NIS2-Umsetzung in Deutschland – Fluch oder Segen?

Chancen, Fallstricke und Herausforderungen

Digital Security
Progress. Protected.

Maik Wetzel

Strategic Business Development Director DACH
- ESET Deutschland GmbH -

Digital Security
Progress. Protected.

Vorstellung

Status Quo

Digital Security
Progress. Protected.

(wichtigste) gesetzliche Grundlagen

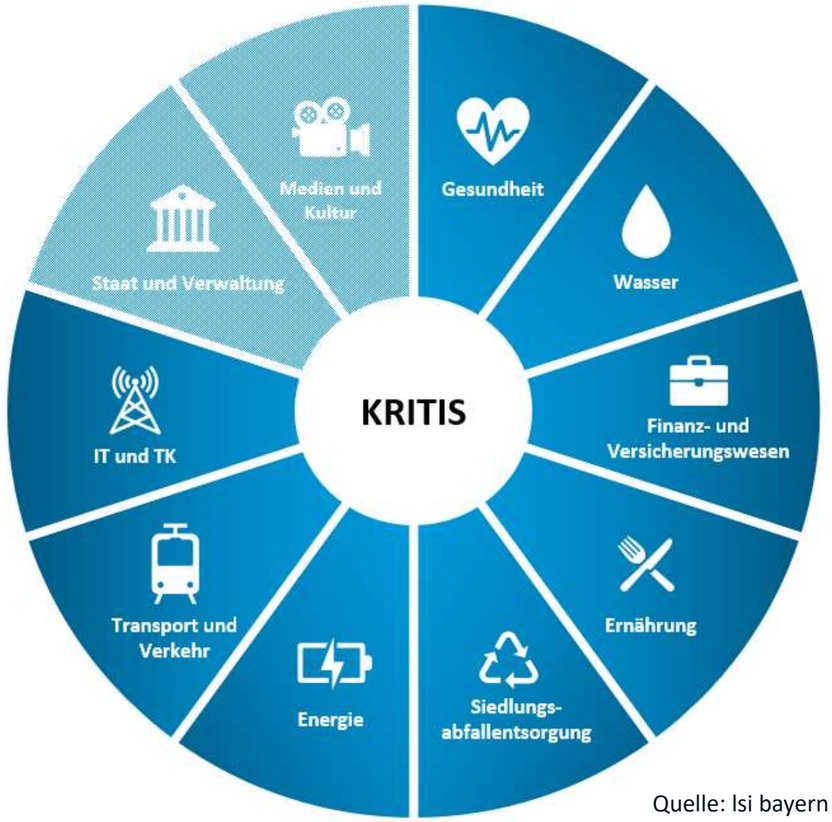
BSI-Gesetz / IT-Sicherheitsgesetz (IT-SIG 2.0) – seit Mai 2021

- 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. 5.500 Unternehmen betroffen)
- Anlagen zur Umsetzung

Sektorspezifische Regulierung (z.B. DORA, EnWG)



