

Cybercrime - Bedrohungslage und Handlungsempfehlungen des LKA MV Schwerin, den 18.06.2025

LKA MV, Abt. 7 - Digitales Service- und Kompetenzzentrum (DiSK)
KHK Stephan Gäfke
BTZ Werkstraße 600 19061 Schwerin



Angebot der Zentralen Ansprechstelle Cybercrime MV – ZAC MV



Präventionsvorträge,
Beratung



Aufnahme
Warnhinweise/Meldungen



Durchführung & Koordinierung eilbedürftiger
Maßnahmen für die Strafverfolgung



Vermittlung zur passender
Stelle zur Anzeigenaufnahme



ZAC MV-
Hotline



Erreichbarkeiten aller ZAC:
www.polizei.de/ZAC







```
1  >> Introduction
2
3  Important files on your system was ENCRYPTED and now they have have "${EXTENSION}" extension.
4  In order to recover your files you need to follow instructions below.
5
6  >> Sensitive Data
7
8  Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.
9
10 Data includes:
11 - Employees personal data, CVs, DL, SSN.
12 - Complete network map including credentials for local and remote services.
13 - Financial information including clients data, bills, budgets, annual reports, bank statements.
14 - Complete datagrams/schemas/drawings for manufacturing in solidworks format
15 - And more...
16
17 Private preview is published here: http://alphvmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/[snip]
18
19
20 >> CAUTION
21
22 DO NOT MODIFY FILES YOURSELF.
23 DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
24 YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
25 YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.
26
27 >> Recovery procedure
28
29 Follow these simple steps to get in touch and recover your data:
30 1) Download and install Tor Browser from: https://torproject.org/
31 2) Navigate to: http://sty5r4hbb5oihbq2mwvofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd.onion/?access-key=${ACCESS_KEY}
```

Die Frage lautet nicht OB, sondern
WANN Sie von einem Cyberangriff
betroffen sein werden!

... und WIE OFT?

1. Bedrohungslage

Phänomene Cybercrime

Ransomware		Online-Erpressung mittels Verschlüsselungstrojaner
Phishing		über Mails oder Webseiten - Vorstufe für weitere Phänomene
CEO-Fraud		Geschäftsführerschwindel
Man in the Middle		Geschäftspartnerschwindel
DDoS		• Distributed Denial of Service = Störung der IT-Verfügbarkeit
Datendiebstahl		• Veröffentlichung von Daten → bei Ransomware-Angriffen als Double/Triple Extortion üblich

