20/6/2023

„Stand der Technik“

Wie ein einzelner Begriff die IT-Sicherheit entscheidend verändert

Digital Security
Progress. Protected.

Michael Schröder

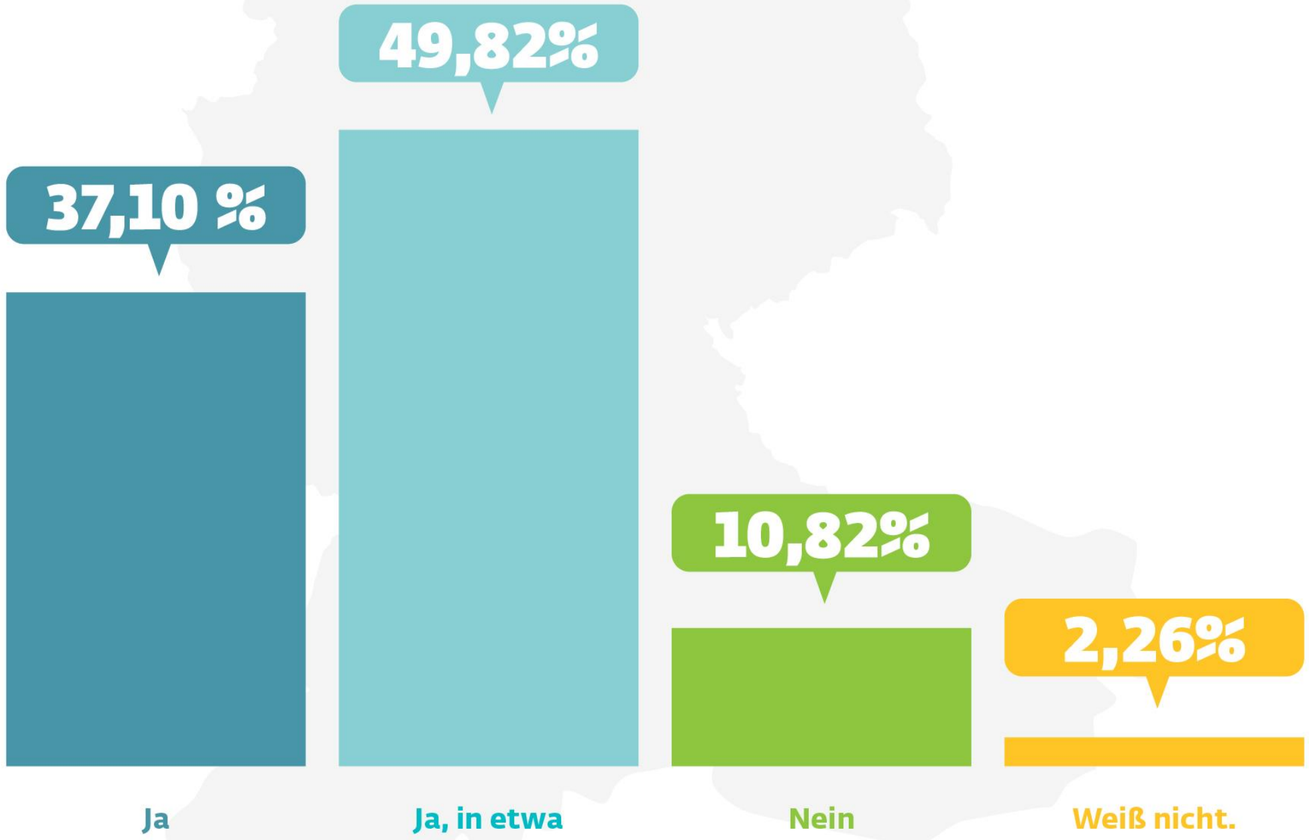
Manager of Security Business Strategy DACH
ESET Deutschland GmbH

michael.schroeder@eset.com

“Stand der Technik”
was ist das jetzt genau?

