NIS2-Umsetzung – Status Quo

Aktuelles zur Umsetzung der NIS2-Richtlinie in Deutschland, Update Februar 2025

Digital Security
Progress. Protected.

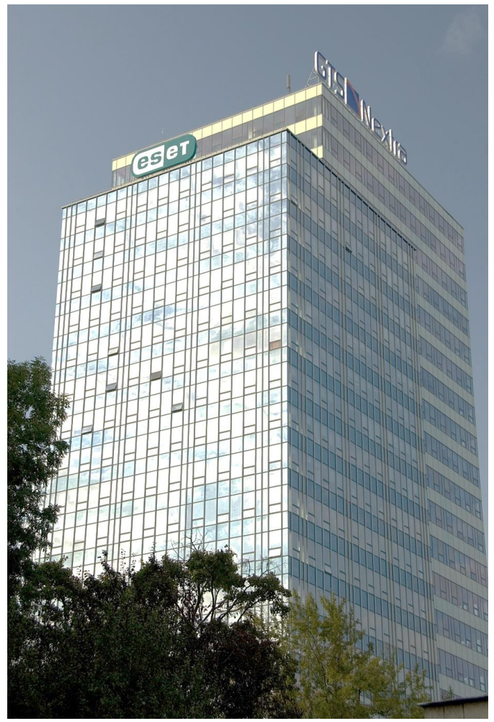
Maik Wetzel

Strategic Business Development Director DACH
- ESET Deutschland GmbH -

Digital Security
Progress. Protected.

Vorstellung

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

Digital Security
Progress. Protected.

Agenda

1. Status Quo
2. Ziele von NIS 2.0
3. Was ist neu?
4. Wer ist von NIS 2.0 betroffen?
5. Nationale Umsetzung in Deutschland
6. Handlungsempfehlung
7. Stand der Technik / Compliance
8. Q&A

Warum NIS2??

Digital Security
Progress. Protected.

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

Selbstregulierung des Marktes

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

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)

Maßnahmen §30 NIS2UmsuCG - Regierungsentwurf

Risikomanagementmaßnahmen :

- müssen auf einem gefahrenübergreifenden Ansatz beruhen,
- dem bestehenden (festgestellten) Risiko angemessen sein (geeignet, verhältnismäßig, wirksam),
- sollen den Stand der Technik einhalten unter Berücksichtigung der einschlägigen europäischen und internationalen Normen und zumindest Folgendes umfassen:

1. Konzepte für Risikoanalyse und Sicherheit für Informationssysteme
2. Bewältigung von Sicherheitsvorfällen
3. Aufrechterhaltung des Betriebs, wie Backup-Management, Wiederherstellung nach einem Notfall und Krisenmanagement
4. Sicherheit der Lieferkette
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
10. Verwendung Multi-Faktor-Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme

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 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 (?)

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

Hilfe, bin ich betroffen?

1. BSI – NIS2-Betroffenheitsprüfung:

   https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html

2. Anlagen 1+2 Nis2UmsuCG
3. NACE-Code, Klassifikation der Wirtschaftszweige

   https://nacecode.de/

Nationale Umsetzung

Digital Security
Progress. Protected.

Zeitplanung	
1., 2. und 3. geleakter Referentenentwurf	1. HJ 2024
4. Referentenentwurf	24.06.2024
Länder und Verbändebeteiligung	
Kabinettbeschluss / 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	Expertenanhörung: 04.11.2024
Bruch der Ampel	07.11.2024
Versuche für Kompromisslösungen	29.11.2024 „Formulierungshilfe der Bundesregierung“
Diskontinuitätsprinzip greift!	Realistischer Termin für NIS2UmsuCG: Ende 2025