Höchstes
Schadens-
potenzial

Phasen eines Cyberangriffs

Phase 0



Zugangsdaten
erlangen &
Systeme
infiltrieren

Phase 1



Malware
nachladen &
Daten
exfiltrieren

Phase 2



- Systeme
verschlüsseln &
Daten
veröffentlichen
- Double
Extortion

Phase 3



- Weitere
Eskalation
- Triple Extortion

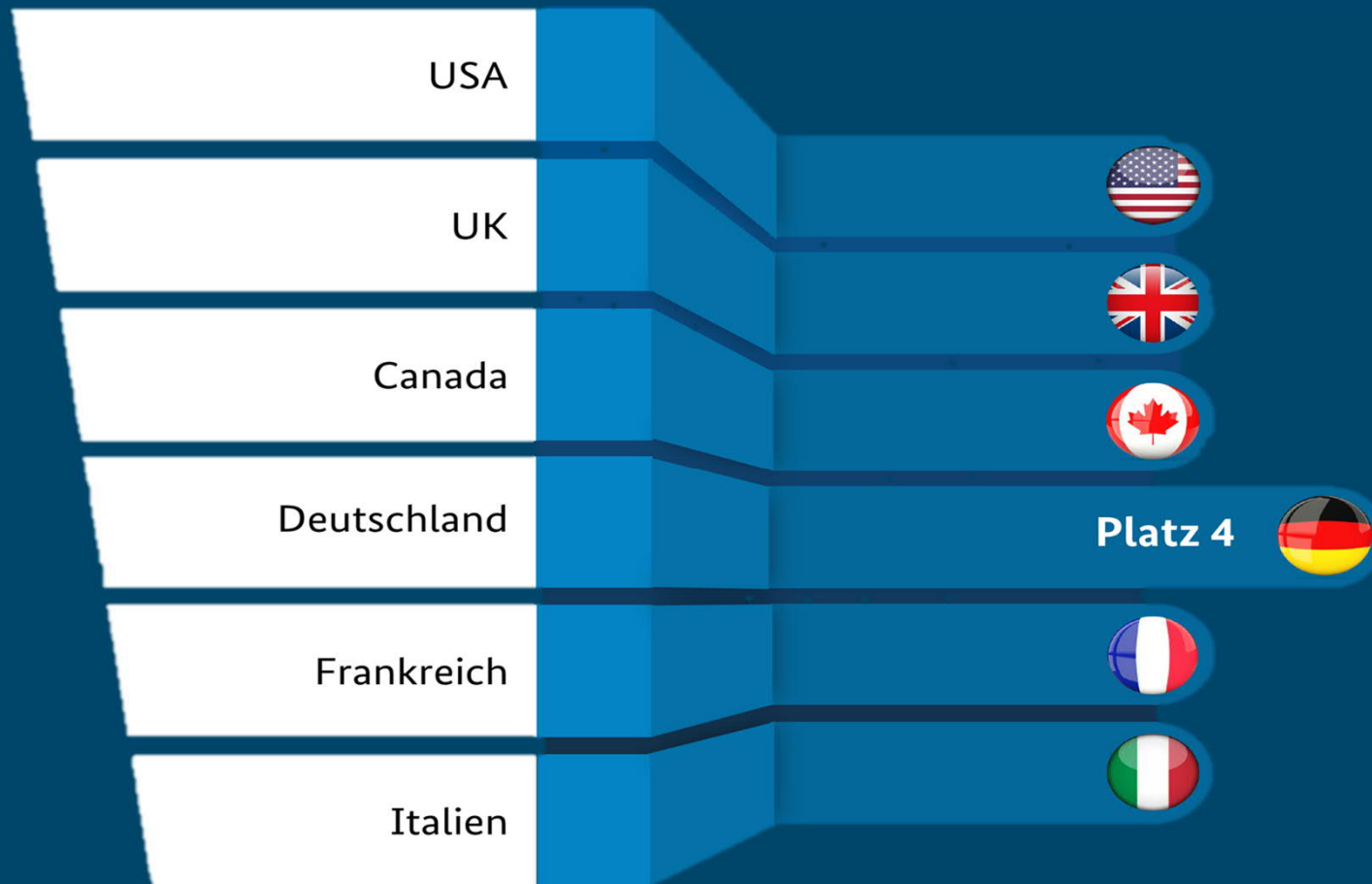
Quelle: BKA

Motivation der Hacker



Betroffene Länder

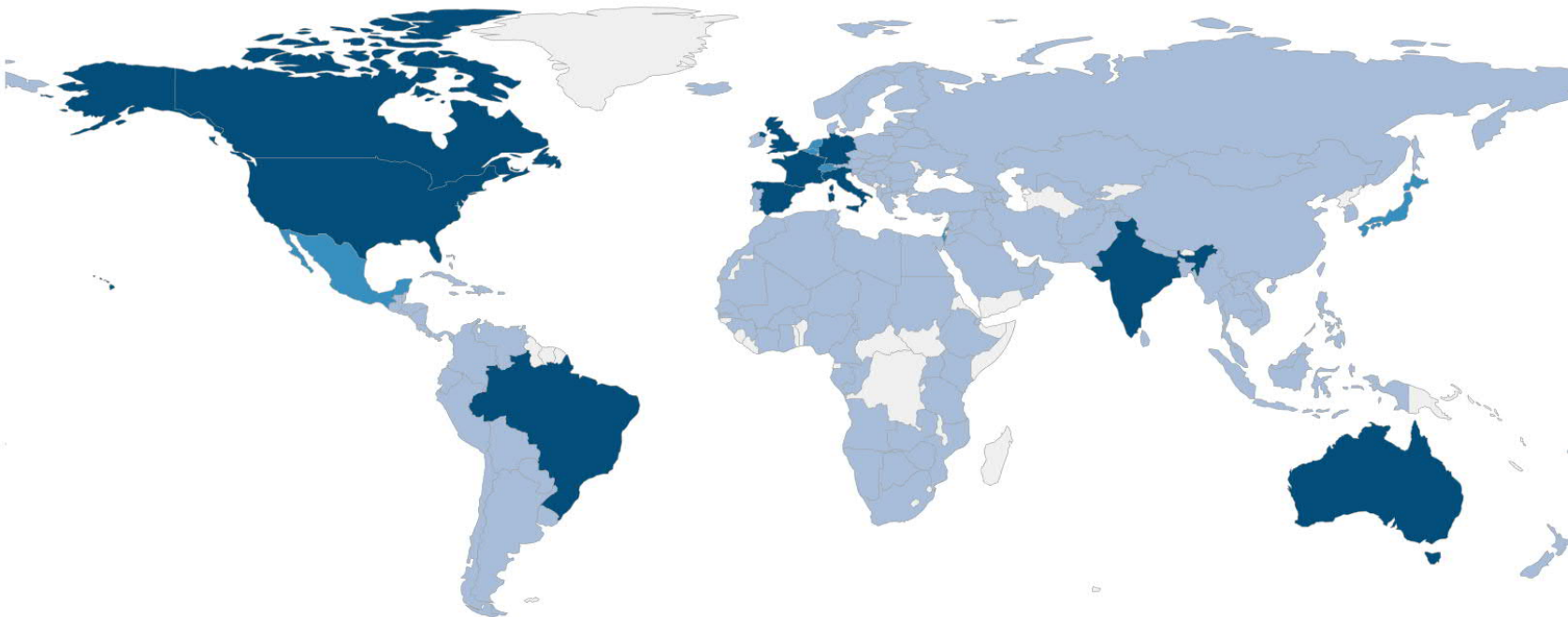
Deutschland
ist ein
lukratives
Angriffsziel



Quelle: BKA

2023 2024 2025 Full Reset

Ransomware Victims by Country (All years)



Die Bedrohungslage im Cyberraum ist anhaltend hoch.

Die Anzahl polizeilich bekannt gewordener Cyberdelikte steigt - maßgeblich hierfür sind vor allem Fälle, bei denen der Handlungsort des Täters unbekannt oder im Ausland ist.



rund **90%**
Dunkelfeld

Täter in
Deutschland
131.391
Fälle

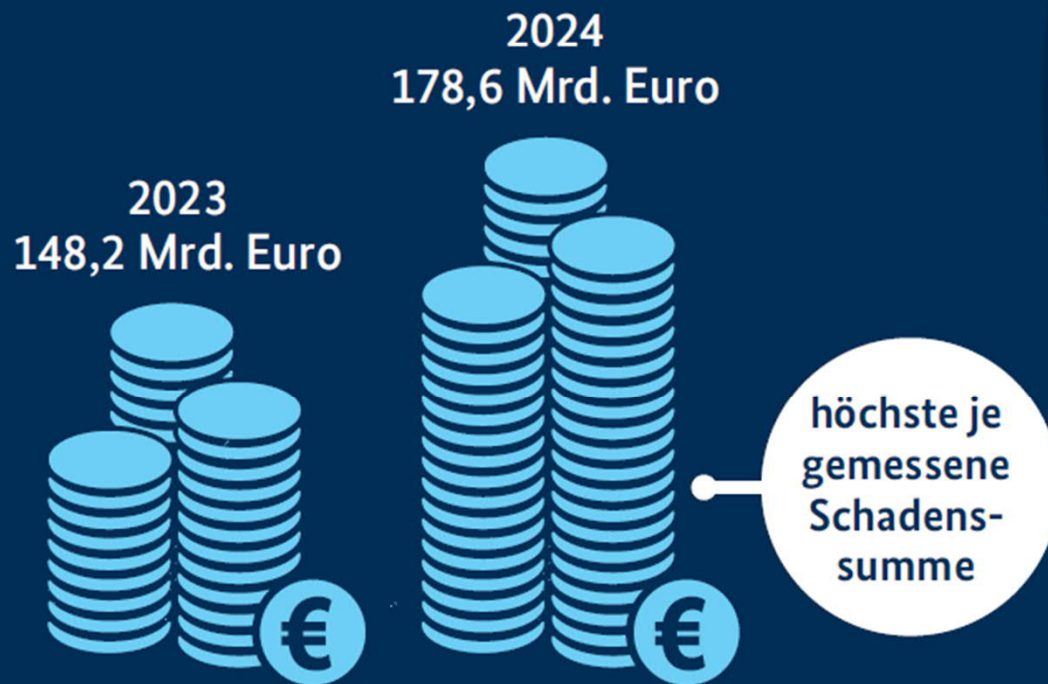
Täter im Ausland/
unbekannt¹
201.877
Fälle

Gründe für die Nicht-Anzeige
sind oft Scham, Angst vor
Reputationsverlust oder der
Angriff wurde gar nicht bemerkt.

