



Mecklenburg-Vorpommern

Landeskriminalamt
Mecklenburg-Vorpommern

Cyber-Sicherheit

Webinar Recht KOMPAKT der IHK Schwerin

Schwerin, den 24.05.2023

LKA MV, Projekt Digitales Service- und Kompetenzzentrum (DiSK)

Polizeioberrat Maik Schröder, Leiter 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!

Inhalt / Übersicht

1. Vorbemerkungen
2. Zahlen, Daten, Fakten Cybercrime
3. Cybercrime Bekämpfung in Mecklenburg-Vorpommern
4. Ausgewählte Cybercrime-Phänomene
5. Umfragen zum Schutz im Internet (Digitalbarometer)
6. Handlungsempfehlungen LKA MV
7. IT-Sicherheitsvorfall als Prozess
8. Möglichkeiten LKA MV – ZAC MV

Vorbemerkungen

Ubiquität des Internets

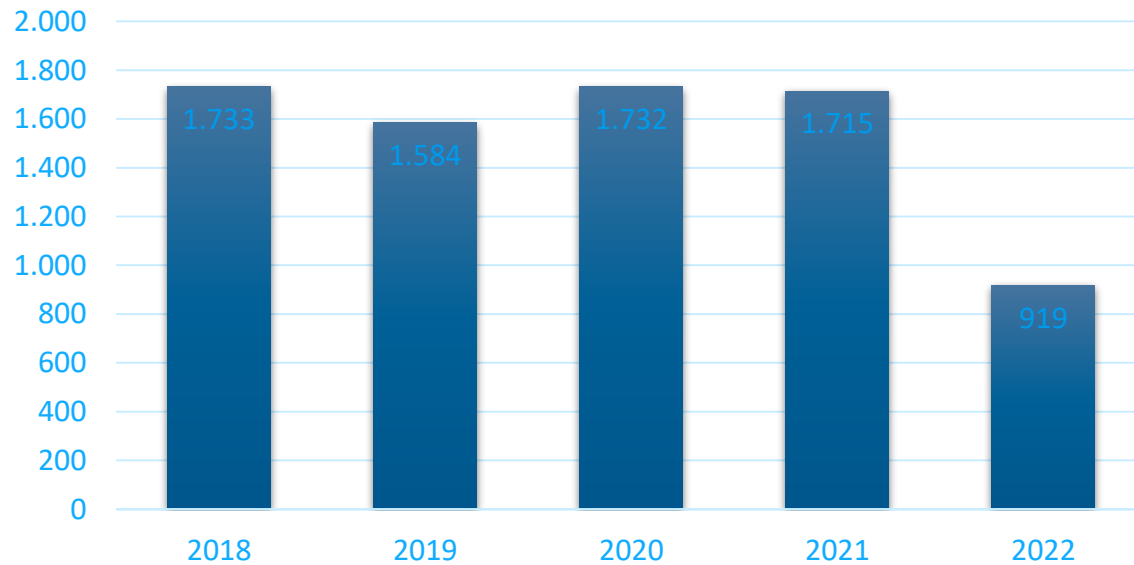


- Internetnutzung ist Bestandteil des Alltags
- Opfer wie Täter führen/nutzen jederzeit komplexe IT-Systeme im Westentaschenformat
- Internet immer häufiger zur Begehung von Straftaten genutzt, in allen Kriminalitätsphänomenen (z.B. Betrug)
- Solange Internet und E-Mails genutzt werden, sind Opfer und Hacker in einem Netz
- Strafverfolgungsbehörden müssen technische Ermittlungsmaßnahmen durchführen/initiieren

