NIS2-Umsetzung in Deutschland

Gamechanger oder Rohrkrepierer?

Digital Security
Progress. Protected.

Maik Wetzel

Strategic Business Development Director DACH
- ESET Deutschland GmbH -

Digital Security
Progress. Protected.

Vorstellung

Über ESET

Digital Security
Progress. Protected.

★ EU-Hersteller ★
★ Technologieführer ★
★ Mehr als 30 Jahre Erfahrung ★

30 Jahre Erfahrung
Made in EU

Cyber-sicherheits-lösungen

Passgenau und flexibel

Zentral verwaltet

UNABHÄNGIG
INHABERGEFÜHRT
WERTEBASIERT

Breites Händlernetz

Trainiert + Zertifiziert

Unterstützt durch Support aus DE

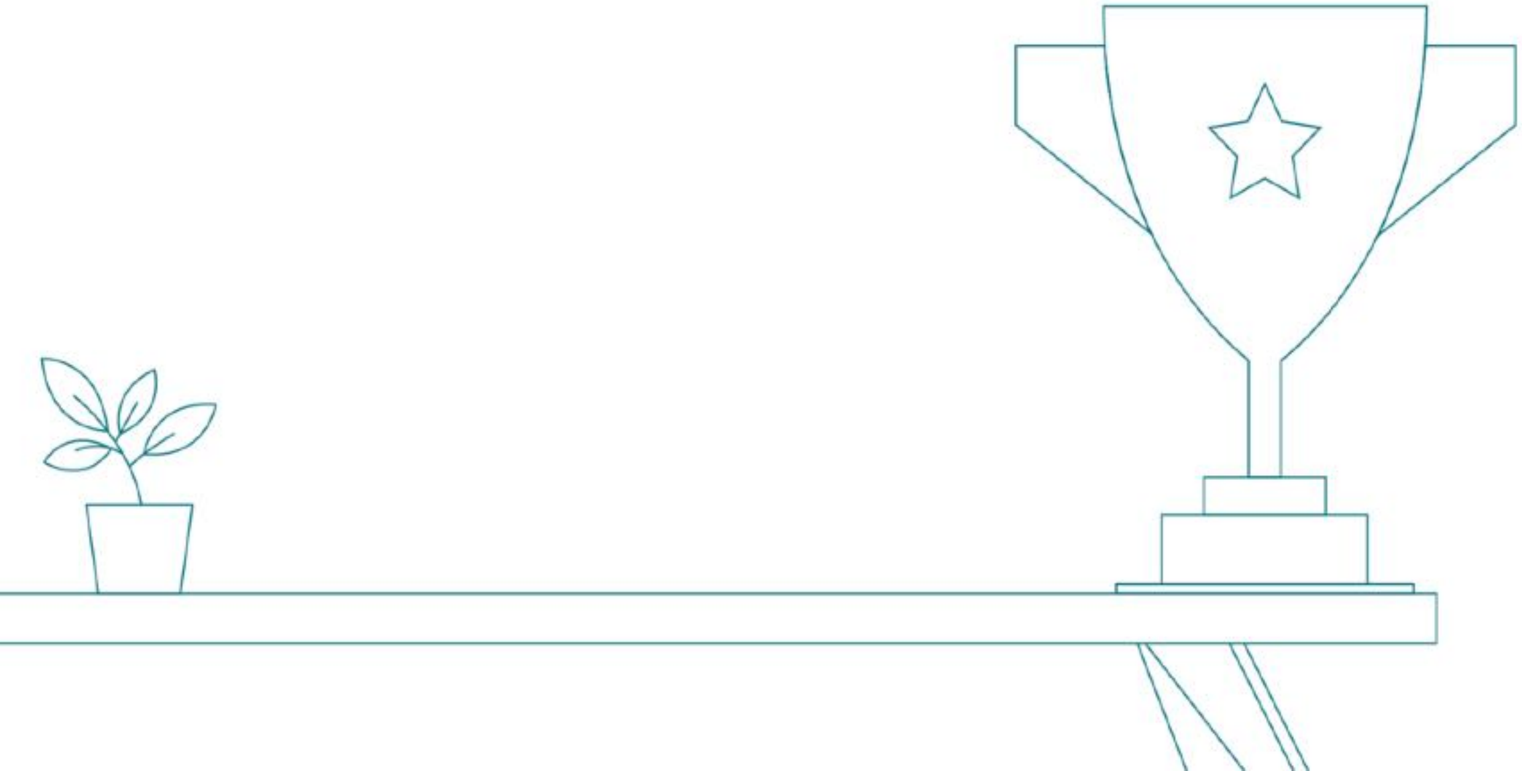
Vielfach ausgezeichnet

kontinuierliche Produktqualität

ESET®

Digital Security
Progress. Protected.

