Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Aktuelle Cyber-Gefahren für Kritische Infrastrukturen und andere Institutionen

März 2023

Dr. Harald Niggemann

Leitsatz

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Kurzprofil des BSI

Gründung
01. Januar 1991

217 Mio. Euro
Budget Haushalt 2022

Stellen 2022
1733 ↗

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.

Produkte und Dienstleistungen

Übernahme technischer Schutzmaßnahmen

Sichere mobile Lösungen, Schadsoftware-Prävention, Analysen, DDoS-Mitigation, IT-Notfallmanagement für Regierungsnetze, Angriffserkennung, Nationales IT-Lagezentrum, Technische Richtlinien (TR)

Kooperation

Nationales Verbindungswesen, Cyber-Sicherheitstage, IT-Grundschutztage, Jahrestagung der Informationssicherheits-beauftragten (ISB), Beirat Digitaler Verbraucherschutz, Cyber-Abwehrzentrum, Allianz für Cybersicherheit, UP KRITIS

Technische Unterstützung und Dienstleistungen

CERT-Bund, Kryptosysteme, Abstrahl-/Lauschabwehrprüfungen, IS-Penetrationstests, Mobile Incident Response Teams (MIRTs), technische Evaluierung, Malware Information Sharing Platform (MISP), Warnungen

Begleitung in der Aus- und Fortbildung

ISB-Ausbildung, Sensibilisierungsvorträge (u. a. Live Hacking), Übungszentrum Netzverteidigung

Beratung

Managementsystem für Informationssicherheit (ISMS), Abhörsicherheit, nach Vorfallsmeldungen, Unterstützung Digitalisierungsprojekte, Digitaler Persönlichkeits- und Verbraucherschutz, Gesellschaftlicher Dialog, Service-Center

Information

IT-Grundschutz, Mindeststandards, Technische Richtlinien (TR), CS-Empfehlungen, Liste zertifizierter und zugelassener Produkte, Lageberichte, Zertifizierungen, IT-Sicherheits-kennzeichen (IT-SiK)

Unterstützung durch das BSI bei Vorfällen

1 Vorbereitung

Cybersicherheits-Empfehlungen
BSI Grundschutz, ISi-Reihe, Mindeststandards, ...

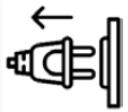
Sektorspezifische Papiere
B3S, Cyber-Sicherheitswarnungen

2 Identifikation

Netzwerke & Übungen
ACS, CV, UPKRITIS, G4C, ...

Meldestelle & Benachrichtigungen
Nationales IT-Lagezentrum , CERT-Bund Reports, ...

3 Eindämmung



Technische Unterstützung
Beratung, Analysen, IR, MIRT, ...

Detektion
BSOC, ...

4 Bereinigung

Management-Unterstützung
Support beim Incident Management & Kommunikation

Forensische Analysen
Host-/Net-/Log-Forensik, Malware Analyse

5 Wiederherstellung

Behördenkoordination
Cyber-Abwehrzentrum (BKA, BfV, BND, KdoCir, BBK, ...)

Expertenvermittlung
Qualifizierte Dienstleister

Umsetzung in Empfehlungen
Sektor, Branchen

6 Erkenntnisse

Wiederaufbau
(Beratung), Papiere, Zweitmeinung, ...

Threat-Intelligence & Sharing
TTPs, IOCs

Tiefenanalyse
Malware Reverse Engineering , ...

Schutz von KRITIS ist wesentlich für das Funktionieren der Gesellschaft.

Zunehmende Digitalisierung führt zu geänderter Bedrohungslage.