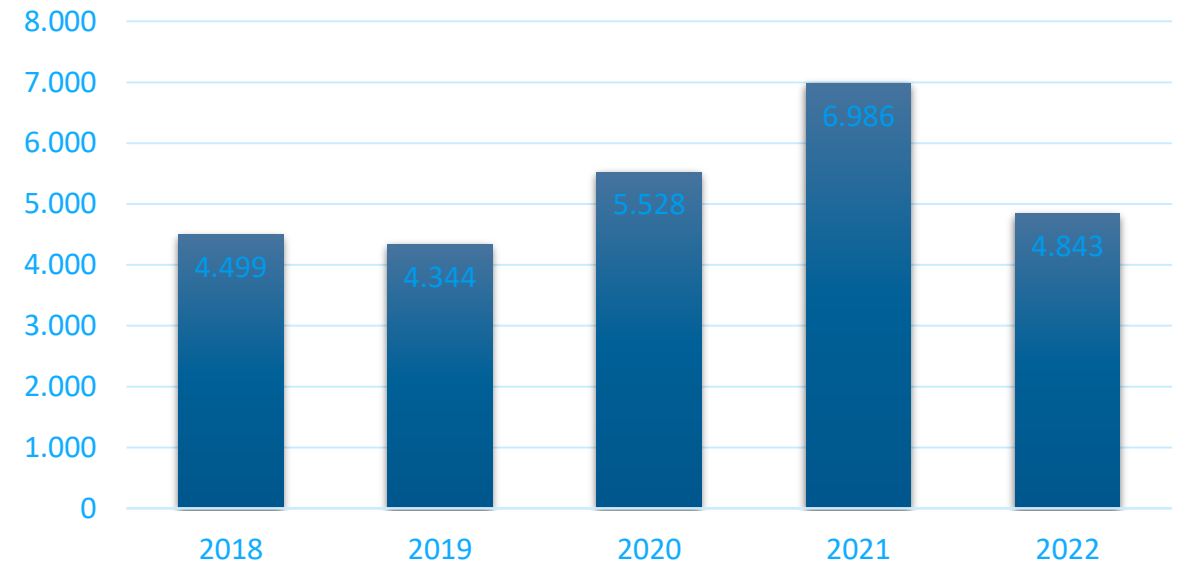
2. Zahlen, Daten, Fakten Cybercrime

Zahlen, Daten und Fakten

Fallaufkommen Cybercrime*



Fallaufkommen Tatmittel Internet*



* Erfassung nur, wenn konkrete Anhaltspunkte für Tathandlung in Deutschland

Quelle: PKS MV

Lage IT-Sicherheit Bundeslagebild BKA (2021)

- Zahl der Cyberangriffe erreicht 2021 neuen Höchstwert
- Anstieg über zwölf Prozent auf 146.363 Delikte
- **Deutschland überdurchschnittlich stark von Cyberattacken betroffen**
- nicht wegen fehlender Sicherheitsstandards, sondern „**lukratives Angriffsziel**“
- Zuwachs vor allem im Bereich Ransomware und bei DDoS-Angriffe
- fortschreitenden Verlagerung von Kriminalität in den digitalen Raum
- 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**

Lage IT-Sicherheit (2022)

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 2022

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:



15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.



34.000 Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.



78.000 neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

Erster digitaler Katastrophenfall in Deutschland



207 Tage Katastrophenfall
Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, Kfz-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

69% aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.



90% des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

Die Anzahl der Schadprogramme steigt stetig. Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund **116,6 Millionen** zugenommen.



Hackivismus im Kontext des russischen Krieges: Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.



BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikaten.



4.400 → 5.100
2020 → 2021



Zehn Jahre Allianz für Cyber-Sicherheit: 2022 sind wir bereits **6.220** Mitglieder.

Kollateralschaden nach Angriff auf Satellitenkommunikation



20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.



Deutschland Digital-Sicher-BSI

Lage IT-Sicherheit (2022)

IT-Sicherheit - ein Thema für jeden!

Insgesamt spitzte sich die bereits zuvor angespannte Lage weiter zu. Die Bedrohung im Cyber-Raum ist damit so hoch wie nie. Dies betrifft Unternehmen und ihre Angestellten in der Wirtschaft, genau wie alle Ebenen aus Politik, Verwaltung und dem Privatleben. Die Eckdaten aus dem BSI-Bericht für das Jahr 2022:

20.174

bekannte Schwachstellen
in Software-Produkten

10%

mehr kritische
Sicherheitslücken als im
Vorjahr

15 Mio.

Meldungen zu
Schadprogramm-
Infektionen in DE

69%

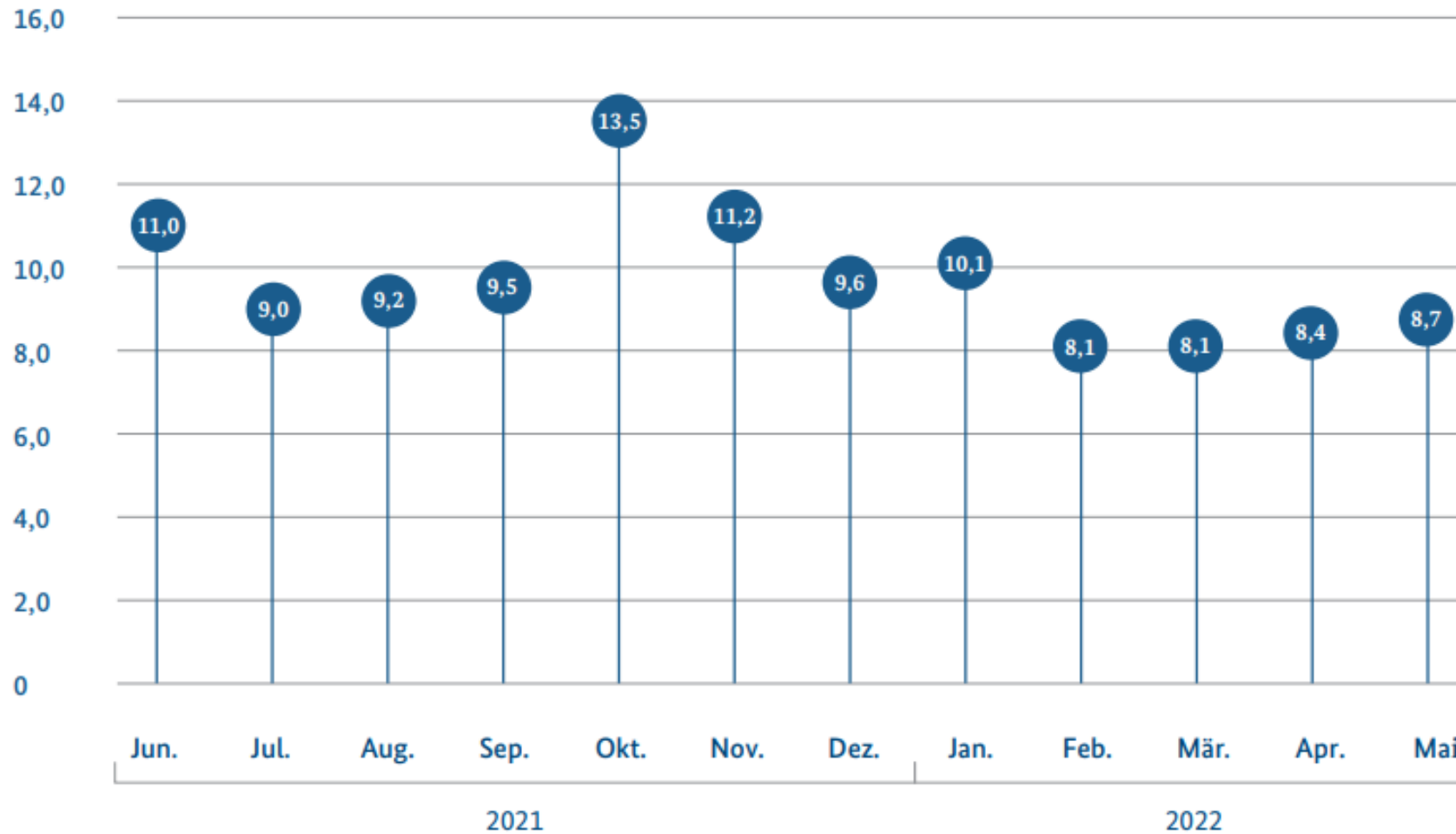
aller Spam-Mails waren
Cyber-Angriffe

Mit den Internet Security Days schließen Sie Wissenslücken, identifizieren den IT-Sicherheitsstand Ihrer Organisation und bekommen Werkzeuge für die nächsten Schritte.

Neue Malware-Varianten von Juni 2021 bis Mai 2022

Anzahl in Millionen

Abbildung 1:
Quelle: Malware-Statistik des BSI auf Basis
von Rohdaten des Instituts AV-Test GmbH



Lage IT-Sicherheit (2021/2022)

Homeoffice auf „Autopilot“ – Fake-President-Schaden in Höhe von 400.000 Euro

So auch bei einem Fake-President-Betrug, der sich vor Kurzem in Mitteldeutschland ereignete. Die Leiterin der Buchhaltung hinterfragt eine große Überweisungsaufforderung nicht, die sie im Homeoffice erreicht. Sie prüft nicht einmal die E-Mail-Adresse näher. Per Teams bittet sie eine Sachbearbeiterin im Homeoffice, die notwendige Zweitunterschrift zu leisten. So erhält die vom vermeintlichen CEO beauftragte Zahlung für angebliche Aktienkäufe über 400.000 Euro eine Freigabe.

In der Regel ist für den Erfolg beim CEO Fraud das "Social Engineering" entscheidend. Für diese Manipulation der Opfer ist eine Konversation in Echtzeit essenziell: Die Täter äußern Wertschätzung, zerstreuen Bedenken, bauen Druck auf oder beantworten Fragen – alles mit dem Ziel, das maximale Vertrauen in die Echtheit des Auftrags zu vermitteln.