Quelle: BKA

Bedrohungslage

Wirtschaftlicher Schaden durch Cyberattacken



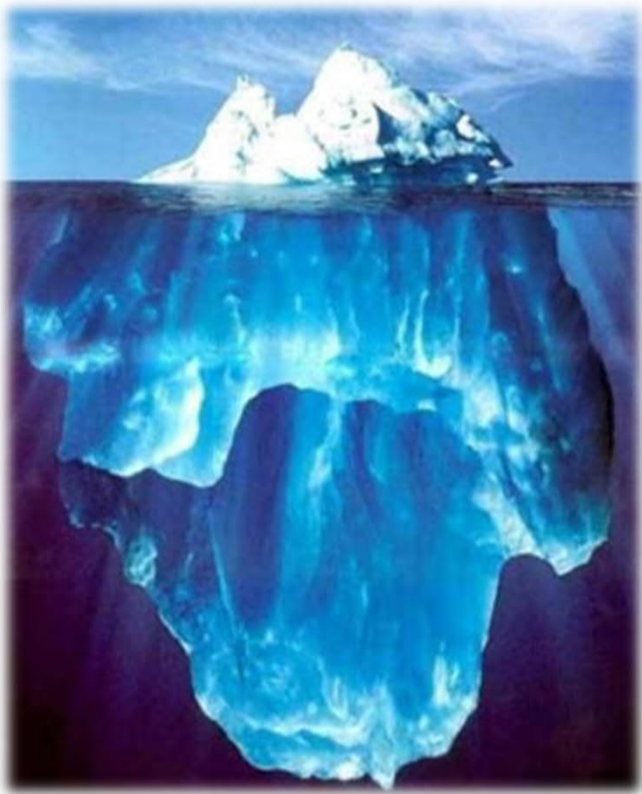
Quelle: Bitcom e.V.

Underground Economy

Cyberkriminelle agieren hochprofessionell und arbeitsteilig. Sie bieten in industriellem Maßstab kriminelle Dienstleistungen zur Begehung von Cyberstraftaten an.



