Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Aktuelles zur Cyber-Sicherheitslage

November 2024

Dr. Harald Niggemann

Kurzprofil des BSI

Gründung
01. Januar 1991

237,9 Mio. Euro
Budget Haushalt 2024

Stellen 2024

1.784,7

BSI vor Ort

- Standorte
- Stützpunkte
- Verbindungsstellen

Darüber hinaus engagiert sich das BSI seit Langem intensiv im internationalen und nationalen Rahmen, unter anderem in enger Zusammenarbeit mit bilateralen Partnern sowie in multilateralen Handlungsfeldern rund um EU und NATO.

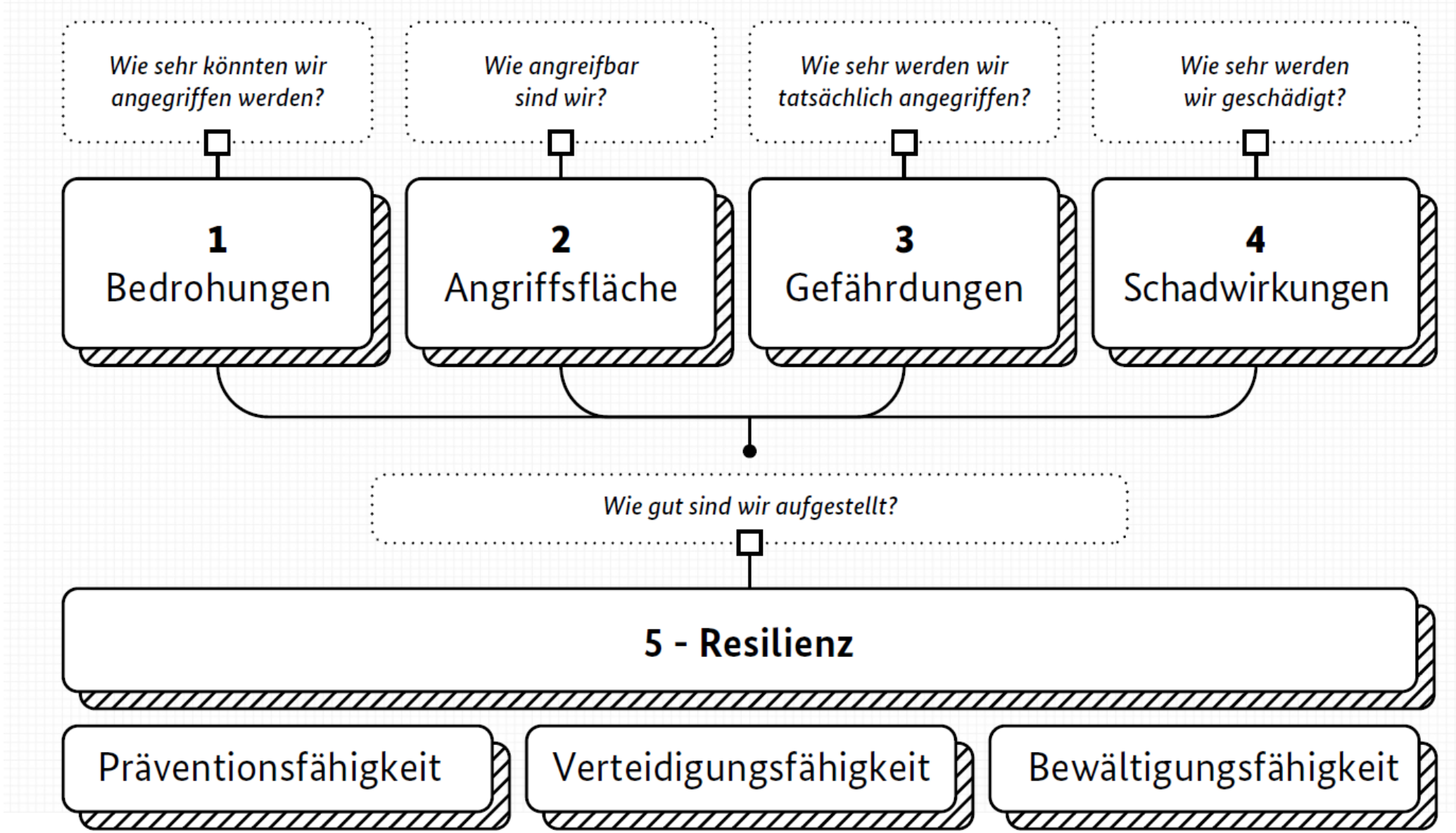
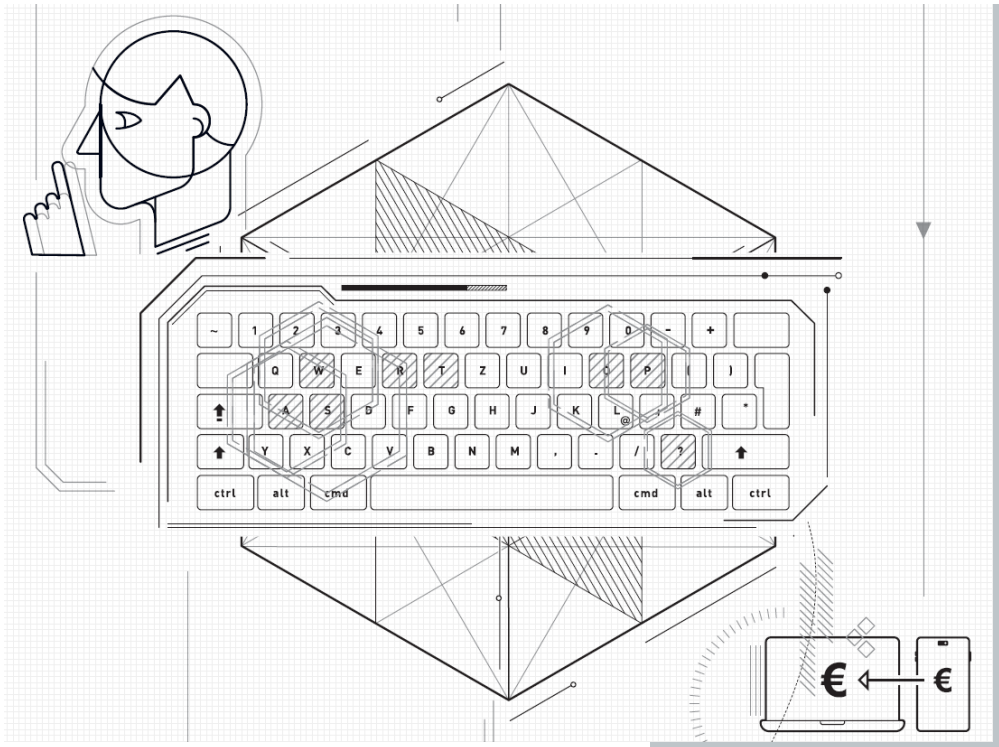


