

TeleTrust-interner Workshop

Berlin, 26. - 27.06.2024

**"Cybernation Deutschland - mit Kooperation
mehr Cybersecurity verwirklichen"**

Stefan Becker, BSI



Cybernation Deutschland – mit Kooperation mehr Cybersecurity verwirklichen

Stefan Becker
Bundesamt für Sicherheit in der Informationstechnik
26. Juni 2024 | TeleTrusT interner Workshop

Aktuelle Situation – gefühlte Lage in Deutschland

- → Unternehmen und Institutionen in Deutschland werden jeden Tag von Cyberkriminellen angegriffen.
- → IT-Störungen und Cyberangriffe auf Kritische Infrastrukturen gefährden die tägliche Versorgung Deutschlands.
- → Deutschland ist Ziel von Cyberspionage und -sabotage.
- → Der gesellschaftliche Zusammenhalt in Deutschland wird von außen gefährdet, z. B. durch Desinformation.
- → Die Menschen in Deutschland sind im Cyberraum nicht ausreichend geschützt.
- → Deutschland verliert bei der Digitalisierung den Anschluss an die Weltspitze.
- → Deutschland spielt bei digitalen Technologien keine echte Rolle mehr.
- → Das Vertrauen der Menschen in den Staat und seine Digitalisierung schwindet.

Status quo: Produkt- und Serviceresilienz

Digitale Produkte und Services werden oft nicht im Hinblick auf Sicherheit entwickelt und über ihren Lebenszyklus gemanagt.

→ Security by Design/Default und Herstellerverantwortung sind nötig.

Produkte und Services entsprechen oft nicht den Mindestanforderungen an Sicherheit.

- Security by Design/Default ist nicht hinreichend gegeben.
- Oft gibt es keinen gemanagten Lebenszyklus, d. h. keine (Security-)Updates.
- Lieferketten sind oft komplex und zu wenig überwacht.
- Transparenz zu verwendeter Software in Produkten fehlt.
- Sichere Technologien sind vorhanden, werden aber nicht (flächendeckend) genutzt .

Cyber Resilience Act bringt Herstellerverantwortung.

Es werden Anforderungen an die Sicherheit von Produkten mit digitalen Elementen gestellt. Dies betrifft den gesamten Produktzyklus (Planung, Konzeption, Entwicklung, Herstellung, Lieferung, Wartung).

Status quo: Firmen- und Institutionsresilienz

Viele Unternehmen und Institutionen sind auf Digitalisierungen und Cybersicherheit unzureichend vorbereitet.

→ Konsequente Betreiber- und Nutzerverantwortung sind nötig.

Fast **75 %** der Unternehmen und Institutionen in Deutschland sind von Cyberkriminalität betroffen.

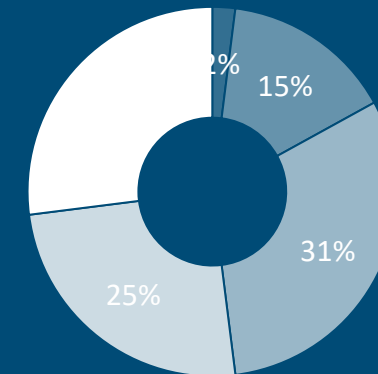
Die Unternehmen und Institutionen sind sich der Relevanz des Themas durchaus bewusst, haben aber vielfach große Defizite im Bereich Cybersicherheit und Resilienz. Das macht sie verwundbar.

Die europäische Cybersecurity-Richtlinie NIS 2 nimmt Betreiber und Nutzer stärker in die Pflicht. Denn sie

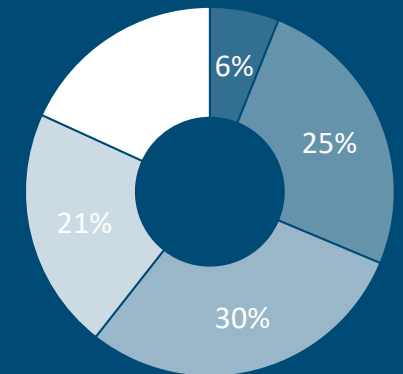
- erweitert den Adressatenkreis von Unternehmen und Einrichtungen,
- bringt neue Anforderungen und verschärftes Aufsichts- und Sanktionsregime und
- muss in DE bis Okt. 2024 gesetzlich umgesetzt werden.

