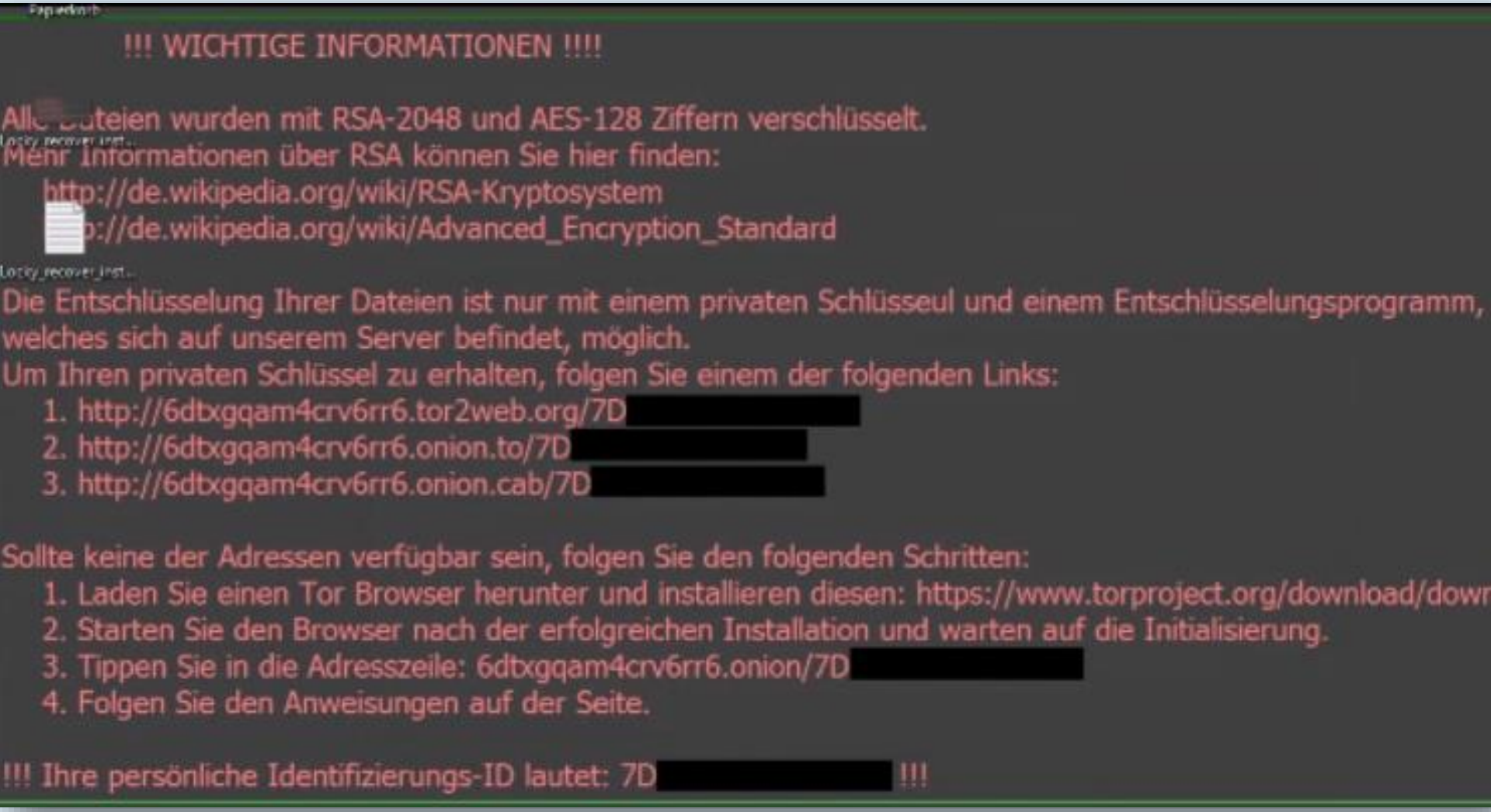
Landeskriminalamt
Mecklenburg-Vorpommern

Cybercrime – aktuelle Bedrohungslage mit Handlungsempfehlungen des LKA MV
CITS MV Cloud-IT-Sicherheit 08.09.2022

LKA MV, Projekt Digitales Service- und Kompetenzzentrum (DiSK)
Polizeirat 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 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[redacted]
2. http://6dtxgqam4crv6rr6.onion.to/7D[redacted]
3. http://6dtxgqam4crv6rr6.onion.cab/7D[redacted]

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[redacted]
4. Folgen Sie den Anweisungen auf der Seite.

!!! Ihre persönliche Identifizierungs-ID lautet: 7D[redacted] !!!

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

Inhalt / Übersicht

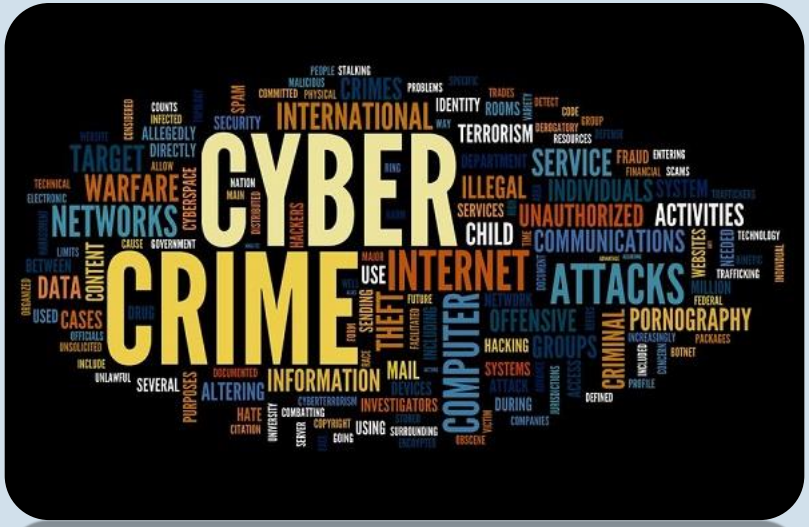
1. Vorbemerkungen
2. Zahlen, Daten, Fakten Cybercrime
3. Cybercrime Bekämpfung in Mecklenburg-Vorpommern
4. Ausgewählte Cybercrime-Phänomene
5. Handlungsempfehlungen LKA MV
6. IT-Sicherheitsvorfall als Prozess
7. Möglichkeiten LKA MV – ZAC MV

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 Hackern in einem Netz**
- Strafverfolgungsbehörden müssen technische Ermittlungsmaßnahmen durchführen/initiieren

Begriffsbestimmung

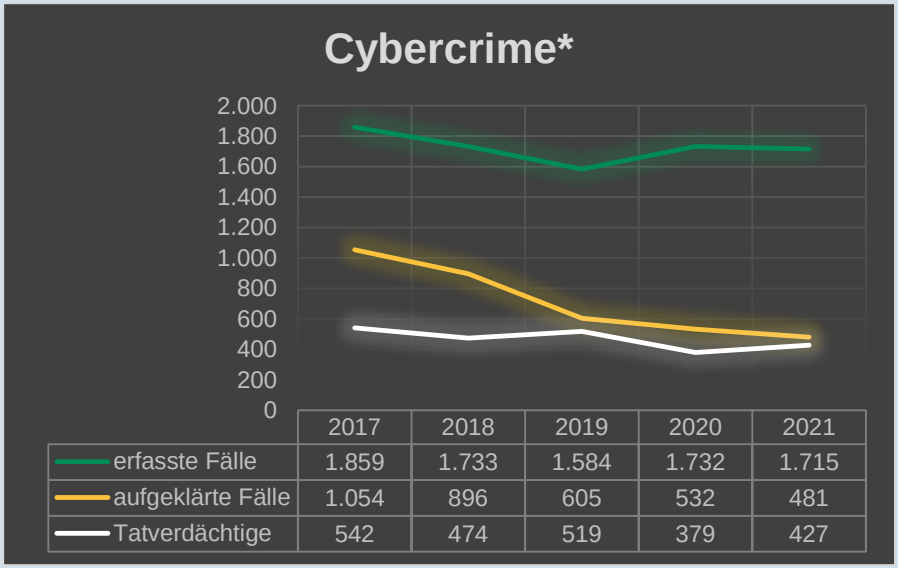


Quelle: Sondermeldedienst Cybercrime
Stand: 10.12.2012

- 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.

