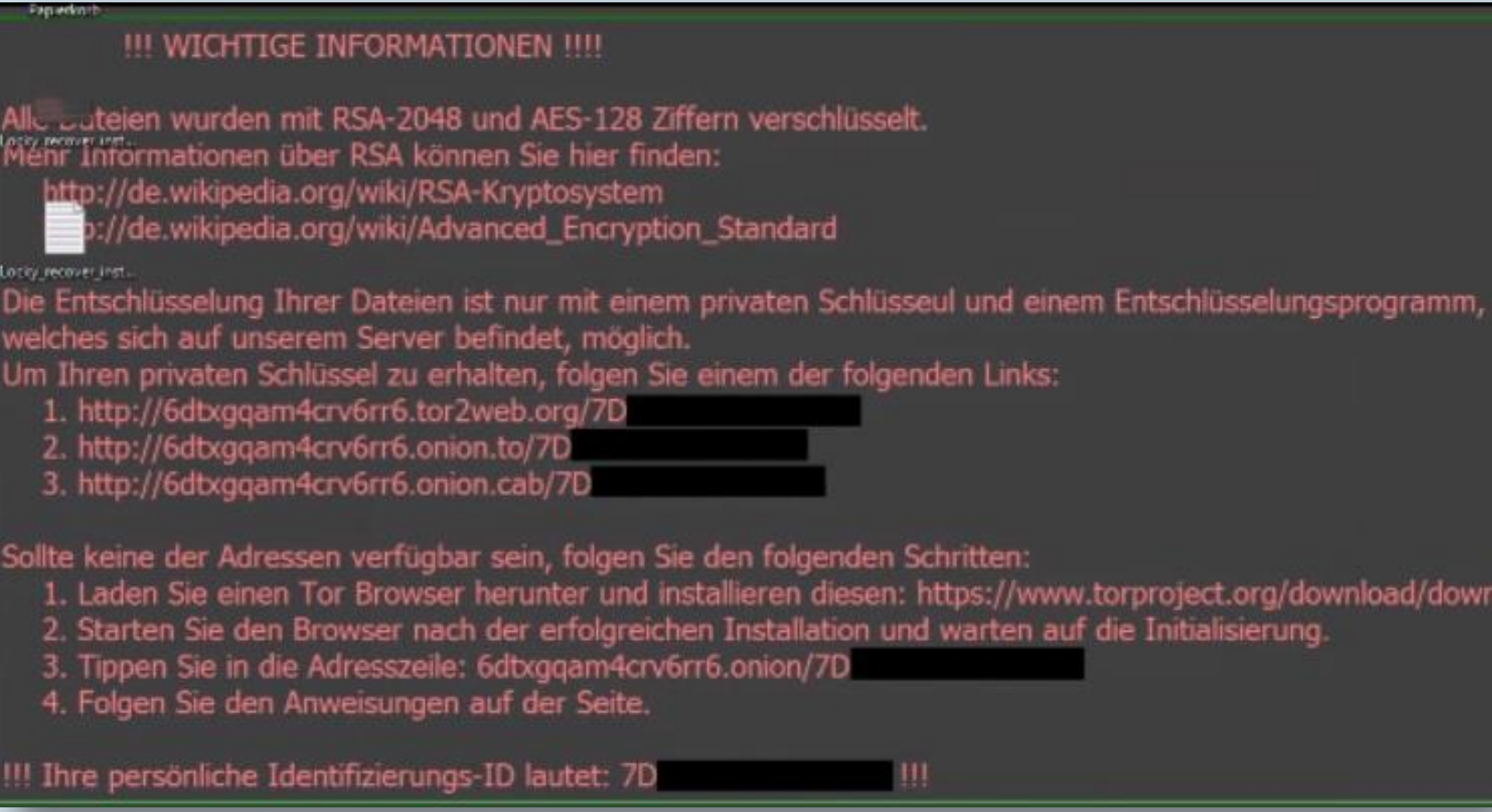
Landeskriminalamt
Mecklenburg-Vorpommern

Bürgermeisterforum Wirtschaft:
„Cybercrime – Gefahr für Wirtschaft und Kommunen“ (IHK Schwerin 01.12.2021)

Projekt Digitales Service- und Kompetenzzentrum (DiSK)
PR Maik Schröder, Leiter DiSK – 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 Schlüsseul 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/down
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 !!!

Inhalt / Übersicht

1. Zahlen, Daten, Fakten
2. Cybercrime Bekämpfung in Mecklenburg-Vorpommern
3. Ausgewählte Cybercrime-Phänomene
4. Handlungsempfehlungen LKA MV
5. IT-Sicherheitsvorfall als Prozess
6. Möglichkeiten LKA MV – ZAC MV

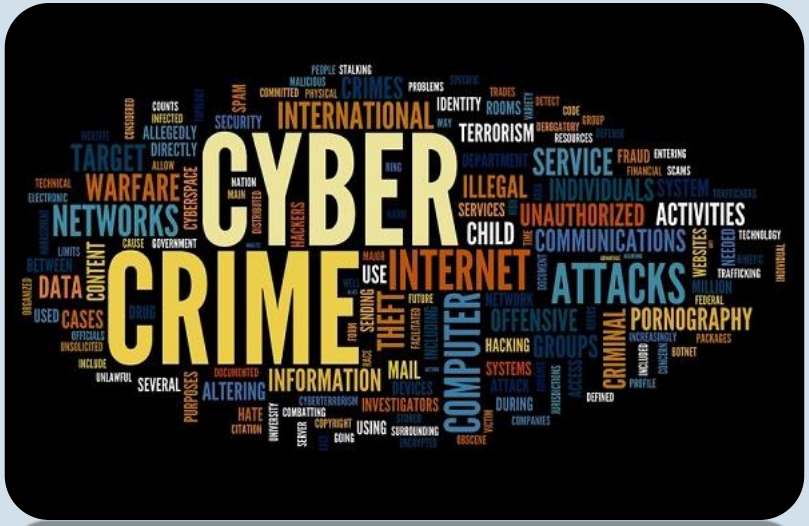
1. Zahlen, Daten, Fakten

Vorbemerkungen

Ubiquität des Internets

- Internetnutzung ist selbst-verständlicher Bestandteil des Alltags
- die Miniaturisierung der Geräte fördert diese Entwicklung
- Opfer wie Täter führen/nutzen jederzeit komplexe IT-Systeme im Westentaschenformat
- das Internet wird immer häufiger zur Begehung von Straftaten in allen Kriminalitätsphänomenen (z.B. Betrug) genutzt
- Strafverfolgungsbehörden müssen technische Ermittlungsmaßnahmen durchführen/initiieren

Begriffsbestimmung



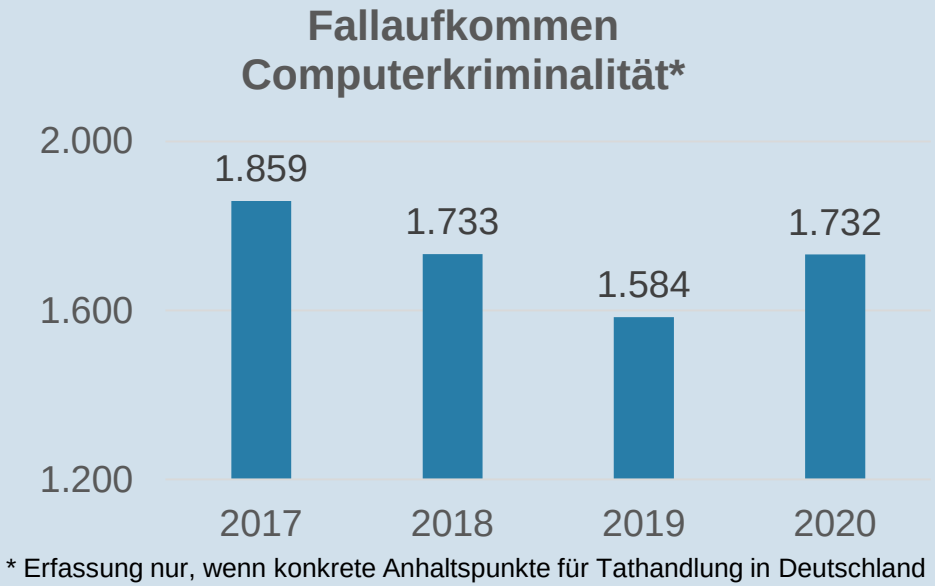
Quelle: Sondermeldedienst Cybercrime
Stand: 10.12.2012

- Internetkriminalität = Cybercrime
- Cybercrime umfasst die Straftaten, die sich **gegen** das Internet, weitere Datennetze und informationstechnische Systeme oder deren Daten richten.
- Cybercrime umfasst auch solche Straftaten, die **mittels** dieser Informationstechnik begangen werden.