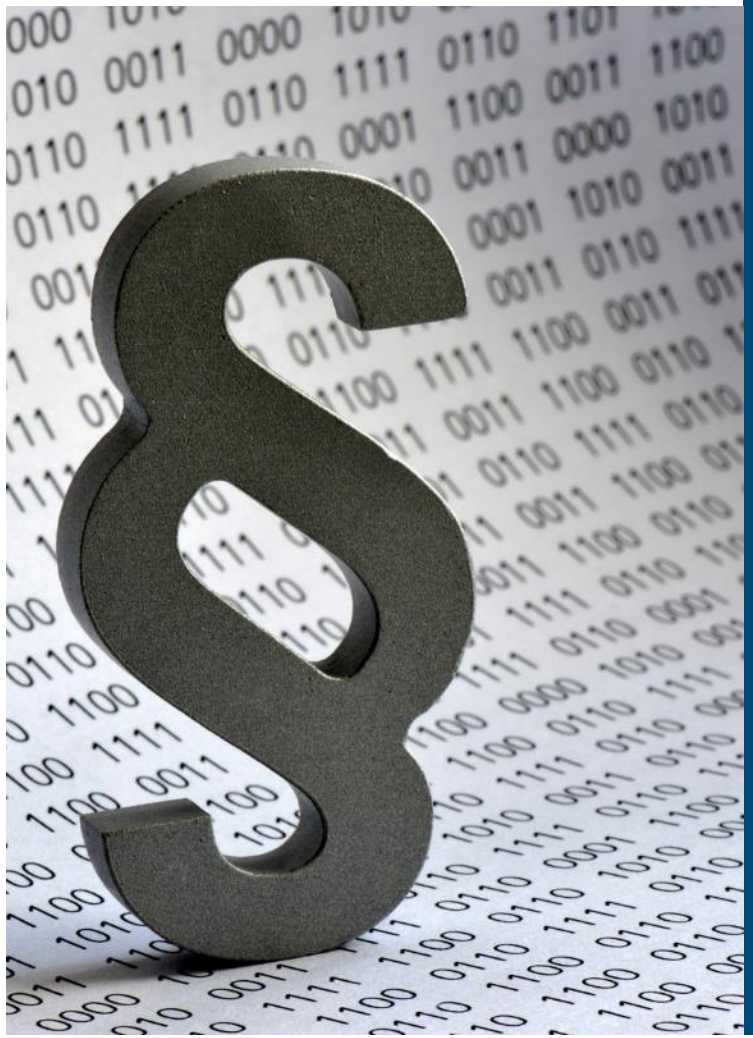
Stetige Weiterentwicklung der Schutzkonzepte ist erforderlich.

KRITIS-Sektoren

Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon aus folgenden Sektoren:

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Siedlungsabfallentsorgung

Regelungen des BSIG für KRITIS-Betreiber



Betreiber müssen

- gegenüber dem BSI eine Kontaktstelle benennen (§ 8b BSIG)
- ihre (für kritische Versorgungsleistungen erforderliche) IT absichern
- diese Absicherung mindestens alle zwei Jahre gegenüber dem BSI nachweisen (§ 8a BSIG)
- erhebliche Vorfälle dem BSI melden (§ 8b BSIG, EnWG, TKG, AtG).

Betreiber können

- Branchenspezifische Sicherheitsstandards („B3S“) vorschlagen und vom BSI anerkennen lassen
- SPOCs einrichten.

UP KRITIS

Teilnehmer:

- Betreiber Kritischer Infrastrukturen
- Verbände
- Zuständige Behörden

UP KRITIS

Produkte des UP KRITIS:

- Teilnahme an Branchen- und Themenarbeitskreisen
- Positionspapiere
- Arbeitshilfen (z. B. Security Level Agreement)
- Meldewesen und Diskussion von Vorfällen
- Krisenmanagementstrukturen
- Koordinierte Krisenreaktion und -bewältigung
- Teilnahme an Notfall- und Krisenübungen
- Gemeinsames Handeln gegenüber Dritten