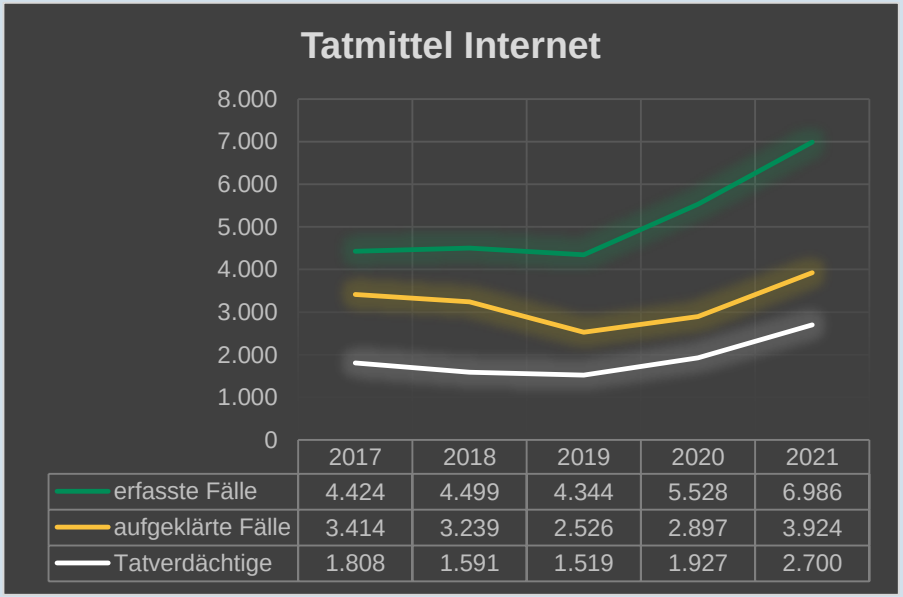
2. Zahlen, Daten, Fakten Cybercrime

Zahlen, Daten und Fakten



	2017	2018	2019	2020	2021
erfasste Fälle	1.859	1.733	1.584	1.732	1.715
aufgeklärte Fälle	1.054	896	605	532	481
Tatverdächtige	542	474	519	379	427

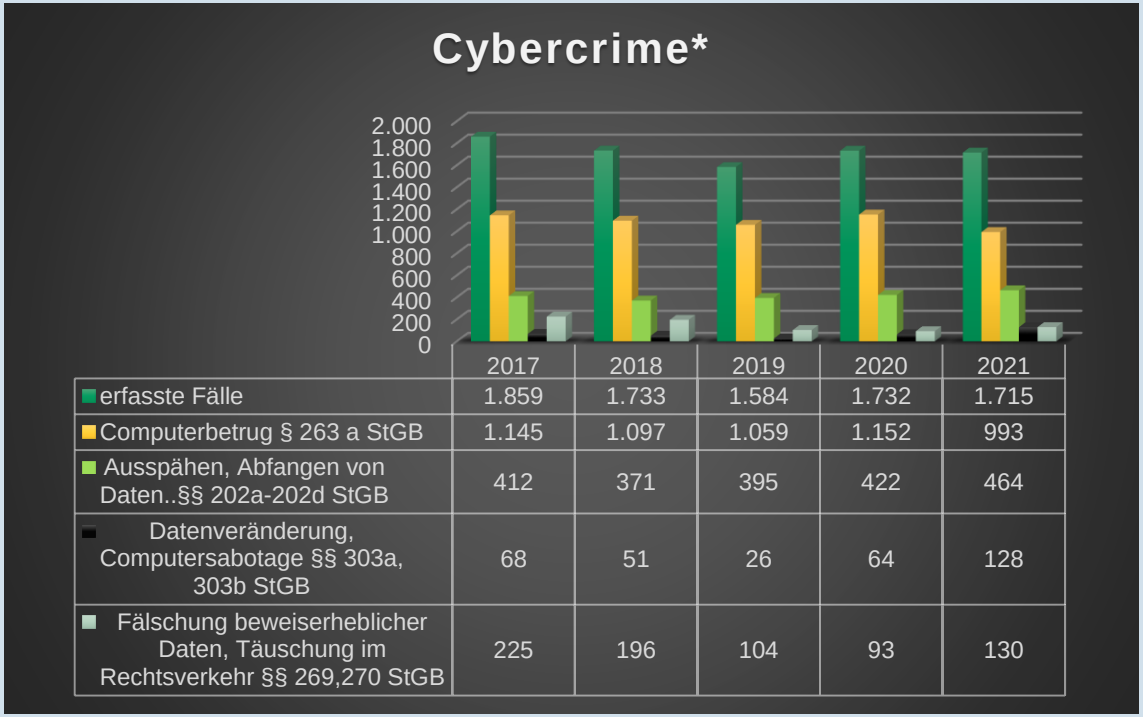
* Erfassung nur, wenn konkrete Anhaltspunkte für Tathandlung in Deutschland (PKS 2022: Umbenennung Computerkriminalität in Cybercrime)



	2017	2018	2019	2020	2021
erfasste Fälle	4.424	4.499	4.344	5.528	6.986
aufgeklärte Fälle	3.414	3.239	2.526	2.897	3.924
Tatverdächtige	1.808	1.591	1.519	1.927	2.700

Quelle: PKS MV

Zahlen, Daten und Fakten



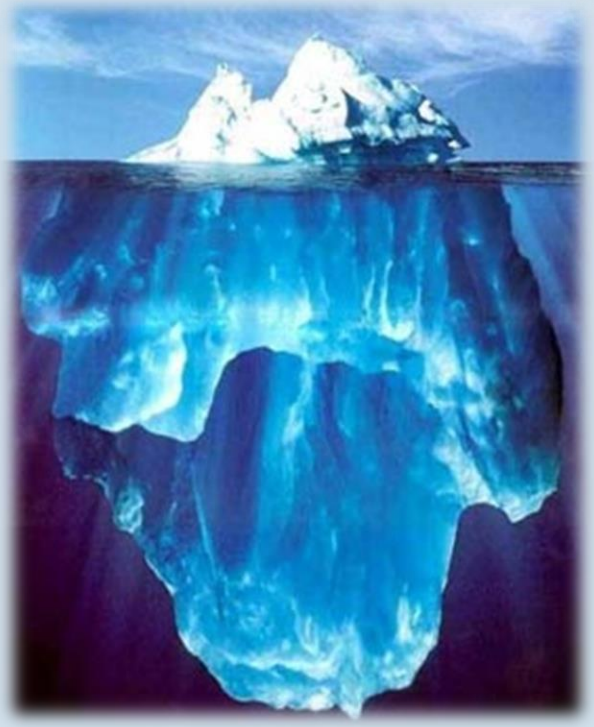
	2017	2018	2019	2020	2021
erfasste Fälle	1.859	1.733	1.584	1.732	1.715
Computerbetrug § 263 a StGB	1.145	1.097	1.059	1.152	993
Ausspähen, Abfangen von Daten..§§ 202a-202d StGB	412	371	395	422	464
Datenveränderung, Computersabotage §§ 303a, 303b StGB	68	51	26	64	128
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr §§ 269,270 StGB	225	196	104	93	130