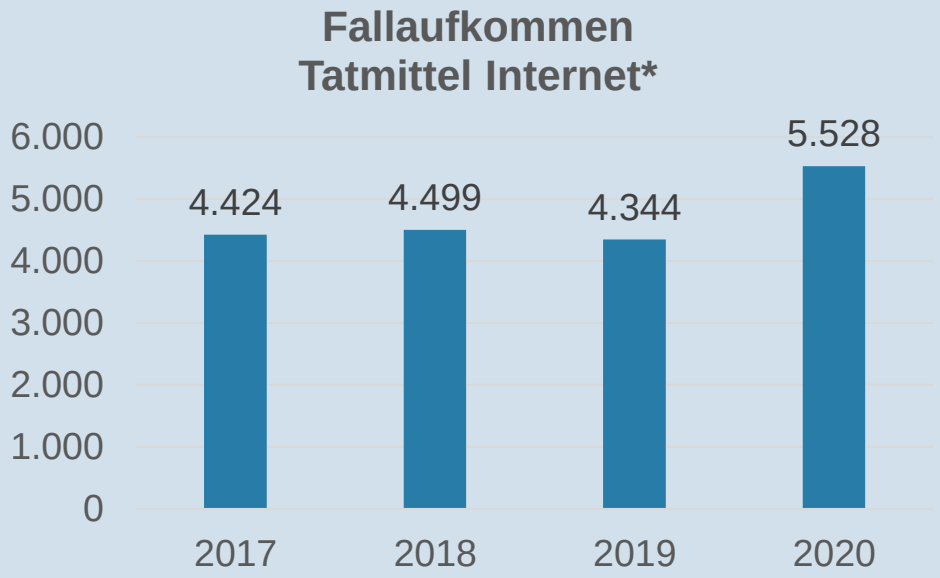
Cybercrime - Straftatbestände

- Ausspähen von Daten
- Abfangen von Daten
- Vorbereiten des Ausspähens und Abfangens von Daten
- Datenveränderung
- Datenhehlerei
- Fälschung beweiserheblicher Daten
- Computerbetrug
- Computersabotage

Zahlen, Daten und Fakten



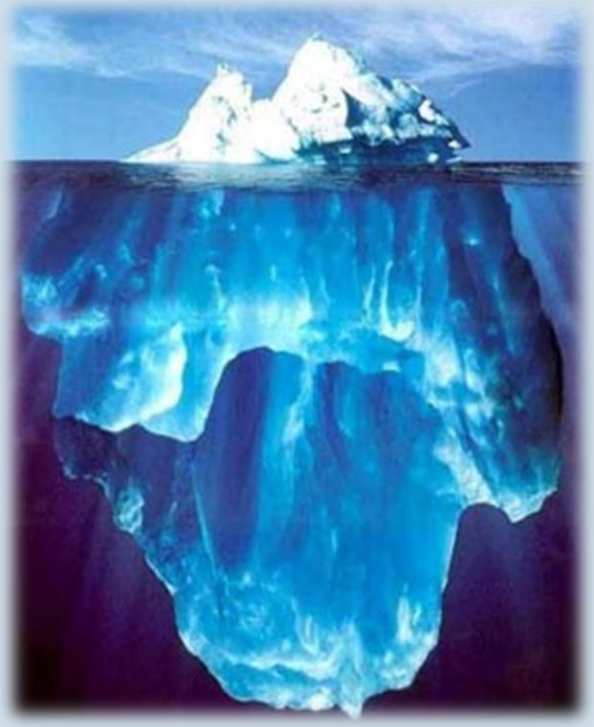
* Erfassung nur, wenn konkrete Anhaltspunkte für Tathandlung in Deutschland



Quelle: PKS MV

Zahlen, Daten und Fakten

Dunkelfeldstudie LKA MV



- 8.151 Fragebögen
- an Bürger ab 16 Jahren
- mit Hauptwohnsitz in Mecklenburg-Vorpommern
- 3.170 Fragebögen waren statistisch auswertbar

- **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. *<u>mögliche Gründe:</u>*

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

KFN - Unternehmensbefragung

Obwohl …

- Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) hat Unternehmen zum Thema Cyberkriminalität befragt (2020)
- Risiko von Cyberangriffen steigt
- insbesondere Angriffe mit Schadsoftware und Phishing
- IT-Sicherheit von Unternehmen durch die Corona-Krise beeinträchtigt (Homeoffice, VPN-Verbindungen)

KFN - Unternehmensbefragung

- Hälfte der Unternehmen schätzte Risiko eines schädigenden ungezielten Cyberangriffs in den nächsten zwölf Monaten als sehr hoch oder zumindest eher hoch ein.
- 60 % der 635 im Jahr 2020 erneut befragten Unternehmen musste innerhalb eines Jahres auf mindestens einen Cyberangriff reagieren.
- Unterschieden nach Angriffsarten: Phishing (42 %) und Schadsoftwareangriffen (Ransomware*: 14 %, Spyware: 16 % und sonstige Schadsoftware: 36 %)

* Höhe der Lösegeldforderungen bei Ransomware-Angriffen nehmen zu und haben mit einer Betriebsunterbrechung gravierende Auswirkungen für betroffene Unternehmen.

2. Cybercrime Bekämpfung in Mecklenburg-Vorpommern

Cybercrime-Bekämpfung

Zentrale Ansprechstellen

- Befürchtungen entgegenzuwirken
- Erwartungshaltung externer Partner: Fach- und Sachkompetenz auf Seiten der Strafverfolgung
- Schaffung eines zentralen Ansprechpartners im Netzwerk der Sicherheitsbehörden als **S**ingle **P**oint **o**f **C**ontact
- Im Ergebnis Einrichtung von **Z**entralen **A**nsprechstellen **C**ybercrime 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 **A**nsprechstellen **C**ybercrime

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

2 Polizeipräsidien

LKA[3]

SICHERHEITS PARTNERSCHAFT Mecklenburg-Vorpommern

8 Polizei-inspektionen[1]

4 Kriminalpolizei-inspektionen

DiSK - Cybercrime

Dez 61 - Prävention

8 Kriminal-kommissariate

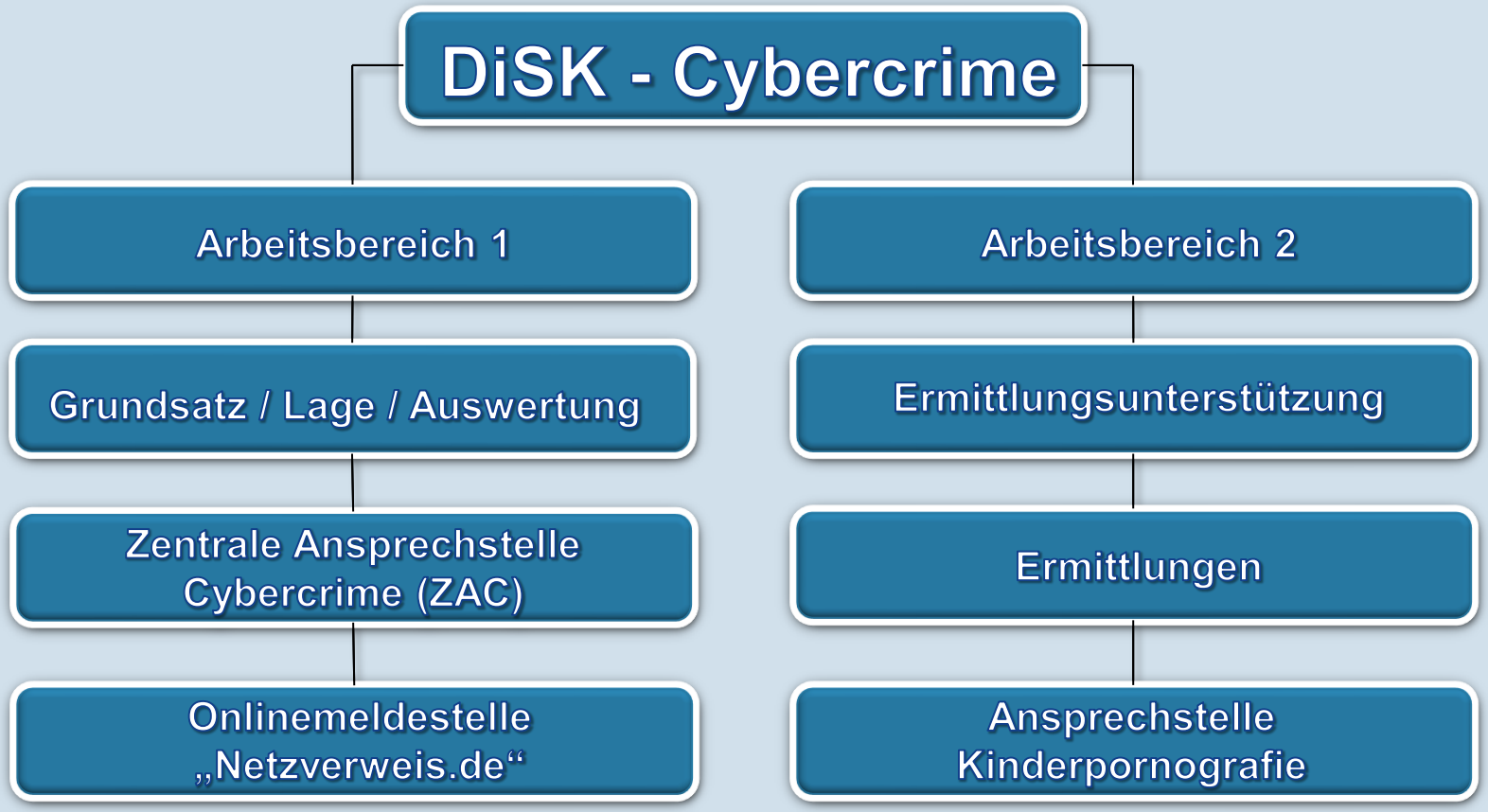
4 Fach-kommissariate 5[2]