Quelle: lsi bayern

Bedrohungslage

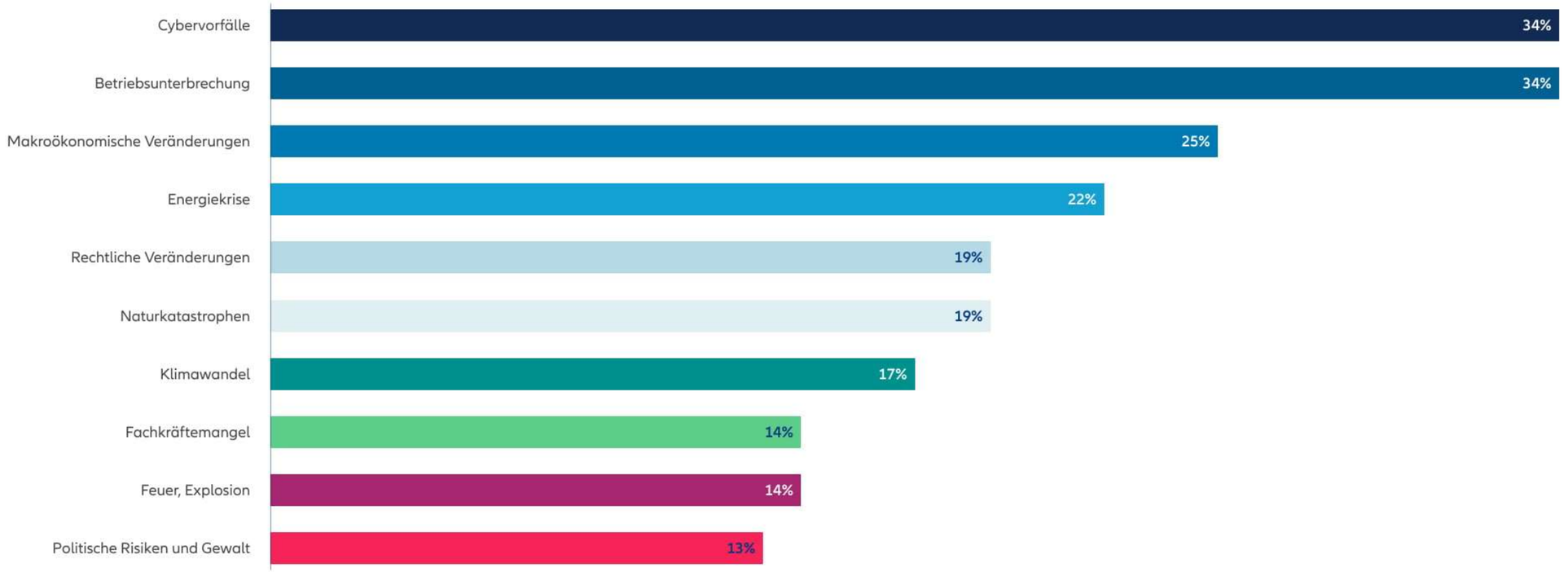
- Lage ist angespannt bis kritisch
- Cyber-Erpressungen sind größte Bedrohung
- Qualität und Anzahl der Angriffe nahmen beträchtlich zu
- Umgang mit Schwachstellen bleibt eine der größten Herausforderungen
- Social Engineering großes Thema
- Arbeitsteilung und Professionalisierung auf Seite der Angreifer
- Geopolitische Zeitenwende führt zu weiterer Verschärfung
- Hybride Bedrohungslage“
- Lageveränderung jederzeit möglich

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

NIS 2.0 Umsetzung kommt!
Fluch oder Segen?

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 Data Act
- EU Digital Markets Act
- EU AI Act
- EU Cloud Act
- EU Krypto Act
- GAIA-X
- …

Wer ist betroffen?

Sektoren nach Anhang I (wesentliche Einrichtungen)

- Energie
- Verkehr und Transport
- Bankwesen
- Finanzmärkte
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- ICT* Service Management (Managed Service Provider - MSP)
- Öffentliche Verwaltung
- Weltraum

A wesentliche Einrichtungen

Große Betreiber aus elf Sektoren 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

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. 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

*„Die Anforderungen und Standards gelten im Zweifel im gleichen Maße **für Dienstleister, Zulieferer**… und zukünftig quasi **für jeden** der eine **Cyberversicherung** abschließen möchte!“*

Und dann ist da noch…

- Registrierung beim BSI
- 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
    – 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

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 (?)

Roadmap nationale Umsetzung

- Richtlinie EU 2022/2555 des EU-Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (in Kraft seit 16.01.2023)
- Umsetzungsfrist für Mitgliedstaaten in nationales Recht bis **17.10.2024**
- **(inoffizieller) Referentenentwurf NIS2UmsuCG vom 03.07.2023**
- Parallel: Referentenentwurf des „Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)“
- Zeitnah: Länder- und Verbändebeteiligung
- Herbst 2023: Gesetzgebungsverfahren und Beschluss
- Verordnung zum NIS2UmsuCG (analog KRITIS Verordnung)
- Deadline zur Umsetzung: **17.10.2023**

Anmerkung:

Prognostizierter **Erfüllungsaufwand für die Wirtschaft**:

- Einmalig: 1,37 Mrd Euro
- Jährlich: +1,65 Mrd Euro

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.

„…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)

Zielgruppe:
CISOs
Geschäftsführer
Vorstände / Beiräte
Security-Verantwortliche

Eckdaten:
25 Seiten
5 Kapitel

Herkunft und Definition
Cyberversicherungen
Anforderungen
Technische Maßnahmen
Handlungsempfehlungen

Digital Security
Progress. Protected.

