Note :“Mangelhaft„

Auf dem Zeugnis nicht akzeptabel in der IT Security schon?

Digital Security
Progress. Protected.


befriedigend
mangelhaft
ausreichend
mangelhaft
befriedigend
ungenügend
ausreichend

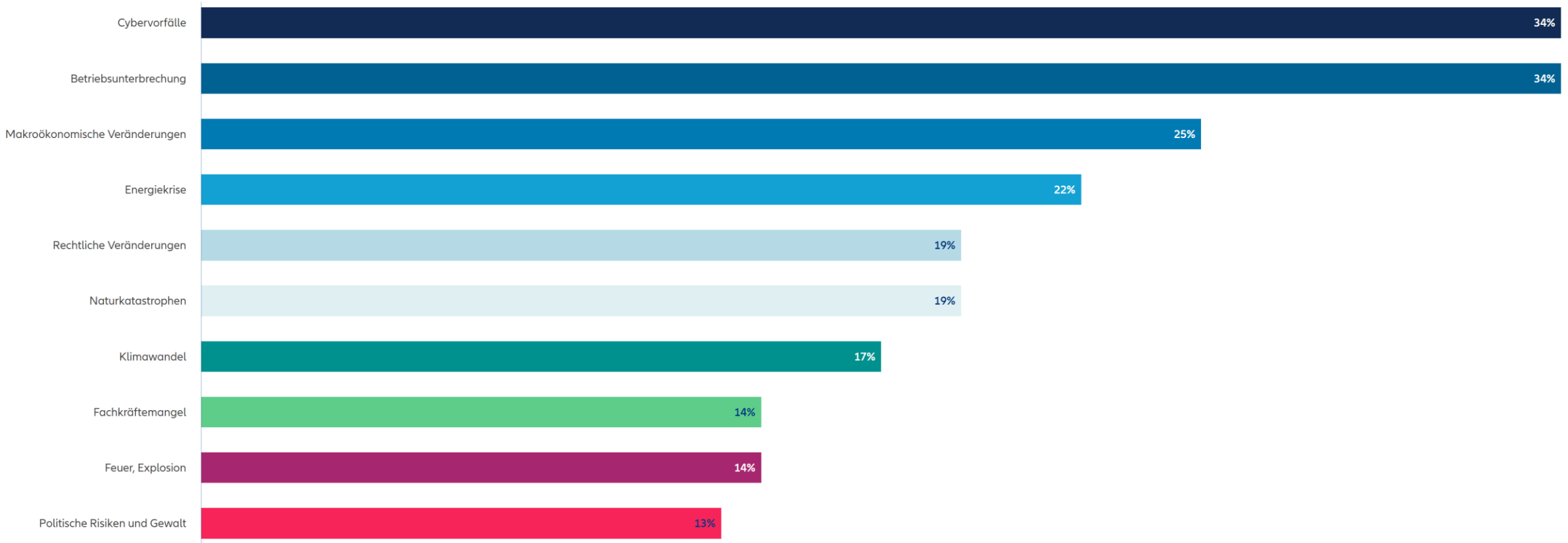
Stand der IT Sicherheit 2023

Digital Security
Progress. Protected.

Top 10 Geschäftsrisiken weltweit in 2023

Allianz Risk Barometer 2023

Basierend auf den Antworten von 2.712 Risikomanagement-Experten aus 94 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.

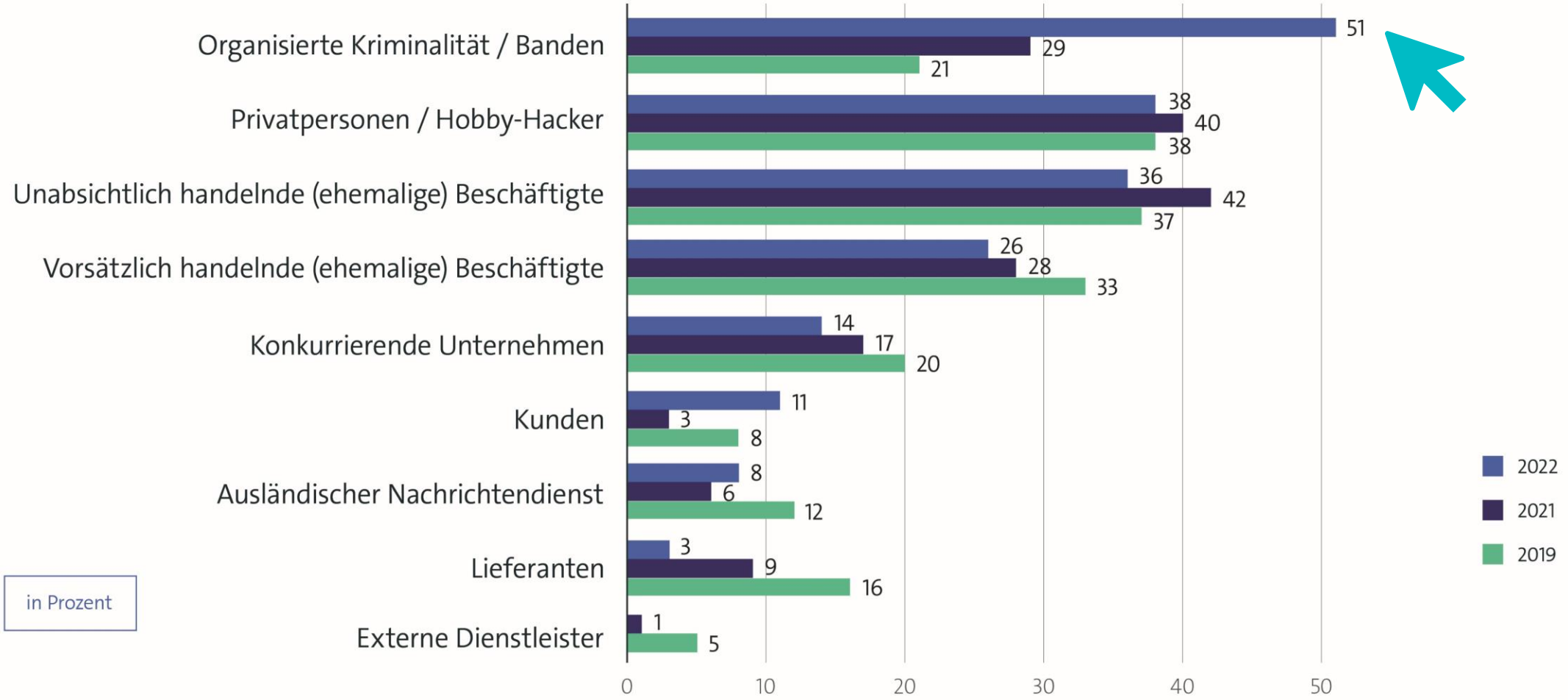


AGCS News & Inisghts

Source: Allianz Global Corporate & Specialty

Attacken auf die Wirtschaft werden professioneller

Von welchem Täterkreis gingen Handlungen in den letzten 12 Monaten aus?



Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen IT-Supply-Chain: Abhängig	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

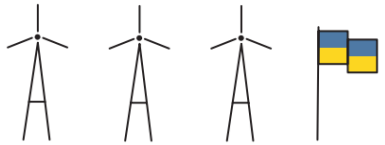
116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden

nach Angriff auf Satelliten-kommunikation



20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

34.000

Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000

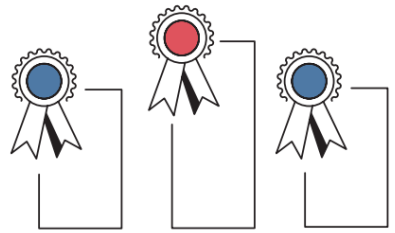
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.



BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikaten.

4.400 (2020) → **5.100** (2021)

Zehn Jahre Allianz für Cyber-Sicherheit:
2022 sind wir bereits

6.220 Mitglieder.

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•


Detailbetrachtung
„Stand der IT Sicherheit 2023“
ESET Deutschland
n=374
... WICHTIG!

In welchem Land ist Ihr Dienst-/Hauptsitz?

83,42% Deutschland

7,76% Schweiz

8,82% Österreich

Endkunden & Reseller

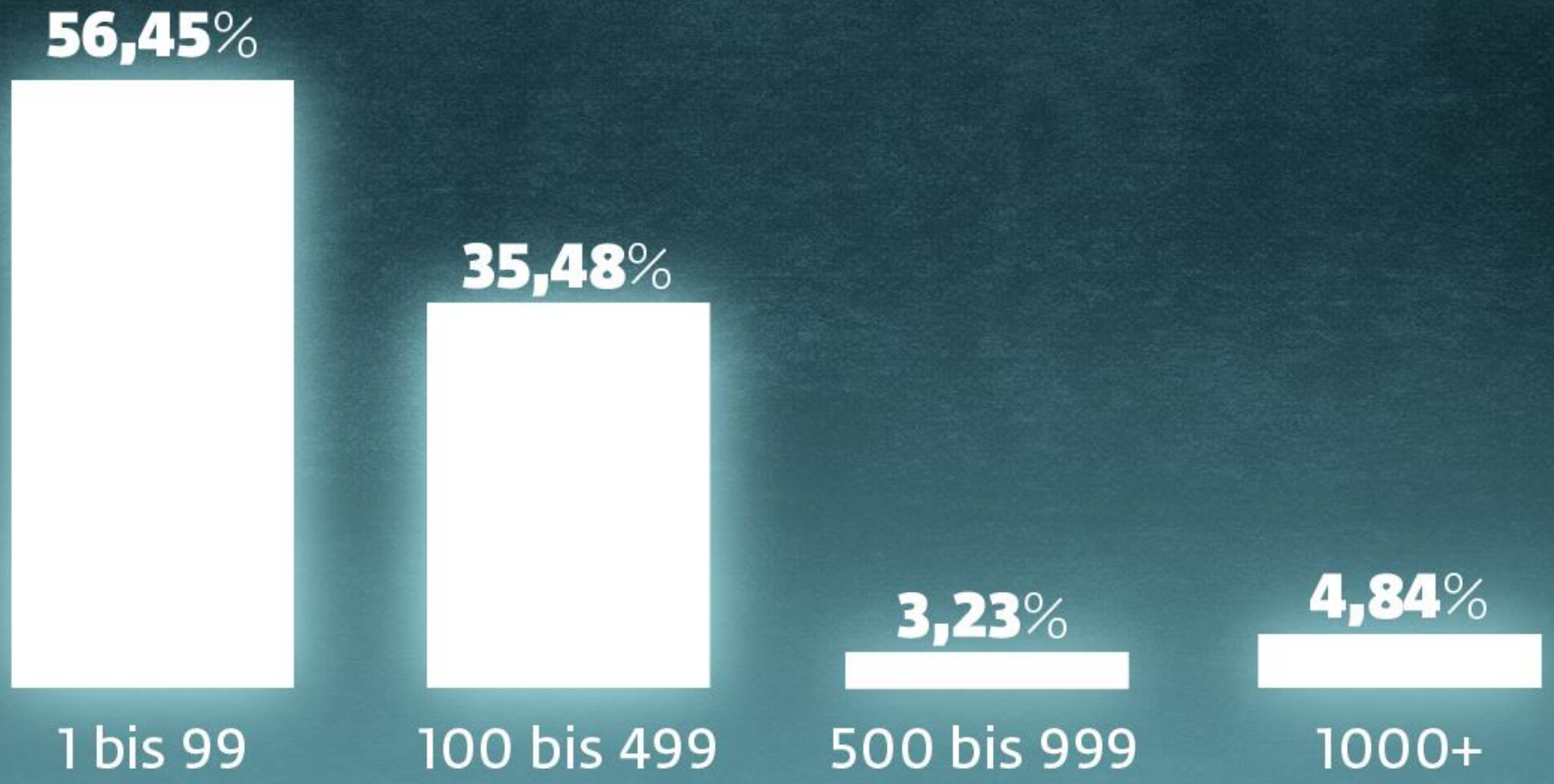
Wird Ihre IT-Security durch einen Dienstleister betreut?

