Leibniz Universität Hannover

LUIS Kundentagung 2023 / Lagebericht zur IT-Sicherheit

- Die Lage der IT-Sicherheit in Deutschland 2023 (*BSI-Lagebericht*)
- Aktuelle Sicherheitslage der LUH
- Die Awareness-Kurzfilme der LUH

BSI Lagebericht 2023

Leibniz Universität Hannover

A Bedrohungslage

B Gefährdungslage

C Herausgehobene Trends in der IT-Sicherheit

BSI Lagebericht 2023

Leibniz Universität Hannover

A Bedrohungslage
- Angriffsmittel
- Angriffsarten
- Schwachstellen
- Große KI-Sprachmodelle

B Gefährdungslage

C Herausgehobene Trends in der IT-Sicherheit

BSI Lagebericht 2023

Leibniz Universität Hannover

A Bedrohungslage

Angriffsmittel
Angriffsarten
Schwachstellen
Große KI-Sprachmodelle

B Gefährdungslage

Erkenntnisse zur Gefährdungslage in der Gesellschaft
Erkenntnisse zur Gefährdungslage in der Wirtschaft
Erkenntnisse zur Gefährdungslage in Staat und Verwaltung

C Herausgehobene Trends in der IT-Sicherheit

BSI Lagebericht 2023

A Bedrohungslage

Angriffsmittel
Angriffsarten
Schwachstellen
Große KI-Sprachmodelle

B Gefährdungslage

Erkenntnisse zur Gefährdungslage in der Gesellschaft
Erkenntnisse zur Gefährdungslage in der Wirtschaft
Erkenntnisse zur Gefährdungslage in Staat und Verwaltung

C Herausgehobene Trends in der IT-Sicherheit

Künstliche Intelligenz
Quantentechnologien
Sicherheit moderner Telekommunikationsinfrastrukturen (5G/6G)
eID: Novellierung der eIDAS-Verordnung
Bund-Länder-Zusammenarbeit

BSI Lagebericht 2023

Leibniz Universität Hannover

BPK zur Vorstellung des Berichts (96 S.) am 2.11.2023

27 Kommunalverwaltungen sind gefallen

Die Lage ist „besorgniserregend"

Schaden: 206 Mrd. Euro (43% des Bundeshaushalts)

70 neue Schwachstellen pro Tag (+24%)

21000 Systeme fallen pro Tag

250000 Schadsoftware-Varianten pro Tag

Ransomware ist das dringendste Problem

- Arbeitsteilung
- Datendiebstahl und Erpressung

Spionage (wirtschaftlich und politisch)

Sabotage

politische Einflussnahme und Desinformation

- KI Content und KI Angriffe

Trusted Channel

- vertrauenswürdige Produkte mit Siegel?

Deutschland muss Cybernation werden

BSI Lagebericht 2023
Bedrohungslage

Leitbegriffe

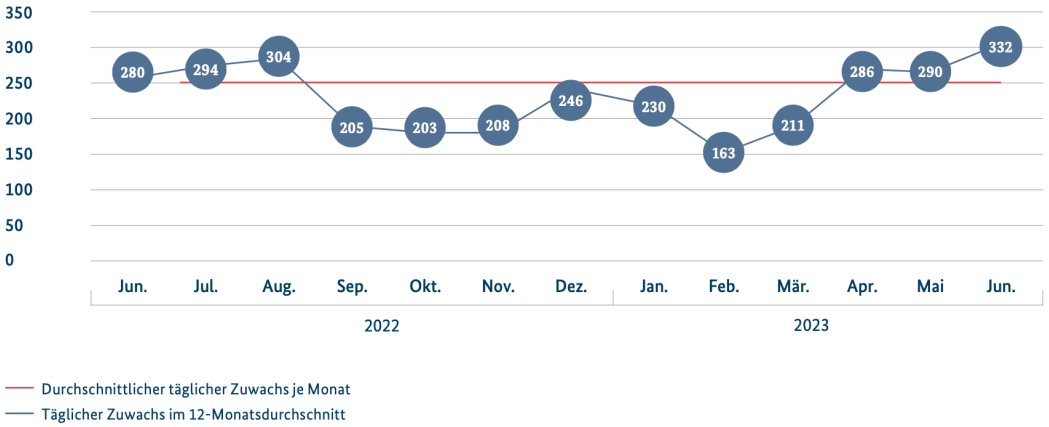
- Ausbau cyberkrimineller Schattenwirtschaft
- Cyberresilienz
- DDoS-Hacktivismus
- Advanced Persistent Threat
- Schwachstellen
- In der Umsetzung: Patching, Updates, IAM, Backup, Notfallpläne

