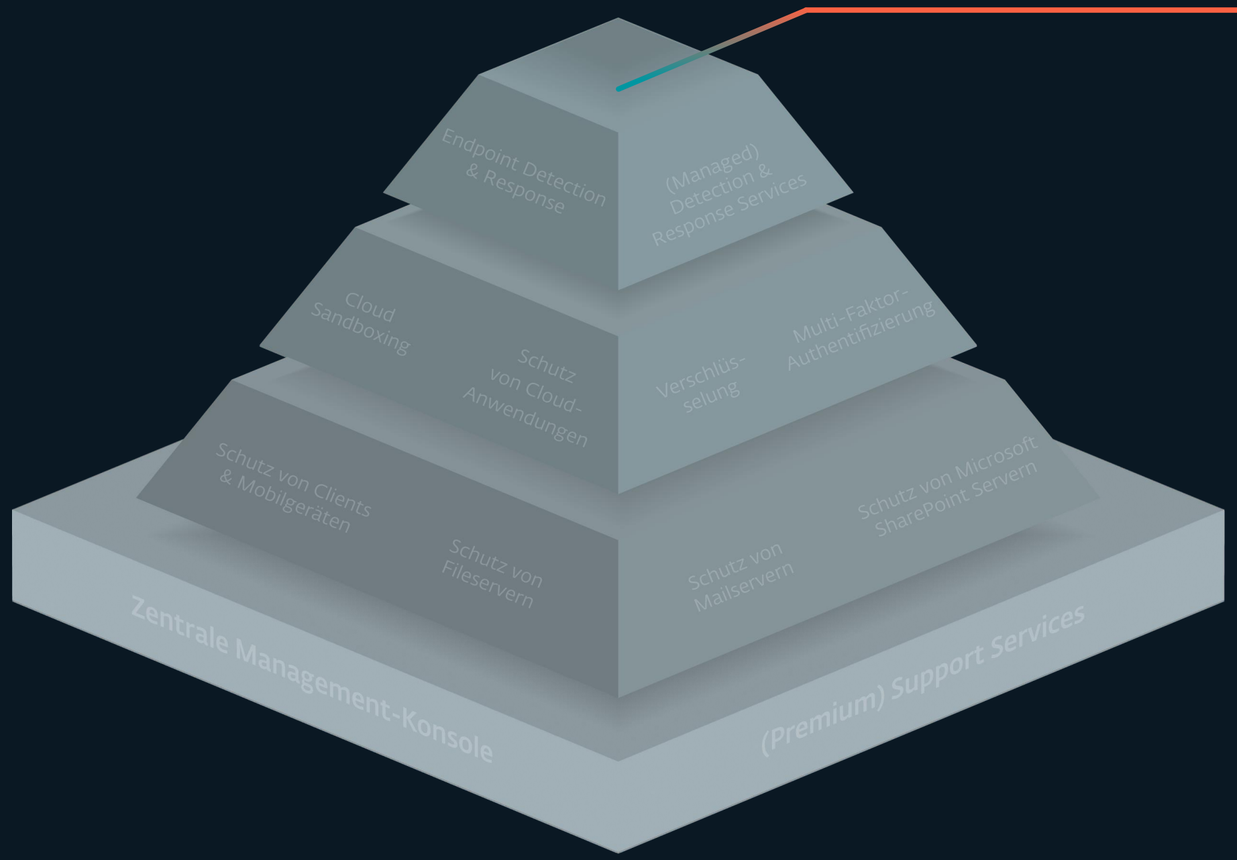
• GEFAHRENSUCHE UND ABWEHR - INNENSICHT



Reifegrad der IT-Organisation:

- Automatisierte Incident Detection und Threat Monitoring inkl. Forensik
- Evolutionäre Policies und Regeln durch Erkenntnisse aus der XDR-Plattform

• GANZHEITLICHES LAGEBILD - AUSSENSICHT



Reifegrad der IT-Organisation:

- Frühwarnsystem mittels SIEM-/SOC-Umgebung
- Umfangreiche präventive Sicherheitsmaßnahmen durch externes Lagebild