35,48% Ja

64,52% Nein

befragte Endkunden

Wie viele Geräte (PCs/Notebooks/Mobilgeräte) sind in Ihrer Organisation im Einsatz?



befragte Endkunden

*„**46,79%** der Verantwortlichen kämpfen noch immer mit fehlenden Budgets und/oder Personal, dagegen glauben immerhin **74,6%** das IT-Security zwischenzeitlich den richtigen Stellenwert einnimmt!“*

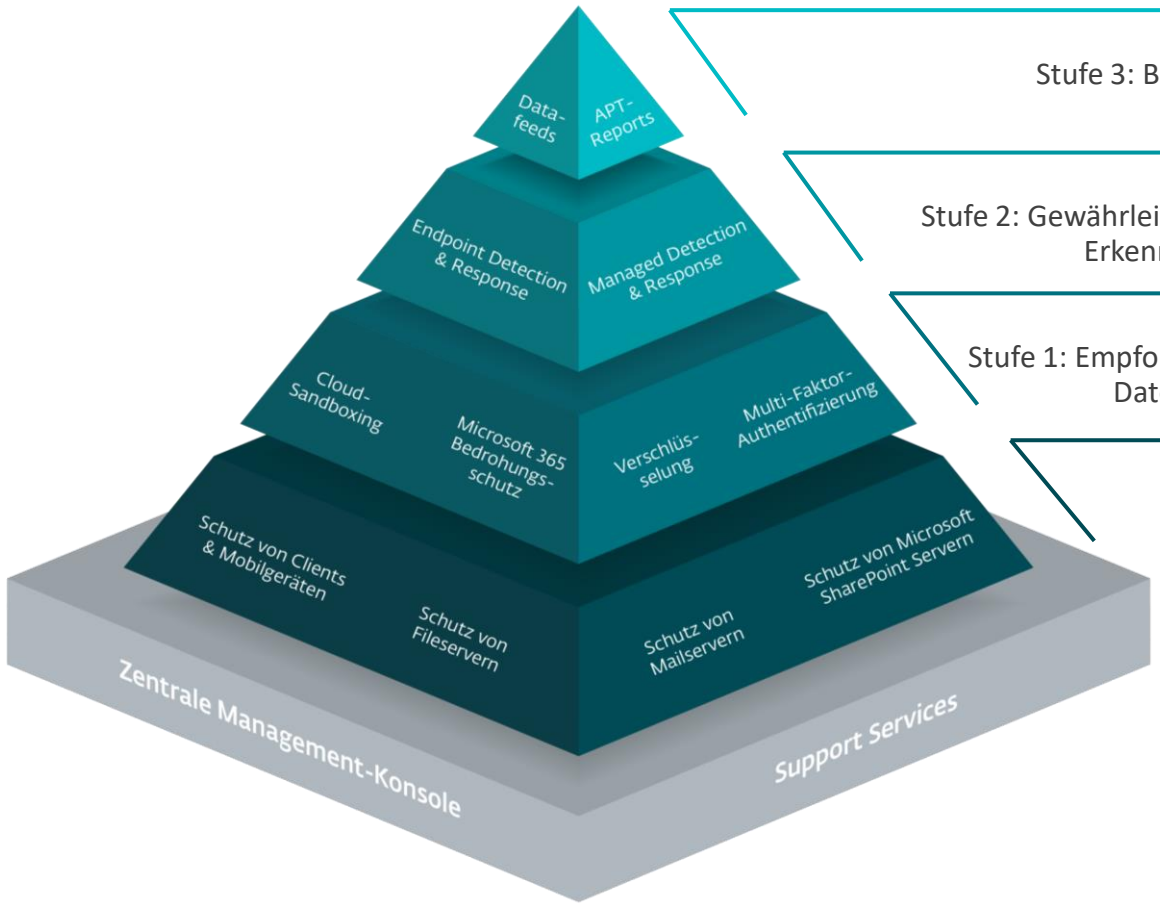
ESET Stand der IT Sicherheit (374 Teilnehmer D/A/CH, Q4 2022)

*„**57,75%** der Befragten schätzen den finanziellen Aufwand für IT-Security in den nächsten 3 Jahren als Hoch oder sogar sehr Hoch ein – Lediglich **3,74%** rechnen mit geringen oder mäßigen Mehrkosten“*

ESET Stand der IT Sicherheit (374 Teilnehmer D/A/CH, Q4 2022)

Woran soll ich mich orientieren?

Zero-Trust-Security by ESET



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

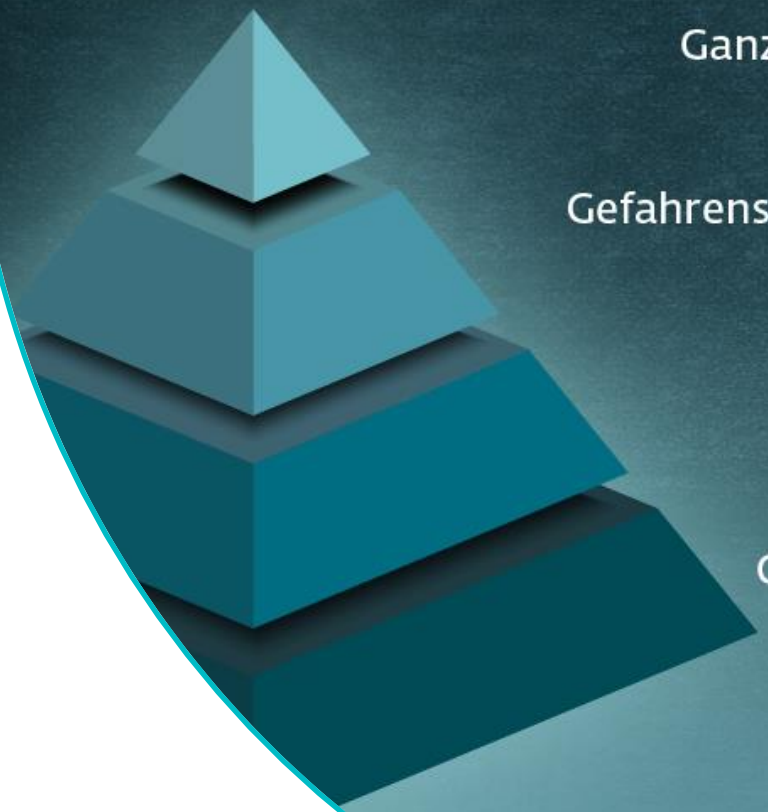
Kennen Sie den Begriff „Zero-Trust-Security“ im Allgemeinen?