Angriffsmittel

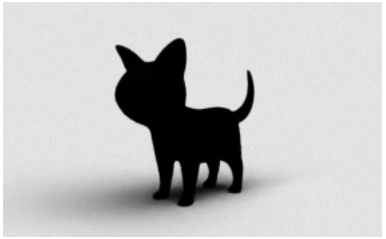
- Neue Schadprogramm-varianten
- Botnetze

Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten
Anzahl in Tausend

Abbildung 1: Durchschnittlicher täglicher Zuwachs neuer Schadpraogramm-Varianten
Quelle: *Malware*-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH



BSI Lagebericht 2023
Bedrohungslage



Angriffsarten

Ransomware

Angreifermotivation und Angriffsablauf

Cyberkriminelle Schattenwirtschaft

Schweigegeld-Erpressung mit Datenleaks und weitere Methoden

Mutmaßliche Opfer aus Deutschland auf Leak-Seiten
Anzahl

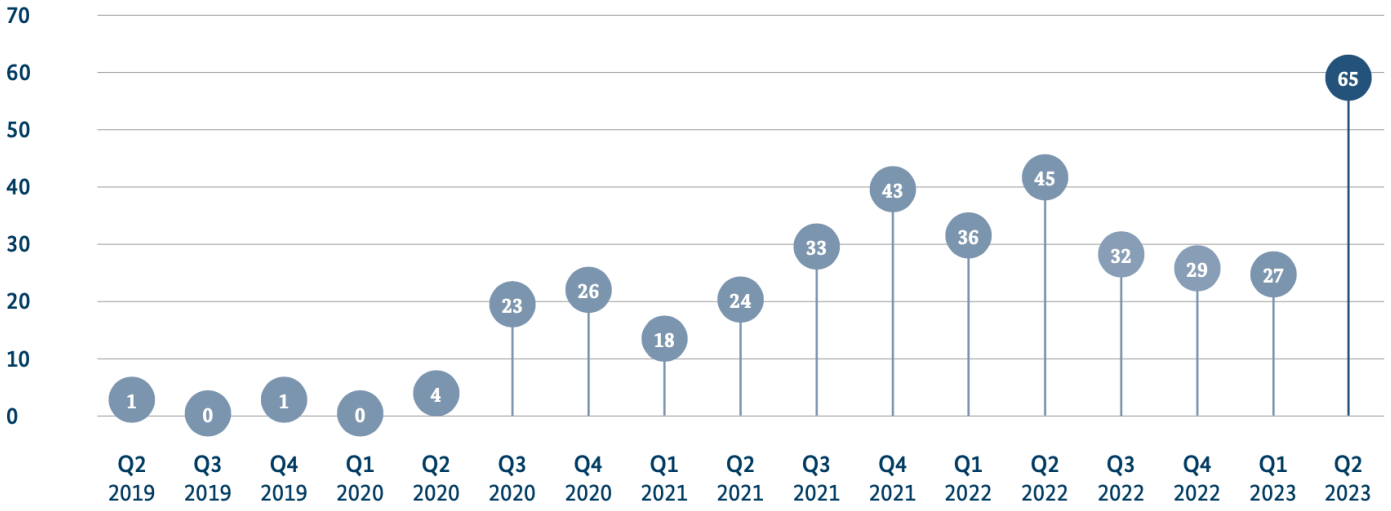


Abbildung 3: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten (Anzahl)
Quelle: Leak-Opfer-Statistik des BSI

BSI Lagebericht 2023
Bedrohungslage

Bekannt gewordene *Ransomware*-Opfer in Deutschland im Berichtszeitraum nach Art des Opfers
Anzahl