Kritikpunkte Referentenentwurf

- Rolle BSI
- CISO für Bundeseinrichtungen
- Umsetzung für Staat und Verwaltung (Ausnahmen bei Bundeseinrichtungen)
- Umgang mit Schwachstellen
- §9b BSIG wird zu §41 NIS2UmsuCG – Untersagung kritischer Komponenten – hat bisher zu langen, komplizierten Verfahren und vielen Fragen geführt, gilt nun für viel mehr betroffene Unternehmen, Lerneffekt nicht erkennbar
- Sicherheitsüberprüfungen des sicherheitsrelevanten Personals (z.B. Admins) betroffener Unternehmen durch staatliche Stellen nicht vorgesehen
- Gravierende Defizite der (deutschen) Cybersicherheitsarchitektur bleiben bestehen
- …

Entwurf EU-NIS2-Durchführungsverordnung

- betrifft fast alle Einrichtungsarten der regulierten Sektoren „Digitale Infrastruktur“ und „Anbieter digitaler Dienste“

  Vertrauensdiensteanbieter, Social-Media-Plattformen, Online-Suchmaschinen, Online-Marktplätze**, Managed Service und Managed Security Service Provider**, Cloud- und Rechenzentrumsanbieter sowie DNS-Diensteanbieter, TLD-Namenregister und Content Delivery Networks

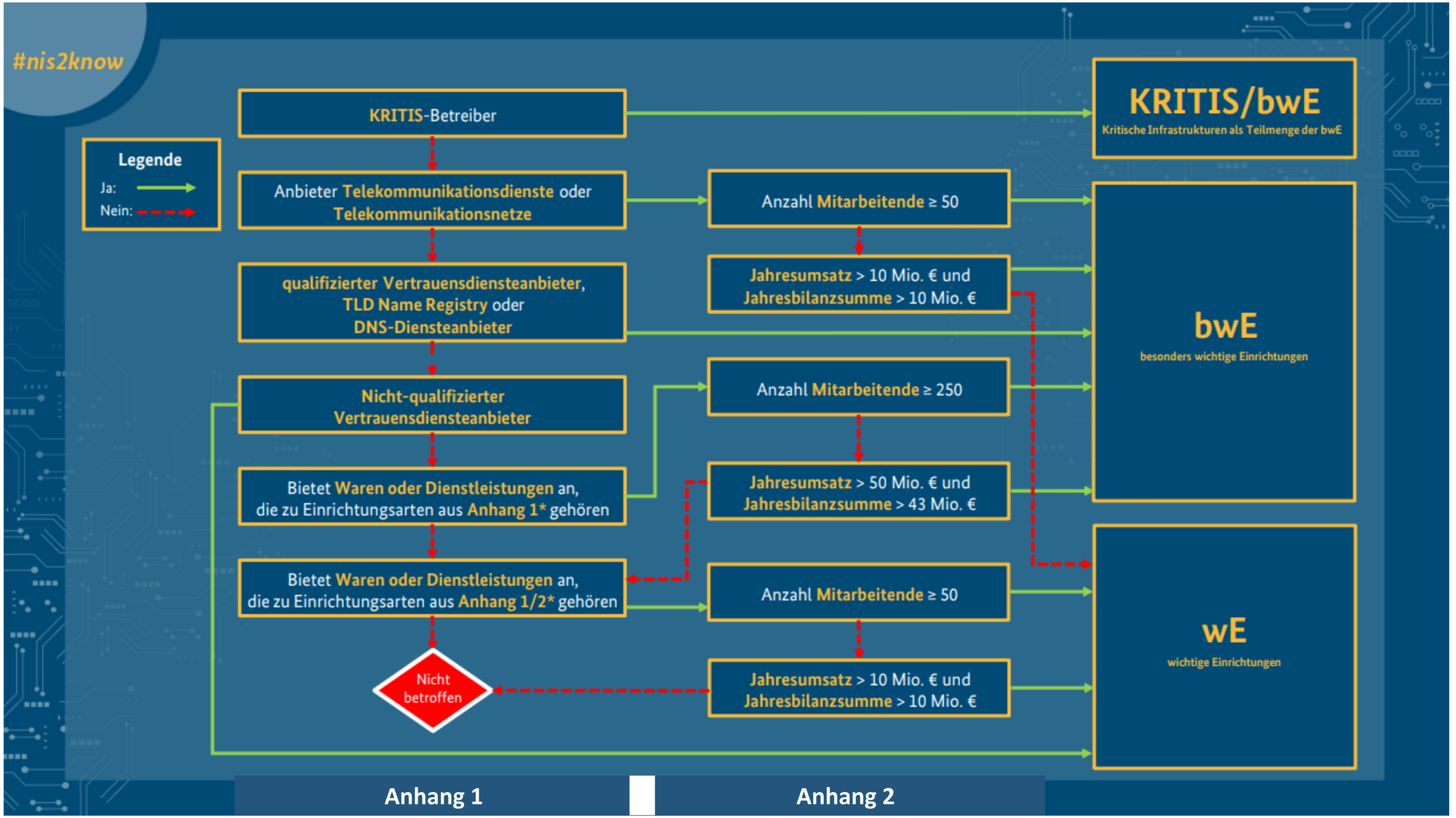
- legt Kriterien fest zu signifikanten (meldepflichtigen) Sicherheitsvorfällen, z.B.
  - Betriebsunterbrechung, Ausfall von Diensten, Wiederholung
  - Reputationsschäden
  - Schäden an Gesundheit/Versehrtheit oder Tod
  - Finanzieller Verlust
- Für andere Sektoren kann EU ähnliche Verordnungen erlassen (außerdem Ermächtigung dazu im NIS2UmsuGG für BMI)
- Sicherheits- und Risikomanagementanforderungen „ausformuliert“ (Policies, Technologie, etc.)
- Gilt ab 18.10. (bzw. mit Inkrafttreten der Umsetzungsgesetzgebung)