Abbildung 1: Systematik der BSI-Lagebeobachtung

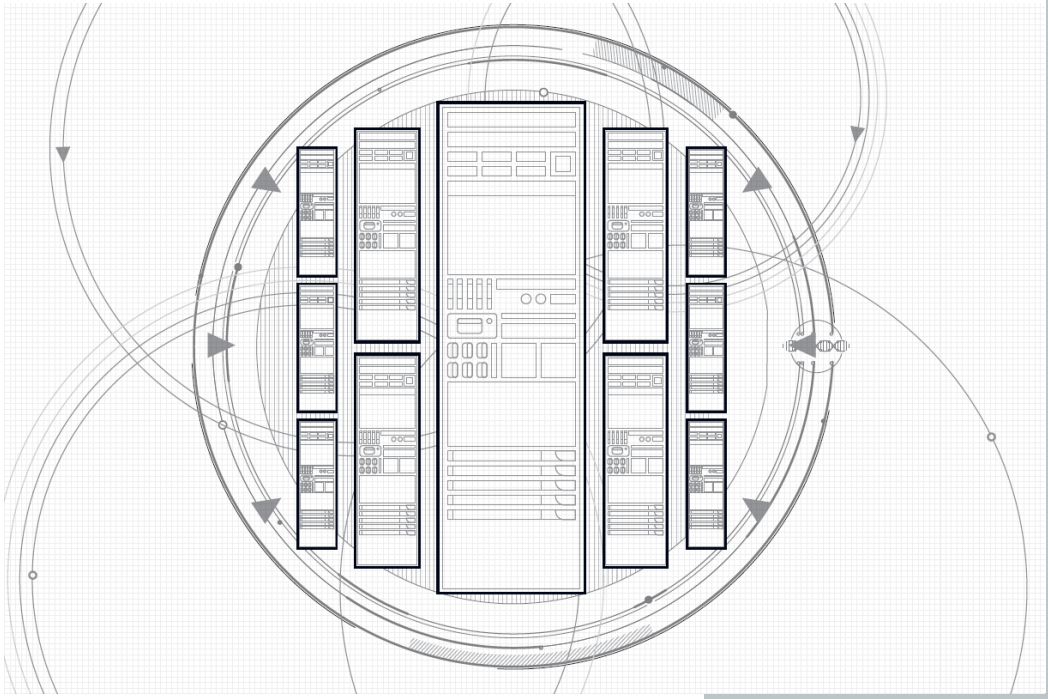
Wie bedroht ist Deutschlands Cyberraum? - Bedrohungen