Nr. 1 der Cybersecurity-Unternehmen **in der EU**



Digital Security
Progress. Protected.

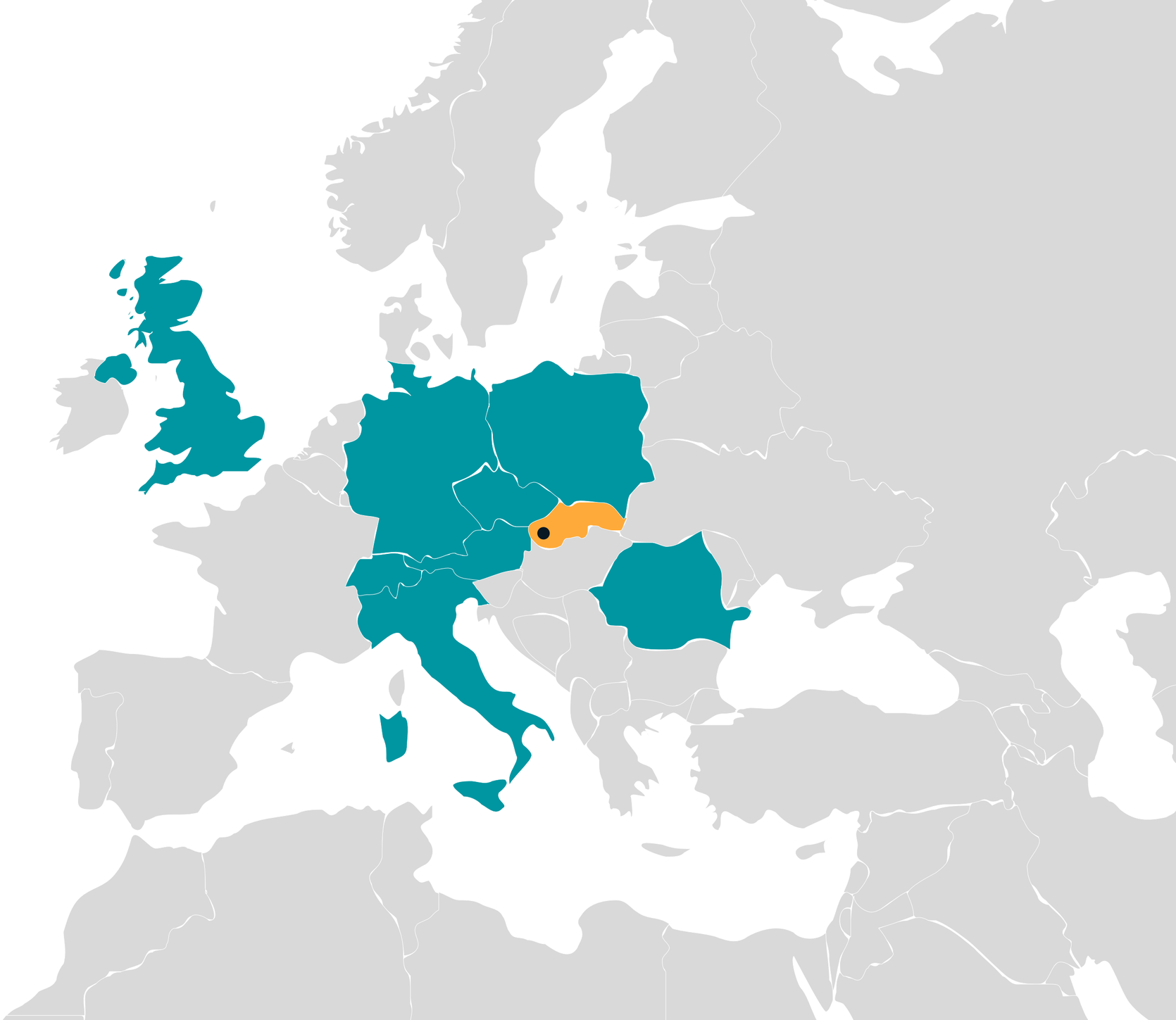
Über ESET

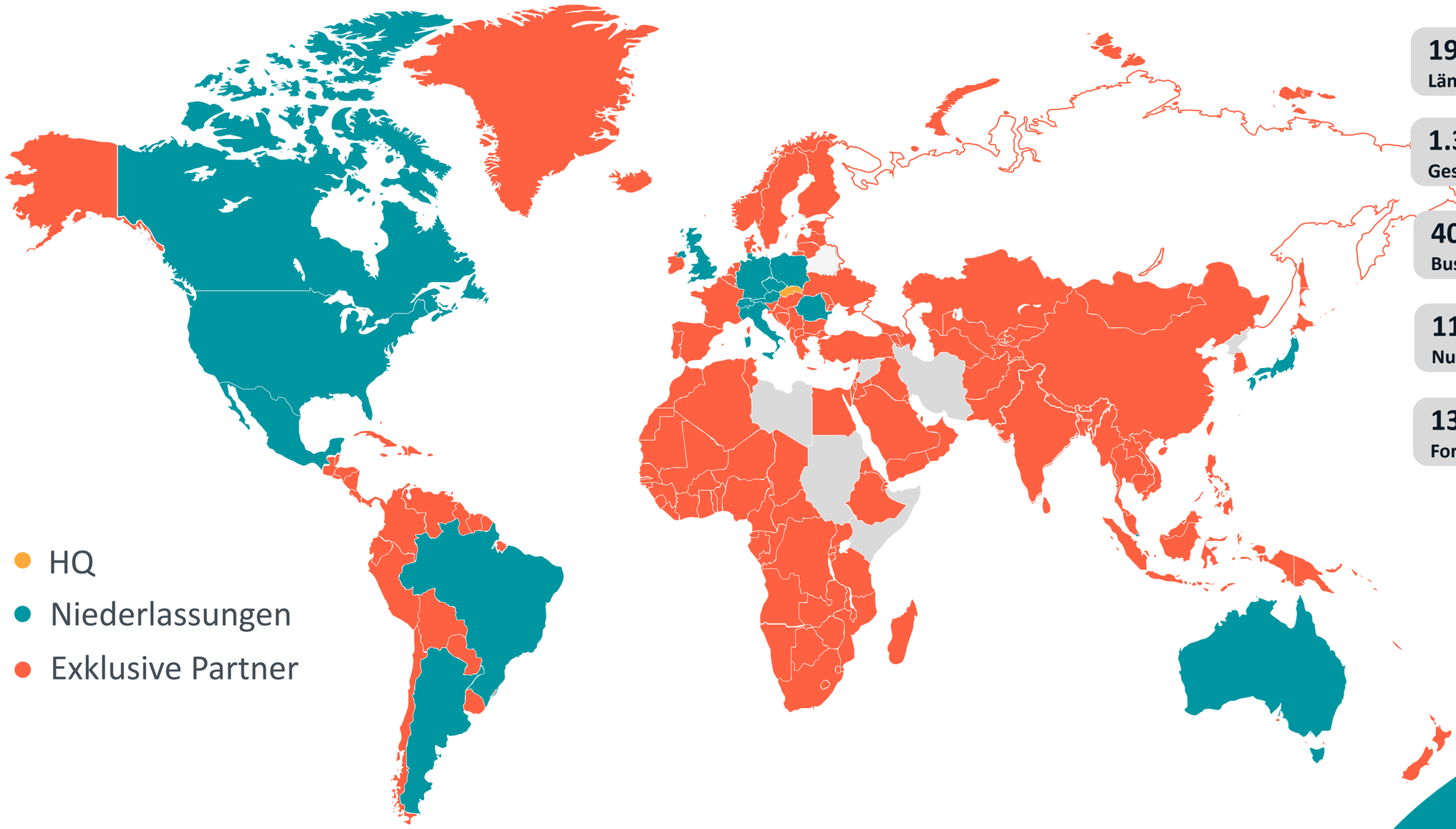
INNOVATION
SEIT 1987

Eigenentwicklung unserer Technologien und Lösungen mit reinem Fokus auf die Sicherheit unserer Kunden

Digital Security
Progress. Protected.

Im Herzen Europas





195+
Länder & Regionen

1.300.000.000+
Geschützte Internetnutzer

400.000+
Business-Kunden

110.000.000+
Nutzer

13
Forschungs- und Entwicklungszentren

eset® Digital Security
Progress. Protected.

Über ESET


Canon
MITSUBISHI MOTORS
SPARTA ROTTERDAM
HAWK-EYE INNOVATIONS
BVB 09
StaDt Wien

SPAR

Marienhospital
Bottrop
gGmbH

GRENZEBACH

kohlpharma

StaDt
Wien

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 / Life Demo
8. Q&A

Status Quo

Digital Security
Progress. Protected.