Handlungsempfehlung

Digital Security
Progress. Protected.

Betroffenheit prüfen

BSI-Betroffenheitsprüfung



ISMS & Co.

- 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 - Beispiele

- 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

- Dem festgestellten Risiko angemessene Sicherheitsmaßnahmen implementieren.
- umfasst sowohl technische als auch organisatorische Maßnahmen

Melde- und Unterrichtspflichten beachten

Zuständigkeiten für Meldepflichten festlegen und Erfüllung sicherstellen (24x7!)

- 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

Zuständigkeiten für Unterrichtspflichten festlegen und Erfüllung sicherstellen

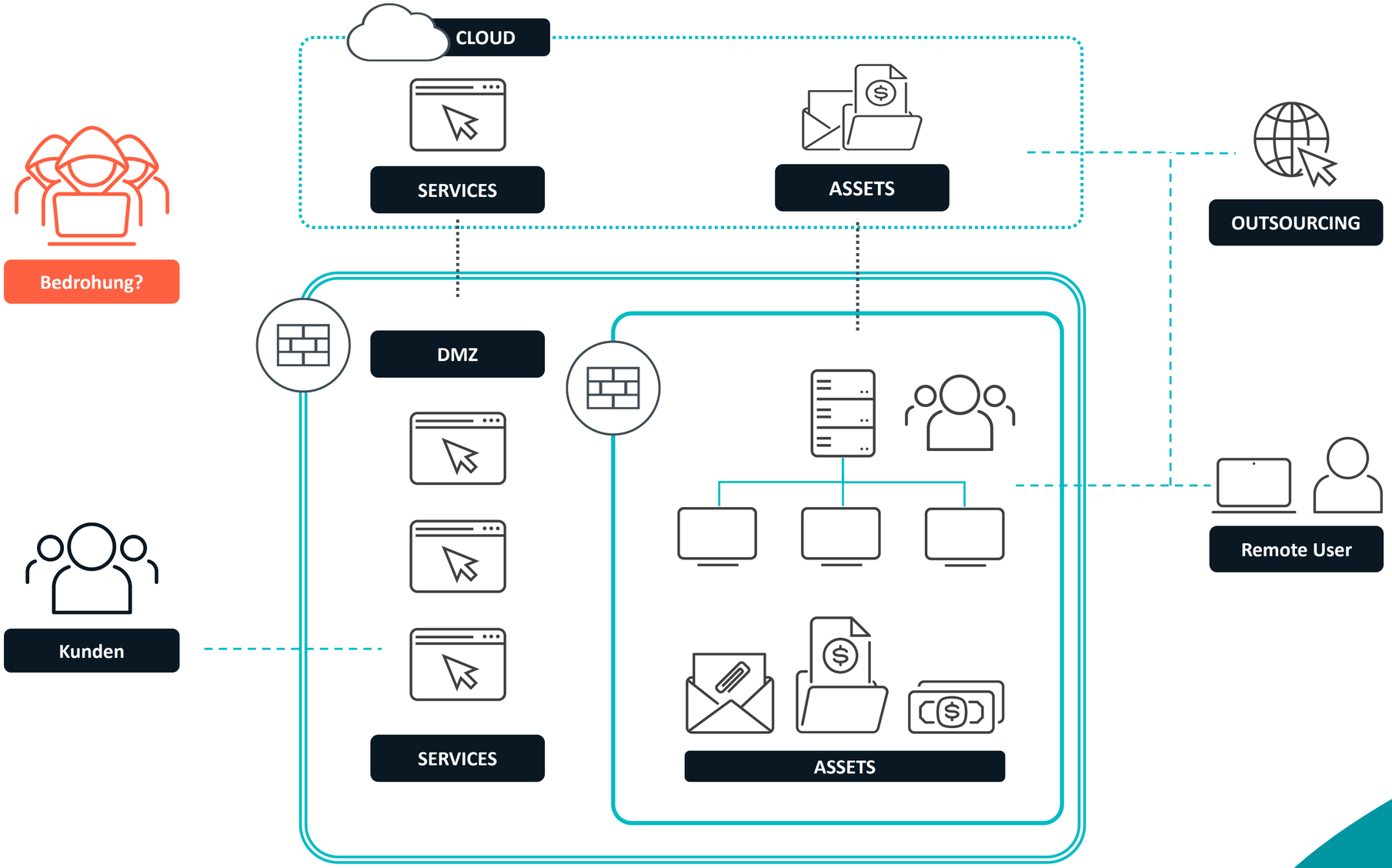
- Generell bei erheblichen Sicherheitsvorfällen
- Information aller Empfänger der Dienste der Einrichtung (Kunden) über Vorfall und Abhilfemaßnahmen

