

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



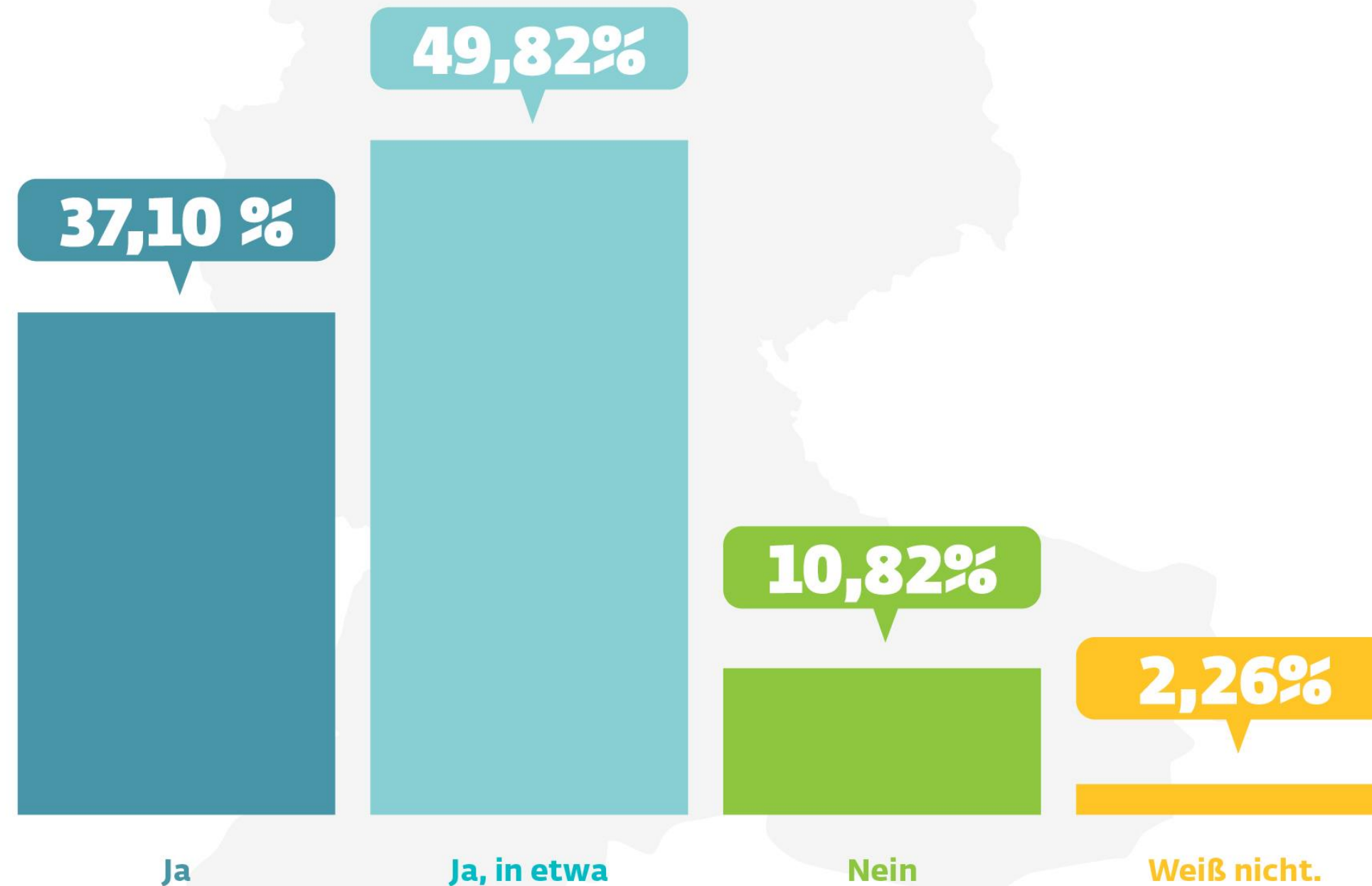
Wie war das doch gleich mit dem Stand der Technik?

**“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?



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

Wenn das Produkt ist veraltet ist,
d.h. älter als 10 Jahre oder es dafür
keine Updates vom Hersteller mehr gibt.

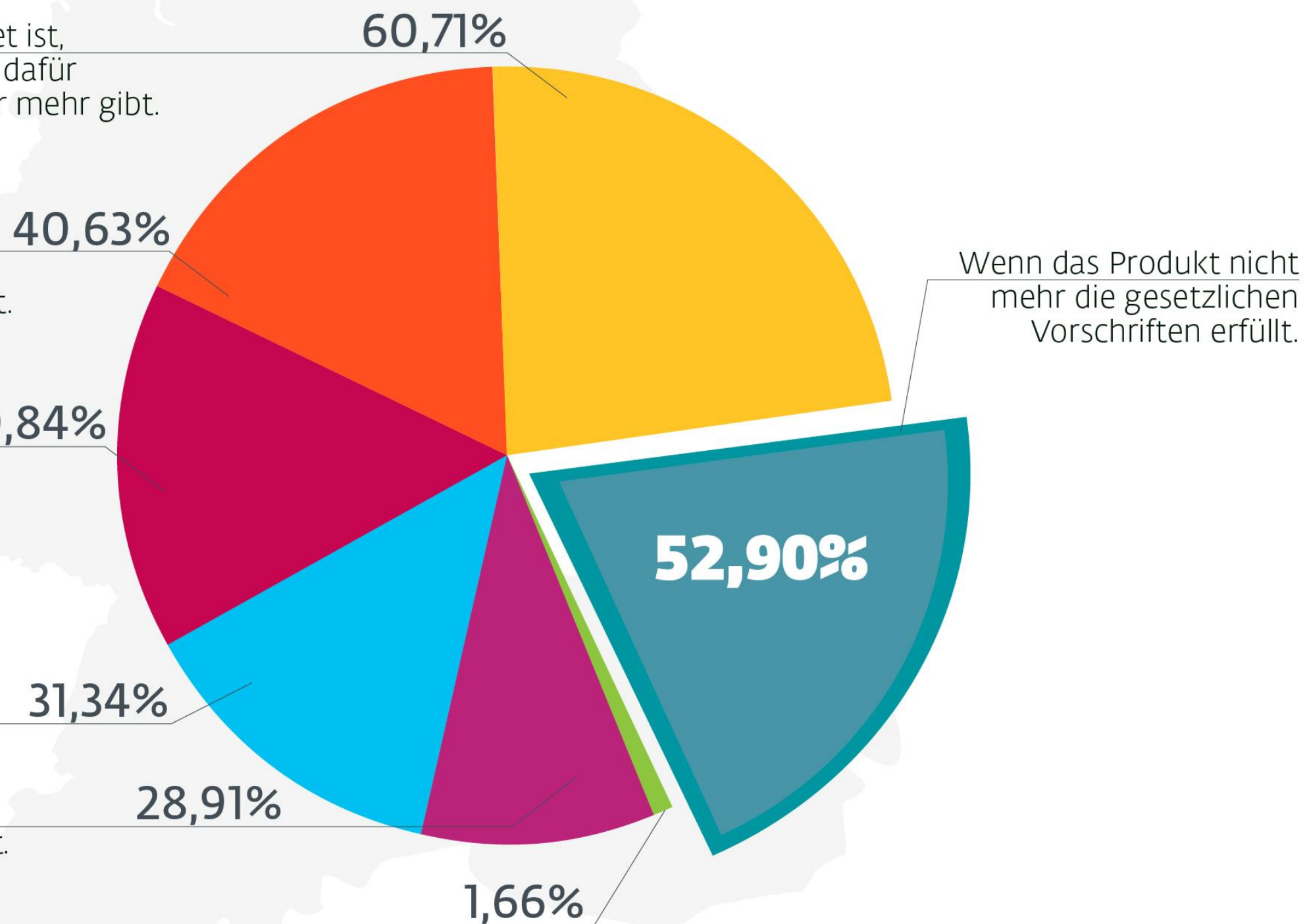
Wenn es für das Produkt
ein Nachfolgeprodukt / eine
neue Produktgeneration gibt.

