Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Aktuelles zur Cyber-Sicherheitslage

April 2024

Dr. Harald Niggemann

Vision

Strategische Ziele

Für die Cybernation werden folgende sechs strategische Ziele definiert, um uns in unserem Handeln zu leiten und die dazugehörigen Maßnahmen zu bündeln.

Cybersicherheit auf die Agenda heben

Cyberresilienz substantiell erhöhen

Technologie-kompetenz gezielt nutzen

Digitalisierung konsequent voranbringen

Cybersicherheit pragmatisch gestalten

Cybermarkt Deutschland aufbauen

Kurzprofil des BSI

Gründung
01. Januar 1991

217 Mio. Euro
Budget Haushalt 2022

Stellen 2022
1.733 ↗

183
Neue Stellen zum Vorjahr

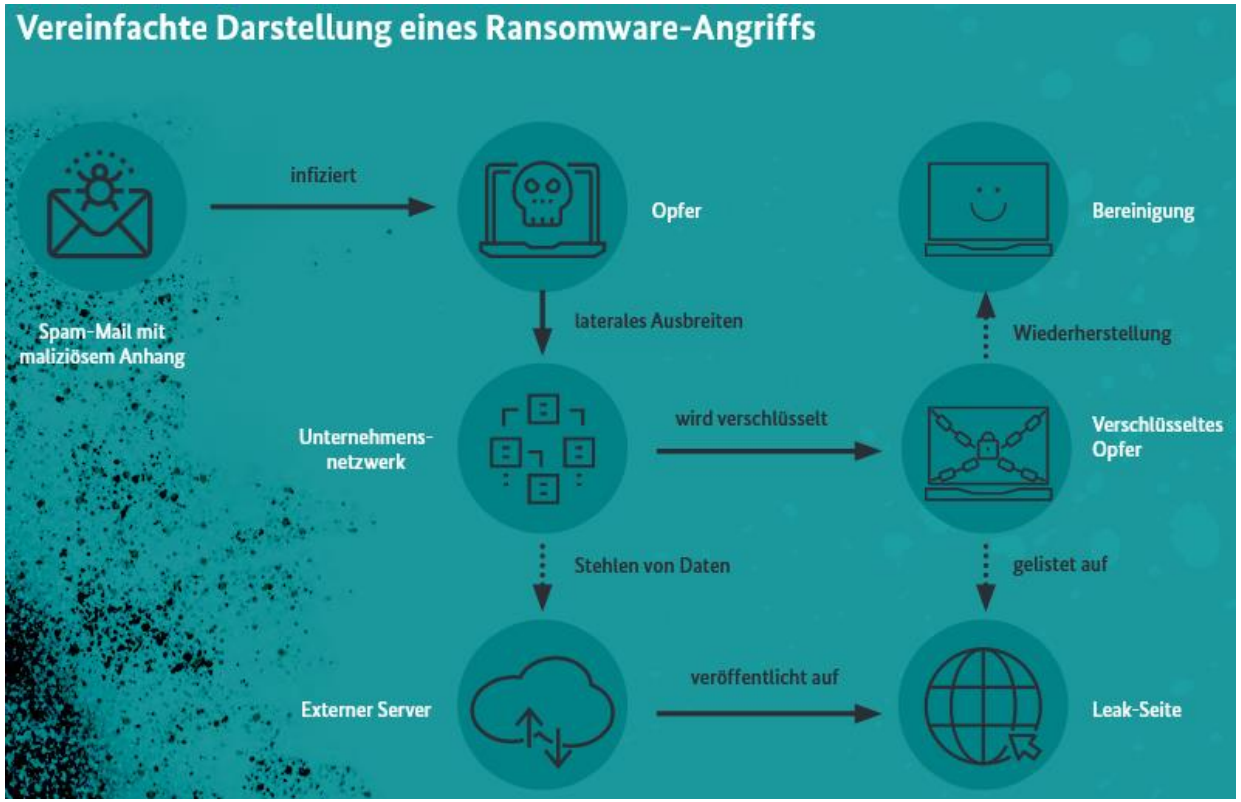
BSI vor Ort

- 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.