Ja **81,28%**

Nein **18,72%**

Endkunden & Reseller

In welcher Zero-Trust-Stufe sehen Sie Ihre Organisation aktuell am ehesten?

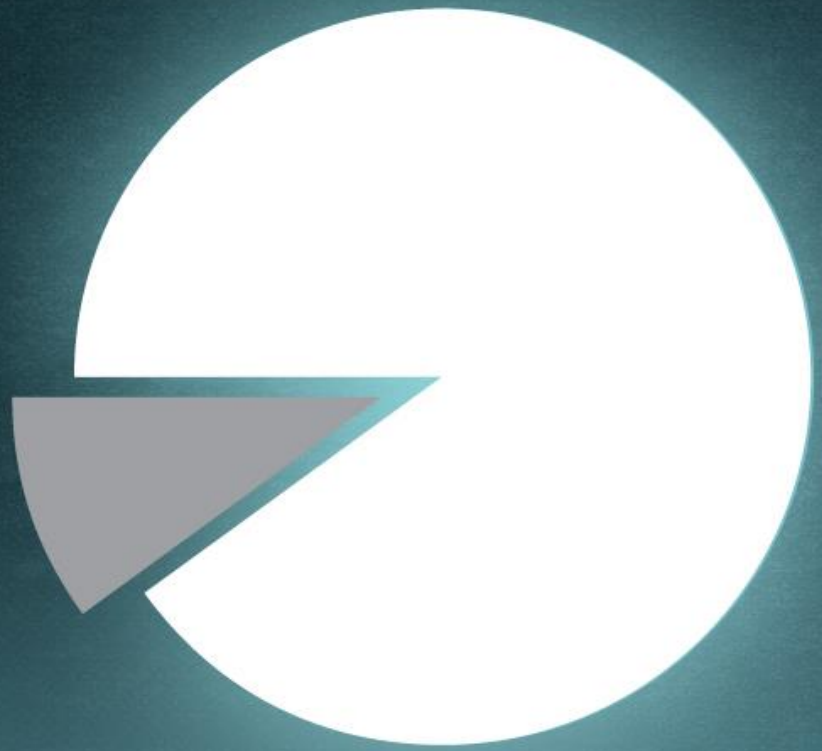


Ganzeitliches Lagebild - Außensicht	5,08%
Gefahrensuche und Abwehr - Innensicht	26,47%
Grundschutz Plus	44,12%
Grundschutz Basis	24,33%

Endkunden & Reseller

„Nur 10% der befragten Unternehmen sehen im Grundschutz Basis das passende und ausreichende Schutzlevel zur vollständigen Absicherung ihres Netzwerkes.“

„Lediglich 14% der Befragten sind sich sicher, dass sie mit ihren derzeitigem Schutzlevel den aktuellen Bedrohungen gewachsen sind.“



9 von 10

IT-Verantwortliche sind sich sicher, dass dieses strategische Modell als Orientierungshilfe dient.

7 von 8

IT-Verantwortliche glauben, dass der Zero-Trust-Security-Ansatz von ESET dabei helfen kann, die IT-Sicherheit in der eigenen Organisation zu verbessern.

Fazit der Umfrage

- Technologischer Nachholbedarf vor allem bei KMUs
- Der Stellenwert von IT-Security wächst rapide
- Bewusstsein für die aktuelle Bedrohungslage
- Verantwortliche schätzen und suchen Orientierung

„Stand der Technik“ besser als der Ruf?

Digital Security
Progress. Protected.

Audi

*„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:

Allgemeines Verständnis:

Welche Schutzziele werden durch die Maßnahme abgedeckt?

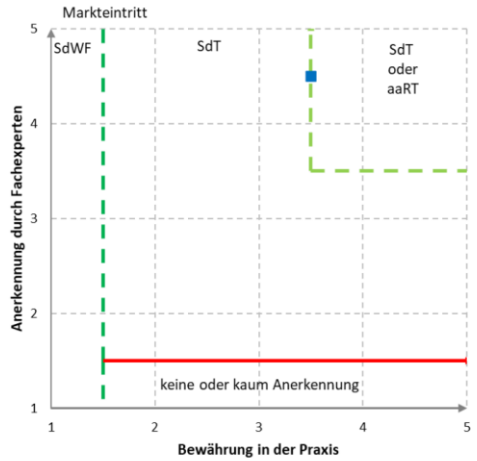
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung der Maßnahme



Am Ende des Tages sollte die Dynamik um den „Stand der Technik“ als Chance für Europa und als Qualitätsmerkmal für Organisationen jeder Größe verstanden werden!

Zielgruppe:

CISOs
Geschäftsführer
Vorstände / Beiräte
Security-Verantwortliche

Eckdaten:

25 Seiten
5 Kapitel:

Herkunft & Definition
Cyberversicherungen
Anforderungen
Technische Maßnahmen
Handlungsempfehlungen

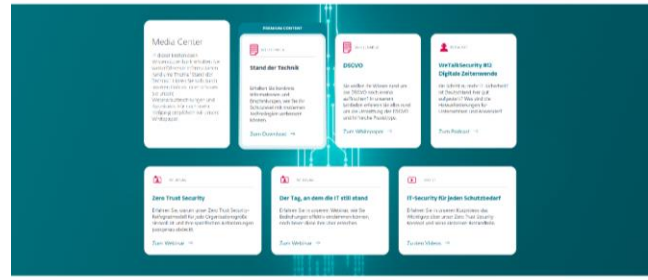
Landingpage:

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)



