Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

KI und andere Trends im Hacking und Social Engineering

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

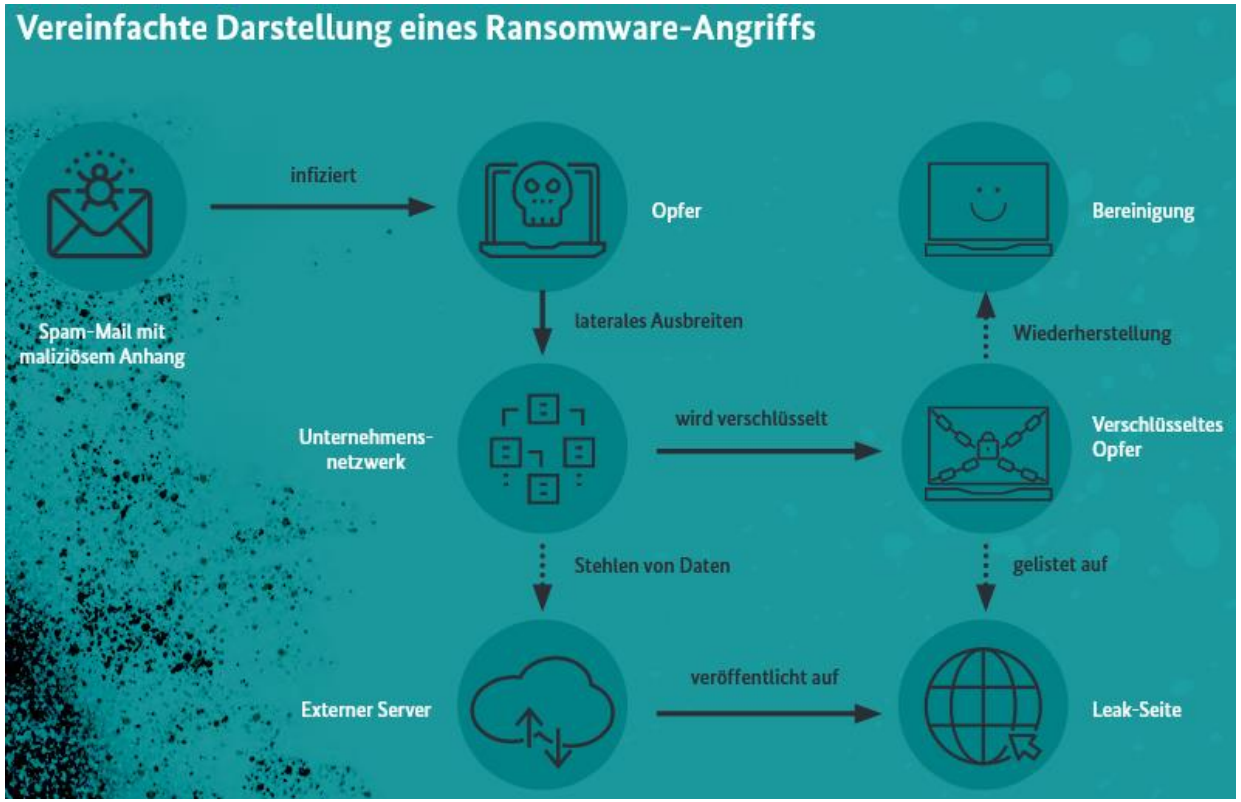
BSI vor Ort

- 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

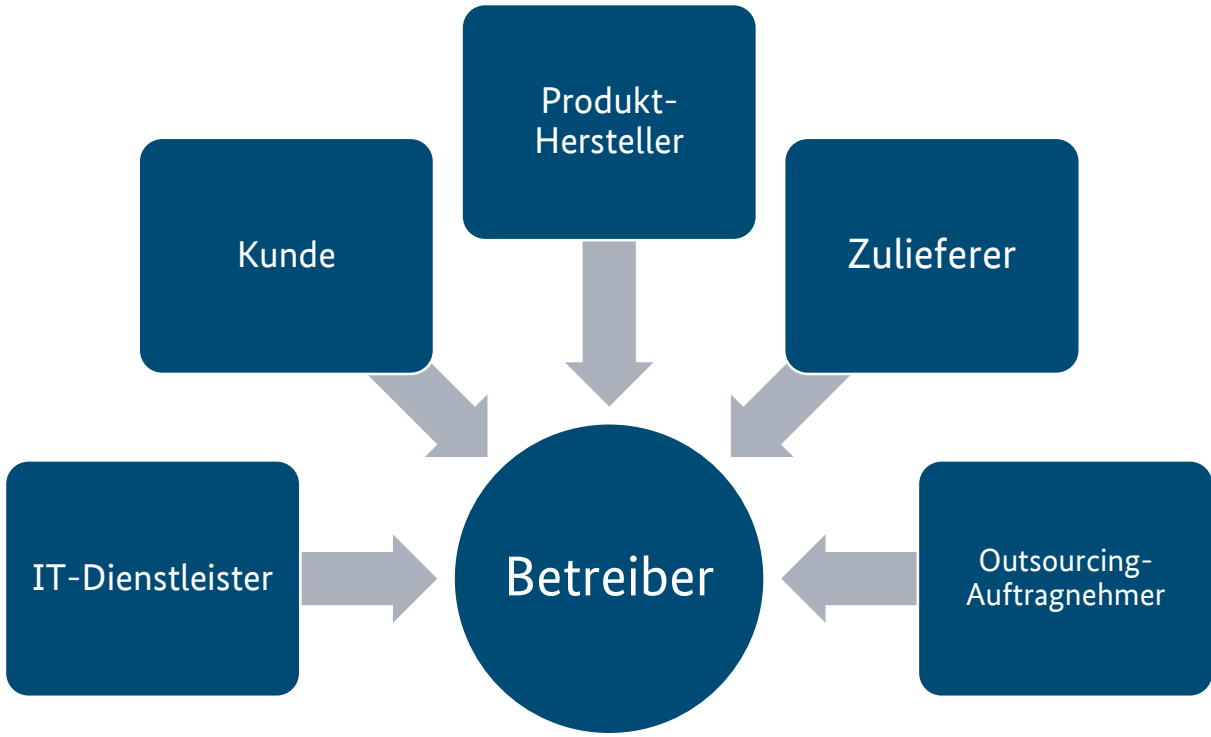
- **Größte operative Bedrohung**
