

Fortbildungsveranstaltung für Zahnärzte in M-V

Cybercrime – Bedrohungslage und Handlungsempfehlungen des LKA MV

am 11.09.2024 (KZVMV)

Abteilung 7 – Digitales Service und Kompetenzzentrum
Zentrale Ansprechstelle Cybercrime (ZAC), LKA MV
KHK Jörg Patzer, 1. Sachbearbeiter Dezernat - Cybercrime



!!! WICHTIGE INFORMATIONEN !!!!

Alle Dateien wurden mit RSA-2048 und AES-128 Ziffern verschlüsselt.

Mehr Informationen über RSA können Sie hier finden:

<http://de.wikipedia.org/wiki/RSA-Kryptosystem>

http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

Die Entschlüsselung Ihrer Dateien ist nur mit einem privaten Schlüssel und einem Entschlüsselungsprogramm, welches sich auf unserem Server befindet, möglich.

Um Ihren privaten Schlüssel zu erhalten, folgen Sie einem der folgenden Links:

1. <http://6dtxgqam4crv6rr6.tor2web.org/7D>
2. <http://6dtxgqam4crv6rr6.onion.to/7D>
3. <http://6dtxgqam4crv6rr6.onion.cab/7D>

Sollte keine der Adressen verfügbar sein, folgen Sie den folgenden Schritten:

1. Laden Sie einen Tor Browser herunter und installieren diesen: <https://www.torproject.org/download/download.html>
2. Starten Sie den Browser nach der erfolgreichen Installation und warten auf die Initialisierung.
3. Tippen Sie in die Adresszeile: 6dtxgqam4crv6rr6.onion/7D
4. Folgen Sie den Anweisungen auf der Seite.

!!! Ihre persönliche Identifizierungs-ID lautet: 7D

Bild: Ransomnote

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

Agenda

1. Vorbemerkungen
2. Zahlen, Daten, Fakten Cybercrime
3. Ausgewählte Cybercrime-Phänomene
4. Handlungsempfehlungen LKA MV
5. KI-Themen
6. IT-Sicherheitsvorfall als Prozess
7. Zentrale Ansprechstelle Cybercrime

Vorbemerkungen

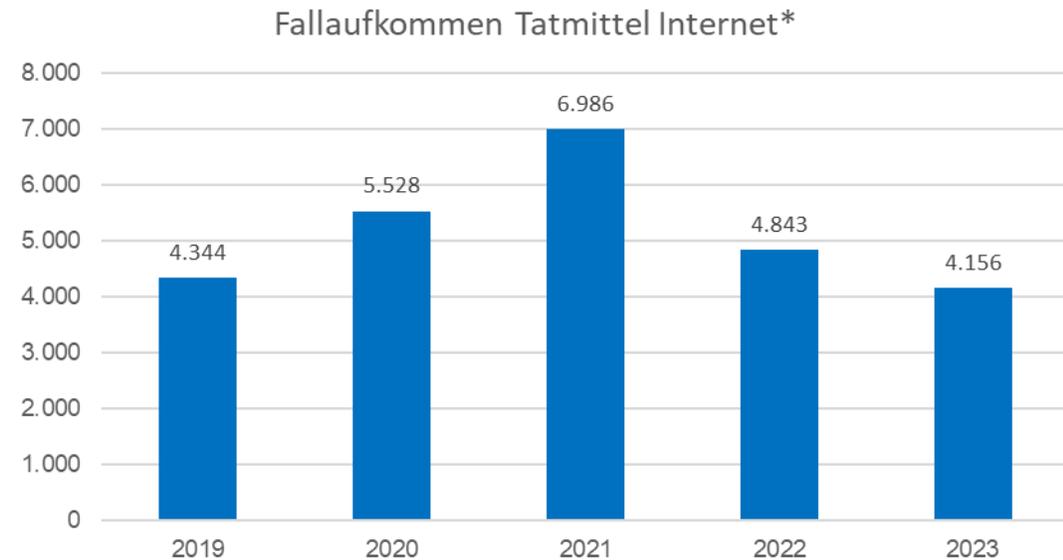
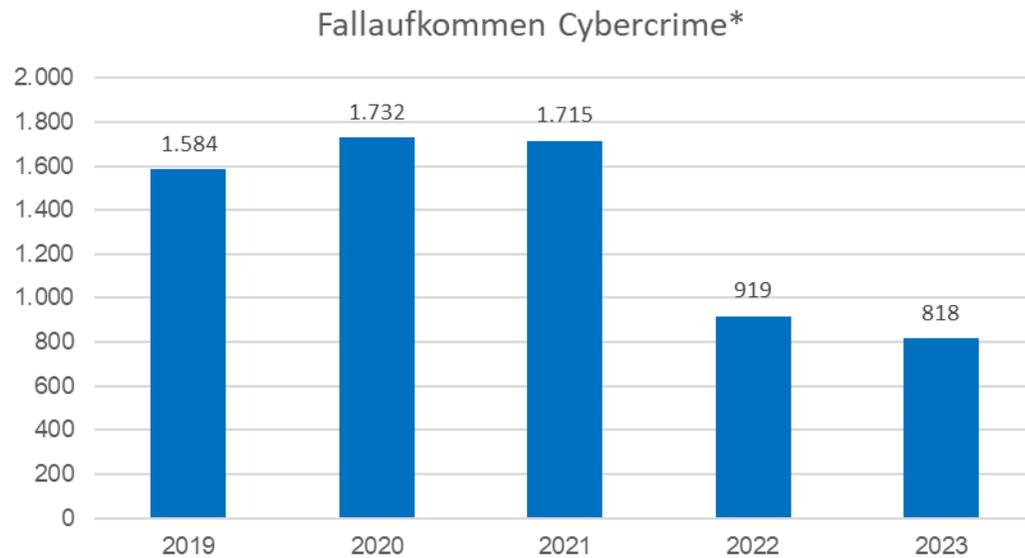
Ubiquität des Internets



- Solange Internet und E-Mails genutzt werden, sind Opfer und Hacker in einem Netz
- Cyberkriminelle passen sich flexibel an technische und gesellschaftliche Entwicklung an

2. Zahlen, Daten, Fakten Cybercrime

Zahlen, Daten und Fakten - PKS

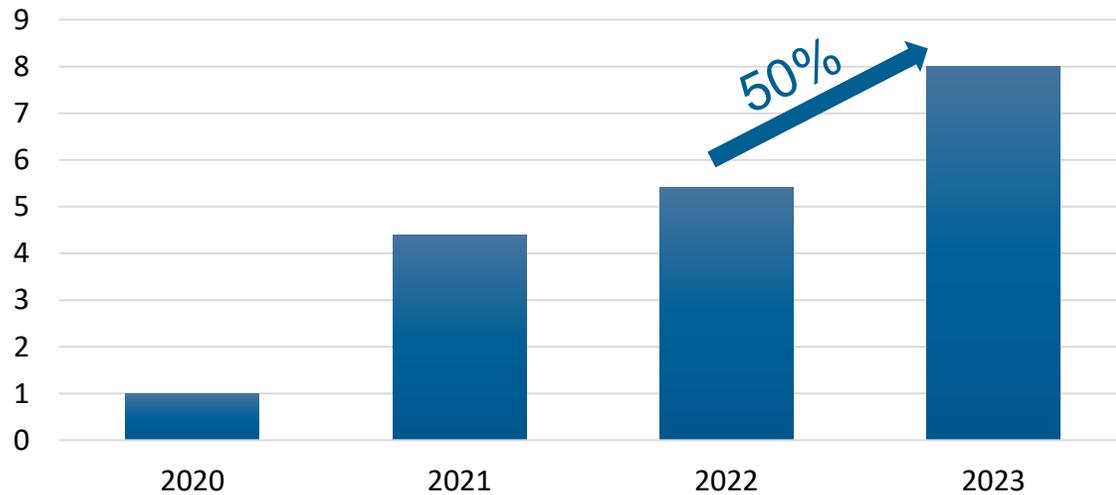


- Erfassung in PKS nur, wenn konkrete Anhaltspunkte für Tathandlung in Deutschland
- Keine Auslandsstraftaten erfasst

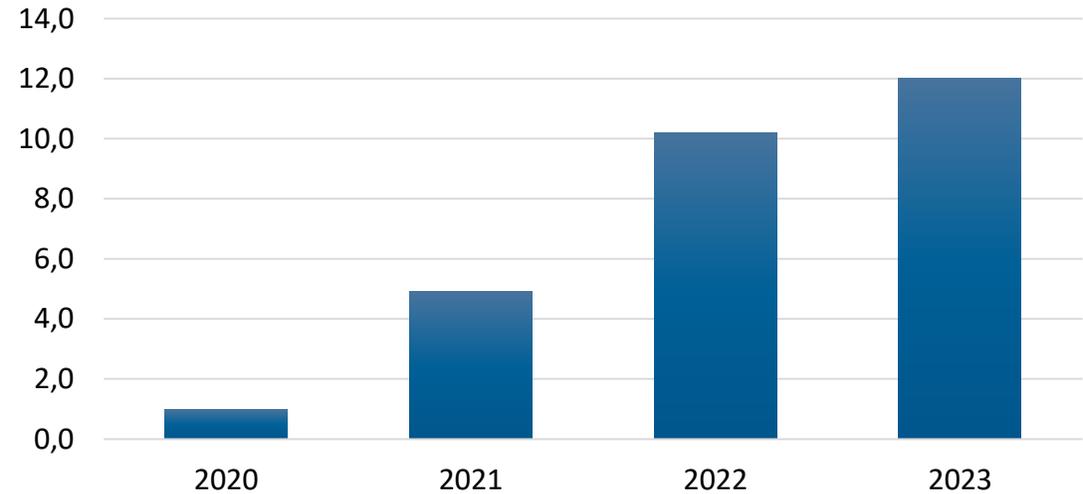
Quelle: PKS MV

Zahlen, Daten und Fakten – Cybercrime Auslandsstraf­taten in MV

Cybercrime*



Tatmittel Internet*



* Trend Auslandsstraf­taten

(Der Indexwert zeigt die Entwicklung seit der ersten Erfassung. Der Basiswert für das Jahr 2020 wurde auf eins festgelegt, die Folgejahre stehen in Relation zum Basiswert)

Quelle: Polizeiliche Kriminalstatistik MV

Lage IT-Sicherheit - Bundeslagebild Cybercrime 2023 (BKA)

- **deutlicher Anstieg Auslandsstraftaten: +28%**
- Anteil Cybercrime Inland-PKS: **2,2%**, Anteil bei Auslandsstraftaten: **26,5%**