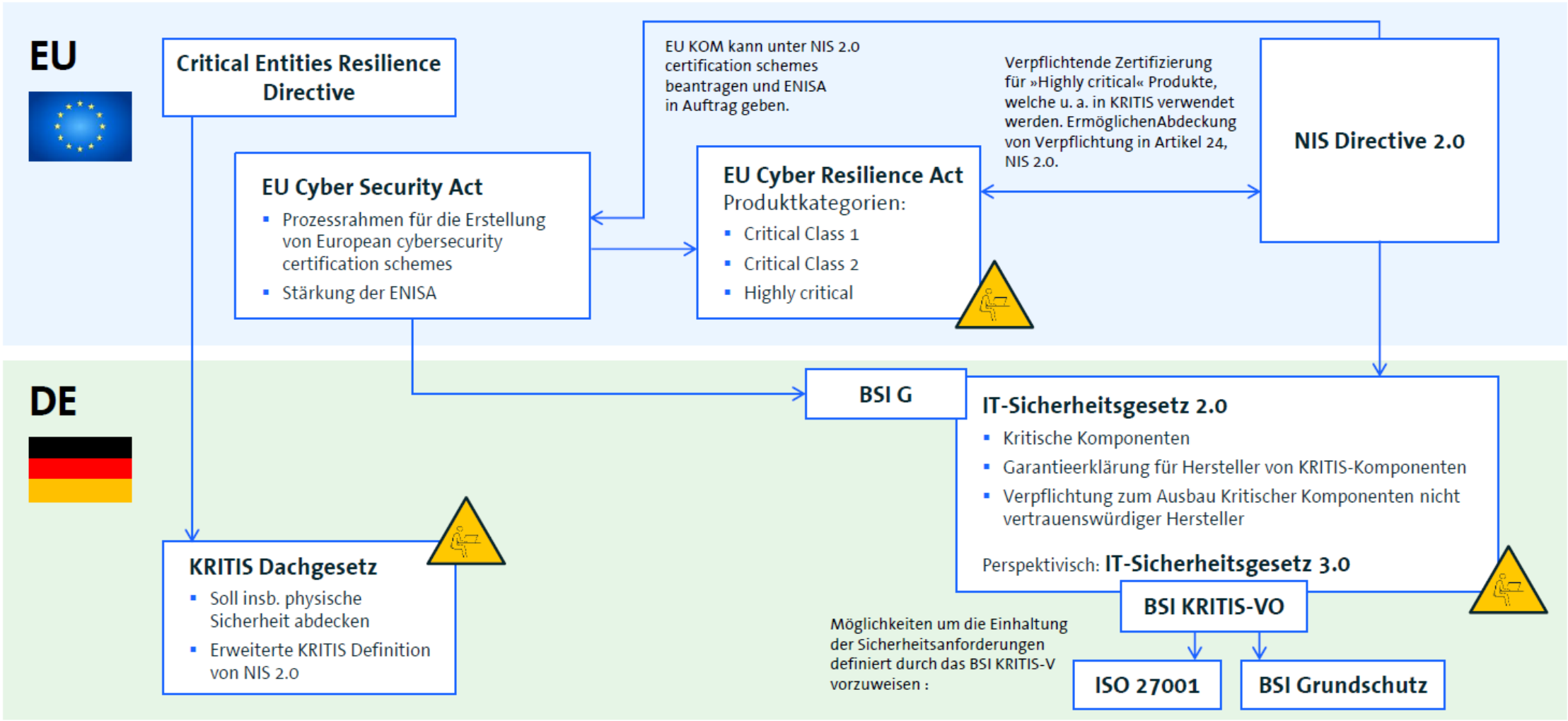
NIS 2.0 und die Reiter der Apokalypse?

Digital Security
Progress. Protected.

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

(Richtlinie für Netzwerk und Informationssicherheit)

Legislative Interdependenz



bitkom

Sektoren

Sektoren nach Anhang I (essential Entities)	Sektoren nach Anhang II (important Entities)
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 (MSP)	
Öffentliche Verwaltung	
Weltraum	

NEU!

Betreiber und Sektoren

Zwei Gruppen von Betreibern (Entities) in achtzehn Sektoren, die in der EU Dienstleistungen erbringen und nach Größe reguliert werden

- **A Essential Entities** – Große Betreiber aus elf Sektoren und Sonderfälle
- **B Important Entities** – Große/Mittlere Betreiber aus sieben Sektoren
- Unterschiede: Umfang der staatlichen Aufsicht und Sanktionen

Mittlere Unternehmen	Große Unternehmen	Unabhängig von Unternehmensgröße
• Mindestens 50 Beschäftigte • Jahresumsatz/Jahresbilanz > 10 Mio Euro	• Mindestens 250 Beschäftigte • Umsatz > 50 Mio Euro • Bilanz > 43 Mio Euro	Qualifizierende Faktoren, z.B.: • Kritische Tätigkeit • Auswirkung auf öffentliche Ordnung • Systemrisiken • Grenzüberschreitende Auswirkungen

