Cybersicherheit - Großwetterlage

Game Changer Zeitenwende?

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

Digital Security
Progress. Protected.

Maik Wetzel

Strategic Business
Development Director DACH
- ESET Deutschland GmbH -

ÜBER ESET

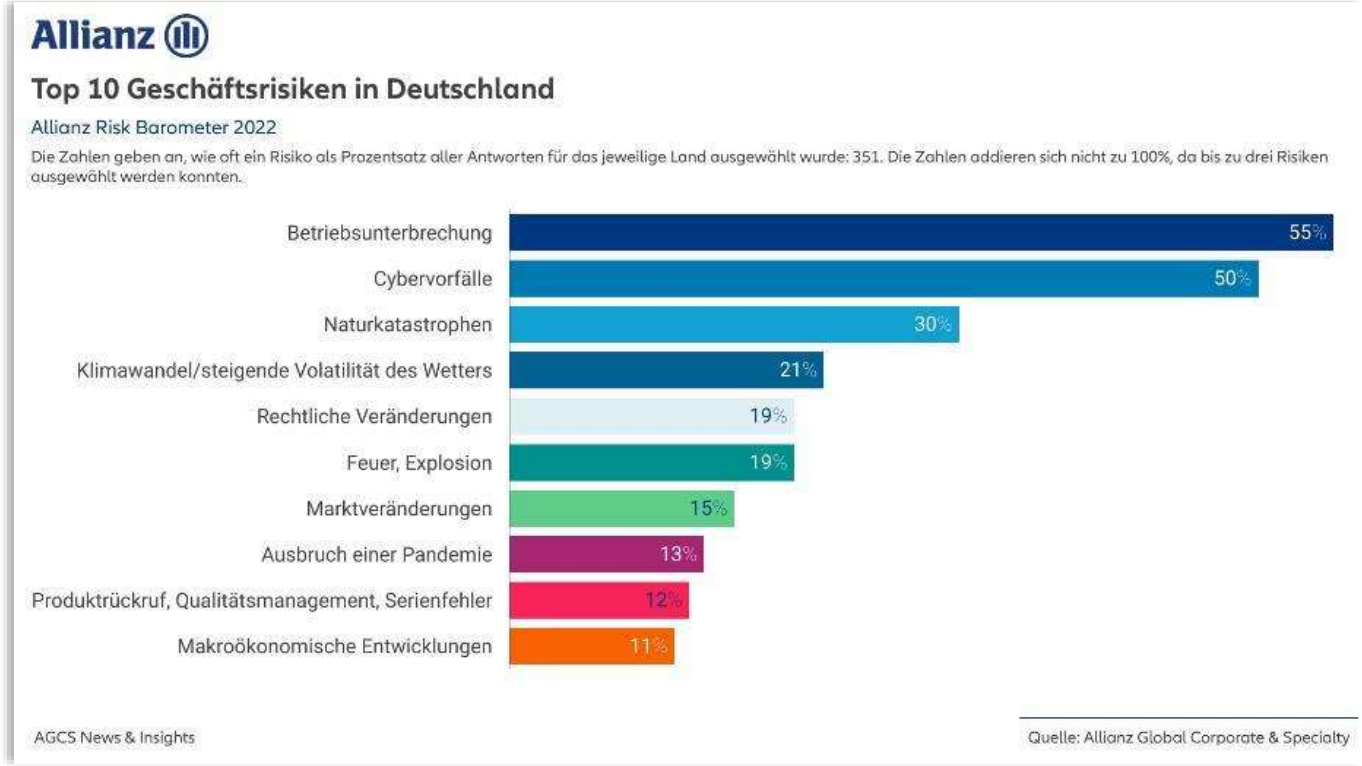
- #1 EU-Hersteller IT-Security
- unabhängig, inhabergeführt
- 1992 gegründet
- HQ in Bratislava, weltweite Präsenz (21 Niederlassungen, 13 R&D Zentren)
- ca. 110 Mitarbeiter in Deutschland (Jena/München)
- ca. 2.000 Mitarbeiter global
- ca. 6.500 qualifizierte Reseller (IT-Dienstleister) in Deutschland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

Cybersicherheit – Status Quo

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



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:

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

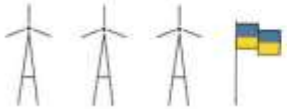
116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden

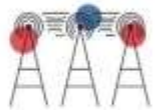
nach Angriff auf Satelliten-kommunikation



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

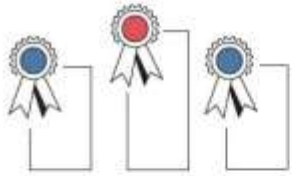
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