(wichtigste) gesetzliche Grundlagen

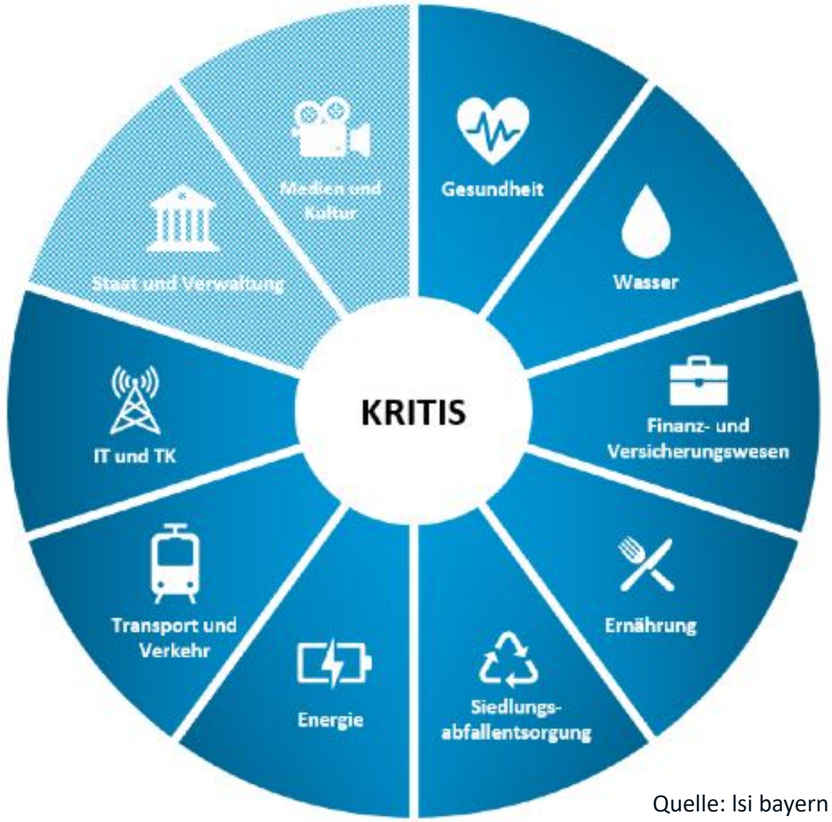
BSI-Gesetz / IT-Sicherheitsgesetz (IT-SIG 2.0) – seit Mai 2021

- Regulierung zur Erhöhung der IT-Sicherheit bei KRITIS
- Definition von Mindeststandards für KRITIS und Bundesbehörden
- Pflichten für KRITIS-Betreiber

BSI-Kritisverordnung (BSI-KritisV) – konkretisiert das IT-SIG

- **Schwellenwerte** (heute ca. 5.000 Unternehmen betroffen)
- Anlagen zur Umsetzung

Sektorspezifische Regulierung (z.B. DORA, EnWG)