Cyber Security Maßnahmen NIS 2.0

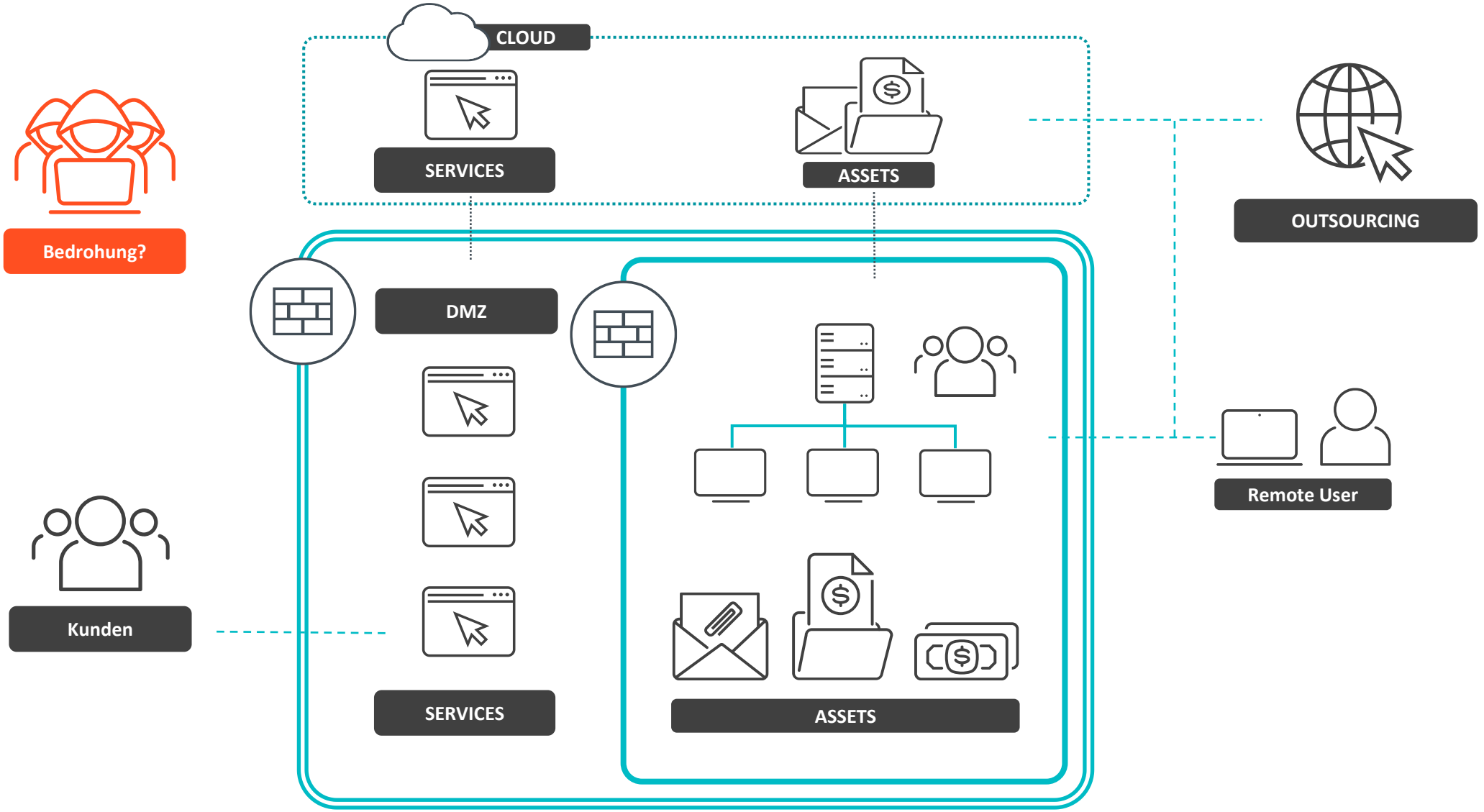
Mindestanforderungen, deren Einhaltung die Geschäftsführung von Betreibern nach nationaler Gesetzgebung überwachen und dafür haftbar gemacht werden soll.

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 und SSO
- **Kommunikation:** Einsatz sicherer Sprach-, Video- und Text-Kommunikation
- **Notfall-Kommunikation:** Einsatz gesicherter Notfall-Kommunikations-Systeme

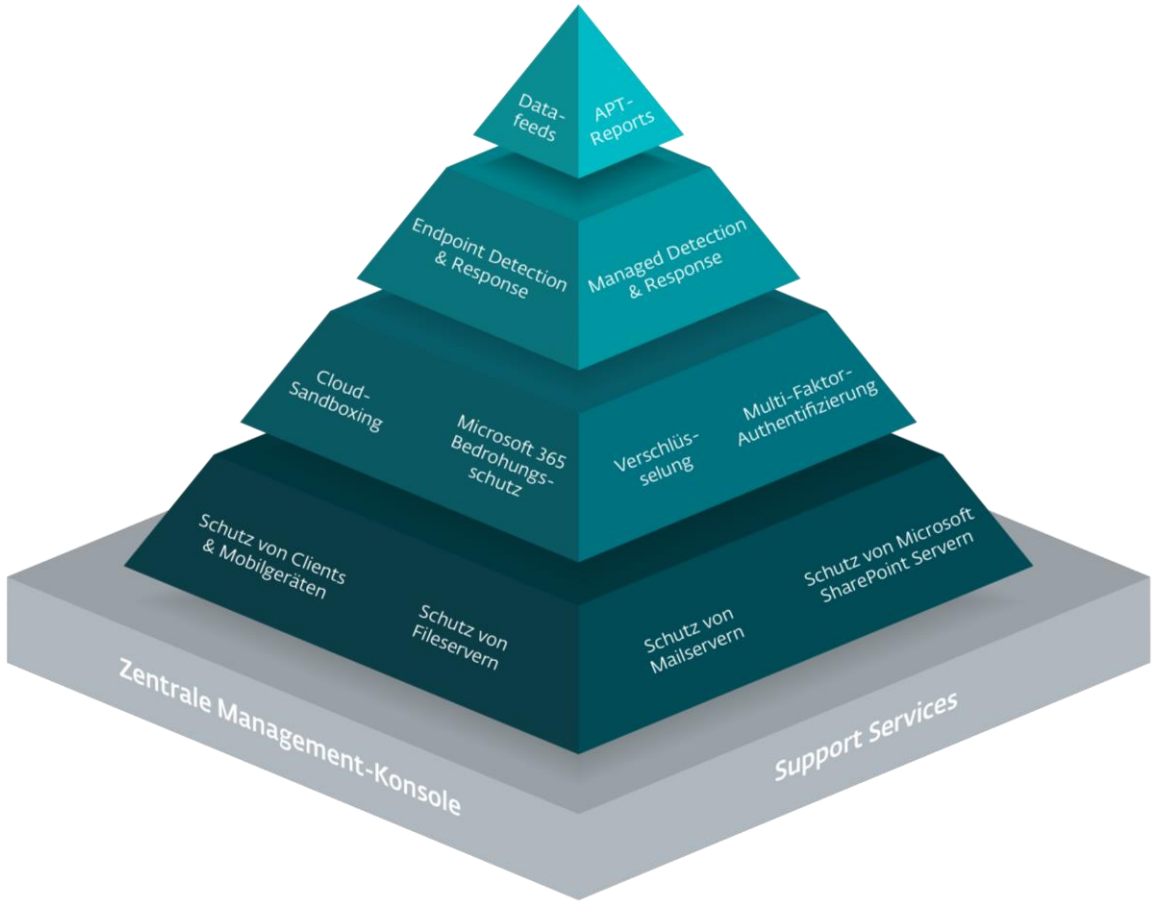
„Risikominimierung statt Raketenwissenschaft“!

Digital Security
Progress. Protected.