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·

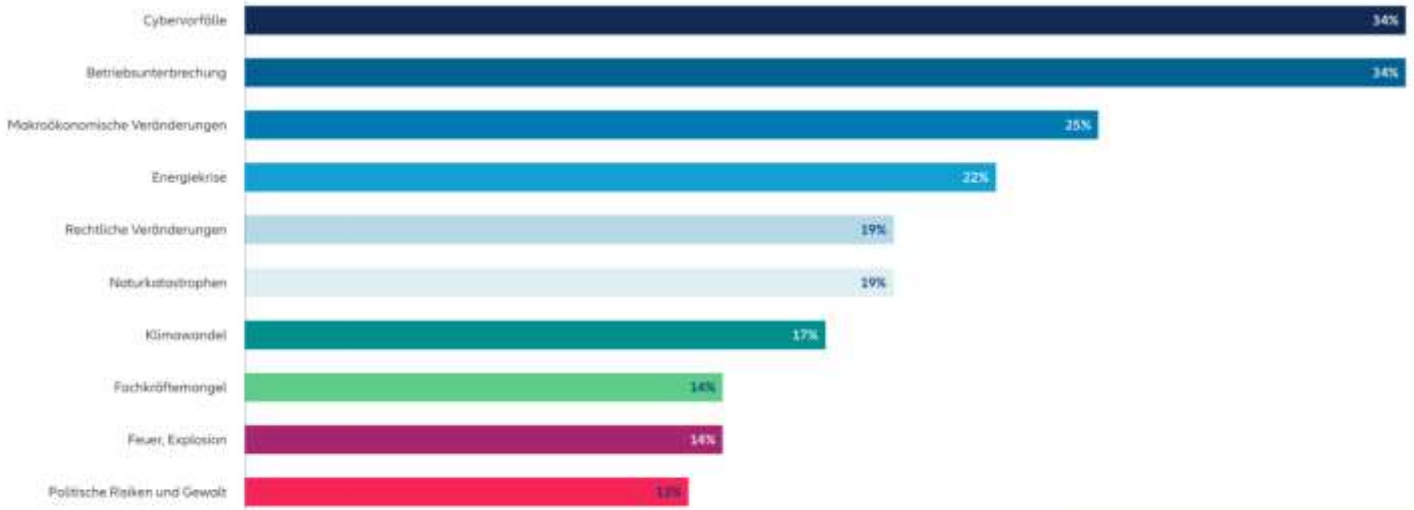
ALLIANZ RISK BAROMETER 2022

Allianz

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.

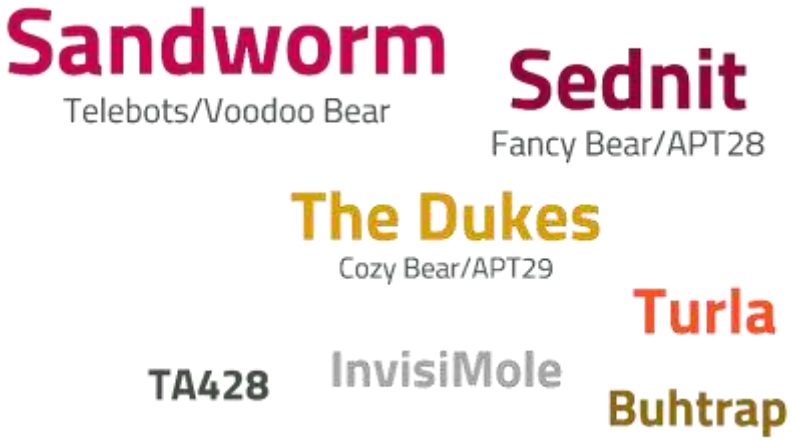


AGCS News & Inisghts

Source: Allianz Global Corporate & Specialty

Cyberwar in der Ukraine

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

Turla

Gamaredon

FSB

The Dukes

Cozy Bear/APT29

SVR

Sandworm

Telebots
/Voodoo Bear

GRU

Sednit

Fancy
Bear/APT28

Sources:

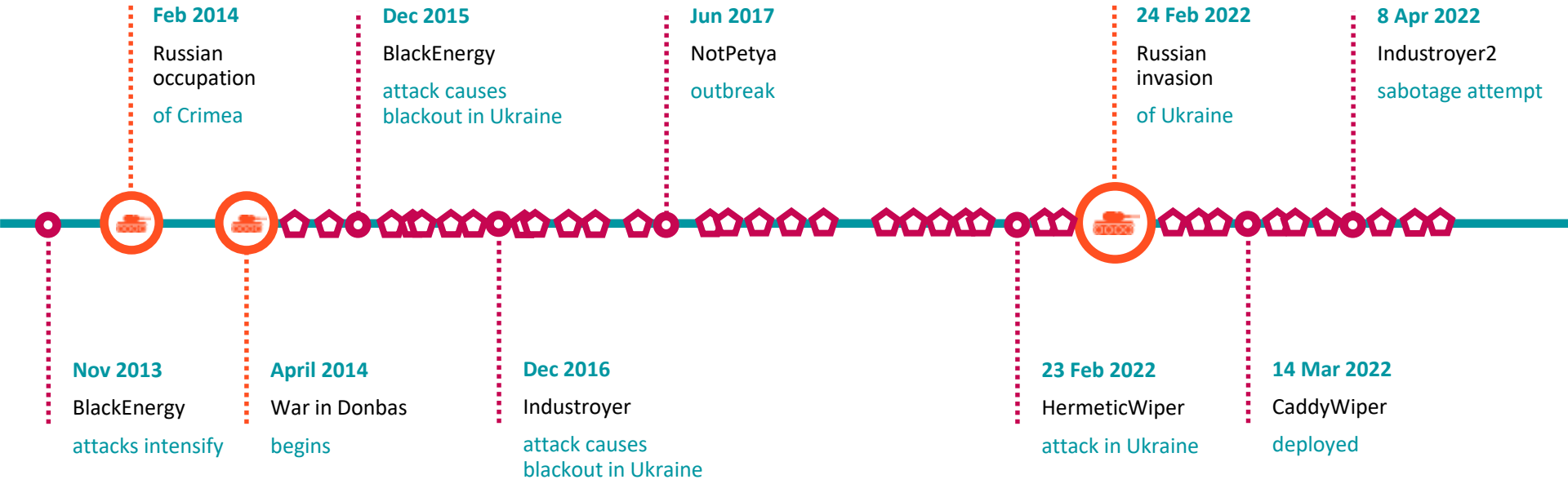
FBI

National Cyber Security Centre

Militaire Inlichtingen en Veiligheidsdienst

SECURITY SERVICE OF UKRAINE

Microsoft


Feb 2014
Russian occupation of Crimea
Dec 2015
BlackEnergy attack causes blackout in Ukraine
Jun 2017
NotPetya outbreak
24 Feb 2022
Russian invasion of Ukraine
8 Apr 2022
Industroyer2 sabotage attempt
Nov 2013
BlackEnergy attacks intensify
April 2014
War in Donbas begins
Dec 2016
Industroyer attack causes blackout in Ukraine
23 Feb 2022
HermeticWiper attack in Ukraine
14 Mar 2022
CaddyWiper deployed