Überblick

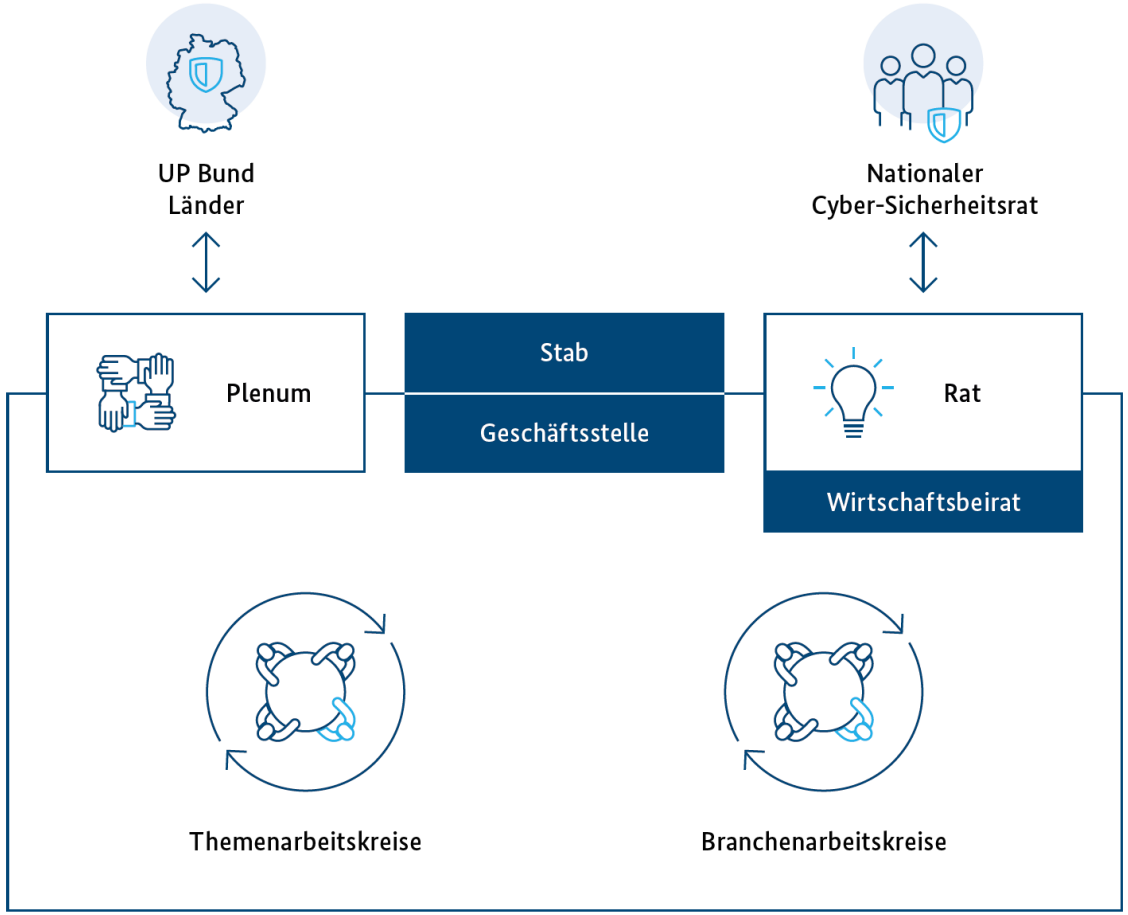
Öffentlich-private Kooperation zwischen

- Betreibern Kritischer Infrastrukturen,
- deren Verbänden und
- den zuständigen staatlichen Stellen.

Ziel: Aufrechterhaltung der Versorgung mit kritischen Infrastrukturdienstleistungen in Deutschland.

Strategisch-konzeptionelle Mitarbeit

- Fachliche und politische Gremien
- Cybersicherheit ist ein Schwerpunkt der Arbeiten.