* 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. *mögliche Gründe:*

- 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
- Flyer_Cyberattacken

Lage IT-Sicherheit (Studien-/Umfrageergebnisse)

Studie Digitalverband Bitcom (2018) – „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie“

- 68% Industrieunternehmen sind in den vergangenen 2 Jahren Opfer gewesen
- Schaden rund 43,4 Mrd. in den letzten 2 Jahren

Bundesamt für Sicherheit und Informationstechnik (BSI) – Cybersicherheitsumfrage (2018)

- 33% der befragten Organisationen von Cyber-Sicherheitsvorfällen betroffen
- 9 von 10 Institutionen (88%) erwarten durch Digitalisierung Verschärfung der Bedrohungslage

Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG – „e-Crime in der deutschen Wirtschaft 2019“

- 40% in den letzten 2 Jahren betroffen
- nur 40% der betroffenen Unternehmen haben Strafanzeige erstattet
- Schäden zwischen 20.000€ – 150.000€, aber auch vereinzelt 500.000€ und mehr

Lage IT-Sicherheit (Studien-/Umfrageergebnisse)

Unternehmensbefragung des Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) zur Cyberkriminalität (2020)

- Risiko von Cyberangriffen steigt, insbesondere durch Schadsoftware und Phishing
- IT-Sicherheit von Unternehmen durch die Corona-Krise beeinträchtigt (HO, VPN)
- **Hälfte** der Unternehmen schätzte Risiko eines schädigenden ungezielten Cyberangriffs als **sehr hoch/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.

Lage IT-Sicherheit (2021)

ZEIT ONLINE vom 09.05.2022

Zahl der Cyberangriffe erreicht 2021 neuen Höchstwert

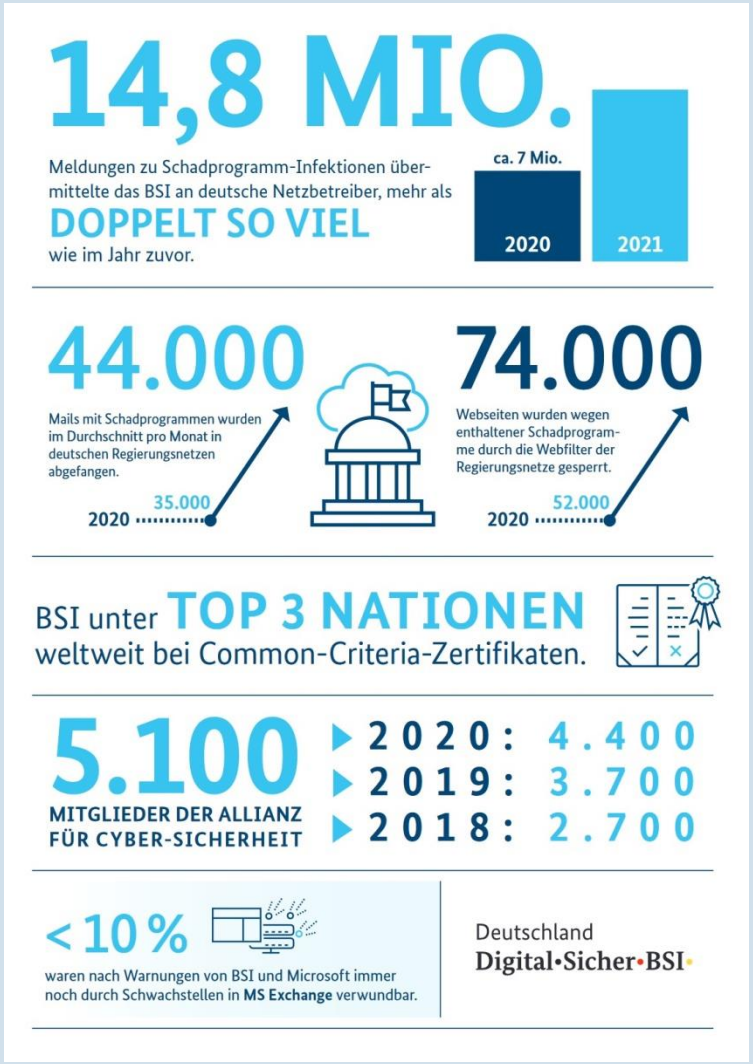
Deutschland ist **überdurchschnittlich stark von Cyberattacken betroffen**. Das liegt aber nicht an fehlenden Sicherheitsstandards, wie das Bundeskriminalamt berichtet. Die Zahl erfasster Cyberstraftaten hat im vergangenen Jahr einen neuen Höchstwert erreicht. Insgesamt wurden 146.363 Delikte erfasst, wie aus dem vom Bundeskriminalamt (BKA) veröffentlichten sogenannten Bundeslagebild Cybercrime hervorgeht. Im Vergleich zum Vorjahr **stieg** die Zahl der Straftaten im Bereich der Internetkriminalität um **mehr als zwölf Prozent**. Deutschland ist von Cyberattacken demnach überdurchschnittlich stark betroffen, was nach Einschätzung der Sicherheitsbehörden allerdings nicht daran liegt, dass es Hackern hierzulande durch schwache IT-Sicherheitsvorkehrungen leichter gemacht wird als anderswo, sondern schlicht daran, dass **Deutschland** wohl als **"lukratives Angriffsziel„** gelte, sagte die Vizepräsidentin des BKA, Martina Link.

Vor allem im Bereich Ransomware und bei DDoS-Angriffen sei ein starker Zuwachs festgestellt worden. Als Ransomware werden Schadprogramme bezeichnet, die bei den Opfern den Zugriff auf Daten und Systeme einschränken oder verhindern, indem sie beispielsweise alle Festplatten verschlüsseln. Für die Entschlüsselung verlangen die Angreifer dann ein Lösegeld, im Englischen ransom. Bei DDoSAttacken, was für Distributed Denial of Service steht, versuchen Angreifer, Server mit einer Flut von Anfragen lahmzulegen. Im vergangenen Sommer waren nach einem DDoS-Angriff auf einen deutschen IT-Dienstleister für Banken teilweise Websites, Onlinebanking und weitere Dienste vorübergehend nicht erreichbar oder nur eingeschränkt nutzbar. Zu den relevantesten Angriffen zählte das BKA auch eine Attacke mit der Ransomware Conti vom November. Hier traf es dem Lagebild zufolge ein Unternehmen, dessen Software in etwa einem Viertel der deutschen Arztpraxen verwendet wird.

Die Kriminalität verlagert sich ins Digitale. Dass die Zahl der Cyberangriffe zunehme, während die Zahl der Straftaten insgesamt rückläufig sei, wertete die BKA-Vizepräsidentin als "Ausdruck der **fortschreitenden Verlagerung von Kriminalität in den digitalen Raum**". Die zunehmende Verzahnung internationaler Lieferketten sowie die durch die Corona-Pandemie beschleunigte Digitalisierung schaffe für Cyberkriminelle neue Tatgelegenheiten. **Betroffen** ist von dieser Art von Kriminalität **fast jede Branche**. Die Täter agieren dabei mit "**zunehmender Professionalität und hochgradig arbeitsteilig**". Der Angriffskrieg Russlands gegen die Ukraine und dabei eingesetzte hybride Angriffsformen haben dem Lagebild nach das Potenzial, "als weiterer Katalysator für Cybercrime zu dienen". Die Aufklärungsquote lag mit 29,3 Prozent weiterhin auf einem "niedrigen Niveau". Dafür sind den Ermittlern zufolge unter anderem die **verstärkte Anonymisierung im Netz** sowie die komplexe Ermittlung von im Ausland befindlichen Tätern verantwortlich. Der Bereich der Internetkriminalität ist zudem weiter von einem "**überdurchschnittlich großen Dunkelfeld**" geprägt, weil Straftaten sehr häufig nicht angezeigt werden. "Das Bundeslagebild zeigt, dass die Bedrohungslage durch Cybercrime weiterhin sehr hoch ist", sagte Link.