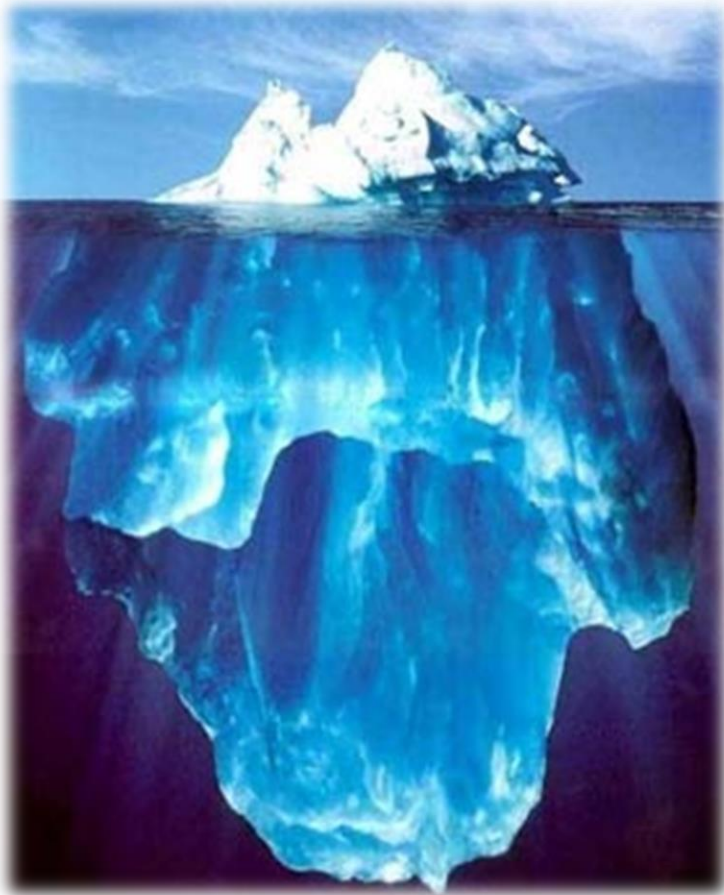
Plötzlich am Pranger: Cyberattacken bergen auch große Haftungsrisiken für Manager

Cyberkriminalität birgt neben finanziellen und datenschutzrechtlichen Risiken auch zunehmend Compliance- und Haftungsrisiken für Manager. Nicht umsonst steigen die Fälle, bei denen Unternehmen ihre eigenen Manager in Regress nehmen, in den letzten Jahren stark an. Der Vorwurf: Sorgfaltspflichtverletzungen oder mangelnde Risikoanalyse.

„Manager müssen im Zweifelsfall nachweisen, dass sie geeignete Vorsorgemaßnahmen getroffen haben und sie keine Schuld trifft“, sagt Jesko Trahms, Fachanwalt für Strafrecht und Partner bei BDO Legal Rechtsanwalts-gesellschaft mbH. „Ohne entsprechende Beweise ist das jedoch oft schwierig bis unmöglich – gerade bei Cybercrime oder Betrug. Auch beim Thema Compliance haben viele Unternehmen noch Nachholbedarf.“

Quelle: <https://www.eulerhermes.de>

Zahlen, Daten und Fakten



Dunkelfeldstudie LKA MV

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

Zahlen, Daten und Fakten

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
- Flyer_Cyberattacken

3. Cybercrime Bekämpfung in Mecklenburg-Vorpommern

Cybercrime-Bekämpfung

Zentrale Ansprechstellen

- Befürchtungen der Unternehmen entgegenzuwirken
- Erwartungshaltung externer Partner: Fach- und Sachkompetenz auf Seiten der Strafverfolgung
- Schaffung eines zentralen Ansprechpartners im Netzwerk der Sicherheitsbehörden als **Single Point of Contact**
- Einrichtung von **Zentralen Ansprechstellen Cybercrime** im Bundeskriminalamt und den Landeskriminalämtern als
- **zentraler Ansprechpartner für öffentliche und nicht-öffentliche Stellen, insbesondere die Wirtschaft**