- Qualität steigt stetig
- Ransomware als Dienstleistung (RaaS)
- **Gezielte Kampagnen** mit Double Extortion
- Angriffe mit hoher Agilität
- **BSI rät von Zahlungen ab!**



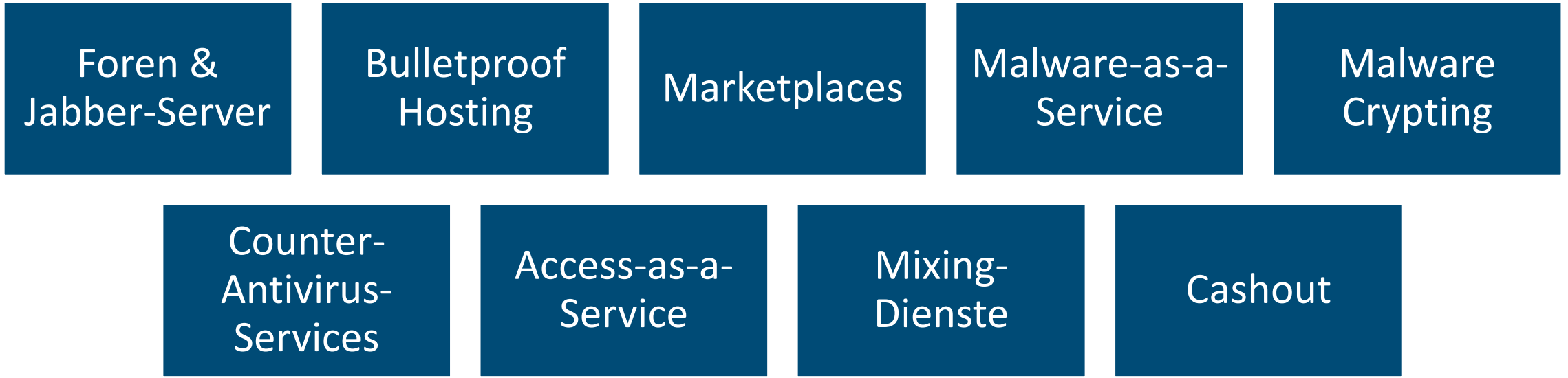
BSI-Magazin 2022/02:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2022_02.html

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).