Beispiel Kritische Infrastrukturen (KRITIS)

Information Security Management System



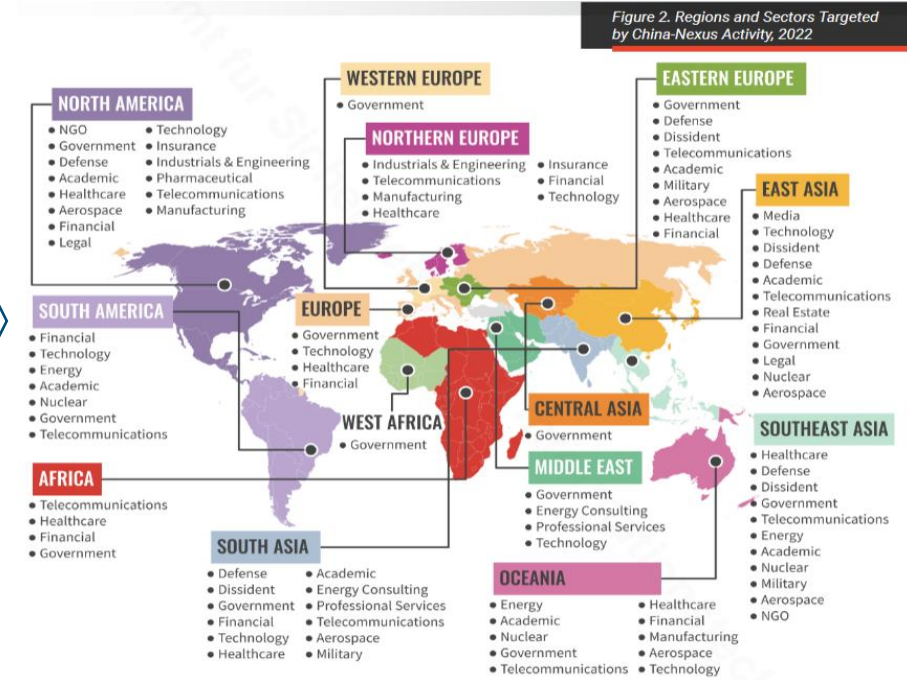
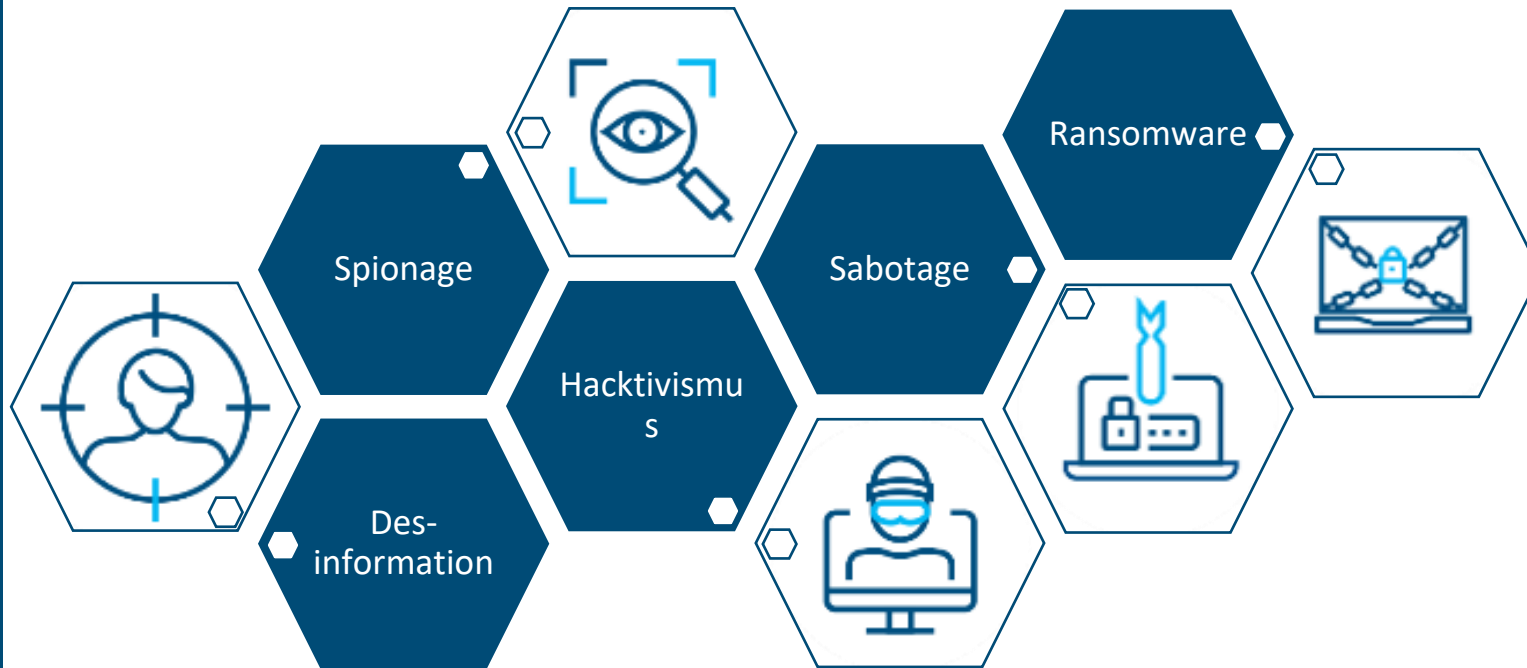
Business Continuity Management