Wenn das Produkt
unbrauchbar geworden ist.

Wenn das Produkt
kaputt / defekt ist.

Wenn das Produkt nicht
mehr allgemein /
gesellschaftlich akzeptiert ist.

Sonstiges



„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)

IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

Technische und organisatorische Maßnahmen

2021

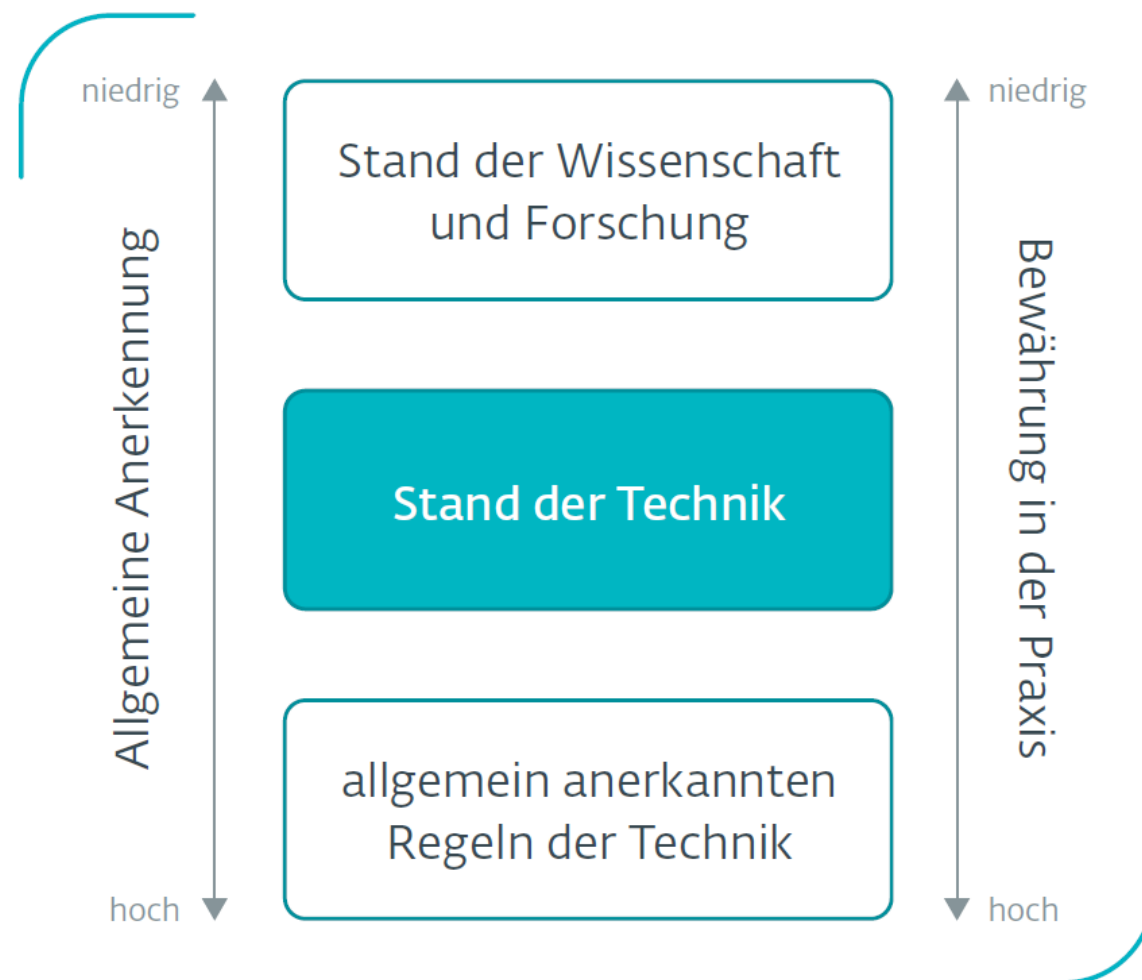


Abbildung 1 - Drei-Stufen-Theorie (Quelle: BVerfGE, 49, 89 [135 f])

