Freistaat SACHSEN

# Live Hacking

mit

Colin Brown

René Johansen

ML GRUPPE

Sie bestimmen die Strategie, wir setzen sie um.

info@mlgruppe.de
+49 2234 / 92 03 – 0
Horbeller Str. 15
50858 Köln

ML GRUPPE
Das Bildungsunternehmen

# Let's get started

# Colin Brown

Certified Ethical Hacker
IT-Consultant
Inhaber IT mit Sicherheit

Freistaat
SACHSEN

# Let's get started

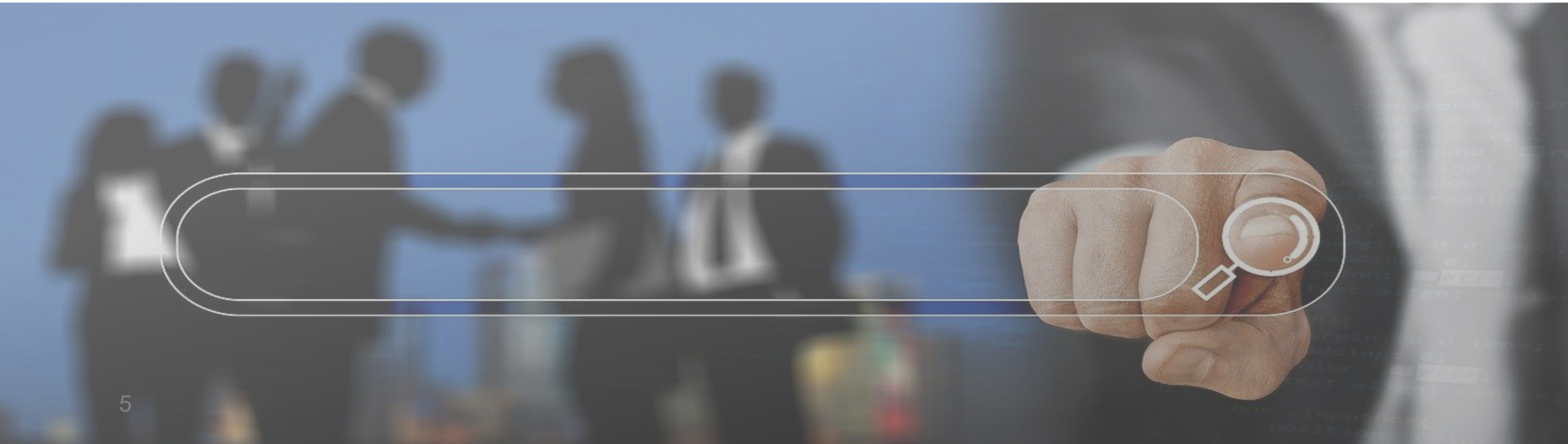
# René Johansen

Informationssicherheits-Consultant
Zertifizierter IT-Grundschutz-Praktiker
Inhaber tech2mind

# Organisation

Dauer ca. 180 Minuten, inkl. 20 Minuten Pause

Fragen können jederzeit gestellt werden



Freistaat SACHSEN

# KEINE Hackerausbildung!

## Strafgesetzbuch (StGB)
## § 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) § 149 Abs. 2 und 3 gilt entsprechend.

Es gibt zwei Arten von Unternehmen: solche, die schon **gehackt wurden**, und solche, **die es noch werden.**

Robert S. Mueller III, ehemaliger Direktor des FBI, 2012

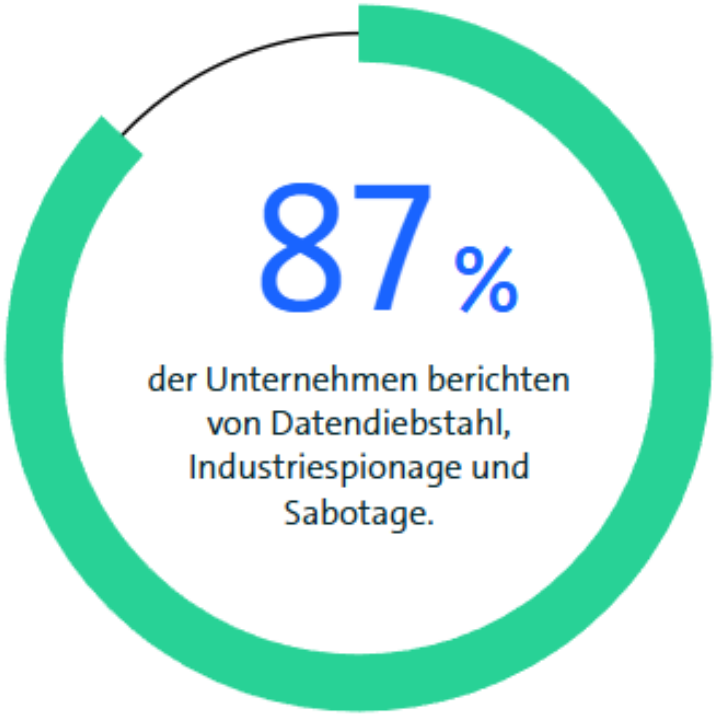
Freistaat SACHSEN

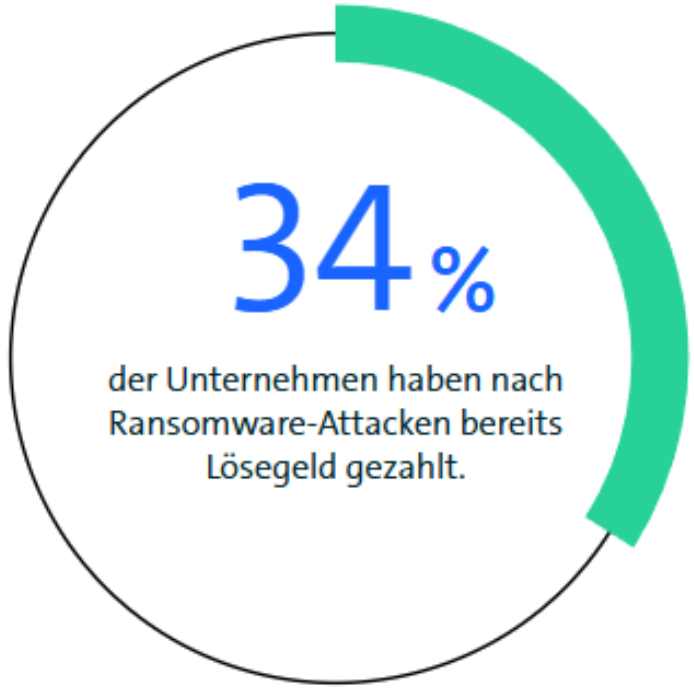
# Im Visier von Angreifern

Sicherheit

## Wie groß ist die Cybergefahr für Unternehmen?

Angriffe auf die deutsche Wirtschaft haben in den vergangenen zwölf Monaten weiter zugenommen – und immer öfter führt die Spur nach Russland und China. Der Schaden steigt auf 289 Milliarden Euro.