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

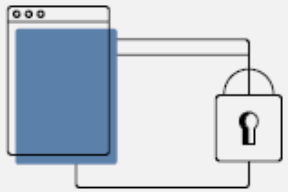


Die Lage der IT-Sicherheit in Deutschland 2023 im Überblick

Ransomware

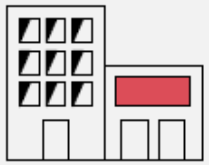
ist weiterhin die größte Bedrohung.

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**.



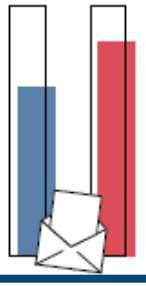
Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

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	***Ransomware***	***Ransomware***
Sextortion	Abhängigkeit innerhalb der IT-Supply-Chain	APT
Phishing	Schwachstellen, offene oder falsch konfigurierte Onlineserver	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

Gefahren durch DeepFakes – Beispiele

Gesichter

- Face Swapping
- Face Reenactment

Stimmen

- Text-to-Speech
- Voice Conversion

Texte

- etc. pp.

DeepFakes: Beispielszenarien

Überwindung biometrischer Systeme, z. B.

- Spracherkennung
- Video-Identifikation

Social Engineering

- Spear-Phishing
- CEO-Fraud

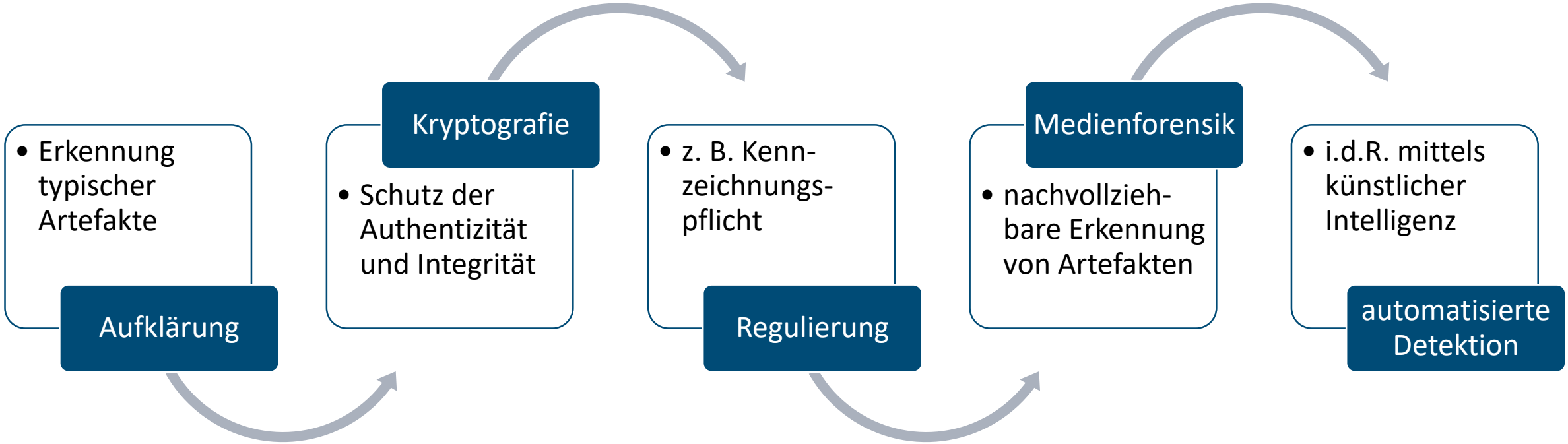
Desinformationskampagnen

- manipulierte Medieninhalte von Schlüsselpersonen

Verleumdung

- beliebige Aussagen
- beliebige Situationen

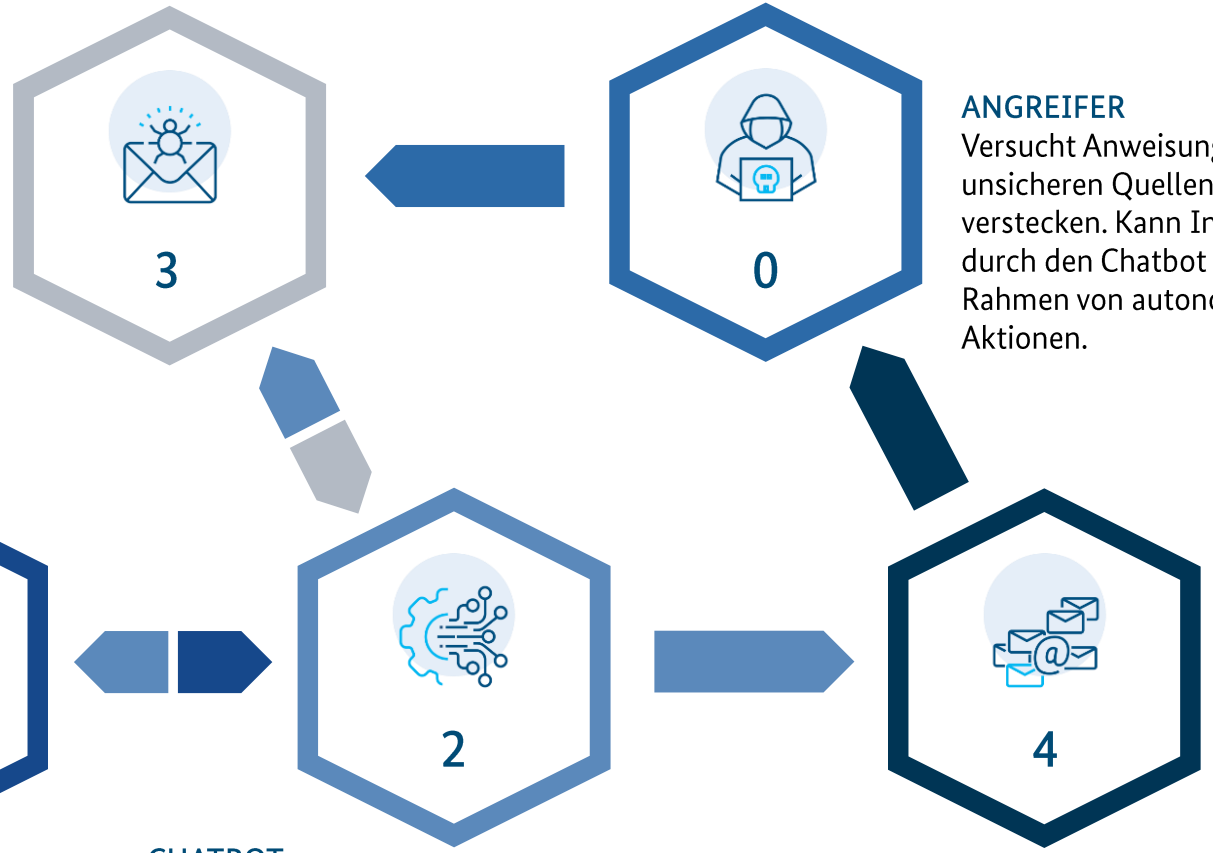
DeepFakes: Gegenmaßnahmen



Indirect Prompt Injections – Intrinsische Schwachstelle in anwendungsintegrierten KI-Sprachmodellen

- Große KI-Sprachmodelle (LLMs) werden beispielsweise eingesetzt für
  - automatisierte Textverarbeitung
  - chatbasierte Assistenz.
- Wenn LLMs ungeprüfte Daten aus unsicheren Quellen verarbeiten, besteht eine Gefahr durch Indirect Prompt Injections.
- Angreifer können Daten in unsicheren Quellen u. U. manipulieren und auf diese Weise dort unerwünschte Anweisungen für LLMs platzieren.
- Weiterführende Informationen:
  - https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-249034-1032_csw.html

Indirect Prompt Injections



UNSICHERE QUELLEN
E-Mails, Websites, Nutzerdokumente können dem Chatbot wichtige Informationen liefern. Allerdings können sie unsicher sein.