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

Stand der Technik – Compliance

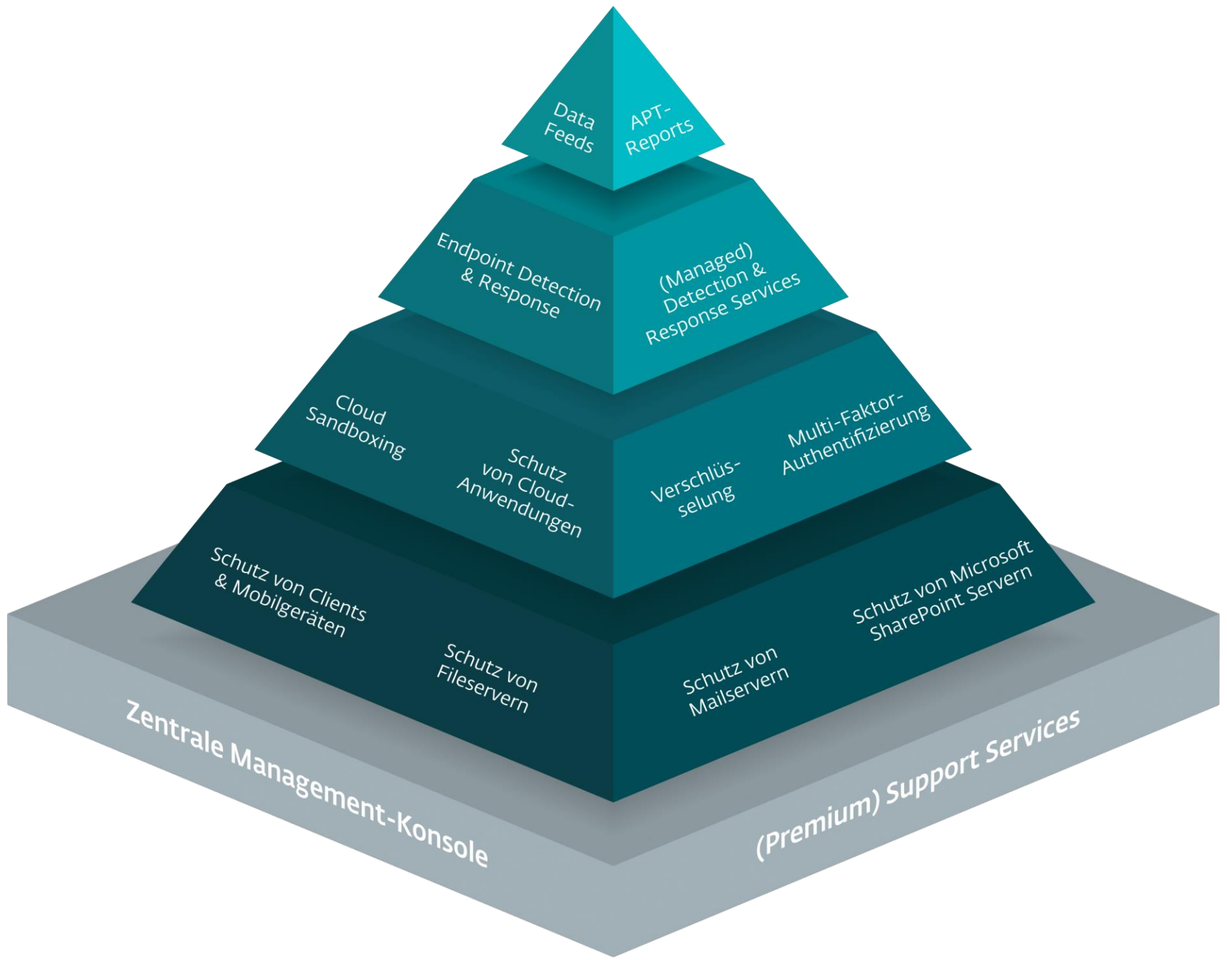
Digital Security
Progress. Protected.



Digital Security
Progress. Protected.

Unsere Strategie: Zero Trust Security

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“.

Digital Security
Progress. Protected.