Mecklenburg-Vorpommern

Lage IT-Sicherheit (2021)



Lage 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."

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 **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*

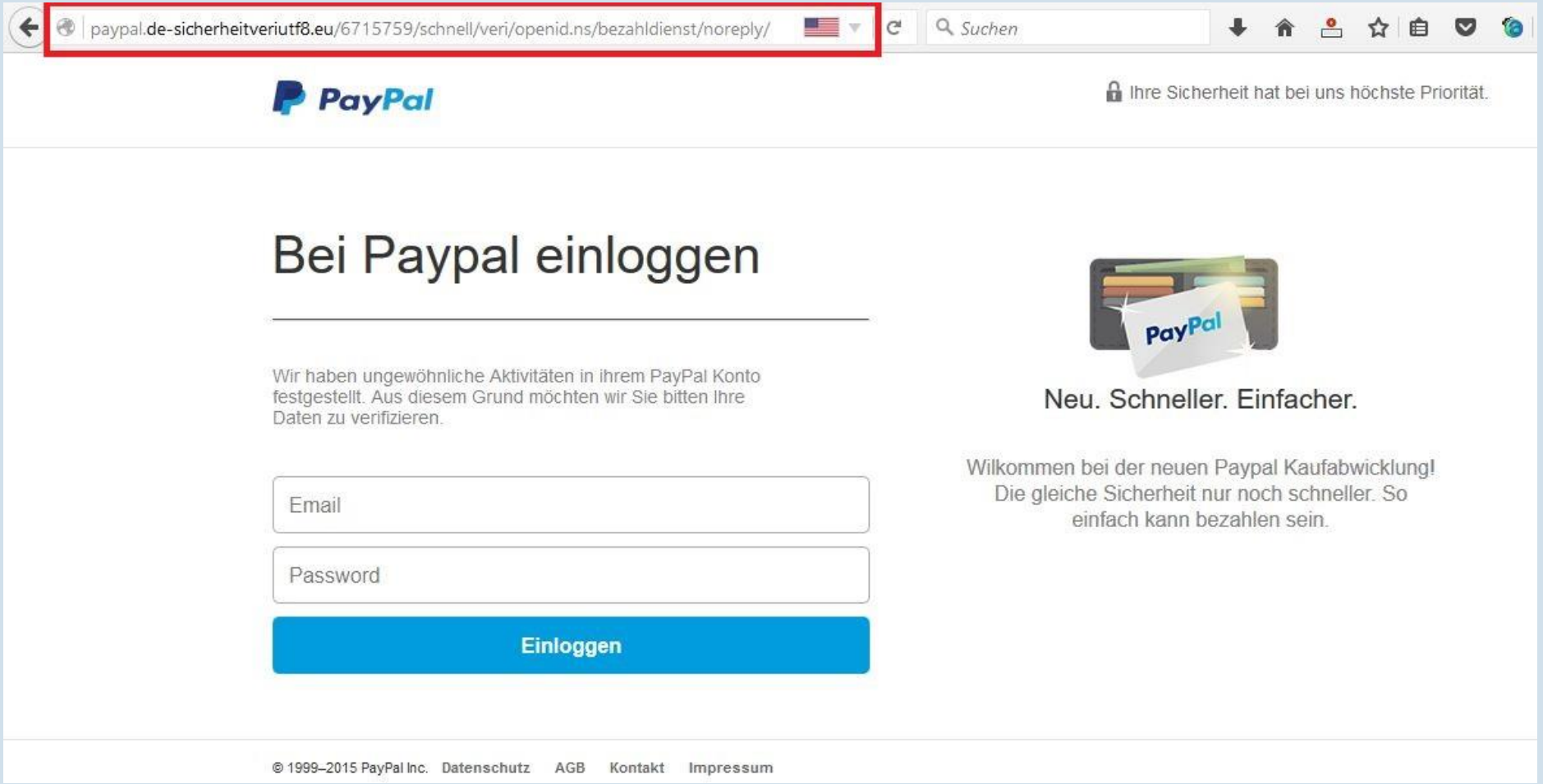
[2] *Wirtschaftskriminalität/Cybercrime*