ANGREIFER
Versucht Anweisungen in unsicheren Quellen zu verstecken. Kann Informationen durch den Chatbot erhalten im Rahmen von autonomen Aktionen.

NUTZER
Person, die den Chatbot für verschiedene Aufgaben verwendet, indem sie Anfragen sendet und Antworten erhält.

AKTIONEN
Durch das LLM autonom ausgeführte bzw. ausgelöste Aktionen, z. B. Senden einer E-Mail oder Aufruf einer URL.

CHATBOT
Greift auf zusätzliche, potenziell unsichere Datenquellen zu, um die Ausgaben zu verbessern. Verarbeitet Daten und beantwortet Usereingaben oder/und handelt autonom.

In Kürze: Neue BSI-Studie zum Thema "How is AI changing the cyber threat landscape?"

Table of Contents

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!

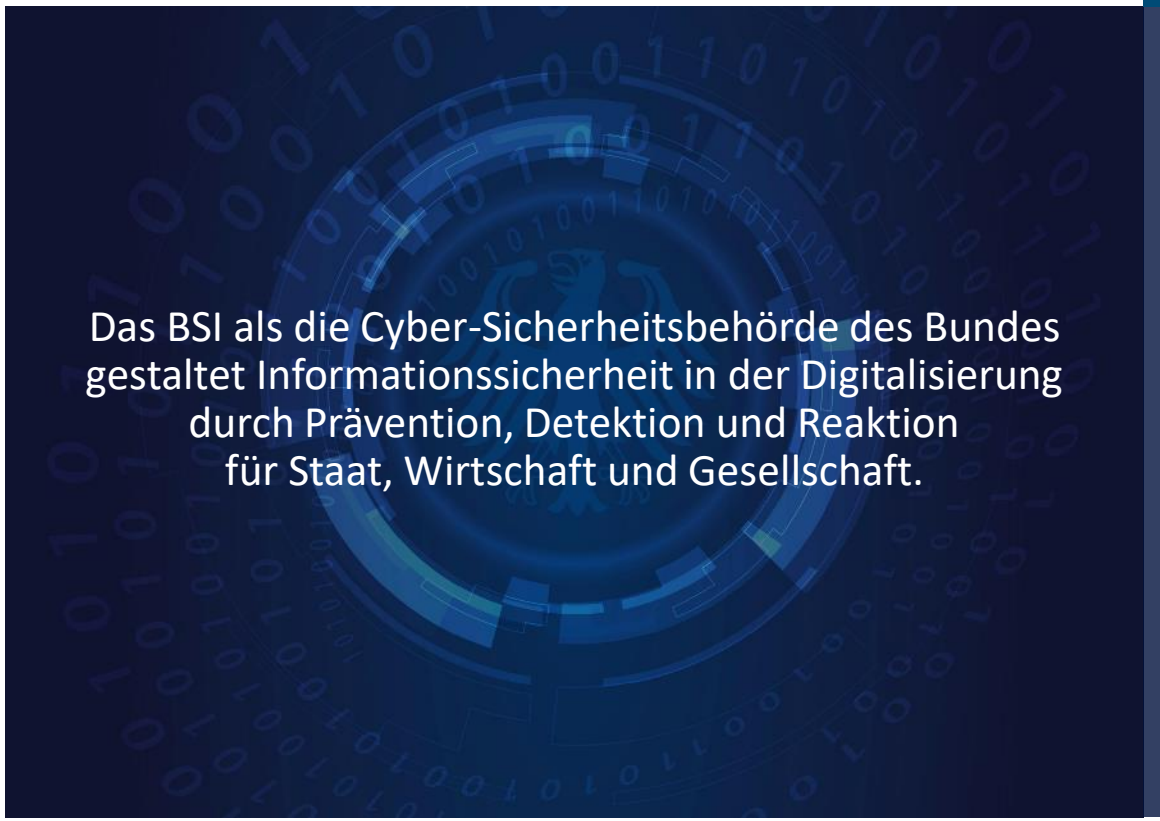
Deutschland
Digital•Sicher•BSI•

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•