Cybercrime-Bekämpfung



Cybercrime-Bekämpfung

Zentrale Ansprechstellen

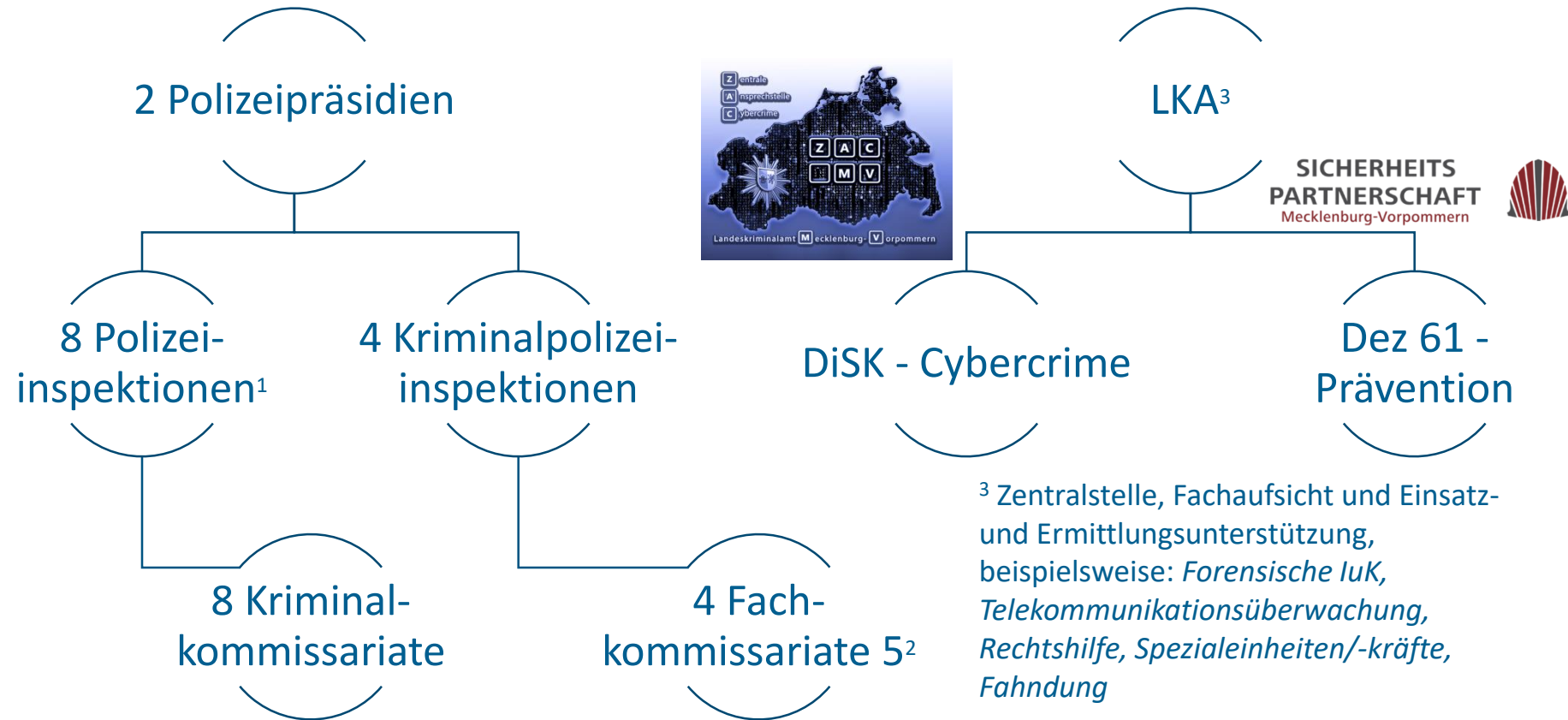


Gemeinsame Broschüre aller
Zentralen Ansprechstellen Cybercrime
des BKA und der Polizeien der Länder: „**Cybercrime –
Handlungsempfehlungen für die Wirtschaft in Fällen
von Cybercrime**“

abrufbar auf der Homepage des BKA
www.bka.de



Organisation Cybercrime-Bekämpfung



¹ mit Präventionsberatern

² Wirtschaftskriminalität/Cybercrime

4. Ausgewählte Cybercrime-Phänomene

Phänomene Cybercrime

- Phishing (über Mails oder Webseiten - Vorstufe für weitere Phänomene)
- Ransomware (Online-Erpressung mittels Verschlüsselungstrojaner)
- CEO-Fraud (Geschäftsführerschwindel)
- Man-in-the-Middle-Angriff (z.B. Geschäftspartnerschwindel)
- Online-Erpressung mittels **DDoS-Angriffe** (Distributed Denial of Service = Störung der IT-Verfügbarkeit)
- Datendiebstahl/Veröffentlichung von Daten (mittlerweile bei Ransomwareangriffen als Double/Triple Extortion üblich)

Wichtig: Es gibt eine Vielzahl von verschiedene Tätermotiven (gezielte bzw. breit gestreute Angriffe) und verschieden Vorgehensweisen dabei.

Phänomene Cybercrime – Phishing (über Webseite oder Mail)



🔒 Ihre Sicherheit hat bei uns höchste Priorität.

Bei Paypal einloggen

Wir haben ungewöhnliche Aktivitäten in Ihrem PayPal Konto festgestellt. Aus diesem Grund möchten wir Sie bitten Ihre Daten zu verifizieren.

Einloggen



Neu. Schneller. Einfacher.

Willkommen bei der neuen Paypal Kaufabwicklung!
Die gleiche Sicherheit nur noch schneller. So
einfach kann bezahlen sein.

© 1999–2015 PayPal Inc. [Datenschutz](#) [AGB](#) [Kontakt](#) [Impressum](#)