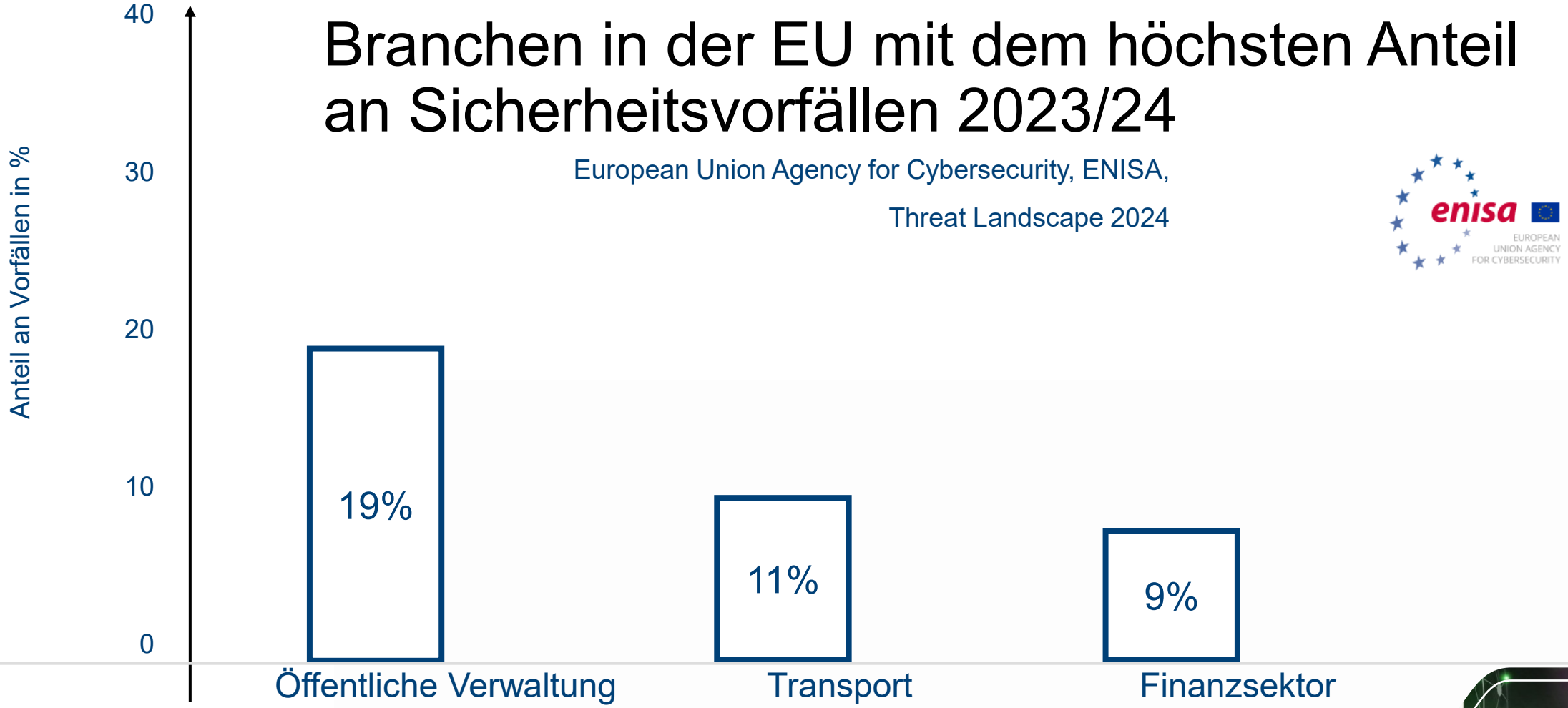




bitkom dataverse

# Branchen in der EU mit dem höchsten Anteil an Sicherheitsvorfällen 2023/24

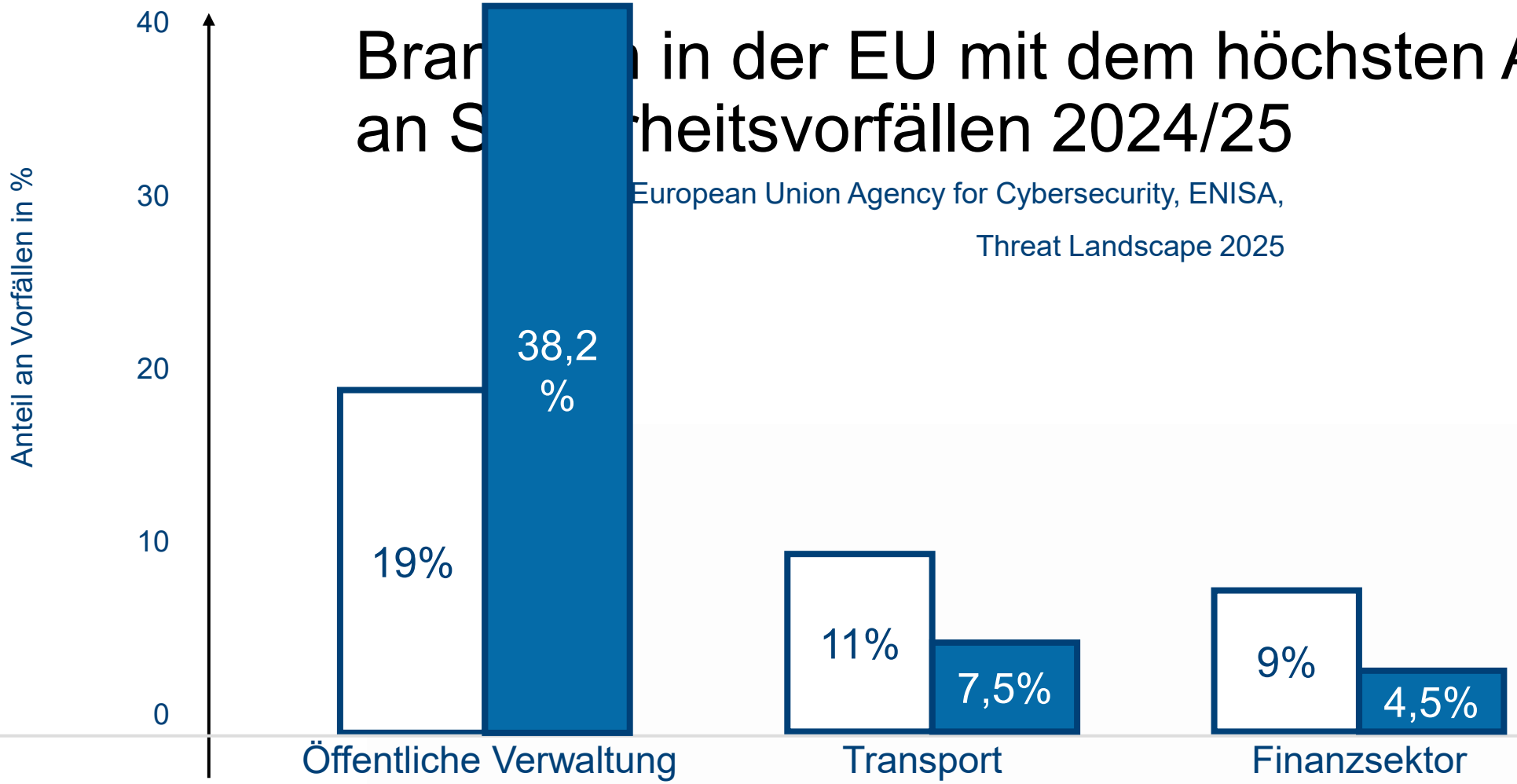
European Union Agency for Cybersecurity, ENISA,

Threat Landscape 2024



# Bran[illegible]n in der EU mit dem höchsten Anteil an S[illegible]rheitsvorfällen 2024/25

European Union Agency for Cybersecurity, ENISA, Threat Landscape 2025



# Im Visier von Angreifern

NETZPOLITIK.ORG

Attacke auf Politik und Journalismus

## Signal-Phishing gegen Julia Klöckner erfolgreich

Markus Reuter

23. April 2026, 14:49 Uhr

*Quelle: Netzpolitik.org, 2026*

# Agenda

- Opportunistische Angriffe
- Die Anatomie eines Cyberangriffs
- Open Source Intelligence
- Angriffe durch E-Mail-Anhänge
- Pause

Freistaat SACHSEN

# Agenda

- Die aktuelle Gefährdungslage
- Künstliche Intelligenz
- Password Cracking
- Ransomeware-Angriffe
- Informationsbeschaffung über mobile Geräte

Freistaat SACHSEN

# Agenda

Smarte Smartphone-Nutzung

Sicherheitstipps für Zuhause

Fragen und Antworten

Freistaat SACHSEN

# Opportunistische Angriffe

- DEMO
  Informationsbeschaffung
- Beispiel
  Ausnutzung menschlicher Schwachstellen

# Opportunistische Angriffe

Freistaat SACHSEN

Schwachstellen ausnutzen, sobald sich eine Gelegenheit bietet …

# Bedrohung

## Spontane Aktionen

*Automatisierte Suche nach Schwachstellen*

*Massenausnutzung bekannter Lücken*

*Ungezielte Verbreitung von Schadsoftware*

*Breit gestreute Phishing-Kampagnen*

*Zufällige Kompromittierung von Systemen*

*Monetarisierung in Massen*

*Wenig Aufwand für Tarnung*

Opportunistisch

**Ressourcen-nutzung & schnelle Bereicherung**

Freistaat SACHSEN

# Die Anatomie eines Cyberangriffs

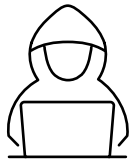
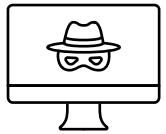
- Geplante, gezielte Angriffe
- Beispiel
  Ransomware-as-a-Service
- Ursachen für Sicherheitsvorfälle
- Die Angriffskette eines APT-Angriffs

# Gezielte Angriffe

Strukturiert geplant und auf ein bestimmtes Ziel ausgerichtet…

# Organisationen hinter gezielter Cyberkriminalität

Freistaat SACHSEN

| Staatliche Akteure | Hacktivisten | Cyberkriminelle |
| --- | --- | --- |
|  |  |  |
| Informationsbeschaffung | Manipulation der Politik | Gezielte Monetarisierung |
| Störung, Sabotage, Krieg | Aufmerksamkeit | Fokus Kosten/Nutzen |
| Beispiel: APT-Gruppen | Einfluss auf die Gesellschaft | Erpressung/Ransom |

