POLIZEI
SACHSEN-ANHALT

Landeskriminalamt

Mathias Matschoß

M.Sc. IT Governance, Risk and Compliance Management

ZAC - Zentrale Ansprechstelle Cybercrime für die Wirtschaft

Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

CYBERCRIME

Bedrohungen

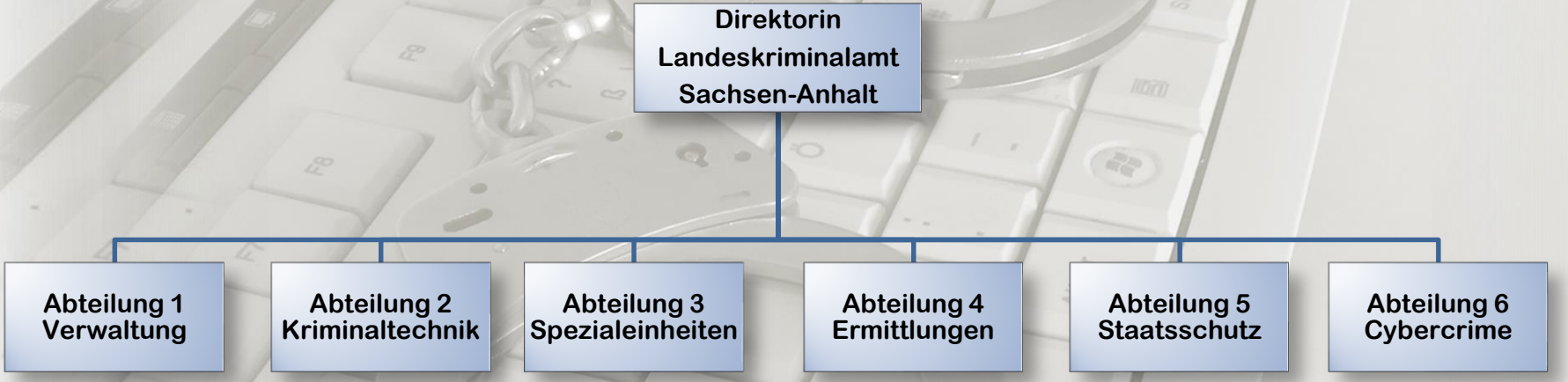
Erscheinungsformen

Abwehr

„ Impulsvortrag - Landespräventionsrat“
10. November 2021

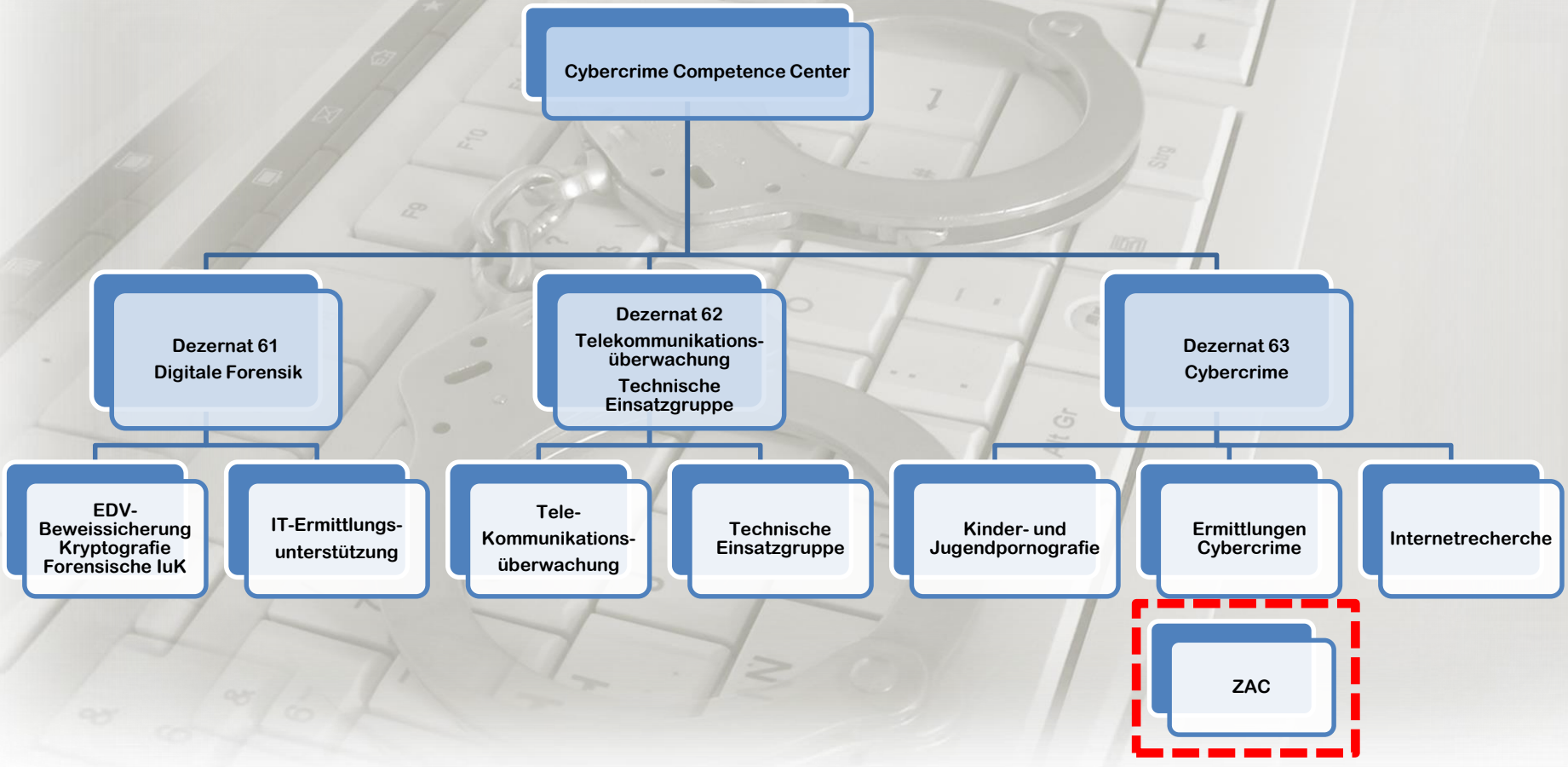
POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Landeskriminalamt Sachsen-Anhalt



POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Cybercrime Competence Center



POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

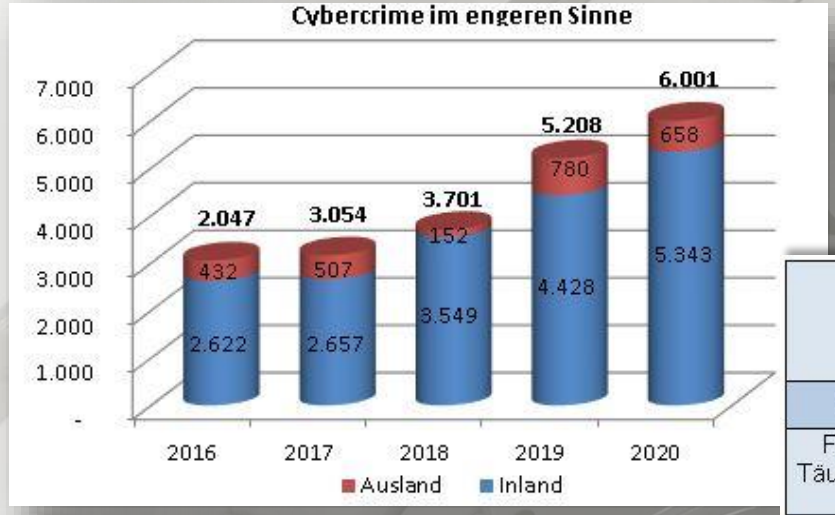
Entwicklung der Cybercrime im Überblick

	2019	2020	Vergleich in %	Tendenz
Straftaten Cybercrime im engeren Sinne	4.067	4.914	+20,8	↗
Straftaten Tatmittel Internet	12.816	15.286	+19,3	↗
Schäden in Euro Cybercrime im engeren Sinne	3.035.615	2.590.135	-14,7	↘

Quelle: PKS - Polizeiliche Kriminalstatistik 2020

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Fallentwicklung Cybercrime 2020



Cybercrime im engeren Sinn

Schwerpunkte

Straftaten(-gruppen)	erfasste Fälle in der PKS		Vergleich	
	2019	2020	Steigerung/Verringerung absolut	%
alle Arten des Computerbetrugs	3.520	4.260	+740	+21,0
Fälschung beweiserheblicher Daten Täuschung im Rechtsverkehr bei Datenverarbeitung	127	87	-40	-31,5
Datenveränderung/Computersabotage	108	82	-26	-24,1
Ausspähen/Abfangen von Daten	673	914	+241	+35,8
gesamt	**4.428**	**5.343**	**+915**	**+20,7**

Aufklärungsquote

2016	2017	2018	2019	2020
47,9 %	39,0 %	43,6 % (21%)	32,8 % (31%)	31,1 % (7,1%)

Quelle: PKS - Polizeiliche Kriminalstatistik 2020

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Fallentwicklung Cybercrime 2020

Quelle: PKS - Polizeiliche Kriminalstatistik 2020

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Fallentwicklung Cybercrime 2020