Quelle: lsi bayern

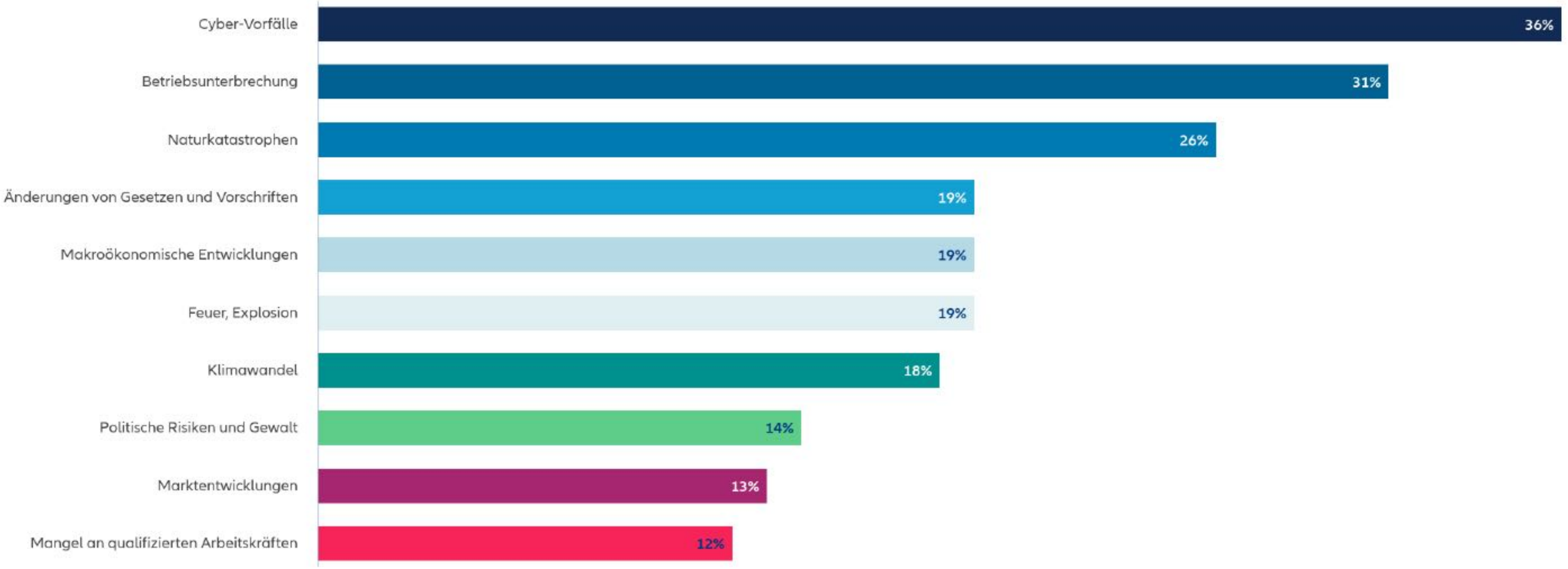
Bedrohungslage

- Lage ist kritisch
- **Bedrohung im Cyberraum so hoch wie nie zuvor**
- Cyber-Erpressungen sind größte Bedrohung
- Qualität und Anzahl der Angriffe nahmen beträchtlich zu
- Umgang mit Schwachstellen bleibt eine der größten Herausforderungen
- Social Engineering großes Thema
- **Arbeitsteilung und Professionalisierung auf Seite der Angreifer**
- Cybercrime as a Service
- Geopolitische Zeitenwende führt zu weiterer Verschärfung
- Staatlich gelenkte Akteure
- **„Hybride Bedrohungslage“**
- **Zunehmend Angriffe auch gegen kleine und mittlere Organisationen**
- Lageveränderung jederzeit möglich
- Schaden der Wirtschaft pro Jahr 223 Mrd. Euro (Bitkom)

Top 10 Geschäftsrisiken weltweit in 2024

Allianz Risk Barometer 2024

Basierend auf den Antworten von 3,069 Risikomanagement-Experten aus 92 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



Allianz Commercial News & Insights

Source: Allianz

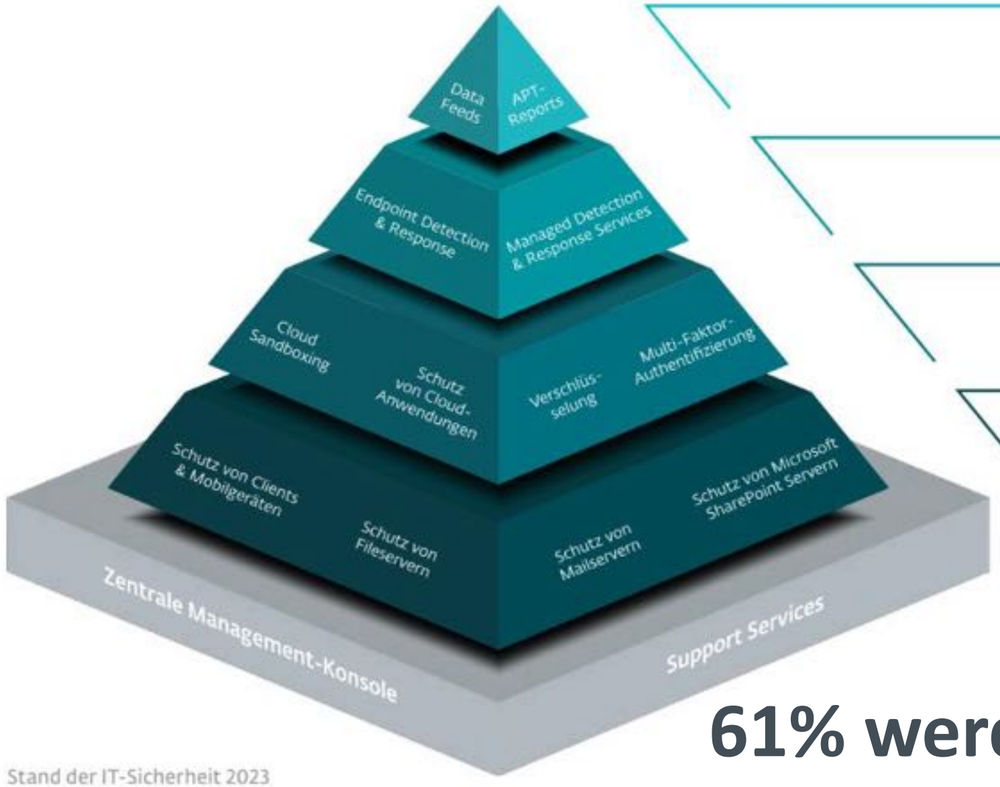
Stand der IT-Sicherheit 2024 - erste exklusive Ergebnisse

355

374 Teilnehmer

eset Digital Security
Progress. Protected.

