

NIS2-Umsetzung in Deutschland – Fluch oder Segen?

Status Quo, Chancen, Fallstricke und
Herausforderungen



Maik Wetzel

Strategic Business Development Director DACH
- ESET Deutschland GmbH -

Über ESET

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



Cyber-
sicherheits-
lösungen
Passgenau
und flexibel
Zentral
verwaltet

UNABHÄNGIG
INHABERGEFÜHRT
WERTEBASIIERT



Breites
Händlernetz

Trainiert +
Zertifiziert

Unterstützt
durch Support
aus DE



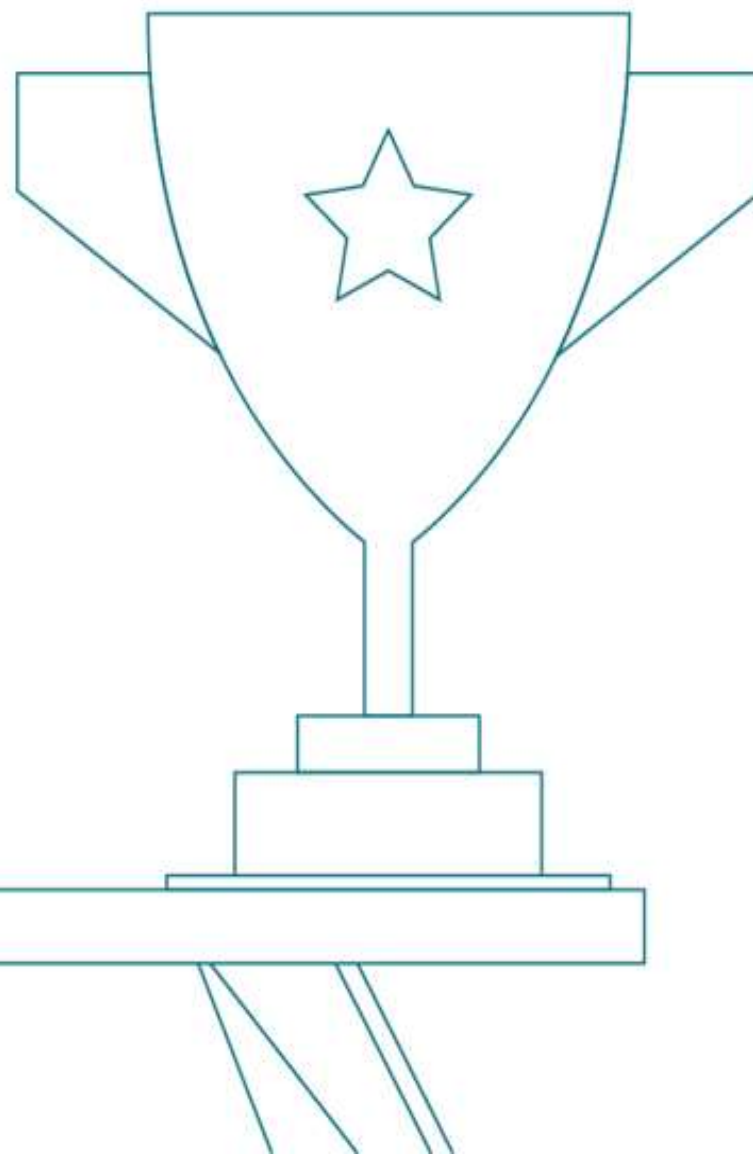
Vielfach
ausgezeichnet

kontinuierliche
Produktqualität



Digital Security
Progress. Protected.