# Bedrohung

## Zielgerichtete Aktionen

***Diebstahl sensibler oder strategischer Informationen***

***Sabotage***

***Ransomware-Angriffe***

***Bewusste Desinformation***

***Gezielte staatliche Kontrolle/Überwachung***

**Manipulation**
**Persistenz**
**Lateral Movement**
**Langfristig**

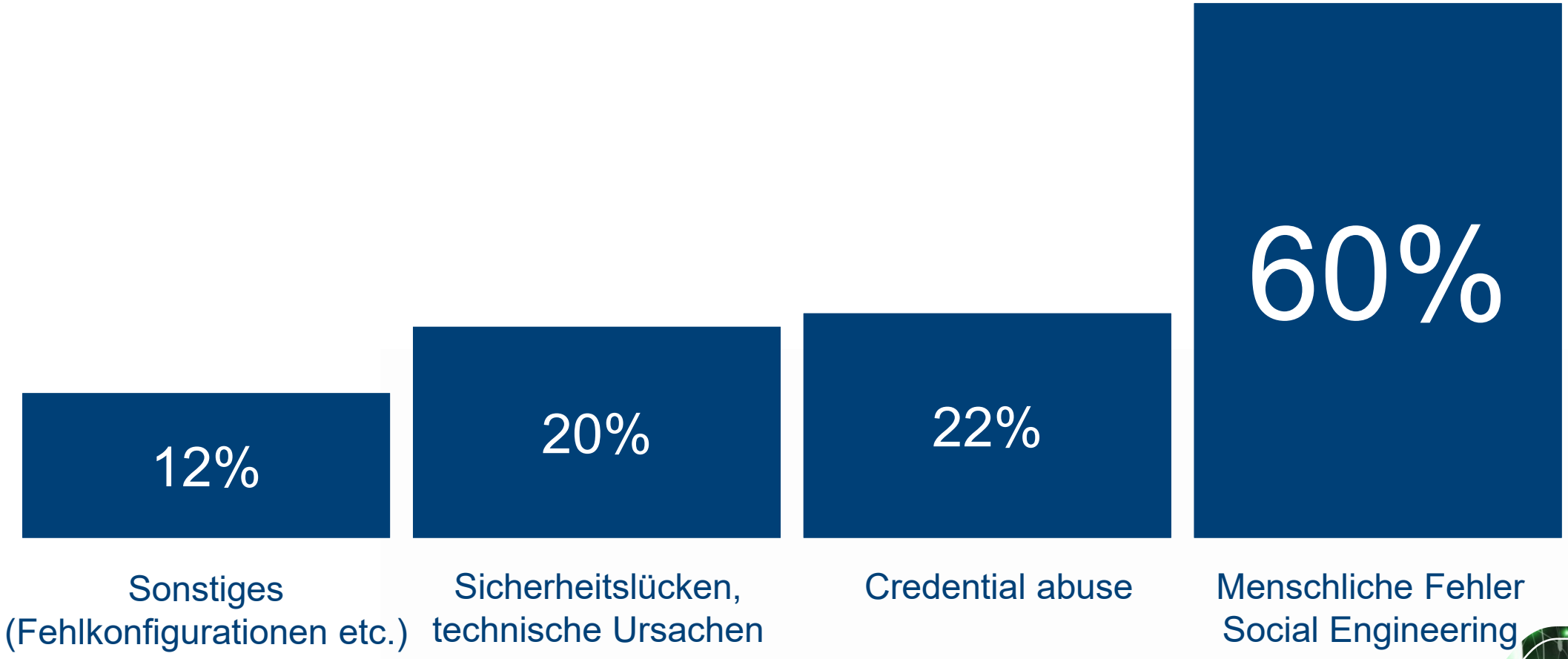
Gezielt

# Ursachen für Sicherheitsvorfälle 2023/24

Freistaat SACHSEN

Verizon Data Breach Investigation Report 2025

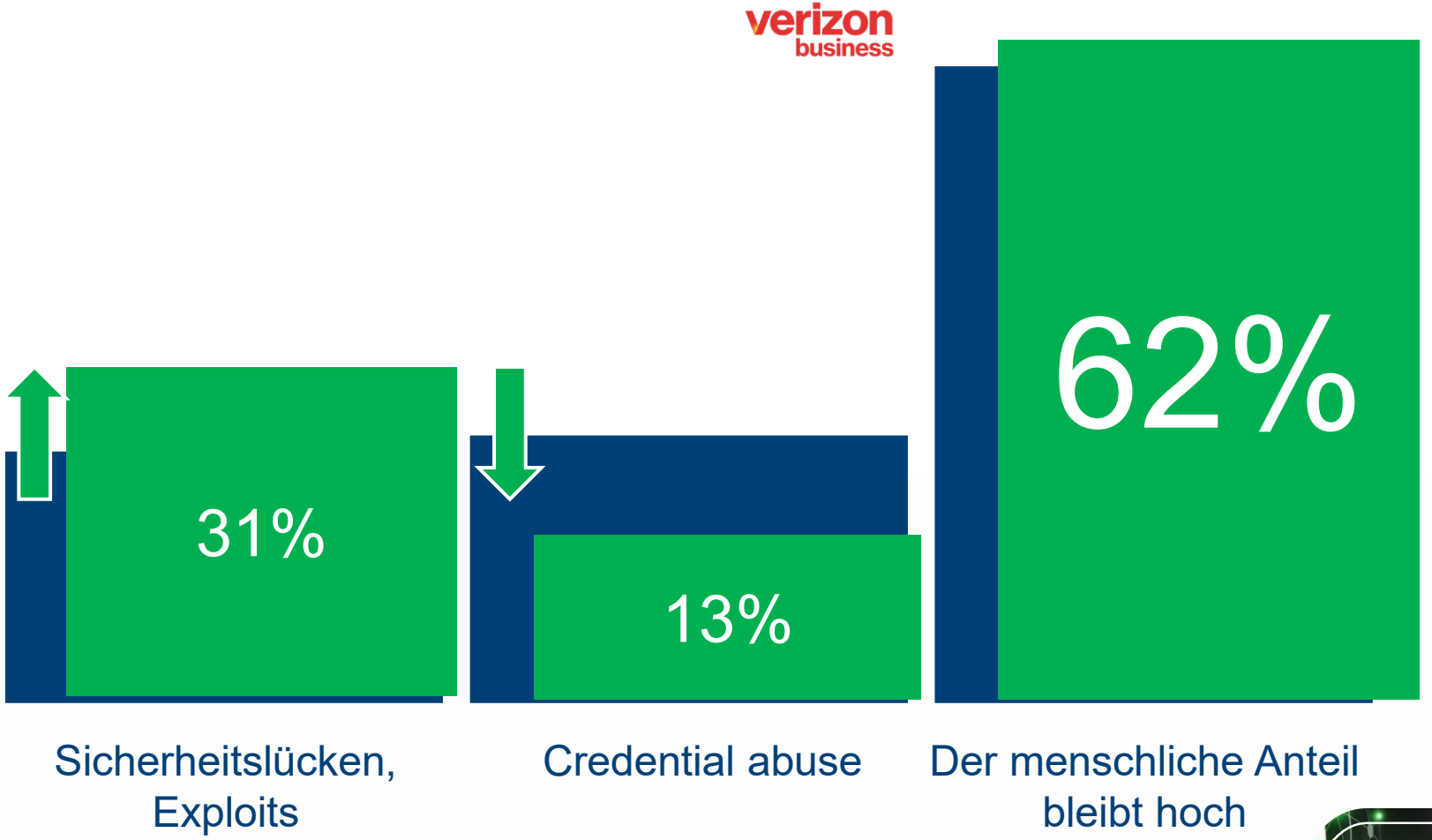
verizon business



# 2026: Mehr technische Erstkompromittierung

Verizon Data Breach Investigation Report 2026

Der menschliche Anteil bleibt bei 62%, aber Schwachstellen-Exploitation überholt Credential abuse als häufigster Initial Access Vector.



# Die Angriffskette eines APT-Angriffs

Freistaat SACHSEN

**A**DVANCED
**P**ERSISTENT
**T**HREAT

1. Aufklärung — Ich schau mich mal um
2. Bewaffnung — Ich bau meinen Köder
3. Lieferung — Post ist da!
4. Ausnutzung — Danke für‘s Draufklicken!
5. Installation — Ich bleibe hier!
6. Steuerung — Unter voller Kontrolle
7. Aktionen am **Ziel** — Jetzt geht‘s zur Sache!

Quelle: Cyber Kill Chain nach Lockheed-Martin


Freistaat SACHSEN

# KEVIN VON KLICKBERG

## APT BÜRONAUTICS

**SPEZIALITÄT:**

**VERTEILT PDFS MIT ANIMIERTEN LADEBALKEN, DIE NIE ENDEN – BIS DAS ZIEL FRUSTRIERT AUF „MAKROS AKTIVIEREN“ KLICKT…**

# Was will der Angreifer?

Freistaat SACHSEN

**A**DVANCED
**P**ERSISTENT
**T**HREAT

Institut für Prognostizierte Innovations-hemmung
IPI

## Absolut sicherer Datenschutz-Proxy

Eine revolutionäre Privacy- und Sicherheits-Engine, die den gesamten Internetverkehr einer Person oder Organisation vollständig verschleiert – auch gegenüber künftigen Quantencomputern.

# Der Anwender

## DR. THEO WIRRWITZ

### INSTITUT FÜR PROGNOSTIZIERTE INNOVATIONSHEMMUNG (IPI)


Institut für Prognostizierte Innovations-hemmung
IPI


**„WIR SIND AUF EINEM GUTEN WEG.
WIR WISSEN NUR NOCH NICHT, AUF WELCHEM.“**

**AUFGABENGEBIET:**

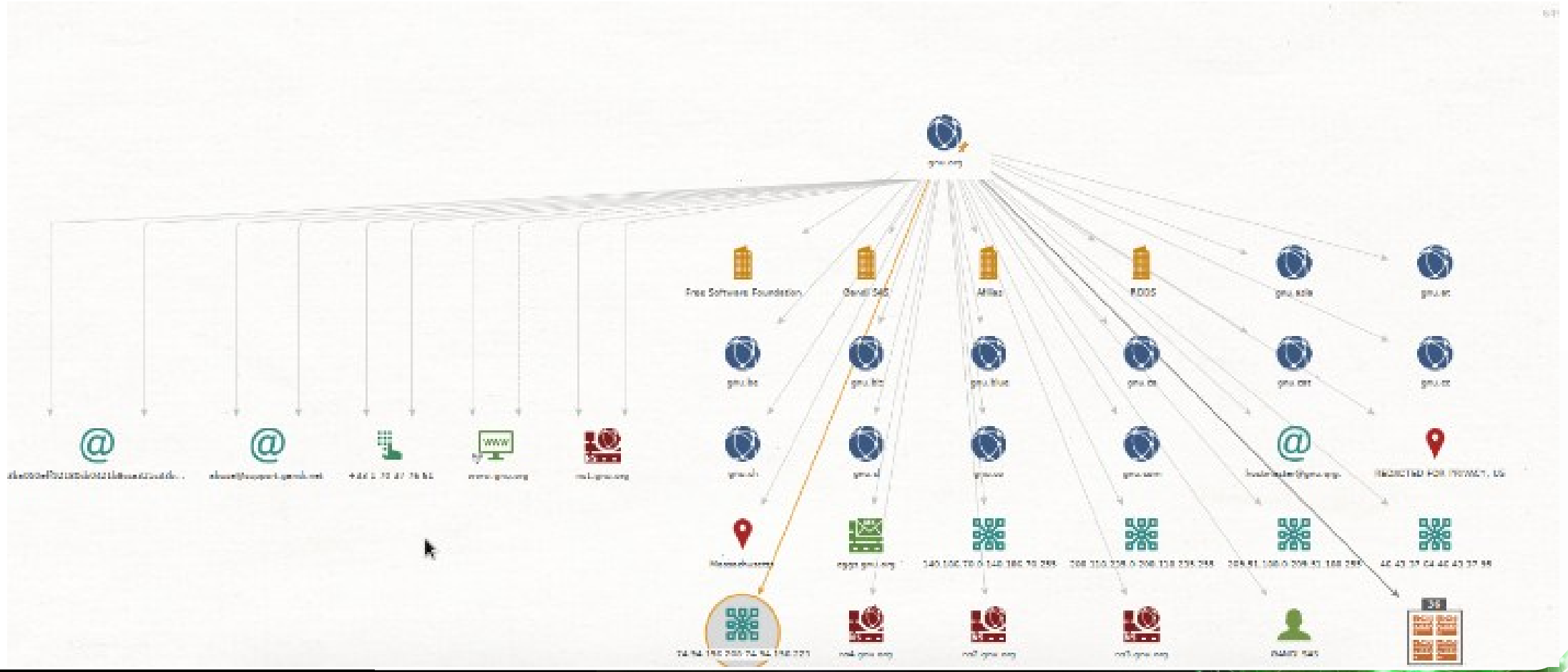
**UNTERSUCHUNG, WIE NEUE WIRKUNGSVOLLE TECHNOLOGIEN MÖGLICHST LANGE IGNORIERT WERDEN KÖNNEN.**