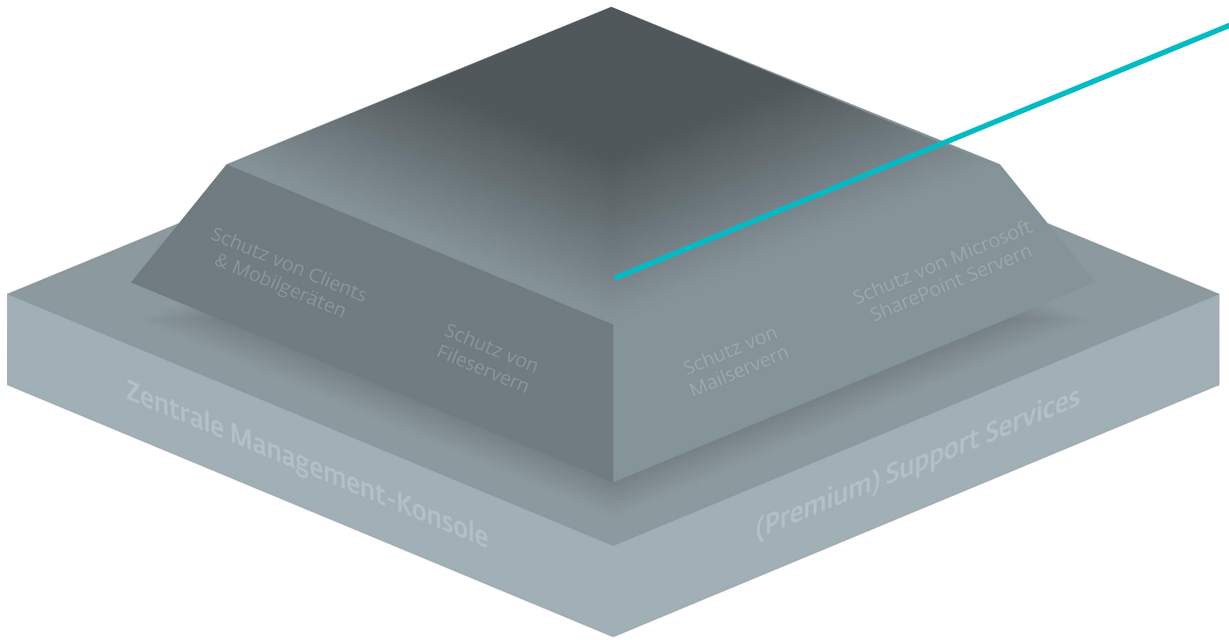
GRUNDSCHUTZ BASIS

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



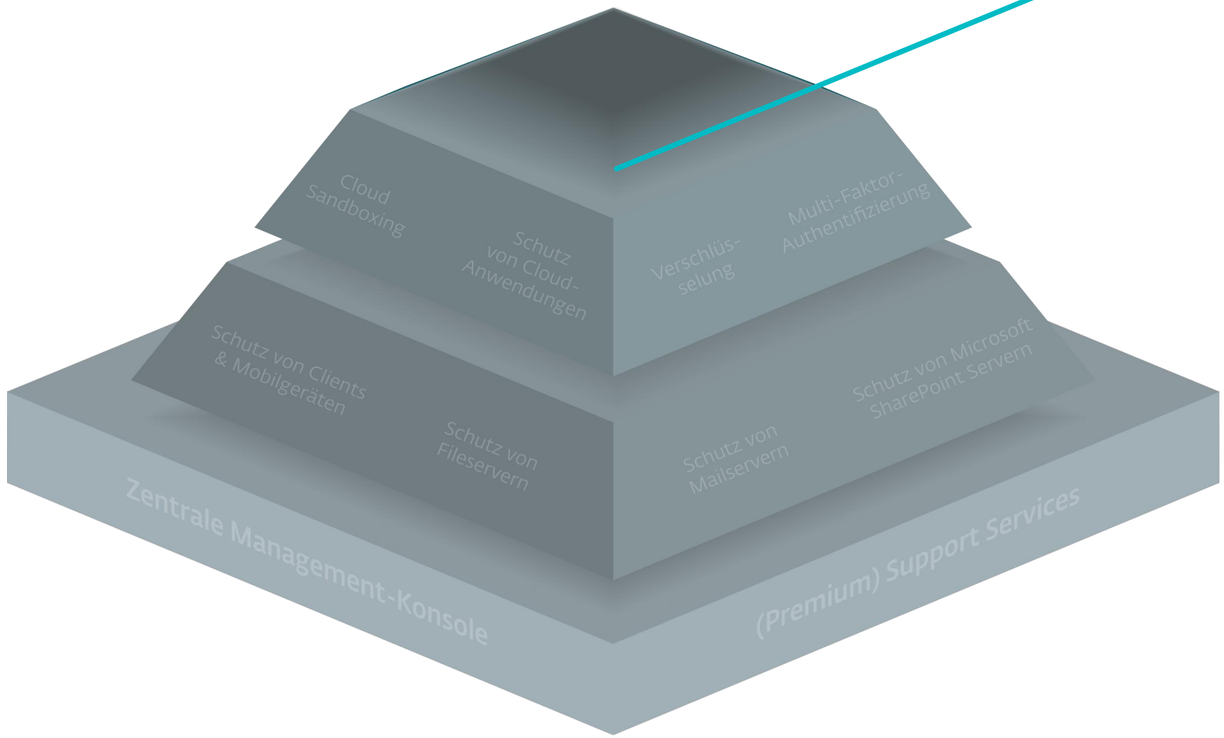
Stufe 1:
Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero-Days

Reifegrad der IT-Organisation:

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

ESET Digital Security
Progress. Protected.