Phänomene Cybercrime – Ransomware

Verschlüsselungstrojaner

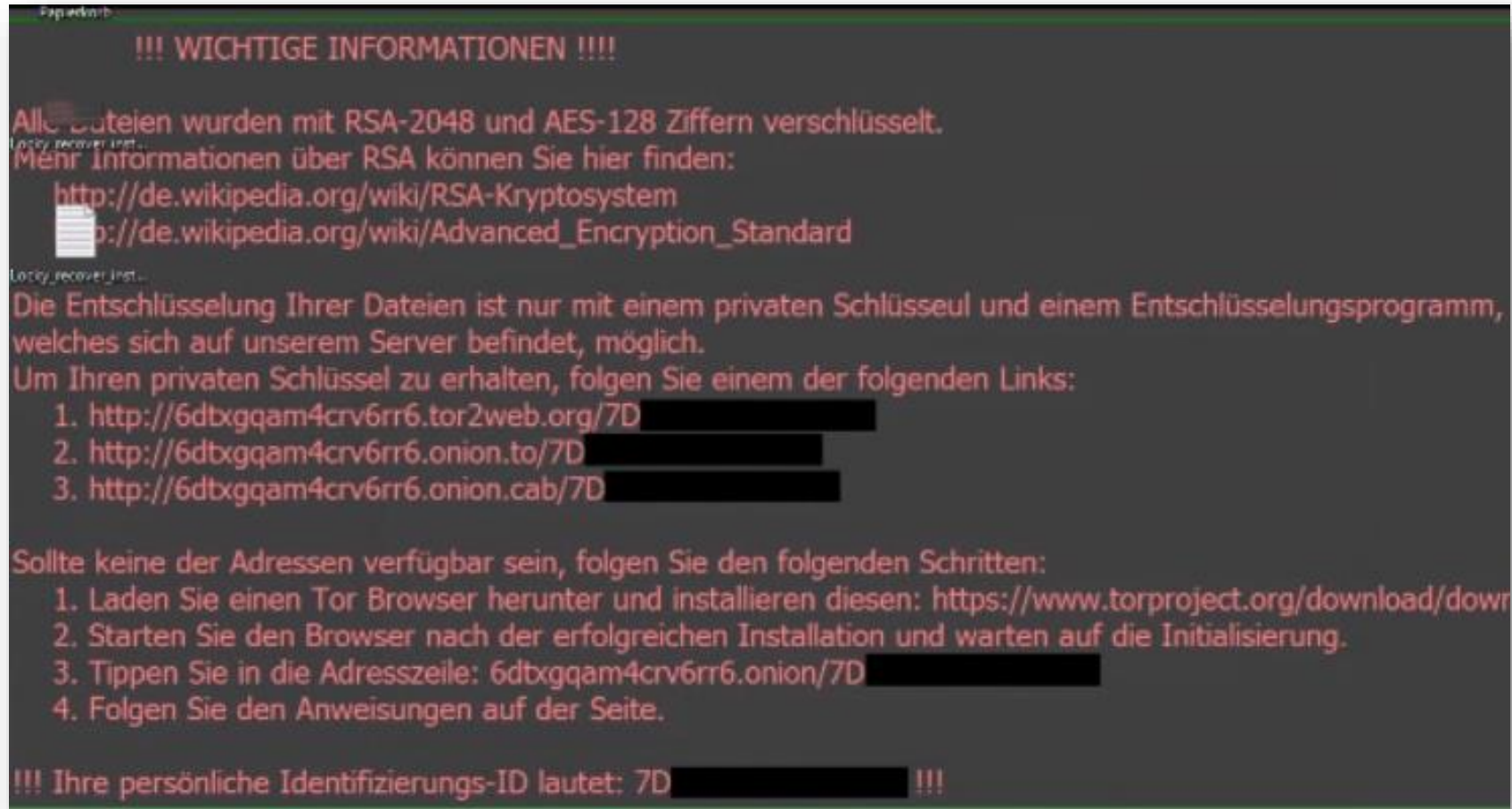
- Verbreitung durch: E-Mail, beim Surfen, Handy-Apps
- Risiken: Rechner wird gesperrt, Daten werden verschlüsselt, finanzielle Einbußen
- zur Entsperrung/Entschlüsselung wird Lösegeld (Ransom) verlangt
- in Underground-Foren werden Baukastensysteme der Schadsoftware oder Dienstleistungen zum Kauf angeboten



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

Phänomene Cybercrime – Ransomware

Lösegeldaufforderung nach Infektion





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

Begehungsweise

Von: [REDACTED]
Gesendet: Montag, 13. Juni 2016 13:03
An: [REDACTED]
Betreff: Re: AW: AW: Vertraulich

Unsere Firma wird sich in Kürze erweitern, um uns den Eintritt in neue Marktsegmente gewährleisten zu können. Ich bitte Sie um die notwendige Diskretion und Vertraulichkeit bezüglich dieser Verhandlung.

Die öffentliche Bekanntmachung wird am Freitag, den 1. Juli, in unseren Geschäftsräumen in Anwesenheit der Direktion und der Finanzmarktbehörde erfolgen.

Bitte nehmen Sie sofort und diskret Kontakt mit [REDACTED] Maier, der Rechtsanwältin unserer Anwaltskanzlei auf. Sie erreichen sie unter der Telefonnummer: [REDACTED] 170060 [REDACTED], oder der E-Mail Adresse: [REDACTED].maier@fouquet-michel[REDACTED]

Sie wird Sie über das weitere Vorgehen informieren und Ihnen eine Bankverbindung mitteilen, damit das Übernahmeangebot bestätigt und die Überweisung sofort getätigt werden kann.

Ich möchte Sie nochmals darauf hinweisen, dass es sich um ein absolut vertrauliches Geschäft handelt, von dem kein Dritter in Kenntnis gesetzt werden darf.

Bitte machen Sie keine Andeutungen, weder im persönlichen Gespräch, noch telefonisch. Dies ist eine von der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) vorgesehene Vorsichtsmaßnahme.