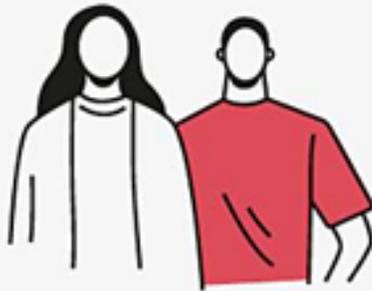
- **Deutschland überdurchschnittlich stark von Cyberattacken betroffen – Platz 4 weltweit**
- nicht wegen fehlender Sicherheitsstandards, sondern „**lukratives Angriffsziel**“
- vor allem im Bereich **Ransomware** und bei **DDoS-Angriffe**
- fast **jede Branche** betroffen

- **Täter** agieren mit **zunehmender Professionalität** und hochgradig **arbeitsteilig**
- verstärkte Anonymisierung im Netz und **komplexe Ermittlung** von im **Ausland** befindlichen Tätern
- überdurchschnittlich großes **Dunkelfeld (ca. 90%)**

Lage IT-Sicherheit – BSI Lagebericht 2023

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft



Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Wirtschaft



Ransomware
Schwachstellen, offene oder falsch konfigurierte Online-Server
IT-Supply-Chain: Abhängigkeiten und Sicherheit

Staat und Verwaltung



Ransomware
APT
Schwachstellen, offene oder falsch konfigurierte Online-Server

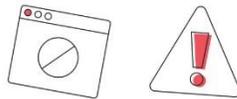
Quelle: BSI – Lagebericht zur IT-Sicherheit Deutschland

Ransomware ist weiterhin größte Bedrohung

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

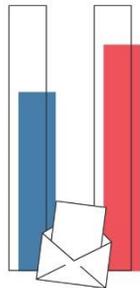


Eine Viertelmillion neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



66%

aller Spam-Mails im Berichtszeitraum waren Cyberangriffe: 34 % Erpressungsmails, 32 % Betrugsmails



84%

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erhebung von Authentisierungsdaten, meist bei Banken und Sparkassen.

Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit im Vergleich 2021 = 100

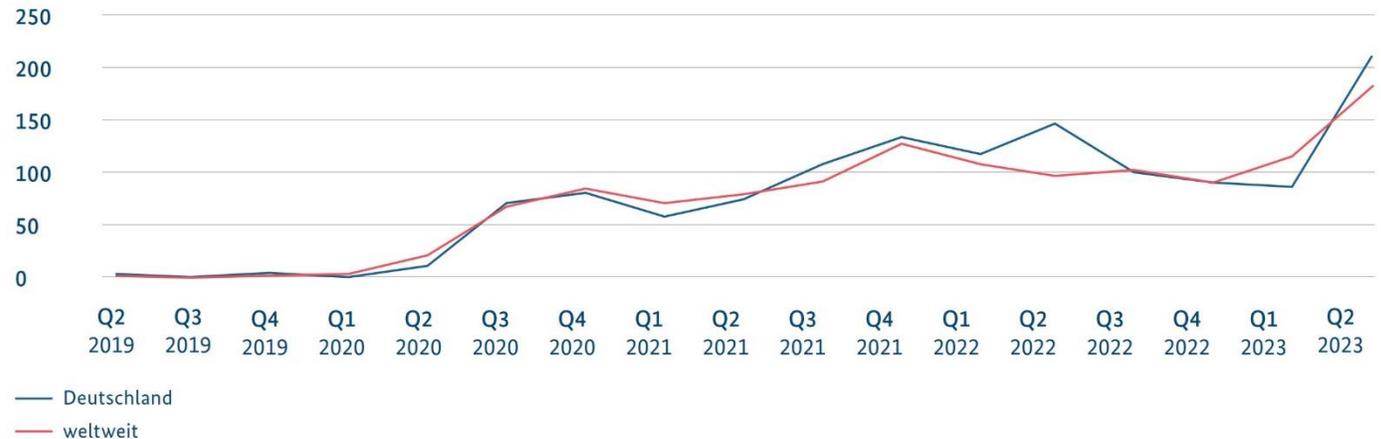


Abbildung 2: Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit im Vergleich (2021=100)
Quelle: Leak-Opfer-Statistik des BSI

Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten

Anzahl in Tausend

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



— Durchschnittlicher täglicher Zuwachs je Monat
— Täglicher Zuwachs im 12-Monatsdurchschnitt

BSI Lagebericht 2023

Umfrageergebnisse Digitalbarometer 2022



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

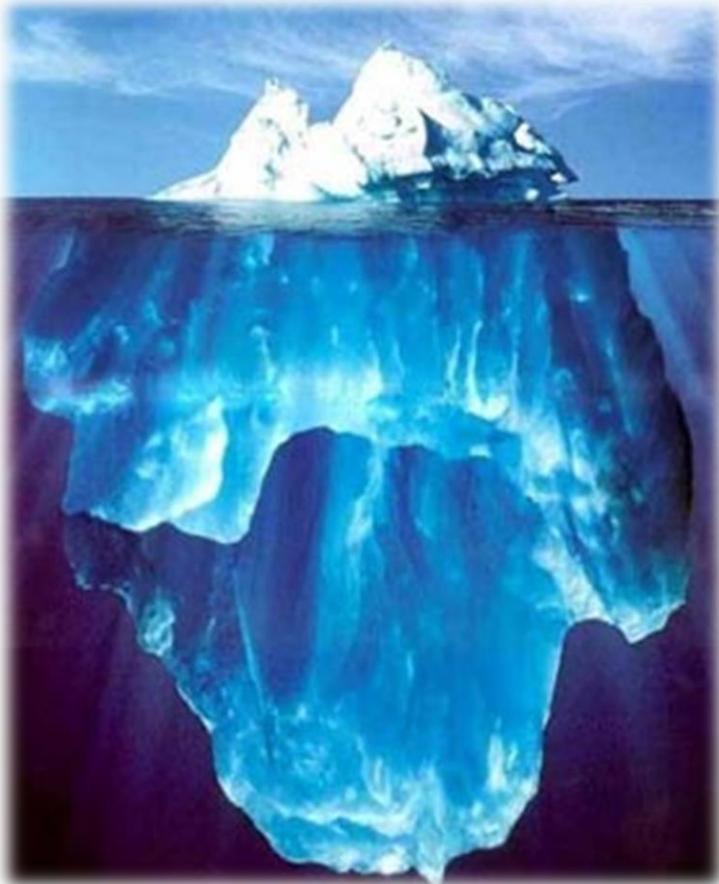
- 29% sind schon einmal Opfer von Cyber-Kriminalität geworden
- 39% erlebten Cyber-Kriminalität mindestens einmal in den vergangenen zwölf Monaten
- 62% erhielten betrügerische Phishing-Mail, ohne auf diese eingegangen zu sein

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

Lage IT-Sicherheit – Bitkom Wirtschaftsschutz 2023

- **203 Mrd. €** Cybercrime-Schäden 2022 in Deutschland - Verdopplung zu 2019
- Cyberattacken sorgen für fast **drei Viertel der Schäden** (72%, ca. 150 Mrd. €)
- 2022 waren es nur 63%
- **8 von 10** Unternehmen wurden häufiger angegriffen
- Erstmals fühlt sich die Mehrheit der Unternehmen (52%) durch Cyberattacken in ihrer **Existenz bedroht**
- Häufige Schäden durch Phishing, Passwortklau & Malware
- Täter kommen öfter aus der **organisierten Kriminalität**

Dunkelfeld Cybercrime



Dunkelfeldstudie LKA MV

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

Gründe für Nichtanzeige

Das Anzeigeaufkommen im Bereich Cybercrime ist gerade aus der Wirtschaft äußerst gering.



Mögliche Gründe:

- Straftaten werden nicht als solche erkannt
- ein **Imageverlust befürchtet** bei Anzeigenerstattung
- **Aufklärungschance** wird als **zu gering** oder erfolglos eingeschätzt
- befürchtete **negative Auswirkungen** unter **Konkurrenz-/Wettbewerbsaspekten**
- **Angst vor Strafverfahren** gegen die eigene Firma, wenn nicht lizenzierte Software genutzt oder illegale Inhalte entdeckt werden

Cybercrime-Bekämpfung

Zentrale Ansprechstellen Cybercrime (ZAC)

- Befürchtungen entgegenwirken
- Fach- und Sachkompetenz auf Seiten der Strafverfolgung
- Single Point of Contact bei den Sicherheitsbehörden
- Einrichtung von **Zentralen Ansprechstellen Cybercrime** im Bundeskriminalamt und den Landeskriminalämtern als
- **zentraler Ansprechpartner für öffentliche und nicht-öffentliche Stellen, insbesondere die Wirtschaft**



Cybercrime-Bekämpfung

Zentrale
Ansprechstelle
Cybercrime



Landeskriminalamt **M**ecklenburg-**V**orpommern



Organisation Cybercrime-Bekämpfung



¹ mit Präventionsberatern

² Wirtschaftskriminalität/Cybercrime

Cybercrime-Bekämpfung



Gemeinsame Broschüre aller
Zentralen Ansprechstellen Cybercrime
des BKA und der Polizeien der Länder:

**„Cybercrime – Handlungsempfehlungen für die
Wirtschaft in Fällen von Cybercrime“**

abrufbar auf der Homepage des BKA
<https://www.bka.de/>

[https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsb
ernetKriminalitaet/handlungsempfehlungenWirtschaft.html](https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsb
ernetKriminalitaet/handlungsempfehlungenWirtschaft.html)



3. Ausgewählte Cybercrime-Phänomene

Phänomene Cybercrime

Phishing

- über Mails oder Webseiten - Vorstufe für weitere Phänomene

Ransomware

- Online-Erpressung mittels Verschlüsselungstrojaner

CEO-Fraud

- Geschäftsführerschwindel

DDoS-Angriffe

- Distributed Denial of Service = Störung der IT-Verfügbarkeit

Datendiebstahl

- Veröffentlichung von Daten
→ mittlerweile bei Ransomware-Angriffen als Double/Triple Extortion üblich

Es gibt verschiedene Tätermotive und Angriffsformen - **gezielte** bzw. **breit gestreute** Angriffe.