Was uns 2023ff beschäftigen wird

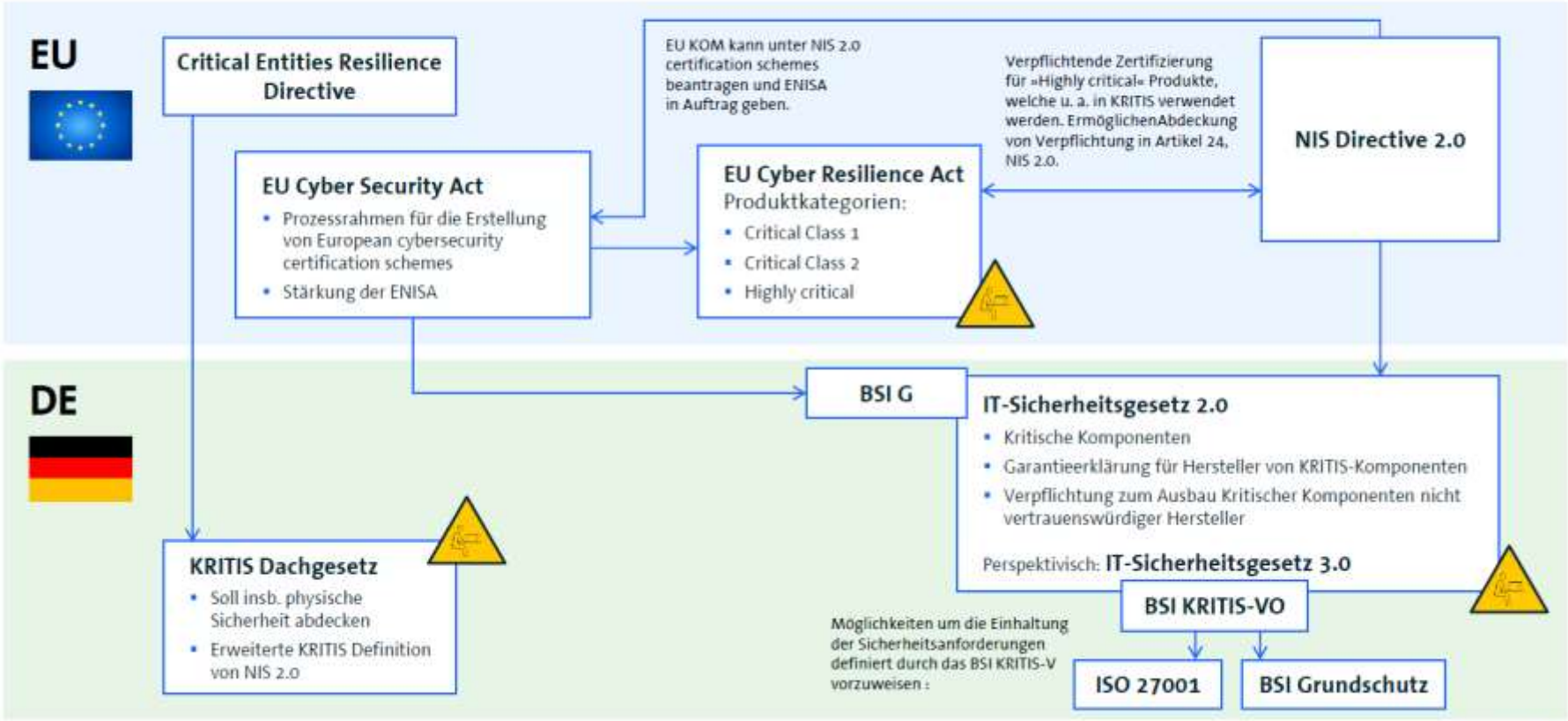
REGULIERUNG

- 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



bitkom

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

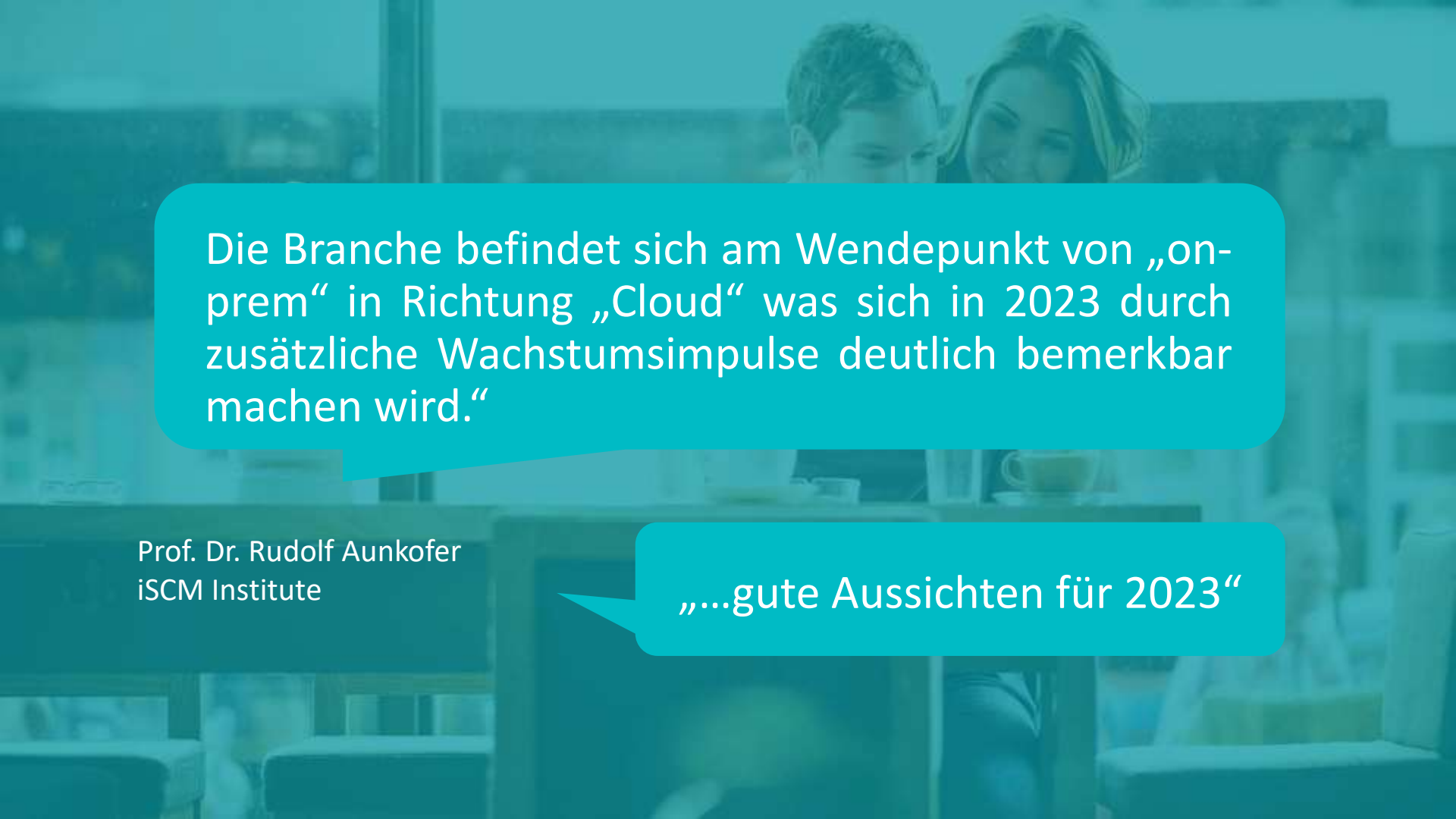
DIGITALPOLITISCHE ZIELE BIS 2025

- 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

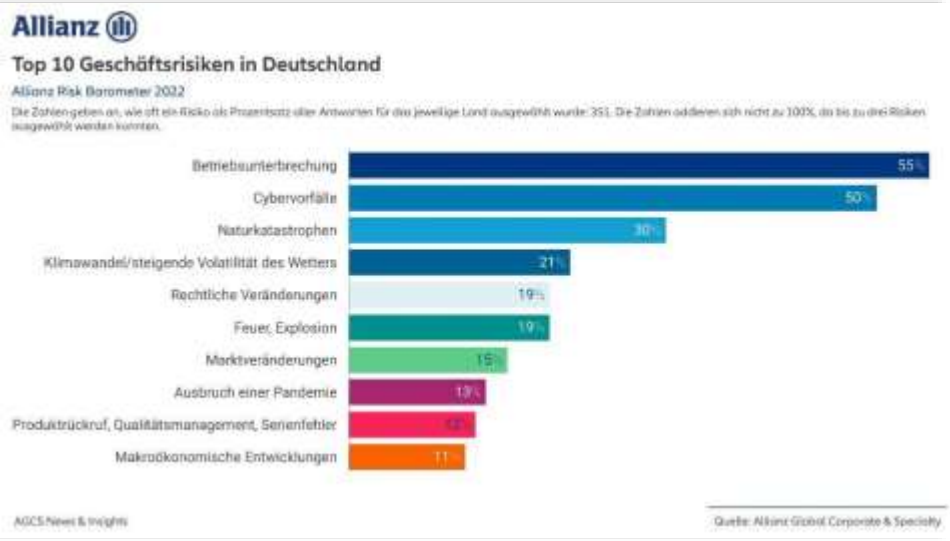
- Cybersicherheit modernisieren und harmonisieren
- Cyberfähigkeiten und Digitale Souveränität der Sicherheitsbehörden stärken
- Cybercrime und strafbare Inhalte im Internet bekämpfen
- Cybersicherheit der Behörden des Bundes stärken
- **Cyber-Resilienz Kritischer Infrastrukturen stärken**
- Schutz ziviler 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)
Jährliche Wachstumsrate: 10,5%
5,7
6,9
7,8
8,5
9,4
10,3
2020
2021
2022
2023
2024
2025
Quelle: Bitkom
statista