4. Ausgewählte Cybercrime-Phänomene

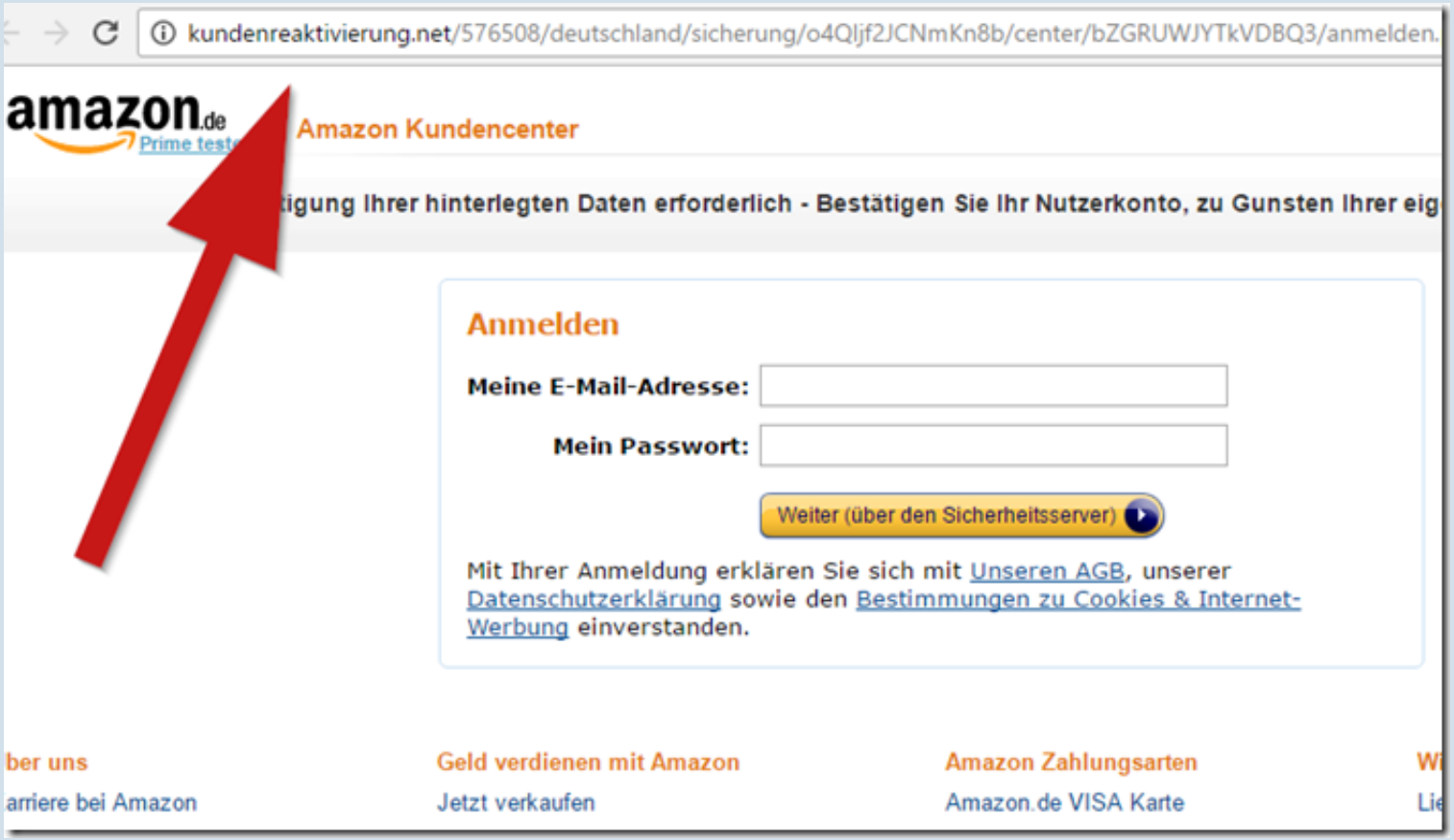
Phänomene Cybercrime

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

Phänomene Cybercrime – Phishing



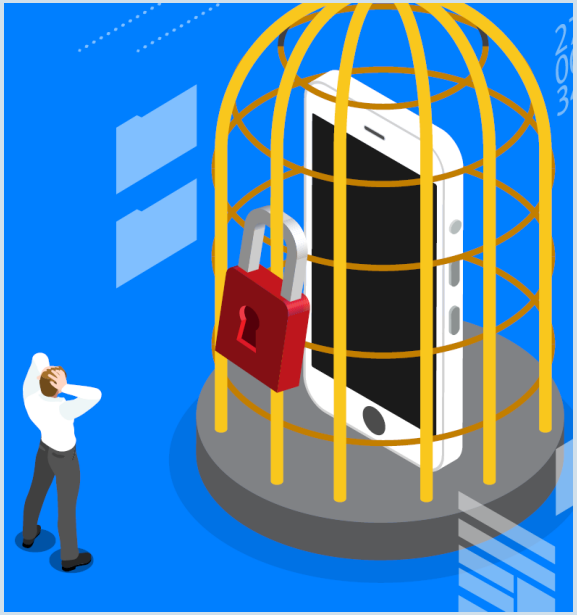
Phänomene Cybercrime – Phishing



Phänomene Cybercrime – Ransomware

Verschlüsselungstrojaner

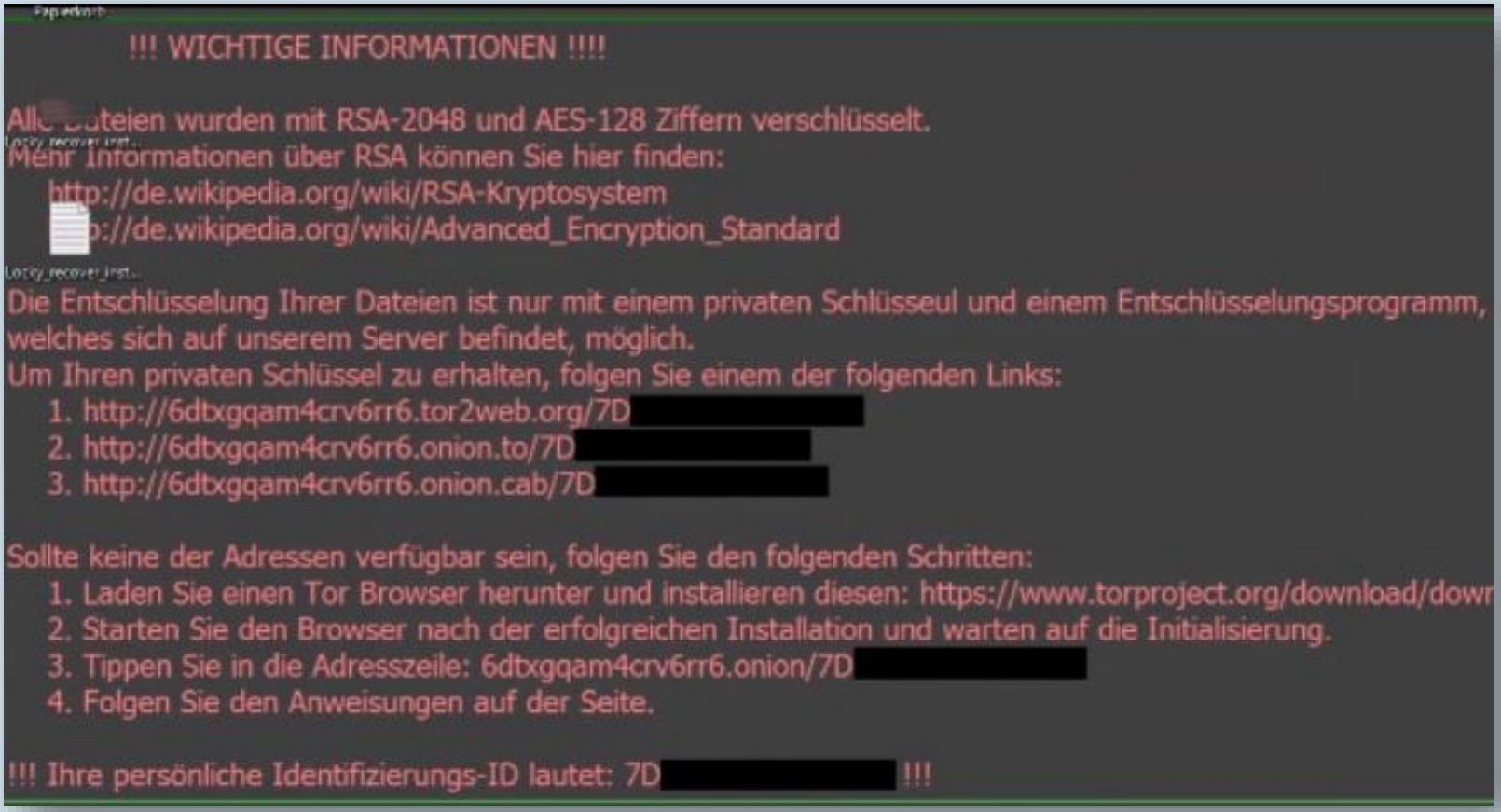
- seit 2014/2015 verstärkt bundesweite und internationale Verbreitung
- Verbreitung durch: E-Mail, beim Surfen, Handy-Apps
- **Risiken: Rechner wird gesperrt, Daten werden verschlüsselt, finanzielle Einbußen**
- **zur Entsperrung/Entschlüsselung wird Lösegeld (Ransom) verlangt**
- in Undergroundforen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



