

Cybersicherheit - Großwetterlage

Game Changer Zeitenwende?

Maik Wetzel | 15. März 2023 | Mittelstand trifft Mittelstand 2023



Maik Wetzel

Strategic Business
Development Director DACH
- ESET Deutschland GmbH -



ÜBER ESET

- ✓ #1 EU-Hersteller IT-Security
- ✓ unabhängig, inhabergeführt
- ✓ 1992 gegründet
- ✓ HQ in Bratislava, weltweite Präsenz (21 Niederlassungen, 13 R&D Zentren)
- ✓ ca. 110 Mitarbeiter in Deutschland (Jena/München)
- ✓ ca. 2.000 Mitarbeiter global
- ✓ ca. 6.500 qualifizierte Reseller (IT-Dienstleister) in Deutschland
- ✓ breite Installations- und Kundenbasis
- ✓ 110 Mio Anwender

Cybersicherheit – Status Quo



Digital Security
Progress. Protected.

LAGE VOR DEM 24. FEBRUAR 2022



- ✔ Lage angespannt bis kritisch
- ✔ Cyber-Erpressungen sind größte Bedrohung
- ✔ Qualität und Anzahl der Angriffe nahmen beträchtlich zu
- ✔ Anzahl neuer Schadprogramme steigt stark
- ✔ Angriffe werden komplexer
- ✔ Umgang mit Schwachstellen bleibt eine der größten Herausforderungen
- ✔ Arbeitsteilung und Professionalisierung auf Seite der Angreifer
- ✔ „zumindest in Teilbereichen Alarmstufe rot!“

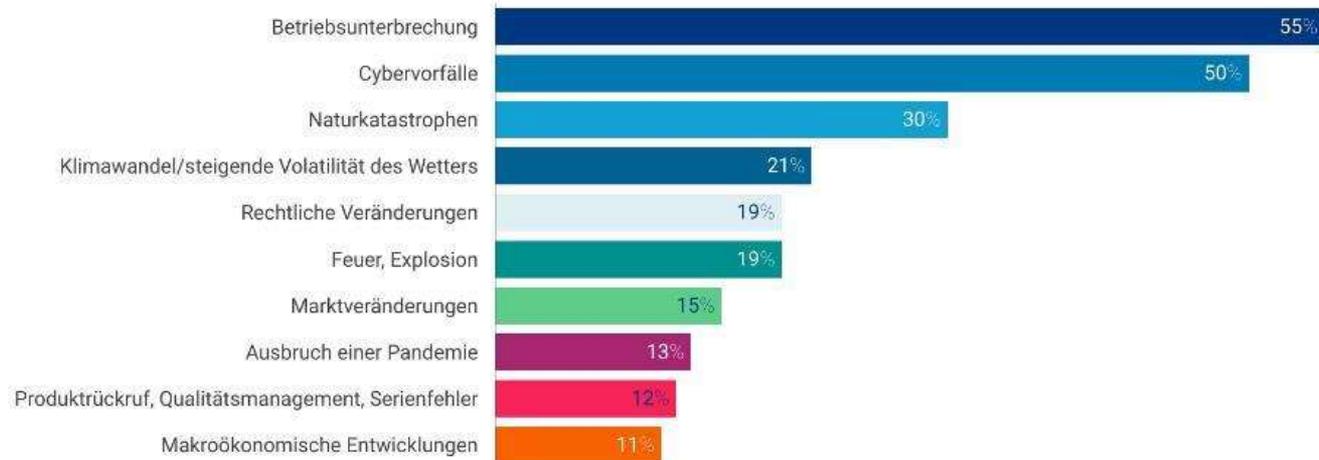
ALLIANZ RISK BAROMETER 2022



Top 10 Geschäftsrisiken in Deutschland

Allianz Risk Barometer 2022

Die Zahlen geben an, wie oft ein Risiko als Prozentsatz aller Antworten für das jeweilige Land ausgewählt wurde: 351. Die Zahlen addieren sich nicht zu 100%, da bis zu drei Risiken ausgewählt werden konnten.



ZEITENWENDE UND CYBER-BEDROHUNGEN



- ✓ weitere Verschärfung der Bedrohungslage
- ✓ „Hybride Bedrohungslage“
- ✓ Hacktivismus mit Eskalationspotential
- ✓ Spillover-Effekte
- ✓ „einzelne“ IT-Sicherheitsvorfälle
- ✓ besonderer Zielfokus: KRITIS und Public Sector
- ✓ Lageveränderung jederzeit möglich
- ✓ Blick/Fokus auf Cyber-Sicherheitslage Ukraine

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:



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.

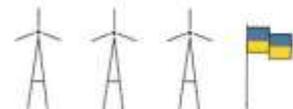


Hackivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.



Kollateralschaden nach Angriff auf Satelliten- kommunikation



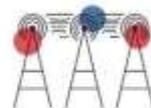
20.174

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

Malware mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsmailboxen abgefangen.



78.000

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

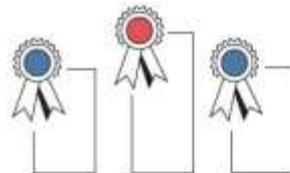
69%

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 → 5.100
2020 → 2021



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

6.220

Mitglieder.