CLOUD
SERVICES
ASSETS
OUTSOURCING
Bedrohung?
DMZ
Remote User
Kunden
SERVICES
ASSETS


Passwörter
Integrität
Flexibilität
IOCs
Zero-Day Malware
Komplexe Lösungen
RollOut
Ransomware
Biometrie
Budget
Forensik
Phishing
Reportings
HomeOffice
EDR
Digitale Prozesse
Verschlüsselung
ISO Zertifizierung
Compliance
DSGVO
APTs
Ressourcen
Personalmangel
Mobile Geräte
Cyberversicherung
Microsoft 365 Migration

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“.

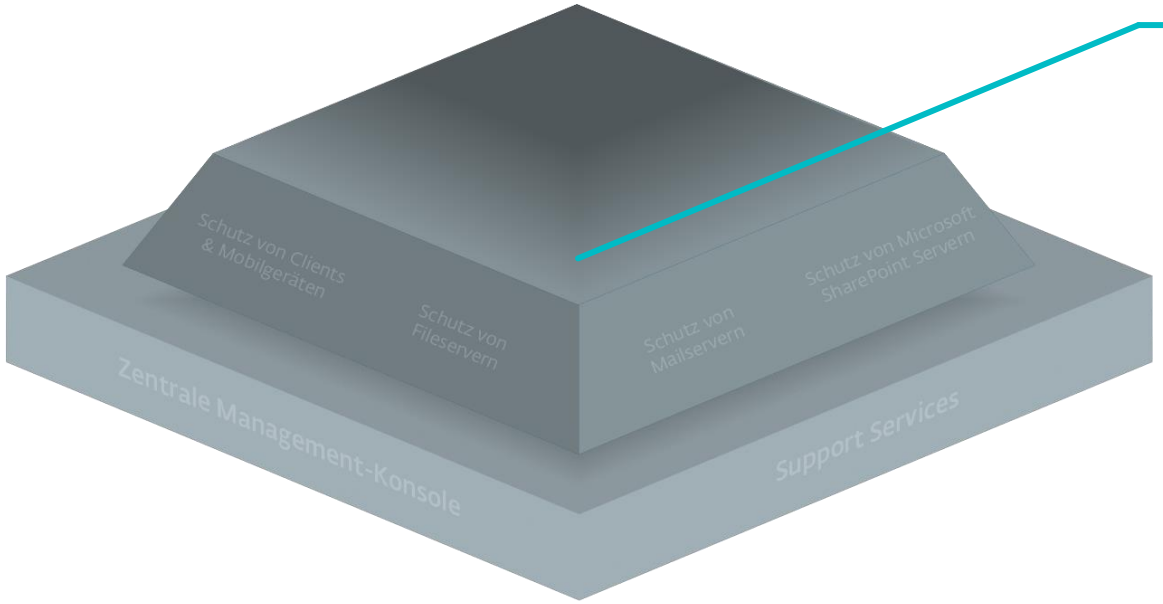
GRUNDSCHUTZ BASIS

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