[3] Zentralstelle, Fachaufsicht und Einsatz- und Ermittlungsunterstützung, beispielsweise: *Forensische IuK, Telekommunikationsüberwachung, Rechtshilfe, Spezialeinheiten/-kräfte, Fahndung*

[1] *mit Präventionsberatern*

[2] *Wirtschaftskriminalität/Cybercrime*

Organisation Cybercrime-Bekämpfung



Cybercrime-Bekämpfung ZAC MV

Durch die ZAC werden neben den Aufgaben als SPOC im Rahmen der Prävention Maßnahmen anderer Stellen unterstützt (Auszug):

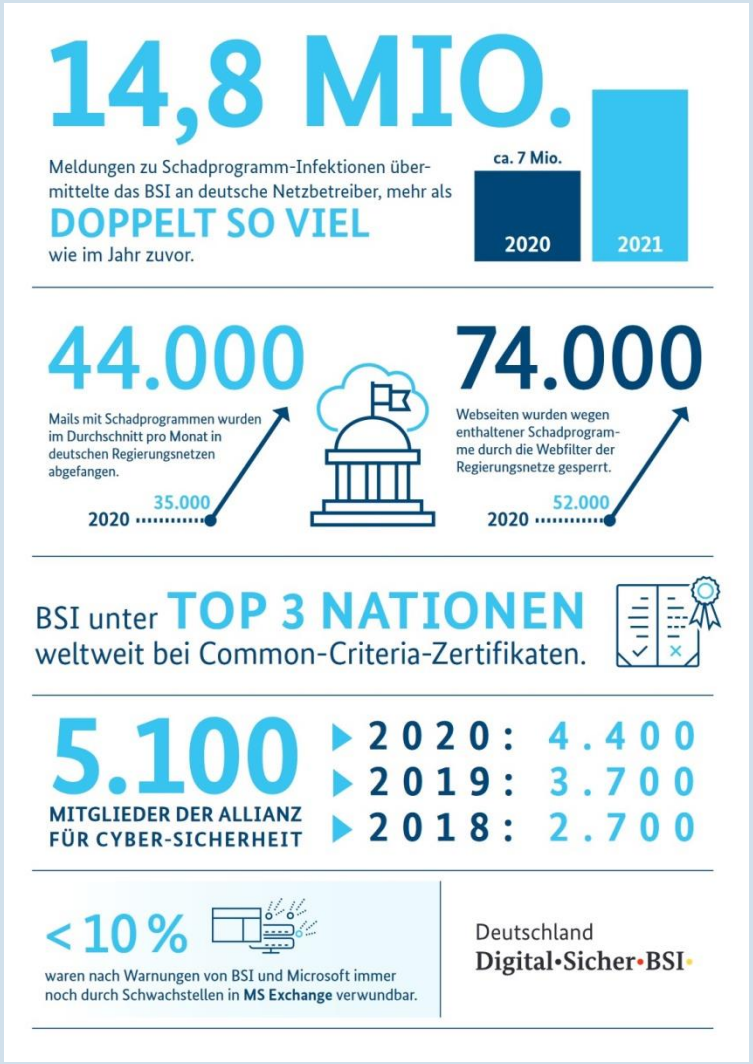
- Regionalgruppenveranstaltung der **Ingenieurkammer M-V** zum Thema: „Cyberkriminalität und Datensicherheit“ (14.06.2018)
- Arbeitstreffen mit **IT-Sicherheitsbeauftragten des Landtages MV** (17.07.2018)
- ZAC-Veranstaltung: **Tag des norddeutschen Handels** (04.09.2018)
- ZAC-Veranstaltung: Fachveranstaltung des **Bauverbandes MV** (23.10.2018)

Cybercrime-Bekämpfung ZAC MV

- **Artikel: Vorstellung der ZAV MV** in den **Kammerzeitschriften der IHK** im 1. Quartal 2019
- Präventionsgespräche mit **Mitgliedern des Landtages** sowie MA der Fraktionen (Jan. 2019)
- Cybercrime-Vortrag auf **Bürgermeisterwoche** vom Zweckverband Kommunales Studieninstitut Mecklenburg-Vorpommern (Feb. 2019)
- Cybercrime für die **Wasserwirtschaft - Actemium H&F GmbH** Vortrag (April 2019)

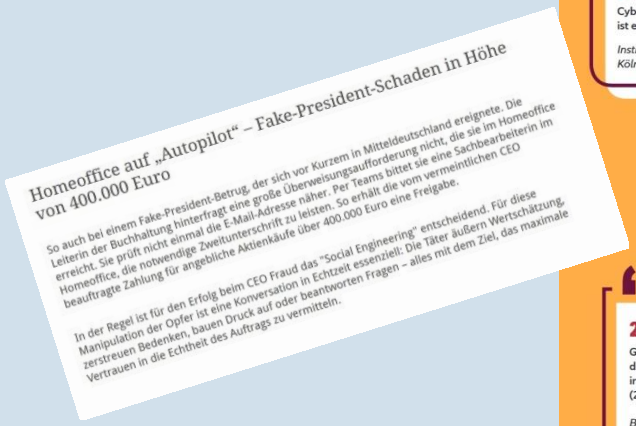
3. Ausgewählte Cybercrime-Phänomene

Lage zur IT-Sicherheit (2021)



Lage zur IT-Sicherheit (2021)