Reifegrad 1 2 3 4 5

Skala von 1 = geplant bis 5 = umgesetzt und regelmäßig verbessert

Auswirkungen der aktuellen geopolitischen Verwerfungen



Quelle: CrowdStrike, Annual Threat Report 2022 (von Januar 2023)

Unsicherheitsfaktoren: Russisch-Ukrainischer Krieg, Hegemonialstreben Chinas, Nahostkonflikt, US-Wahlen

Künstliche Intelligenz – auf Angreiferseite.....

Codegenerierung (Malware) durch KI

Phishingtexte durch KI

Übersetzung durch KI

DeepFake Nutzung....

Wir sind hier beim TeleTrustT

29.06.2023 Prof. Dr. Michael Waidner beim TeleTrustT

Die wahren Probleme der IT-Sicherheit

„Deutschland hat hohes Potential, realisiert es aber nicht“

02.09.2021 TeleTrust-IT-Sicherheitsagenda 2029

Deutschland und Europa müssen angemessen und souverän die digitale Zukunft gestalten können. Dazu hält es der Bundesverband IT-Sicherheit e.V. (TeleTrust) für dringend erforderlich, dass Deutschland im Bereich der IT-Sicherheit eine Vorreiterrolle einnimmt. Für die nächsten beiden Legislaturperioden des Deutschen Bundestages hat TeleTrust deshalb mit der "IT-Sicherheitsagenda 2029" wichtige Forderungen aufgestellt.

Und was hat sich getan?

- XZ Utils Backdoor
- Microsoft Master Key für Azure „verloren“ (heise.de 03.04.2024)
- Seit Monaten greifen staatlich geförderte Cyberkriminelle die Systeme von Microsoft an (Quellcode abhanden gekommen - heise.de 09.03.2024)
-

Strategieziele für eine Cybernation Deutschland und das BSI

Cybersicherheit

auf die Agenda heben

Digitalisierung

voranbringen

Resilienz

erhöhen

Cybersicherheit

gestalten

**Technologie-
kompetenz**

nutzen

**Cybermarkt
Deutschland**

aufbauen

29.06.2023 Prof. Dr. Michael Waidner beim TeleTrustT

Wir können es uns nicht leisten, es nicht zu schaffen

- Deutschland hat die besten Chancen, zur „Cybernation“ zu werden
- Gelingt es uns nicht, wachsen unsere Abhängigkeiten und sinkt unsere digitale Souveränität..

**Wir bauen gemeinsam die Cybernation
Deutschland.**

Informationen:



Stefan Becker

Referatsleiter – WG22 Cyber-Sicherheit für die Wirtschaft und Allianz für Cyber-Sicherheit

Kontakt

stefan.becker@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 87

53175 Bonn

www.bsi.bund.de

www.allianz-fuer-cybersicherheit.de