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

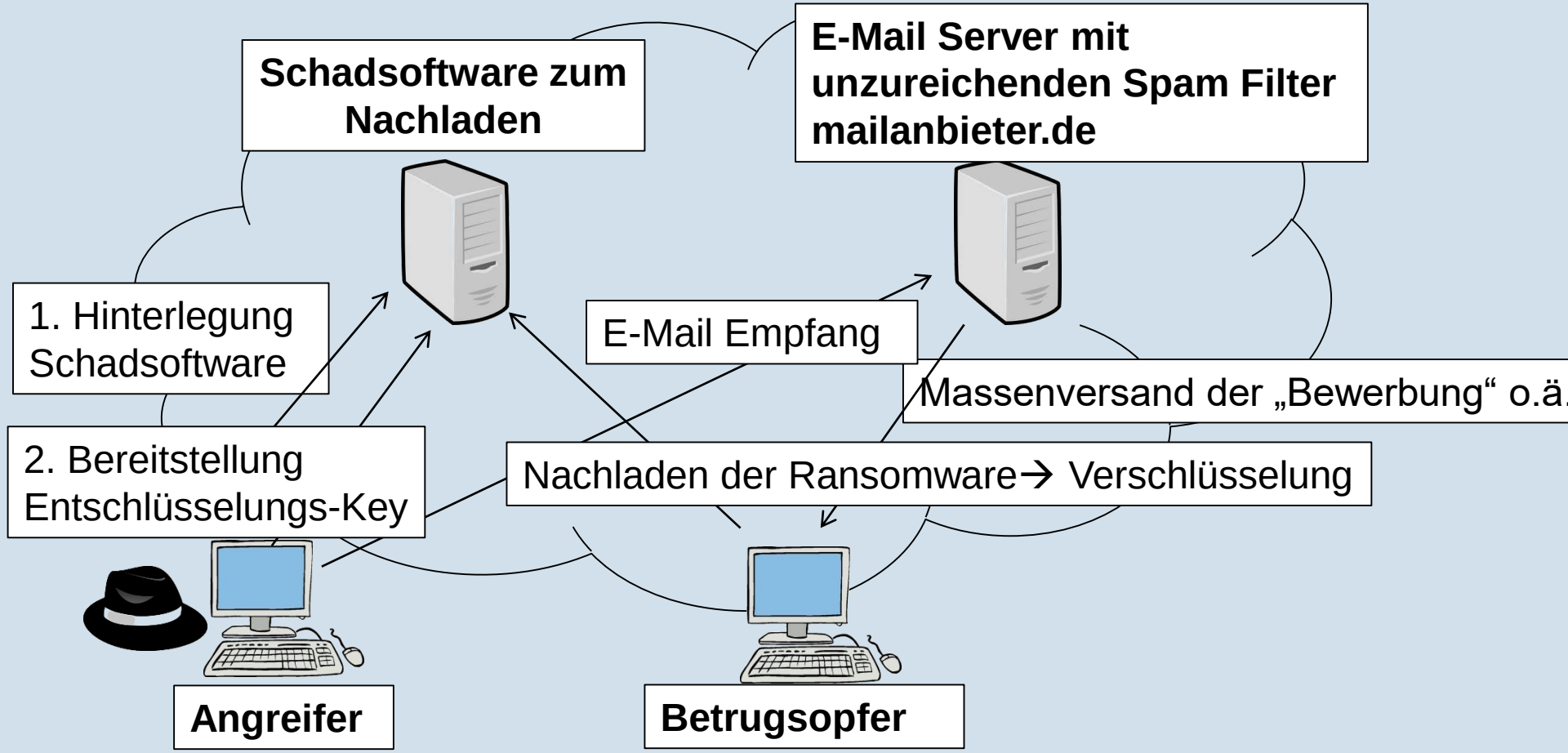
Phänomene Cybercrime – Ransomware

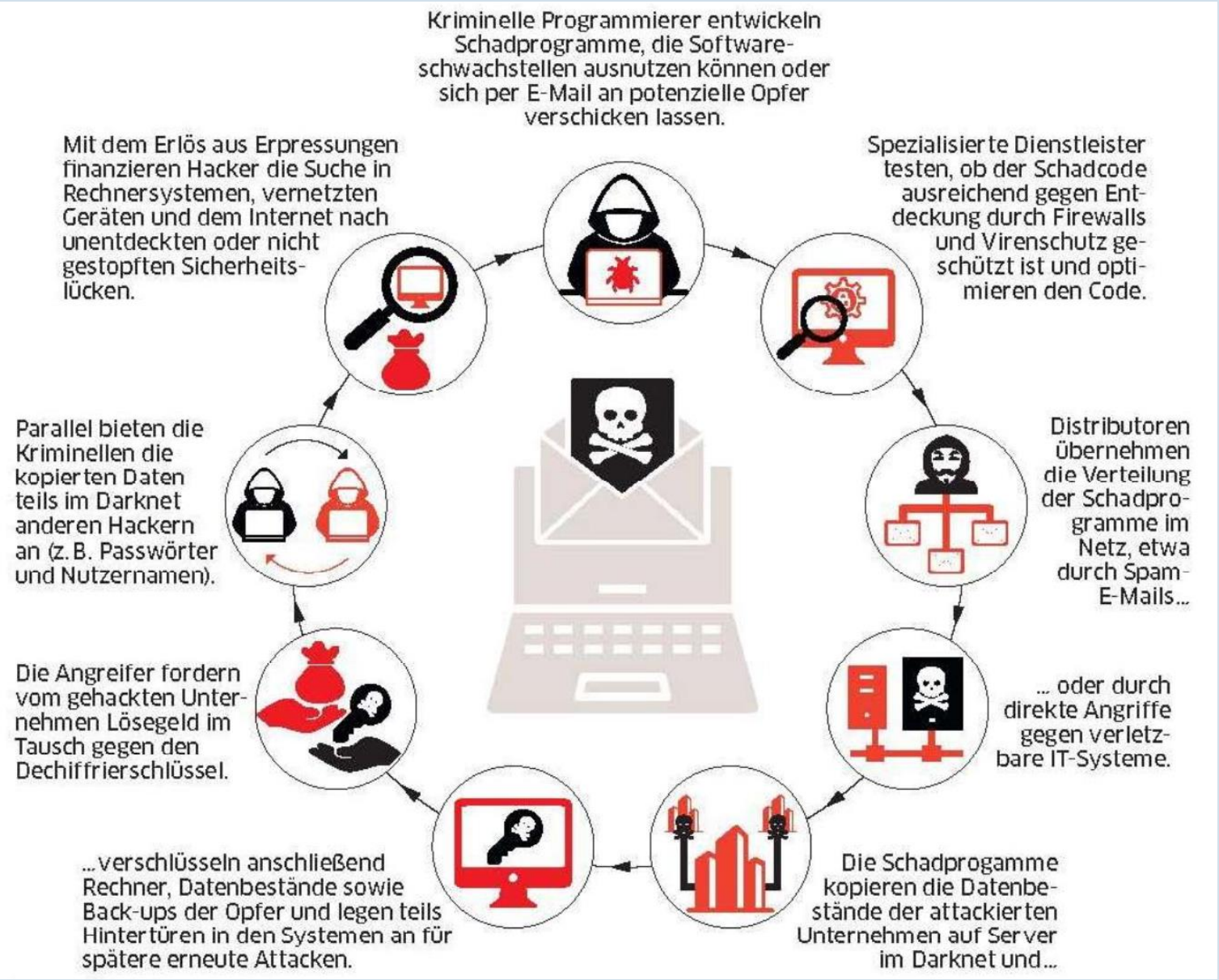
Lösegeldaufforderung nach Infektion



Phänomene Cybercrime – Ransomware

Verschlüsselungstrojaner




Kriminelle Programmierer entwickeln Schadprogramme, die Software-schwachstellen ausnutzen können oder sich per E-Mail an potenzielle Opfer verschicken lassen.
Spezialisierte Dienstleister testen, ob der Schadcode ausreichend gegen Entdeckung durch Firewalls und Virenschutz geschützt ist und optimieren den Code.
Distributoren übernehmen die Verteilung der Schadprogramme im Netz, etwa durch Spam-E-Mails...
... oder durch direkte Angriffe gegen verletzbare IT-Systeme.
Die Schadprogamme kopieren die Datenbestände der attackierten Unternehmen auf Server im Darknet und...
...verschlüsseln anschließend Rechner, Datenbestände sowie Back-ups der Opfer und legen teils Hintertüren in den Systemen an für spätere erneute Attacken.
Die Angreifer fordern vom gehackten Unternehmen Lösegeld im Tausch gegen den Dechiffrierschlüssel.
Parallel bieten die Kriminellen die kopierten Daten teils im Darknet anderen Hackern an (z. B. Passwörter und Nutzernamen).
Mit dem Erlös aus Erpressungen finanzieren Hacker die Suche in Rechnersystemen, vernetzten Geräten und dem Internet nach unentdeckten oder nicht gestopften Sicherheitslücken.