Sie dürfen lediglich mit der Rechtsanwaltskanzlei über dieses Geschäft sprechen. So sehen es die Normen unseres Übernahmeangebotes vor.

Im Rahmen der von der BaFin vorgeschriebenen Vorgehensweise, wird unsere Korrespondenz in Zukunft nur über meine persönliche E-Mail-Adresse laufen: [REDACTED]@mail.com.

Ich freue mich, Ihnen mitteilen zu können, dass Sie dieses Kaufgeschäft abwickeln werden.

Mit freundlichen Grüßen,

[REDACTED]

Phänomene Cybercrime – CEO Fraud

Begehungsweise, weiteres Beispiel:

- Angeblicher Chef (= Kay) schreibt seine Finanzbuchhalterin vom Unternehmen an.

Von: Kay

Gesendet: Freitag, 2018 08:39

An: @ [l.de](#)

Betreff: Dringend

Wir müssen eine internationale Zahlung von 54.225,00 EUR machen. Können wir das heute machen?

grüße,
Kay

Phänomene Cybercrime – CEO Fraud

Begehungsweise

- Im nächsten Schritt wird eine Kontoverbindung und Zahlungsanweisung vom angeblichen Chef (= Kay) an die Finanzbuchhalterin vom Unternehmen geschickt.

Von: Kay [\[mailto: \[redacted\]@aol.com\]](mailto: [mailto: [redacted]@aol.com])
Gesendet: Freitag, 01.08.2018 09:19
An: [redacted]@ [redacted].de
Betreff: AW: Dringend

Ok, ich werde die Dokumentation später senden. Bitte zahlen:

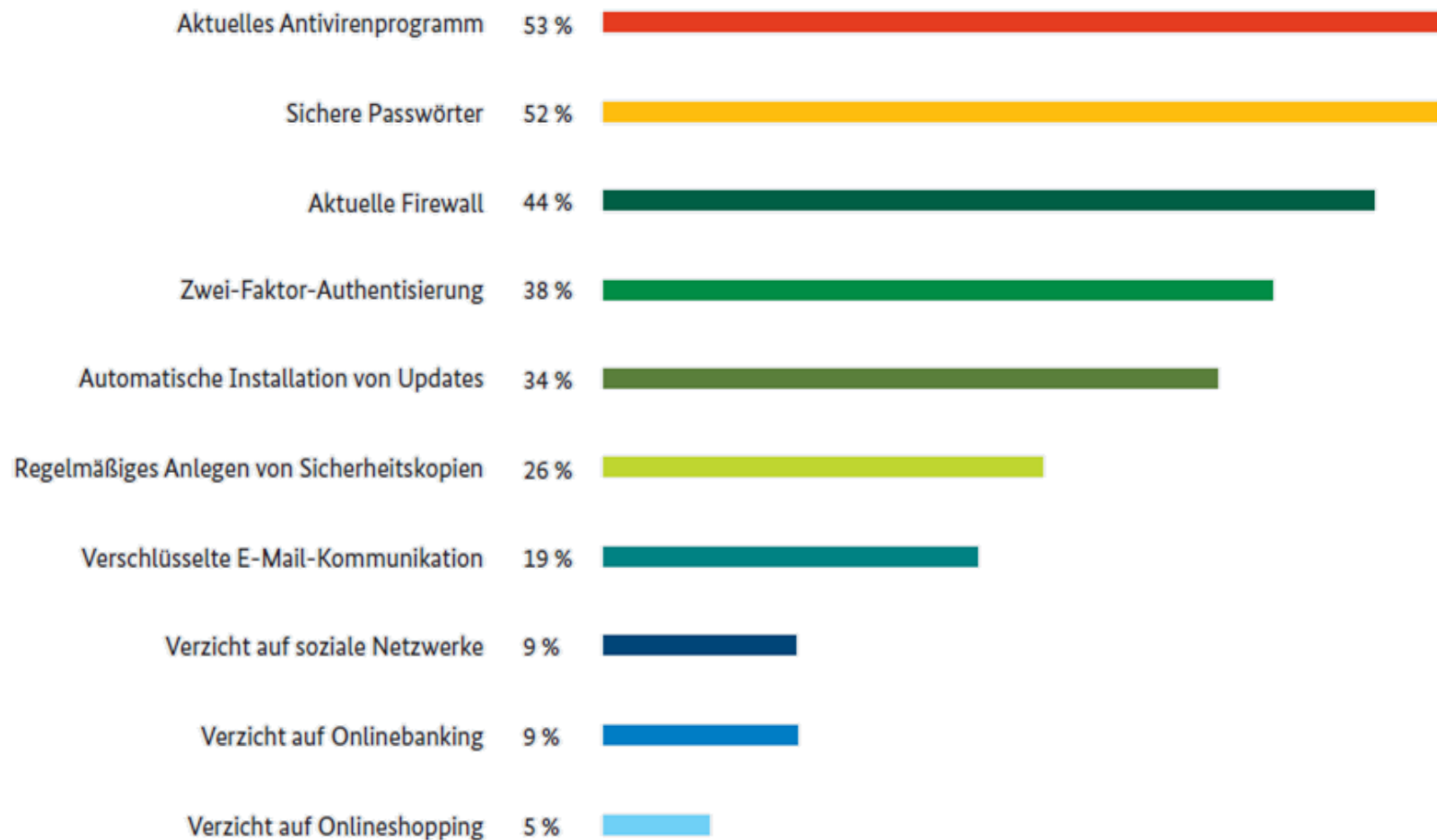
KONTOBEZEICHNUNG: san
ADRESSE: ! /entry 1 1GX
IBAN: 43
BIC: H
SC: 40
KONTO NUMMER: 4
BANK: HSBC BANK PLC
ZWECK: A' [redacted] [redacted]
REFERENZ: AI