Lageübersicht

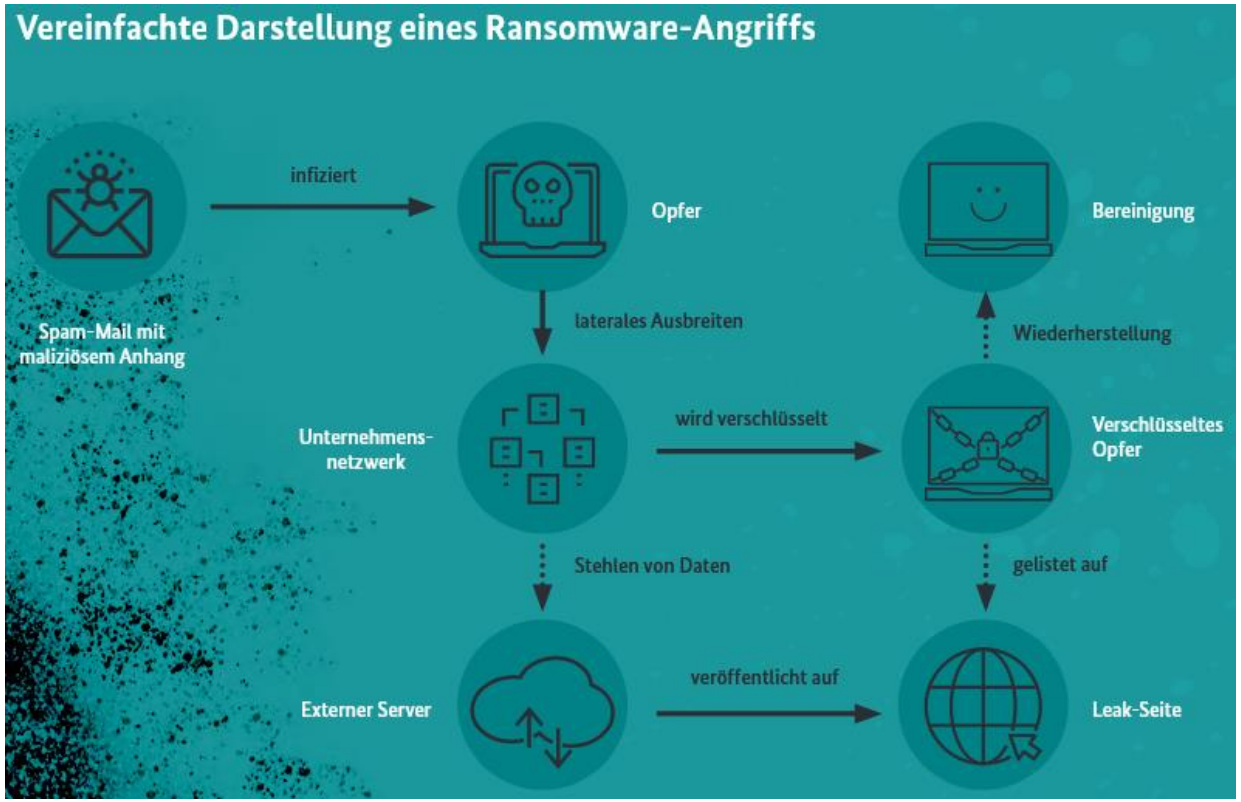
- Durch den russischen Angriffskrieg gegen die Ukraine hat sich die **Bedrohungslage in Deutschland insgesamt weiter erhöht**.
- Die Vorfälle im Kontext des Krieges in der UKR treffen auf **eine ohnehin angespannte Bedrohungslage** (insbesondere durch Ransomware).
- **Cybercrime** ist eine stetig zunehmende Bedrohung.
- **Zunehmende Vernetzung und Abhängigkeiten** der Lieferketten erhöhen die Angriffsfläche.
- **Ransomware** ist **derzeit eine der größten Bedrohungen** für die IT von Unternehmen / Organisationen.
- **Big Game Hunting**: Trend zu gezielten Angriffen auf Unternehmen.

Cyber-Sicherheitslage im Kontext Ukraine-Krieg

- Seit Beginn des Krieges sind eine **Reihe von Aktivitäten** im Cyber-Raum zu beobachten.
- Bisher vor allem **unzusammenhängende Einzelereignisse**.
  Keine zentral gesteuerte Kampagne, wie in einem Hybriden Krieg erwartet, erkennbar.
- Das vermutete **Potenzial von Cyber-Kampagnen** wird nach derzeitigem Kenntnisstand von keiner Seite **ausgeschöpft**.
- Für Deutschland und Europa besteht eine **erhöhte Gefährdungslage**.
- Die Cyber-Sicherheitslage ist **weiterhin durch Hacktivismus geprägt**.
- Seit Ende April 2022 beobachtet das BSI wiederholt **DDoS-Angriffe von Hacktivisten** auf **Ziele in Deutschland und international**.

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

01/2023: Weltweiter Ransomware-Angriff

- Laut Medienberichten **tausende ESXi-Server verschlüsselt**.
- ESXi-Server werden u. a. zur Virtualisierung von IT-Fachverfahren genutzt.
- **Schwerpunkt der Angriffe** lag dabei auf Frankreich, den USA, Deutschland und Kanada.
- Wahrscheinlich eine **bereits im Februar 2021 gepatchte Schwachstelle** als Angriffsvektor ausgenutzt.
- Das BSI hatte zu dieser Zeit vor der Ausnutzung von Schwachstellen im entsprechenden Produkt gewarnt.
- Das BSI hat eine aktuelle Cyber-Sicherheitswarnung mit **Schutzmaßnahmen veröffentlicht**.

01/2023: DDoS-Kampagne gegen ausgewählte Ziele in DE

- **Angriffe insbesondere auf Websites** von Flughäfen und einzelne Ziele im Finanzsektor.
- Websites der angegriffenen Unternehmen waren **zeitweise nicht erreichbar**.
- Angriffe waren von der russischen Hackergruppierung **Killnet** angekündigt worden.
- **Angriffe auf Websites der Bundes- und Landesverwaltung** konnten größtenteils **abgewehrt** werden und sind **ohne gravierende Auswirkungen** geblieben.