Hackertypen



Scriptkiddies

- Verwenden Programme aus dem Internet (Bsp. RaaS)
- Motivation vielfältig



Whistleblower

- „Malicious Insiders“
- Ziel: Informationen offenlegen, evtl. auch Schaden anrichten



Hacktivists

- Aufdecken von Verbrechen, religiöse Ziele, etc.
- Ziel: soziale Veränderungen erreichen



Cyber-Terroristen

- religiösen oder politischen Motive
- Ziel: Angst, Schrecken und Gewalt zu verbreiten



Staatlich gesponserte Hacker

- Greifen Zivilpersonen, Unternehmen und fremde Regierungen an
- Militärische Ziele



Spammer, Dynamite Phisher, Spray and Pray

- Massenhaft und ziellos, Malware in Mailanhängen, Links oder Phishing, Nutzung von Bots
- Ziel: Geld, Werbung



Spionage-Hacker

- Stehlen Geschäftsgeheimnisse, Datenklau i.d.R durch APT
- Ziel: Erfolg fürs eigene Unternehmen



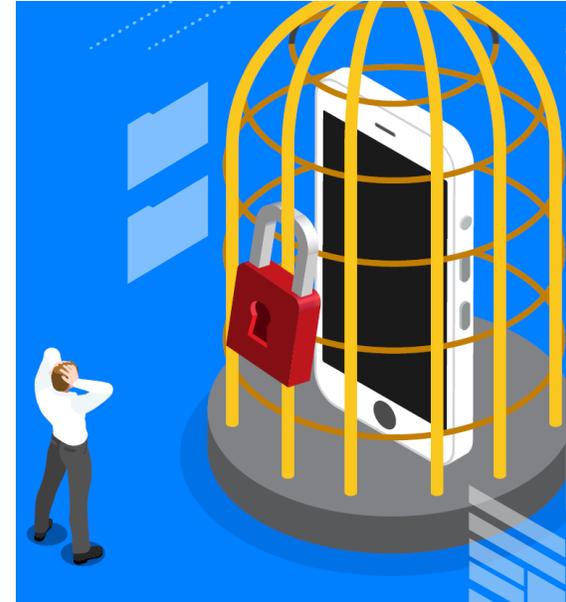
Der Infrastruktur-Hacker

- greifen Schwachstellen kritischer Infrastrukturen an
- Ziel: kritische Infrastrukturen blockieren und lahmlegen

Phänomene Cybercrime – Ransomware

Verschlüsselungstrojaner

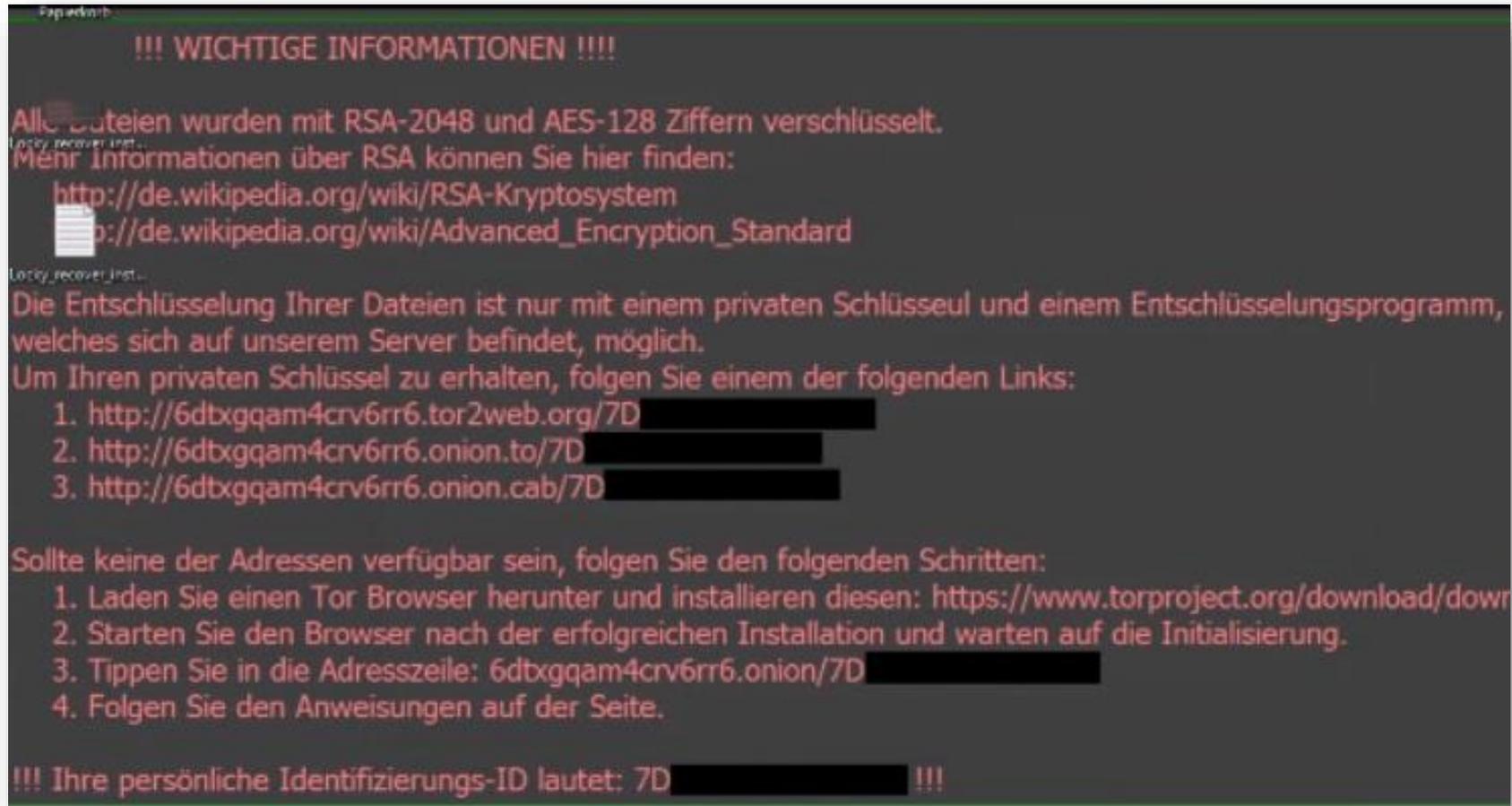
- Verbreitung durch: E-Mail, beim Surfen, Handy-Apps
- Risiken: Rechner wird gesperrt, Daten werden verschlüsselt, finanzielle Einbußen
- zur Entsperrung/Entschlüsselung wird Lösegeld (Ransom) verlangt
- in Underground-Foren werden Baukastensysteme der Schadsoftware oder Dienstleistungen zum Kauf angeboten
- Zunahme der Anzahl der Gruppierungen und die Höhe der Lösegeldsumme



Quelle: <https://www.sicherheitspartnerschaft-mv.de/downloads.html?file=files/pdf/Downloads/mobile%20Ransomware.pdf>

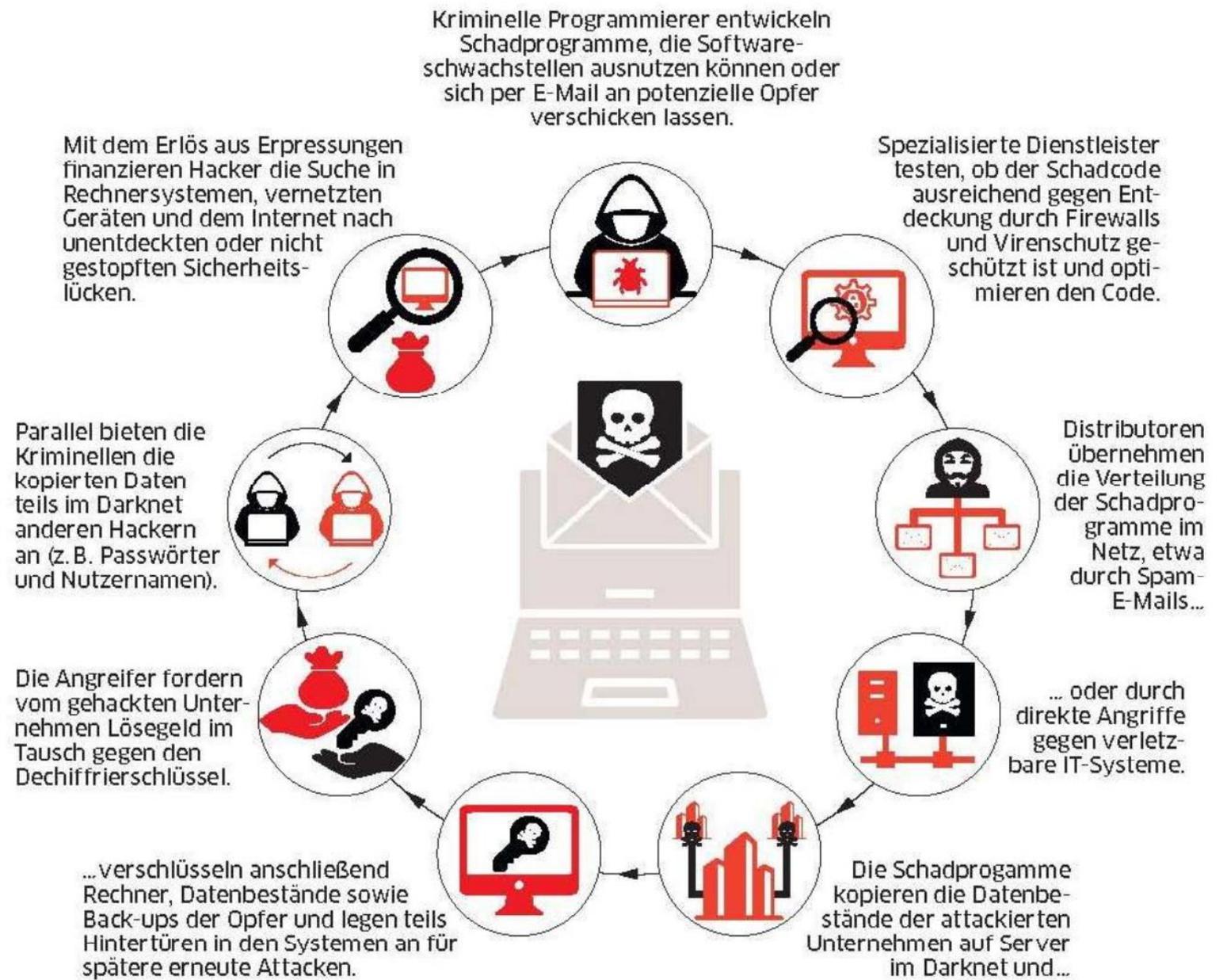
Phänomene Cybercrime – Ransomware

Lösegeldaufforderung nach Infektion



9 Säulen der Cybercrime

- Cybercrime as a Service (CaaS)
- Ransomware as a Services (RaaS)



Phänomene Cybercrime – Phishing

- Kreativität grenzenlos
- beinahe täglich neue Varianten
- phantasievoll erfundene Geschichten
- Anknüpfung an aktuellen Ereignissen, um glaubwürdig zu erscheinen
- Bonus oder Preis soll zur Eingabe persönlicher Informationen verlocken
- nach wie vor haben Phishing-Wellen vor allem Bankkunden im Visier



Zahlen und Fakten zu Emails

40 % mehr Phishing weltweit, im letzten Jahr (2023) über 34 Mio. Phishing Angriffe auf deutsche Nutzer/ Firmen