GEFAHRENSUCHE UND ABWEHR - INNENSICHT



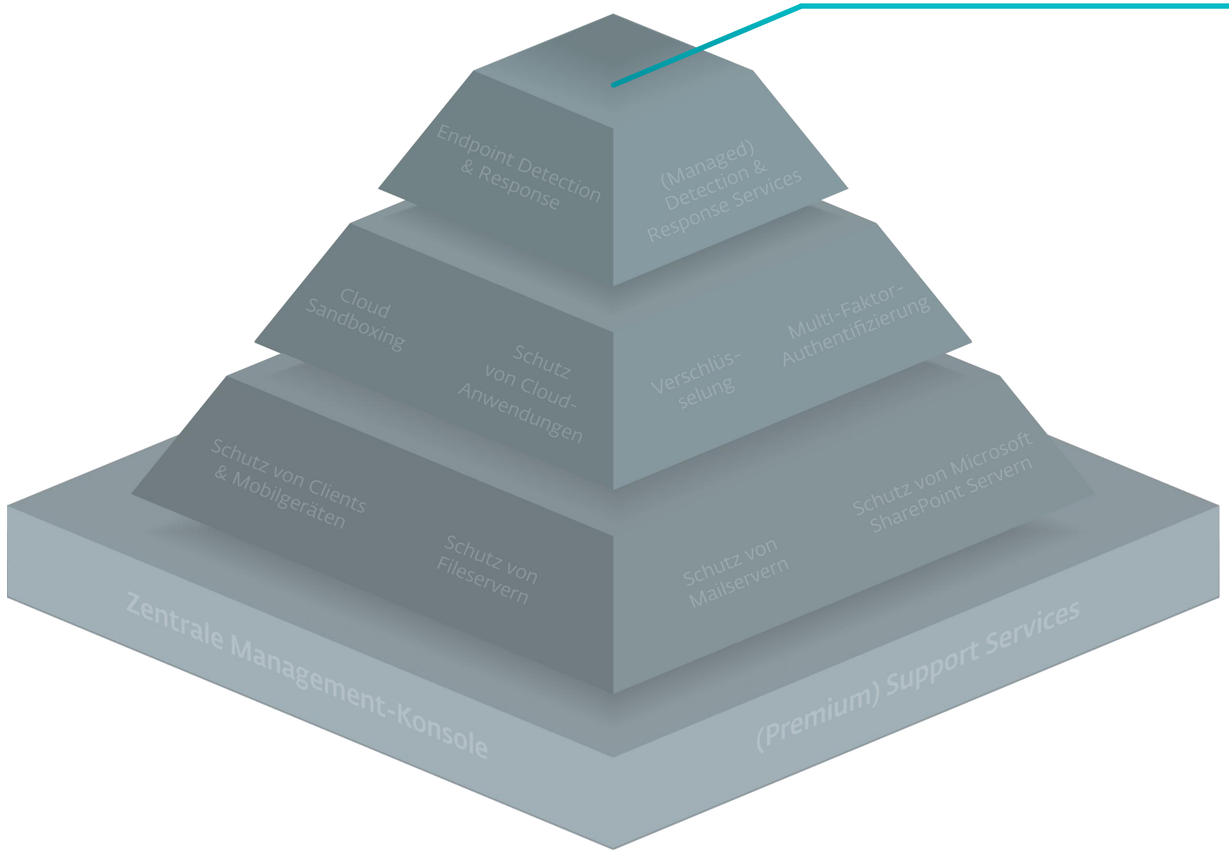
Stufe 2:
Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalieerkennung, Schwachstellen-analyse und Incident Management

Reifegrad der IT-Organisation:

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

Digital Security
Progress. Protected.

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

Digital Security
Progress. Protected.