12/2022: Stadt Potsdam: Hinweise auf Cyber-Angriff

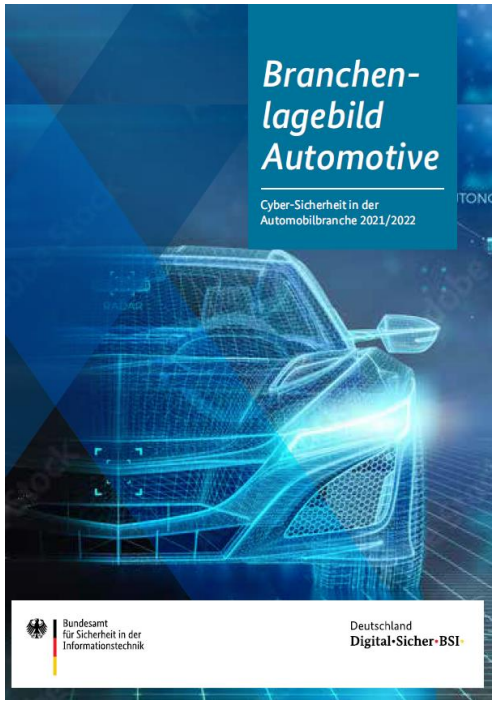
- Warnung der Sicherheitsbehörden des Landes Brandenburg vor einem unmittelbar bevorstehenden Cyber-Angriff.
- IT-Systeme am 29.12.2022 präventiv vom Internet getrennt.
- **Brute-Force-Angriff** auf IT-Systeme detektiert.
- Fachverfahren und **Dienstleistungen für Bürger eingeschränkt**.
- **Schrittweise Wiederaufnahme** des Betriebs.
- Die Stadt Potsdam war bereits Anfang des Jahres 2020 Ziel eines Cyber-Angriffs.

11/2022: Ransomware-Angriff auf Klinikverbund Lippe

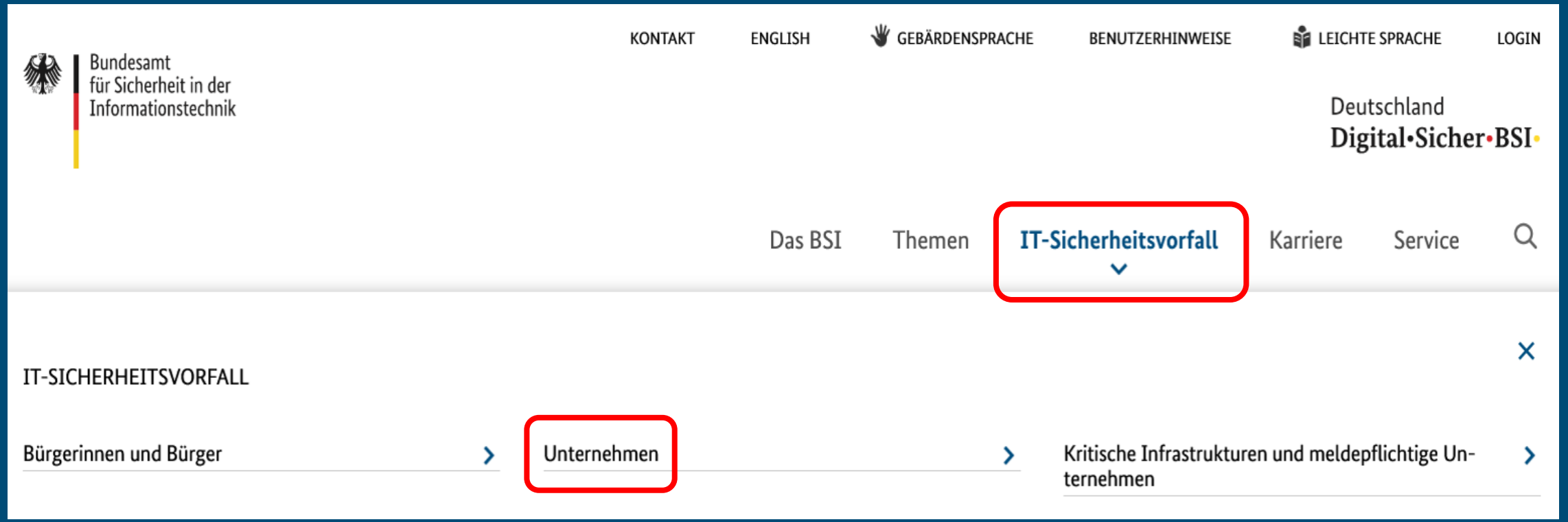
- IT-Systeme im Klinikverbund heruntergefahren.
- **Mehrere Standorte betroffen**.
- Deutliche **Einschränkungen im Krankenhaus-Betrieb**.
- Planbare Operationen und Behandlungen zunächst ausgesetzt.
- **Notfallversorgung gewährleistet**.
- Unterstützung durch externen Dienstleister.
- Verschlüsselte **Daten aus vorhandener Datensicherung wiederhergestellt**.