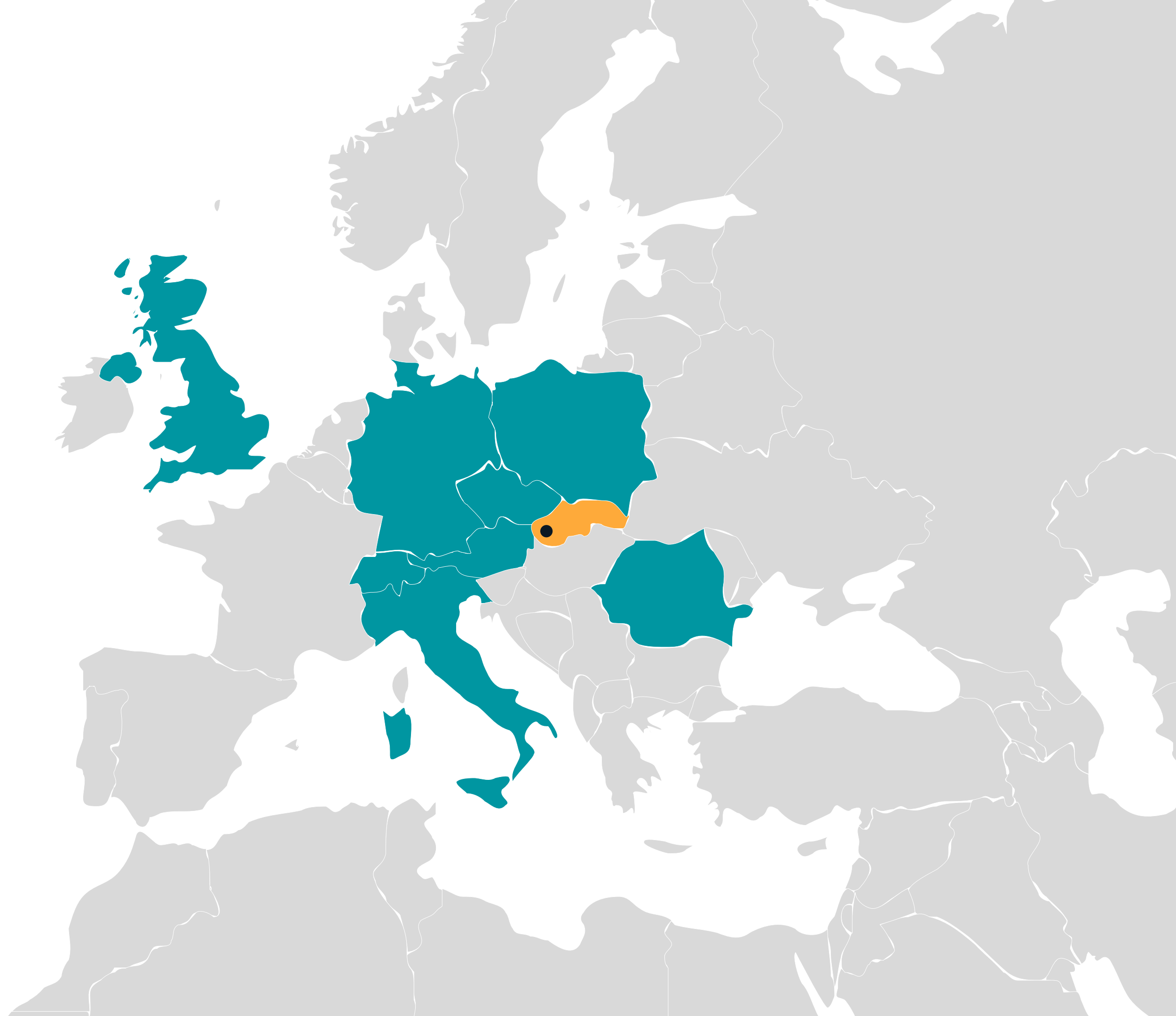
Nr. 1 der Cybersecurity- Unternehmen in der EU