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital • Sicher • BSI

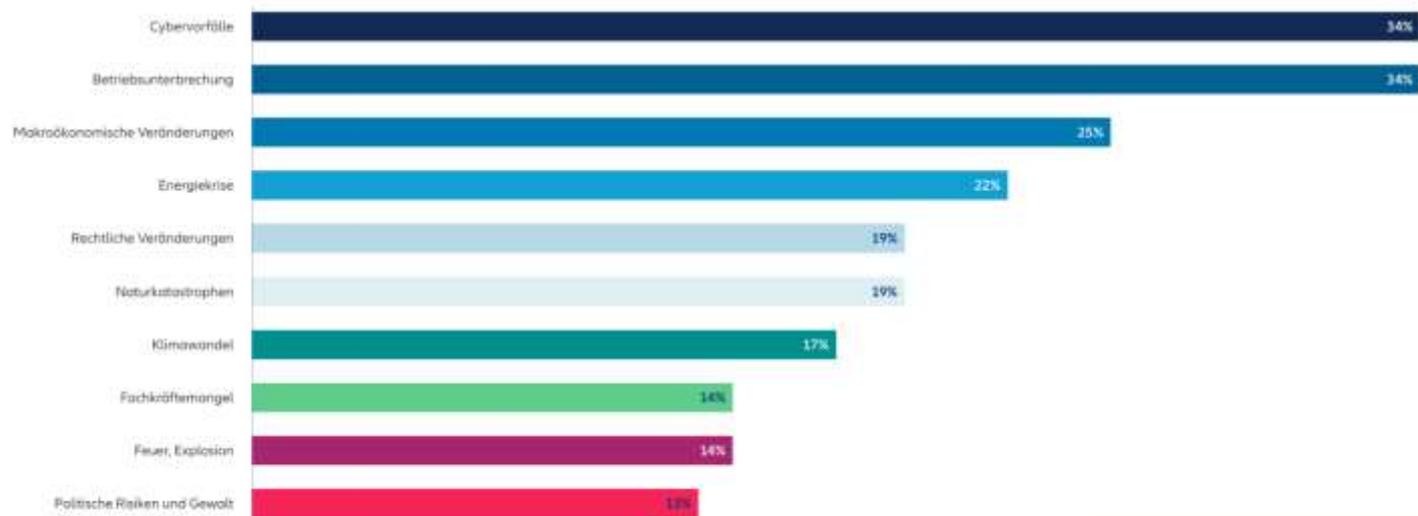
ALLIANZ RISK BAROMETER 2022



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.



Cyberwar in der Ukraine



Digital Security
Progress. Protected.

Sandworm

Telebots/Voodoo Bear

Sednit

Fancy Bear/APT28

The Dukes

Cozy Bear/APT29

TA428

InvisiMole

Turla

Buhtrap

SITUATION IN DER UKRAINE

- ✓ Seit Jahren Cyber-Schlachtfeld Ukraine
- ✓ Zahlreiche APT-Angriffe auf Regierungsorganisationen, öffentliche Verwaltung, KRITIS und Unternehmen
- ✓ Angriffe auf „Lieferketten“ und Multiplikatoren
- ✓ APT-Hackergruppen zielen auf die Ukraine, aber auch auf andere Länder
- ✓ Ziel u.a.: Destabilisierung der Gesellschaft
- ✓ ESET veröffentlicht Ergebnisse u.a. auf www.welivesecurity.de, über Social Media, Pressemeldungen, im ESET Threat Report bzw. als Service für Kunden (ETI)

Buhtrap

InvisiMole

Energetic
Bear



FSB

The Dukes

Cozy Bear/APT29



SVR

Sandworm

Telebots
/Voodoo Bear



GRU

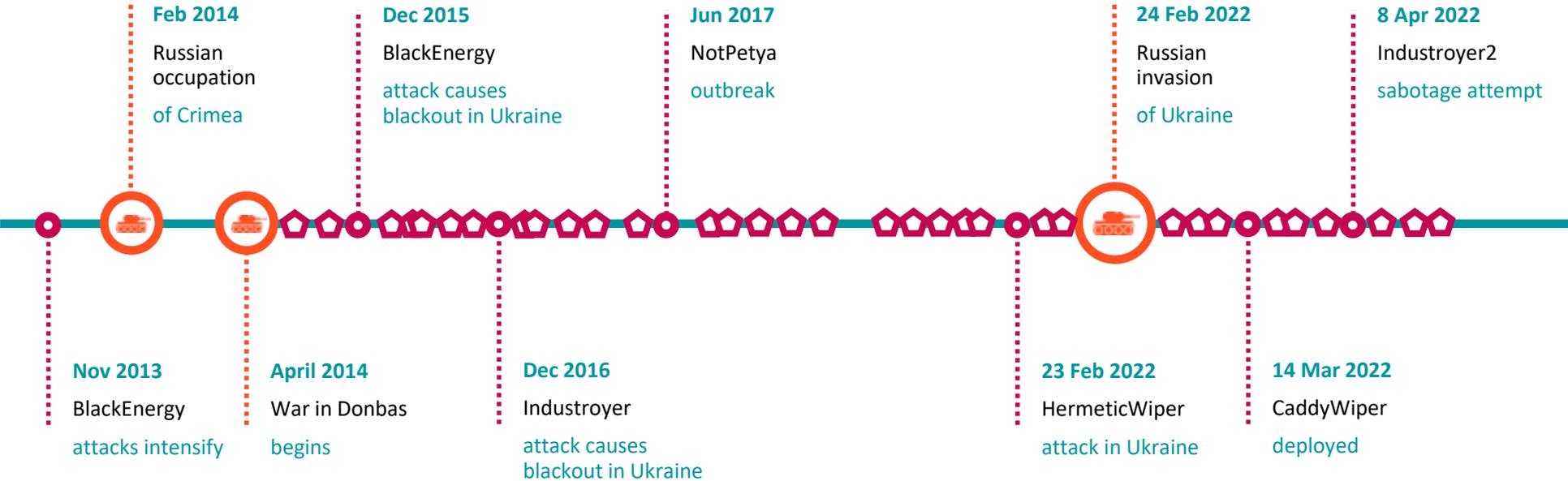
Turla

Gamaredon

Sednit

Fancy
Bear/APT28





Was uns 2023ff
beschäftigen wird



Digital Security
Progress. Protected.