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

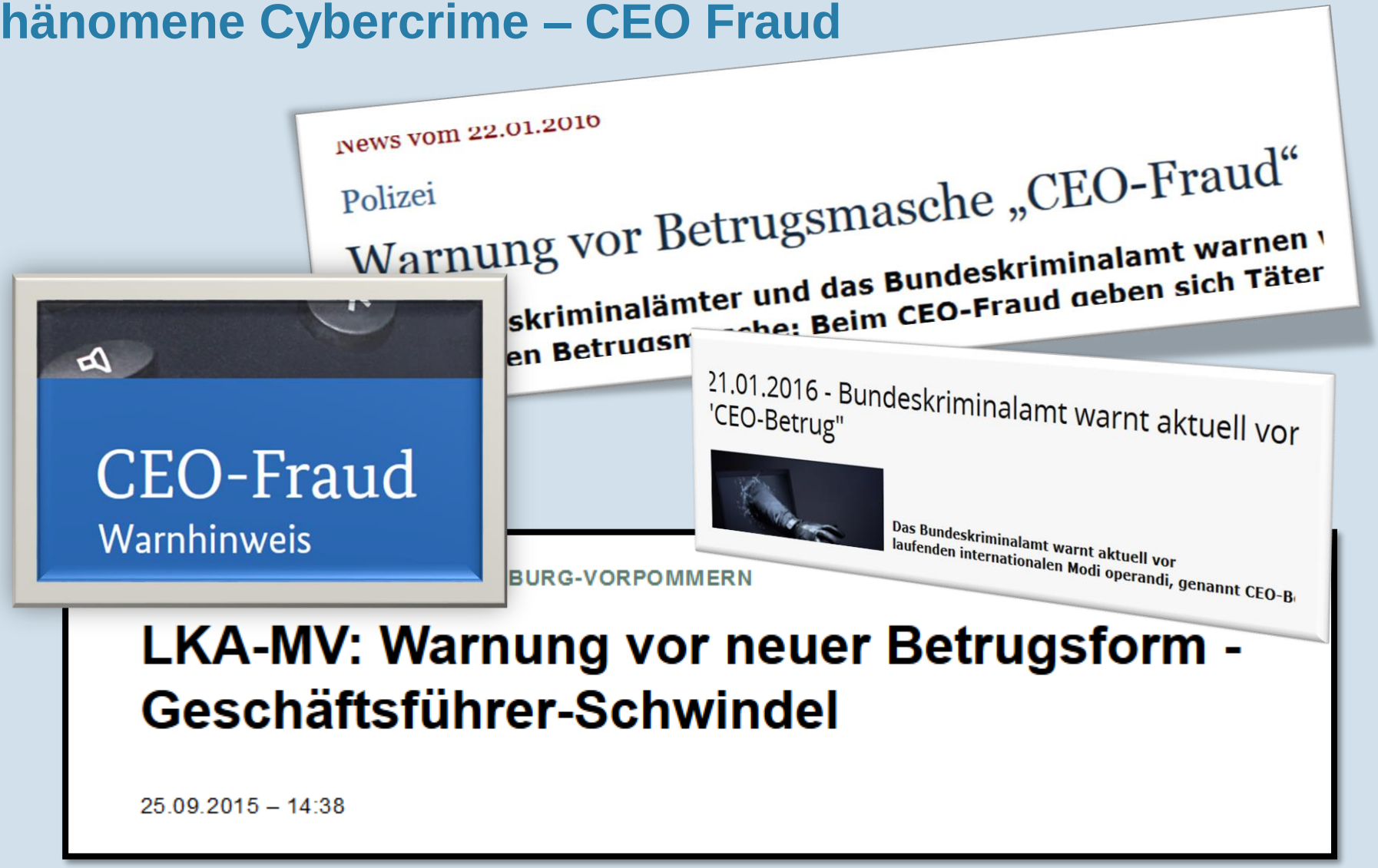
recovery+*.* ***.cerber** decrypt my file*.* help_file_*.* *.coverton *warning-!!*.* +recover+*.* _recover_*.* *rec0ver*.* _help_instruct*.*

Ransomware-Liste (Stand 29.03.2016)

Phänomene Cybercrime – Ransomware

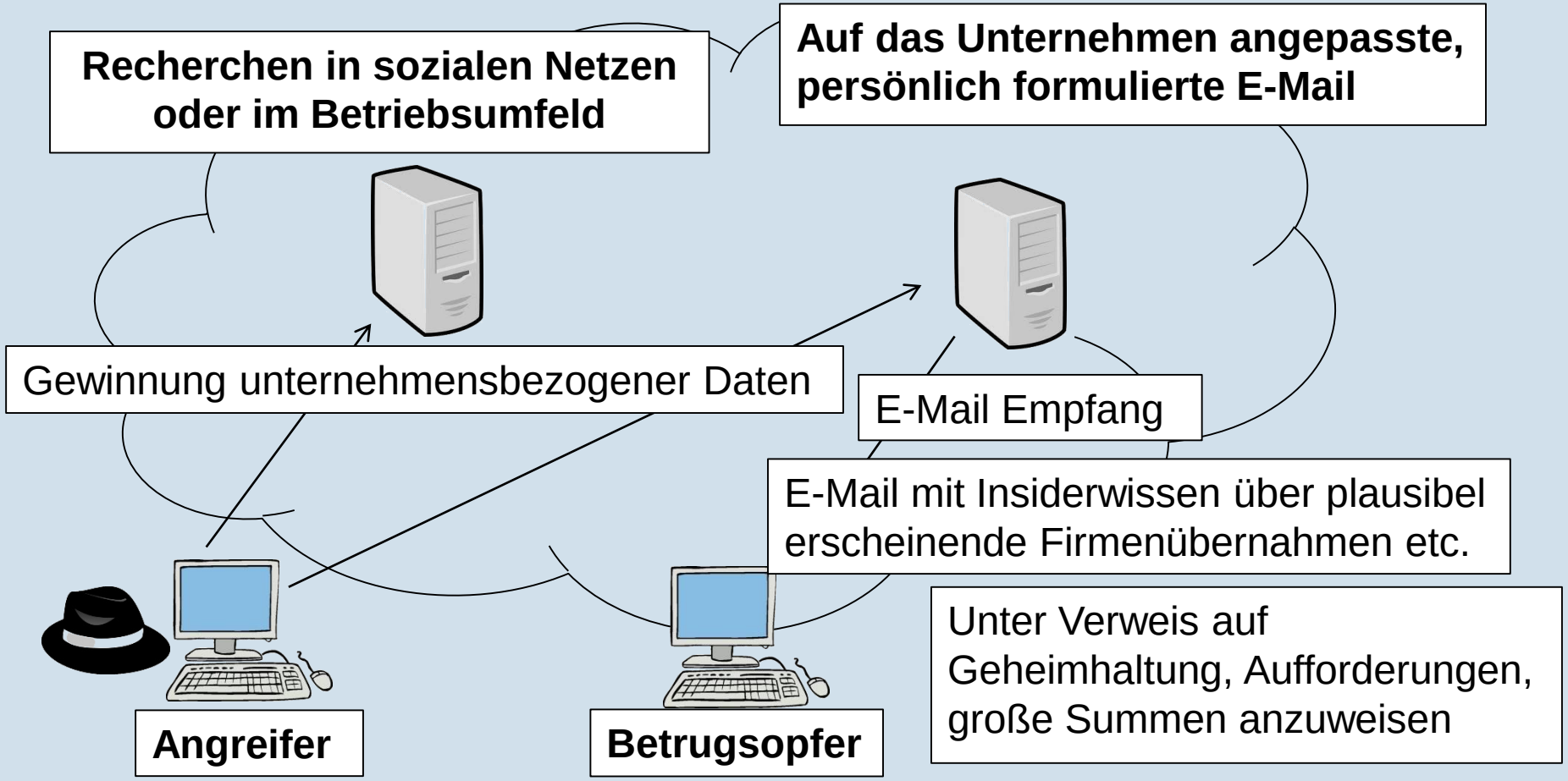
Hilfe durch nomoreransom.org

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.