Stand der Technik und Cyber-Versicherung

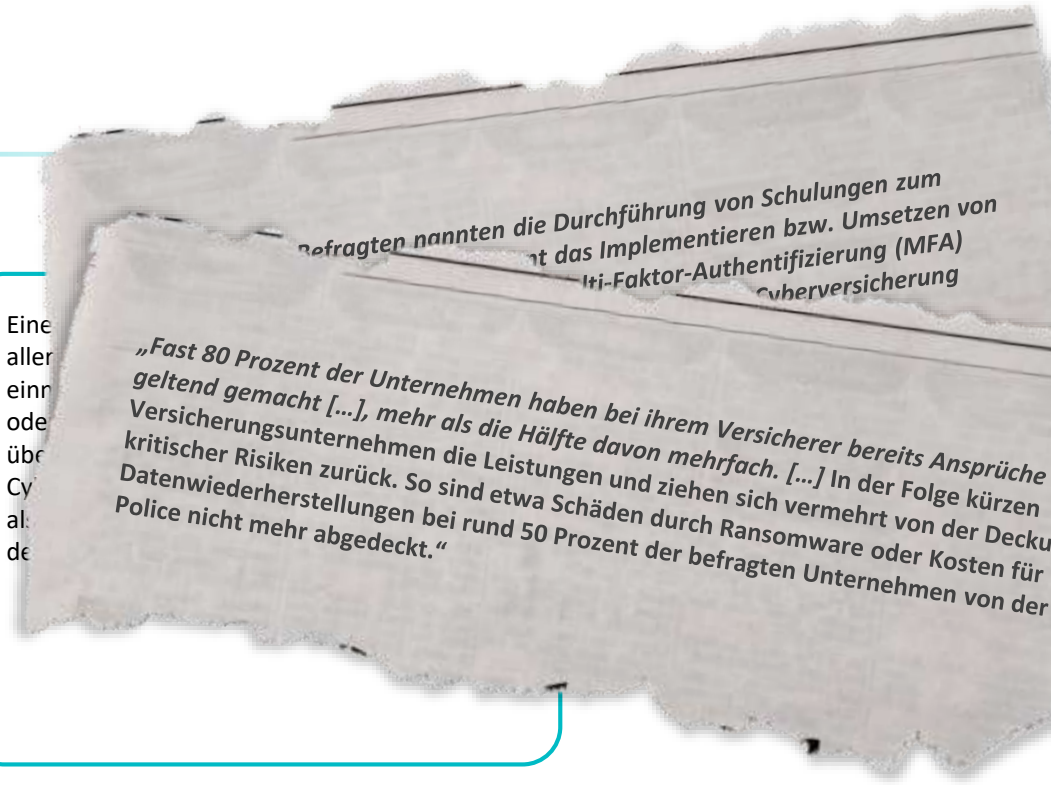
ALLIANZ RISK BAROMETER 2022/2023



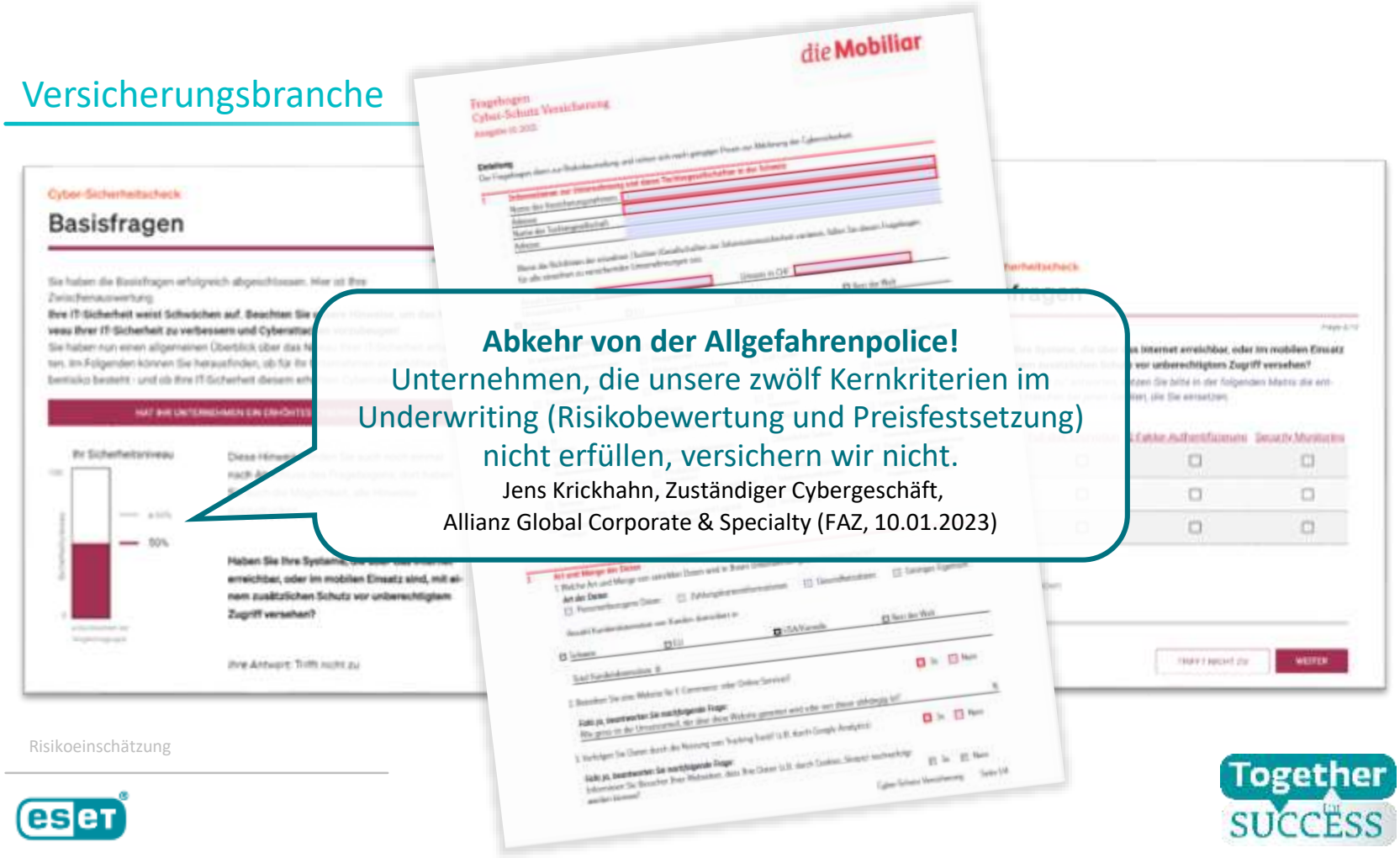
Versicherungsbranche

„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
einr
ode
übe
Cy
al
de



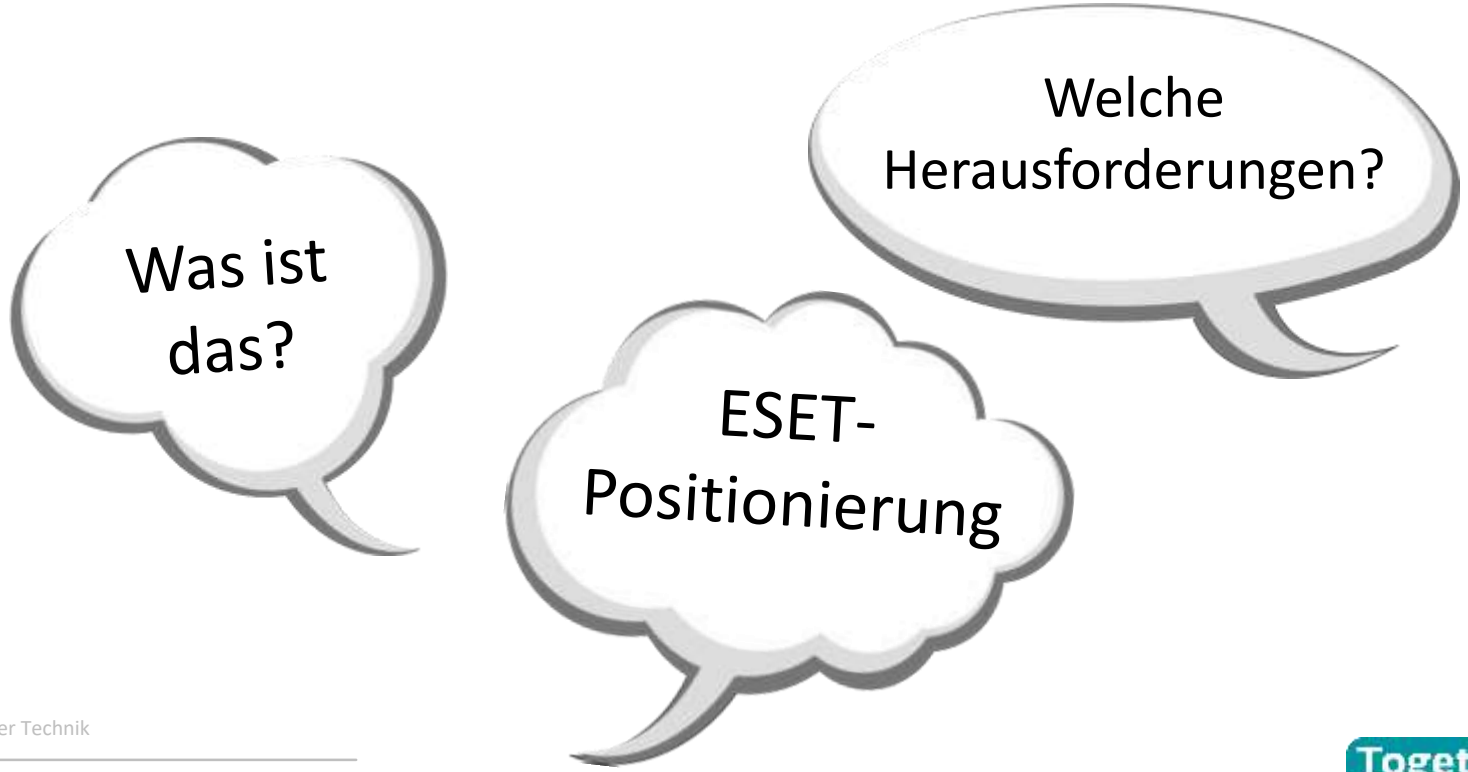
Versicherungsbranche



Risikoeinschätzung