- Die Lage der IT-Sicherheit in Deutschland **war und ist besorgniserregend.**
- Weiterhin professioneller werdende **arbeitsteilige cyberkriminelle Schattenwirtschaft**
- **APT-Gruppen in Deutschland – darunter die gefährlichsten – bleiben weiterhin aktiv.**
- **Bei Malware gewinnt Android als Zielsystem an Bedeutung**.



Wie bedroht ist Deutschlands Cyberraum? - Angriffsfläche

- Pro Tag wurden 78 **neue Schwachstellen in Softwareprodukten** bekannt
- mind. 37 % der 45.000 **Exchange-Server in Deutschland** verwundbar
- 25 % der **Android-Geräte** in Deutschland erhalten **keine Sicherheits-Updates** mehr.
- **Schwachstellen nehmen seit Jahren kontinuierlich zu.**
- **Vielfältige Angriffstechniken treffen auf einen digitalisierten Alltag – alle können angegriffen werden.**

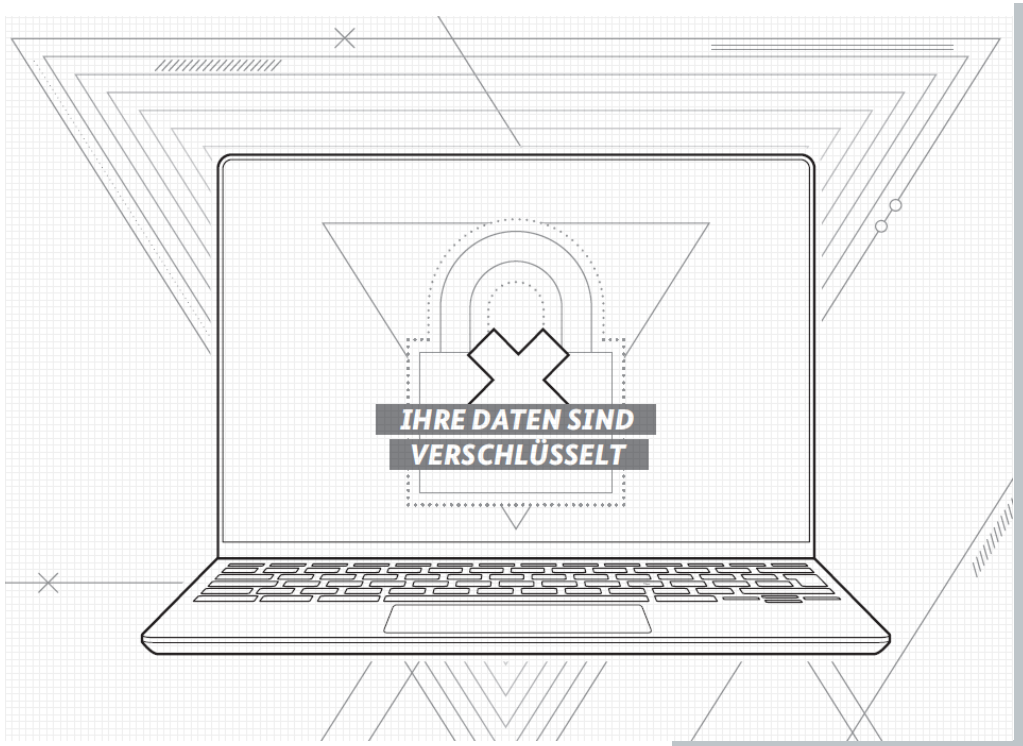


Wie bedroht ist Deutschlands Cyberraum? - Gefährdungen

- **Öffentliche Verwaltung** EU-weit von allen Branchen am stärksten **von IT-Sicherheitsvorfällen betroffen**
- Häufig Angriffe auf **Public-Cloud-Infrastrukturen**
- **Der Anteil bandbreitenstarker DDoS-Angriffe hat sich gegenüber dem langjährigen Durchschnitt verdoppelt.**
- **Phishing-Angriffe nicht mehr nur durch Missbrauch von Bank-Namen**