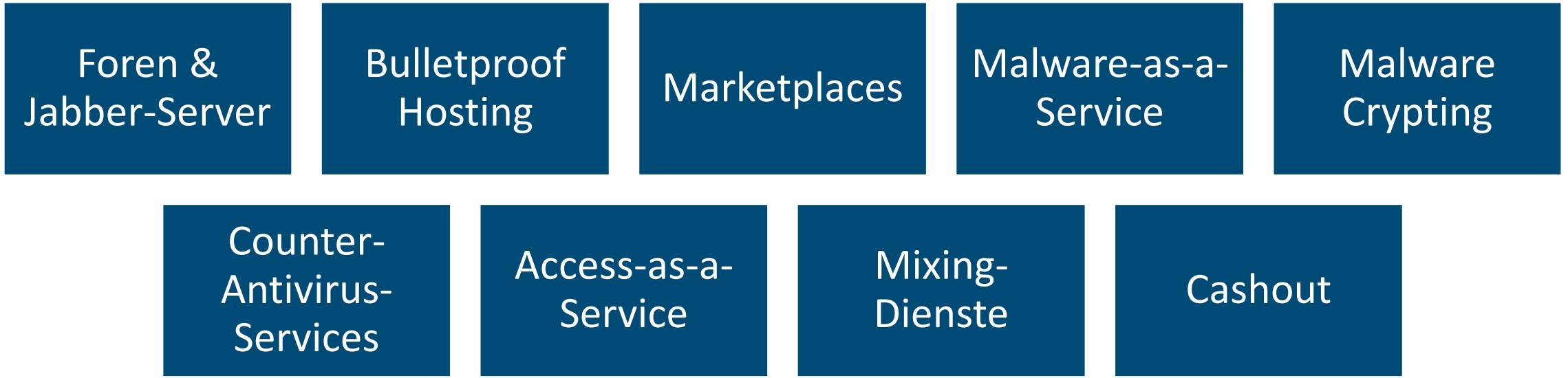
Ransomware

- **Größte operative Bedrohung**
- Qualität steigt stetig
- Ransomware als Dienstleistung (RaaS)
- **Gezielte Kampagnen** mit Double Extortion
- Angriffe mit hoher Agilität
- **BSI rät von Zahlungen ab!**



BSI-Magazin 2022/02:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2022_02.html

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



Trends bei der Erpressung im Big Game Hunting [1/2]

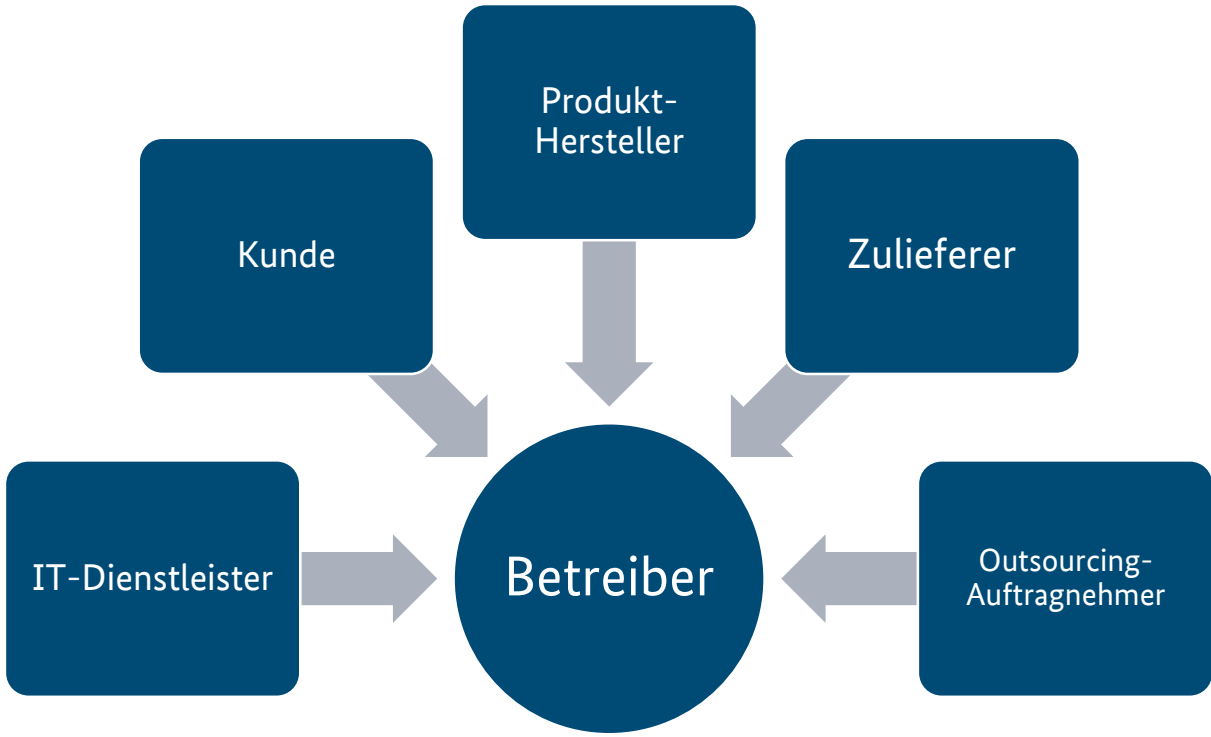
Daten-Leaks & -Verkäufe	• Daten-Leaks auf dedizierten Leak-Seiten erreichbar über Tor • Alternativ Auktionen und direkte Verkäufe
Presse informieren	• Direktes Ansprechen der Presse, auch mit gestohlenen Daten
Kunden & Partner informieren	• Beispielsweise automatisiert per E-Mail anhand von Adressen aus dem Daten-Leak
Datenschutzbehörden informieren	• Androhen eines Hinweises an Datenschutzbehörden wegen möglichen Datenschutzverstößen im Kontext von Daten-Leaks