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

Einordnung der Maßnahmen

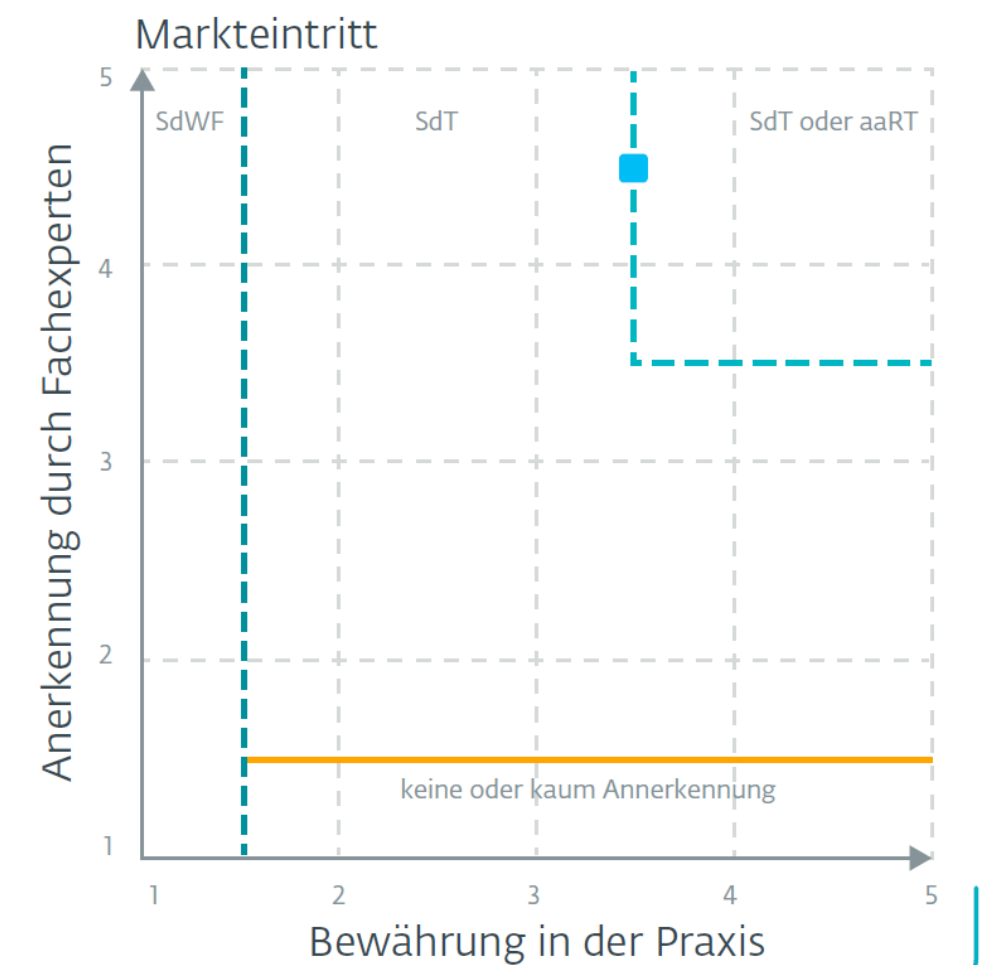


Abbildung 2 - Beispiel: Einordnung der Maßnahme Multi-Faktor-Authentifizierung | Grafikquelle: [TeleTrust Handreichung](#)

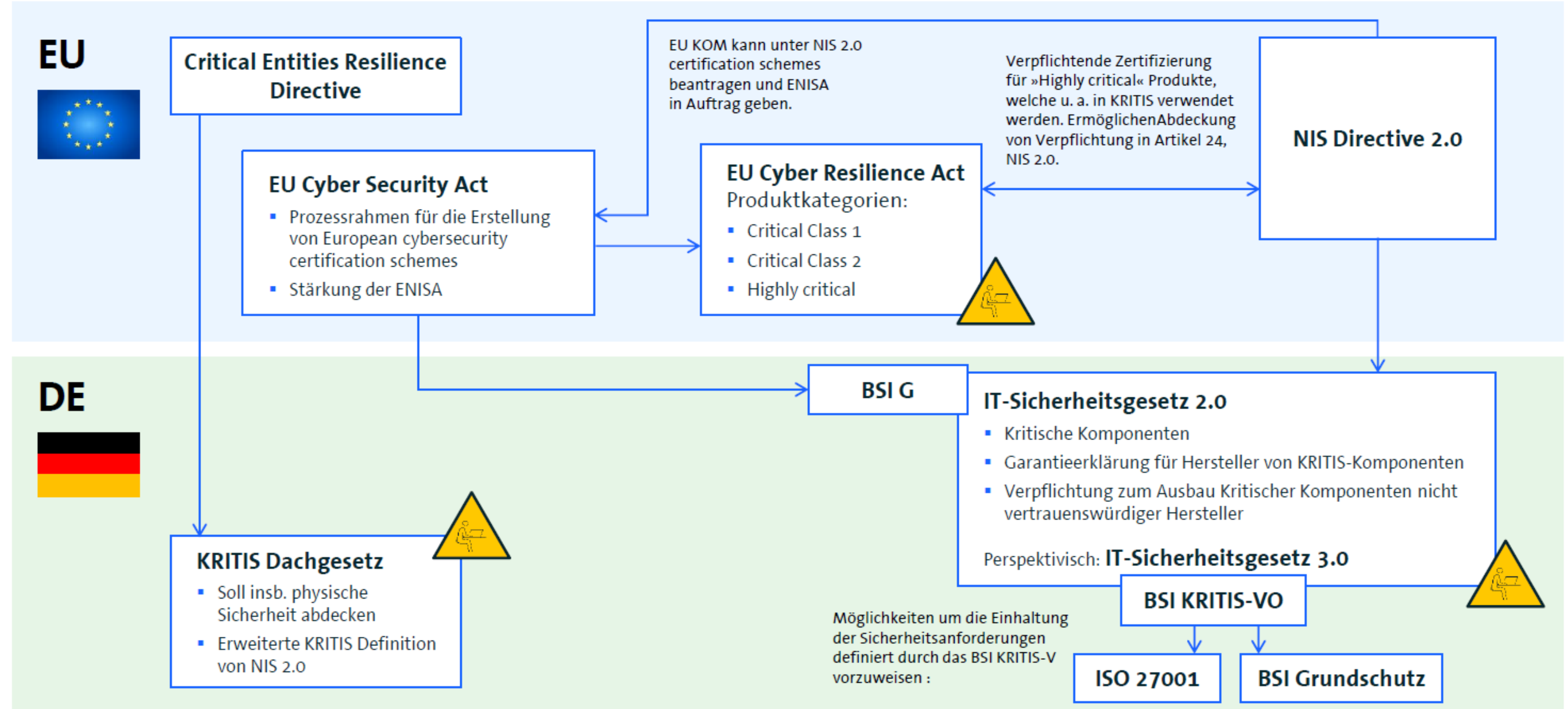
NIS 2 und die Reiter der Apokalypse ?