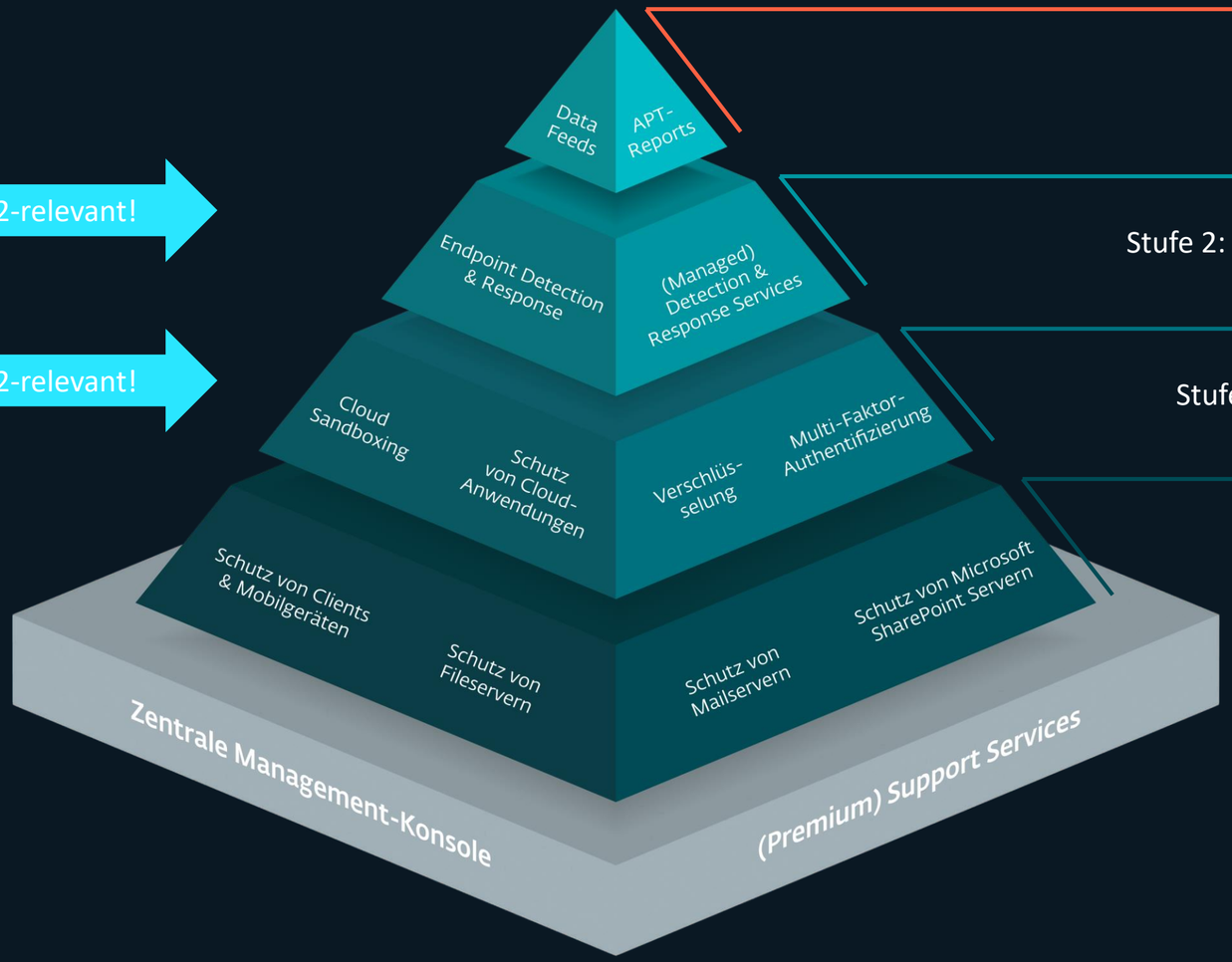
NIS 2 & Zero Trust Security

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

ESET 100% Made in EU IT-Security


EDR
Incident
Dashboard
221
MDR

Lösungsübersicht

ESET PROTECT

Modul	Entry (CLOUD ON-PREM MSP)	Advanced (CLOUD ON-PREM MSP)	Enterprise (CLOUD ON-PREM MSP)	Complete (CLOUD ON-PREM MSP)	Elite (CLOUD MSP)	MDR (CLOUD)	MDR Ultimate (CLOUD)	Mail Plus (CLOUD MSP)
Zentrale Management-Konsole	●	●	●	●	●	●	●	●
Schutz von Clients, Mobilgeräten und Fileservern	●	●	●	●	●	●	●	○
Cloud Sandboxing	○	●	●	●	●	●	●	●
Verschlüsselung	○	●	●	●	●	●	●	○
Schutz von Mailservern	○	○	○	●	●	●	●	●
Schutz von Cloud-Anwendungen	○	○	○	●	●	●	●	○
Schwachstellen- & Patch-Management	○	○	○	●	●	●	●	○
Multi-Faktor-Authentifizierung	○	○	○	○	●	●	●	○
Endpoint Detection and Response	○	○	●	○	●	●	●	○
SERVICES								
ESET Premium Support	○	○	○	○	○	Essential	Advanced	
ESET Detection & Response	○	○	○	○	○	ESET MDR	Ultimate	

ESET Digital Security
Progress. Protected.

ESET PROTECT Bundles

Zielgruppe:
CISOs
Geschäftsführer
Vorstände / Beiräte
Security-Verantwortliche

Mehr Information:
www.eset.de/nis2

Digital Security
Progress. Protected.

Herzlichen Dank für Ihre Aufmersamkeit!
Fragen?

Digital Security
Progress. Protected.

ESET Deutschland GmbH

Spitzweidenweg 32

07743 Jena

Deutschland

www.eset.de

Digital Security
Progress. Protected.