Freistaat SACHSEN

# Open Source Intelligence

- DEMO
  Maltego
- DEMO
  Deepfake

# Open Source Intelligence



# Der Köder

## DIPL.-INF. KLAUS CHAOSINSKI

### ZENTRALE KOORDINATIONSSTELLE FÜR DIGITALE VERWIRRUNG (ZKDV)





**“WIR UNTERSTÜTZEN SIE SELBSTLOS BEI DER EINFÜHRUNG UNNÖTIG KOMPLEXER SOFTWARELÖSUNGEN IN DER VERWALTUNG!“**

Zentrale Koordinationsstelle für Digitale Verwirrung

ZKDV

**AUFGABENGEBIET:**

**KOORDINATOR FÜR DIE VERMISCHUNG INKOMPATIBLER SOFTWAREPAKETE.**

# Angriffe durch E-Mail-Anhänge

- DEMO
  MAKRO
- DEMO
  PDF

# Schutz vor Cyberangriffen: E-Mail-Anhänge

Freistaat SACHSEN

## Absender prüfen

Nur Anhänge von bekannten und vertrauenswürdigen Absendern öffnen – auf Schreibfehler und ungewöhnliche Domains achten.

## Anhänge hinterfragen

Bei nicht angeforderten Dateien: Rückfrage über sicheren Kanal (z. B. Telefon, Teams).

## Keine Makros aktivieren

Office-Dateien, die zur Aktivierung von Makros auffordern, nicht ausführen – hohes Risiko!

> Das schwächste Glied in der Sicherheitskette ist der Mensch.

Kevin Mitnick, Hackerlegende & IT-Experte

# Reiz und Reaktion

**Zwischen**
**Reiz und Reaktion liegt ein Raum.**
**In diesem Raum liegt unsere Macht**
**zur Wahl unserer Reaktion.**

Viktor Frankl, Psychiater, Begründer der Logotherapie


Waage
Have
a
Break

Freistaat SACHSEN

# Die aktuelle Gefährdungslage

- BSI-Lagebericht 2025
- Bundeslagebild Cybercrime BKA 2025
- Lage der IT-Sicherheit in Sachsen

# DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2025

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

*Quelle: Bundesamt für Sicherheit in der Informationstechnik, (BSI), Lagebericht 2025*

# Drei zentrale Erkenntnisse aus dem BSI-Lagebericht 2025

Freistaat SACHSEN

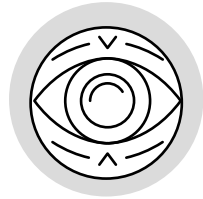
## Zunehmende Angriffsflächen und wachsende Schwachstellen

Cyberkriminalität ist zunehmend arbeitsteilig und hochprofessionell organisiert. 2024/25 wurden täglich zwei bis drei schwere Ransomware-Angriffe polizeilich gemeldet.

## Öffentliche Verwaltung im Fokus

Angriffe durch APT-Gruppen mit hoher Professionalität und durch Hacktivisten nehmen zu.

Der öffentliche Sektor ist attraktiv: große Wirkung, Relevanz, oft komplexe IT-Infrastruktur.



## Weiterhin eine hoch angesetzte Bedrohungslage — Deutschland bleibt verwundbar

Es ist nicht mehr die Frage *ob* ein Angriff erfolgt, sondern *wann* und mit welchen Konsequenzen — Vorbereitung und Widerstandskraft sind entscheidend.

**„Der Schutz der Angriffsflächen ist 2026 der entscheidende Hebel, um die Cybersicherheit zu verbessern.“**

# Bundeslagebild Cybercrime

Deutschland 2025

Bundeskriminalamt

BKA

# Das aktuelle Lagebild Cybercrime I

*Quelle: Bundeskriminalamt (BKA), Bundeslagebild Cybercrime 2025*

Nach einem weiteren Anstieg der Auslandstaten auf 207.888 Fälle übersteigen sie die Straftaten der Inlands-PKS mit 126.034 Fällen deutlich.

**333.922**

Gesamtfallzahl Cybercrime-Delikte

KI wird zunehmend für cyberkriminelle Aktivitäten genutzt.

**1.041**

Ransomware-Angriffe wurden deutschlandweit angezeigt.

**15,5 Mio. $**

Die Ransomware-Zahlungen in Deutschland liegen bei umgerechnet 15.515.377 US-Dollar.

# Das aktuelle Lagebild Cybercrime II

*Quelle: Bundeskriminalamt (BKA), Bundeslagebild Cybercrime 2025*

**36.706**

DDoS-Angriffe im Netz der DTAG gemessen (+25 %).

mehr als **700**

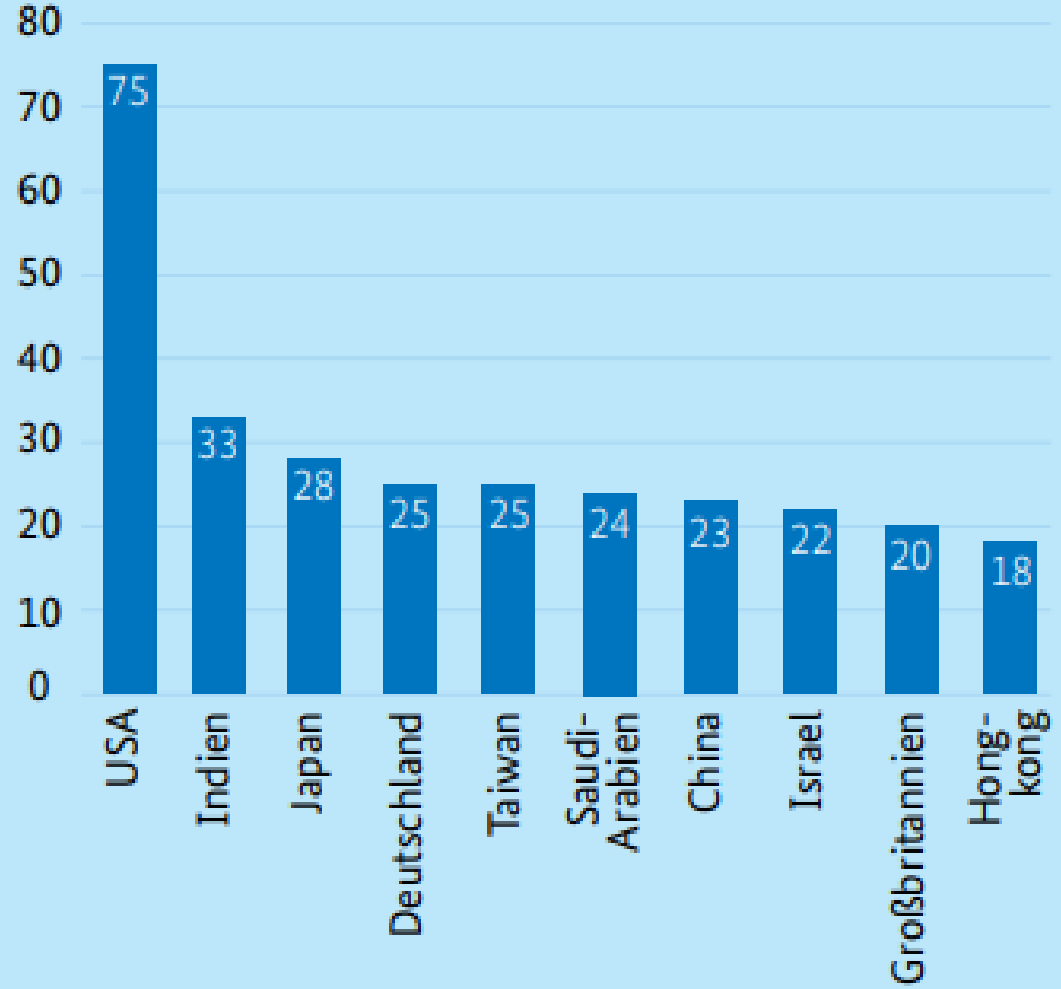
Angriffsankündigungen und -meldungen durch hacktivistische Akteure auf Ziele in Deutschland.

**202.400.000.000 €**

Der durch den Bitkom e.V. festgestellte Schaden durch Cyberattacken beträgt 202,4 Mrd. Euro.