Digital Security
Progress. Protected.

„NIS 2.0 ist wie die DSGVO, nur viel krasser!“
(Richtlinie für Netzwerk und Informationssicherheit)

Legislative Interdependenz



Wer ist direkt
betroffen?

Sektoren nach Anhang I (wesentliche Einrichtungen)

Energie

Verkehr und Transport

Bankwesen

Finanzmärkte

Gesundheitswesen

Trinkwasser

Abwasser

Digitale Infrastruktur

ICT* Service Management (Managed Service Provider - MSP)

Öffentliche Verwaltung

Weltraum

Sektoren nach Anhang II (wichtige Einrichtungen)

Post- und Kurierdienste

Abfallwirtschaft

Produktion, Herstellung und Handel mit chemischen Stoffen

Produktion, Verarbeitung und Handel von Lebensmitteln

Verarbeitendes Gewerbe/Herstellung von Waren

Anbieter digitaler Dienste

Forschungseinrichtungen

A wesentliche Einrichtungen

Große Betreiber aus elf Sektoren und Sonderfälle

Mittlere Unternehmen

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

Große Unternehmen

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

B wichtige Einrichtungen

Große/Mittlere Betreiber aus sieben Sektoren

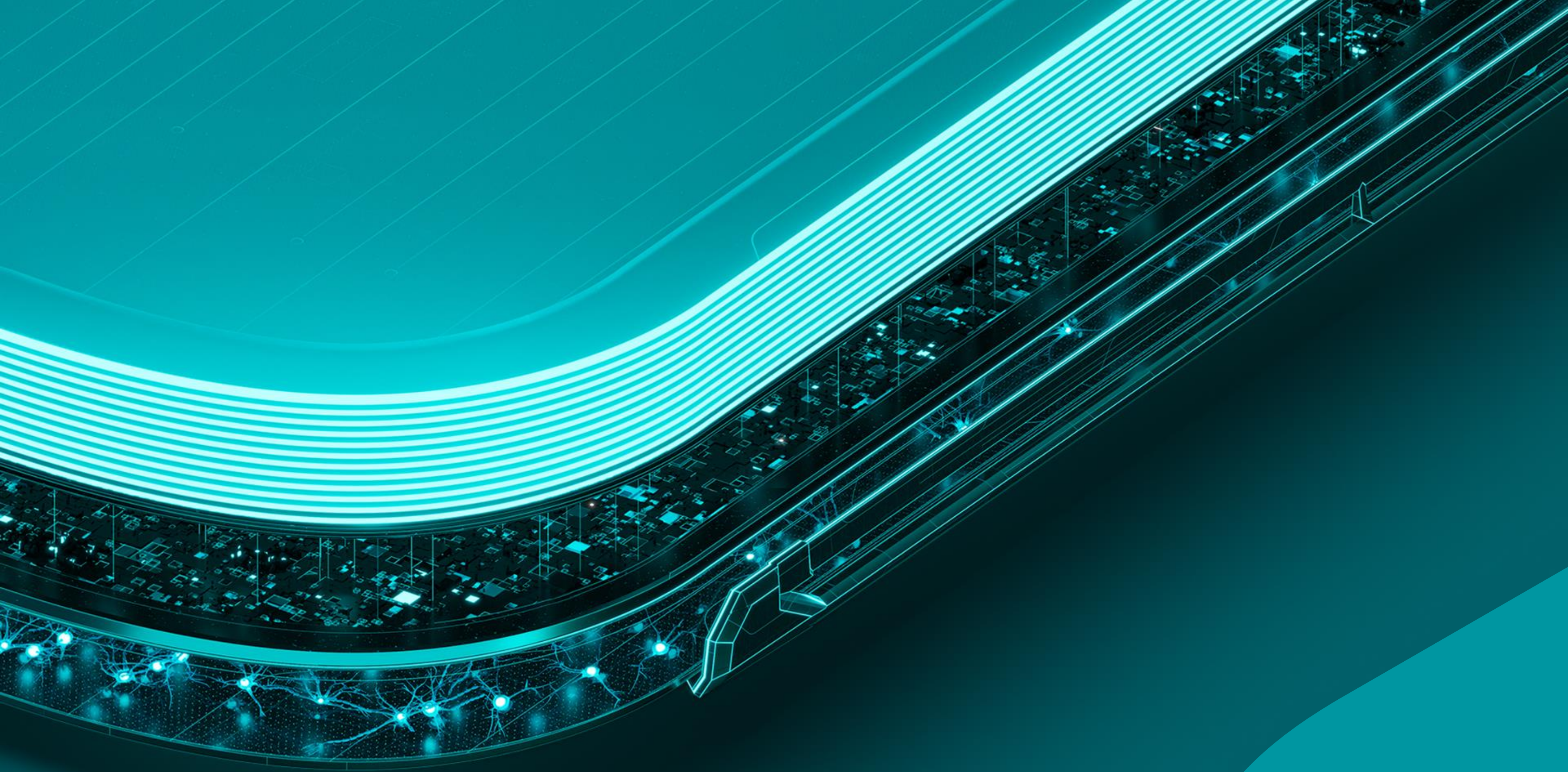
Unabhängig von Unternehmensgröße

- Qualifizierende Faktoren, z.B.:
- Kritische Tätigkeit
 - Systemrisiken
 - Auswirkung auf öffentliche Ordnung
 - Grenzüberschreitende Auswirkungen