Trends bei der Erpressung im Big Game Hunting [2/2]

DDoS-Angriffe	• In der Verhandlungsphase zur Erhöhung des Drucks
Telefonanrufe bei Mitarbeitern und Entscheidern	• Ermittlung wichtiger Mitarbeiter und Entscheider per OSINT oder aus Daten-Leak • Verschleierung durch Spoofing und Voice over IP
Insider-Handel für Short-Seller	• Angebot von exklusiven Informationen an Short-Seller
Erpressung von Kunden direkt	• Bei sehr sensiblen Informationen zusätzliche Erpressung der Kunden selbst

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).

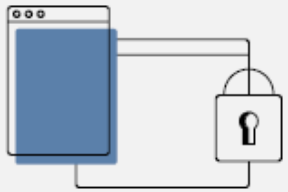


Die Lage der IT-Sicherheit in Deutschland 2023 im Überblick

Ransomware

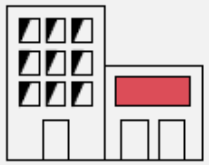
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

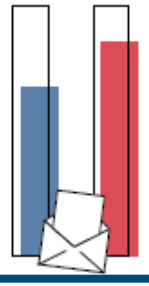
15 davon richteten sich gegen **IT-Dienstleister**.



Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

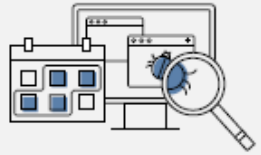
66% aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34 % Erpressungsmails,
32 % Betrugsmails



84% aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

Top-3-Bedrohungen je Zielgruppe:

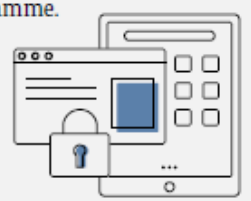
Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Phishing	***Ransomware*** Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Onlineserver	***Ransomware*** APT Schwachstellen, offene oder falsch konfigurierte Onlineserver



Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.