Quelle:
https://www.eulerhermes.de



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

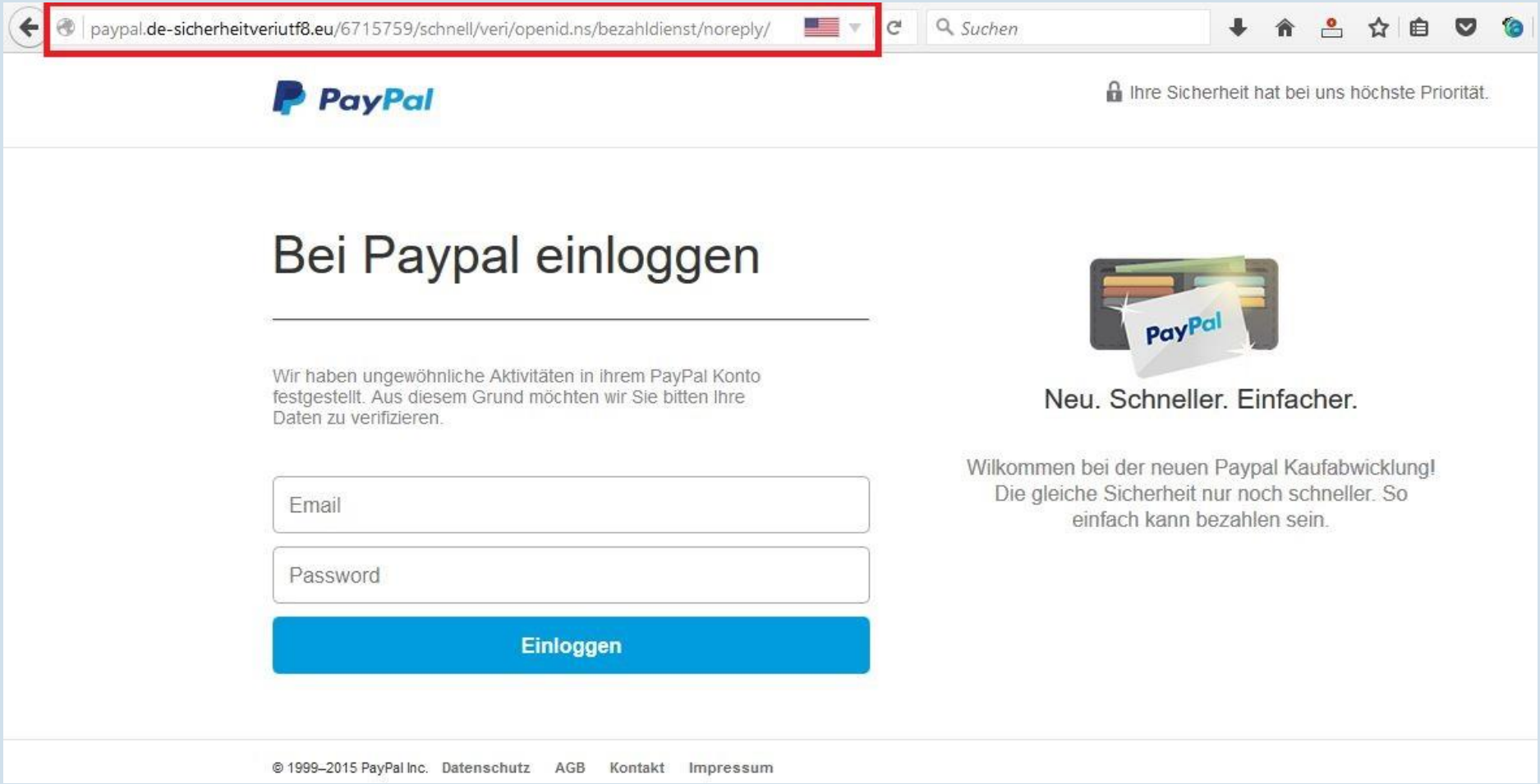
Cyberkriminalität birgt neben finanziellen und datenschutzrechtlichen Risiken auch zunehmend Compliance- und Haftungsrisiken für Manager. Nicht umsonst steigen die Fälle, bei denen Unternehmen ihre eigenen Manager in Regress nehmen, in den letzten Jahren stark an. Der Vorwurf: Sorgfaltspflichtverletzungen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

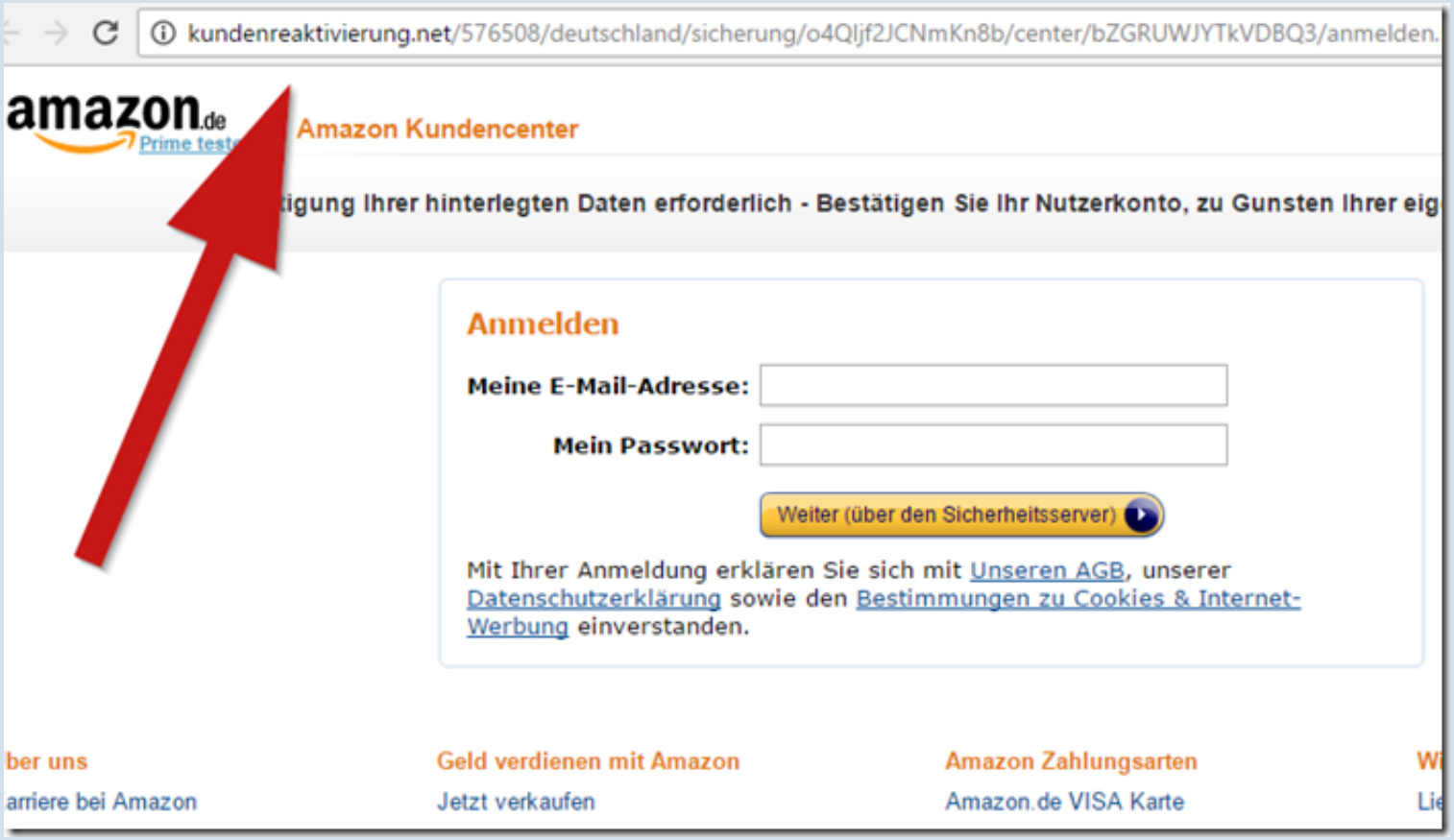
Phänomene Cybercrime

- **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** (Störung der Seitenverfügbarkeit)
- Datendiebstahl/Veröffentlichung von Daten