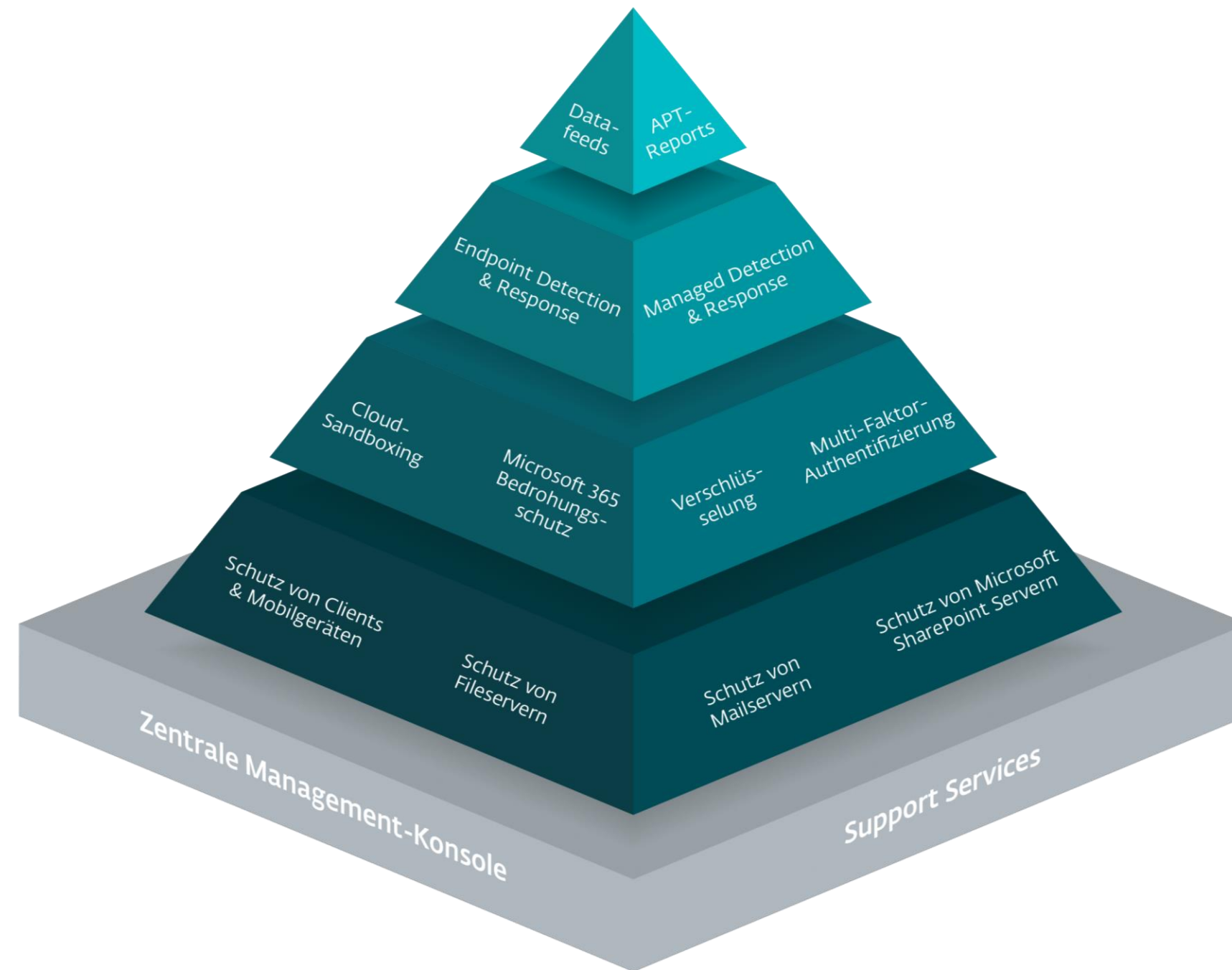
„Die Anforderungen und Standards gelten im Zweifel im gleichen Maße für Dienstleister, Zulieferer... und zukünftig quasi für jeden der eine Cyberversicherung abschließen möchte!“

**Woran soll ich
mich orientieren?**





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

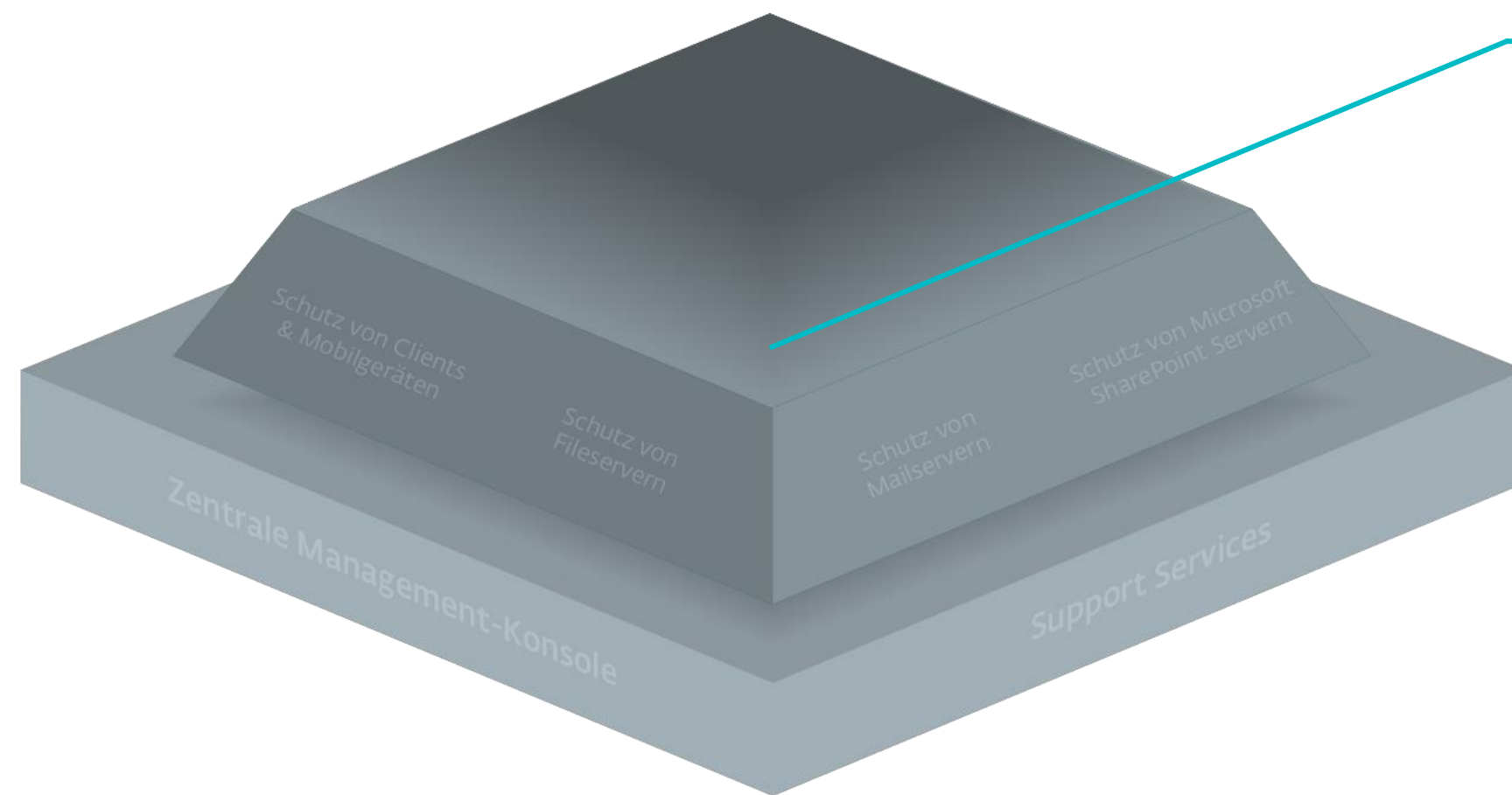
Stufe 0: Mindestabsicherung für Endgeräte und Server