Herausforderung aus Kundensicht

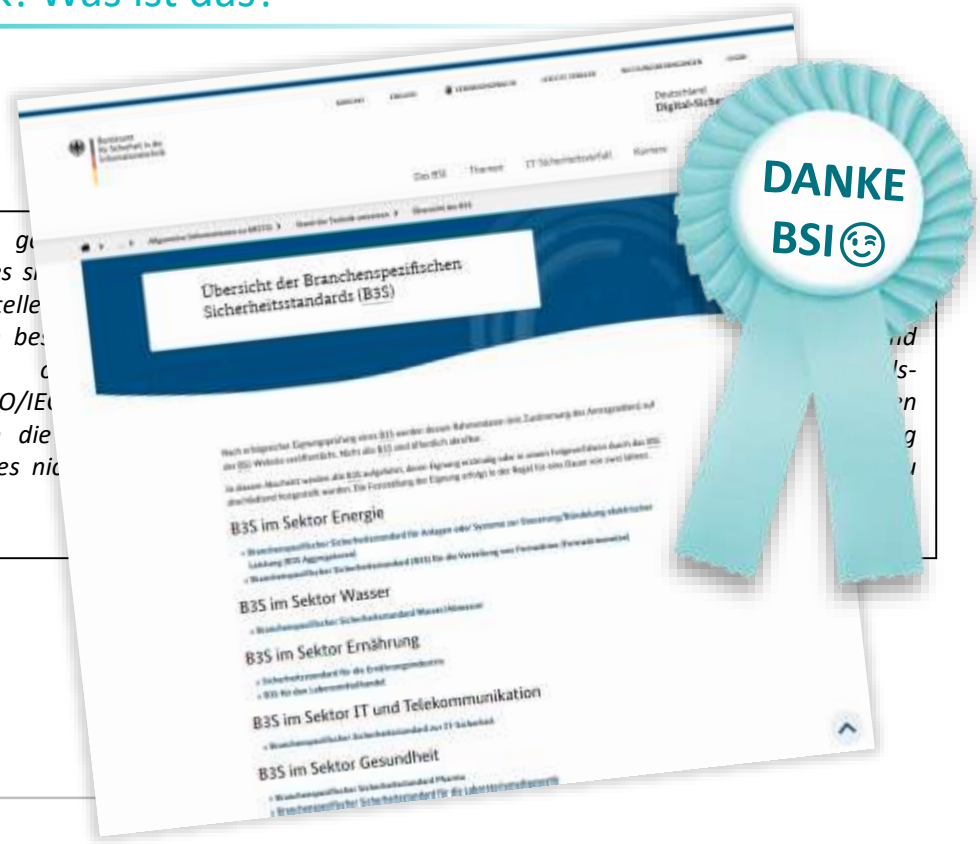
Stand der Technik



Stand der Technik! Was ist das?

Stand der Technik" ist ein g
Gesetzgebung. Daher hat es s
"Stand der Technik" abzustelle
festzulegen. Was zu einem be
existierender nationaler
weise DIN, ISO, DKE oder ISO/IE
Bereich ermitteln. Da sich die
unterscheiden können, ist es ni