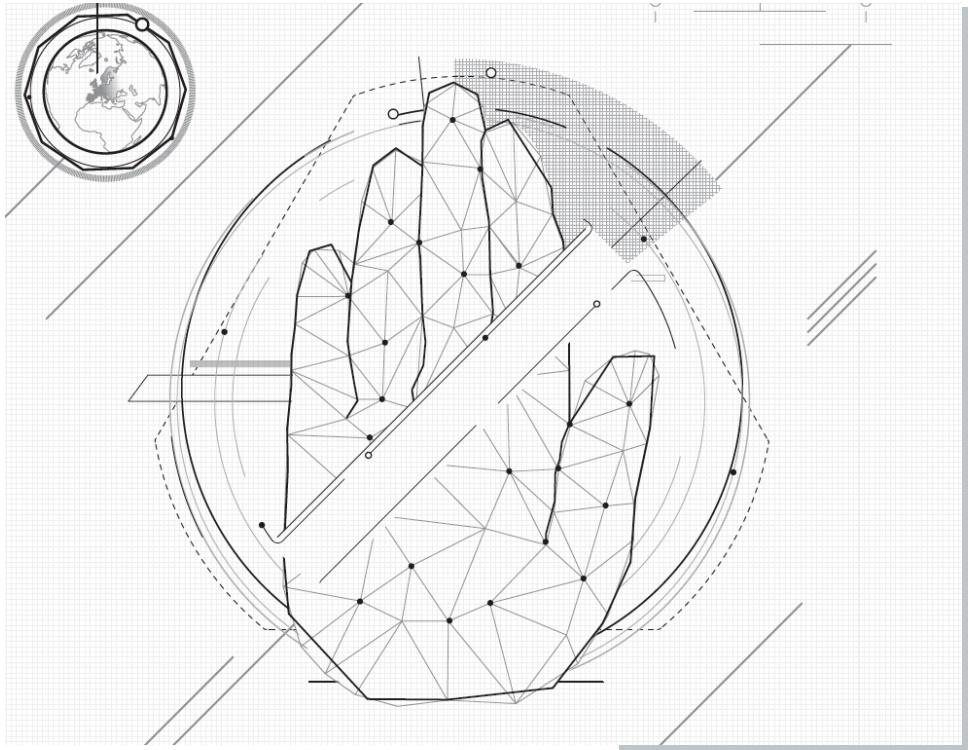
Wie bedroht ist Deutschlands Cyberraum? - Schadwirkung

- Laut Bitkom 179 Milliarden Euro **Schaden bei deutschen Unternehmen durch Cyber-Angriffe** in 2024
- Hoher Schaden durch **fehlerhaftes Update bei CrowdStrike/Falcon**: 5 Milliarden Dollar
- **Exfiltrierte Daten wesentlich mehr wert als verschlüsselte Daten -> Fähigkeit zur Prävention muss gestärkt werden.**
- **Schäden im Milliardenbereich, unvorhergesehene Ereignisse, menschliches Versagen -> Fähigkeit zur Vorfallsbewältigung muss gestärkt werden.**