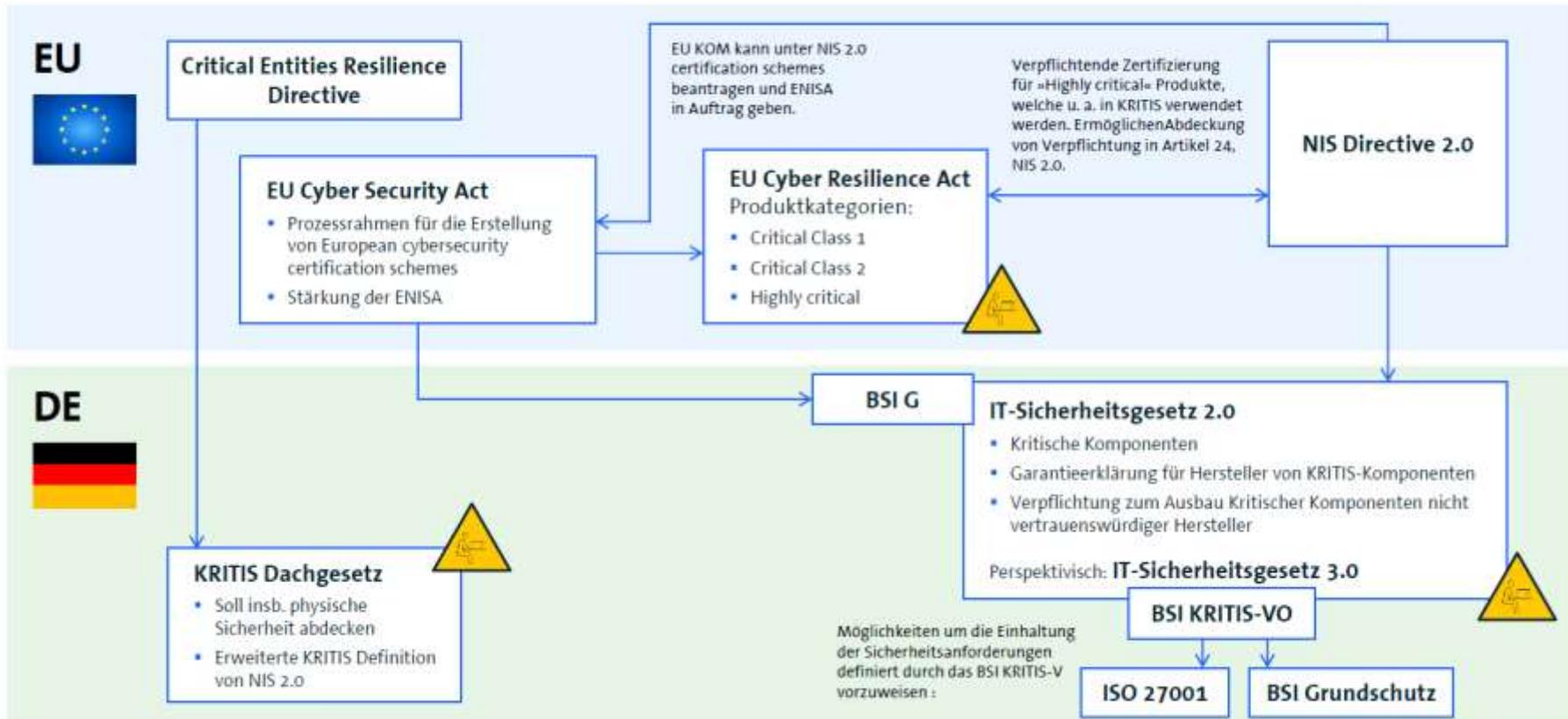
REGULIERUNG

- ✓ NIS 2.0
- ✓ EU Cyber Resilience Act
- ✓ EU Data Act
- ✓ EU Digital Markets Act
- ✓ EU AI Act
- ✓ EU Krypto Act
- ✓ GAIA-X
- ✓ ...

Übergeordnete Ziele:

Digitale Souveränität und Resilienz verbessern!

Legislative Interdependenz



NIS 2.0 - UMSETZUNG

- allgemeine Compliance Anforderung für die Wirtschaft!!
- Massive Ausweitung des Anwendungsbereichs (18 Sektoren)
- physische, technische und organisatorische Maßnahmen zum besseren Schutz vor Cybergefahren
- technische Mindeststandards weit über klassischem Endpoint-Schutz
- Harmonisierung / Förderung von Standards
- Umsetzung innerhalb von 21 Monaten nach Inkrafttreten (Januar 2023)
- aufgrund der besonderen Bedeutung für Staat und Gesellschaft „technologische (digitale) Souveränität“ von großer Bedeutung
- Sanktionen/Bußgeldkatalog / Haftung Leitungsorgane
- erhebliches Potential für IT-Security Branche!

Ziele NIS 2.0

Verbesserung
der Resilienz /
Cybersicherheit

Harmonisierung
– EU-weite
Standards

Verbesserung
der
Zusammenarbeit

Reorganisation Cyber Sicherheit in DE?

- Zuständigkeiten und Befugnisse Bund – Länder
 - Klärung und Reorganisation für Cyber Security und Cyber Abwehr (aktiv/passiv)
 - Beseitigung von „Defiziten“
 - BSI als (unabhängige) Zentralstelle für Cyber Sicherheit
 - Kommando CIR für Cyber Abwehr?
 - Rolle von Diensten und Ermittlungsbehörden
- Cybersicherheitsstrategie (letzter Stand 2021)
- Zentrale Koordination (Kanzleramt?)
- Überarbeitung IT-SIG 2.0
- Deutliche Erweiterung der betroffenen Einrichtungen in DE
- Einbeziehung öffentlicher Sektor wird diskutiert