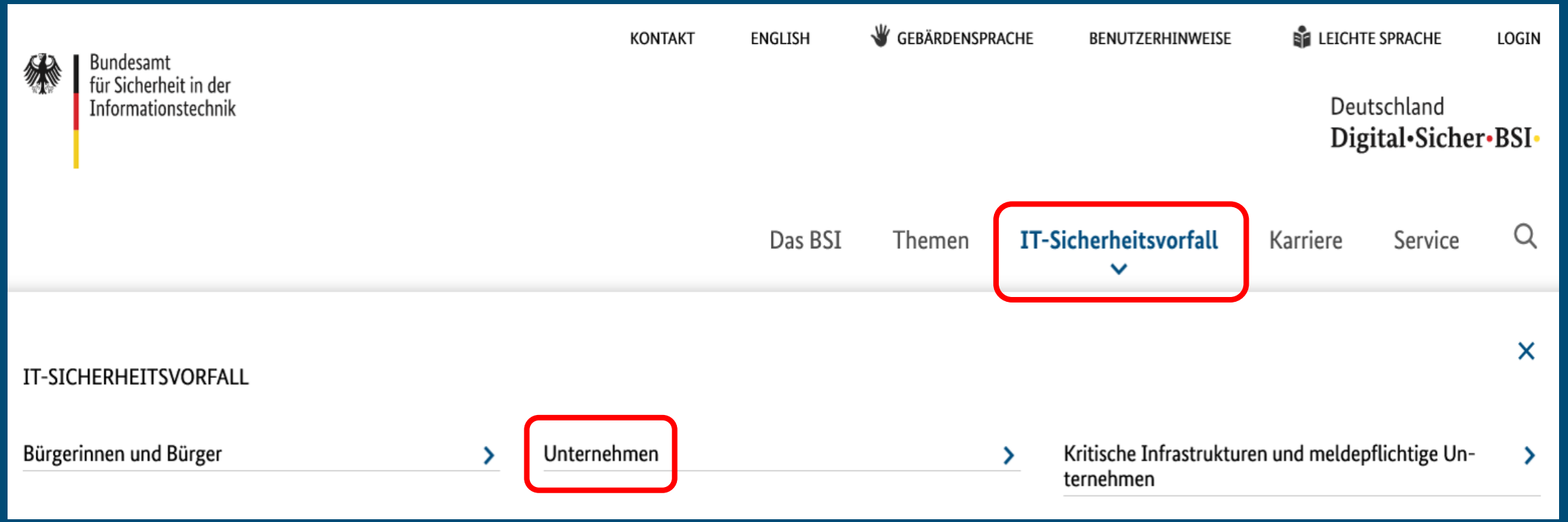
6.220 2022
5.100 2021

7.120 Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland Digital•Sicher•BSI•

Bundesamt für Sicherheit in der Informationstechnik

Informationsangebote auf BSI-Website [1]



Informationsangebote auf BSI-Website [2]

Ich habe einen Vorfall – Was soll ich tun?

› Mehr

Ich habe einen Vorfall – Checkliste Organisatorisches

› Mehr

Ich habe einen Vorfall – Checkliste Technik

› Mehr

Ich möchte einen IT-Sicherheitsvorfall melden.

› Mehr

Ich suche grundsätzliche Informationen, um mich vor einem IT-Sicherheitsvorfall zu schützen

› Mehr

Ich suche aktuelle Informationen über Bedrohungen.