# APT-Gruppen

## APT-Gruppen 2025* weltweit nach Zielland (Top 10, Anteile in %)



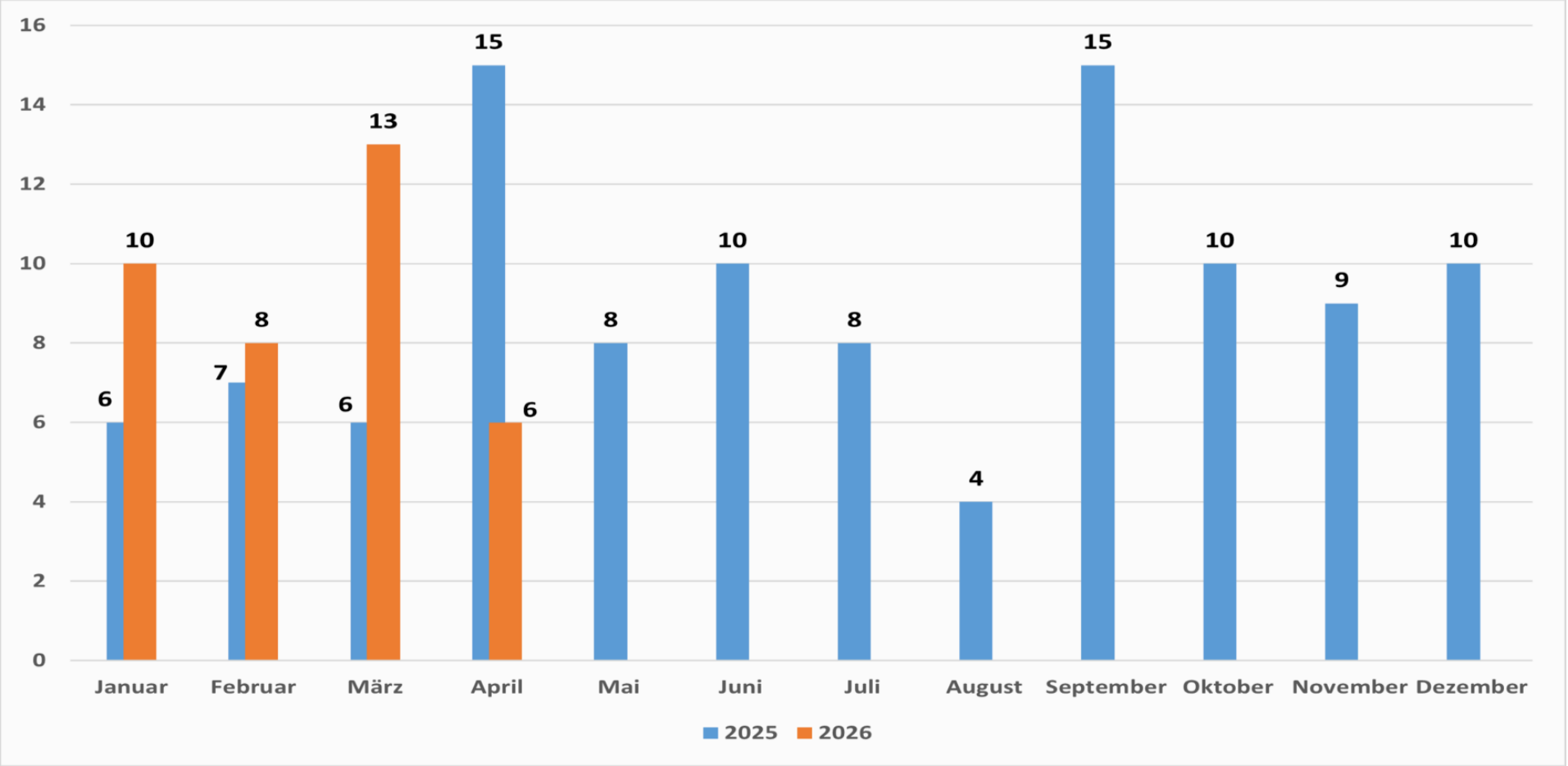

75 % der APT-Gruppen, die sich gegen mindestens eines der Top-10-Zielländer richteten, zielten auf die USA. Deutschland lag mit 25 % dieser APT-Gruppen auf Platz 4.

* Mehrfachnennungen möglich | *Quelle: TAS*

# Zahlen aus Sachsen

Freistaat SACHSEN

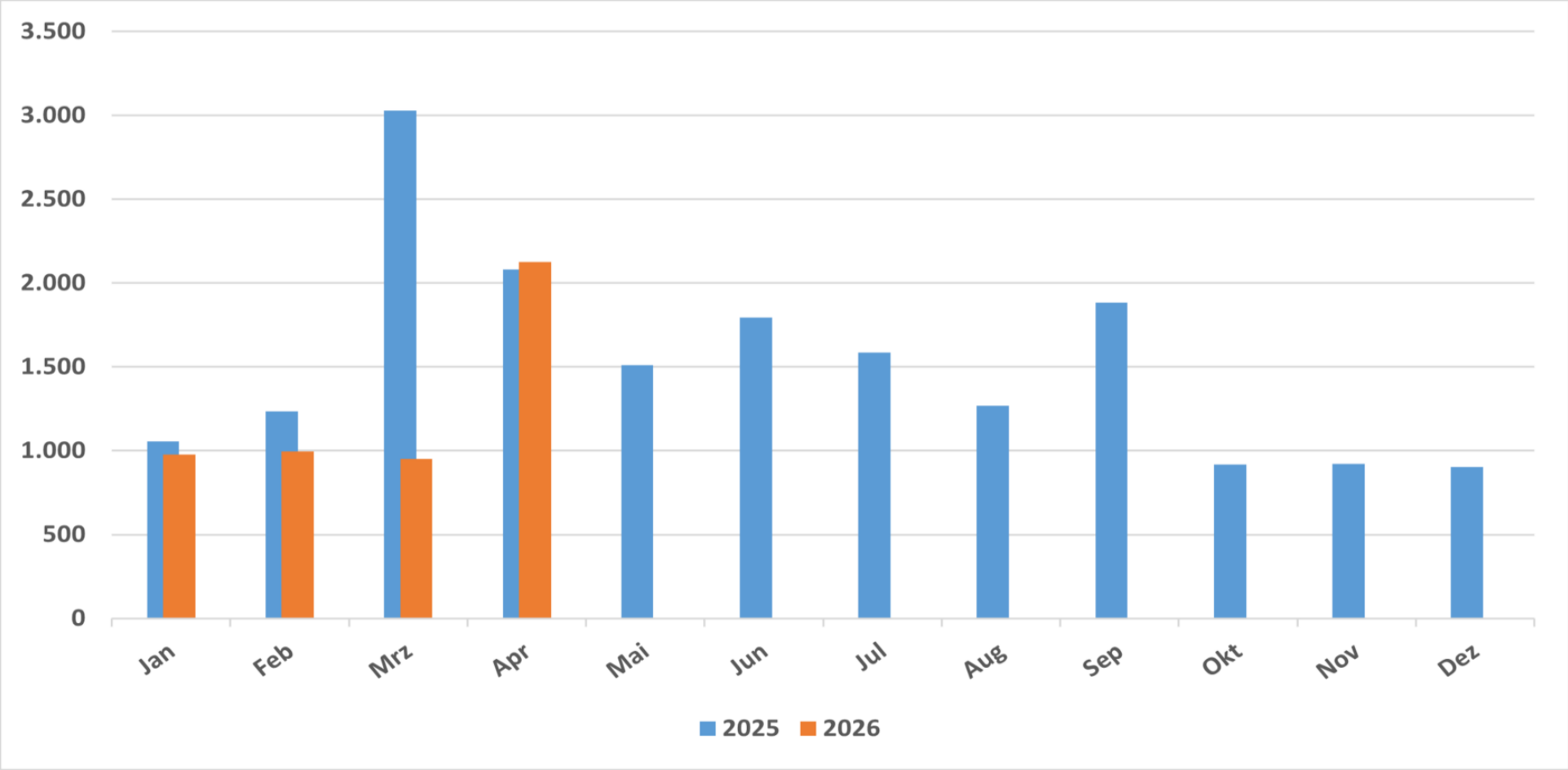
Anzahl der Vorfallmeldungen an das SAX.CERT



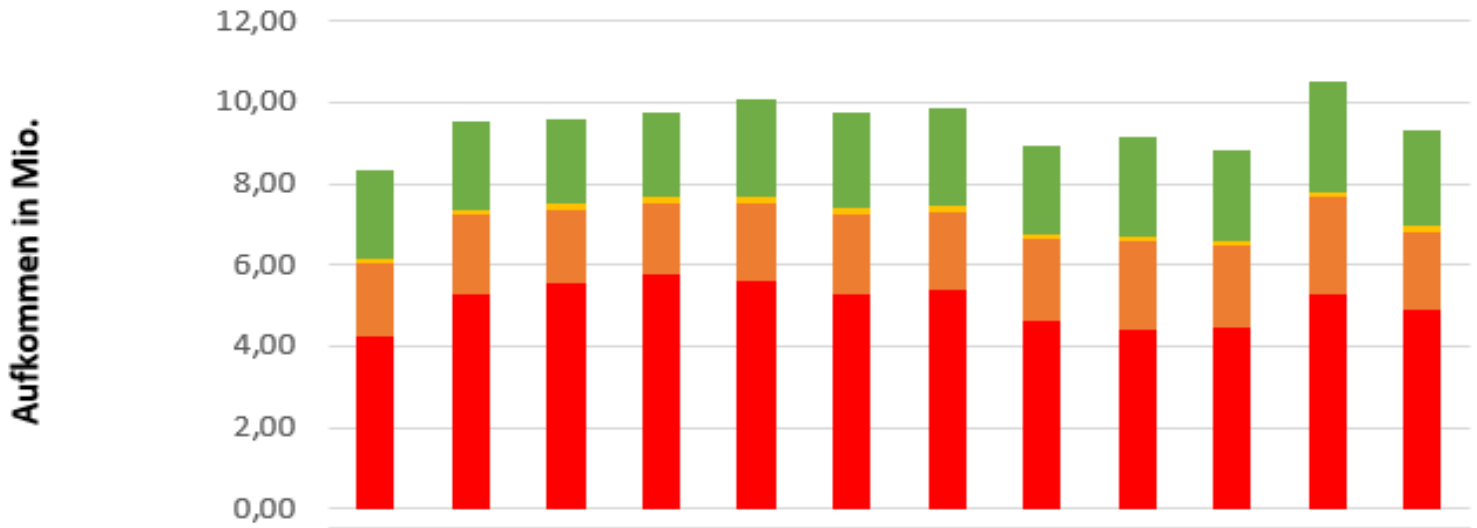
# Zahlen aus Sachsen

Freistaat SACHSEN

Abgefangene Schadsoftware aus E-Mails



# Zahlen aus Sachsen




| | Mai 25 | Jun 25 | Jul 25 | Aug 25 | Sep 25 | Okt 25 | Nov 25 | Dez 25 | Jan 26 | Feb 26 | Mrz 26 | Apr 26 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E-Mail - unmarkiert | 2,16 | 2,17 | 2,05 | 2,08 | 2,38 | 2,35 | 2,44 | 2,21 | 2,43 | 2,21 | 2,70 | 2,37 |
| E-Mail - Linkreputation markiert | 0,13 | 0,15 | 0,18 | 0,16 | 0,16 | 0,14 | 0,13 | 0,09 | 0,11 | 0,11 | 0,13 | 0,13 |
| E-Mail - Spam markiert | 1,82 | 1,93 | 1,81 | 1,78 | 1,95 | 1,97 | 1,93 | 2,03 | 2,17 | 2,04 | 2,40 | 1,95 |
| E-Mail - abgewiesen | 4,22 | 5,29 | 5,55 | 5,74 | 5,58 | 5,28 | 5,38 | 4,62 | 4,43 | 4,44 | 5,28 | 4,88 |