Phänomene Cybercrime – Phishing



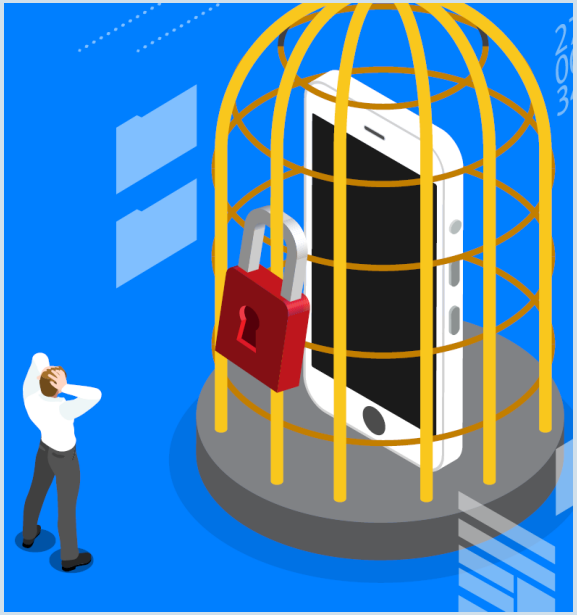
Phänomene Cybercrime – Phishing



Phänomene Cybercrime – Ransomware

Verschlüsselungstrojaner

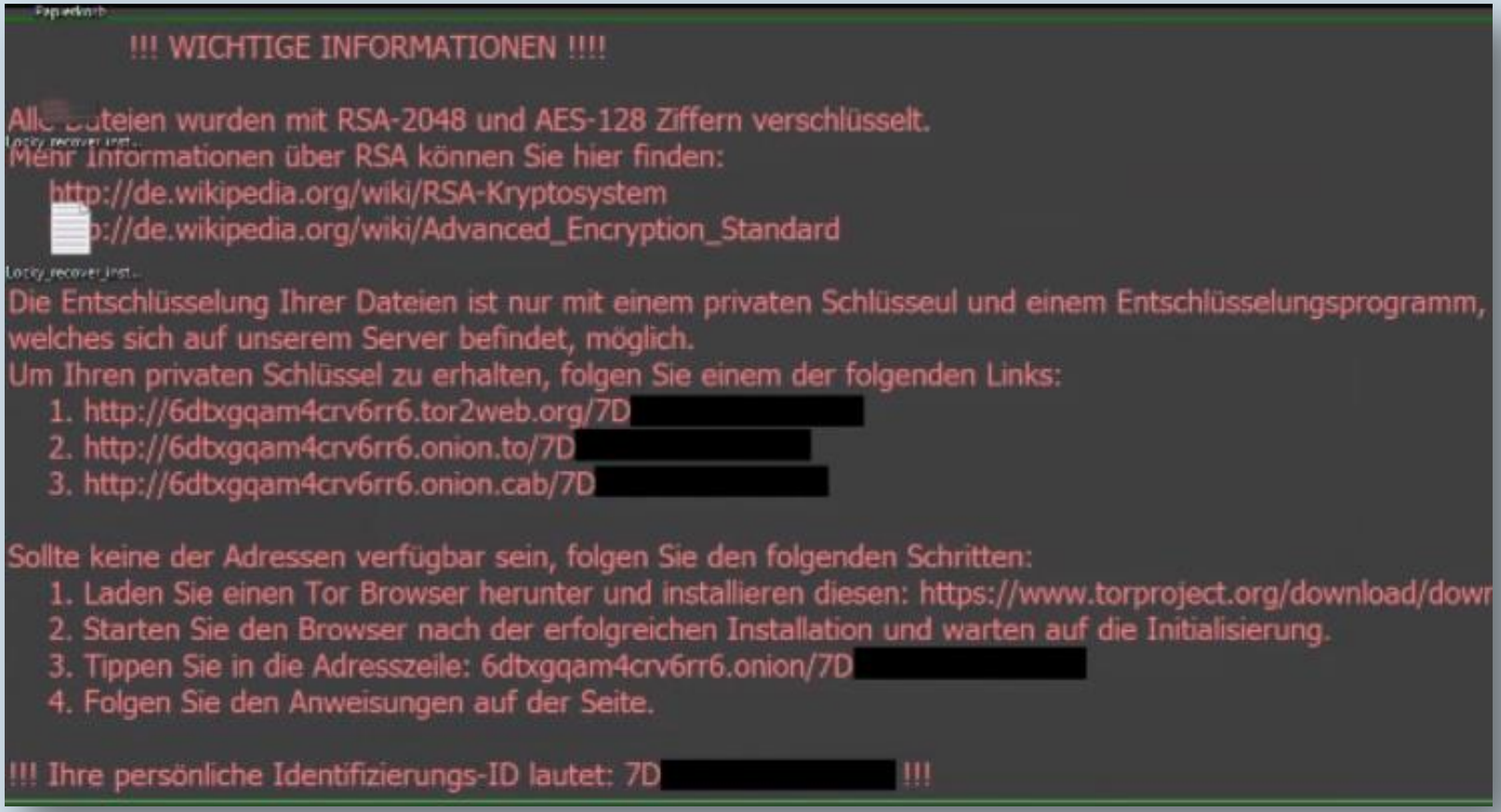
- seit 2014/2015 verstärkt bundesweite und internationale Verbreitung
- Verbreitung durch: E-Mail, beim Surfen, Handy-Apps
- **Risiken: Rechner wird gesperrt, Daten werden verschlüsselt, finanzielle Einbußen**
- **zur Entsperrung/Entschlüsselung wird Lösegeld (Ransom) verlangt**
- in Undergroundforen werden Baukastensysteme der Schadsoftware zum Kauf angeboten



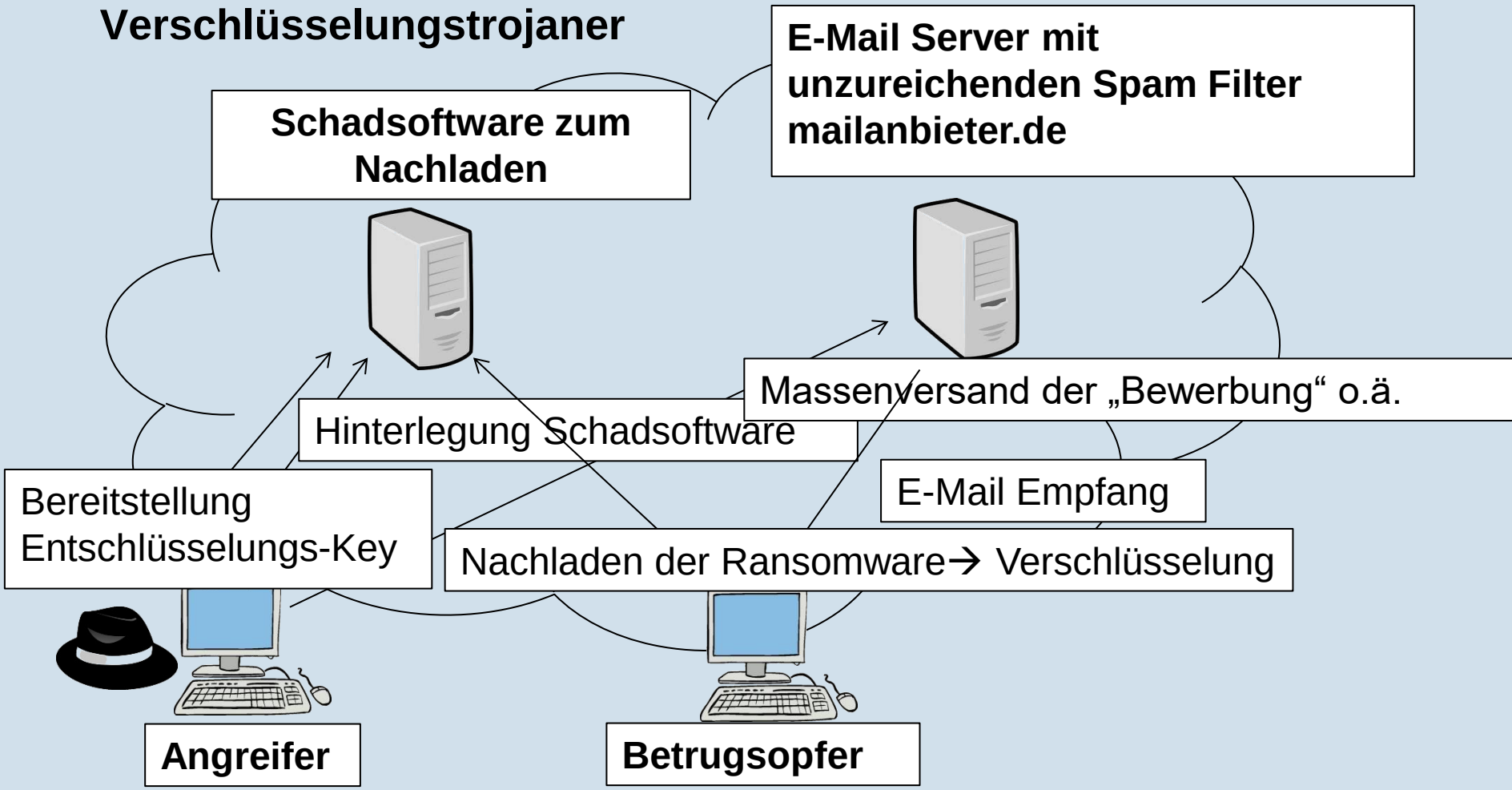
Quelle: https://www.sicherheitspartnerschaft-mv.de/downloads.html?file=files/pdf/Downloads/mobile%20Ransomware.pdf

Phänomene Cybercrime – Ransomware

Lösegeldaufforderung nach Infektion



Phänomene Cybercrime – Ransomware



Phänomene Cybercrime – Ransomware

Verschlüsselungstrojaner – bekannte Vertreter/Dateien

*.crjoker *.cryptotorlocker* *.ecc *.encrypted *.exx *.ezz *.frtrss

.hydracrypt_ID ***.locky** *.micro *.r5a *.surprise *.ttt *.vault *.vvv *.xxx *gmail*.crypt *recover_instruction*.* *restore_fi*.* *want your files back.* confirmation.key **cryptolocker.*** decrypt_instruct*.* enc_files.txt help_decrypt*.* help_recover*.* help_restore*.* help_your_file*.* how to decrypt*.* how_recover*.* how_to_decrypt*.* how_to_recover*.* howto_restore*.* howtodecrypt*.* install_tor*.* last_chance.txt message.txt readme_decrypt*.* readme_for_decrypt*.* recovery_file.txt recovery_key.txt vault.hta vault.key vault.txt your_files.url