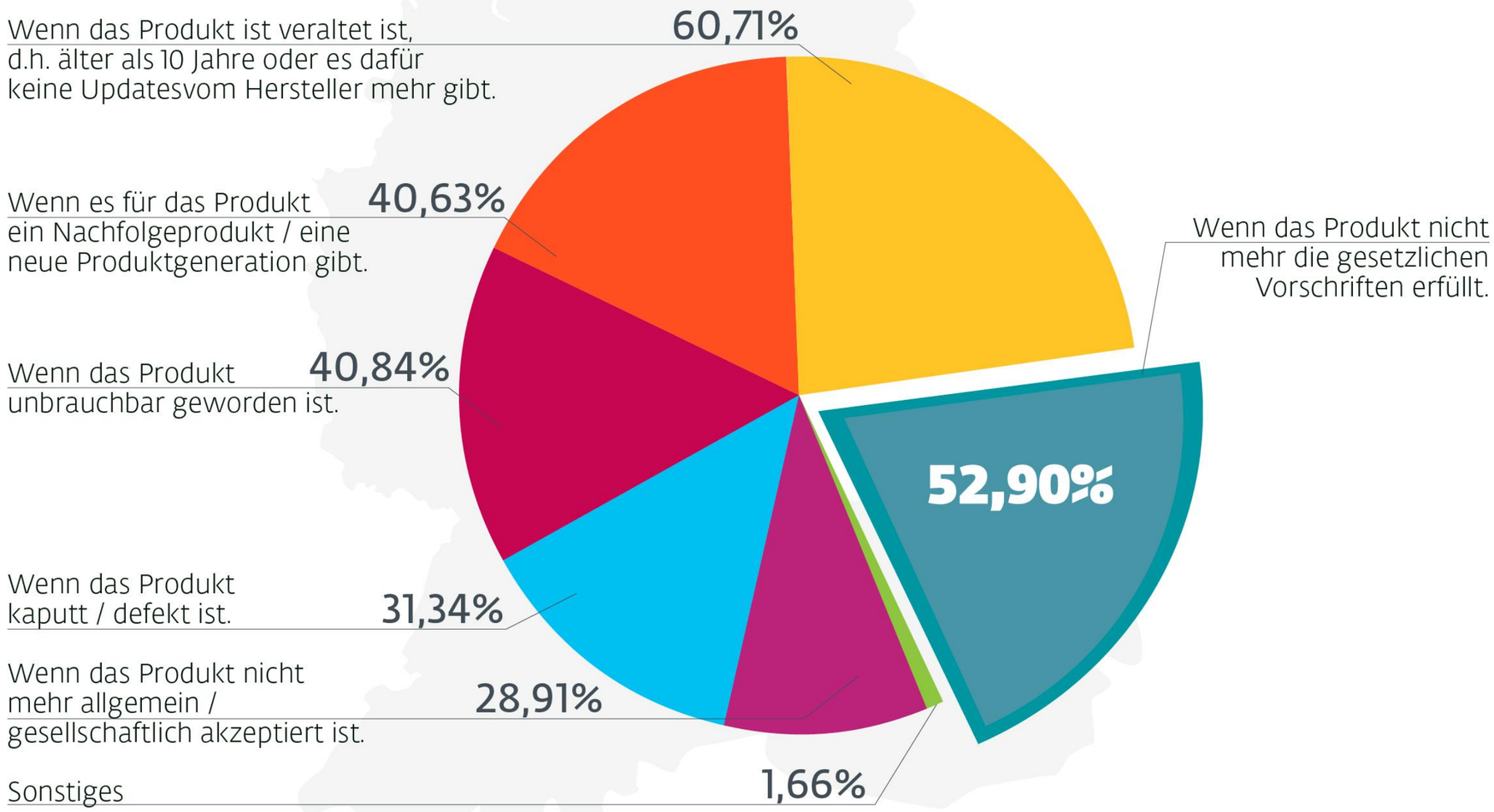
Digital Security
Progress. Protected.

Können Sie erklären, was mit dem Begriff "Stand der Technik" im Bereich IT-Sicherheit gemeint ist?



ESET Umfrage: 982 Befragte, Befragungszeitraum: April 2023

Wann erfüllt Ihrer Meinung nach ein IT-Produkt nicht mehr den "Stand der Technik"?



ESET Umfrage: 982 Befragte, Befragungszeitraum: April 2023

*„Unter Berücksichtigung des Stands der Technik, der **Implementierungskosten** und der Art, des Umfangs, der Umstände und der **Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen, treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um **ein dem Risiko angemessenes Schutzniveau zu gewährleisten**."*

(Art. 32 DSGVO)

*„…ein **gängiger juristischer Begriff**. Die technische Entwicklung ist schneller als die Gesetzgebung… seit vielen Jahren bewährt, in Gesetzen auf den "Stand der Technik" abzustellen, statt zu versuchen, konkrete technische Anforderungen bereits im Gesetz festzulegen. Was **zu einem bestimmten Zeitpunkt "Stand der Technik" ist**, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards und Normen von beispielsweise **DIN, ISO, DKE oder ISO/IEC** oder anhand erfolgreich **in der Praxis erprobter Vorbilder** für den jeweiligen Bereich ermitteln. Da sich die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung unterscheiden können, ist es **nicht möglich**, den "Stand der Technik" **allgemeingültig und abschließend zu beschreiben.***

(Quelle BSI)

Allgemeines Verständnis

Abbildung 1 - Drei-Stufen-Theorie (Quelle: BVerfGE, 49, 89 [135 f])
Grafikquelle: TeleTrust Handreichung

Welche Schutzziele werden durch die Maßnahmen abgedeckt?