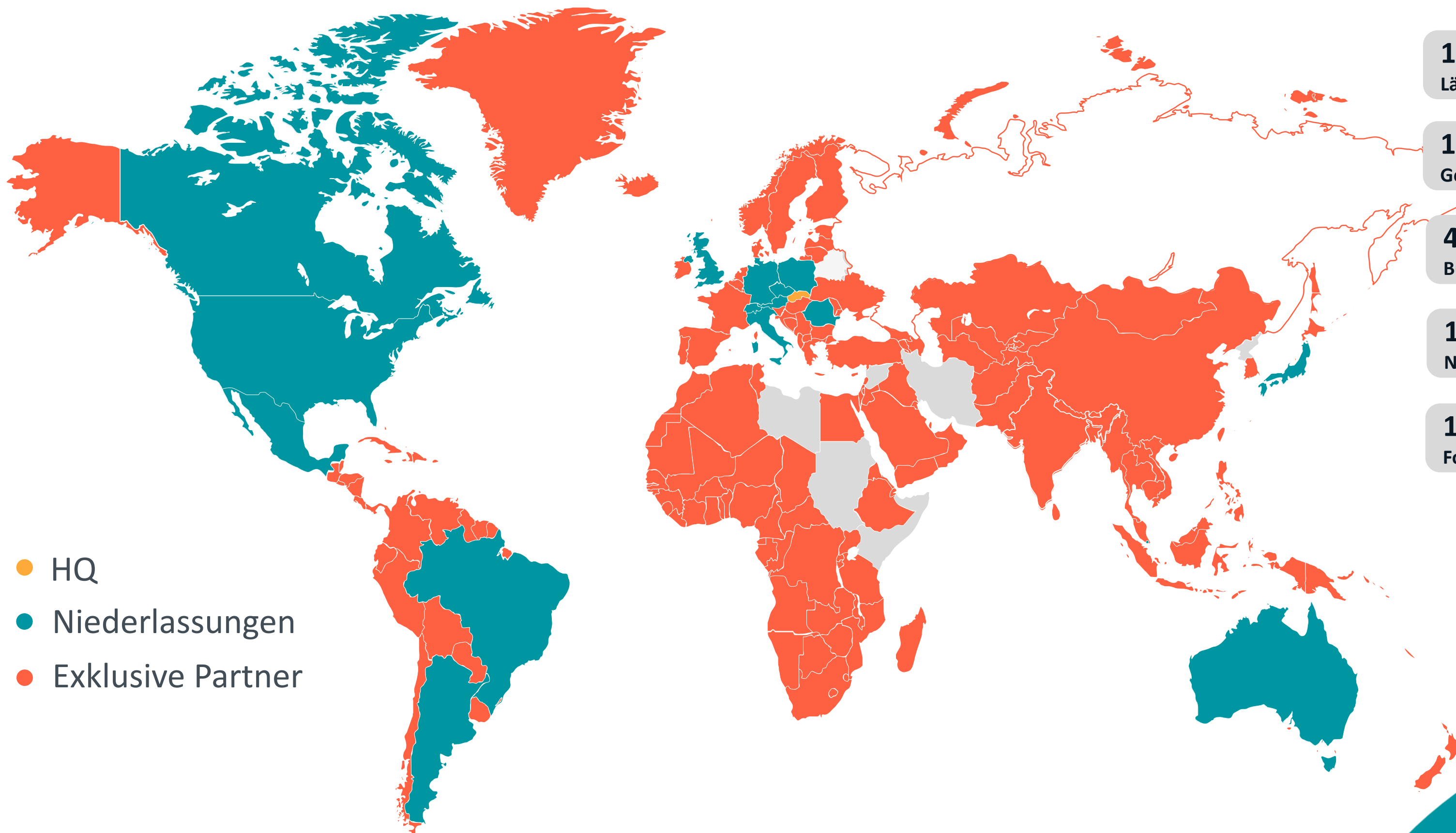


INNOVATION SEIT 1987

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

Im Herzen Europas





- HQ
- Niederlassungen
- Exklusive Partner

195+
Länder & Regionen

1.300.000.000+
Geschützte Internetnutzer

400.000+
Business-Kunden

110.000.000+
Nutzer

13
Forschungs- und Entwicklungszentren



Canon

T...