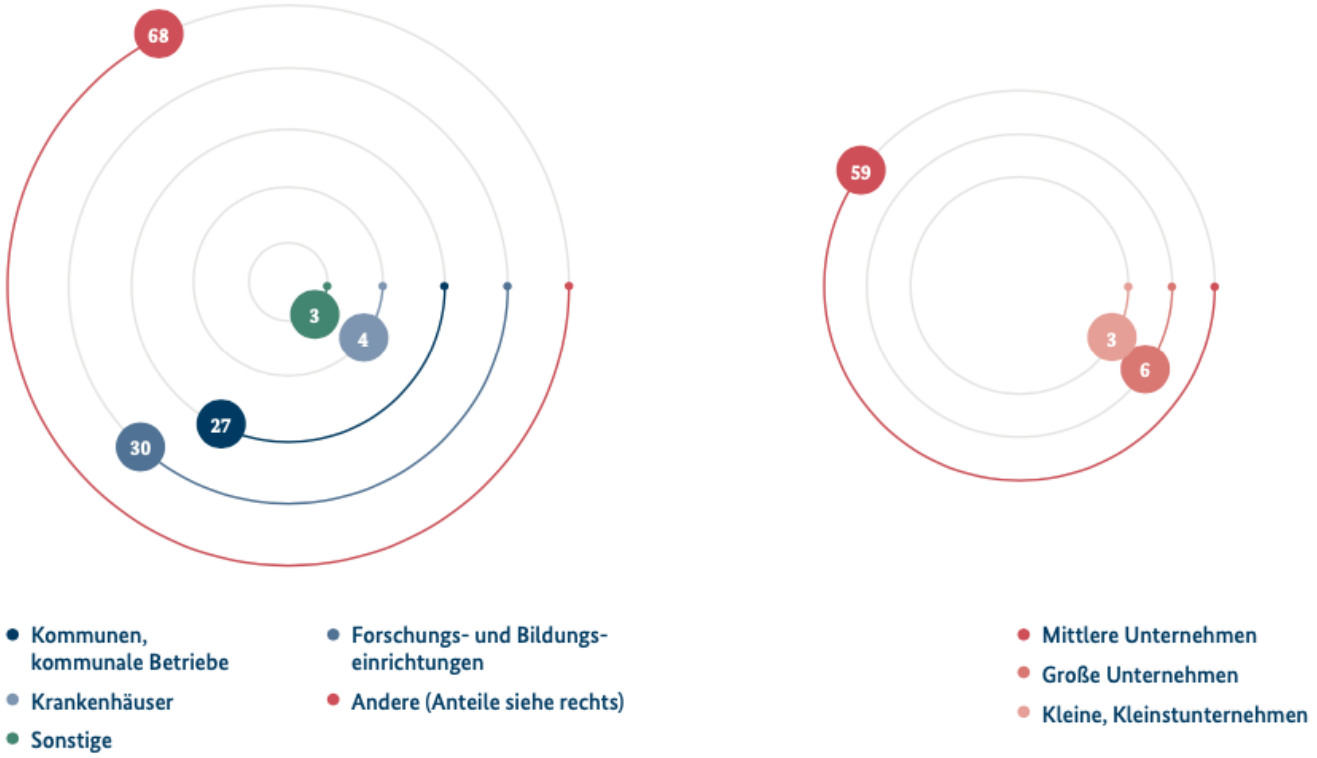


Abbildung 16: Bekannt gewordene *Ransomware*-Opfer in Deutschland
Quelle: *Ransomware*-Opfer-Statistik des BSI