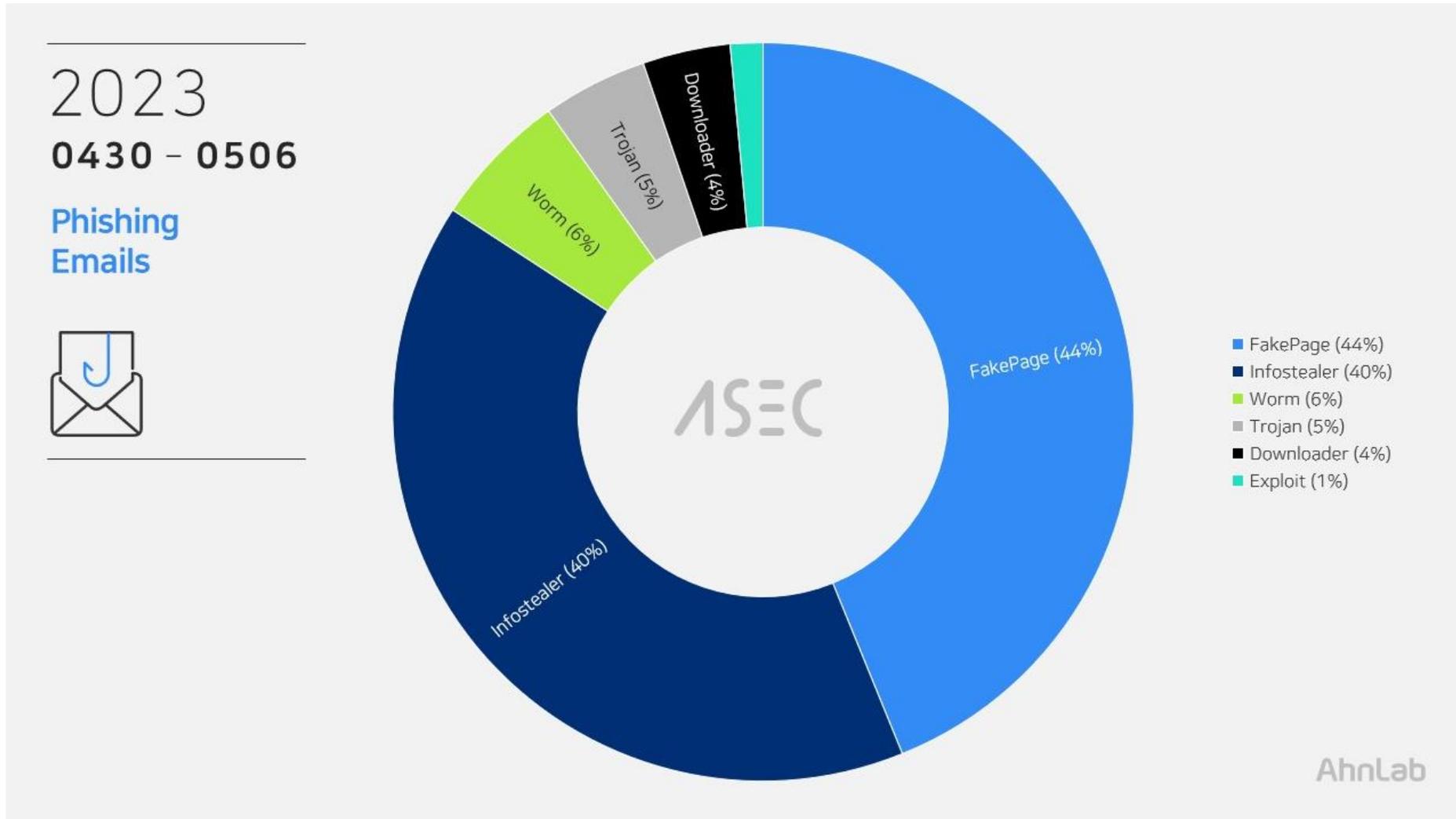
Bei **46 %** aller E-Mails weltweit handelt es sich um gefährliche Nachrichten (SPAM, Links, Inhalte, Anlagen)

88 % waren bereits Business-E-Mail-Compromise (Geschäftsführersc hwindel) ausgesetzt

100 % aller Firmen waren schon von Phishing betroffen

Quelle: https://www.kaspersky.de/about/press-releases/2024_kaspersky-report-40-prozent-mehr-phishing-weltweit

Zahlen und Fakten zu Emails



Phänomene Cybercrime – CEO Fraud



CEO-Fraud
Warnhinweis

News vom 22.01.2010

Polizei

Warnung vor Betrugsmasche „CEO-Fraud“

Die Landeskriminalämter und das Bundeskriminalamt warnen vor einer neuen Betrugsmasche: Beim CEO-Fraud geben sich Täter

21.01.2016 - Bundeskriminalamt warnt aktuell vor 'CEO-Betrug'



Das Bundeskriminalamt warnt aktuell vor laufenden internationalen Modi operandi, genannt CEO-B.

LANDESKRIMINALAMT MECKLENBURG-VORPOMMERN

LKA-MV: Warnung vor neuer Betrugsform - Geschäftsführer-Schwindel

25.09.2015 – 14:38

Phänomene Cybercrime – CEO Fraud

<https://sosafe-awareness.com/de/glossar/ceo-fraud/>

The image shows an email interface with several red callouts highlighting suspicious elements:

- 1 Falsche E-Mail-Adresse:** Points to the sender's email address, alexandrra43@gmail.com.
- 2 Außerhalb der Geschäftszeiten:** Points to the timestamp, 3. August 2023, 21:20.
- 3 Rechtschreibfehler:** Points to the word 'gespert' in the first paragraph.
- 4 Überweisungsanfrage:** Points to the phrase 'überweisen' in the first paragraph.
- 5 Dringlichkeit:** Points to the phrase 'Wir müssen uns beeilen' in the second paragraph.
- 6 Vertraulichkeit:** Points to the phrase 'vertraulichen Inhalts' in the second paragraph.
- 7 Ungewöhnlicher Kommunikationsstil:** Points to the closing 'Auf Wiedersehen'.

Header: Alexandra Schmidt <alexandrra43@gmail.com>
Dringend: Wichtige Geschäftsmöglichkeit
An: daniel@quantumlynx.com

Body:
Hallo Daniel,

hier ist Alexandra, dein CEO. Ich wurde bei meinem Geschäftskonto gespert, weshalb ich dich von meiner persönlichen E-Mail aus in einer sehr wichtigen Angelegenheit kontaktiere. Es gibt eine dringliche Geschäftsmöglichkeit, die sich ergeben hatte, und ich brauche dich, um 20.000 € bis zum Ende des Tages auf dieses Konto zu überweisen.

Die Details sind wie folgt:
• Kontonummer: 1234567890
• Bankleitzahl: 987654321
• Bank: GlobalBank

Bitte behandle diese Angelegenheit mit höchster Priorität. Wir müssen uns beeilen, also wäre ich dir dankbar, wenn du das sofort erledigen könntest. Aufgrund des vertraulichen Inhalts dieser Transaktion möchte ich dich bitten, diese Angelegenheit vorerst unter uns zu behalten.

Auf Wiedersehen
Alexandra
CEO von Quantumlynx

5. Handlungsempfehlungen des LKA MV

Aktuelle Schwachstellen



Sicherheitsforscher des amerikanisch-israelischen IT-Sicherheitskonzerns **Check Point Research** haben eine als kritisch eingestufte Sicherheitslücke mit der Bezeichnung **CVE-2024-21413** in Microsoft Outlook entdeckt. Die Schwachstelle ist sowohl gefährlich als auch einfach auszunutzen, wird aber erfreulicherweise bereits mit den jetzt verfügbaren Sicherheitsupdates für Februar 2024 geschlossen.

Die Schwachstelle ermöglicht es einem Angreifer, die geschützte Office-Ansicht zu umgehen und das Dokument im Bearbeitungsmodus statt im geschützten Modus zu öffnen. Auch das Vorschaufenster für E-Mails in Microsoft Outlook reicht als Angriffsvektor aus. Nutzt ein Angreifer die Schwachstelle erfolgreich aus, kann er Privilegien wie Lese-, Schreib- und Löschrchte freischalten.



Sicherheitslücken: Angreifer können Juniper-Netzwerkgeräte lahmlegen

Da die Auflistung der bedrohten Geräte der Firewall-Serie SRX, der Switch-Reihen EX/QFX und die MX-Router-Serie den Rahmen dieser Meldung sprengen würde, finden Admins diese Informationen in den unterhalb dieser Meldung verlinkten **Warmmeldungen...**

12.04.2024 | Security

Die xz-Hintertür: Das verborgene Oster-Drama der IT

Mit einer Hintertür in einer unbekanntem Kompressionsbibliothek hätten Unbekannte beinahe große Teile des Internets übernehmen können. Leider kein Scherz.



(Bild: BeeBright / Shutterstock.com)

02.04.2024, 17:10 Uhr | Leszeit: 8 Min. | Security
Von Jürgen Schmidt



Phishing-Warnung vor betrügerischen ELSTER-Mails
Das Thüringer Finanzministerium warnt vor einer Phishing-Welle mit ELSTER-Bezug. Die Betrüger haben es auf Kontoinformationen abgesehen.
23. August 2024, 13:26 Uhr | 13



ALERT Sicherheitslücken
Codeschmuggel-Lücke in diversen HP Laser-Druckern
HP warnt mit gleich zwei Sicherheitsmeldungen vor Lücken in diversen Laserjet-Druckern. Firmwareupdates sollen sie schließen.



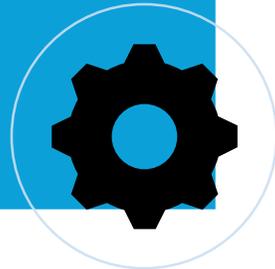
Webbrowser: Weitere Lücke aktiv ausgenutzt, Adobe PDF-Viewer aktualisiert
Google meldet das Ausnutzen einer weiteren Lücke in freier Wildbahn. Die Updates von Edge schließen auch ein Leck im Adobe PDF Viewer.
heute, 08:57 Uhr | 3 | 27.08.2024

Handlungsempfehlungen

- Patch-Management
- Segmentierung der IT-Netze und Firewalls
- Backups (aber richtig !)

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

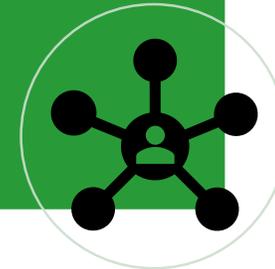
Technische
Sicherheit



- 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!**

Handlungsempfehlungen

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

- **IT-Sicherheit ist Chefsache**
- 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**

Handlungsempfehlungen - E-Mail-Sicherheit

→ Schutz vor Spoofing, Phishing und Fälschung

SPF = Absenderadress-Fälschungen vermeiden

- Festlegung, welche Server im Namen der Domäne E-Mails versenden dürfen. Empfänger prüft Versandberechtigung des Absenders und kann so die E-Mails ablehnen.

DKIM = Sender-Authentifizierung

- Beim Empfang der E-Mail wird mittels Signatur erkannt, ob es sich um den korrekten Absender handelt und ob die E-Mail manipuliert wurde.

DMARC = Kontrollsystem

- Kontrollsystem mit Regelwerk, das über SPF und DKIM hinaus geht. Bsp. Reaktionen auf abgelehnte E-Mails sowie aktives Berichtswesen

Mail Sicherheit - Fazit

Warum sollten Sie SPF, DKIM und DMARC verwenden?