Bundesministerium
des Innern
und für Heimat

DIGITALPOLITISCHE ZIELE BIS 2025

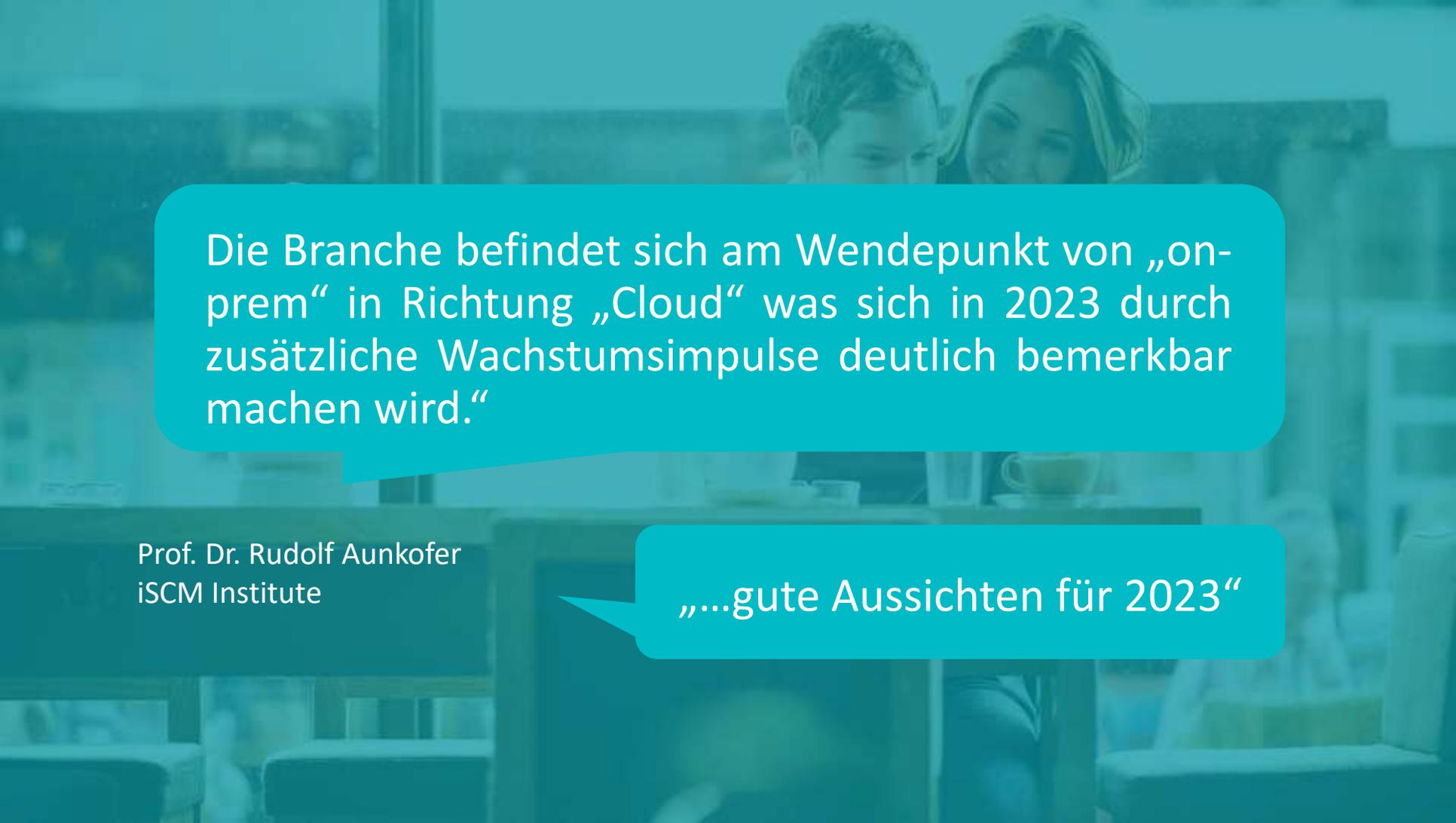
- ✓ Staatliche Leistungen für Menschen und Unternehmen digitalisieren
- ✓ Staat modernisieren
- ✓ Cybersicherheit modernisieren und harmonisieren
- ✓ Daten rechtssicher erschließen und nutzen
- ✓ Digitale Souveränität festigen und interoperable Infrastruktur schaffen



Bundesministerium
des Innern
und für Heimat

CYBERSICHERHEITS- AGENDA DES BMI

- ✓ Cybersicherheit modernisieren und harmonisieren
- ✓ Cyberfähigkeiten und Digitale Souveränität der Sicherheitsbehörden stärken
- ✓ Cybercrime und strafbare Inhalte im Internet bekämpfen
- ✓ Cybersicherheit der Behörden des Bundes stärken
- ✓ **Cyber-Resilienz Kritischer Infrastrukturen stärken**
- ✓ Schutz ziviler Infrastrukturen vor Cyberangriffen
- ✓ **Digitale Souveränität in der Cybersicherheit stärken**
- ✓ Krisenfeste Kommunikationsfähigkeit schaffen und Sicherheit der Netze ausbauen



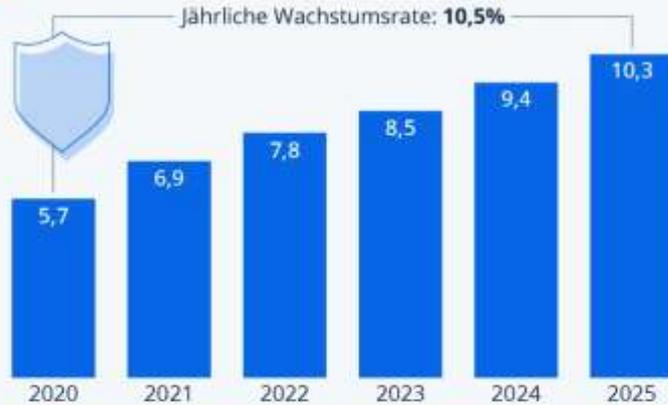
Die Branche befindet sich am Wendepunkt von „on-prem“ in Richtung „Cloud“ was sich in 2023 durch zusätzliche Wachstumsimpulse deutlich bemerkbar machen wird.“

Prof. Dr. Rudolf Aunkofer
iSCM Institute

„...gute Aussichten für 2023“

IT-Sicherheitsmarkt soll 2025 die 10-Mrd.-Euro-Grenze knacken

Geschätzte Ausgaben für IT-Sicherheit in Deutschland
(in Mrd. Euro)



Quelle: Bitkom



statista 

Stand der Technik und Cyber-Versicherung



Digital Security
Progress. Protected.