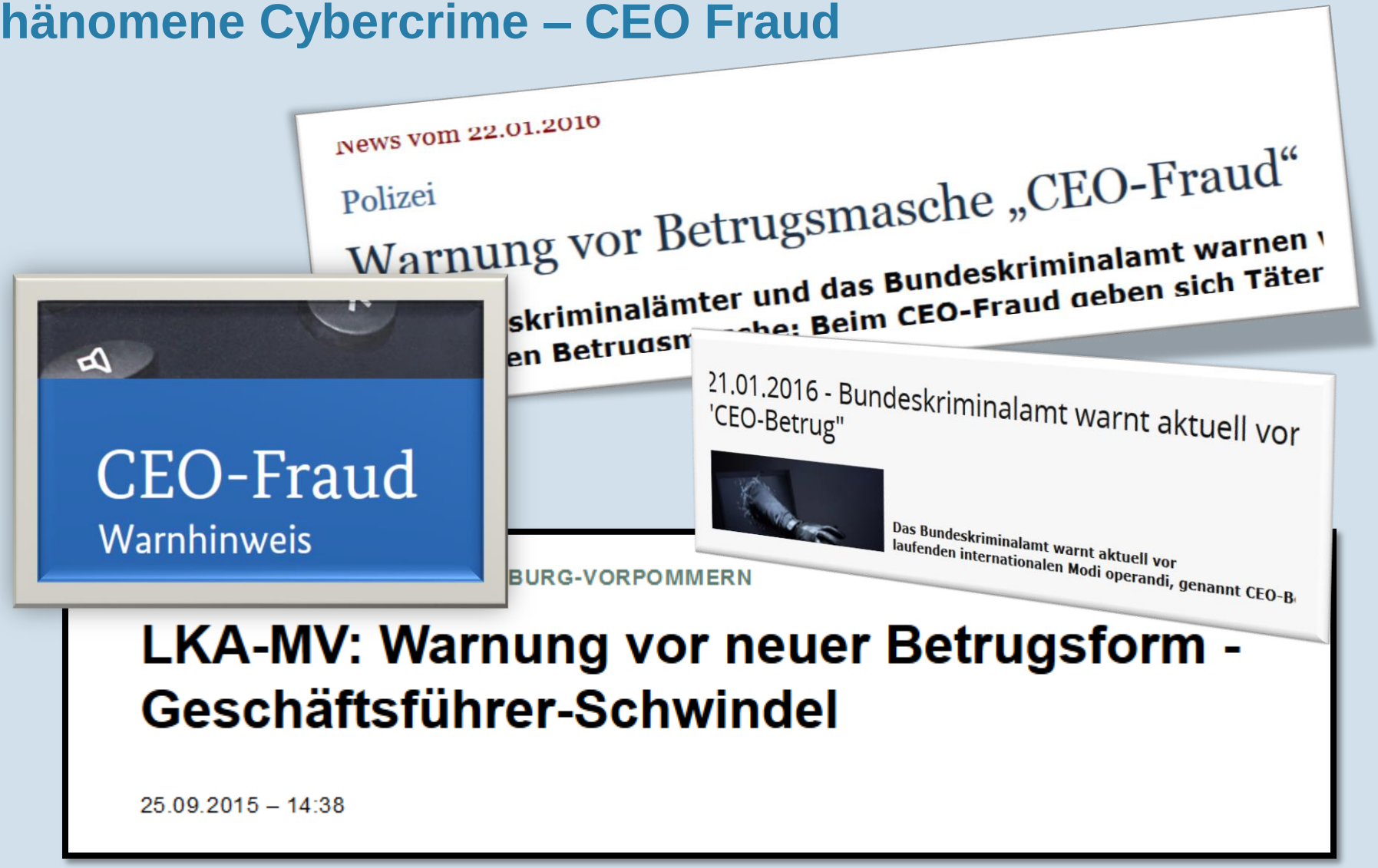
recovery+*.* ***.cerber** decrypt my file*.* help_file_*.* *.coverton *warning-!!*.* +recover+*.* _recover_*.* *rec0ver*.* _help_instruct*.*

Ransomware-Liste (Stand 29.03.2016)

Phänomene Cybercrime – Ransomware

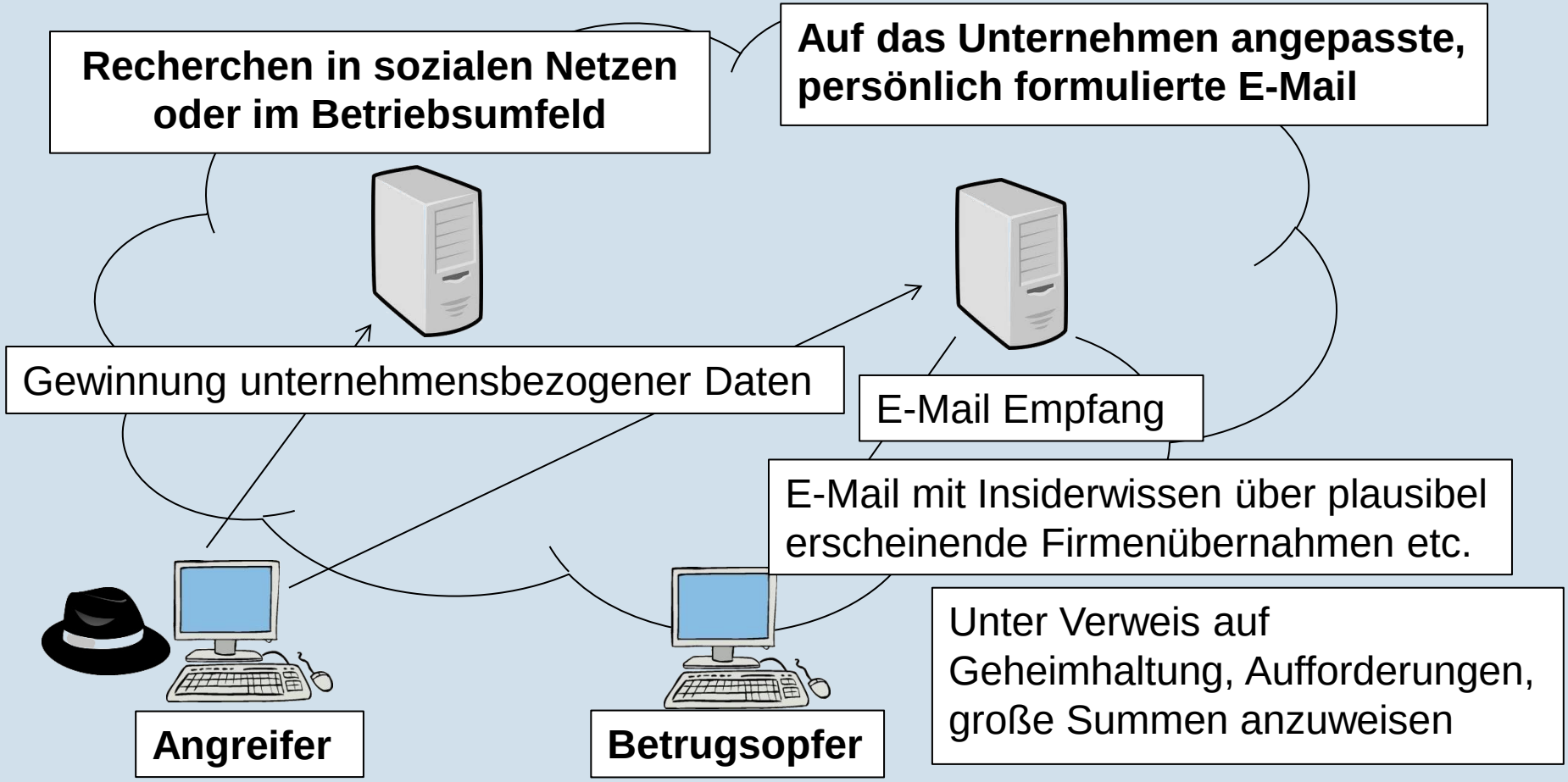
Hilfe durch nomoreransom.org

Phänomene Cybercrime – CEO Fraud



Phänomene Cybercrime – CEO Fraud

Begehungsweise schematisch



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.