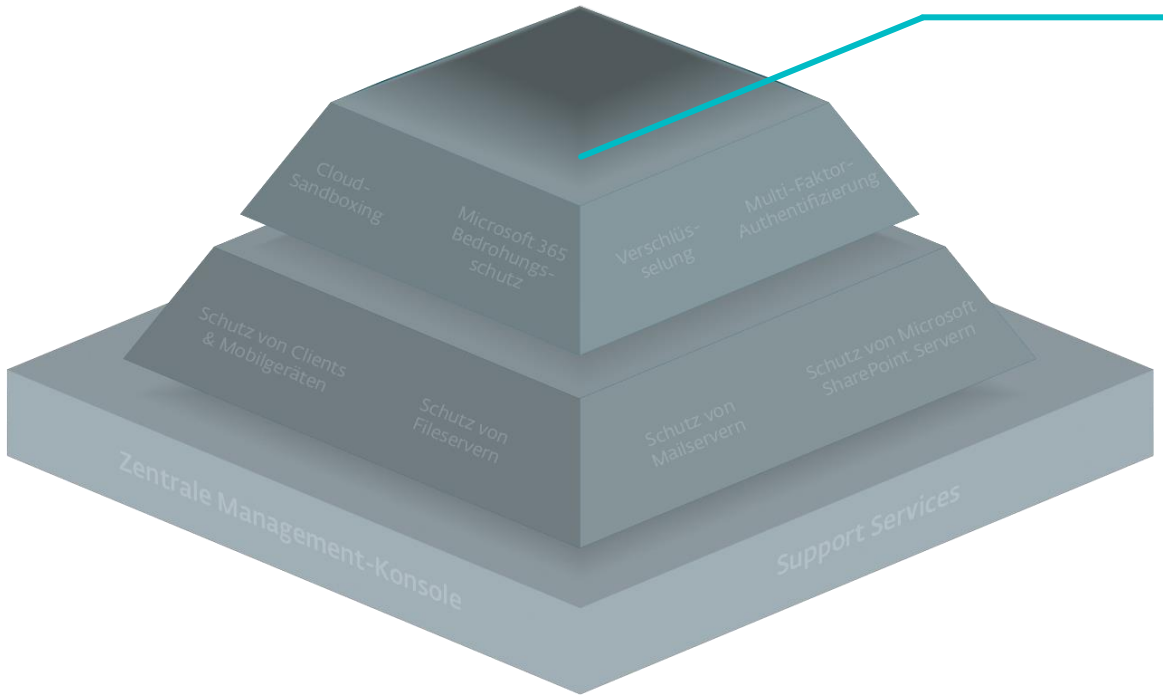


Stufe 1:
Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero-Days

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

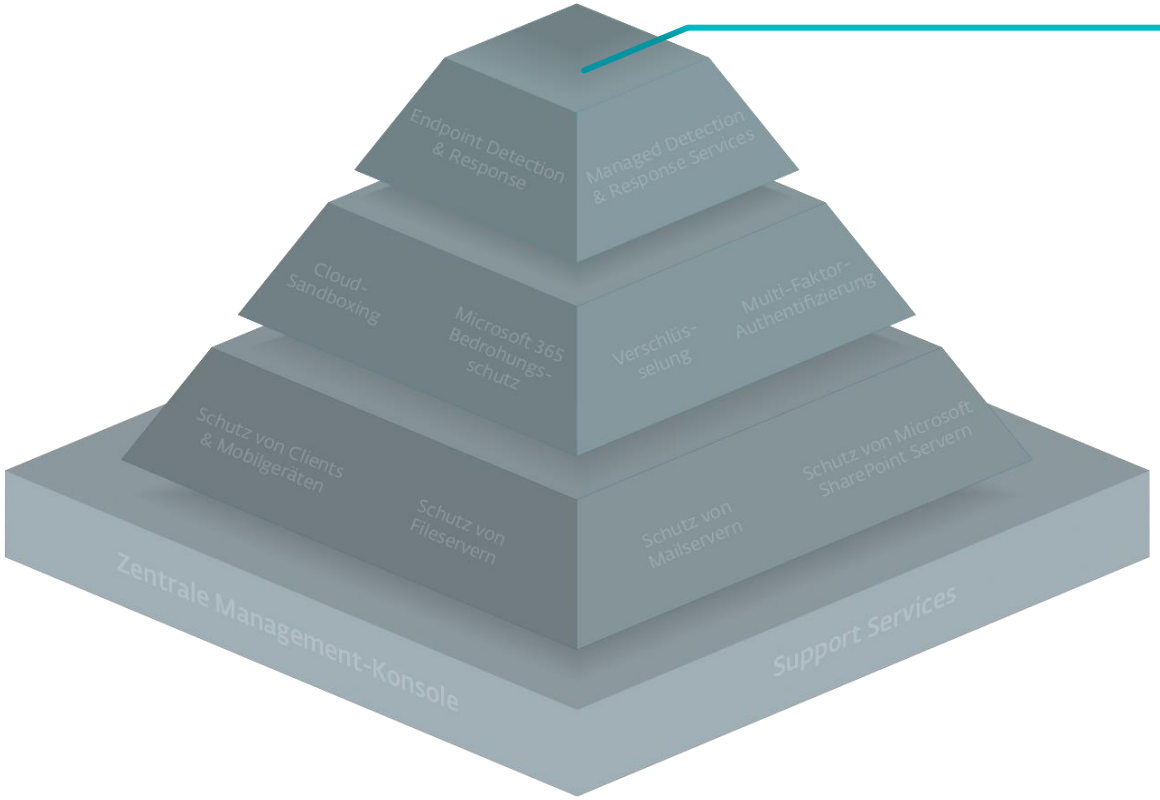


Stufe 2:
Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalie-Erkennung, Schwachstellen-analyse und Incident Management

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



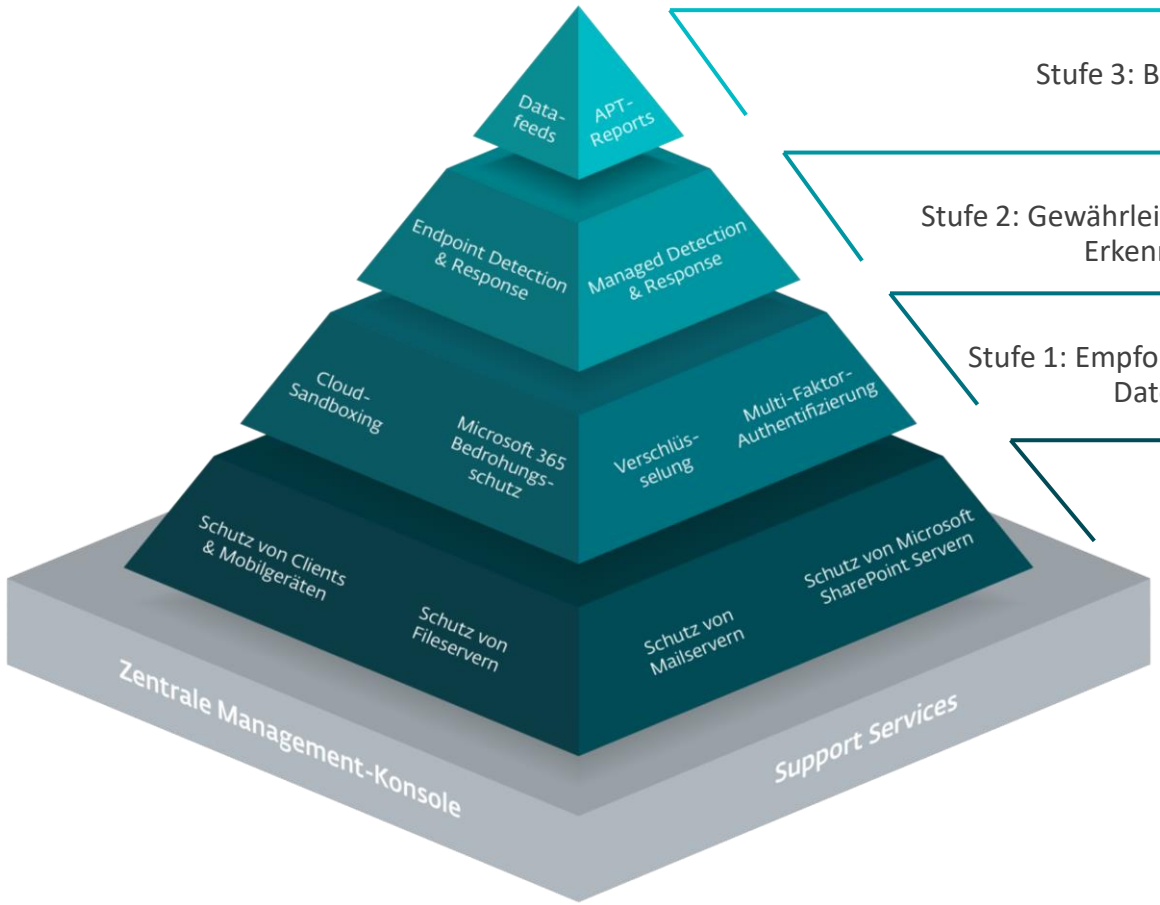
Stufe 3:
Bietet Einblicke in die globale Bedrohungsland-schaft als Grundlage für einen SOC-/SIEM-Betrieb

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