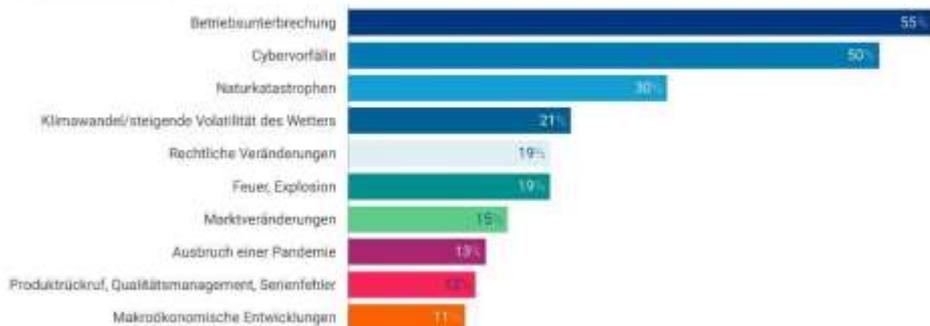
ALLIANZ RISK BAROMETER 2022/2023



Top 10 Geschäftsrisiken in Deutschland

Allianz Risk Barometer 2022

Die Zahlen geben an, wie oft ein Risiko als Prozentsatz aller Antworten für das jeweilige Land ausgewählt wurde. 251. Die Zahlen addieren sich nicht zu 100%, da bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

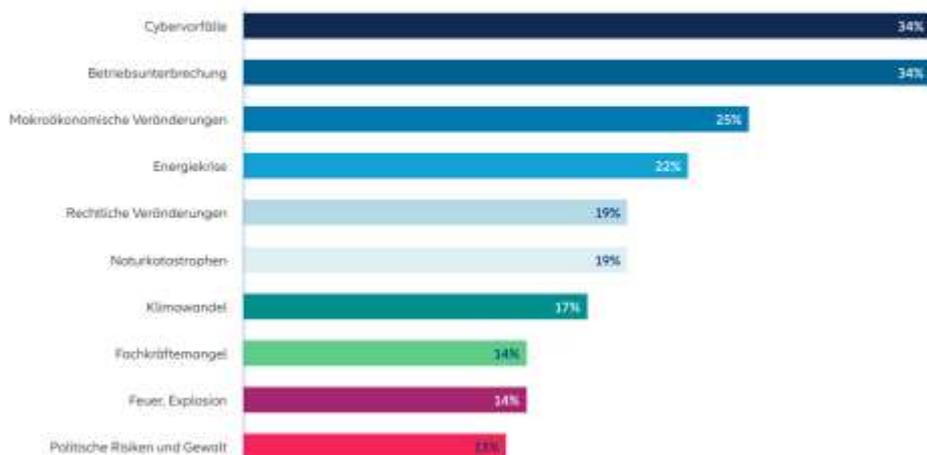
Quelle: Allianz Global Corporate & Specialty



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 & Insights

Source: Allianz Global Corporate & Specialty

Versicherungsbranche

„Der [Gesamtverband der Deutschen Versicherungswirtschaft e.V.](#) (GDV) rät zur Überprüfung, ob das eigene Unternehmen – oder das von Kunden – gefährdet und hinreichend für den Fall eines Cyberangriffs vorbereitet ist. Dafür hat der Verband einen [Fragebogen](#) auf der Webseite, der für etwas Klarheit sorgen soll.“

Eine
aller
ein
ode
üb
Cy
ak
de

Befragten nannten die Durchführung von Schulungen zum
nt das Implementieren bzw. Umsetzen von
Iri-Faktor-Authentifizierung (MFA)
Cyberversicherung

„Fast 80 Prozent der Unternehmen haben bei ihrem Versicherer bereits Ansprüche geltend gemacht [...], mehr als die Hälfte davon mehrfach. [...] In der Folge kürzen Versicherungsunternehmen die Leistungen und ziehen sich vermehrt von der Deckung kritischer Risiken zurück. So sind etwa Schäden durch Ransomware oder Kosten für Datenwiederherstellungen bei rund 50 Prozent der befragten Unternehmen von der Police nicht mehr abgedeckt.“

Versicherungsbranche

Cyber-Sicherheitscheck
Basisfragen

Sie haben die Basisfragen erfolgreich abgeschlossen. Hier ist Ihre Zwischenbewertung.
Ihre IT-Sicherheit weist Schwächen auf. Beachten Sie: Wenn Ihre IT-Sicherheit zu verbessern und Cyberberater Sie haben nur einen allgemeinen Überblick über das System. Im Folgenden können Sie herausfinden, ob für Ihr Unternehmen besteht - und ob Ihre IT-Sicherheit diesem entspricht.

Ihre Sicherheitsniveau

100%	50%
50%	50%

Haben Sie Ihre Systeme, die über Ihre Unternehmensgrenzen hinweg erreichbar, oder im mobilen Einsatz sind, mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen?
Ihre Antwort: **Trifft nicht zu**

die Mobiliar
Fragebogen Cyber-Schutz Versicherung August 10 2022

Erklärung
Die Fragebogen dient zur Risikobewertung und liefert ein rechtsgültiges Protokoll zur Minderung der Cyberbedrohungen.