...Senden mir den Überweisungsbeleg.

grüße,
Kay

5. Umfragen zum Schutz (Digitalbarometer)

Wie schützen Sie sich vor Gefahren im Internet?



Basis: Alle Befragten (2022: n = 2000). Mehrfachnennungen möglich. Quelle: Digitalbarometer zur Cyber-Sicherheit 2022, ProPK und BSI

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

6. Handlungsempfehlungen des LKA MV

Aktuelle Schwachstellen



ALERT Patchday

Angreifer infizieren Windows mit Nokoyawa-Ransomware

Microsoft hat wichtige Sicherheitsupdates für etwa Azure, Dynamics 365 und Windows veröffentlicht.

🗨️ 58 | heise Security



ALERT IT Security

BSI warnt vor kritischen Zero-Day-Lücken im NTP-Server

Ein IT-Forscher hat fünf Sicherheitslücken im Zeitserver NTP gemeldet. Das BSI stuft die Lücken als kritisch ein. Ein Update steht bislang noch nicht bereit.

🗨️ 57 | heise Security

Aktuelle Schwachstellen



ALERT Jetzt patchen!

QueueJumper-Lücke gefährdet hunderttausende Windows-Systeme

Sicherheitsforscher haben nach weltweiten Scans über 400.000 potenziell angreifbare Windows-Systeme entdeckt. Sicherheitspatches sind verfügbar.

59 | heise Security

Handlungsempfehlungen

Wichtig: Es gibt nicht nur den einen Tipp.

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

- Patch-Management (Systeme aktuell halten)
- Segmentierung der IT-Netze (Einsatz von Firewalls)
- Sensibilisierung der Mitarbeiter (alle „mitnehmen“ / Human Firewall / Fehlerkultur)
(keine unglaublichen E-Mails, Anhänge oder Links öffnen)
- Eingeschränkte Benutzer- und Admin-Rechte (Ideal: 2FA, MFA)
- Regelmäßige Backups (Wichtig! Auch offline, unabhängig vom Wirkbetriebsnetz)
- Überprüfung der Backups und Training des Einspielens
- IT-Notfall-Management (siehe IT-Sicherheitsvorfall)

Kein Lösegeld zahlen → Finanzierung weiterer Angriffe!

Handlungsempfehlungen

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

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

Handlungsempfehlungen - Passwortsicherheit

Für Anwender:

- Empfehlung: 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)
- Plugins für Browser/Mailclient (z.B. Flagfox, MailHops)

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 - E-Mail-Sicherheit

→ Schutz vor Spoofing, Phishing und Fälschung

SPF (Sender Policy Framework) = 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 (DomainKeys Identified Mail) = 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 (Domain-based Message Authentication, Reporting and Conformance) = Kontrollsystem

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

7. 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 arbeitet erforderlichenfalls 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!**

8. Möglichkeiten LKA MV – ZAC MV

Angebot der ZAC MV

- Warnmeldungen an die Wirtschaft, aufgrund erlangter Ermittlungserkenntnisse
- SPoC für Wirtschaftsunternehmen
- Vorträge bei Kammerversammlungen
- Artikel in Kammerzeitschriften
- ✓ Sensibilisierung zu ausgewählten Phänomenen der Cybercrime
- ✓ Verhaltens- und Handlungsempfehlungen im Vorfeld und 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

Landeskriminalamt Mecklenburg - Vorpommern
Projekt Digitales Service- und Kompetenzzentrum (DiSK)
Zentrale Ansprechstelle Cybercrime (ZAC MV)
Retgendorfer Straße 9
19067 Rampe

Hotline ZAC: 03866 / 64 - 9494

E-Mail: zac@lka-mv.de

Fragen?

Vielen Dank für Ihre Aufmerksamkeit

Ansprechpartner/ Rückfragen:

**Landeskriminalamt Mecklenburg-Vorpommern
POR Maik Schröder, Leiter Dezernat Cybercrime
Hotline ZAC: 03866 / 64 – 9494
E-Mail: zac@lka-mv.de**

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