- ☐ Verfügbarkeit
- ☑ Integrität
- ☑ Vertraulichkeit
- ☑ Authentizität

SdWF - Stand der Wissenschaft und Forschung
SdT - Stand der Technik
aaRT - allgemein anerkannten Regeln der Technik

Einordung der Maßnahmen

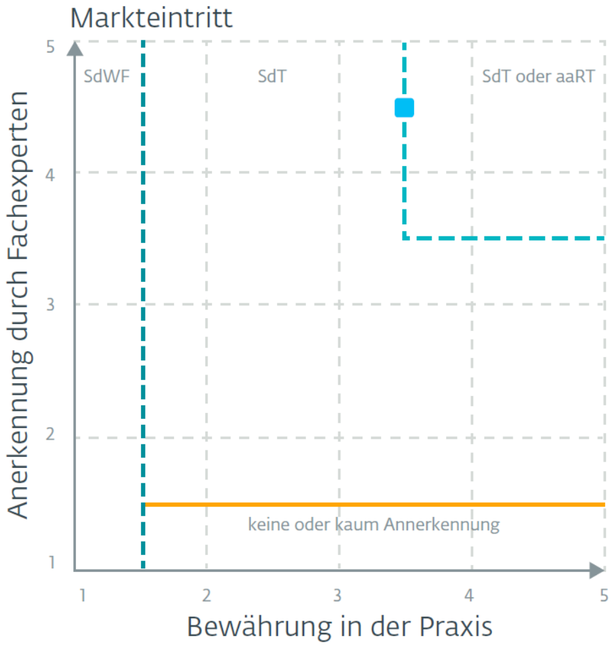


Abbildung 2 - Beispiel: Einordnung der Maßnahme Multi-Faktor-Authentifizierung | Grafikquelle: TeleTrust Handreichung

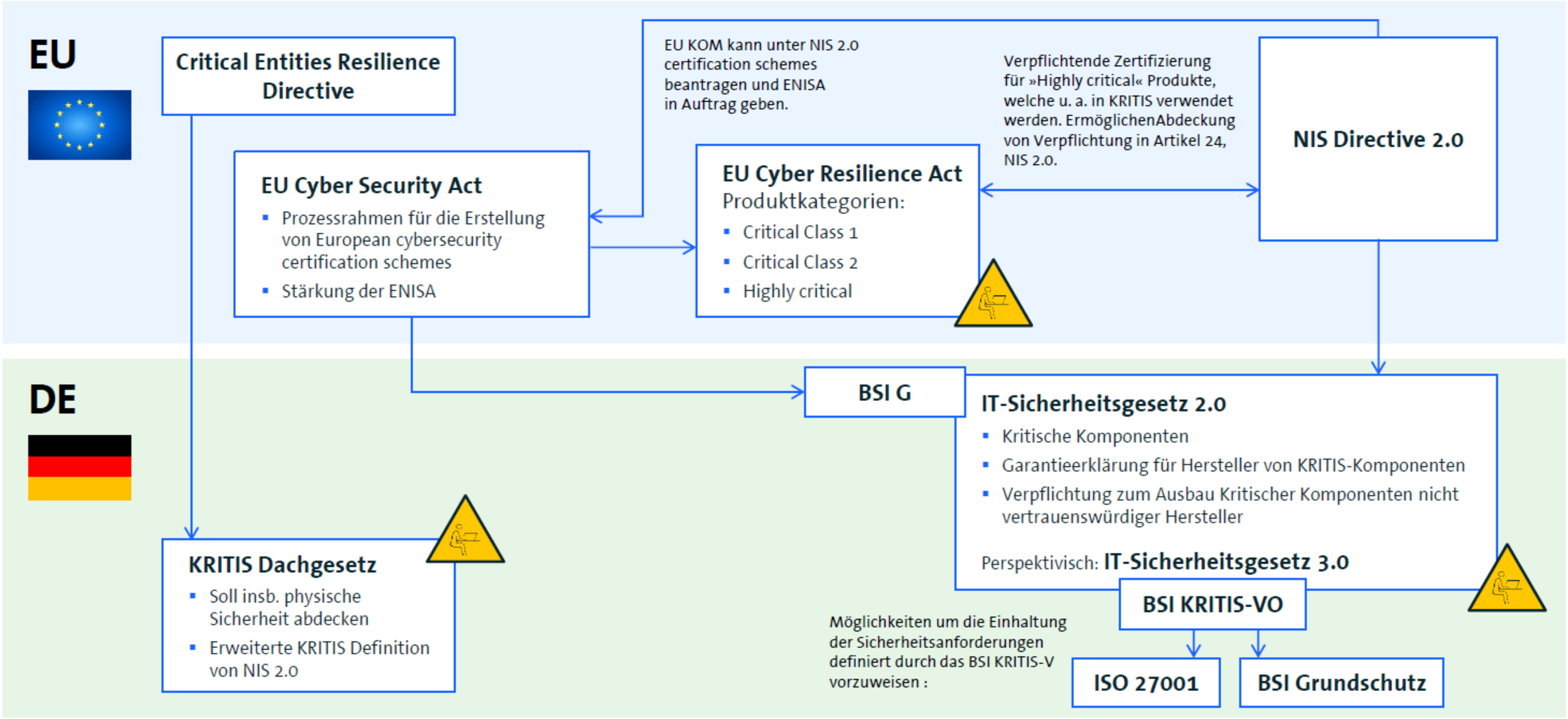
NIS 2 und die Reiter der Apokalypse ?

Digital Security
Progress. Protected.

„NIS 2.0 ist wie die DSGVO, nur viel krasser!“

(Richtlinie für Netzwerk und Informationssicherheit)

Legislative Interdependenz



bitkom

Einfluss und Rangfolge Europäischer Gesetzgebung

Wer ist direkt betroffen?