# Phishing -> Beispiel Sharepoint.com und OneNote

Dr. Willmar Schwabesche gemeinnützige Heimstättenbetriebsgesellschaft mbH

JK Jaworski, Katrin <katrin.jaworski@drws-pflege.de>
An Jaworski, Katrin

Antworten | Allen antworten

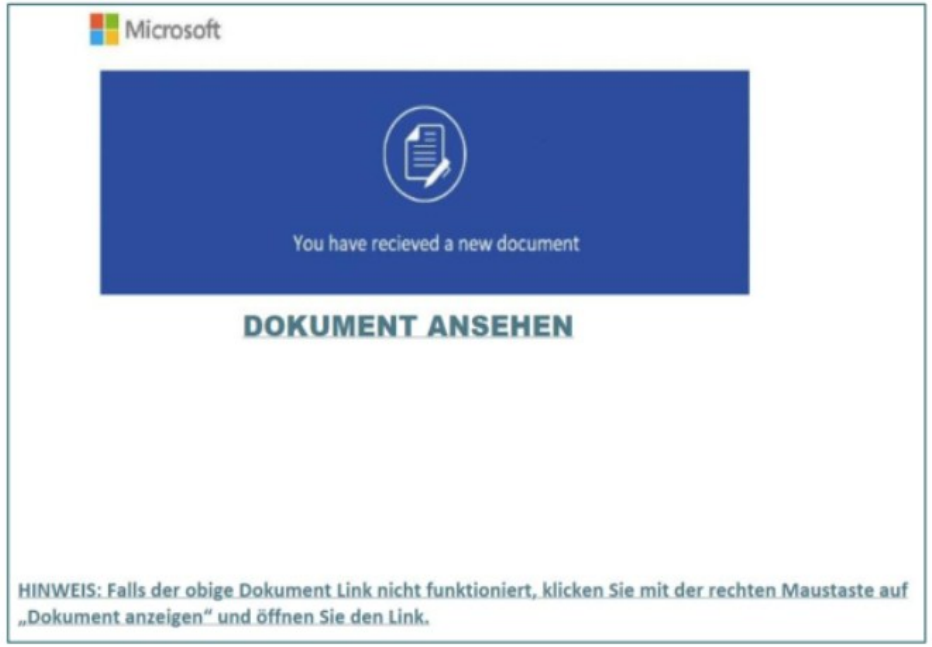
Wir haben zusätzliche Zeilenumbrüche aus dieser Nachricht entfernt.
Diese Nachricht wurde in das Nur-Text-Format konvertiert.

Hallo,

Bitte beachten Sie die untenstehende Datei, die Ihnen von der

Dr. Willmar Schwabesche gemeinnützige Heimstättenbetriebsgesellschaft mbH zugesandt wurde.

Dr. Willmar Schwabesche gemeinnützige Heimstättenbetriebsgesellschaft inv_269094 <https://skvversicherung-my.sharepoint.com/:o:/g/personal/simone_teambergmann_at/IgBqCvBaGcs-Qa8V3Uksth8-AeSkmrKvG3FRHuANdFo31AE?e=SNRju5>




Di 26.05.2026 11:40

?P?rpl?xity ?I <info@email.eroomia.fr>

**Ihre monatliche Perplexity Pro Rechnung vom 26. Mai 2026**

An SK BfIS-Land

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

P

## Perplexity AI

Offizielle Zahlungsaufforderung

Sehr geehrte Kundin, sehr geehrter Kunde,

Ihr **Perplexity Pro** Abonnement wird automatisch für den nächsten Abrechnungszeitraum verlängert. Bitte begleichen Sie die ausstehende monatliche Gebühr, um ununterbrochenen Zugriff auf erweiterte KI-Funktionen, bevorzugte Antwortzeiten und erweiterte Kontextlänge zu gewährleisten.

Perplexity Pro – Monatliche Mitgliedschaft **17,00 USD**
Nächster Abrechnungszeitraum 30. Juni 2026 – 29. Juli 2026

**Gesamtbetrag (inkl. MwSt.) 17,00 USD**

Zahlung durchführen:

Jetzt sicher bezahlen

Nach erfolgreicher Zahlung wird Ihr Konto sofort als „bezahlt" gekennzeichnet. Der Link führt zu einem gesicherten Zahlungsportal von Perplexity AI. Bitte verwenden Sie denselben Link nicht mehrfach, falls die Zahlung bereits erfolgt ist.

Rechnungsnummer: `INV-2026-05-26-9X4L`
Kundennummer: `CUST-8723-PERP`

Freistaat SACHSEN

Aktenzeichen : BKA-CC/2025-06-449821!!

B BPOL <kontakt@bundespolizei-pädophilen2.de>
An kontakt@bundespolizei-pädophilen2.de

Antworten | Allen antworten | Weiterleiten | ...
Di 12.05.2026 10:31

**BUNDESPOLIZEI**
Direktion für justizielle Operationen

**Aktenzeichen : BKA-CC/2026-06-449821**

Sehr geehrte Dame, sehr geehrter Herr,

gemäß **§ 112 StPO** wurde gegen Sie ein Haftbefehl der Staatsanwaltschaft Berlin erlassen.

**Sie sind verpflichtet, innerhalb einer Frist von 72 Stunden nach Erhalt dieser Nachricht auf diese E-Mail zu antworten, um die Angelegenheit mit uns zu erörtern.** Diese ausdrückliche Aufforderung zur schriftlichen Diskussion per E-Mail basiert auf **§ 145a StPO** (Nachfristsetzung bei Ladung).

⚠ Gemäß **§ 230 StPO** gilt: Wenn Sie nicht innerhalb der Frist per E-Mail antworten, kann das Gericht Ihre Vorführung anordnen oder Haftbefehl erlassen – ohne weitere Benachrichtigung.

Für die gesamte schriftliche Kommunikation (insbesondere für Ihre Antwort auf diese Nachricht) nutzen Sie ausschließlich folgende E-Mail-Adresse:

bpoli.justiz.berlin@outlook com

**Anlage :** *Haftbefehl_2026-0429_BPol.pdf*

Wir erwarten Ihre kontaktdiskutierende Antwort per E-Mail innerhalb der genannten 72 Stunden und danken für Ihre umgehende Mitwirkung.

Leiter der Direktion für justizielle Operationen
*Dieses Dokument wurde digital erstellt und ist rechtsverbindlich.*

BUNDESPOLIZEI – DIREKTION FÜR JUSTIZIELLE OPERATIONEN – PLATZ DER REPUBLIK 1, 11014 BERLIN

# Künstliche Intelligenz

- DEMO
  Der gefakte Ausweis

# Password Cracking

- DEMO
  Bopscrk
- DEMO
  Password Crack

# Schutz vor Cyberangriffen: Sicherer Umgang mit Passwörtern

Freistaat SACHSEN

## Komplexität & Länge

Mindestens 12 Zeichen, besser mehr, mit Groß-/Kleinbuchstaben, Zahlen & Sonderzeichen.

## Einzigartigkeit

Jedes Konto – eigenes Passwort. → Verhindert Kettenreaktionen bei Datenlecks.

## Mehrfaktor-authentifizierung

Identitätsbestätigung durch mindestens einen weiteren unabhängigen Faktor.

## Wechselnde Passwörter für unterschiedliche Zwecke

Passwörter nach Wichtigkeit oder Einsatzbereich passend wählen (z. B. privat vs. dienstlich, kritisch vs. unkritisch).

## Passwortmanager nutzen

Ein Passwortmanager speichert komplexe, einzigartige Passwörter sicher an einem Ort und hilft, sie bequem zu verwalten. KeePass ist besonders vertrauenswürdig, da es quelloffen und lokal speicherbar ist.

# Ransomware-Angriffe

- DEMO
  Angriff mit Ransomware
- Links in E-Mails

# Schutz vor Cyberangriffen: Links in E-Mails

Freistaat SACHSEN

## Absender verifizieren

Nur Links von bekannten und vertrauenswürdigen Absendern öffnen – auf Schreibfehler und ungewöhnliche Domains achten.

## Ziel-Links prüfen

Mit der Maus über Links fahren (nicht klicken!) zeigt unten oder in einem Tooltip den echten Link.

## Links lesen lernen

Gewusst wie?
Testen Sie sich!

> Wer glaubt, Technologie könne alle Sicherheitsprobleme lösen, versteht weder die Probleme noch die Technologie.