Die Authentifizierungsmethoden SPF und DKIM zählen zu den Schlüsselpunkten zur Optimierung Ihrer Zustellbarkeit und hat sich zum Standard in der E-Mail-Welt entwickelt. Aber das ist nicht der einzige Vorteil.

Tatsächlich verbessert die Implementierung dieser Protokolle die Zustellbarkeit von E-Mails. Dank dieser Methoden werden IHRE E-Mails besser von ISPs (Internet Service Providern) und den E-Mail-Clients Ihrer Empfänger identifiziert.

Diese Protokolle dienen zur Überprüfung der Identität von Absendern und zählen zu den effektivsten Möglichkeiten, um zu verhindern, dass Phisher (Betrügerische E-Mails mit dem Ziel sensible Daten wie Kundenlogin, Bankverbindungen etc. zu erbeuten) und andere Betrüger sich als legitimer Absender ausgeben, dessen Identität sie unter demselben Domainnamen angeben könnten.

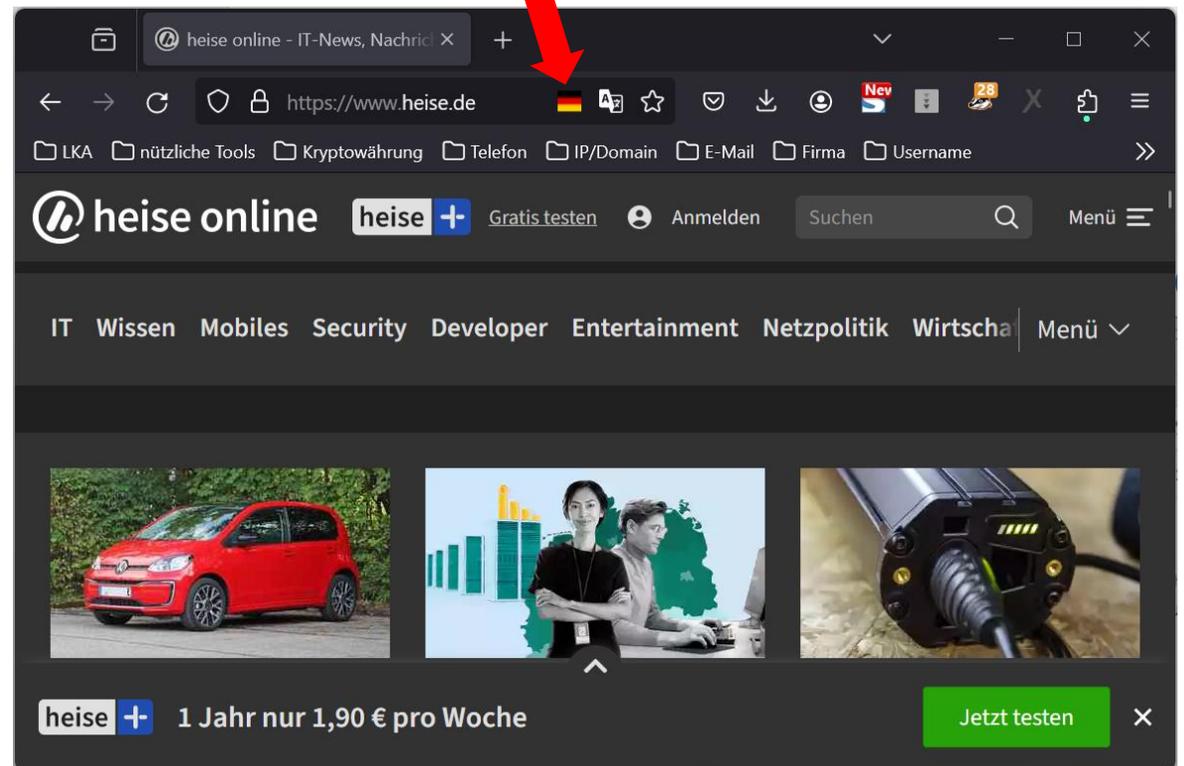
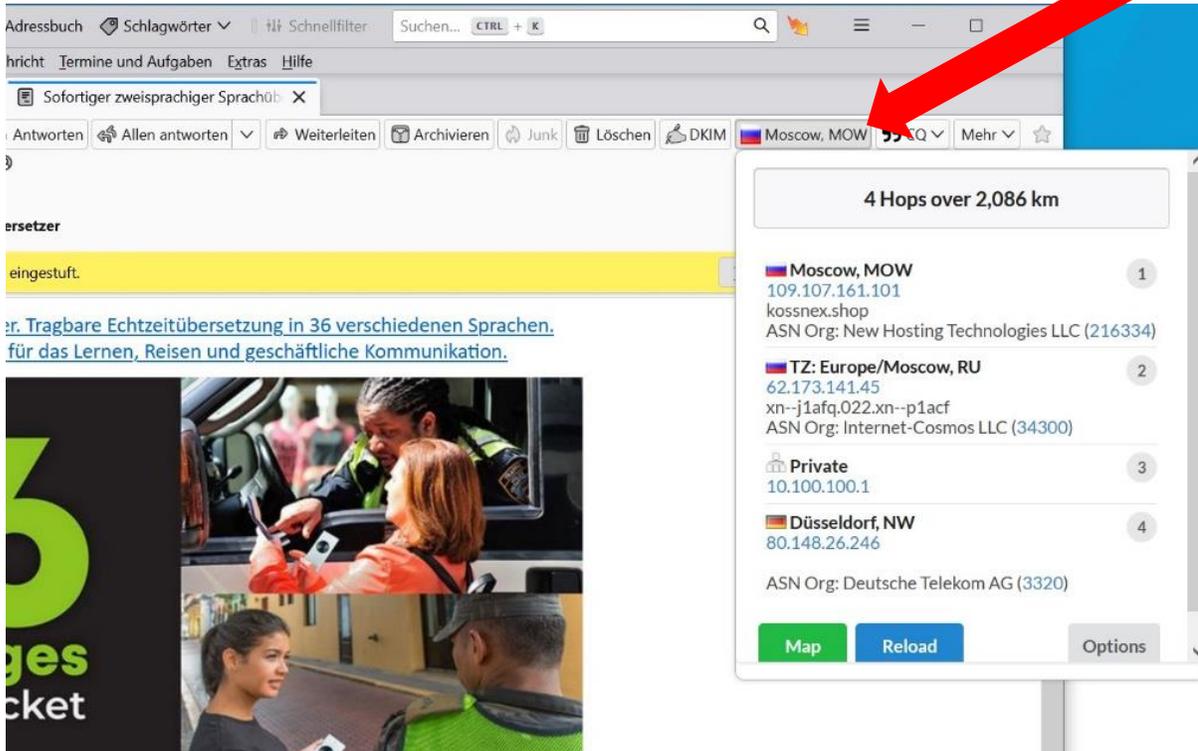
Handlungsempfehlungen - E-Mail-Sicherheit

→ Schutz vor Spoofing, Phishing und Fälschung mit Addons

The screenshot shows the Thunderbird Add-ons website interface. At the top, there are links for "Neu registrieren" and "oder anmelden", and a section for "Andere Anwendungen". The main header features the "Add-ons" logo and navigation tabs for "ERWEITERUNGEN", "THEMES", "SAMMLUNGEN", and "MEHR...". A search bar is located on the right with the placeholder text "Suche nach Add-ons". A welcome message reads: "Willkommen bei den Thunderbird-Add-ons. Fügen Sie Zusatzfunktionen und Stile hinzu, um sich Thunderbird zu Eigen zu machen." Below this, the "MailHops" extension is featured. It has a red location pin icon with an '@' symbol, a version number of 4.4.0, and is by Andrew Van Tassel. The description states: "MailHops maps the route an email took to get to you. Displaying the senders location, weather, user-agent and authentication used." To the right of the description, it shows a 4.5-star rating, 38 user reviews, and 2,429 users. A green button labeled "+ jetzt herunterladen" and a link for "Datenschutzerklärung" are provided. Below the extension card, it notes "Kompatibel mit Thunderbird 112.0 - *" and a link to "Andere Versionen ansehen". At the bottom, three preview images show the extension's interface: a list of hops, a map of the United States, and a data table with a bar chart. A blue double arrow points to the right.

Handlungsempfehlungen - E-Mail-Sicherheit

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



Handlungsempfehlungen - Passwortsicherheit

Für Anwender:

- **Passwortmanager**, ggf. in Kombination mit Passphrase
- **lange** (mind. 8 Zeichen, je länger desto besser), durch PW-Manager zufällig generierte PW
- **1 PW pro Dienst**, keine Wiederverwendung
- wichtige Dienste (z.B. Banking und E-Mail-Account [wg. PW-vergessen-Funktion] und den Manager selbst) mit 2. Faktor absichern (**2FA**)

Für Dienstanbieter:

- KEINE Änderung erzwingen, außer bei Kompromittierungsverdacht
- keine strengen Regeln bzgl. Komplexität
- lediglich automatisierter Abgleich des gewählten PWs mit Leaks/Breaches
- geeignetes Hash-Verfahren mit Salt verwenden zum Speichern der PWs
- 2FA anbieten

Quellen:

Paper des NIST aus 2020: <https://pages.nist.gov/800-63-3/sp800-63-3.html>

Video als Kurzzusammenfassung: <https://www.nist.gov/video/password-guidance-nist-0>

Heise-Beitrag: <https://www.heise.de/news/Weisenrat-fuer-Cyber-Sicherheit-gegen-strenge-Regeln-fuer-Passwoerter-4793420.html>

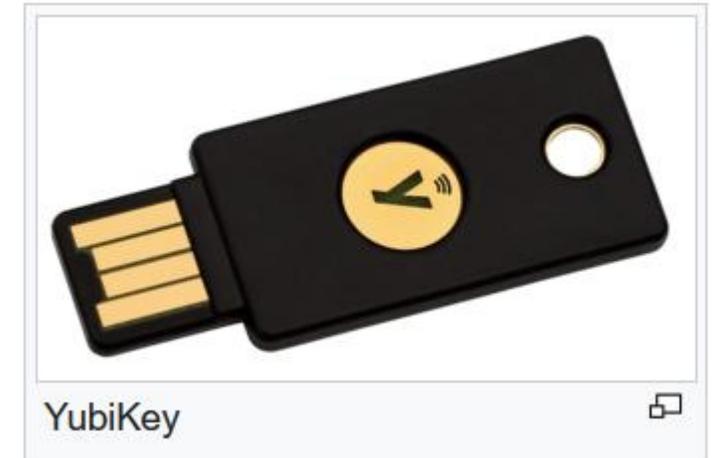
Handlungsempfehlungen

Wichtig: Es gibt nicht nur den einen Tipp.