Schrittweise zur Unterbrechung und damit Terminrückmeldung in der Summe

Name des Versicherungsnehmers: _____
Adresse: _____
Name des Tochtergesellschaft: _____
Mitarbeiter: _____

Bitte die Rückfragen der einzelnen (Teil-)Fragebogen zur Informationsweitergabe vorlesen. Haben Sie diesen Fragebogen für alle einzelnen zu versichernde Unternehmensbereiche auszufüllen?
 Ja Nein Nicht an Cyber Nicht an der Welt

Sie sind Mängel des Daten

Welche Art und Menge von sensiblen Daten wird in Ihrem Unternehmen gespeichert?
 Finanzdaten Zahlungsdaten Identifikationsdaten Gesundheitsdaten Sonstige Angaben

Art der Daten:
 Personalbezogene Daten Zahlungsdaten Identifikationsdaten Sonstige Angaben

Wozu werden Kundenbeziehungen von Kunden gespeichert in:
 Software IT SA-Werkzeuge Rest der Welt

Wird Kundendaten in die Cloud gespeichert?
 Ja Nein

Beziehen Sie sich auf die Website für E-Commerce oder Online-Service?
 Ja Nein

Zusätzliche, beantwortete Sie nachfolgende Frage:
Wie genau ist die Unternehmens-IT über diese Website geschützt und wie von dieser abhängig ist?
 Ja Nein

Nachfragen Sie Daten durch die Nutzung von Tracking Tools (z.B. durch Google Analytics)?
 Ja Nein

Zusätzliche, beantwortete Sie nachfolgende Frage:
Informieren Sie Besucher Ihrer Webseiten, dass Ihre Daten (z.B. durch Cookies, Skripten) weitergegeben werden können?
 Ja Nein

© Allianz Global Corporate & Specialty AG

Abkehr von der Allgefahenpolice!
Unternehmen, die unsere zwölf Kernkriterien im Underwriting (Risikobewertung und Preisfestsetzung) nicht erfüllen, versichern wir nicht.
Jens Krickhahn, Zuständiger Cybergeschäft,
Allianz Global Corporate & Specialty (FAZ, 10.01.2023)

Risikoeinschätzung



Herausforderung aus Kundensicht



Digital Security
Progress. Protected.

Was ist
das?

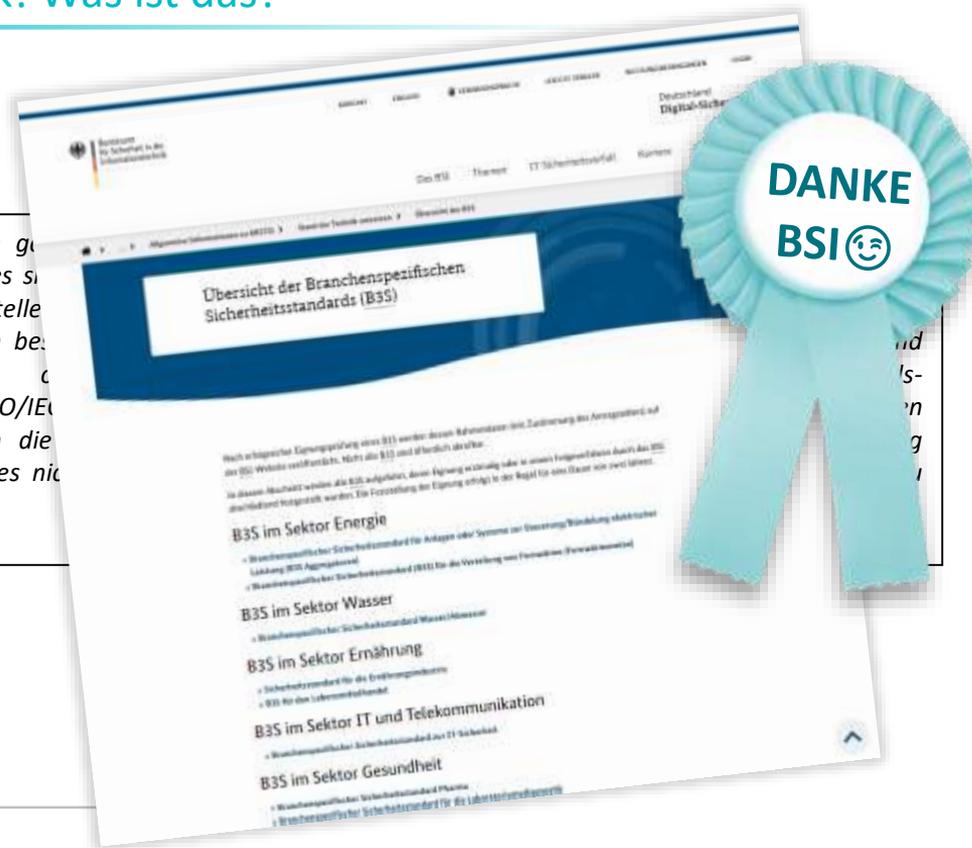
Welche
Herausforderungen?

ESET-
Positionierung

Stand der Technik! Was ist das?

"Stand der Technik" ist ein Begriff, der in der Gesetzgebung verwendet wird, um den aktuellen Stand der Technik abzustellen und festzulegen. Was zu einem bestimmten Zeitpunkt existierender nationaler oder internationaler Normen wie DIN, ISO, DKE oder ISO/IEC im Bereich ermitteln. Da sich die Normen unterscheiden können, ist es nicht

(BSI 2022)



Stand der Technik



Herausforderung aus Kundensicht

„Versicherungsschutz wird nur gewährt für ... Schäden, die TROTZ Beachtung des anerkannten Standes der Technik und Methodik, der Einhaltung branchenüblicher Qualitätssicherungsverfahren (insbesondere Test- und Abnahmeverfahren) oder sonst anerkannter Regeln des Software-Engineerings eingetreten sind.“

„Da sich die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung jedoch unterscheiden können, ist es nicht möglich, den „Stand der Technik“ für die IT-Sicherheit allgemeingültig und abschließend zu beschreiben.“