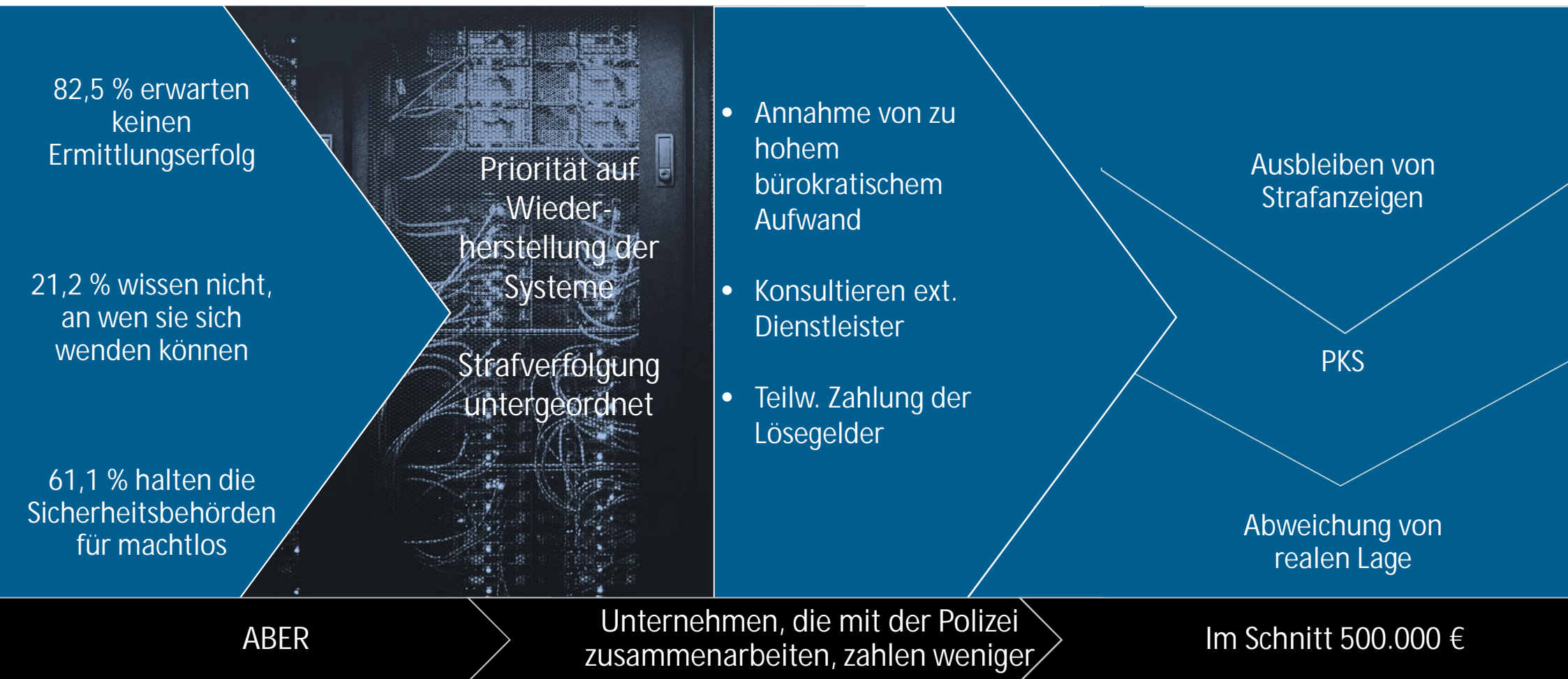
Dunkelfeldstudie MV



Dunkelfeldstudie LKA MV

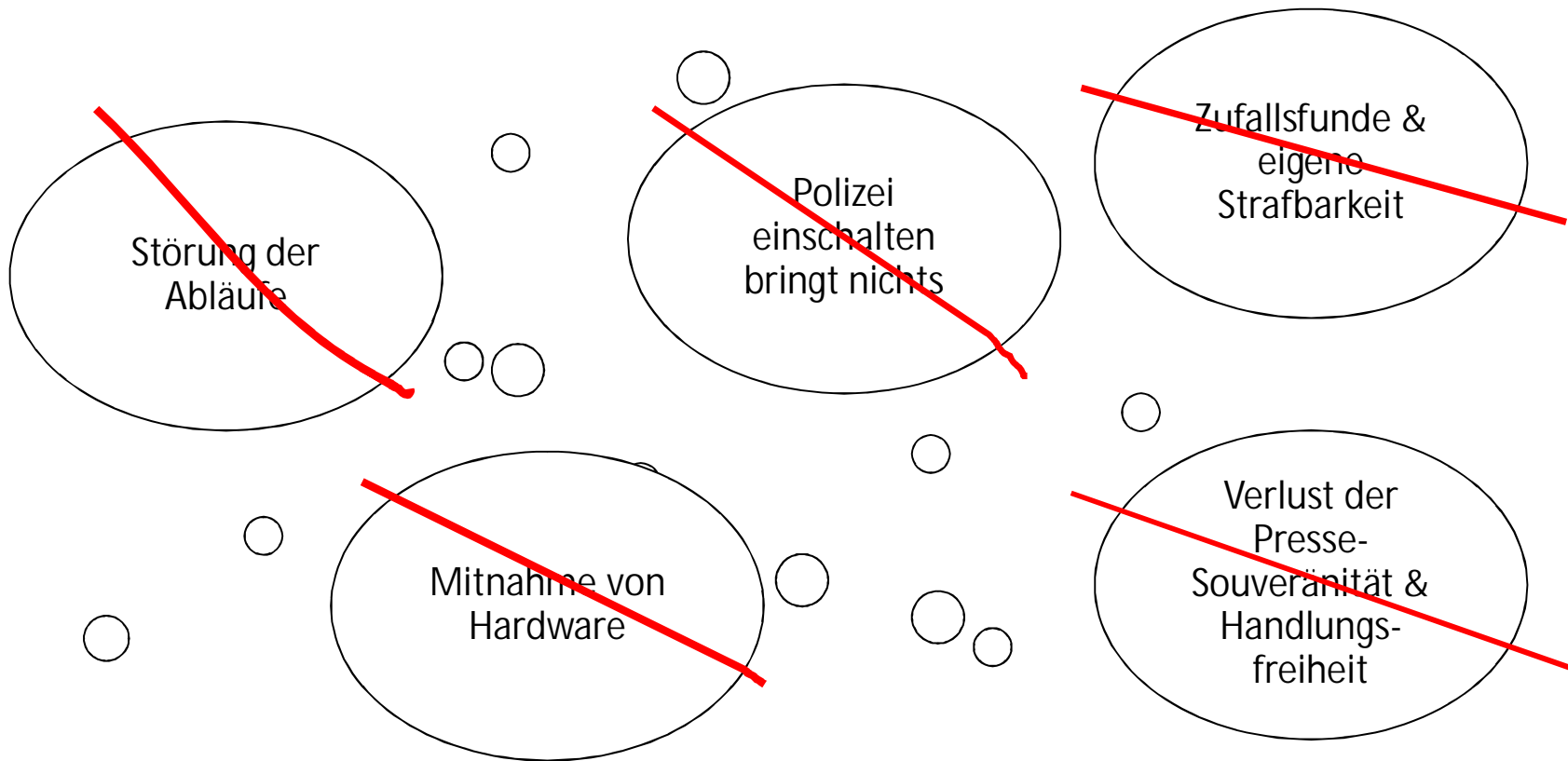
- über 90% gaben an, Opfer von Cybercrime geworden zu sein
- nur etwa jede 135. Straftat wird der Polizei bekannt

Dunkelfeldstudie Bitkom



Quelle: Studie Bitkom 2022/23; BKA

Mythencheck



2. Wie kommt es zu Cyber-Vorfällen?

Umfrageergebnisse Digitalbarometer



Updates & Patches

- 27% nutzen veraltete Software
- 31% aktualisieren Apps oder das mobiles Betriebssystem nur dann, wenn neue Funktionen angekündigt werden
- 8% aktualisieren das Smartphone nie
- → Bedeutung und Wichtigkeit von Updates sowie ihre Notwendigkeit nicht im Bewusstsein



Passwörter

- 41 % nutzen dasselbe Passwort für mehrere Accounts
- 4% nutzen immer dasselbe Passwort bei allen Accounts

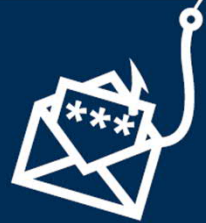


Erfahrungen mit Cyber-Kriminalität

- 29% sind schon einmal Opfer von Cyber-Kriminalität geworden
- 39% erlebten Cyber-Kriminalität mindestens einmal in den vergangenen zwölf Monaten
- 62% erhielten betrügerische Phishing-Mail, ohne auf diese eingegangen zu sein

Quelle: vgl. Digitalbarometer zur Cyber-Sicherheit 2022, ProPK und BSI

Trends und Entwicklungen



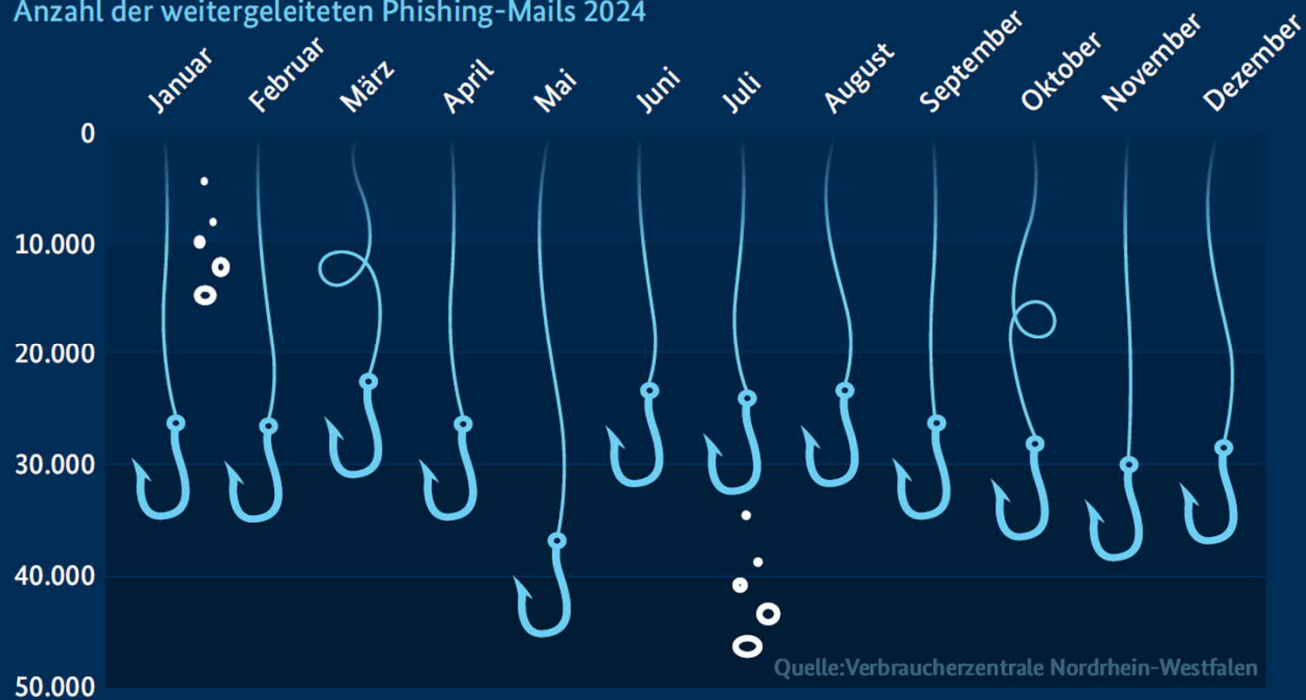
Phishing

400.000

vgl. zu 2023:
Anstieg um fast
70%

Phishing-E-Mails wurden 2024 der Verbraucher-
zentrale Nordrhein-Westfalen gemeldet