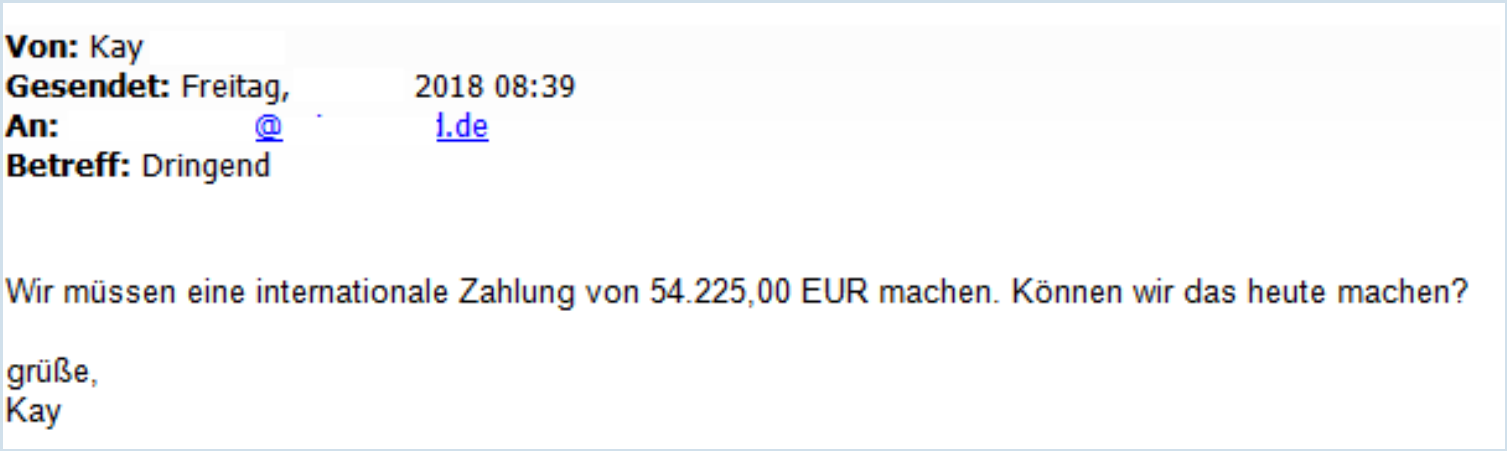
Mit freundlichen Grüßen,

[redacted]

Phänomene Cybercrime – CEO Fraud

Begehungsweise

- weiteres Beispiel:



Von: Kay
Gesendet: Freitag, 2018 08:39
An: @ l.de
Betreff: Dringend

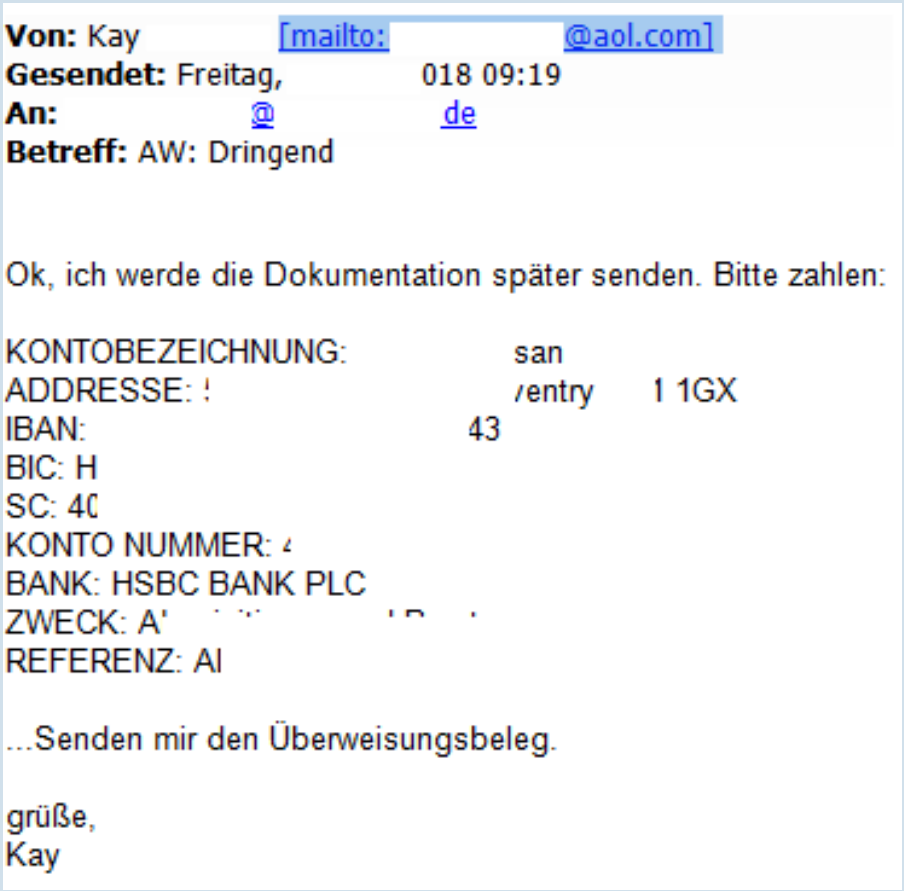
Wir müssen eine internationale Zahlung von 54.225,00 EUR machen. Können wir das heute machen?

grüße,
Kay

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

Phänomene Cybercrime – CEO Fraud

Begehungsweise



Von: Kay [mailto: @aol.com]
Gesendet: Freitag, 018 09:19
An: @ de
Betreff: AW: Dringend

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

KONTOBEZEICHNUNG: san
ADDRESSE: ! /entry 1 1GX
IBAN: 43
BIC: H
SC: 4(
KONTO NUMMER: 4
BANK: HSBC BANK PLC
ZWECK: A'
REFERENZ: Al

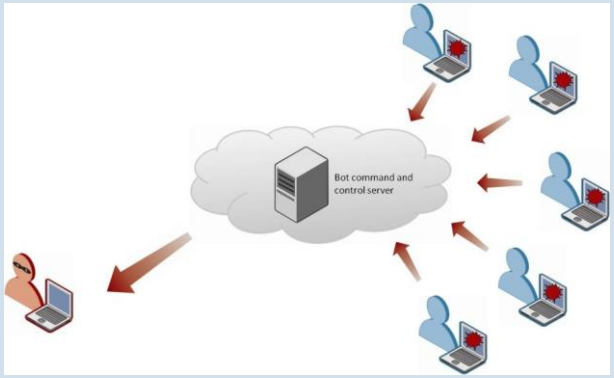
...Senden mir den Überweisungsbeleg.