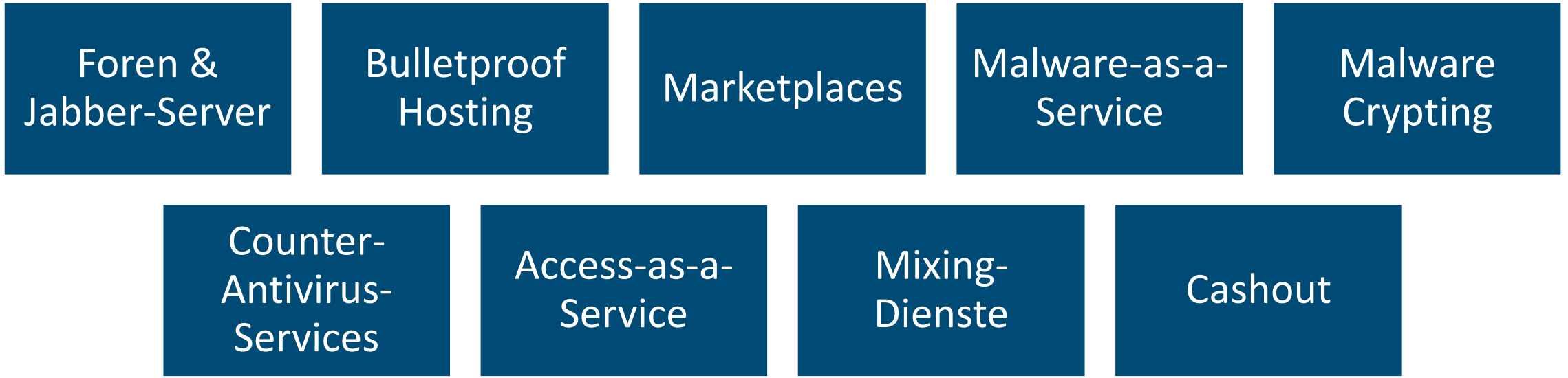


Wie bedroht ist Deutschlands Cyberraum? - Resilienz

- Deutschland ist den Bedrohungen **nicht schutzlos ausgeliefert**.
- **Warnsysteme des BSI:** von technischen Warnungen über herausgehobene Einzelfälle bis hin zu ernstzunehmenden Gefährdungen
- **Alle Beteiligten** müssen ihren Beitrag zur **Cyberresilienz Deutschlands** leisten.
- **Kooperation gewinnt**.



Cybercrime-as-a-Service, das Cybercrime-Ökosystem



Durchschnittliche Lösegeldzahlungen nach Quartal

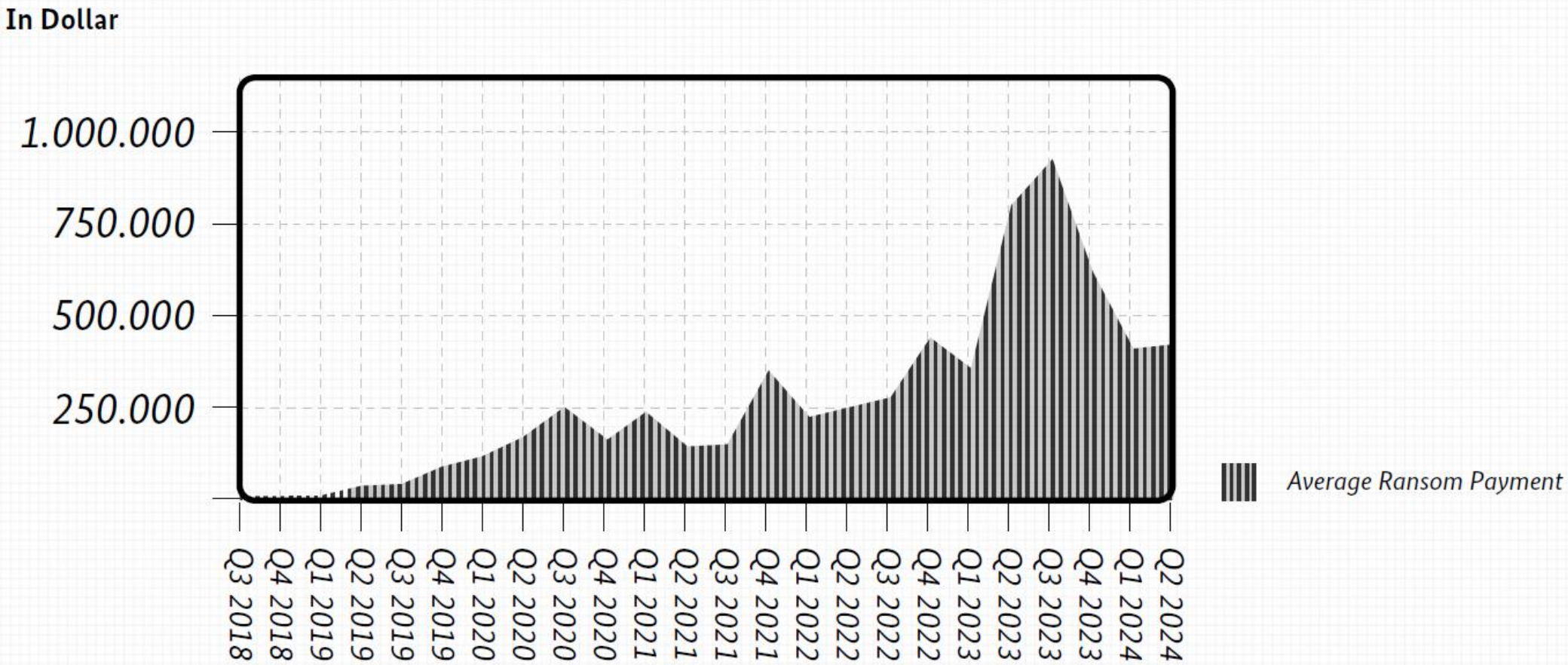


Abbildung 12: Durchschnittliche Lösegeldzahlungen nach Quartal (US-Dollar), (Quelle: Coveware)