Anzahl der weitergeleiteten Phishing-Mails 2024

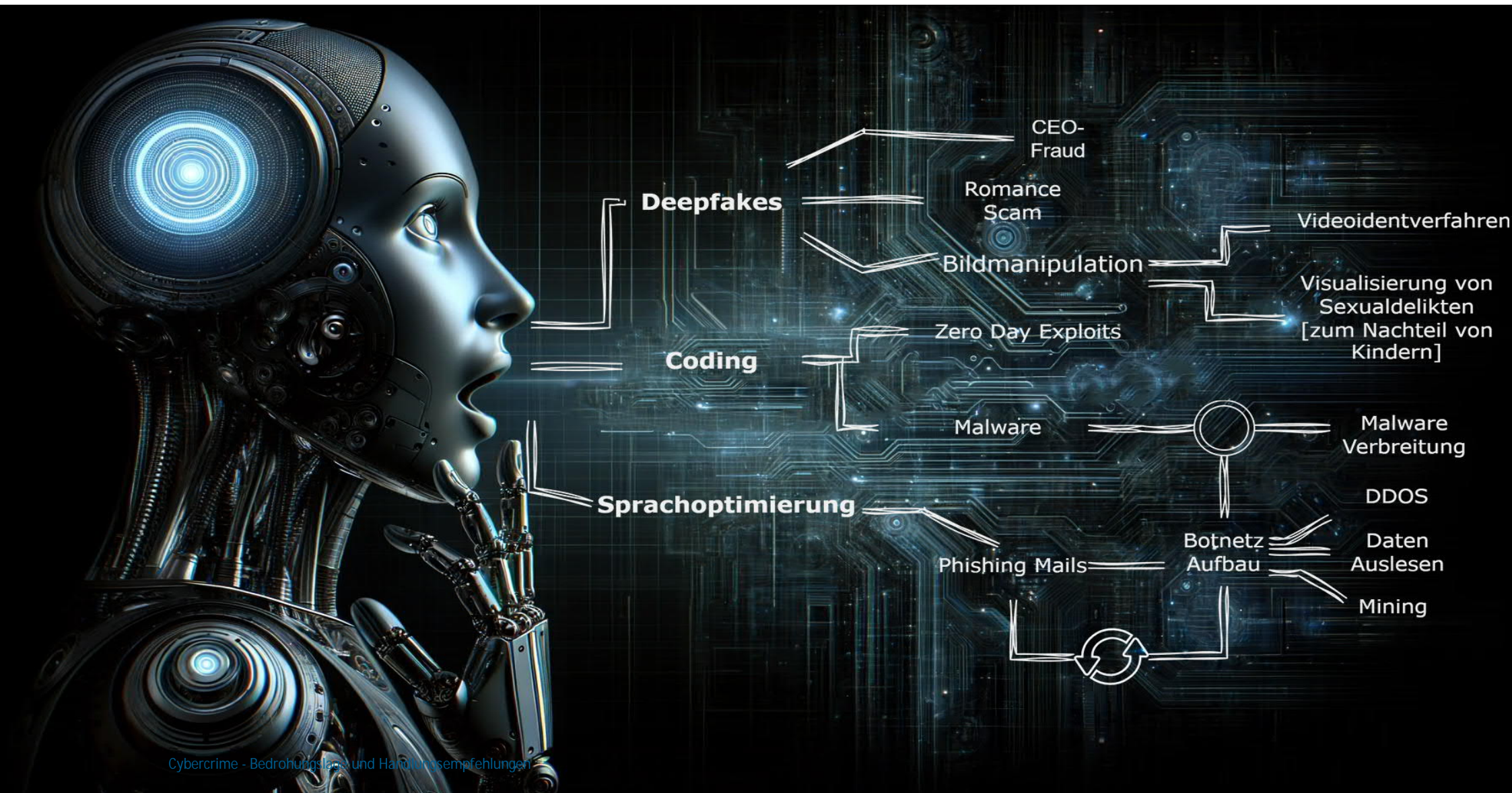


Quelle: Verbraucherzentrale Nordrhein-Westfalen



Wie in den Vorjahren
beziehen sich die
häufigsten Narrative
auf den Finanzsektor,
der eine hohe
Bedeutung für Staat
und Bevölkerung hat.

Gefahren KI – das kommt auf uns zu ...



3. Handlungsempfehlungen des LKA MV

Negativbeispiele in MV

keine
Kontaktmöglichkeit,
keine Informations-
steuerung
→ Höchste Gefahr
Ransomware

Keinen
IT-Verantwortlichen/
IT-Dienstleister

schlechte interne
Verifizierung &
Kommunikation
→ Höchste Gefahr
CEO-/BEC-Fraud



Positivbeispiele MV



Angriff abgewehrt → Es bleibt beim Versuch der Straftat
Wenn nur noch die Anzeige aufgenommen wird

- BEC-/CEO-Fraud → mit DKIM, SPF, DMARC wurden die betrügerischen Mails gar nicht durchgestellt
- Ransomware → Backup bei Verschlüsselung nicht betroffen, Daten gesichert und Lessons Learned
- Malvertising → Öffnen von Links zum Internet unterbunden, PDF-Ansicht in Outlook deaktiviert
- DDoS → Load-Balancer

Eskalation eines Cyber-Vorfalls

Fehlerkultur

Notfallplan

Erstattung
einer
Strafanzeige

VERHALTEN BEI IT-NOTFÄLLEN



Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!



IT-Notfallrufnummer:



Wer meldet?



Welches IT-System ist betroffen?



Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?



Wann ist das Ereignis eingetreten?



Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit
am IT-System
einstellen

Beobachtungen
dokumentieren

Maßnahmen nur
nach Anweisung
einleiten

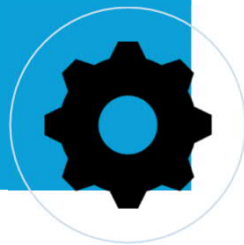
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Handlungsempfehlungen der Zentralen Ansprechstelle Cybercrime MV

- Patch-Management
- Segmentierung der IT-Netze und Firewalls, SIEM
- Backups

• Beispiele:
Backup-Mgmt, Offline-Backup, Restore-Szenarien

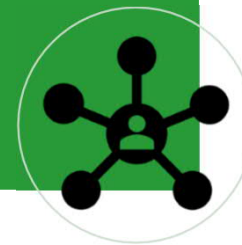
Technische Sicherheit



- Sensibilisierung der Mitarbeiter
- Eingeschränkte Benutzer- und Admin-Rechte
- Klare Vorgaben sowie IT-Notfall-Management

• Beispiele:
„Human Firewall“, Fehlerkultur, 2FA/MFA

Organisatorische Sicherheit



Wichtig:
Es gibt nicht nur
den einen Tipp.