Reifegrad der IT-Organisation:

 Zentrales Management
(Cloud oder On-Prem)

 Policies und Regeln für die
Geräte- und Internetnutzung

GRUNDSCHUTZ PLUS



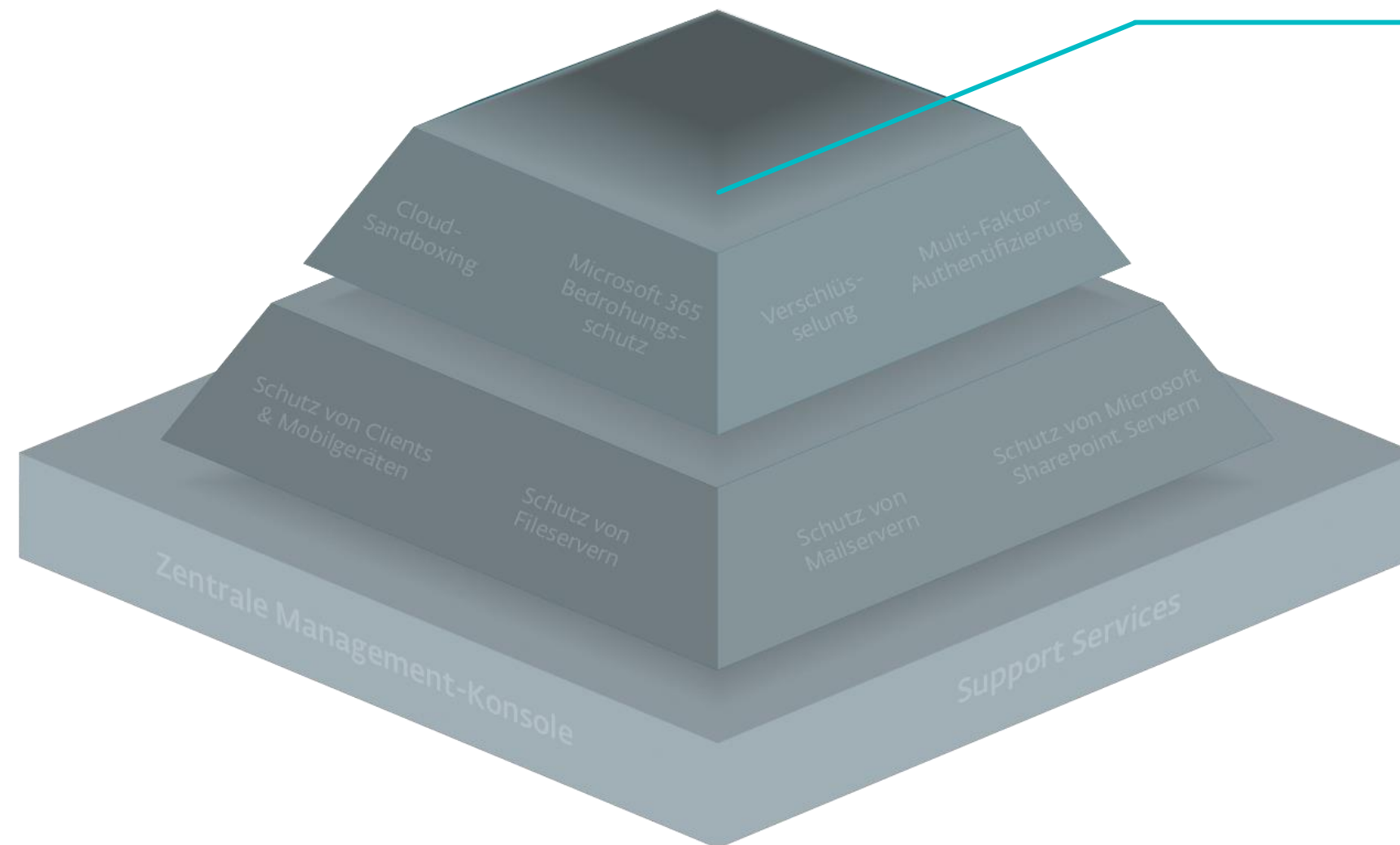
Stufe 1:

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



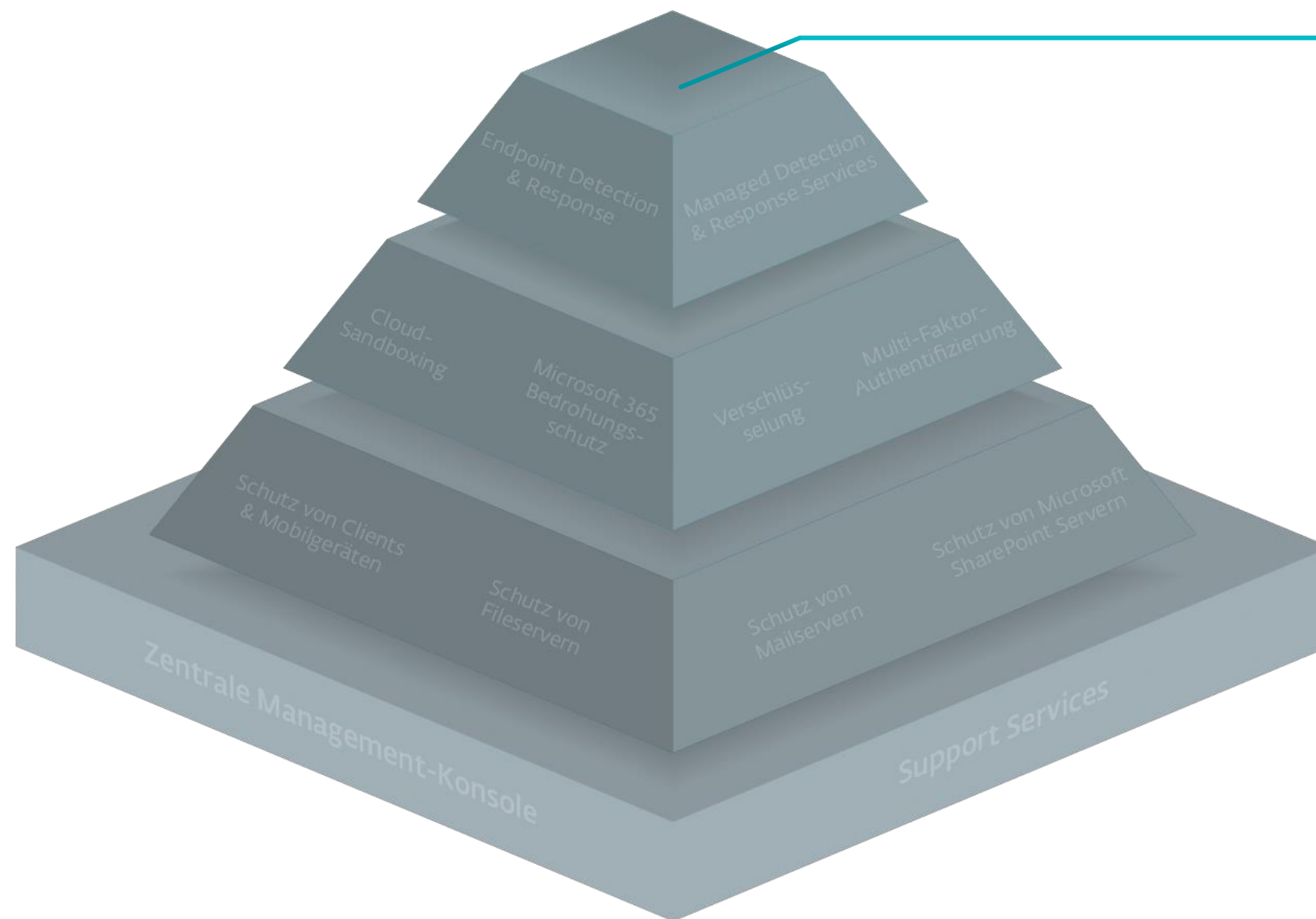
Stufe 2:

Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalie-Erkennung, Schwachstellenanalyse 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



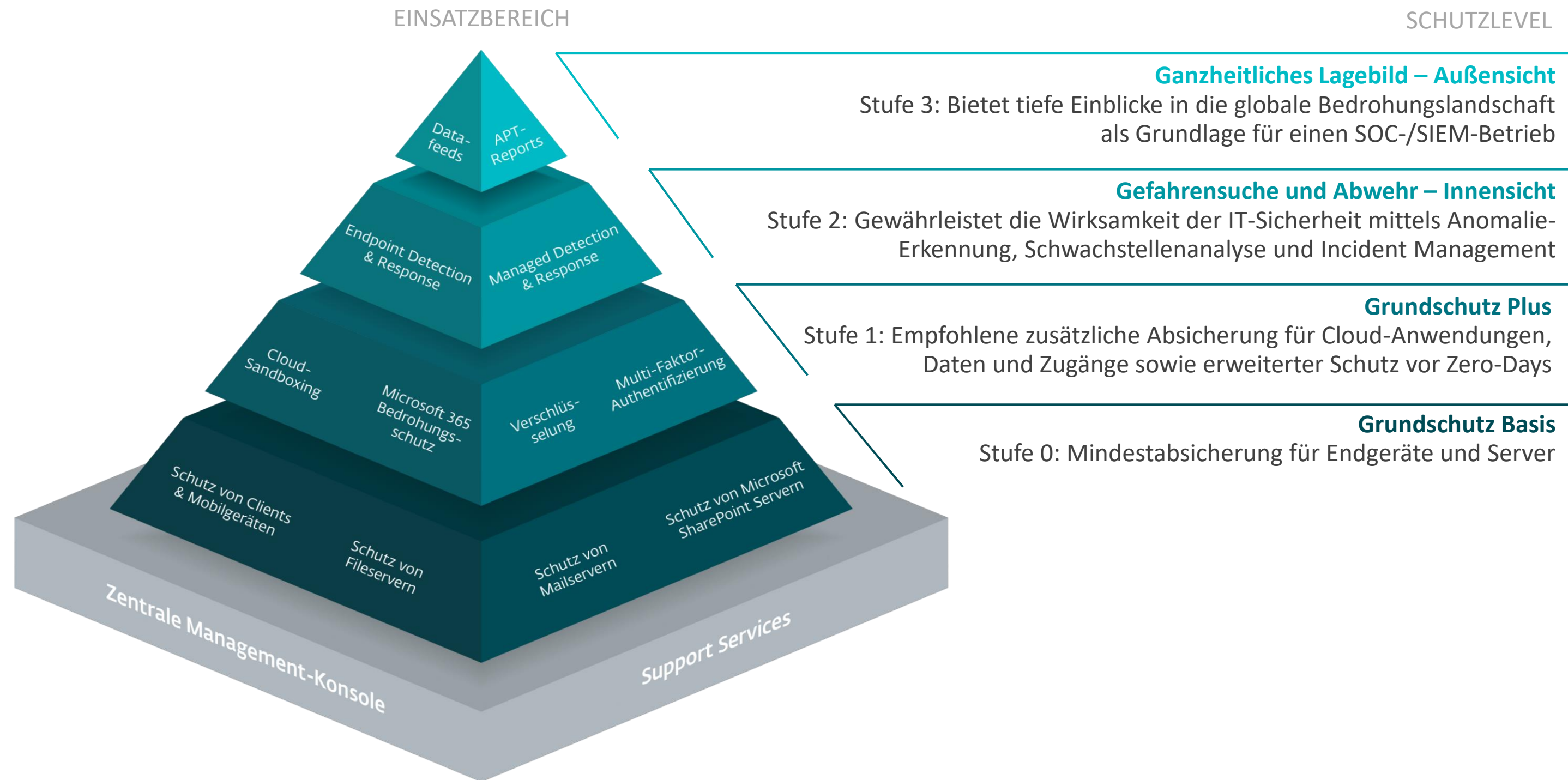
Stufe 3:

Bietet Einblicke in die globale Bedrohungslandschaft 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





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)



Zusammen bringen wir Ihre IT-Sicherheit auf den Stand der Technik.

Haben Sie eine Vorstellung davon, welche Lösungen sie einsetzen müssen, um bei Ihrer IT-Sicherheit up to date zu sein? Oder anders um: Wissen Sie, wann ein Produkt nicht mehr dem Stand der Technik entspricht?

Diese Frage ist nicht nur für persönliche Einschätzungen von IT-Security-Lösungen interessant, sondern vor allem auch im Kontext von Cyberversicherungen oder gesetzlichen Regelungen. Aber selbst hier sind die vage Formulierungen vom "Stand der Technik" häufig nicht weiter kodifiziert. Kein Wunder, gerade in der IT verändern sich Software & Co. schneller als Gaseisbae entstehen. Bisher: allgemein anerkannte Verfahren und IT-Security-Technologien können auf einen nicht mehr ausreichen, um spezifischen Anforderungen zu entsprechen oder den sich verändernden Sicherheitsanforderungen zu genügen.

Wir betriebsinterne als Unternehmen oder Organisation personenbezogene Daten verarbeitet, muss angemessene Schutzmaßnahmen ergreifen, um auf dem Stand der Technik zu sein. Ansonsten würden rechtliche und technische Anforderungen an IT-Sicherheit und Datenschutz nicht im ausreichenden Maße erfüllt.

[Chat stream](#)

Jetzt das aktuelle Whitepaper zum Stand der Technik herunterladen

Das kostenlose ESET-Whitepaper bietet Ihnen als Unternehmen, IT-Security-Menschenfächer und Dienstleister unabhängig von Branche und Größe konkrete Informationen und Empfehlungen, wie Sie up to date bleiben und Ihr Schutzniveau mit modernen Technologien verbessern können. Nicht zuletzt fällt Ihnen das auch beim Thema Cyberversicherung, da die Anbieter mittlerweile hohe Anforderungen an die IT-Sicherheit der Versicherungsnehmer stellen.

Durch Absenden dieses Formulars erklären Sie sich damit einverstanden, von der ESET Deutschland GmbH regelmäßig e-Mails zu IT-Security-Themen, Updates über ESET-Lösungen, Dienstleistungen, Webinars und Veranstaltungen zu erhalten. Sie können diese Benachrichtigungen jederzeit abbestellen. Sie bestätigen gleichzeitig, dass Sie die Bestimmungen der Datenschutzerklärung zur Kenntnis genommen haben.

DOWNLOAD WHITEPAPER

Media Center

IT-Security-News, Experteninterviews, Webinare, Podcasts und mehr. Alles rund um IT-Security. Hier finden Sie alle aktuellen Informationen und Analysen. Sie sind immer auf dem neuesten Stand der IT-Security.

Stand der Technik

Erhalten Sie konkrete Informationen und Empfehlungen, wie Sie Ihr Schutzniveau mit modernen Technologien verbessern können.

DSGVO

Wie stellen Sie sicher, dass Ihre IT-Security up to date ist? In unserem Leitfaden erfahren Sie alles rund um die Umsetzung der DSGVO und IT-Security.

WebTalkSecurity #12: Digitale Zeitenwende

Wie sieht es mit IT-Sicherheit in Deutschland aus? Wie wird die Digitalisierung die IT-Security beeinflussen? Was sind die Herausforderungen für Unternehmen und Anwender?

Zero Trust Security

Erfahren Sie, warum Zero Trust Security ein zentraler Bestandteil für die Cyberabwehr ist und wie Sie Ihre spezifischen Anforderungen integrieren können.

Der Tag, an dem die IT still stand

Erfahren Sie in unserem Webinar, wie Sie Ausfälle vermeiden können, noch bevor diese Ihre IT erreichen.

IT-Security für jeden Schutzbedarf

Erfahren Sie in unserem Katalog, die richtigen IT-Security-Lösungen für Ihre IT-Security-Anforderungen und wie Sie diese integrieren können.

Eishockey-Cracks des ERC Ingolstadt verstärken ihre digitale Defense

Der Deutsche Meister von 2014 setzt bei der Abwehr von Cyber-Angriffen und der Absicherung seiner IT-Infrastruktur auf ESET Active Security.

Borussia Dortmund geht in puncto IT-Sicherheit keine Kompromisse ein

Als Schachmatt der Cyber-Sicherheit ist ESET die globale IT-Security-Lösung. Damit die Borussia die IT-Sicherheit auf ESET Active Security.

IT-Sicherheit auf Rezept

IT-Sicherheit ist die wichtigste Voraussetzung für den Erfolg eines Unternehmens. ESET ist die globale IT-Security-Lösung.

Sie wollen weitere Informationen oder haben Fragen zum Thema "Stand der Technik"?

KONTAKTIEREN SIE UNS



© 2024 ESET, spol. s r.o. Všechna práva vyhrazena.



Fragen?