› Mehr

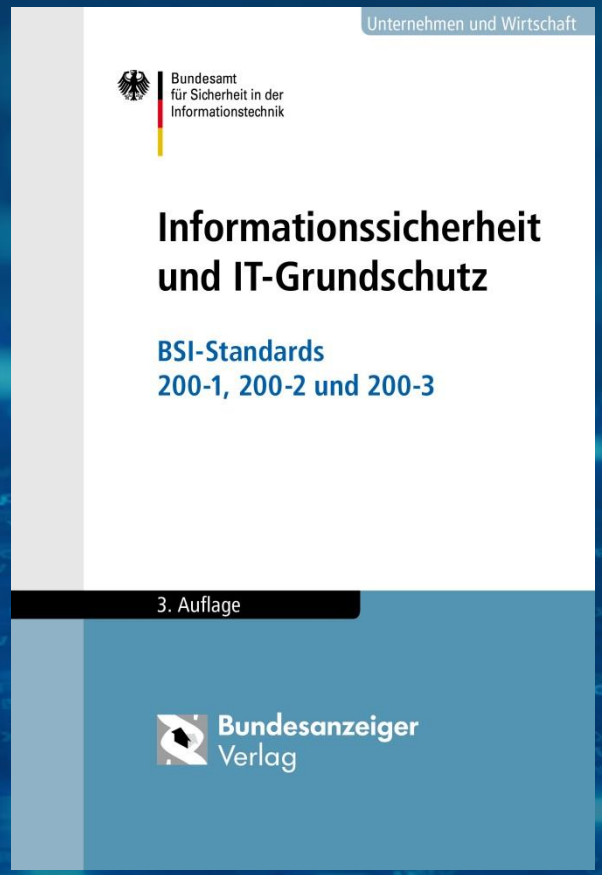
BSI-Standards zum IT-Grundschutz

Inhalt

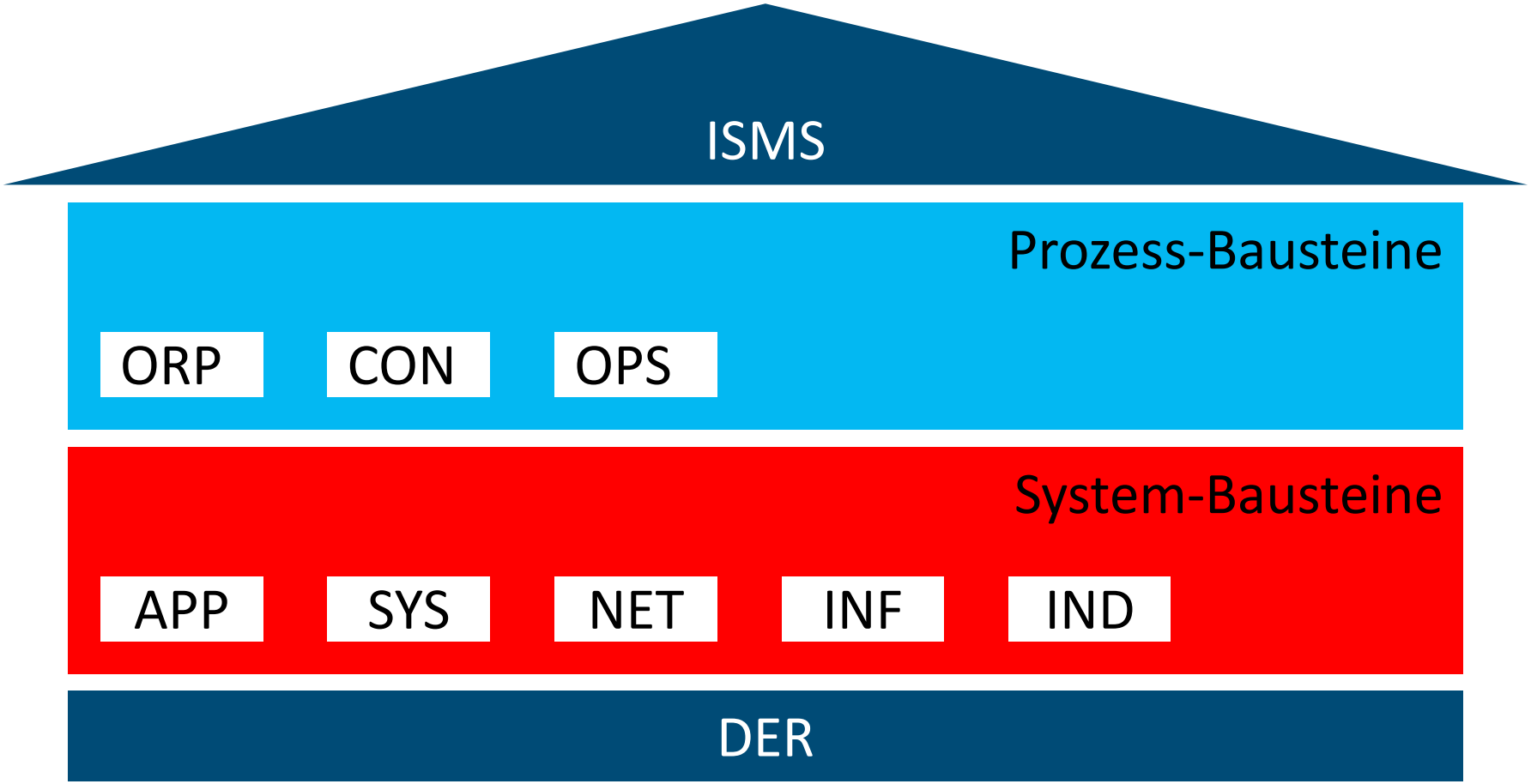
- Managementsysteme für Informationssicherheit
- IT-Grundschutz-Methodik
- Risikoanalyse auf der Basis von IT-Grundschutz