Sichern Sie Ihre IT, wie
sie Ihr eigenes Haus
sichern würden!

Kein Backup – kein Mitleid?

Sichern vor Diebstahl und Zerstörung

- 3-2-1-Regel:



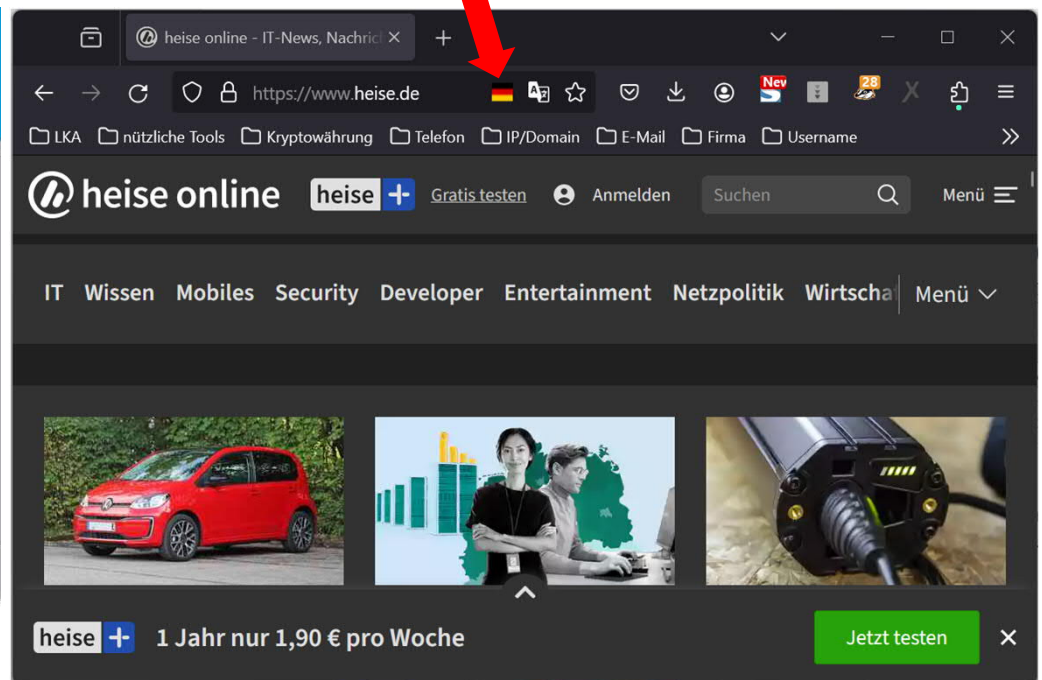
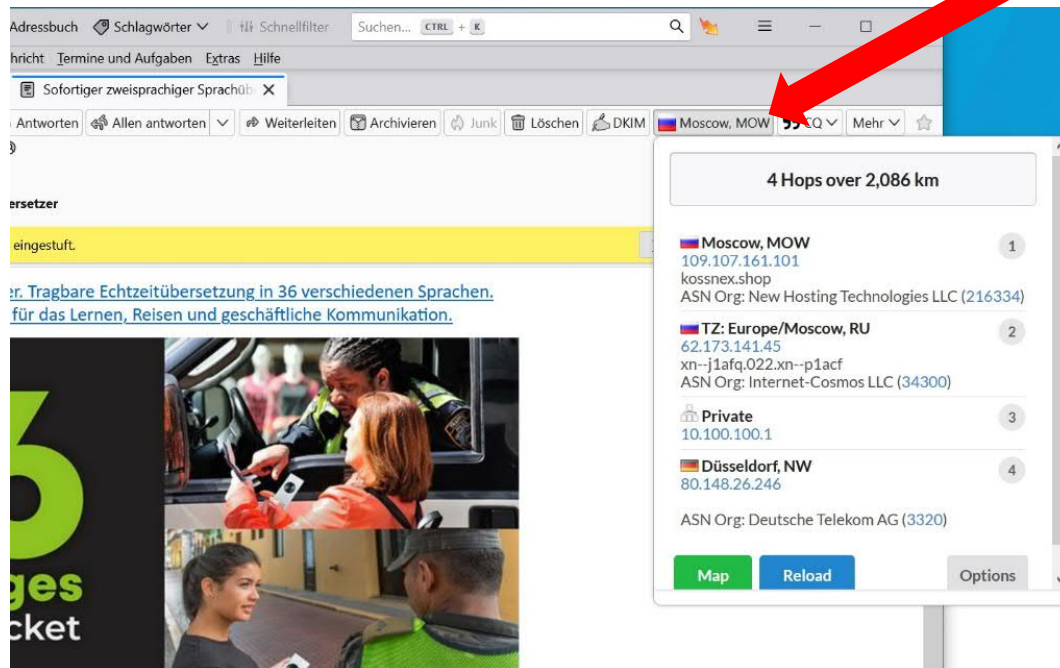
Quelle: it-experte-augsburg.de

- Aktuelle Backup-Strategie und Backup-Zeiten
- Backups auf Vollständigkeit und Fehlerfreiheit prüfen
- BaaS und Software für inkrementelle, differentielle und selektive Backups
- Verschlüsseln



Handlungsempfehlungen - E-Mail-Sicherheit

→ mit Plugins für Mailclient/ Browser (z.B. MailHops und Flagfox)



Handlungsempfehlungen

2FA / MFA – Hardware-Token/ YubiKey bereits in folgenden Bereichen im Einsatz

Professionelle Benutzer: Vertrauen von stark regulierten Branchen



Finanzen

Mit modernen Kryptographie- und Sicherheitsprotokollen, YubiKeys sichern Banken, Mitarbeiter und der Konten ihrer Kunden.



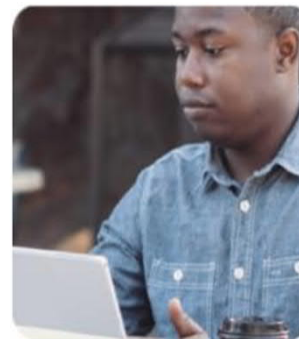
Gesundheitswesen

Die Gesundheitsbranche und andere regulierte Branchen verwenden YubiKeys, um Konten und IT-Infrastruktur in Cerner und anderen EHR-Technologien zu sichern.



Entwickler

Entwickler schützen ihre Projekte mit dem FIDO2-Schutz in YubiKey 5 – dem einzigen von GitHub unterstützten Sicherheitsschlüssel.