(BSI 2022)



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.“

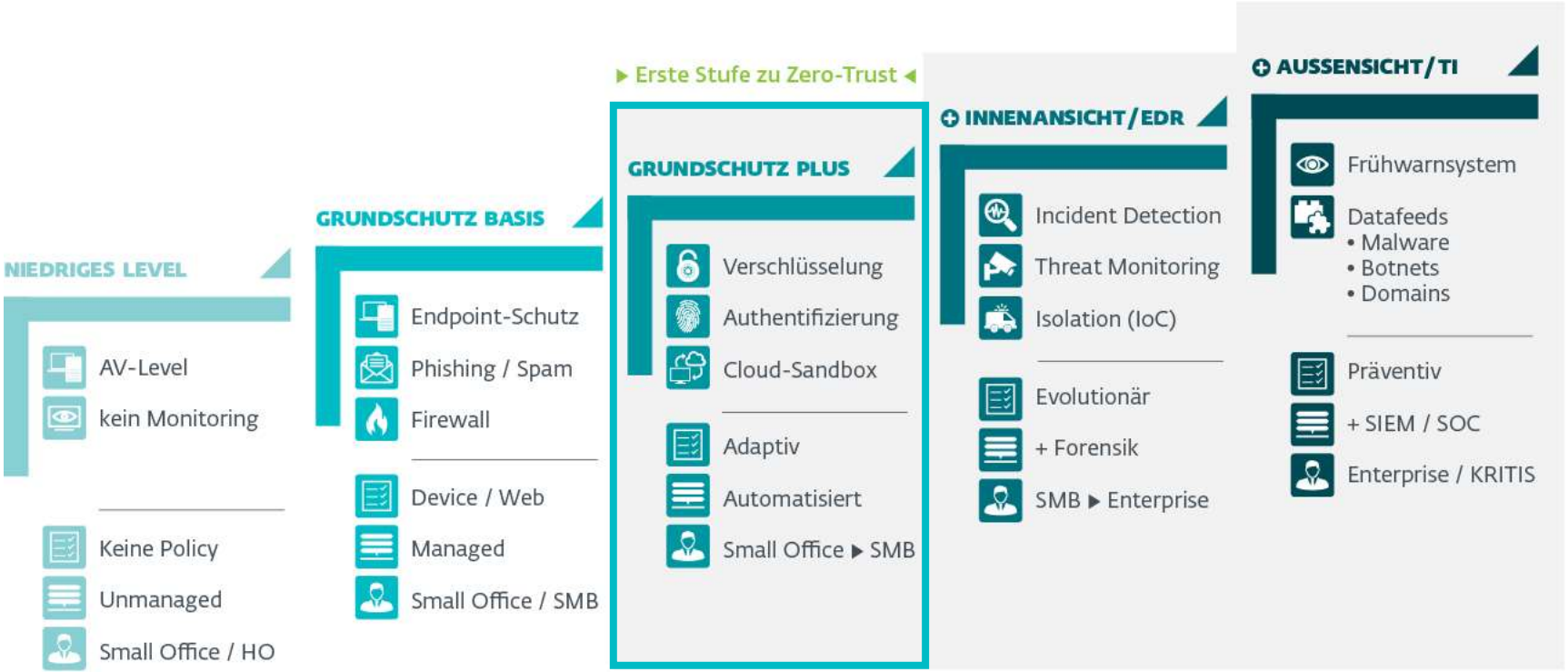
„Da sich die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung jedoch unterscheiden können, ist es nicht möglich, den **„Stand der Technik“ für die IT-Sicherheit allgemeingültig und abschließend zu beschreiben.“**