BSI Lagebericht 2023
Bedrohungslage

Angriffsarten

DDoS

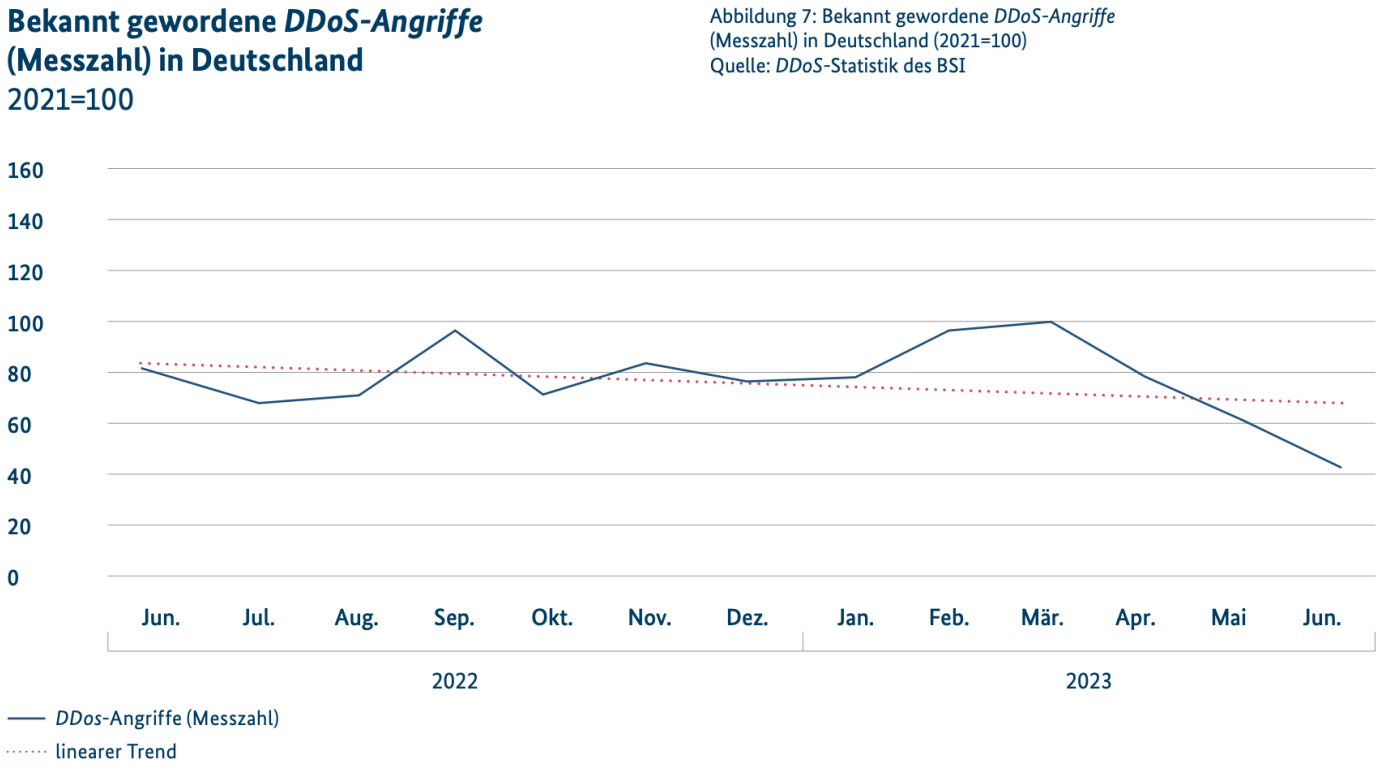


Abbildung 7: Bekannt gewordene *DDoS-Angriffe* (Messzahl) in Deutschland (2021=100)
Quelle: *DDoS*-Statistik des BSI

BSI Lagebericht 2023
Bedrohungslage

Leibniz Universität Hannover

Angriffsarten

APT und Bedrohungen im Kontext des Krieges in der Ukraine

APT-Gruppe	Bevorzugte Ziele	Bevorzugte Techniken
APT15 | VixenPanda | Mirage | Ke3chang	Regierungseinrichtungen | NGOs	*Exploits* gegen aus dem Internet erreichbare Systeme
APT27 | Emissary Panda | LuckyMouse	Energie | Telekommunikation | Pharma	*Exploits* gegen aus dem Internet erreichbare Systeme
APT28 | FancyBear | Sofacy	Regierungseinrichtungen | Militär | Medien | NGOs	*Exploits* gegen aus dem Internet erreichbare Systeme
APT29 | Nobelium | DiplomaticOrbiter	Regierungseinrichtungen	Mails mit Archivdaten als Anhang, die LNK-Dateien enthalten
APT31 | JudgementPanda | ZIRCONIUM	Regierungseinrichtungen | NGOs	*Exploits* gegen aus dem Internet erreichbare Systeme; Bruteforcing
Ghostwriter bzw. Untergruppe UNC1151	Politik | NGOs | Medien	Mails mit Links auf *Phishing*-Seite
Kimsuky | VelvetChollima	Rüstung | Kanzleien	Word-Dokumente, die makrobehaftete Remote Templates nachladen; *Social Engineering*
Lazarus | SilentChollima	Rüstung | Luftfahrt	Mails mit Archivdaten als Anhang, die trojanisierte Anwendungen enthalten; *Social Engineering*
MustangPanda (oder VertigoPanda)	Regierungseinrichtungen	Mails mit Archivdaten als Anhang, die LNK-Dateien enthalten
Snake | VenomousBear | Turla	Regierungseinrichtungen | Export	*Exploits* gegen aus dem Internet erreichbare Systeme
UNC2589	Logistik	Mails mit makrobehafteten Dokumenten im Anhang

Tabelle 1: Für Deutschland relevante APT-Gruppen
Quelle: BSI

ADVERSARY	NATION-STATE OR CATEGORY
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
HAWK	SYRIA
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SPIDER	ECRIME
TIGER	INDIA
WOLF	TURKEY