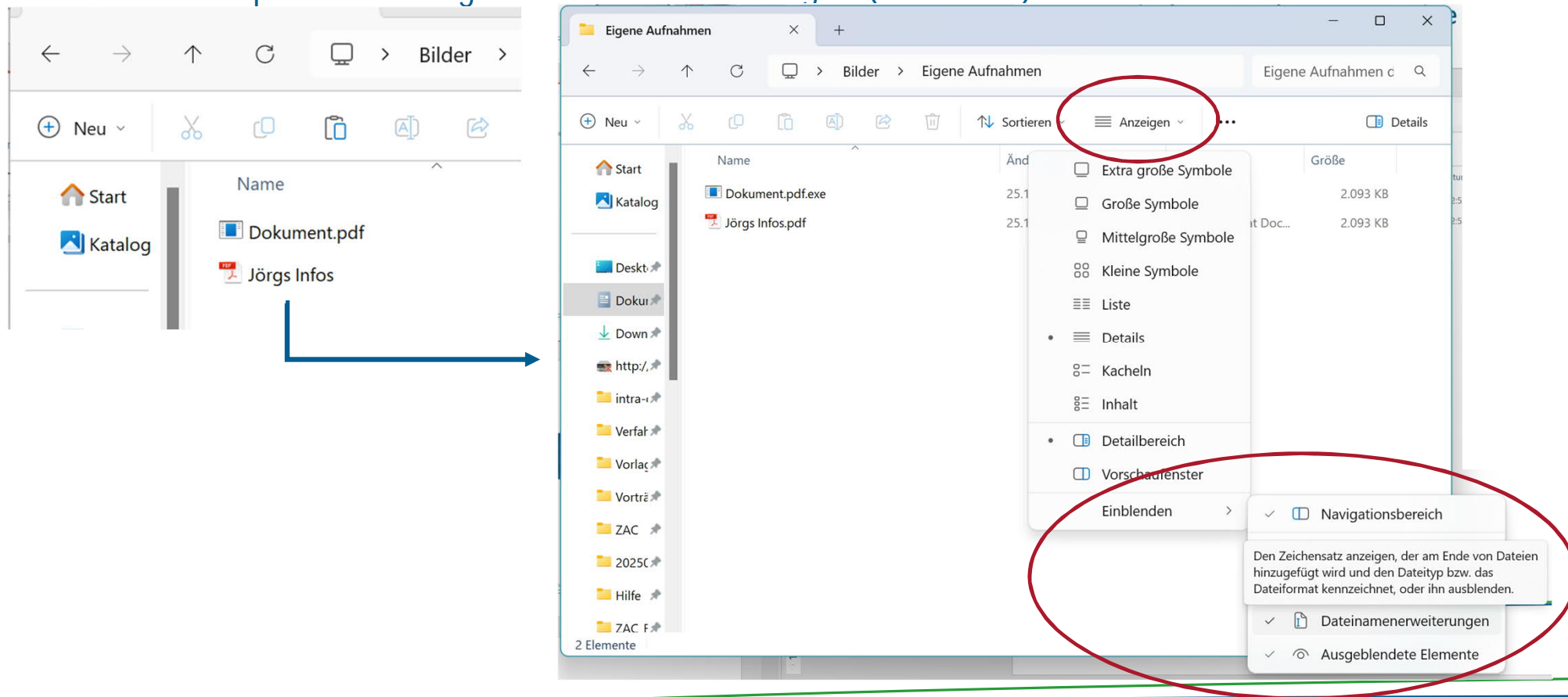
Energie

Der Energiesektor verwendet YubiKeys, um die Authentifizierung für Anwendungen, Daten und Infrastrukturen zu sichern, um Cyber-Bedrohungen standzuhalten.



Handlungsempfehlungen

Windows Explorer – Anzeige der Dateierweiterungen (Extension) einschalten !



Handlungsempfehlungen

Unterstützung und Informationen beim BSI einholen

Kleine- und Mittlere Unternehmen

Informationen und Hilfestellungen für KMU

Kleine und mittlere Unternehmen (KMU) werden zunehmend Ziel von Cyber-Attacken. Nicht selten führen diese zu immensen Schäden und schwächen die Unternehmensreputation. Oftmals werden Daten von Kunden und Kooperationspartnern sowie andere sensible Daten abgegriffen, verändert, gelöscht, verschlüsselt und/oder auf inkriminierten Internetseiten veröffentlicht. Wiederholt nutzen Kriminelle die gestohlenen Daten für weitere Hackerangriffe und andere Straftaten.



Dabei werden KMU meist nicht zielgerichtet zum Opfer, sondern werden von großflächig und automatisiert durchgeführten Angriffen getroffen. Es ist also höchste Zeit auch für KMU, die Informations- und Cyber-Sicherheit auf den neuesten Stand zu bringen und Mitarbeiterinnen und Mitarbeiter beim Gebrauch der Informationstechnik (IT) im Hinblick auf die gängigen Betrugsmaschinen der Hacker regelmäßig zu sensibilisieren.

Auf diesen Seiten gibt das BSI ausgewählte hilfreiche Tipps - für Unternehmen ohne IT-Expertise und für Unternehmen, die sich bereits eigene oder extern beauftragte IT-Fachleute leisten.

MIT Standard sicher

IT-Sicherheit IN DER WIRTSCHAFT

Der CyberRisiko-Check: IT-Sicherheit einfach anpacken

IT-Sicherheitsberatung nach der neuen DIN SPEC 27076

Mittelstand Digital


www.mit-standard-sicher.de

Bundesministerium für Wirtschaft und Klimaschutz

NEU!

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/WIBA/Weg_in_die_Basis_Absicherung_WiBA_node.html

Hier können Sie sich informieren!




Bundeskriminalamt

Es hat Sie erwischt!

CYBER- ANGRIFE AUF IHR UNTERNEHMEN, IHRE BEHÖRDE ODER INSTITUTION

Sie haben Vorbehalte, uns einzuschalten? Das haben wir verstanden! Lassen Sie uns reden.



Ihre Firma

Was bringt es mir, die Polizei zu kontaktieren? Die finden den oder die Täter doch sowieso nicht.

Täterermittlungen sind lediglich ein Strang. Wir werden nicht jeden Hacker finden können. Aber wir können deren IT-Infrastruktur stören oder herunternehmen oder an ihr Geld kommen.

Wenn ich die Polizei verständige, nimmt sie große Teile meiner Hardware mit und bringt sie nicht oder nicht zeitnah zurück.

Wir müssen nicht in jedem Fall bei Ihnen im Unternehmen aktiv werden. In vielen Fällen können Sie uns relevante Daten einfach aushändigen. Nur in Einzelfällen ist eine Datensicherung vor Ort durch die Polizei erforderlich, die wir natürlich mit Ihnen abstimmen.