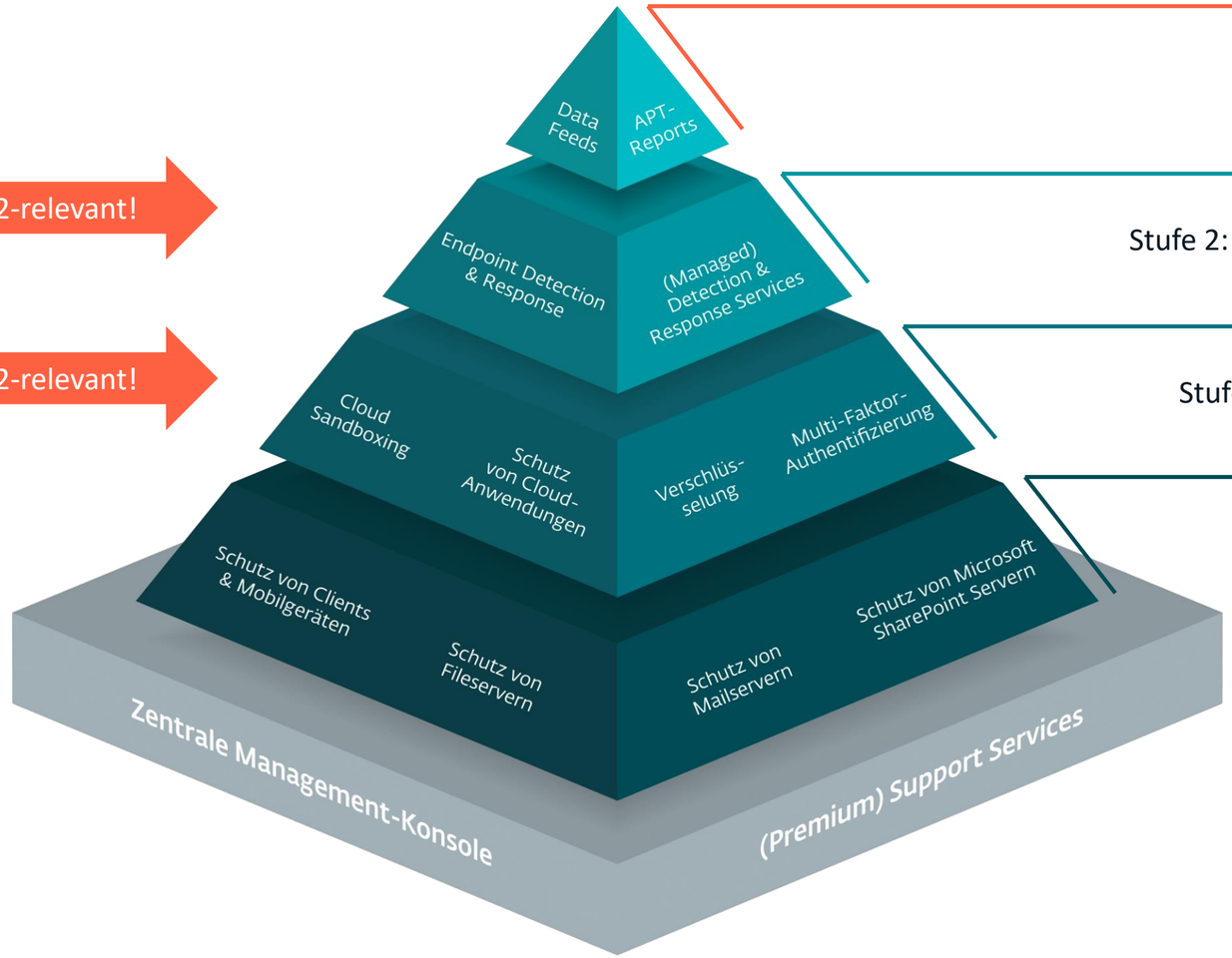
Zero Trust Security

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

Bundle-Übersicht

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.

Zero Trust Security

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

Jetzt herunterladen

Digital Security
Progress. Protected.

Zielgruppe:
CISOs
Geschäftsführer
Vorstände / Beiräte
Security-Verantwortliche

Mehr Information:
www.eset.de/nis2

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.