- 2FA oder MFA z.B. mit Hardware-Token (z.B. YubiKey)

Technische Spezifikationen

Anschluss	USB-A
NFC	Ja
Authentifizierungsmethoden	Starke Zwei-Faktor-Authentifizierung (2FA), starke Multi-Faktor-Authentifizierung (MFA), passwortlos
Design & Haltbarkeit	Wasserfest, stoßfest, keine Batterien erforderlich, keine beweglichen Teile
Gerätetyp	FIDO HID -Gerät, CCID -Smart Card, HID -Tastatur
Herstellung	Hergestellt in Schweden und den USA



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.



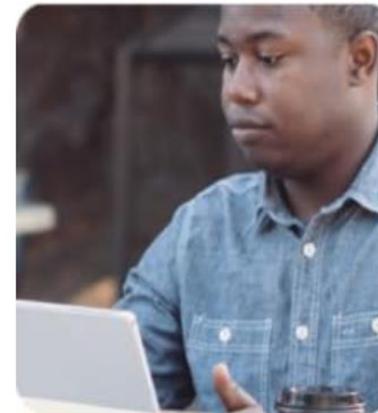
Gesundheitswesen

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.



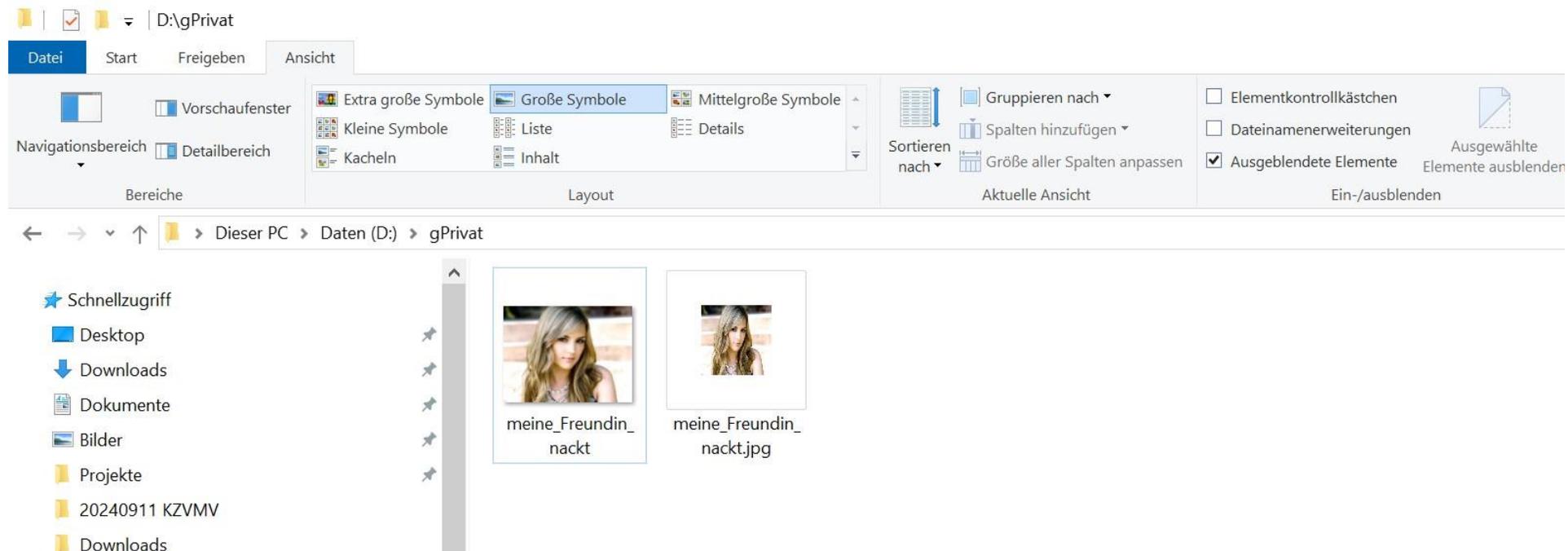
Energie

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



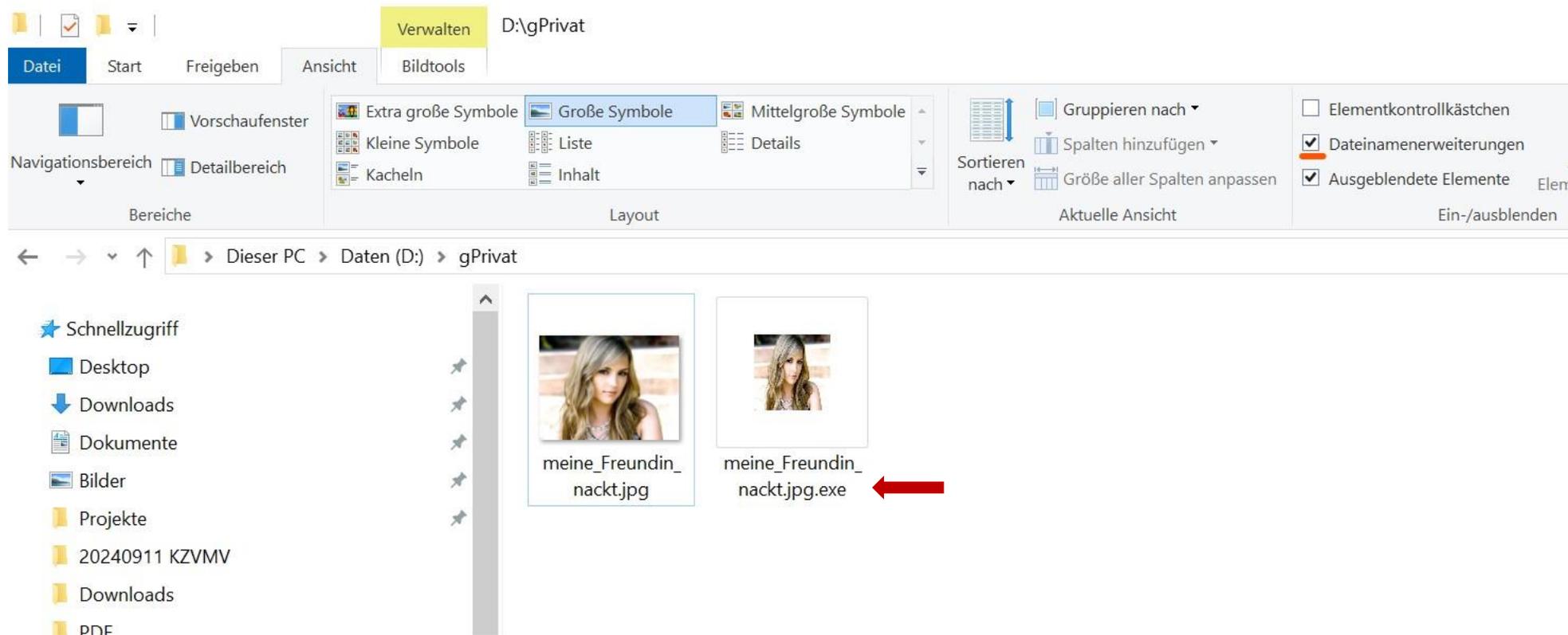
Handlungsempfehlungen

Windows Explorer – Anzeige der Dateierweiterungen
(Extension) einschalten !



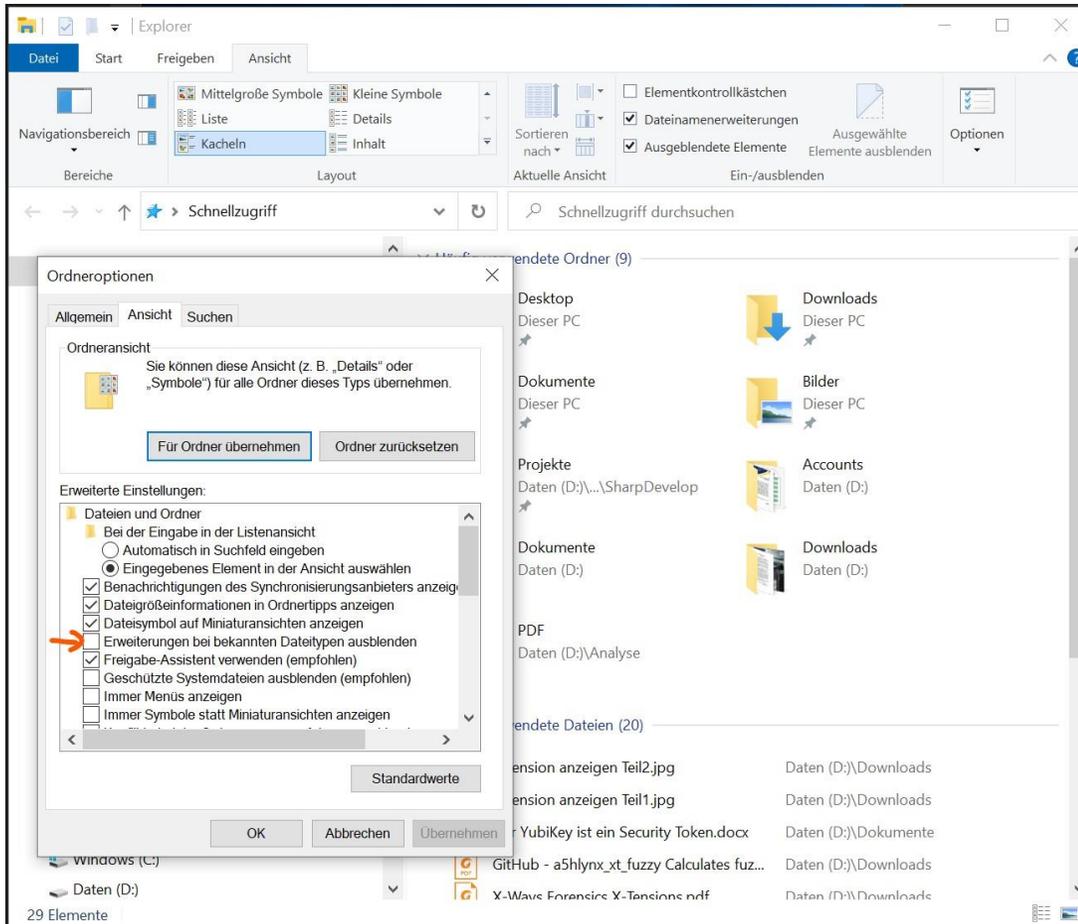
Handlungsempfehlungen

Windows Explorer – Anzeige der Dateierweiterungen
(Extension) einschalten !