DB





Marienhospital
Bottrop
gGmbH



kohlpharma



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

(wichtigste) gesetzliche Grundlagen

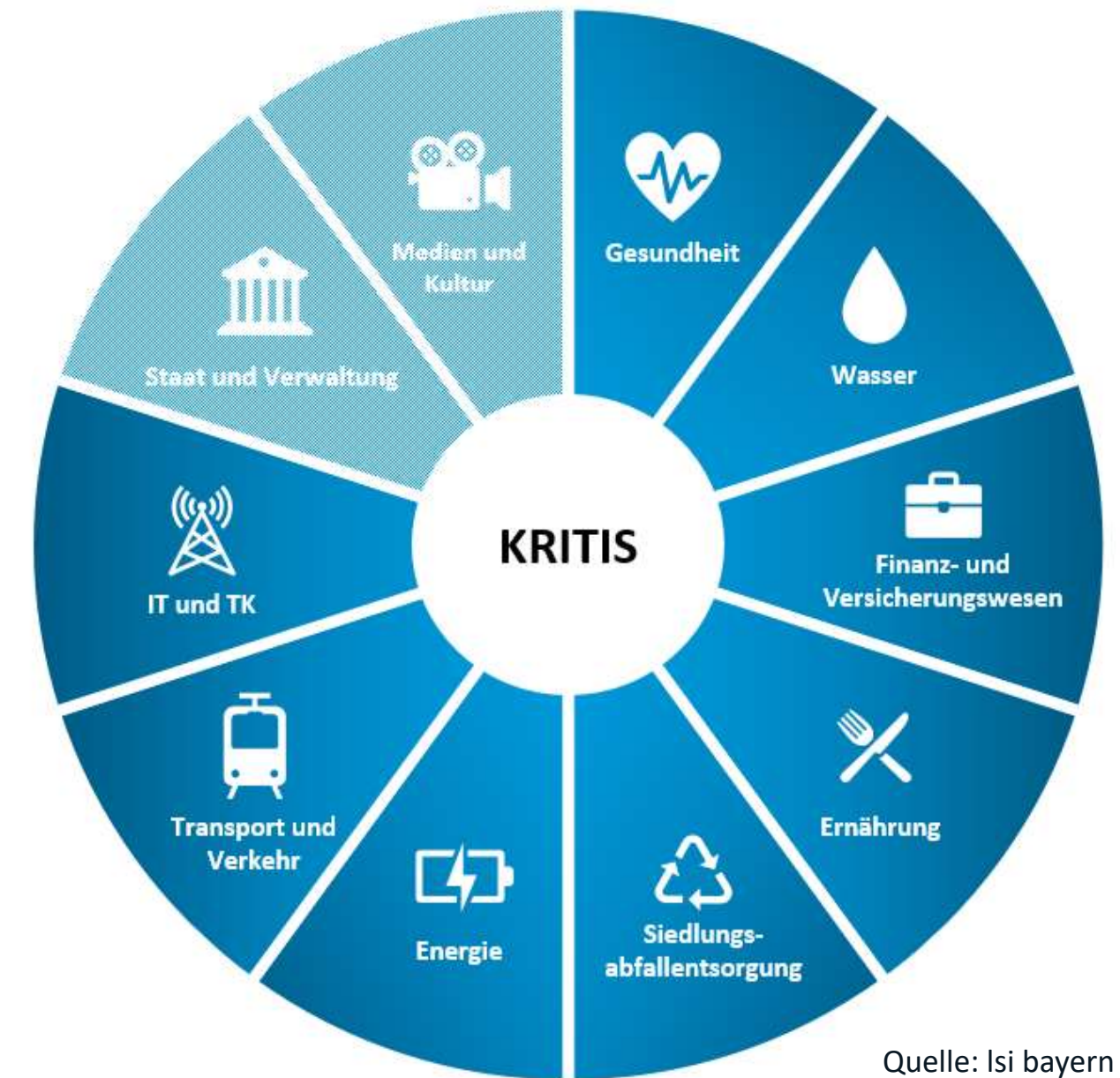
BSI-Gesetz / IT-Sicherheitsgesetz (IT-SIG 2.0) – seit Mai 2021

- 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. 4.000 Organisationen betroffen)
- Anlagen zur Umsetzung

Sektorspezifische Regulierung (z.B. DORA, EnWG)