Ransomware-Opfer, die Lösegeld zahlten

Anteil in Prozent an allen Ransomware-Opfern

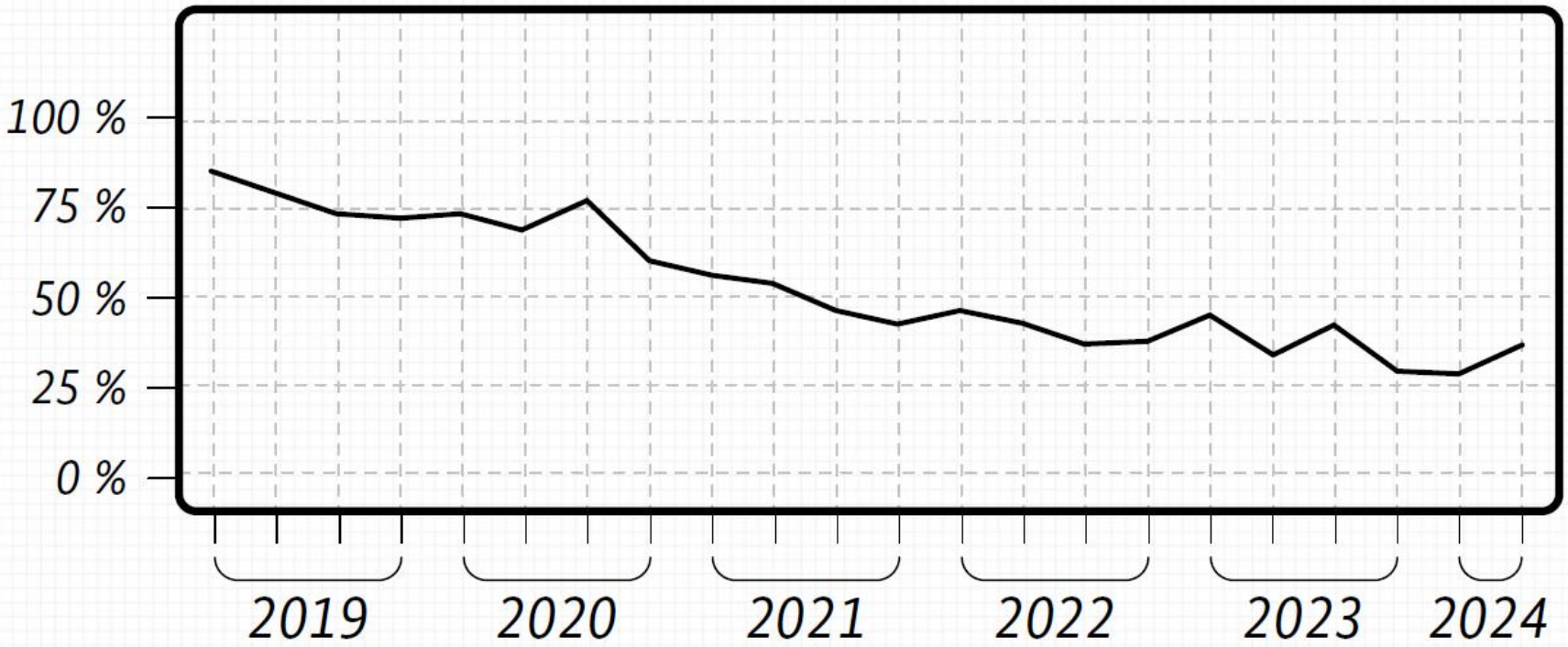
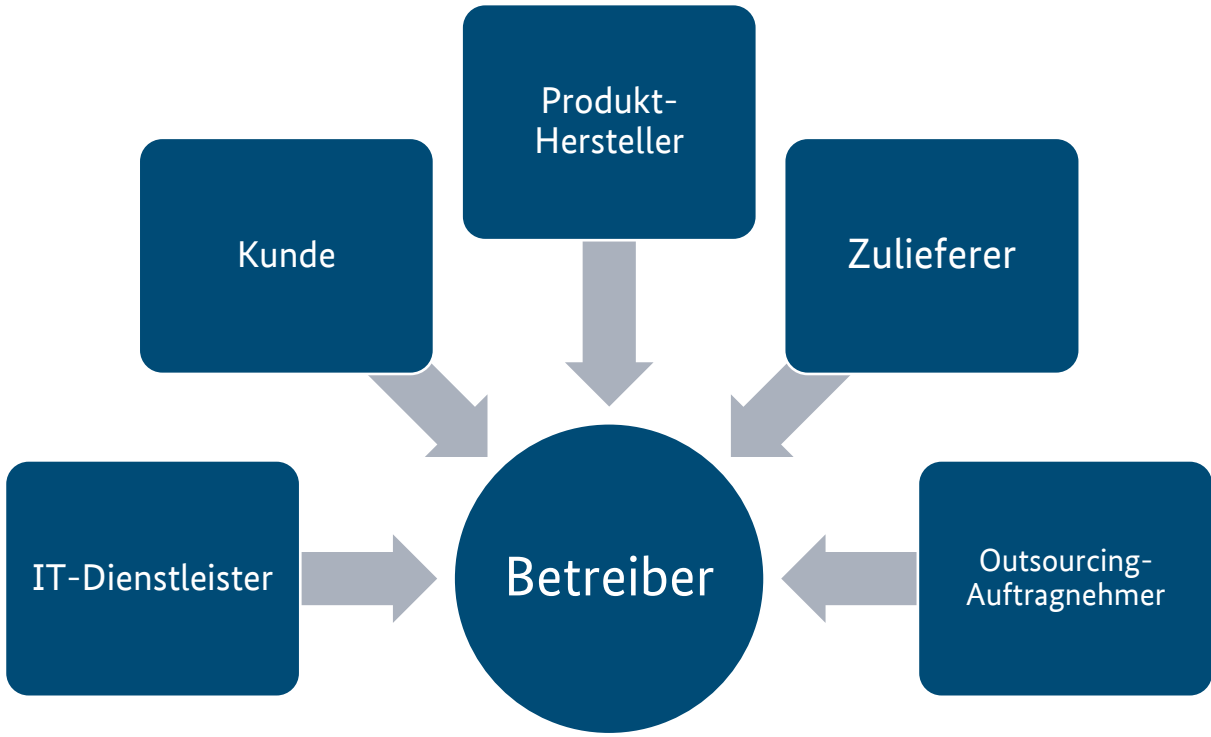