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)

IT-Sicherheit bei KMU



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

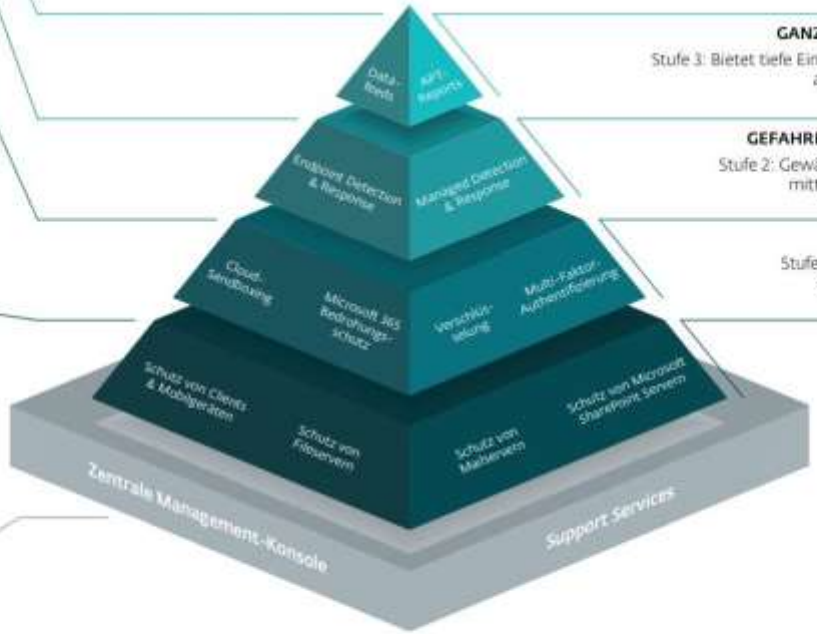
Schutz von Microsoft SharePoint Servern
ESET Security for Microsoft SharePoint Server

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

Support Services
Technischer Support
ESET 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.

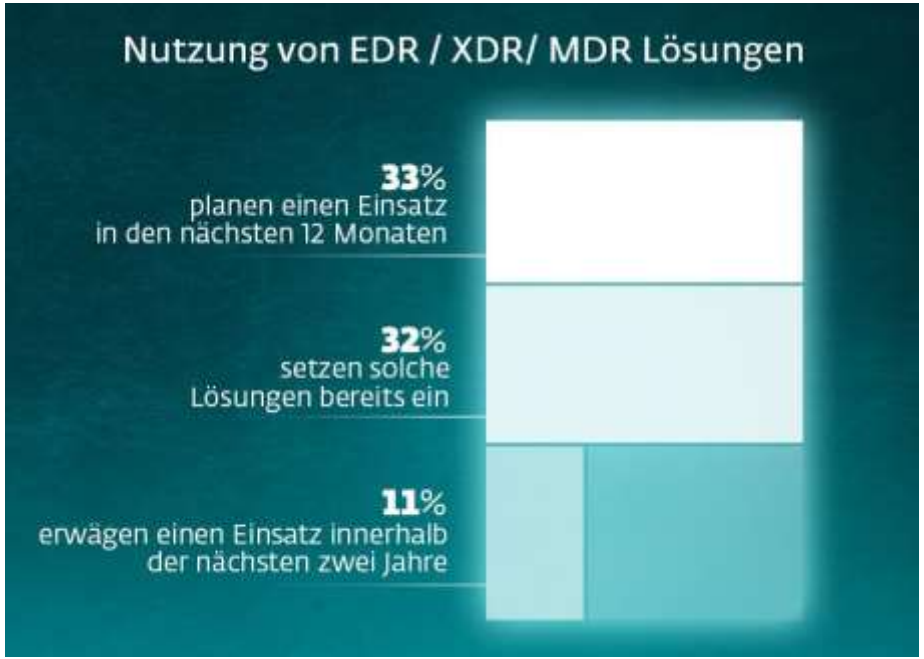
ESET.DE | ESET.AT | ESET.CH

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?

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

Endkunden & Reseller

*„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

ENJOY SAFER TECHNOLOGY™

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.