Bedrohungslage

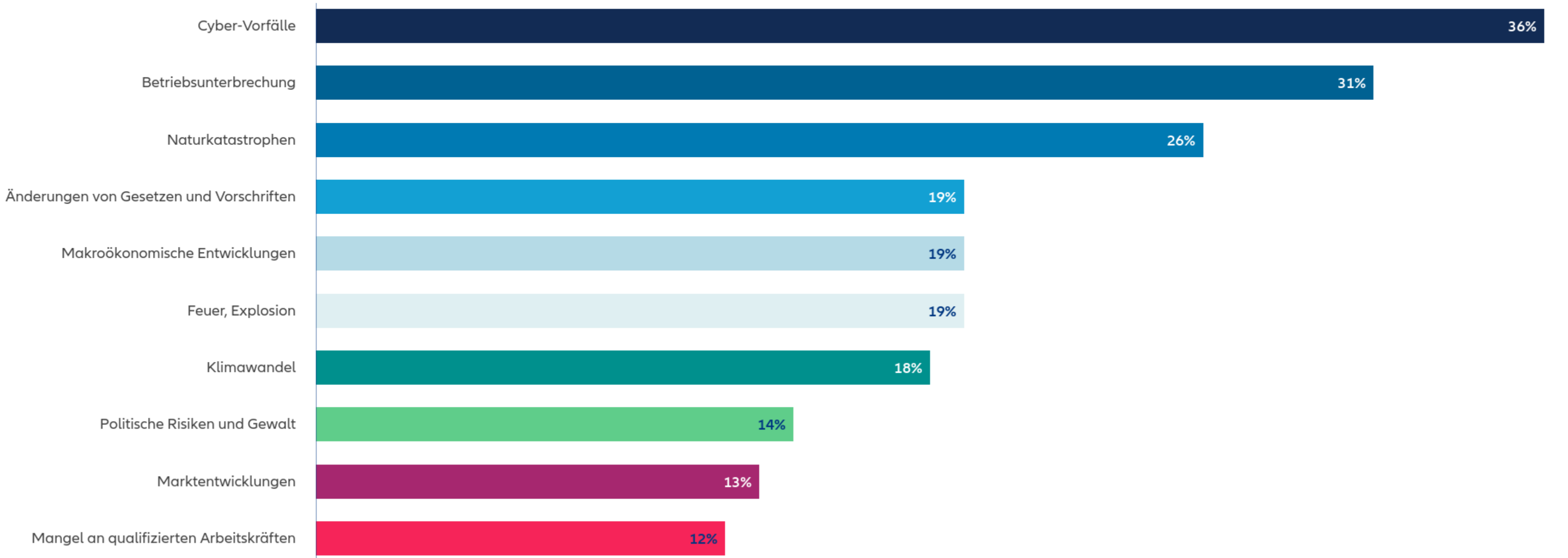
- ✓ Lage ist kritisch
- ✓ **Bedrohung im Cyberraum so hoch wie nie zuvor**
- ✓ Cyber-Erpressungen sind größte Bedrohung
- ✓ Qualität und Anzahl der Angriffe nahmen beträchtlich zu
- ✓ Umgang mit Schwachstellen bleibt eine der größten Herausforderungen
- ✓ Social Engineering großes Thema
- ✓ **Arbeitsteilung 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 148 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.