BSI Lagebericht 2023
Bedrohungslage

Angriffsarten

APT und Bedrohungen im Kontext des Krieges in der Ukraine

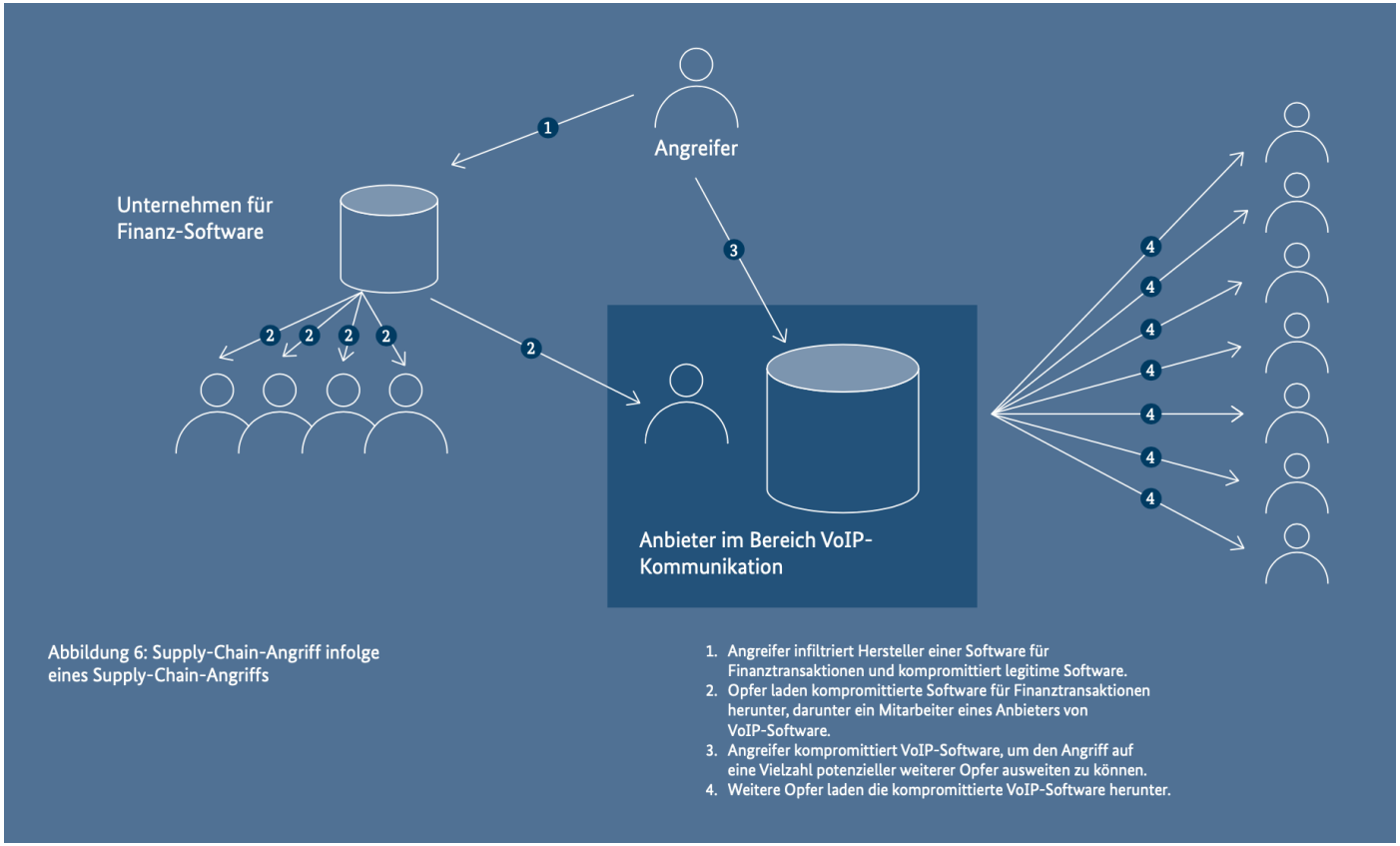


Abbildung 6: Supply-Chain-Angriff infolge eines Supply-Chain-Angriffs

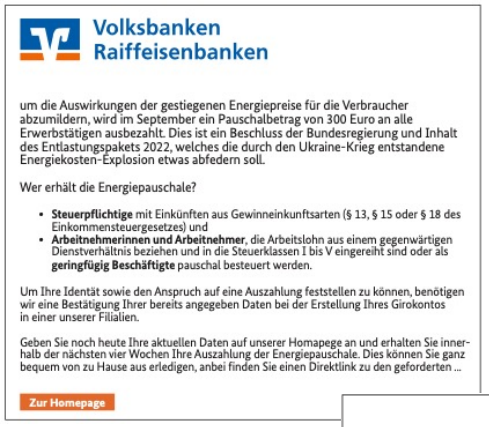
1. Angreifer infiltriert Hersteller einer Software für Finanztransaktionen und kompromittiert legitime Software.
2. Opfer laden kompromittierte Software für Finanztransaktionen herunter, darunter ein Mitarbeiter eines Anbieters von VoIP-Software.
3. Angreifer kompromittiert VoIP-Software, um den Angriff auf eine Vielzahl potenzieller weiterer Opfer ausweiten zu können.
4. Weitere Opfer laden die kompromittierte VoIP-Software herunter.