Stand der IT-Sicherheit 2024 - Selbsteinschätzung



Stand der IT-Sicherheit 2023

EINSATZBEREICH	2023	2024	SCHUTZLEVEL
	5,1%	9,0%	GANZHEITLICHES LAGEBILD – AUSSENSICHT Stufe 3: Bietet tiefe Einblicke in die globale Bedrohungslandschaft als Grundlage für einen SOC-/SIEM-Betrieb
	26,5%	29,6%	GEFAHRENSUCHE UND ABWEHR – INNENSICHT Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalieerkennung, Schwachstellenanalyse und Incident Management
	44,1%	42,5%	GRUNDSCHUTZ PLUS Stufe 1: Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero Days
	24,3%	18,9%	GRUNDSCHUTZ BASIS Stufe 0: Mindestabsicherung für Endgeräte und Server

Entwicklung

61% werden den Anforderungen der NIS 2 somit nicht gerecht! (kein ausreichender Schutz)

Digital Security
Progress. Protected.

Stand der IT-Sicherheit 2024 - Veränderungen zum Vorjahr

75% → **88%**

sind aktuell überzeugt, dass IT-Security den richtigen Stellenwert in ihrer Organisation einnimmt

14% → **20%**

sehen sich aktuellen Bedrohungen gegenüber vollumfänglich gewappnet

47% → **64%**

beklagen einen Mangel an Personal und/oder finanziellen Ressourcen

91% → **93%**

empfinden Zero Trust Security als Orientierungshilfe zur Umsetzung nützlich

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

EU-Regulierung / Standardisierung des Digitalmarktes

- EU NIS 2.0
- EU RCE/CER (Critical Entities Resilience Directive)
- EU Cyber Resilience Act
- EU Cyber Solidary Act
- EU Cyber Security Act
- EU Data Act
- EU Digital Markets Act
- EU AI Act
- EU Digital Operational Resilience Act
- EU Digital Service Act
- EUCC
- EUCS

Was ist neu?

Digital Security
Progress. Protected.

Basics

- Definition von **Mindeststandards für Cybersicherheit**
- 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**
- **Sektorspezifische Vorschriften** und DSGVO gelten vorrangig
- 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 - Referentenentwurf

Risikomanagementmaßnahmen müssen:

- auf einem gefahrenübergreifenden Ansatz beruhen,
- dem bestehenden (festgestellten) Risiko angemessen sein,
- 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…

- **Registrierung beim BSI (§33 NIS2UmsuCG)**
- **Nachweispflichten, Prüfung, Information**
    a. Besonders wichtige Einrichtungen und Betreiber kritischer Anlagen
    – Audits, Zertifizierungen, Prüfungen (ex-ante)
    – Compliance muss alle 2 Jahre nachgewiesen werden
    – Random Checks, Security Scans
    b. Wichtige Einrichtungen
    – Registrierung ohne Nachweise und Audits
    – Ex-post Prüfungen (Stichproben)
- **Unterrichtspflichten (§35 NIS2UmsuCG)**
    – Generell bei erheblichen Sicherheitsvorfällen
    – Information aller Empfänger der Dienste der Einrichtung (Kunden) über Vorfall und Abhilfemaßnahmen
- **Meldepflichten (CSIRT, BSI)**
    – Frühwarnung nach 24 Stunden (ab Kenntnisnahme)
    – innerhalb von 72 Stunden eine Folgemeldung, u.a. mit erster Bewertung des Sicherheitsvorfalls und Indikatoren der Kompromittierung
    – Zwischenbericht auf Anfrage mit Status-Update (ohne Zeitangabe)
    – Abschlussbericht nach spätestes einem Monat nach Folgemeldung

Leitungsorgane

Risikomanagement in wesentlichen und wichtigen Einrichtungen:

- Verantwortlichkeit liegt bei den Leitungsorganen
  - Risikomanagementmaßnahmen zu 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 chem. 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)	
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