The screenshot shows a webpage from VDMA (Verband der Maschinen- und Anlagenbauindustrie) with the following content:

- Header:** VDMA logo and navigation menu (HOME, WIRTSCHAFT, BERATUNG, COACHING, VERBANDSVEREINBARUNG, LEISTUNGEN, GEMEINSAM, LEISTUNGSANBIETER).
- Article Title:** „Stand der Technik“ bei Produkthaftpflicht- und Cyberschäden: Ein unbestimmter Rechtsbegriff stellt Versicherungsnehmer vor Beweisprobleme.
- Image:** A photograph showing hands holding and reviewing documents on a desk.
- Text Snippets:**
 - „Der Versicherungsnehmer...“
 - „Stand der Technik“ bei Beweis der Produkthaftpflichtversicherung...
- Right Sidebar:** VDMA-Mitgliedschaft button and a 'Nachrichten-Archiv' list with years from 2000 to 2024.

Stand der Technik



Sichtweise TeleTrust

„Der in dieser Handreichung beschriebene "Stand der Technik" (im Folgenden auch SdT) fokussiert die durch das ITSiG und die DSGVO geforderten Inhalte. Es ist jedoch im Rahmen der IT-Sicherheits- und Datenschutzgesetze zulässig, bei der Auswahl der Schutzmaßnahmen unter anderem auch wirtschaftliche Aspekte zu berücksichtigen . Ob eine Maßnahme wirtschaftlich ist, kann allerdings nur durch individuelle Betrachtung des eigenen Schutzbedarfes sowie der Realisierungskosten erforderlicher Maßnahmen festgestellt werden. Aus diesem Grund wurde in dieser Handreichung auf die Wirtschaftlichkeitsprüfung verzichtet.“

TeleTrust (https://www.teletrust.de/fileadmin/user_upload/2021-09_TeleTrust-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf)



Stand der Technik



IT-Sicherheit bei KMU



Digital Security
Progress. Protected.

NIEDRIGES LEVEL

- AV-Level
- kein Monitoring

- Keine Policy
- Unmanaged
- Small Office / HO

GRUNDSCHUTZ BASIS

- Endpoint-Schutz
- Phishing / Spam
- Firewall

- Device / Web
- Managed
- Small Office / SMB

► Erste Stufe zu Zero-Trust ◀

GRUNDSCHUTZ PLUS

- Verschlüsselung
- Authentifizierung
- Cloud-Sandbox

- Adaptiv
- Automatisiert
- Small Office ► SMB

INNENANSICHT / EDR

- Incident Detection
- Threat Monitoring
- Isolation (IoC)

- Evolutionär
- + Forensik
- SMB ► Enterprise

AUSSENSICHT / TI

- Frühwarnsystem
- Datafeeds
 - Malware
 - Botnets
 - Domains

- Präventiv
- + SIEM / SOC
- Enterprise / KRITIS

ESET Zero-Trust-Reifegradmodell

ESET PORTFOLIO

Datafeeds + APT-Reports
ESET Threat Intelligence

Endpoint Detection & Response
On-Premises: ESET Inspect*
Cloud: ESET Inspect Cloud*

Managed Detection & Response
ESET Security Services

Cloud-Sandboxing
ESET LiveGuard Advanced

Microsoft 365 Bedrohungsschutz
ESET Cloud Office Security*

Verschlüsselung
ESET Endpoint Encryption*
ESET Full Disk Encryption

Multi-Faktor-Authentifizierung
ESET Secure Authentication*

Schutz von Clients & Mobilgeräten
ESET Endpoint Security
ESET Endpoint Antivirus

Schutz von Fileservern
ESET Server Security

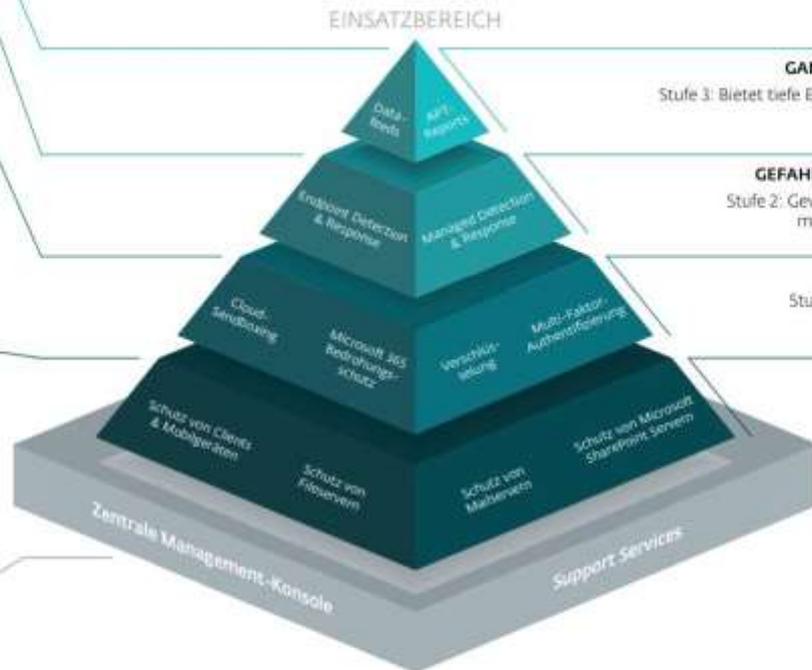
Schutz von Mailservern
ESET Mail Security

Schutz von Microsoft SharePoint Servern
ESET Security for Microsoft SharePoint Server

Zentrale Management-Konsole
On-Premises: ESET PROTECT
Cloud: ESET PROTECT Cloud

Support Services
Technischer Support: [eset.help](#)
ESET Premium Support
ESET Upgrade & Deployment
ESET Healthcheck