Sektoren nach Anhang I (wesentliche Einrichtungen)	Sektoren nach Anhang II (wichtige Einrichtungen)
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 wesentliche Einrichtungen

Große Betreiber aus elf Sektoren und Sonderfälle

B wichtige Einrichtungen

Große/Mittlere Betreiber aus sieben Sektoren

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

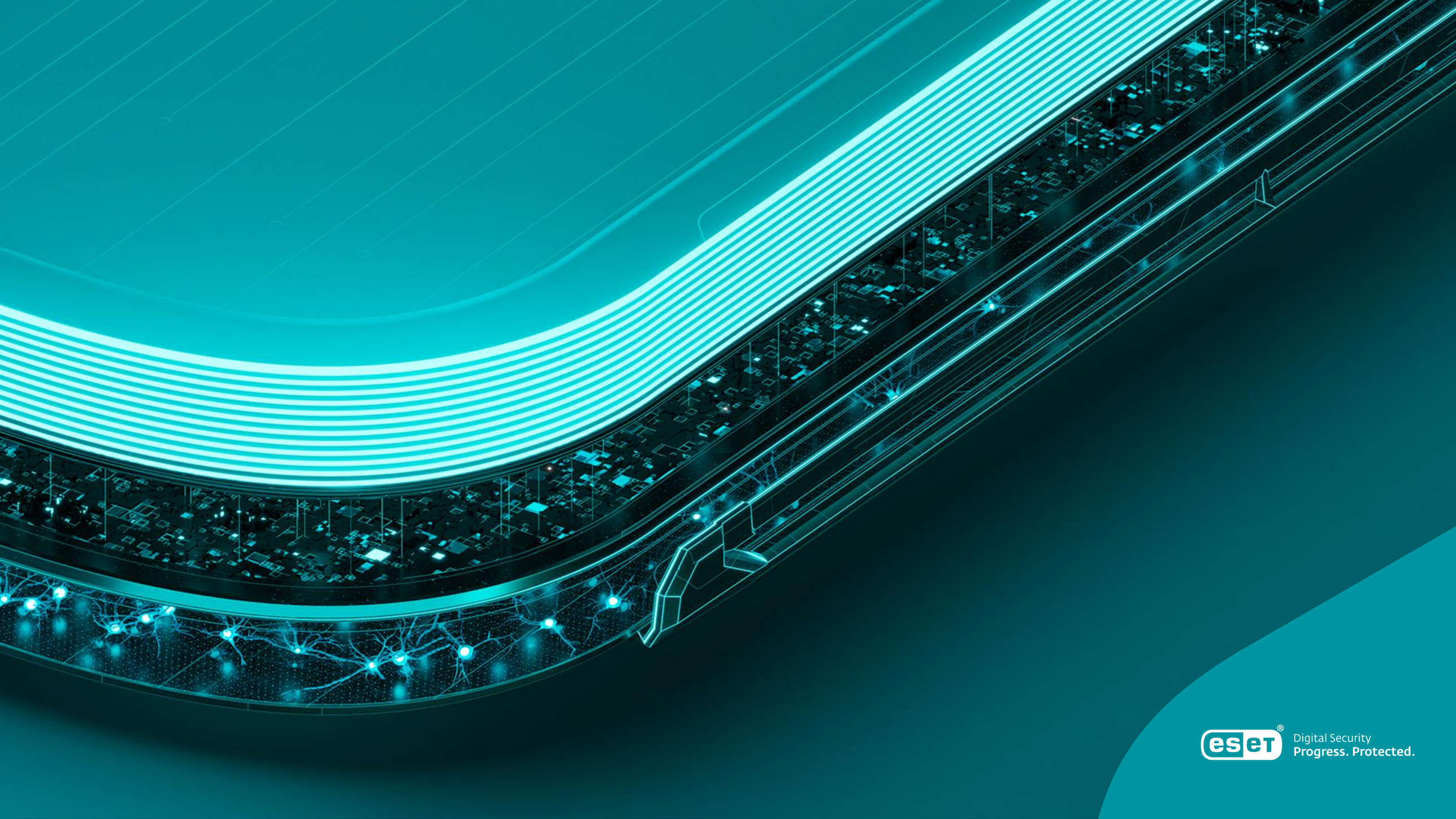
Qualifizierende Faktoren, z.B.:

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

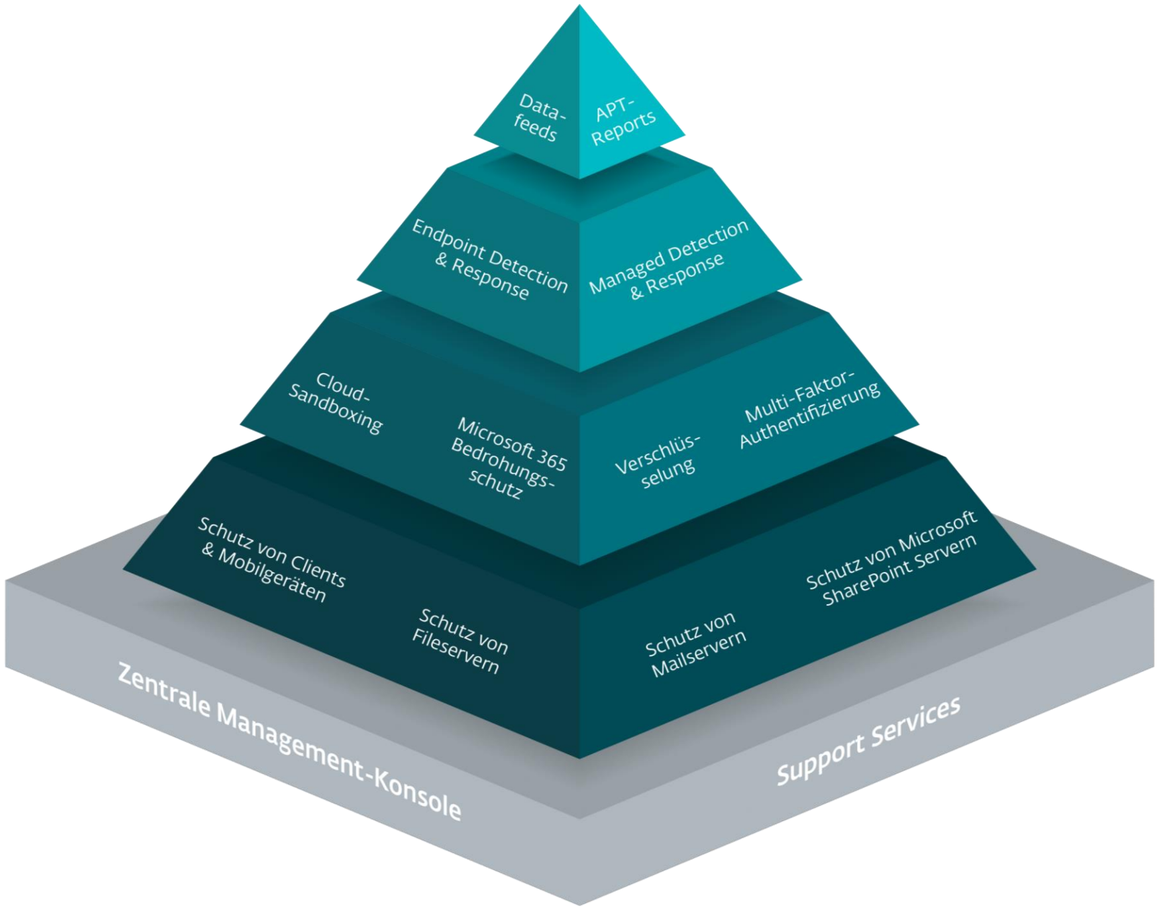
Direkt und Indirekt Betroffene Organisationen

„Die Anforderungen und Standards gelten im Zweifel im gleichen Maße für Dienstleister, Zulieferer… und zukünftig quasi für jeden der eine Cyberversicherung abschließen möchte!“

Woran soll ich mich orientieren?


eset
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“.

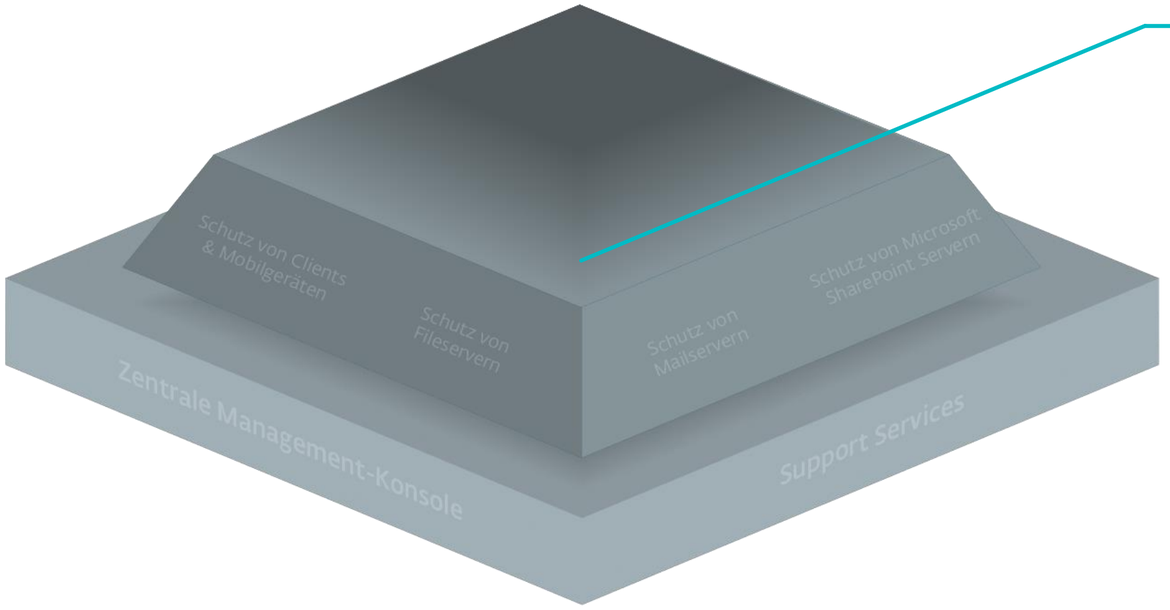
GRUNDSCHUTZ BASIS

Stufe 0:
Mindestabsicherung für Endgeräte und Server

Reifegrad der IT-Organisation:

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

GRUNDSCHUTZ PLUS

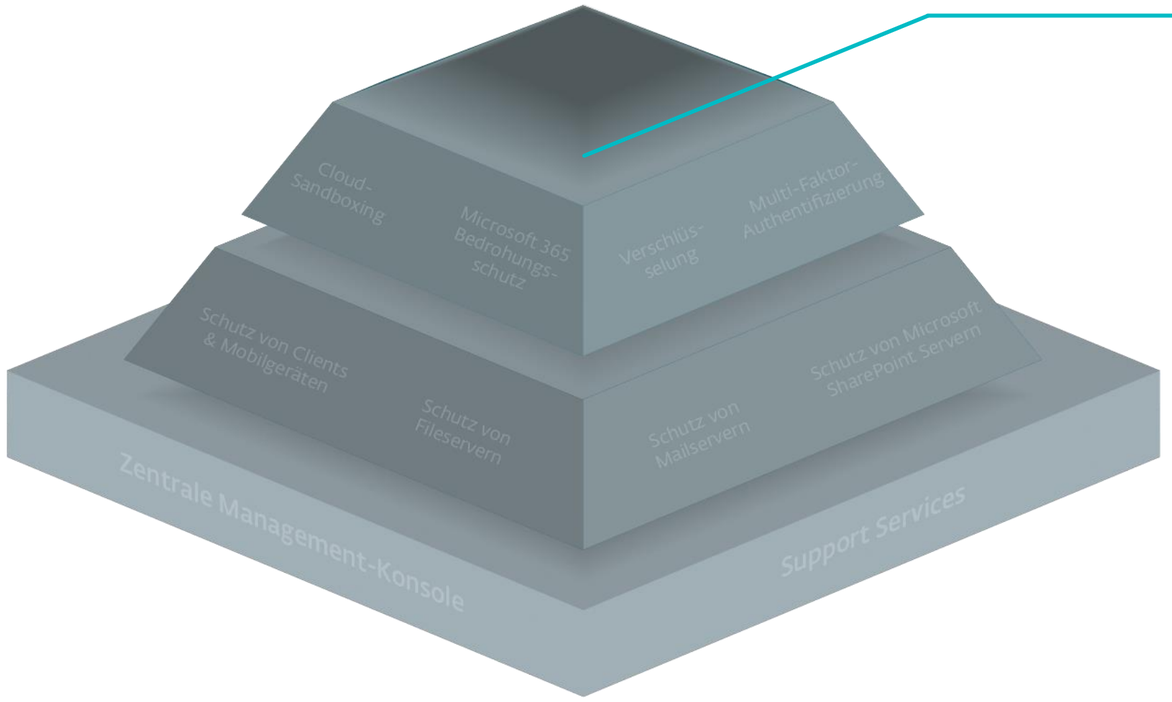


Stufe 1:
Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero-Days

Reifegrad der IT-Organisation:

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

GEFAHRENSUCHE UND ABWEHR - INNENSICHT

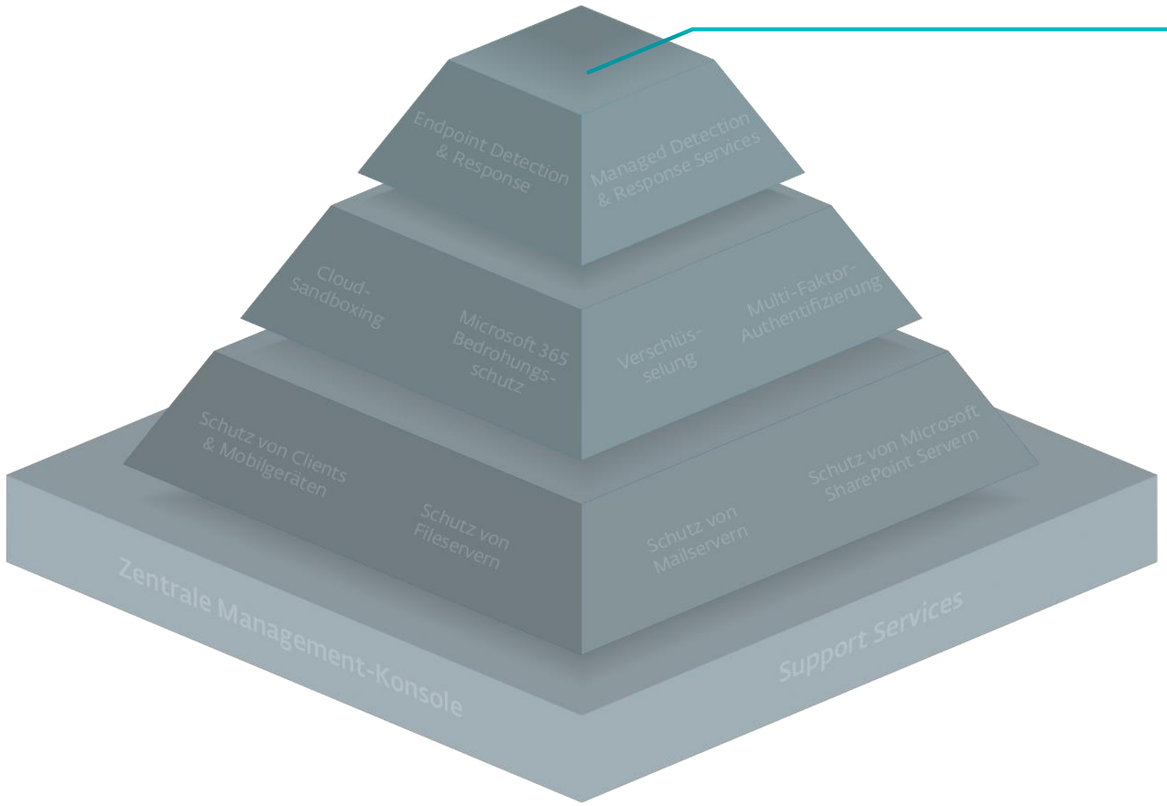


Stufe 2:
Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalie-Erkennung, Schwachstellen-analyse und Incident Management

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



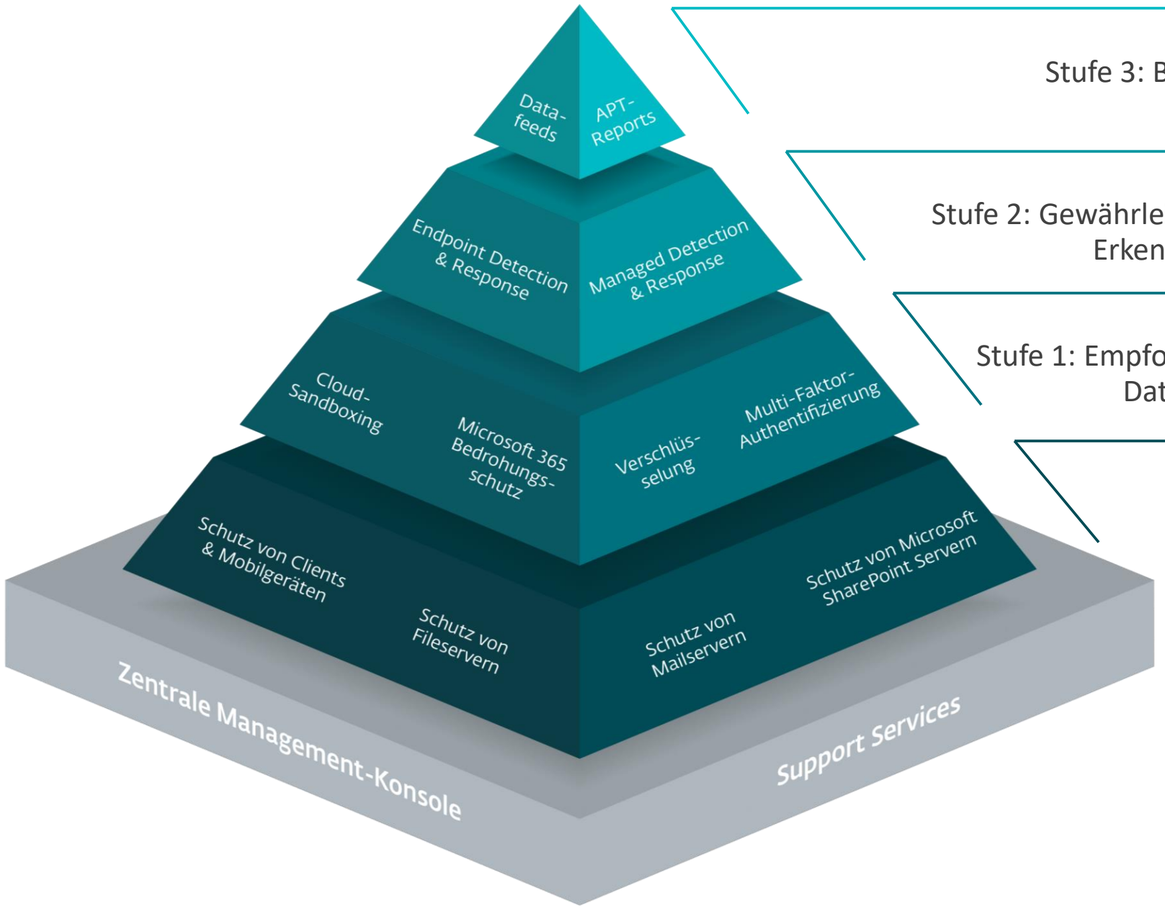
Stufe 3:
Bietet Einblicke in die globale Bedrohungsland-schaft als Grundlage für einen SOC-/SIEM-Betrieb

Reifegrad der IT-Organisation:

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

Zero-Trust-Security

EINSATZBEREICH



SCHUTZLEVEL

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

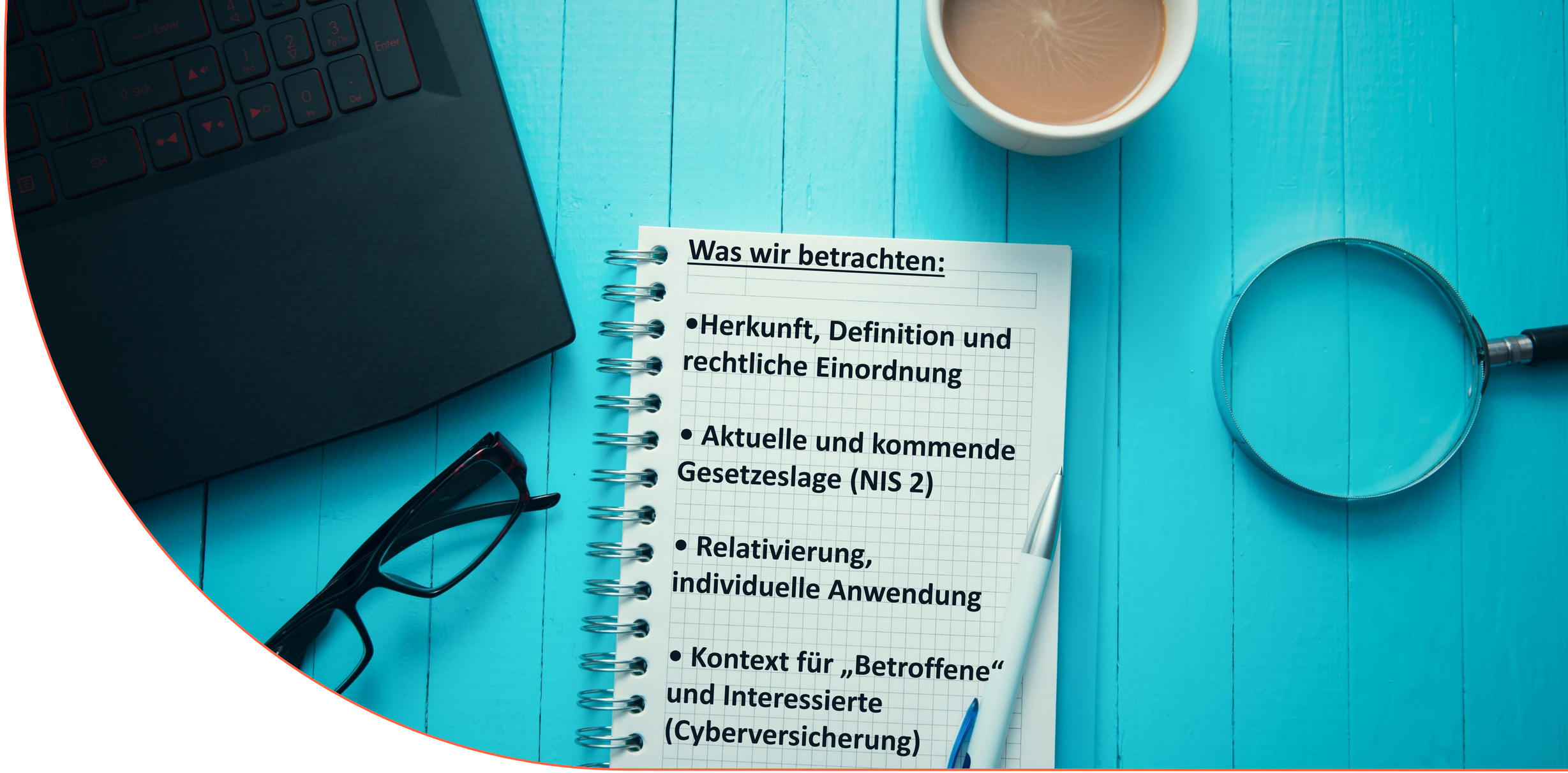
Zielgruppe:

CISOs
Geschäftsführer
Vorstände / Beiräte
Security-Verantwortliche

Eckdaten:

25 Seiten
5 Kapitel:

Herkunft & Definition
Cyberversicherungen
Anforderungen
Technische Maßnahmen
Handlungsempfehlungen


Was wir betrachten:
•Herkunft, Definition und rechtliche Einordnung
• Aktuelle und kommende Gesetzeslage (NIS 2)
• Relativierung, individuelle Anwendung
• Kontext für „Betroffene“ und Interessierte (Cyberversicherung)

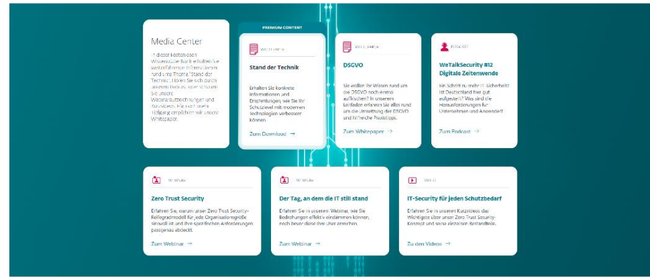
Landingpage:

www.eset.com/de/stand-der-technik

Content-Strecke:

Whitepaper mit Anmeldung (aktuellste Materialien)

DSGVO Leitfaden (Begleitmaterial)
Podcasts
Webinare
YouTube-Videos
Customer-Stories (Dokumente & Videos)



Digital Security
Progress. Protected.

Fragen?