Quelle BSI

BSI Lagebericht 2023
Bedrohungslage

Angriffsarten

SPAM und Phishing



Volksbanken Raiffeisenbanken

um die Auswirkungen der gestiegenen Energiepreise für die Verbraucher abzumildern, wird im September ein Pauschalbetrag von 300 Euro an alle Erwerbstätigen ausbezahlt. Dies ist ein Beschluss der Bundesregierung und Inhalt des Entlastungspakets 2022, welches die durch den Ukraine-Krieg entstandene Energiekosten-Explosion etwas abfedern soll.

Wer erhält die Energiepauschale?

- **Steuerpflichtige** mit Einkünften aus Gewinneinkunftsarten (§ 13, § 15 oder § 18 des Einkommensteuergesetzes) und
- **Arbeitnehmerinnen und Arbeitnehmer**, die Arbeitslohn aus einem gegenwärtigen Dienstverhältnis beziehen und in die Steuerklassen I bis V eingereiht sind oder als **geringfügig Beschäftigte** pauschal besteuert werden.

Um Ihre Identät sowie den Anspruch auf eine Auszahlung feststellen zu können, benötigen wir eine Bestätigung Ihrer bereits angegeben Daten bei der Erstellung Ihres Girokontos in einer unserer Filialien.

Geben Sie noch heute Ihre aktuellen Daten auf unserer Homapege an und erhalten Sie innerhalb der nächsten vier Wochen Ihre Auszahlung der Energiepauschale. Dies können Sie ganz bequem von zu Hause aus erledigen, anbei finden Sie einen Direktlink zu den geforderten ...

Zur Homepage

DHL

Lieber Kunde,

Zur Erinnerung: DHL Express informiert Sie, dass für Ihre Sendung Nr. [redacted] noch Anweisungen von Ihnen ausstehen.

Bestätigen Sie die Zahlung der Heimlieferkosten (1,85 EURO) und den Versand des Pakets, indem Sie auf die folgende Schaltfläche klicken:

Ankunft in der DHL Express Ursprungsanlage: **6.12.2022**

Mein Paket senden

Mit besten Grüßen

Spam im Berichtszeitraum nach Art des _Spam_
Anteile in %

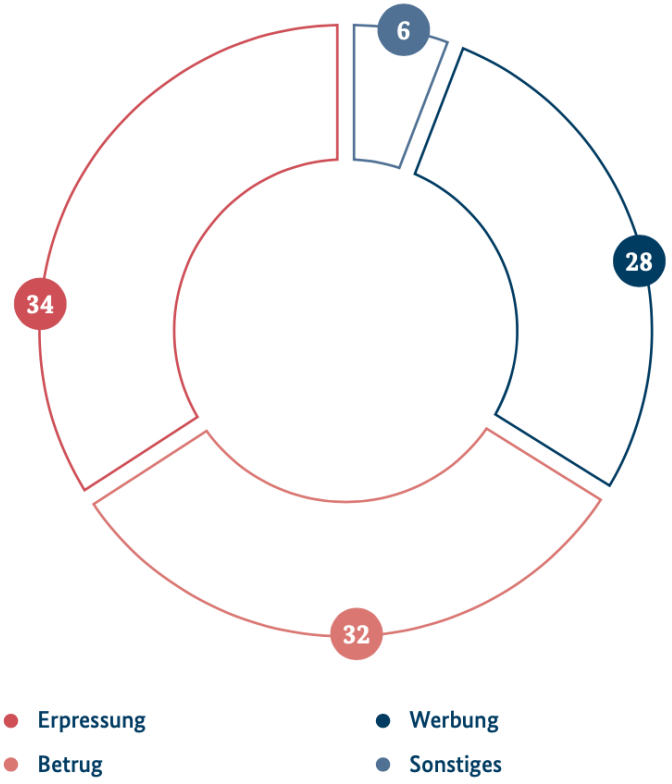


Abbildung 8: _Spam_ im Berichtszeitraum nach Art des _Spam_
Quelle: E-Mail-Verkehrsstatistik des BSI