Polizei und Staatsanwaltschaft ermitteln dann eher gegen mich, wenn sie etwas Belastendes gefunden haben. Dabei bin ich/sind wir das Opfer der Attacke und haben andere Sorgen.

Wir sind auf den Sachverhalt fokussiert, bei dem Sie geschädigt sind. Im Übrigen geben Sie uns die Daten, wir suchen nicht danach in Ihren Systemen.

Wenn ich heute mit der Polizei oder Staatsanwaltschaft spreche, steht morgen alles in der Presse!

Das Gegenteil ist der Fall, gerade in der frühen Phase der Ermittlungen werden generell keine proaktiven Presseauskünfte erteilt. Auch im weiteren Verlauf stimmen wir die Pressearbeit mit Ihnen ab.

Wenn ich Polizei und Staatsanwaltschaft einbinde, darf ich doch am Ende gar nichts mehr entscheiden, also etwa ob ich Erpressungsgeld zahle oder mit den Tätern kommuniziere.

Sie entscheiden - wir beraten. Sie können von unserer Erfahrung in solchen Angriffssituationen profitieren.

Strafverfolgung



Was braucht die Strafverfolgung eigentlich?

- Die Daten zu einem Angriff liegen bei Ihnen. In den Daten liegen die Spuren zu den Tätern und ihrer Infrastruktur.
- Wir möchten **schnellstmöglich** mit diesen Daten arbeiten.
- Wir benötigen von Ihnen:** Malwaresamples, (IP-Adressen aus) Logfiles, E-Mailadressen, von denen mit Ihnen kommuniziert wurde, jede Information zur Täterkommunikation, Hinweise auf Leak-Pages...
- Wir wissen, dass es bei Ihnen **brennt**. Darauf werden wir Rücksicht nehmen. Die Rettung Ihres Unternehmens steht im Fokus Ihres Tuns.
- Daten sind für uns auch von extrem großem Wert, wenn Sie im Eifer des Gefechts **nicht forensisch** gesichert wurden.
- Unsere Empfehlung: Binden Sie die Polizei frühzeitig ein!**
- Lassen Sie Ihre Techniker oder beauftragte IT Security Unternehmen mit unseren Technikern sprechen und sich von uns beraten.
- Wir finden einen Weg, Sie möglichst wenig zu belasten und so schnell wie möglich an notwendige Spuren zu kommen.

Wer hilft mir weiter?

Die **Zentralen Ansprechstellen Cybercrime (ZAC)** der Polizeien des Bundes und der Länder stehen **Unternehmen und öffentlichen Einrichtungen** als kompetente und vertrauensvolle Partner zur Verfügung

- für Informationen und Beratung zur Vermeidung von Cybercrime-Angriffen (Prävention)
- für richtiges Verhalten bei Cybercrime-Angriffen gegen Ihr Unternehmen (Intervention, Strafverfolgung).

Das Bundeskriminalamt ist unmittelbar zuständig für die Strafverfolgung bei Cyberangriffen auf **Kritische Infrastrukturen** (sog. KRITIS-Unternehmen) sowie auf **Behörden und Einrichtungen des Bundes**. Ansprechpartner ist in diesen Fällen die **ZAC BKA** sowie die 24/7 erreichbare **Einsatzbereitschaft Cybercrime**.

In **allen anderen Fällen** sind die **Cybercrime-Dienststellen der Landespolizeibehörden** zuständig. Die örtlich zuständige Dienststelle sowie Informationen und Beratung zum Phänomenbereich Cybercrime erhalten Sie über die ZAC der Landeskriminalämter (ZAC LKÄ).

Bei vielen ZACs findet außerhalb der Bürozeiten eine Weiterleitung an einen Bereitschaftsdienst statt. In **akuten Notfällen**, wenn mit den angegebenen Nummern kein Kontakt hergestellt werden kann, ist auch die Wahl des Notrufes denkbar.

ZAC BUNDESKRIMINALAMT

Referat CC12-ZAC
65173 Wiesbaden
Tel. (reg.): 0611/55-15037
Internet: www.bka.de



WEBSEITE

Was wir von Ihnen brauchen

Allgemein



- Was ist betroffen?
- Einschätzung der Ursache
- Infos über Auswirkungen & Schäden
- Gibt es Incident Response-Dienstleister?
- Hinweise auf Leak-Seiten
- Ansprechpartner innerhalb der Firma

Spezifisch



- Malwaresamples, Images, Dateien, IoCs, Logdaten, etc.
- Netzwerkdaten: IP-Adressen, Clients, Server, Netflowdaten, Firewalldaten, Übersichten, etc.
- Kommunikation mit den Tätern: Mails, Kryptoadressen, Ransomnotes, etc.
- Sonstige Dokumentationen

Handlungsempfehlungen der Zentralen Ansprechstelle Cybercrime MV

Da die Frage nicht lautet OB, sondern WANN Sie von einem Cyberangriff betroffen sein werden, sollte Folgendes gelten:

- IT-Sicherheit ist Chefsache – Eigenverantwortung
- neben Gewährleistung IT-Sicherheit, vorbereitet sein, wenn nichts mehr geht
→ z.B. Mailadresse (unabhängig v. Mailsystem), separater DSL-Anschluss, Telefon (Handy)
- IT-Sicherheit = Prozess, der täglich zu leben und aufrecht zu halten ist
- IT-Sicherheit nicht nur eingesetzte IT-Spezialisten, sondern kontinuierliche Aufgabe aller Mitarbeiter
- Einschalten der Polizei im Schadensfall (Entscheidungsträger festlegen)
- Investition in IT-Sicherheit ist Investition in die Zukunft

Empfehlungen

Webseiten:

www.bsi.bund.de

www.bka.de

www.polizei.de/zac

www.polizei.mvnet.de/onlinewache

www.phish-test.de

Veranstaltungen:

Krisensimulation IHK zu Schwerin

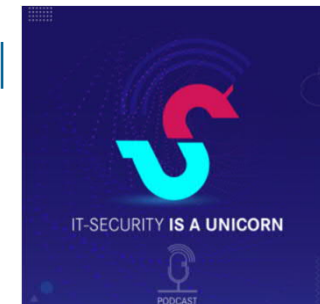
Krisensimulation IHK zu Rostock

Podcasts:

You are fucked –
Deutschlands erste
Cyberkatastrophe



IT-Security is a Unicorn |
für digitale
Führungskräfte





Who you gonna call?



ZAC MV-Hotline
+493866649494

Vielen Dank für Ihre Aufmerksamkeit!

Ansprechpartner/ Rückfragen:

Landeskriminalamt Mecklenburg-Vorpommern

KHK Stephan Gäfke

Hotline ZAC: 03866 / 649494

E-Mail: zac@lka-mv.de

<https://polizei.mvnet.de/Polizei/LKA>