*Verwaltung über separate Management-Konsole



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



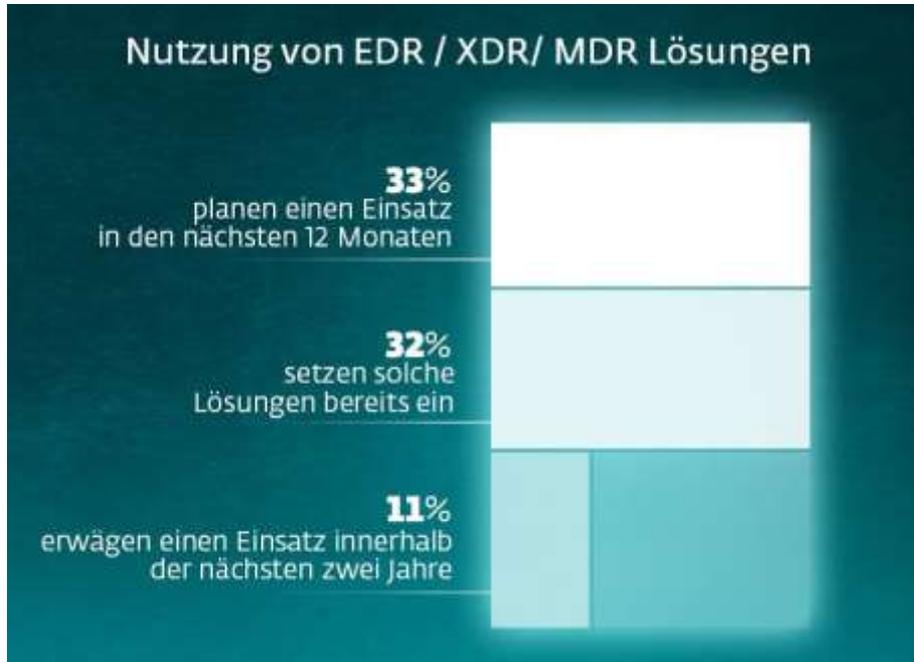
Digital Security
Progress. Protected.

Deutschland

Größenklasse	Unternehmen	Beschäftigte
Mikrounternehmen	2.061.145	5.010.646
Kleine Unternehmen	346.934	6.903.924
Mittlere Unternehmen	62.217	7.102.841
KMU	2.470.296	19.017.411
Große Unternehmen	15.507	15.914.748
Gesamt	2.485.803	34.932.159 Normalarbeitneh.

Größenklasse	Tätige Personen	Jahresumsatz
Kleinstunternehmen	bis 9	und bis 2 Mill. EUR
Kleine Unternehmen	bis 49	und bis 10 Mill. EUR
Mittlere Unternehmen	bis 249	und bis 50 Mill. EUR
Großunternehmen	über 249	oder über 50 Mill. EUR

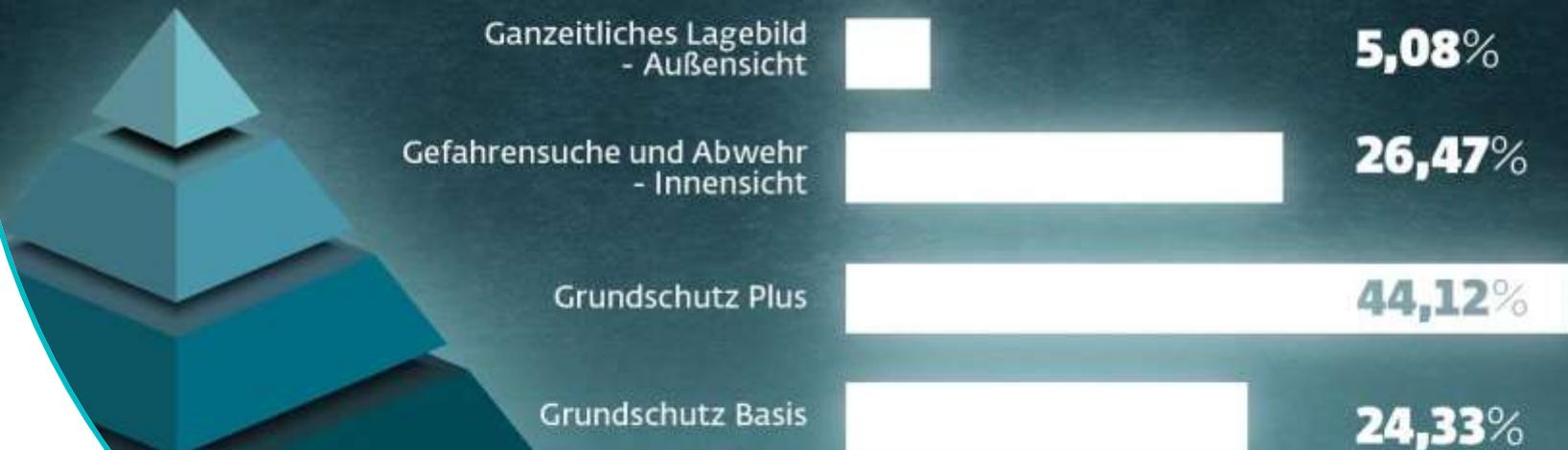
ESET CYBERSICHERHEITSLAGE-UMFRAGE



„26,5% der Verantwortlichen setzen heute bereits eine EDR-Lösung ein. Davon: 18,2% in Verbindung mit Managed Detection und Response Services“

ESET PM-Umfrage ZeroTrust Deutschland

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



*„Lediglich **14,44%** der Befragten sind sich sicher, dass Sie mit Ihrem derzeitigem Schutzlevel den aktuellen Bedrohungen gewachsen sind“*

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)



Maik Wetzel

Strategic Business Development Director DACH



Telefon: +49 3641 3114 211
Mobil: +49 151 401 037 04
maik.wetzel@eset.com

www.eset.de

ESET Deutschland GmbH
Spitzweidenweg 32
07743 Jena
Deutschland



Digital Security
Progress. Protected.