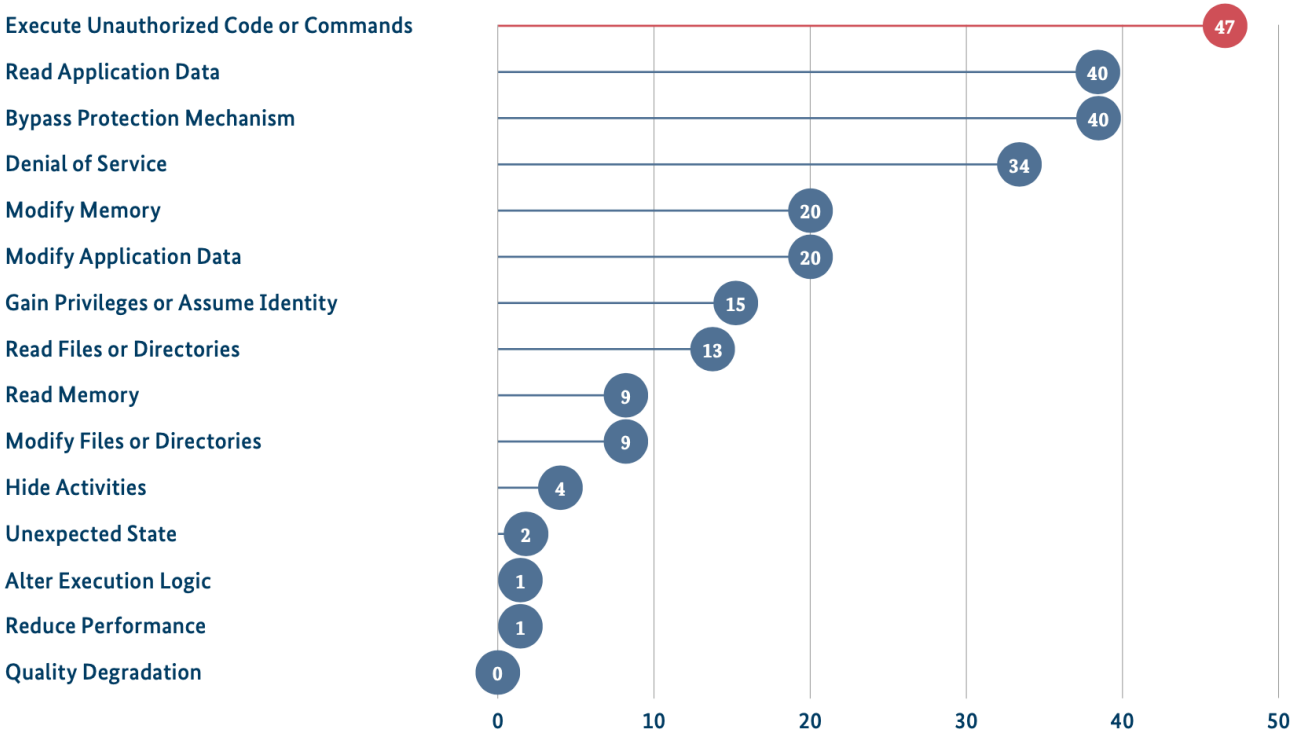
BSI Lagebericht 2023
Bedrohungslage

Schwachstellen (Software)

Bekannt gewordene Schwachstellen nach möglicher Schadwirkung (Top 10)*
Anteile in %

Abbildung 9: Bekannt gewordene Schwachstellen nach Schadwirkung
Quelle: Schwachstellenstatistik des BSI

* Mehrfachnennungen möglich



BSI Lagebericht 2023
Bedrohungslage

Schwachstellen (Hardware)

2017 Meltdown und Spectre

2022 Retbleed, Spectre-BHB, SQUIP, PACMAN, ...

BSI Lagebericht 2023
Bedrohungslage

KI-Sprachmodelle

Selbstreferenzialität

Automatisiertes Social Engineering

Schwachstellen lernen und finden

Fehlerhafte Code-Erzeugung

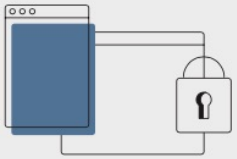
Sammlung von Unternehmensdaten in einer einzigen, schwer zu sichernden Anwendung

BSI Lagebericht 2023
Bedrohungslage

Ransomware

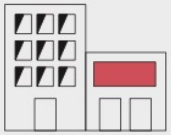
ist weiterhin die größte Bedrohung.

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**.



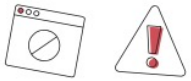
Top-3-Bedrohungen je Zielgruppe:

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.

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

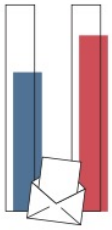
Eine Viertelmillion neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



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.

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.