Bruce Schneier, Experte für IT-Sicherheit und Kryptografie

Freistaat SACHSEN

1

https://www.echter-ort.de/

3 2

1. Such den ersten Schrägstrich
2. Ändere die Lesrichtung
3. Such die beiden nächsten Punkte
4. Dazwischen liegt er, der "echte-Ort"

ML CYBERSEC

# Informationsbeschaffung über mobile Geräte

- DEMO
  Informationsbeschaffung durch verseuchte Apps
- DEMO
  Informationsbeschaffung durch WhatsApp-Monitoring

# Informationsbeschaffung über mobile Geräte

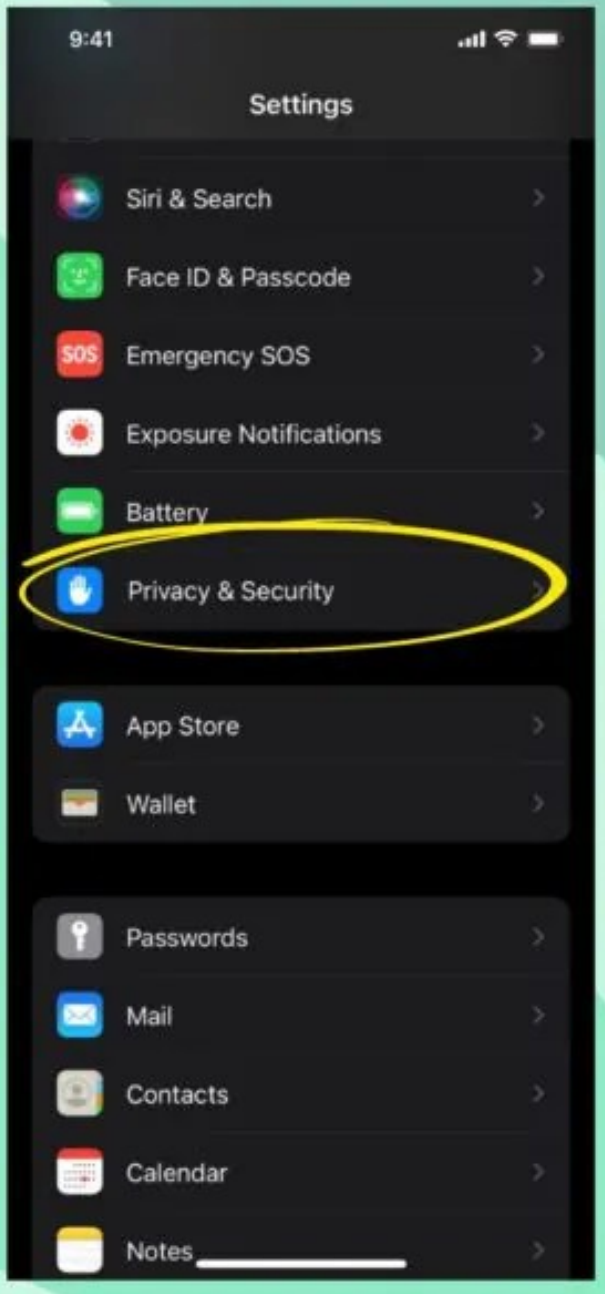
- DEMO
  Informationsbeschaffung durch
  Auswertung von Bewegungsprofilen

# Das Risiko in meiner Hosentasche

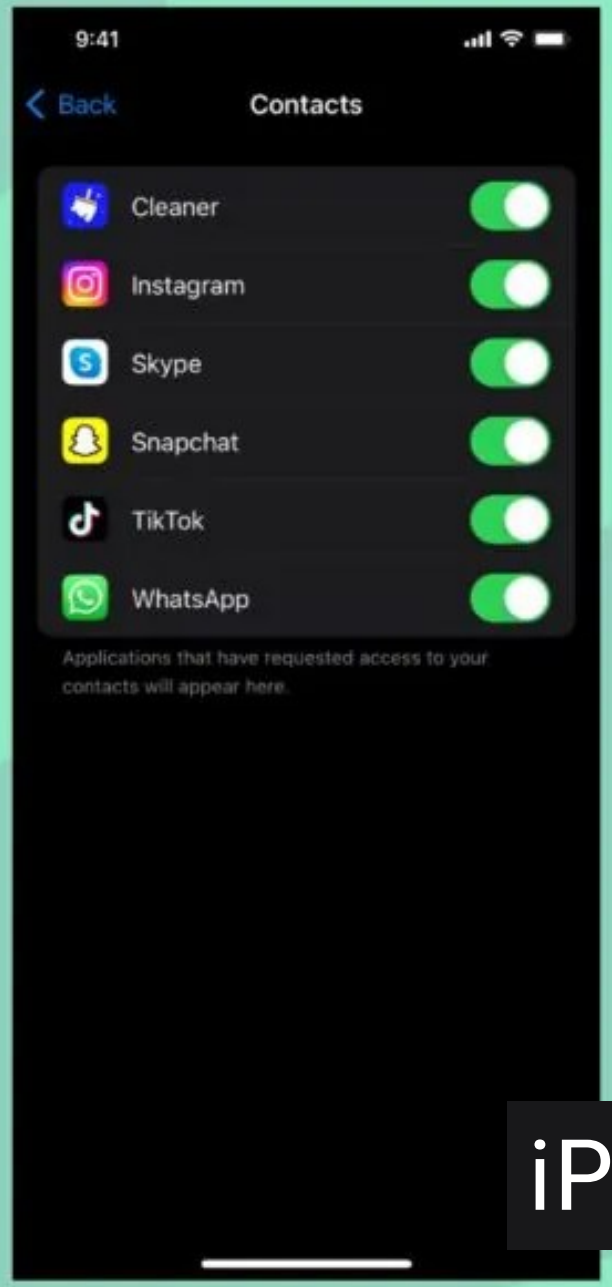
Freistaat SACHSEN

# Smarte Smartphone-Nutzung

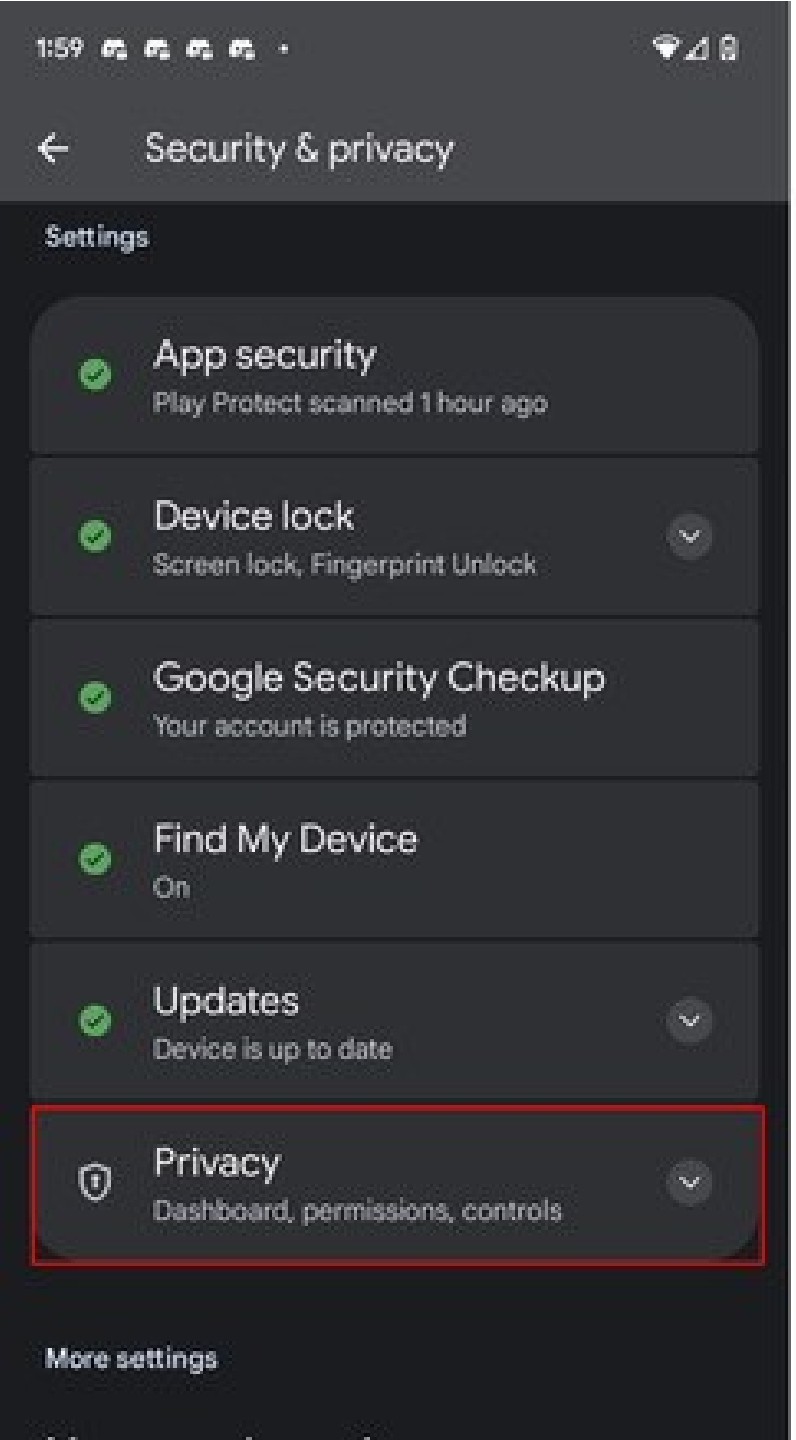
- Umgang mit Apps und App-Berechtigungen