09/2022: Cyber-Sicherheit im Bereich „Automotive“

- Das BSI hat am 19.09.2022 die **zweite Auflage** des Branchenlagebild Automotive vorgestellt.
- **Cyber-Sicherheit ist der Schlüssel für eine funktionierende Automobilindustrie!**
- **Erneut mehrere Ransomware-Vorfälle** bei Automobilzulieferern.
- Neben den bestehenden Auswirkungen der **COVID-19**-Pandemie wird die Lage maßgeblich durch den **Krieg in der Ukraine** geprägt.
- **Neuregelungen** für UBI und im EU-Typgenehmigungsrecht.
- **Enge Zusammenarbeit** BSI – KBA und VDA.



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

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!

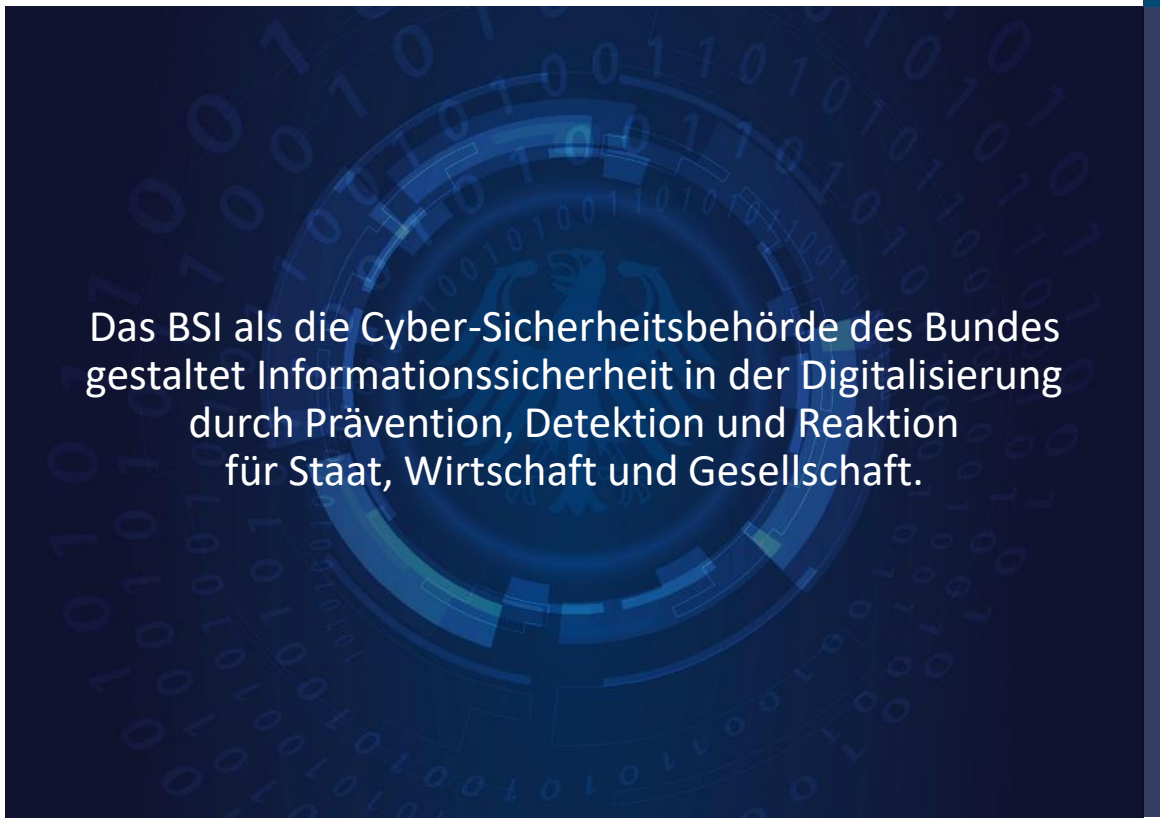
Deutschland
Digital•Sicher•BSI•

Kontakt

Dr. Harald Niggemann

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

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•