6.220 2022
5.100 2021

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

Deutschland **Digital·Sicher·BSI·**

LUH Kennzahlen zur ITS-Lage 2023
DFN-CERT Warnmeldungen

- 113 Bot (Gootkit, AdLoad)
- 10 Bot/HTTP (Avalanche/Andromeda)
- 3 Configuration/Unrestricted Access (Mgmt.-Ports)
- 1 Attack/Phishing

→ Zeitraum: 04.2023 – 11.2023

- Gootkit https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Gootkit/gootkit_node.html
- AdLoad https://www.it-daily.net/it-sicherheit/cybercrime/macos-malware-adload-umgeht-systemeigene-sicherheitsvorkehrungen
- Avalanche/Andromeda https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Botnetz-Avalanche/Schadsoftware/Andromeda/Andromeda_Gamarue.html

LUH Kennzahlen zur ITS-Lage 2023
DFN-CERT Warnmeldungen

Liebe Kolleginnen und Kollegen,

dies ist eine automatische Warnmeldung des DFN-CERT. In den letzten Tagen erhielten wir Informationen über mögliche Sicherheitsprobleme auf Systemen in ihrem Netzwerk.

Die von dieser Meldung betroffenen Netzblöcke und Kontakte finden Sie am Ende dieser E-Mail.

Ereignisse:

IP-Adresse	Ereignistyp	Anzahl	Zuletzt gesehen
130.75.abc.xyz	Bot	5	2023-09-11 14:37:22+00:00
130.75.def.uvw	Bot	3	2023-09-11 19:34:29+00:00

Diese Meldung finden Sie auch im Portal unter

IP-Adresse: 130.75.abc.xyz
Ereignistyp: Bot
Zeitstempel: 2023-09-11 14:37:22+00:00
Anzahl: 5
Beschreibung: Auf dem System scheint eine Bot-Software betrieben zu werden, die versucht, einen Command-and-Control (C2)-Server zu erreichen. Zu den unterschiedlichen Malwaretypen finden Sie im folgenden Dokument mehr Informationen (aktuell nur als PDF verfügbar):
https://www2.dfn.de/fileadmin/CERT/DFN.Security/Meldungstypen.pdf

Zuletzt gesehen	IP-Protokoll	Quellport	Ziel-IP	Zielport	Malware
2023-09-11 11:37:16+00:00 occurences: 1	tcp	49457	5.79.71.225	443	AdLoad
2023-09-11 11:37:16+00:00 occurences: 1		49457	5.79.71.225	443	AdLoad
2023-09-11 12:37:18+00:00 occurences: 1		51354	178.162.217.107	443	AdLoad
2023-09-11 13:37:20+00:00 occurences: 1		53398	85.17.31.122	443	AdLoad
2023-09-11 14:37:22+00:00 occurences: 1		55357	178.162.203.202	443	AdLoad

Meldungstypen

Attack (Angriff von einem System auf DFN-Honeypot) Login, Malware, Adware, Credentials, Virus, ...

Bot (Zugriff auf bekannte CC-Server)

Command and Control Server (System ist Teil einer Steuerungsinfrastruktur)

Configuration (unerwünschte Konfiguration) Open proxy, Open resolver, Amplifier, Unrest. access, Unenc. Comm

Hosting (System stellt unautorisierte Inhalte bereit) Malware, Phishing

Scan (System hat Netzwerkscan durchgeführt) Portscan

SPAM (System hat SPAM versendet)

Vulnerability (System ist nicht ausreichend gegen aktiv genutzte Schwachstellen gesichert)
CVE-xxx, Exchange-Server, FortiGate VPN, Pulse Connect VPN

LUH Kennzahlen zur ITS-Lage 2023
Phishing

- CEO-Frauds
- Geleakte Kommunikationsverläufe + Link
- Geleakte Kommunikationsverläufe + PDF-Anhang mit Link

→ Endpunktschutz bleibt wichtig

Virenschutz etc.

Least Privilege Principle

LUH Kennzahlen zur ITS-Lage 2023 ...kurz vermerkt

- Sicherheitsvorfall Hochschule Hannover
  https://www.hs-hannover.de/ueber-uns/organisation/kom/informationen-fuer-hochschulangehoerige-zum-cyberangriff

- Hinweise zu veralteter Software auf Serversystemen

  Software aktuell halten

  Prüfen ob Dienste einschränkbar sind (z.B. Uni-Intern)

- Gehackte Mailboxen (Maßnahmen beachten inkl. Meldung an den DSB, siehe https://www.luis.uni-hannover.de/de/services/it-sicherheit/ernstfall)

- Schwachstellen

  Zero-Day in MS Office (+zwischenzeitlicher Workaround)

  Ghostscript

LUH Kennzahlen zur ITS-Lage 2023 ...kurz vermerkt

- 6. IT-Security Awareness Days
  https://www.luis.uni-hannover.de/de/news/detailansicht/news/it-sad2023