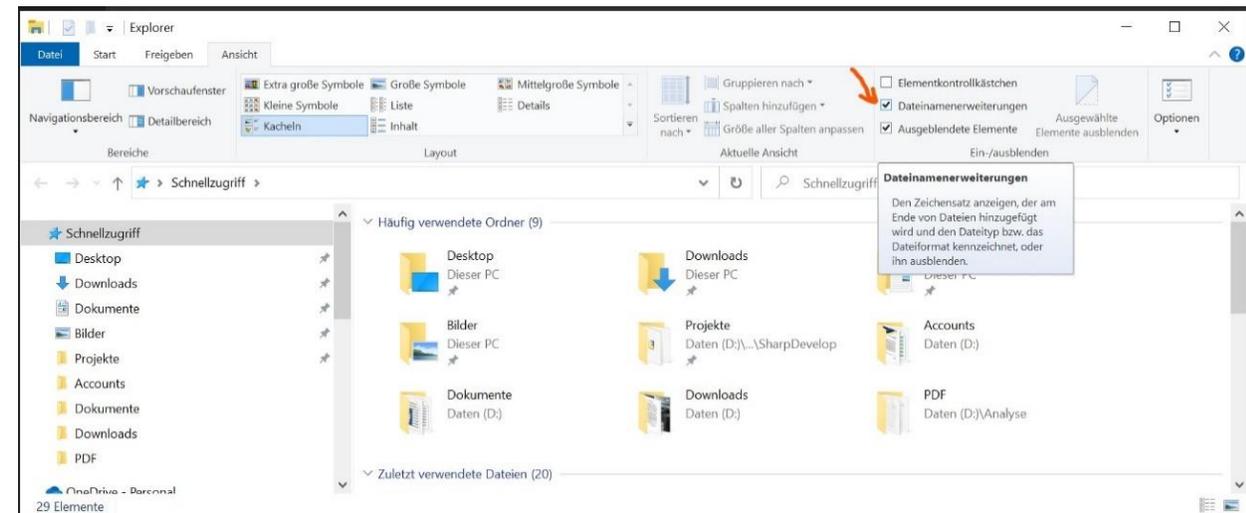


Handlungsempfehlungen

Windows Explorer – Anzeige der Dateierweiterungen (Extension) einschalten !



Oder alternativ so ...



Handlungsempfehlungen

Unterstützung und Informationen beim BSI einholen

Kleine- und Mittlere Unternehmen

Informationen und Hilfestellungen für KMU

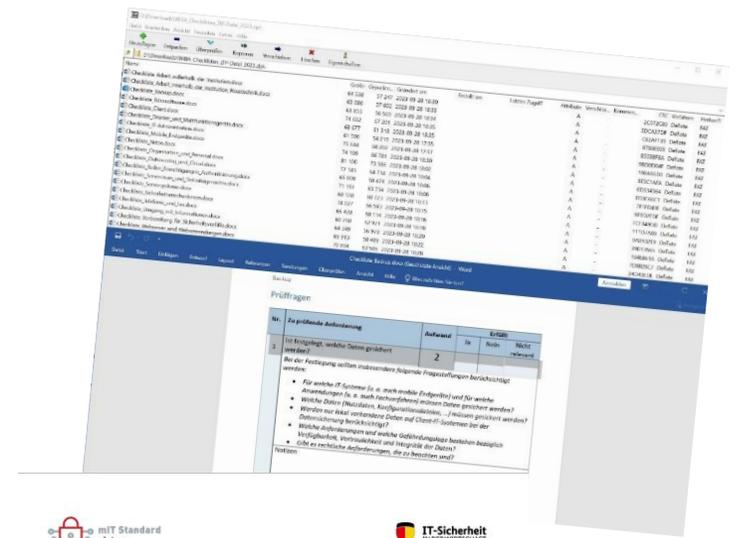
Kleine und mittlere Unternehmen (KMU) werden zunehmend Ziel von Cyber-Attacken. Nicht selten führen diese zu immensen Schäden und schwächen die Unternehmensreputation. Oftmals werden Daten von Kunden und Kooperationspartnern sowie andere sensible Daten abgegriffen, verändert, gelöscht, verschlüsselt 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.

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



NEU!

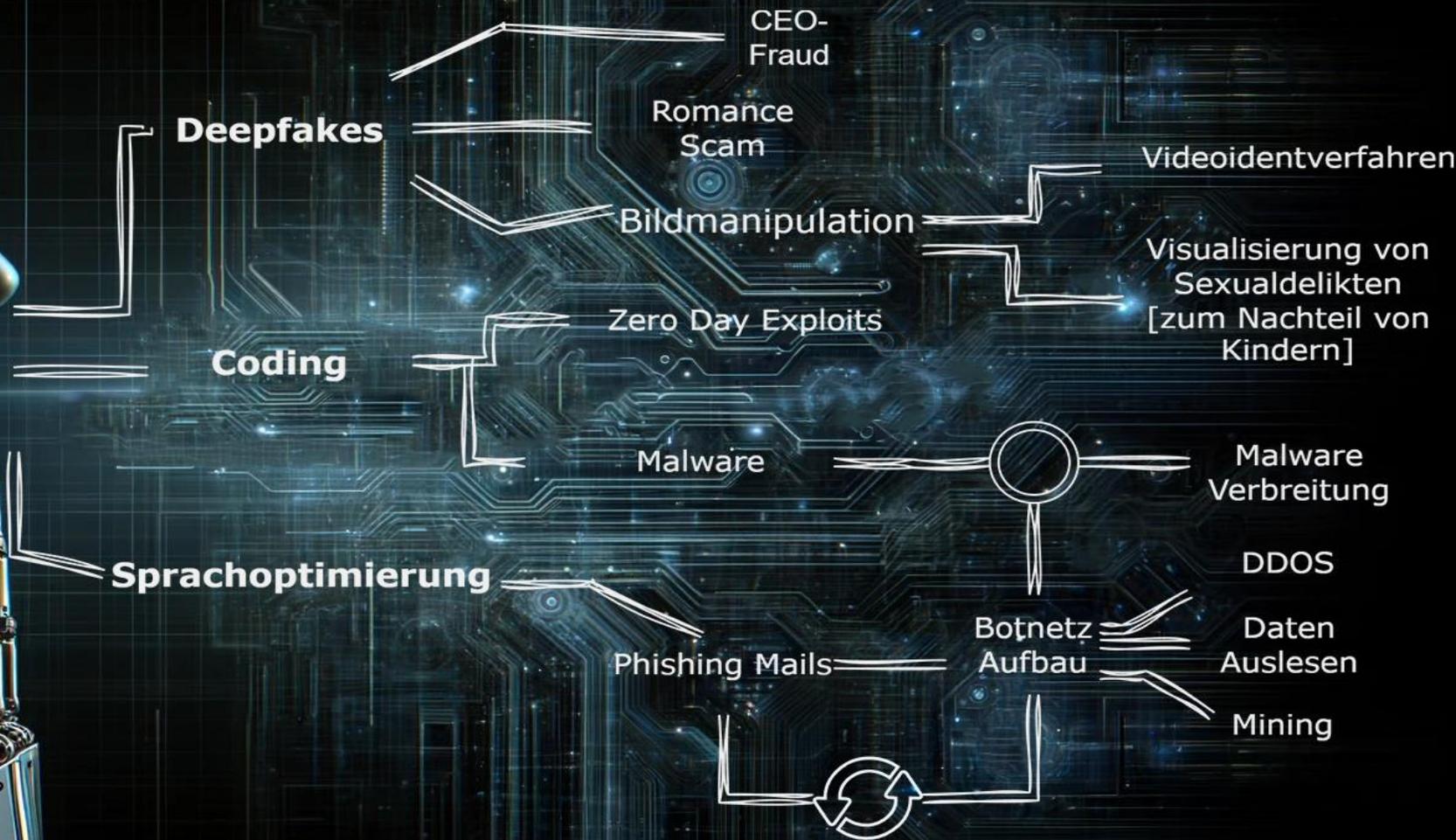


www.mit-standard-sicher.de



4. KI-Themen

Gefahren KI – das kommt auf uns zu ...



Videos / Beispiele

1. Zuschnitt der ersten 3 Videos
2. Video John Finger (Übersetzung)
3. ZDF Sprecher Sievers (Fake)
4. Olaf Scholz verbietet die AfD
5. Hygen: Maik mehrsprachig
6. Hygen: Theresa KI Warnung (Video Avatar)



Webseite – Das kann jeder ...

HeyGen Labs → Go to HeyGen

Video Translate BETA

Translate your videos seamlessly with one click, using a natural voice clone and authentic speaking style!

Drop to Upload

File type: mp4, quicktime, webm
Video duration up to 5 min, file size up to 500 MB

① Requirements

Choose a target language: Voice powered by **11ElevenLabs**

Translate Audio Only

Submit

Results (1) (Total 76.127+ videos processing now. [Upgrade](#) to skip the line)

Translated Video Demo

Quelle: <https://labs.heygen.com/guest/video-translate>

Gefahren – das kommt auf uns zu ...

- Neue gezieltere Art von **Social-Engineering** und **Phishing** (Sprachanrufe, Sprachnachrichten, Video-Calls), höhere Gefahr von CEO- Fraud
 - Mit falscher Werbung auf Webseiten locken, dort Malware platzieren oder zu „finanziellen Fehlritten“ (Betrug) verleiten lassen
 - Bereits bekannte Angriffsszenarien treten als Massenphänomen auf
- Für alle Beteiligten wird es immer schwerer fallen Original und Fake auseinander zu halten

Gefahren – das kommt auf uns zu ...

Beispiele:

Versicherungsunternehmen Euler Hermes hat den ersten Schadensfall mit Künstlicher Intelligenz (KI) mit Stimmimitations-Software dokumentiert. Laut dem Betrugsexperten bei Euler Hermes gab es zuerst einen **Anruf des vermeintlichen CEO der Firma** beim Chef der britischen Tochter mit der Bitte um eine dringende Überweisung. Dieser hatte sich zwar etwas gewundert, da er die **Stimme aber erkannte**, hat er den Auftrag trotzdem ausgeführt. Er hat **220.000 € auf ein Konto in Ungarn überwiesen**. Das gesamte Geld war weg.

Hongkong 04.02.2024 - Ein Angestellter **überwies 23 Millionen Euro an Betrüger**, die sich mithilfe von Deepfakes in einer Videokonferenz als seine Vorgesetzten ausgegeben haben. Der Angestellte erhielt eine **Nachricht über eine dringende, vertrauliche Transaktion, die angeblich vom Finanzchef** seiner Firma in Großbritannien stammte. Obwohl er zunächst skeptisch war, verflüchtigten sich seine Zweifel nach einem **Videoanruf, an dem scheinbar vertraute Kollegen teilnahmen**.

Gefahren – das kommt auf uns zu ...

Beispiele:

Taylor Swift als abschreckendes Beispiel für Deepfakes

Die US-Politik wurde durch die mithilfe von KI-Technik generierten pornografischen Bilder von Taylor Swift, die auf X (Twitter) verbreitet wurden, aufgerüttelt. Es mehren sich Stimmen, die ein härteres Vorgehen gegen Deepfakes fordern. Die Verbreitung der Bilder sorgte für Empörung bis in die US-Regierung hinein.