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

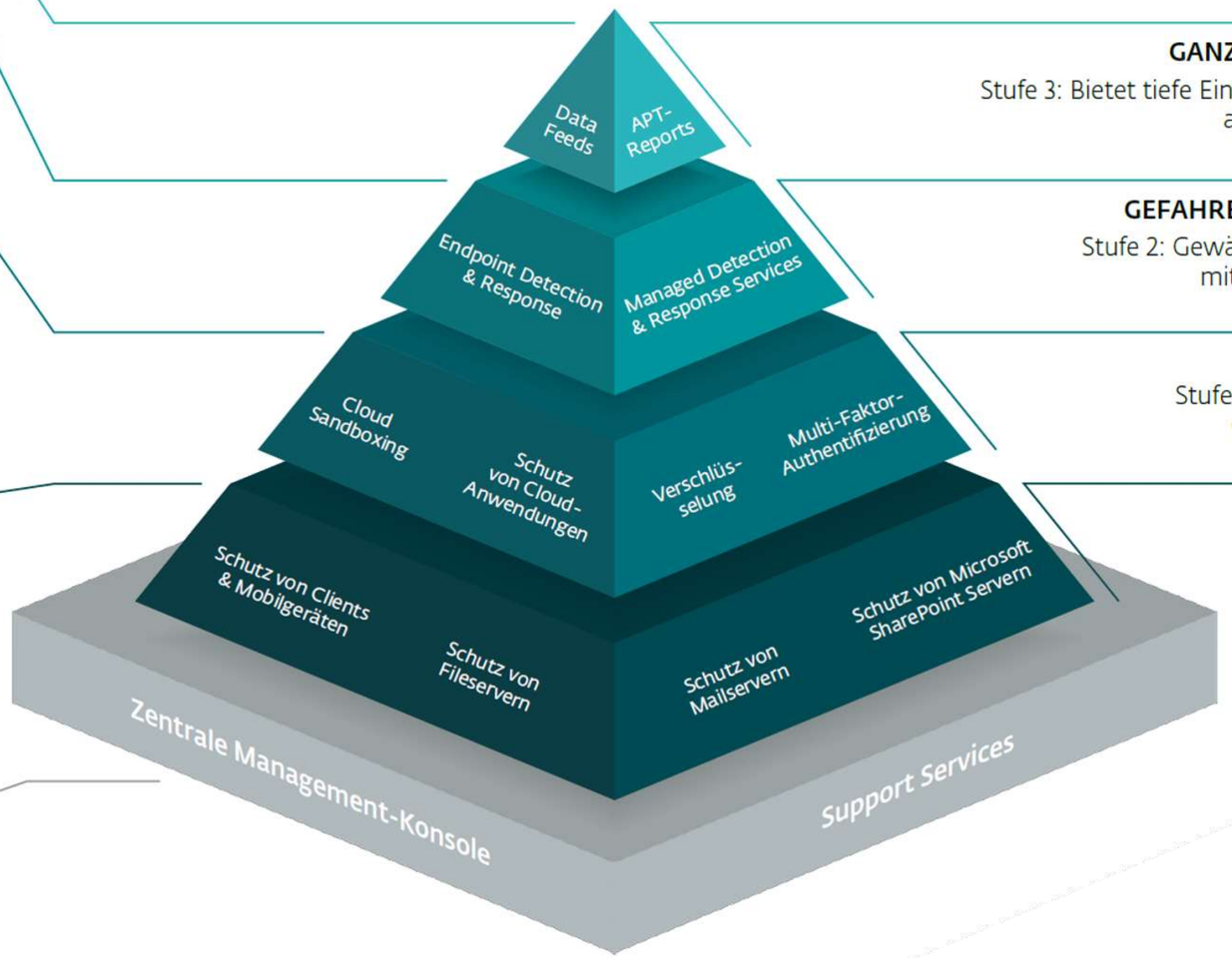
Schutz von Microsoft SharePoint Servern
ESET Security for Microsoft SharePoint Server

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

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

eset® Digital Security
Progress. Protected.

Stand der Technik

Digital Security
Progress. Protected.

Herzlichen Dank für Ihre Aufmerksamkeit!

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.