Stand der IT-Sicherheit 2024 - erste exklusive Ergebnisse



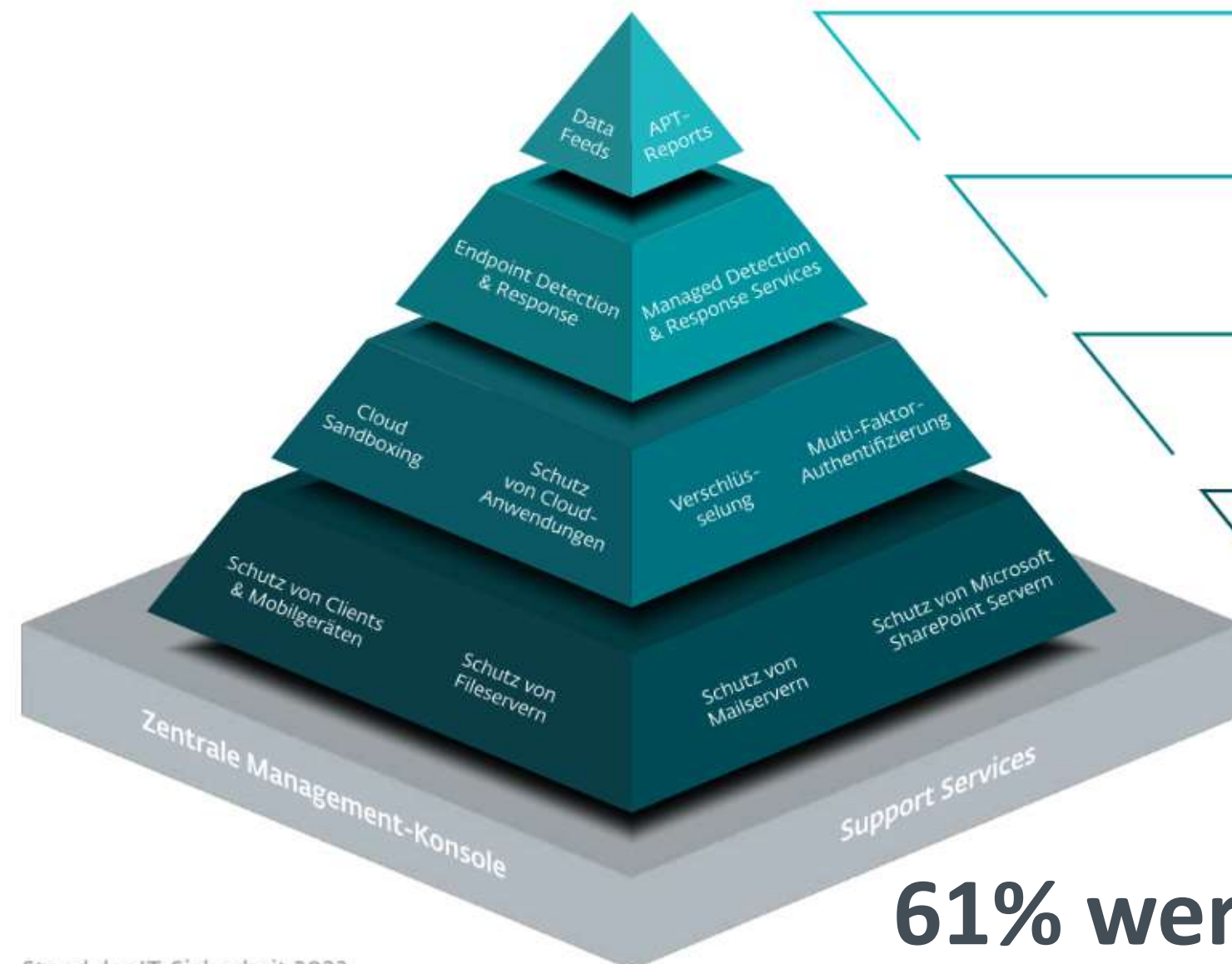
355

Stand der IT-Sicherheit 2024 - Selbsteinschätzung

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

Stand der IT-Sicherheit 2023

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

Ziele von NIS 2.0

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



NIS2- Was ist neu?

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

ISMS – Alternativen zu ISO 27001

In Deutschland gibt es neben der ISO 27001 zwei Alternativen für Informationssicherheitsmanagementsysteme (ISMS):

1. **CISIS12**: Dieses Vorgehensmodell richtet sich an kleine und mittlere Unternehmen sowie Behörden. In 12 Schritten werden konkrete Umsetzungsmaßnahmen und Handlungsempfehlungen aufgezeigt. Die Umsetzung ähnelt dem Aufbau der ISO 27001.
2. **VdS 10000**: Dieser Standard ist ebenfalls eine Alternative zur ISO 27001. Er definiert Anforderungen an ein ISMS und ist insbesondere in Deutschland relevant.

Die ISO 27001 bleibt jedoch der einzige internationale, auditierbare Standard, der die Anforderungen an ein ISMS umfassend beschreibt

Und dann ist da noch...

- **Registrierung beim BSI (§33 NIS2UmsuCG)**
- **Nachweispflichten, Prüfung, Information**
 - a. Betreiber kritischer Anlagen
 - Audits, Zertifizierungen, Prüfungen (ex-ante)
 - Compliance muss alle nachgewiesen werden
 - Random Checks, Security Scans
 - Frühestens nach 3 Jahren
 - b. besonders wichtige Einrichtungen und 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 spätestens 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?

Sektoren nach Anhang I

Energie

Verkehr und Transport

Bankwesen

Finanzmärkte

Gesundheitswesen

Trinkwasser

Abwasser

Digitale Infrastruktur

ICT* Service Management (Managed Service Provider)

Öffentliche Verwaltung

Weltraum

A Besonders wichtige Einrichtungen

Große Betreiber aus 11 Sektoren (Anhang I) und Sonderfälle

Mittlere Unternehmen

- Mindestens 50 Beschäftigte
- Jahresumsatz/Jahresbilanz > 10 Mio. EUR

Große Unternehmen

- Mindestens 250 Beschäftigte
- Umsatz > 50 Mio. EUR
- Bilanz > 43 Mio. EUR

Sektoren nach Anhang II

Post- und Kurierdienste

Abfallwirtschaft

Produktion, Herstellung und Handel mit chem. Stoffen

Produktion, Verarbeitung und Handel von Lebensmitteln

Verarbeitendes Gewerbe/Herstellung von Waren

Anbieter digitaler Dienste

Forschungseinrichtungen

B Wichtige Einrichtungen

Große/Mittlere Betreiber aus allen 18 Sektoren und Sonderfälle, soweit nicht von besonders wichtigen Einrichtungen erfasst