Abbildung 13: Ransomware-Opfer nach Zahlungsverhalten (Anteile) (Quelle: Coveware)

Supply Chain Angriffe

- Steigende Abhängigkeit und Vernetzung der IT-Infrastrukturen
- Mit Supply-Chain-Angriffen lassen sich potentiell große Anzahlen von IT-Netzen kompromittieren
- Cyber-Angriffe qualitativ immer ausgereifter und zielgerichteter
- Office-IT-Netze und Fernzugriffe als Einfallstor (Dienstleister, Home Office)
- Auch Software-Lieferketten betroffen (vgl. Log4j, Kaseya, NotPetya).



DeepFakes: Beispielszenarien

Überwindung biometrischer Systeme, z. B.

- Spracherkennung
- Video-Identifikation

Social Engineering

- Spear-Phishing
- CEO-Fraud

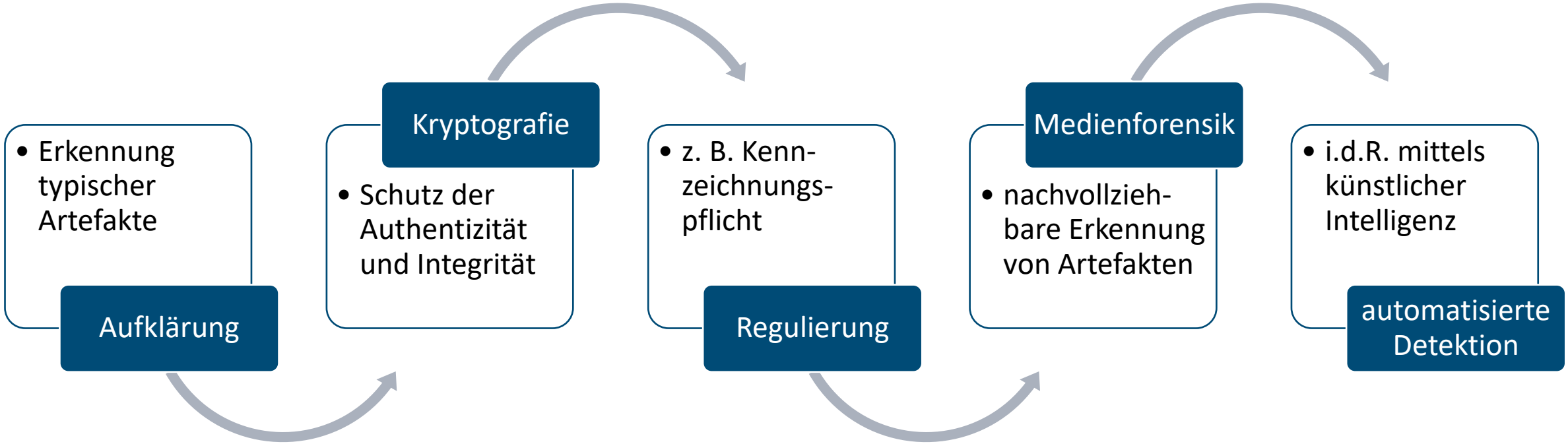
Desinformationskampagnen