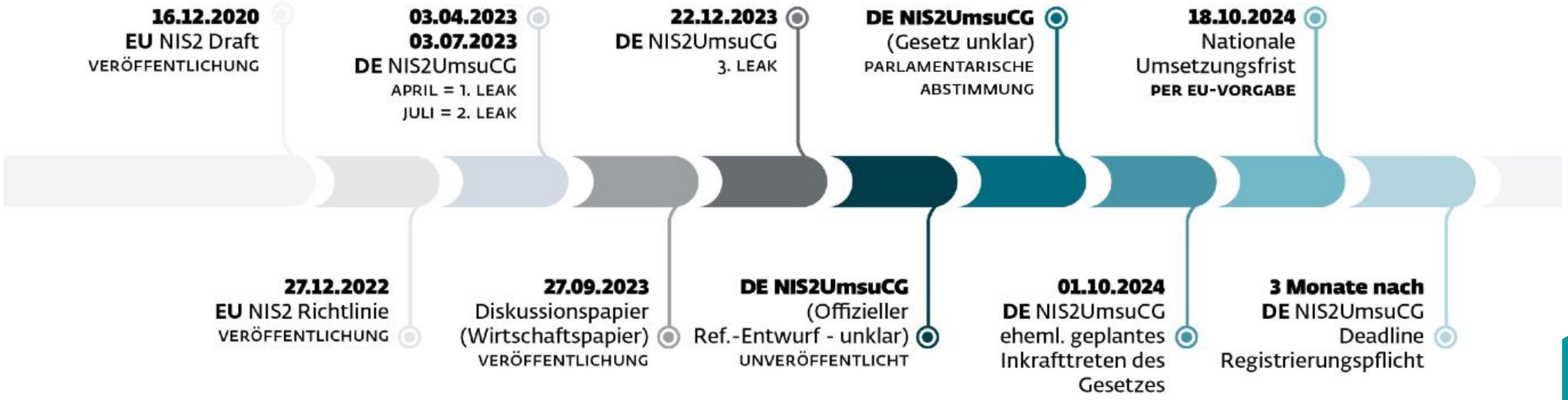
Qualifizierende Faktoren, z.B.:

- Kritische Tätigkeit
- Auswirkung auf öffentliche Ordnung
- Systemrisiken
- Grenzüberschreitende Auswirkungen

Nationale Umsetzung

Digital Security
Progress. Protected.

Roadmap NIS2-Umsetzung



Offizieller Referentenentwurf vom 07.05.2024

- Umsetzungsfrist (17.10.2024) wird definitiv gerissen
- Für Bedenken des AA scheint ein konstruktiver Ansatz gefunden
    - Beurteilung und Einordnung außenpolitischer Aspekte von Cybersicherheits- und Informationssicherheitsvorfällen
    - Sicherheit der Auslandsnetze des Bundes (Zuständigkeit)
- Bedenken BMJ offen, Zustimmung BMJ offen
    - Unabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik (BSI) und geplante Schwachstellenmanagement
- Bundesfinanzministerium (BMF) hat ebenfalls Vorbehalte aufgegeben
    - Erfüllungsaufwand auf staatlicher Seite (Bund)
- realistischer Zeitpunkt für die NIS-2-Umsetzung wird nicht genannt
- Verbändebeteiligung / Stellungnahmen bis 28. Mai 2024
- Verbändeanhörung am 03. Juni 2024

Erfüllungsaufwand

Erfüllungsaufwand Bund:

- Einmalig: 286 Mio Euro
- Jährlich: 209 Mio Euro

Erfüllungsaufwand Wirtschaft:

- Einmalig: 1,37 Mrd Euro
- Jährlich: 2,3 Mrd Euro

Handlungsempfehlung

Digital Security
Progress. Protected.

Ganz schön dickes Brett! Und nun?

- Anfangen!!!!
- Fragen beantworten: ist mein Unternehmen/mein Kunde betroffen? Verändert sich mein/sein Status?
- Hilfe und Beratung suchen?
- Zukünftige Verpflichtungen ableiten
- Maßnahmen planen
- Umsetzung beginnen
- Anpassungen im Bereich von (vorhandenen) Versicherungen erfolgt / erforderlich?

⇒ Pflichten identifizieren!
⇒ Umsetzungsfristen beachten!
⇒ Budgets planen
⇒ Maßnahmen einleiten

Stand der Technik – Compliance

Digital Security
Progress. Protected.

Zielgruppe:
CISOs
Geschäftsführer
Vorstände / Beiräte
Security-Verantwortliche

eset® Digital Security
Progress. Protected.

Stand der Technik

ESET PORTFOLIO

Data Feeds + APT-Reports
ESET Threat Intelligence

Endpoint Detection and Response
Cloud: ESET Inspect Cloud*
On-Premises: ESET Inspect*
Managed Detection and Response Services
ESET Detection and Response (Essential/Advanced/Ultimate)

Cloud Sandboxing
ESET LiveGuard® Advanced
Schutz von Cloud-Anwendungen
ESET Cloud Office Security*
Verschlüsselung
ESET Endpoint Encryption*
ESET Full Disk Encryption
Multi-Faktor-Authentifizierung
ESET Secure Authentication*