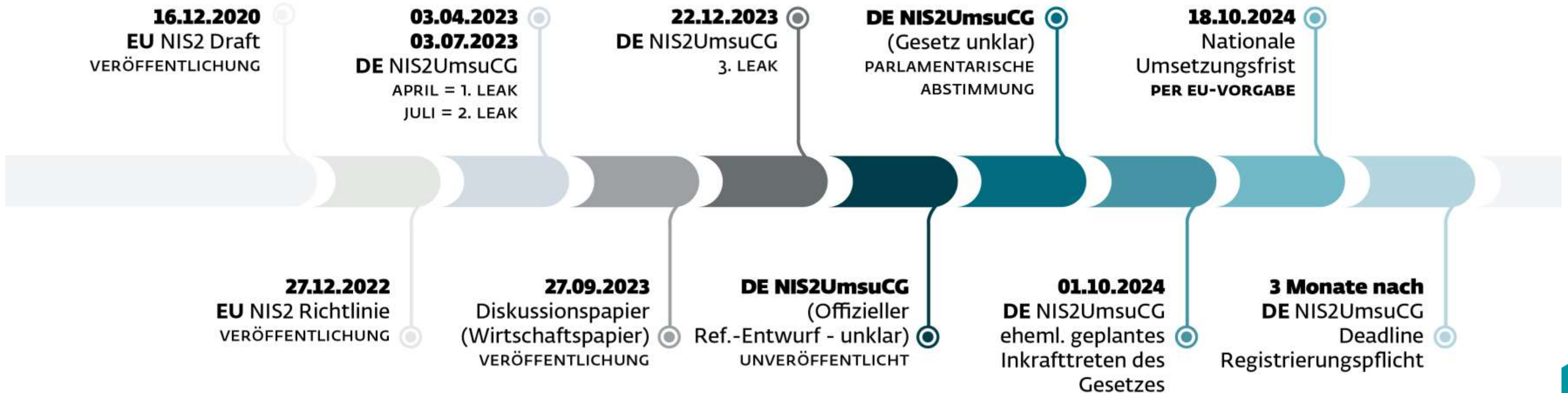
Unabhängig von Unternehmensgröße

Qualifizierende Faktoren, z.B.:

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

Nationale Umsetzung

Roadmap NIS2-Umsetzung



Wo stehen wir?

- 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)
- 3. Referentenentwurf 07.05.2024 / Länder- und Verbändebeteiligung bis 28. Mai 2024
- Verbändeanhörung im BMI am 03. Juni 2024
- 4. Referentenentwurf 24.06.2024
- Länder- und Verbändebeteiligung
- 24.07.2024 Kabinettsbeschluss / Regierungsentwurf
- Parlamentarisches Verfahren
- Gesetz Frühjahr 2025

Kritikpunkte Referentenentwurf

- Keine klare Umsetzungsfrist! (BSI fordert Nachweise erst nach 3 Jahren, aber was passiert bei Vorfall nach dem 17.10.2024?)
- Unzureichende Behandlung der öffentlichen Verwaltung (Kommunen und Länder)
- Wirtschaft muss, Staat hält sich zurück
- Umsetzung auf staatlicher Seite (1.400 neue Planstellen vs. HH-Mittel) – wer bearbeitet eigentlich die von den Unternehmen gemeldeten Vorfälle?
- Information Sharing Portal – gute Idee, aber völlig unklar, wie die Umsetzung erfolgt (bislang keine Einbeziehung Nutzer, Dienstanbieter)
- §9b BSIg wird zu §41 NISUmsuCG – 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
- Unzureichende Abstimmung mit anderen Gesetzen (z.B. KRITIS-Dachgesetz)
- 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)

Erfüllungsaufwand

Erfüllungsaufwand Bund:

- Einmalig: 38 Mio Euro
- Jährlich: 772 Mio Euro

Erfüllungsaufwand Wirtschaft:

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



Ausnahmen

- auf Eigeninitiative des BMI oder per Vorschlag durch
 - das Bundeskanzleramt,
 - das Bundesjustizministerium,
 - das Verteidigungsministerium oder die
 - Innen- und Justizministerien der Länder,
 - Das Bundesfinanzministerium (neu)

kann das BMI „besonders wichtige Einrichtungen“ ganz oder teilweise von den Pflichten befreien

Handlungsempfehlung

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



Zielgruppe:

CISOs

Geschäftsführer

Vorstände / Beiräte

Security-Verantwortliche

Mehr Information:

www.eset.de/nis2

EINSATZBEREICH

SCHUTZLEVEL

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/Ulimate)

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

NIS-2-relevant

NIS-2-relevant

NIS-2-relevant

NIS-2-relevant

GANZHEITLICHES LAGEBILD – AUSSENSICHT

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

GEFAHRENSUCHE UND ABWEHR – INNENSICHT

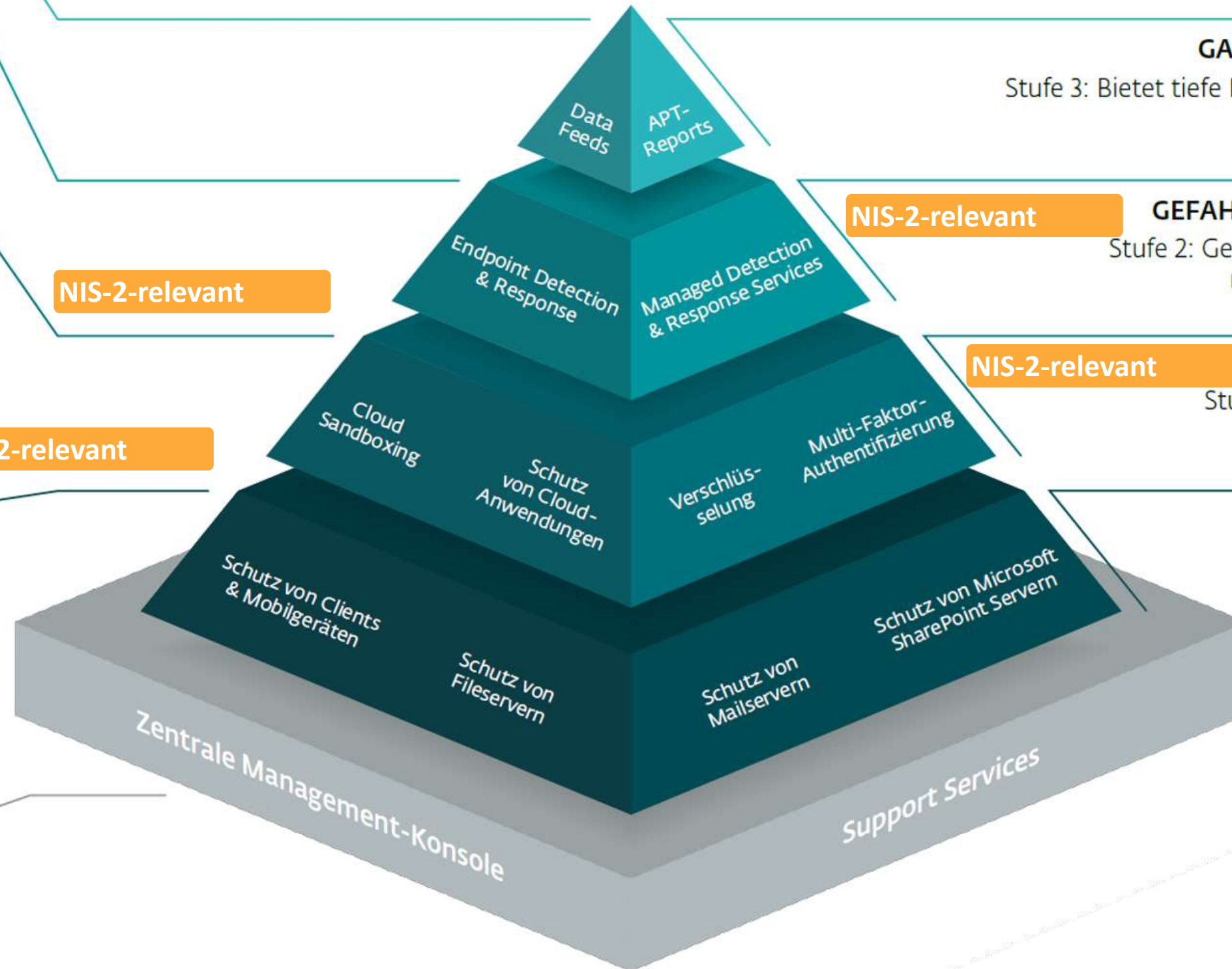
Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalieerkennung, Schwachstellenanalyse und Incident Management

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





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