Cybercrime im weiteren Sinn

Schwerpunkte

Straftaten(-gruppen)	erfasste Fälle		Vergleich	
	2019	2020	Steigerung/Verringerung absolut	%
sonstiger Waren- und Warenkreditbetrug	6.376	7.468	+1.092	+17,1%
Beleidigung	326	448	+122	+37,4%
Geldwäsche	108	75	-33	-30,6 %
Erpressung	323	155	-168	-52,0 %
sonstige Straftaten	5.683	7.140	+1.457	+25,64%

Aufklärungsquote

2016	2017	2018	2019	2020
66,7 %	64,0 %	64,4 %	54,7 %	51,0 %

Quelle: PKS - Polizeiliche Kriminalstatistik 2020

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Deliktisches Dunkelfeld

Defizitäres Anzeigenaufkommen, weil

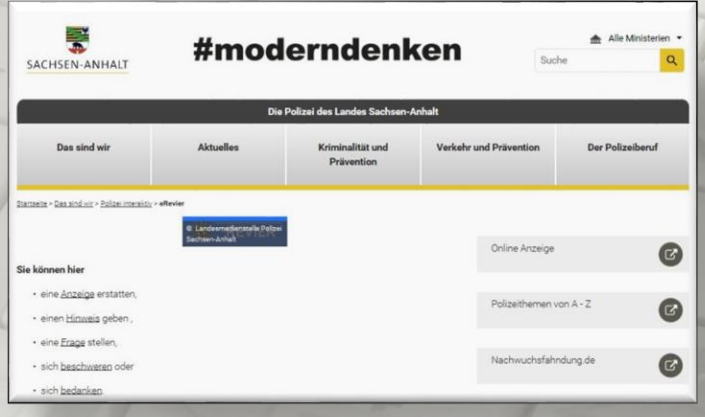
- Opfer bemerkt Schädigung nicht
- keine finanziellen Schäden
- befürchteter Imageschaden
- persönlicher Aufwand als unverhältnismäßig hoch eingeschätzt wird
- vermutete Erfolglosigkeit polizeilicher Ermittlungen

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Deliktisches Dunkelfeld

www.polizei.de

https://polizei-web.sachsen-anhalt.de/



https://polizei-web.sachsen-anhalt.de/das-sind-wir/polizei-interaktiv/erevier/

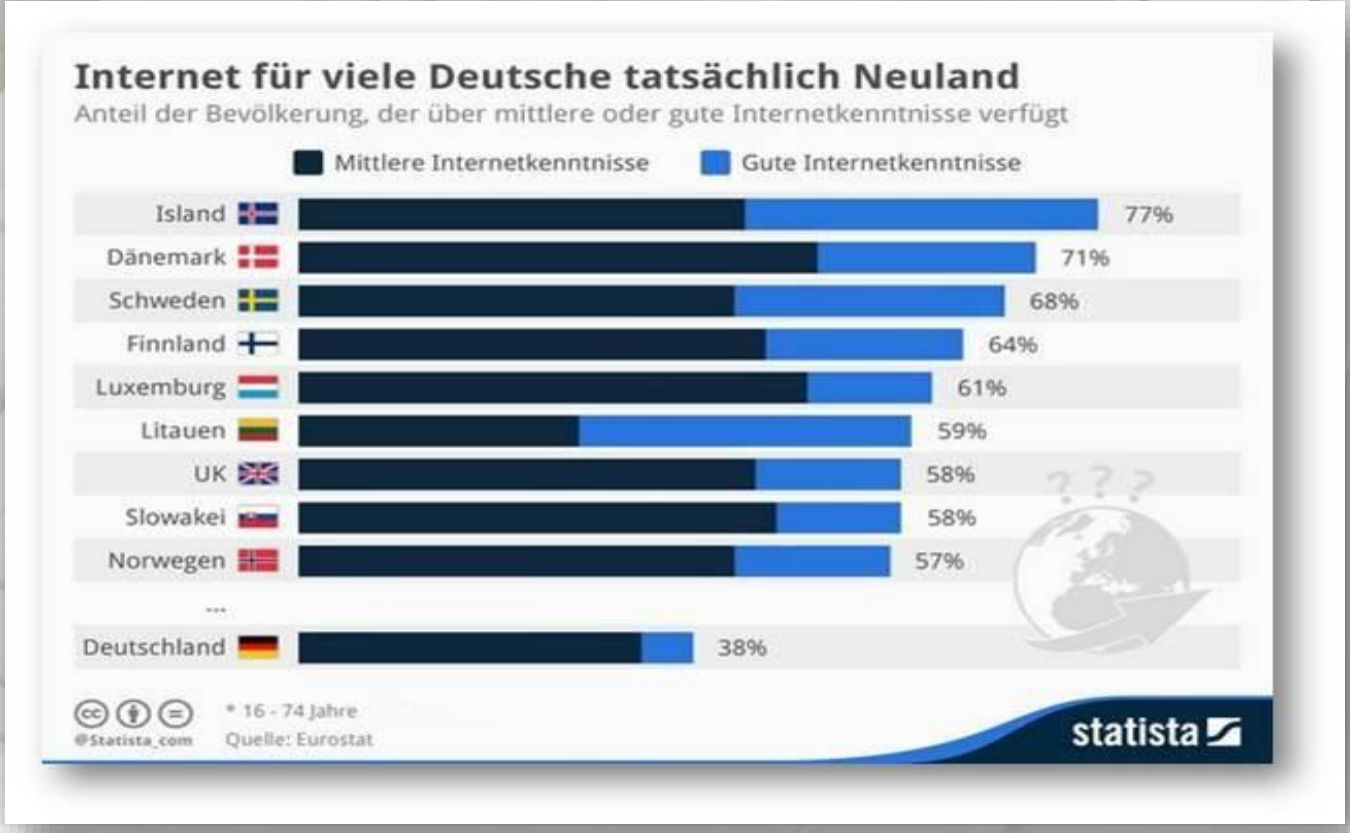
POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