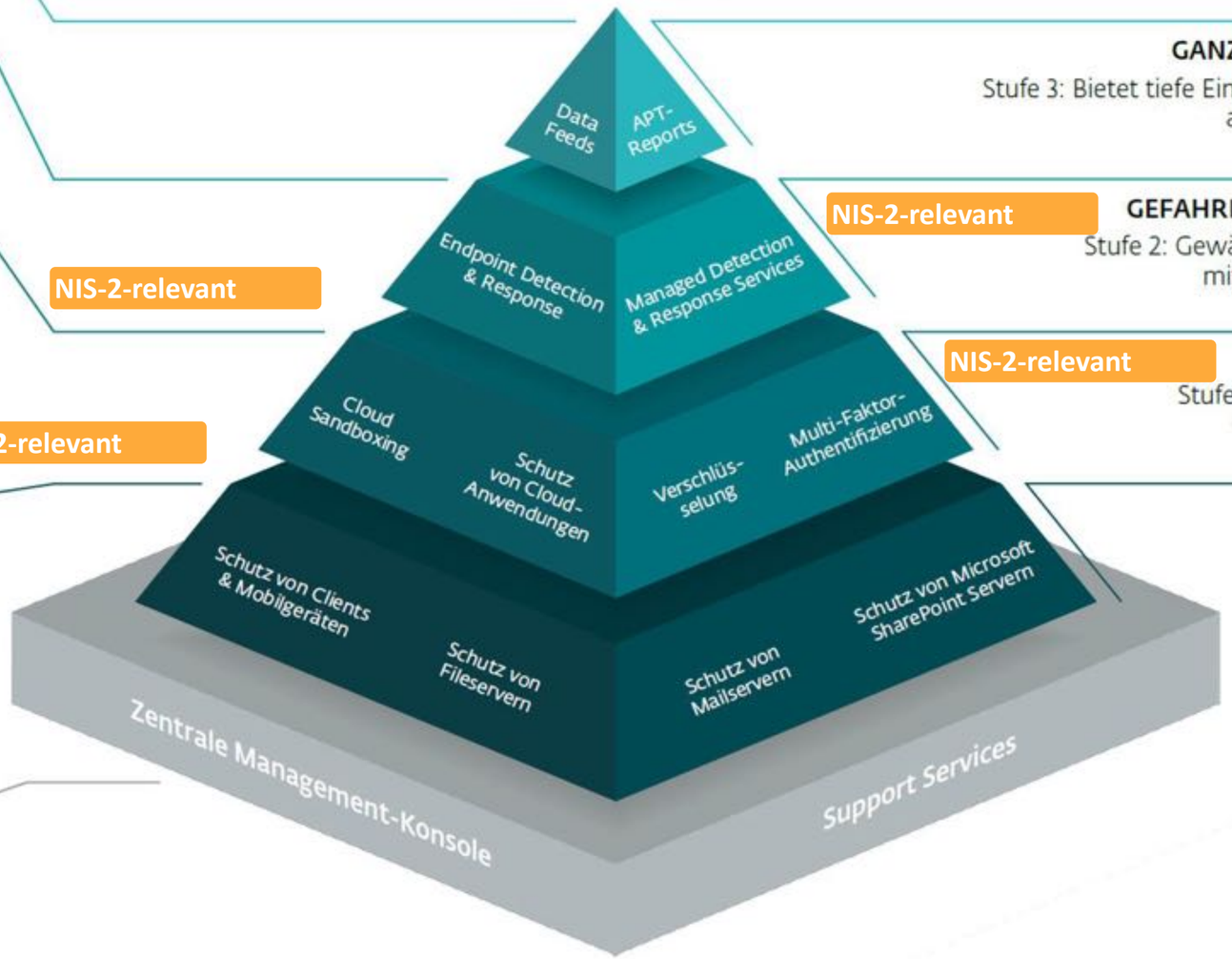
Schutz von Clients und Mobilgeräten
ESET Endpoint Security
ESET Endpoint Antivirus
Schutz von Fileservern
ESET Server Security
Schutz von Mailservern
ESET Mail Security
Schutz von Microsoft SharePoint Servern
ESET Security for Microsoft SharePoint Server

Zentrale Management-Konsole
Cloud: ESET PROTECT Cloud, inkl.:
- Mobile Device Management
- ESET Vulnerability & Patch Management

On-Premises: ESET PROTECT

Support Services
Technischer Support KOSTENFREI
ESET Premium Support (Essential/Advanced)
ESET Upgrade & Deployment
ESET Healthcheck

EINSATZBEREICH



SCHUTZLEVEL

GANZHEITLICHES LAGEBILD – AUSSENSICHT
Stufe 3: Bietet tiefe Einblicke in die globale Bedrohungslandschaft als Grundlage für einen SOC-/SIEM-Betrieb

NIS-2-relevant

GEFAHRENSUCHE UND ABWEHR – INNENSICHT
Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalieerkennung, Schwachstellen-analyse und Incident Management

NIS-2-relevant

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

NIS-2-relevant

GRUNDSCHUTZ BASIS
Stufe 0: Mindestabsicherung für Endgeräte und Server

eset® 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.