- manipulierte Medieninhalte von Schlüsselpersonen

Verleumdung

- beliebige Aussagen
- beliebige Situationen

DeepFakes: Gegenmaßnahmen



Weiterführende Informationen des BSI

- Die Lage der IT-Sicherheit in Deutschland:
  https://www.bsi.bund.de/lageberichte
- Ransomware / Fortschrittliche Angriffe:
  https://www.bsi.bund.de/ransomware
- Künstliche Intelligenz:
  https://www.bsi.bund.de/ki
- IT-Grundschutz:
  https://www.bsi.bund.de/grundschutz

Vielen Dank für Ihre Aufmerksamkeit!

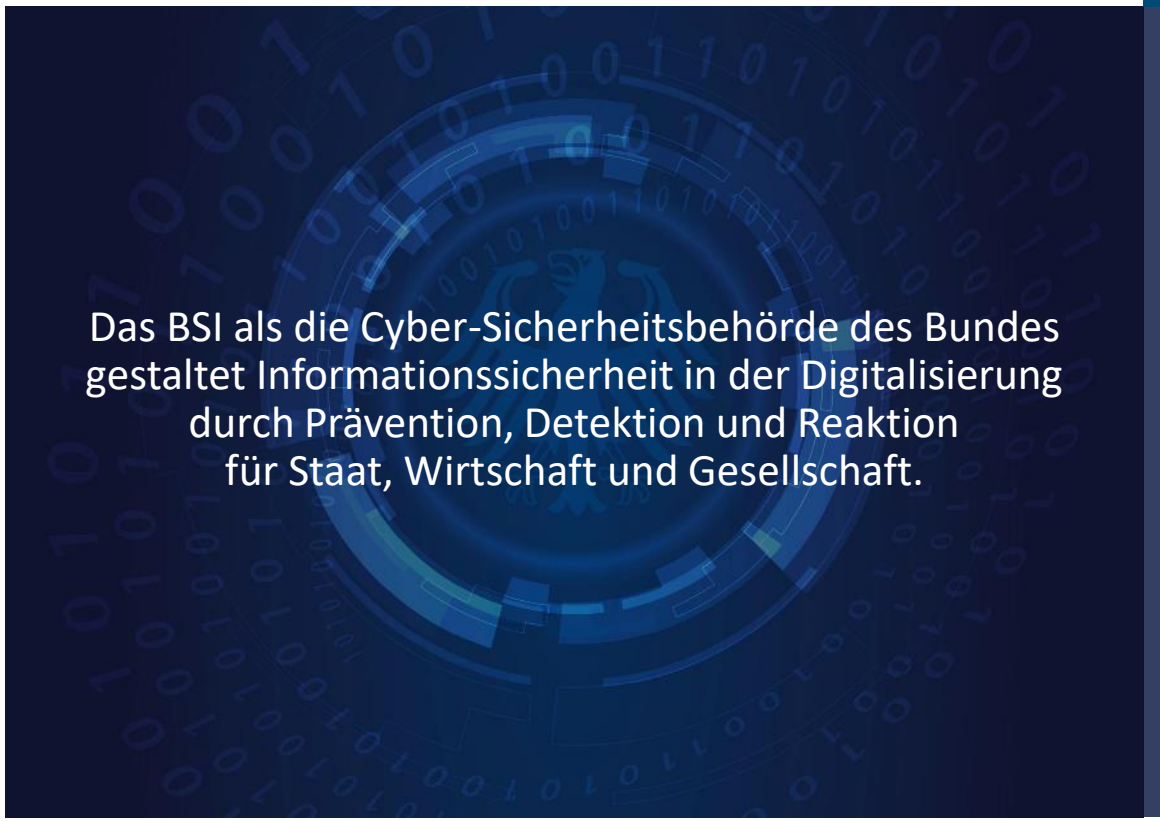
Deutschland
Digital•Sicher•BSI•

Kontakt

Dr. Harald Niggemann
Cyber Security Strategist

harald.niggemann@bsi.bund.de
Telefon: +49 (0) 228 9582 5368

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•