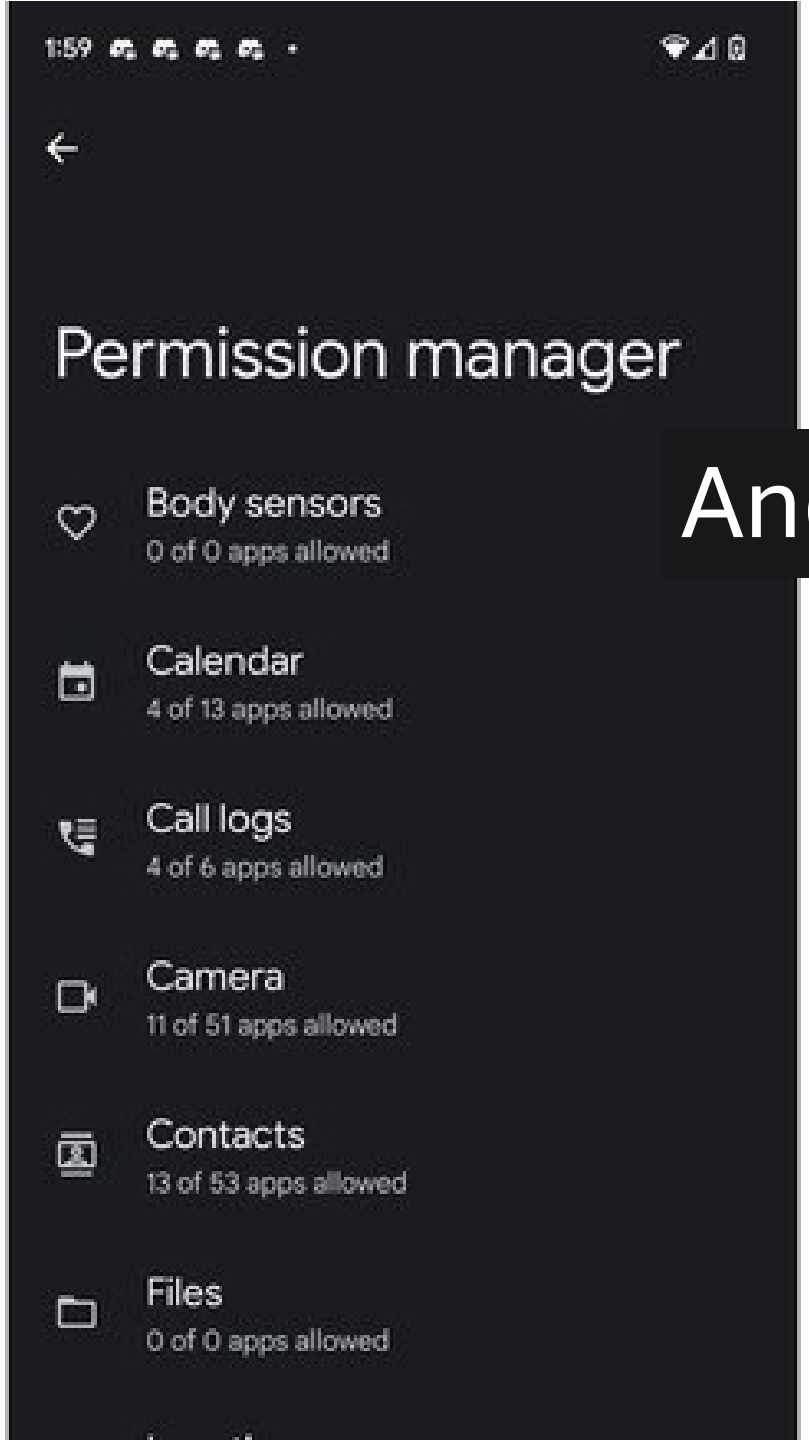

9:41
Settings
Siri & Search
Face ID & Passcode
Emergency SOS
Exposure Notifications
Battery
Privacy & Security
App Store
Wallet
Passwords
Mail
Contacts
Calendar
Notes


9:41
Settings
Privacy & Security
Location Services
On
Tracking
Contacts
Calendars
Reminders
Photos
Bluetooth
Local Network
Microphone
Speech Recognition
Camera
Health
Research Sensor & Usage Data

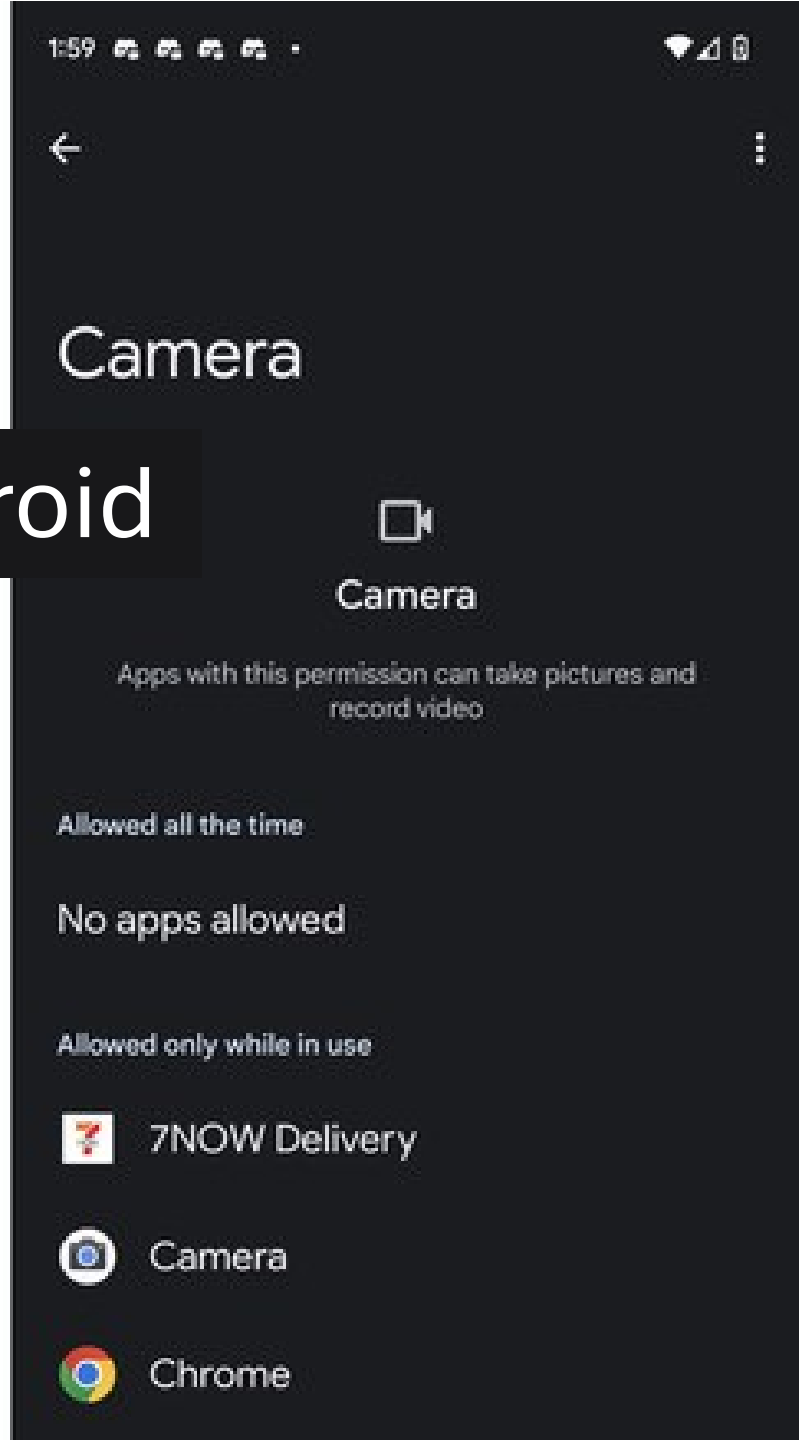

9:41
Back
Contacts
Cleaner
Instagram
Skype
Snapchat
TikTok
WhatsApp
Applications that have requested access to your contacts will appear here.

iPhone


1:59
Security & privacy
Settings
App security
Play Protect scanned 1 hour ago
Device lock
Screen lock, Fingerprint Unlock
Google Security Checkup
Your account is protected
Find My Device
On
Updates
Device is up to date
Privacy
Dashboard, permissions, controls
More settings


1:59
Permission manager
Body sensors
0 of 0 apps allowed
Calendar
4 of 13 apps allowed
Call logs
4 of 6 apps allowed
Camera
11 of 51 apps allowed
Contacts
13 of 53 apps allowed
Files
0 of 0 apps allowed

Android


1:59
Camera
Camera
Apps with this permission can take pictures and record video
Allowed all the time
No apps allowed
Allowed only while in use
7NOW Delivery
Camera
Chrome

# Schutz vor Cyberangriffen: Mobiles Leben und Arbeiten

Freistaat SACHSEN

### Betriebssystem und Apps aktuell halten

Updates schließen bekannte Sicherheitslücken.

### Nur vertrauenswürdige Apps installieren

Apps können Schadsoftware enthalten oder Daten ausspähen.

### App-Berechtigungen auf ein Mindestmaß reduzieren

Apps sollten nur genau die Berechtigungen erhalten, die für ihre Funktion wirklich erforderlich sind.
Grundprinzip: So wenig wie möglich, so viel wie nötig.

> Daten sind ein toxisches Gut.
> Je mehr man sammelt, desto größer wird die Angriffsfläche
> – besonders auf mobilen Geräten.

Bruce Schneier, Experte für IT-Sicherheit und Kryptografie

# Sicherheitstipps

- Angemessenes Verhalten im Sicherheitsvorfall
- Wenn man selbst Administrator ist – 6 Lagen an Sicherheit zuhause

Freistaat SACHSEN

# Sicherheits-vorfall?

B S I

Ereignis mit negativem Einfluss auf die Informationssicherheit – insbesondere auf die Verfügbarkeit, Vertraulichkeit oder Integrität von Informationen oder IT-Systemen.

Phishing-Angriff mit kompromittiertem E-Mail-Konto

Ransomware-Infektion durch verseuchte Datei

Verlust eines unverschlüsselten USB-Sticks mit Bürgerdaten

# Sicherheits-vorfall?

Ein Sicherheitsvorfall ist ein Ereignis, das tatsächlich nachteilige Auswirkungen auf die Informationssicherheit hat.
§ 3 Abs. 5 SächsISichG

Unbefugter Zugriff auf Sozialdaten

Manipulation von Verwaltungsdaten

Klick auf einen vielleicht verseuchten Anhang

# Sicherheits-vorfall?

1. Ruhe bewahren
2. BfIS in der eigenen Behörde ansprechen
3. Keine eigenen Aktivitäten

# Ein Sicherheitskonzept für Zuhause

Freistaat SACHSEN

**Router & WLAN absichern**

Admin-Standardpasswort ändern, ein starkes Kennwort wählen, WPA3-Verschlüsselung nutzen.

**Updates sofort einspielen**

Verzögertes Patchen macht Geräte und Daten unnötig angreifbar.

**Netzwerktrennung einrichten**

Separates Gastnetzwerk einrichten, das logisch vom HeimLAN getrennt ist.

**Starke, einzigartige Passwörter + Passwortmanager + 2FA verwenden**

**Unnötige Programme + Apps löschen, App-Berechtigungen stark einschränken**

**Regelmäßige Datensicherung**

Bei Bedarf Backups nach der 3-2-1-Regel durchführen.

Freistaat SACHSEN

# Live Hacking

Vielen Dank
für Ihre
Aufmerksamkeit!