grüße,
Kay

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

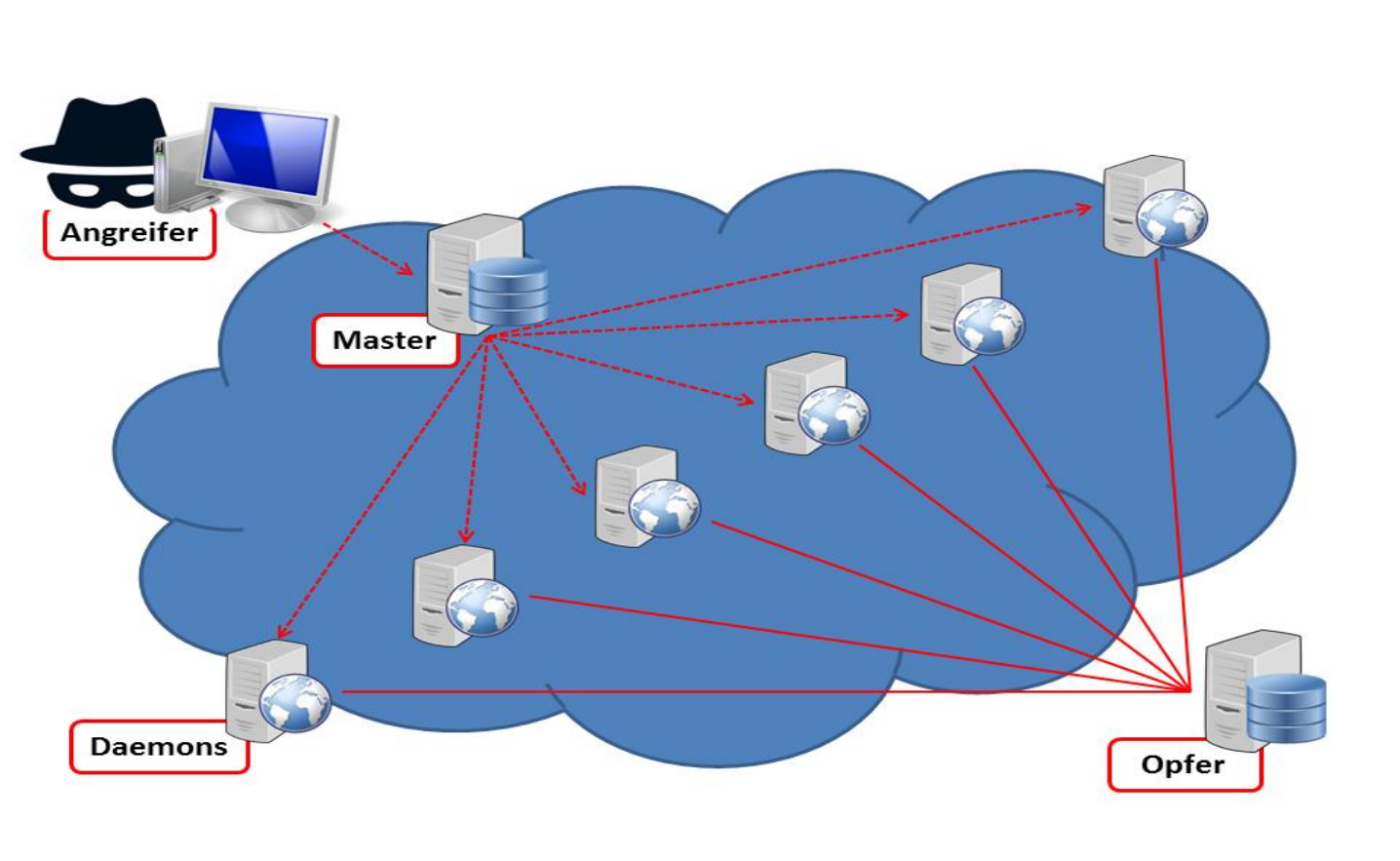
Phänomene Cybercrime – DDOS-Angriff

- **D**istributed **D**enial **o**f **S**ervice (Dienst- oder Serviceverweigerung)
- Durchführung über **Botnetz** (ferngesteuertes Netzwerk)
- Zusammenbruch des Servers (Serviceverweigerung)
- **angegriffene Webpräsenz somit nicht mehr über das Internet erreichbar**
- Versand von E-Mails mit Zahlungsaufforderung
- Forderung von **Bitcoins** o. ä.
- Bsp. Bitcoin-Adresse:
  1Ga2crn3wZEY6SdscmkPo67KouWVKhjtfR



Phänomene Cybercrime – DDOS-Angriff

Phänomenbeschreibung DDoS



4. Handlungsempfehlungen des LKA MV

Handlungsempfehlungen

Wichtig

- Regelmäßige Backup‘s (unabhängig vom Wirkbetriebsnetz)
- Überprüfung der Backup‘s und Training des Einspielens
- IT-Notfall Management (siehe IT- Sicherheitsvorfall)
- Patch Management (Systeme aktuell halten)
- Segmentierung der IT-Netze (Einsatz von Firewall‘s)
- Sensibilisierung der Mitarbeiter (alle „mitnehmen“ / Human Firewall / Fehlerkultur)
  (keine unglaubwürdigen E-Mail, Anhänge oder Links öffnen / Verschlüsselung)
- Eingeschränkte Benutzer- und Admin Rechte (Endziel 2FA)

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
- 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

5. IT-Sicherheitsvorfall als Prozess

IT- Sicherheitsvorfall: Prozess

IT-Sicherheitsvorfall (Phasen und Hilfspunkte)

- Vorbereitung auf einen Vorfall
- Identifizierung des Vorfalls/Sachverhalts
- Eindämmungsphase (Ausbreitung verhindern)
- Beseitigung/Bereinigung
- Wiederherstellung/Inbetriebnahme der Systeme
- „Lessons Learned“ - Erkenntnisse

IT- Sicherheitsvorfall

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

Identifizierung des Vorfalls/ 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

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

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 bösartigen Aktivitäten auf den betroffenen Systemen beseitigt?

IT- Sicherheitsvorfall

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

„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**?

6. Möglichkeiten LKA MV – ZAC MV

Angebot der ZAC MV

- **SPoC** für Wirtschaftsunternehmen
- **Vorträge** bei Kammerveranstaltungen
- **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, Erstatten 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 - 4545**

E-Mail: **cybercrime.lka@polmv.de**

Fragen?

Vielen Dank für Ihre Aufmerksamkeit ☺

CERT M-V
COMPUTER EMERGENCY RESPONSE TEAM
MECKLENBURG-VORPOMMERN

Vorstellung CERT M-V

CERT M-V
COMPUTER EMERGENCY RESPONSE TEAM
MECKLENBURG-VORPOMMERN

CIO M-V
Staatssekretärin
Ina-Maria Ulbrich

CISO
Steffen Tambach

CERT M-V

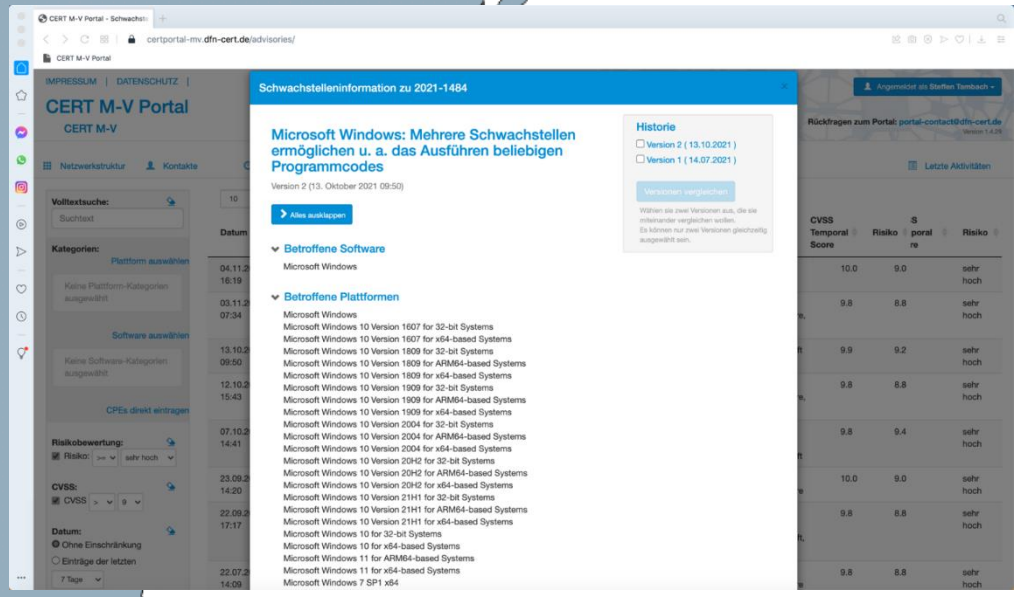
Das CERT M-V ist das CERT des Landes Mecklenburg-Vorpommern

- seit 2016 nach einer mehrjährigen Aufbau- und Pilotphase im Wirkbetrieb
- CERT-Modell: koordinierendes CERT mit aktuell 3 Personen, angesiedelt im Ministerium für Inneres, Bau und Digitalisierung
- Zielgruppen: Landes- und Kommunalverwaltung inkl. kommunale IT-Dienstleister M-V
- derzeitige CERT-interne Projekte:
  - Einführung Malware Information Sharing Plattform (MISP)
  - Einführung C&C-Erkennung (Threat Intelligence)
  - Prüfung Webpräsenzen

CERT M-V
COMPUTER EMERGENCY RESPONSE TEAM
MECKLENBURG-VORPOMMERN

Basisdienste des CERT M-V

Warn- und Informationsdienst (WID) inklusive Alarmierungsdiens



Bereitstellung einer Informationsplattform u. a. zu **Schwachstellen in Soft- und Hardwareprodukten**, aktuellen Bedrohungen und Angriffen auf den Sektor „Öffentliche Verwaltung“, Angriffsvektoren, ...)

CERT M-V
COMPUTER EMERGENCY RESPONSE TEAM
MECKLENBURG-VORPOMMERN

Basisdienste des CERT M-V

weitere Dienste

- Schadcodeanalyse u. a. in E-Mails (Phishingangriffe)
- Sicherheitsvorfallbehandlung
- Sicherheitstechnische Prüfung und Bewertung von Internetauftritten
- Bereitstellung von Informationen über Daten-Leaks
  (Politleak 2019 in Form eines Adventskalenders)

CERT M-V
COMPUTER EMERGENCY RESPONSE TEAM
MECKLENBURG-VORPOMMERN

Sicherheitsvorfallbehandlu

Anschlussbedingungen an das Landesdatennetz CN LAVINE, Punkt 7:

„Wird bei einem Teilnehmer ein IT-Sicherheitsvorfall mit Auswirkung auf die Informationssicherheit des Landesdatennetzes CN LAVINE bekannt oder entdeckt, so ist das CERT M-V unverzüglich zu informieren.“

CERT M-V
COMPUTER EMERGENCY RESPONSE TEAM
MECKLENBURG-VORPOMMERN

Kontaktdaten

Das CERT M-V ist über die nachstehenden Kontaktdaten:

Telefon: +49 (0) 385 588-11333

Fax: +49 (0) 385 509-11333

E-Mail: cert@mv-regierung.de

Threema: 7Z4HD79A, TFFNAPNJ, 3CMYJVTD

zu erreichen.