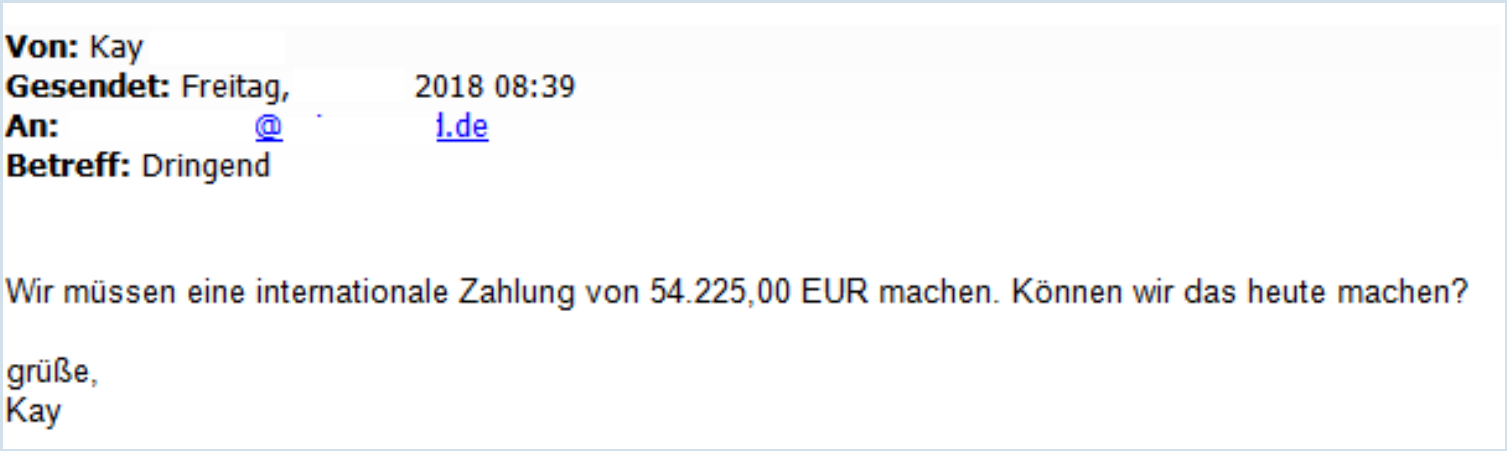
Mit freundlichen Grüßen,

[redacted]

Phänomene Cybercrime – CEO Fraud

Begehungsweise

- weiteres Beispiel:



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

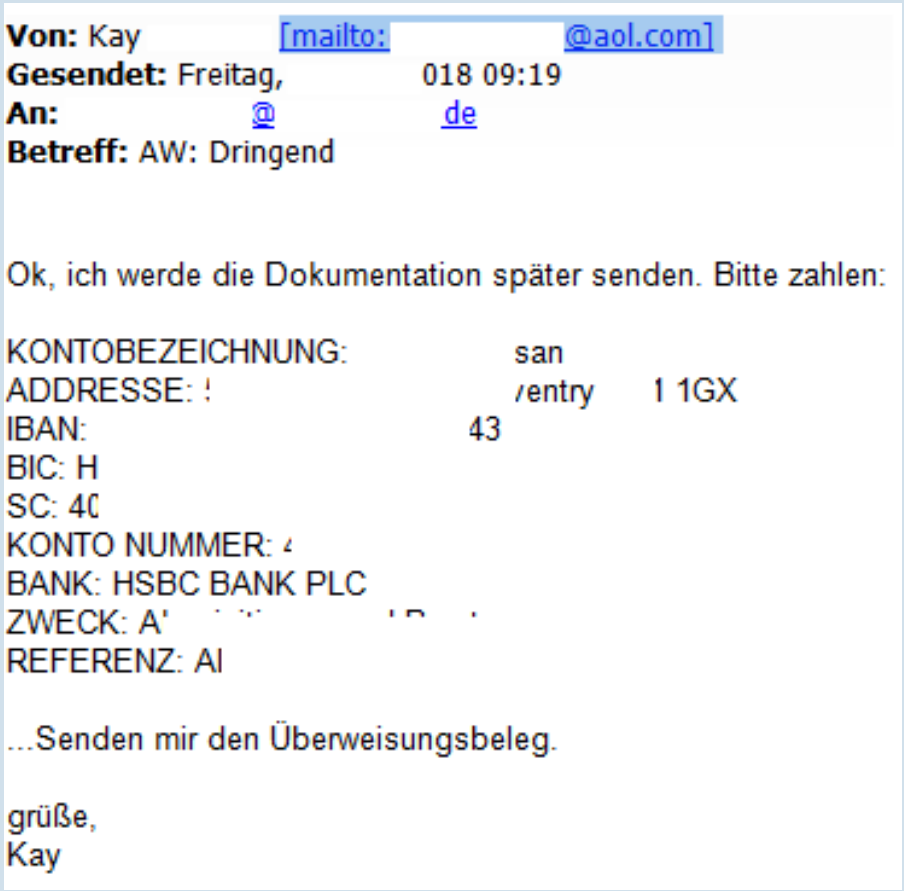
Wir müssen eine internationale Zahlung von 54.225,00 EUR machen. Können wir das heute machen?

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.

5. Handlungsempfehlungen des LKA MV

Handlungsempfehlungen

Wichtig - es gibt nicht nur <u>den einen</u> Tipp

- 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 / Passwortsicherheit

Für Anwender:

- Empfehlung: Passwortmanager (z.B. KeePassXC) ggf. in Kombination mit Passphrase (mehrere Wörter hintereinander)
- 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 (z.B. mittels haveibeenpwned.com)
- geeignetes Hash-Verfahren (z.B. scrypt oder Argon2) mit Salt verwenden zum Speichern der PWs, ggf. Zero-Knowledge-Proof-Verfahren implementieren
- 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

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

Handlungsempfehlungen

E-Mail-Sicherheit → Schutz vor Spoofing, Phishing und Fälschung

SPF

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

DKIM

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

6. IT-Sicherheitsvorfall als Prozess

IT- Sicherheitsvorfall: Phasen

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-Sicherheits-Vorfall (Kreislauf)
01
Vorbereitung
auf einen Vorfall
02
Vorfall
Identifizierung des Sachverhalts
03
Eindämmungs-phase
04
Beseitigung / Bereinigung
05
Wiederher-stellung
der Systeme
06
Erkenntnisse
"Lesson Learned"

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**?

7. 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 - 9494**

E-Mail: **zac@lka-mv.de**

Fragen?

Vielen Dank für Ihre Aufmerksamkeit

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

Polizeirat Maik Schröder, LKA MV - Leiter Dezernat –Cybercrime