Verfügbare Versionen

- Kostenlos als PDF auf BSI-Webseite
- Kostenpflichtige gedruckte Version über Bundesanzeiger Verlag



IT-Grundschutz-Kompendium



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
- Kritische Infrastrukturen:
  https://www.bsi.bund.de/kritis
- IT-Grundschutz:
  https://www.bsi.bund.de/grundschutz

Vielen Dank für Ihre Aufmerksamkeit!

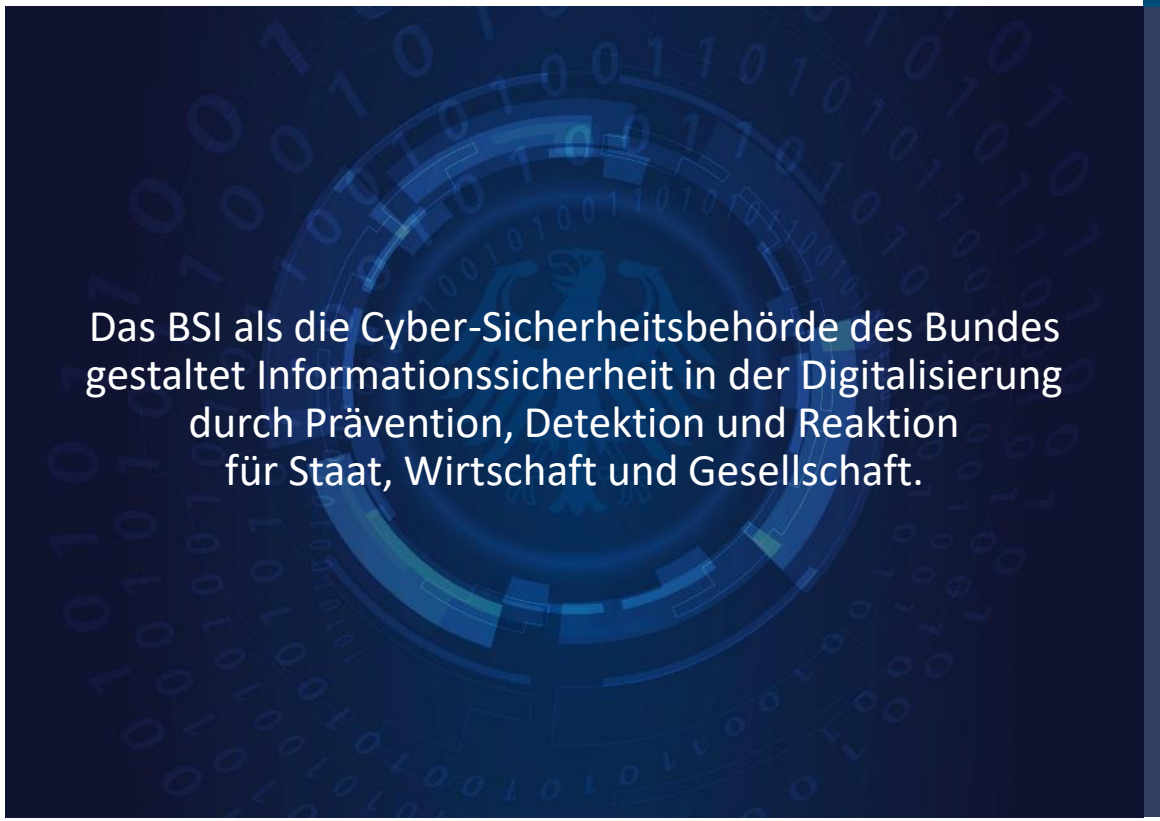
Deutschland
Digital•Sicher•BSI•

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•