(Quelle: <https://www.golem.de/news/deepfake-ki-generierte-pornobilder-von-taylor-swift-schockieren-fans-2401-181530.html>)

„Hören sie zu. Ich habe ihre Tochter“, mit diesen Worten meldete sich am 20. Januar 2023 ein vermeintlicher Entführer bei der US-Amerikanerin Jennifer DeStefano. Laut einem CNN-Bericht hörte die Mutter im Verlauf des Gesprächs die Stimme ihrer weinenden Tochter im Hintergrund. Nur: Der 15-Jährigen ging es gut. Was die Mutter hörte, war ein per Deepfake-Technologie erstelltes Abbild der Stimme ihrer Tochter. Laut dem FBI nehmen Kriminelle in den USA im Schnitt 11.000 US-Dollar mit jeder getürkten Entführung ein.

Wie kann man sich davor schützen?

- **Fakt:** Technik/Software immer besser - Erkennung immer schwerer
(Quelle: Studie CISP, Ruhr-Uni Bochum, Leibniz Uni Hannover, TU Berlin)
→ Seien sie **wachsam** und **skeptisch!**
- Finanzen = **klare Anweisungen** bei Transaktionssummen
→ 3. Instanz zur Absicherung,
→ Rückruf Geschäftsführers (alternatives Telefon/E-Mail-Adresse)
- Vereinbarung von **Codewörtern**, sodass Manipulationen/Fakes abgeblockt bzw. erkannt werden
- Visuelle **Alleinstellungsmerkmale** zur Identifizierung der Person (bei Echtzeitkommunikation)
→ eindeutige Gegenstände, Uhren, Schmuck etc. zeigen lassen
- **Content Awareness:** Welche Informationen werden öffentlich bekannt gegeben?
→ Firmen-Webseite, Soziale Netzwerke

6. IT-Sicherheitsvorfall als Prozess

IT- Sicherheitsvorfall: Phasen

IT-Sicherheitsvorfall (Phasen und Hilfspunkte)

1. Vorbereitung auf einen Vorfall
2. Identifizierung des Vorfalls/Sachverhalts
3. Eindämmungsphase (Ausbreitung verhindern)
4. Beseitigung/Bereinigung
5. Wiederherstellung/Inbetriebnahme der Systeme
6. „Lessons Learned“ - Erkenntnisse



IT- Sicherheitsvorfall

1. Vorbereitung auf einen Vorfall

Ihre **Checkliste** für die Reaktion auf Vorfälle in der Vorbereitungsphase:

- ✓ Haben Sie Sicherheitsrichtlinien für Ihr Unternehmen entwickelt?
- ✓ Wenn ja, kennen die Mitarbeiter diese Richtlinien und kann das Sicherheitsteam sie durchsetzen?
- ✓ Wie lautet die organisatorische Definition eines Sicherheitsvorfalls?
- ✓ Verfügen Sie über ein Verfahren zur Priorisierung und Dokumentation von Sicherheitsvorfällen?
- ✓ Wer ist für die einzelnen Phasen der Reaktion auf Sicherheitsvorfälle verantwortlich (Identifizierung, Eindämmung, Beseitigung, Wiederherstellung und Erfahrungen)?

IT- Sicherheitsvorfall

Verfügt das Incident Responder (IR)-Team über alle Werkzeuge und einen "Einsatzkoffer", die zur Bewältigung von Zwischenfällen erforderlich sind?

- ✓ Ein Incident Responder-Tagebuch (Protokollierung der Vorfälle und Tätigkeiten)
- ✓ Eine Kontaktliste mit allen Mitgliedern des IR-Teams
- ✓ USB-Laufwerke (USB-Sticks, mobile Festplatten zur temporären Datenablage)
- ✓ Ein bootfähiges USB-Laufwerk oder eine Boot- CD für Wiederherstellung und Reparatur (inkl. Antivirus Prüfung)
- ✓ Ein Laptop o. ä. Gerät zur Durchführung forensischer Untersuchungen
- ✓ Dienstprogramme für Endpunktschutz und Anti-Malware-Software
- ✓ Netzwerk- und andere Toolkits zum Hinzufügen/Entfernen von Komponenten

IT- Sicherheitsvorfall

Festlegungen

- ✓ Wer kommuniziert wichtige Aktualisierungen im Zusammenhang mit dem Vorfall?
- ✓ Wer entscheidet über die Einschaltung der Strafverfolgungsbehörden?
- ✓ Wer arbeitet mit den Strafverfolgungsbehörden zusammen?
- ✓ Wer bringt die Systeme im Falle einer schwerwiegenden Datenpanne wieder online?

IT- Sicherheitsvorfall

2. Vorfall - Identifizierung des Sachverhalts

Ihr Sicherheitsteam muss alle Details des Vorfalls gründlich untersuchen und aufzeichnen (protokollieren)

Folgende **Checkliste** enthält einige Fragen, die während der Identifizierungsphase verwendet werden können:

- ✓ Wer hat den Vorfall entdeckt oder gemeldet?
- ✓ Wann wurde der Vorfall entdeckt oder gemeldet?
- ✓ Wo wurde der Vorfall entdeckt oder festgestellt?
- ✓ Welche Auswirkungen hat der Vorfall auf den Geschäftsbetrieb?
- ✓ Welches Ausmaß hat der Vorfall in Bezug auf das Netzwerk und die Anwendungen?
- ✓ Ersten Informationspflichten nachkommen! (Firmenvorstände, Behörden, ...)

IT- Sicherheitsvorfall

3. Eindämmungsphase (Ausbreitung verhindern)

Weiteren Schaden vermeiden, Daten sichern

Fragen:

- ✓ Kann der Vorfall isoliert werden?
- ✓ Sind die betroffenen Systeme von nicht betroffenen Systemen isoliert?
- ✓ Wurden Backups erstellt, um wichtige Daten zu schützen und sind sie nutzbar?
- ✓ Wurden Kopien der infizierten Rechner für die forensische Analyse erstellt?
- ✓ Wurden alle Malware und andere Bedrohungen von den infizierten Systemen entfernt?

IT- Sicherheitsvorfall

4. Beseitigung/Bereinigung

Dauerhafte Lösung für infizierte Systeme

Checkliste, die Sie in dieser Phase durchgehen sollten:

- ✓ Wurden die infizierten Systeme mit neuen Patches abgesichert?
- ✓ Müssen irgendwelche Systeme oder Anwendungen neu konfiguriert werden?
- ✓ Wurden alle möglichen Einfallstore überprüft und geschlossen?
- ✓ Wurden alle Prozesse zur Beseitigung der Bedrohung(en) abgedeckt?
- ✓ Sind zusätzliche Verteidigungsmaßnahmen erforderlich, um die Ausrottung der Bedrohung(en) zu unterstützen?
- ✓ Wurden alle böartigen Aktivitäten auf den betroffenen Systemen beseitigt?

IT- Sicherheitsvorfall

5. Wiederherstellung/Inbetriebnahme der Systeme

Nach Abschluss der Bereinigungsphase Wiederinbetriebnahme

Einige allgemeine Fragen für Ihre Checkliste:

- ✓ Woher werden die Einsatzkräfte Wiederherstellungsdaten und Backups beziehen?
- ✓ Wie werden die infizierten Systeme wieder in Betrieb genommen?
- ✓ Wann werden die infizierten Systeme wieder in Betrieb genommen?
- ✓ Welche Vorgänge werden während der Wiederherstellungsphase wiederhergestellt?
- ✓ Welche Tests und Überprüfungen sollten auf infizierten Systemen durchgeführt werden?
- ✓ Haben die Verantwortlichen dokumentiert, wie die Wiederherstellung durchgeführt wurde?

IT- Sicherheitsvorfall

6. „Lessons Learned“ – Erkenntnisse aus dem Vorfall

- Dokumentation der gewonnenen Erkenntnisse von entscheidender Bedeutung
- Ein detaillierter Bericht sollte alle Aspekte des IR-Prozesses, die behobenen Bedrohungen und künftige Maßnahmen zur Vermeidung abdecken

Fragen, wenn Sie in die Phase der „Lessons Learned“ eintreten:

- ✓ Wurden alle erforderlichen Unterlagen während der IR-Phasen erstellt?
- ✓ Wurde ein Bericht zu den gewonnenen Erkenntnissen erstellt?
- ✓ Deckt der Bericht alle Aspekte des Verfahrens zur Behebung des Vorfalls ab?
- ✓ Wann kann das IR-Team den Bericht veröffentlichen (Teilnehmerkreis)?
- ✓ Wer wird den Bericht „Lessons Learned“ vortragen?
- ✓ Gibt es Bereiche, in denen der Reaktions- Prozess verbessert werden kann?

IT- Sicherheitsvorfall

Wichtig

Diese Checklisten für die Reaktion auf Vorfälle sind ein Anhalt und können dem IR-Team helfen, in jeder Phase der Reaktion auf Sicherheitsvorfälle und deren Behebung auf dem richtigen Weg zu bleiben.

Welche anderen wichtigen Fragen stellte Ihr Team während des IR-Prozesses?

IT- Sicherheitsvorfall

Hinweis

Immer dran denken: **NACH** dem Vorfall ist **VOR** dem Vorfall!

und...

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

7. Zentrale Ansprechstelle Cybercrime



Angebot der Zentralen Ansprechstelle Cybercrime MV – ZAC MV

 **Warnmeldungen an die Wirtschaft**, aufgrund erlangter Ermittlungserkenntnisse

 **SPoC für Wirtschaftsunternehmen**

 **Vorträge bei Kammerversammlungen bzw. Artikel in Kammerzeitschriften**

- Praktische Cybercrime **Workshops**, aktuell zusammen mit den IHK's (Krisensimulation)
 - Sensibilisierung zu ausgewählten Phänomenen der Cybercrime
 - Verhaltens- und Handlungsempfehlungen im Vorfeld sowie bei Betroffenheit von Cybercrime-Delikten

Ziel:

Vertrauen in Ihre Polizei, Erstellen Sie Anzeige, wenden Sie sich an Ihre „**Zentrale Ansprechstelle Cybercrime**“ (ZAC MV).

Nur so kommt „**Licht in die Dunkelheit**“ und es kann gezielter auf Cybercrime reagiert, ermittelt und die Täter gefasst werden.

Erreichbarkeiten

Zentrale Ansprechstelle Cybercrime (ZAC MV)
Landeskriminalamt Mecklenburg - Vorpommern
Digitales Service- und Kompetenzzentrum

Retgendorfer Straße 9
19067 Rampe

Hotline ZAC: **03866 / 64 – 9494 (AB)**
E-Mail: **zac@lka-mv.de**



Vielen Dank für Ihre Aufmerksamkeit

Ansprechpartner/ Rückfragen:

**Landeskriminalamt Mecklenburg-Vorpommern
KHK Jörg Patzer, 1. Sachbearbeiter Dezernat Cybercrime
Hotline ZAC: 03866 / 64 – 9494
E-Mail: zac@lka-mv.de**

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