„Digitale Verwundbarkeit trifft vielerorts auf digitale Sorglosigkeit“

(BSI)

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Verhaltensprävention ist genau so wichtig wie technische Prävention

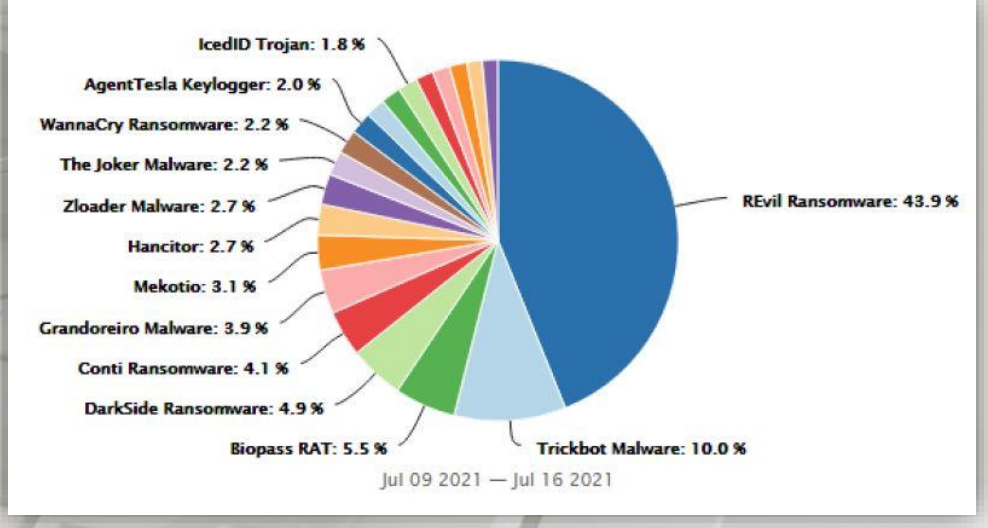


POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Aktuelle Cybercrimetrends

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

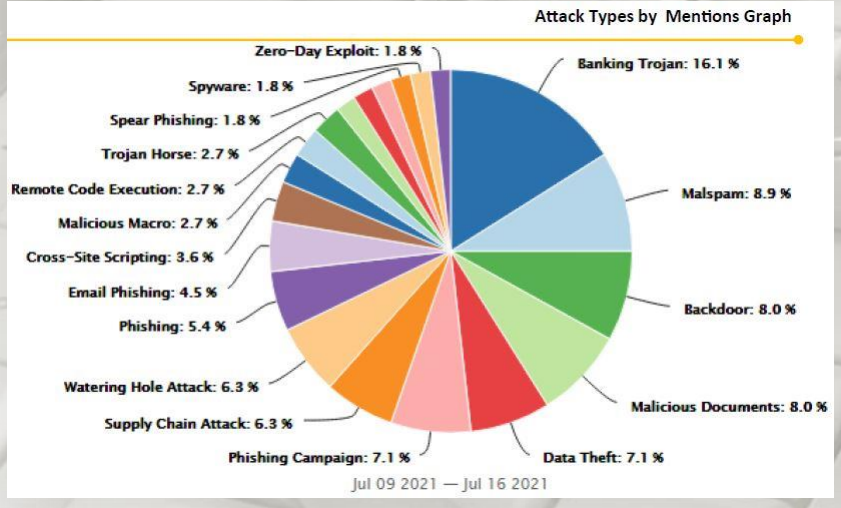
Aktuelle Cybercrimetrends

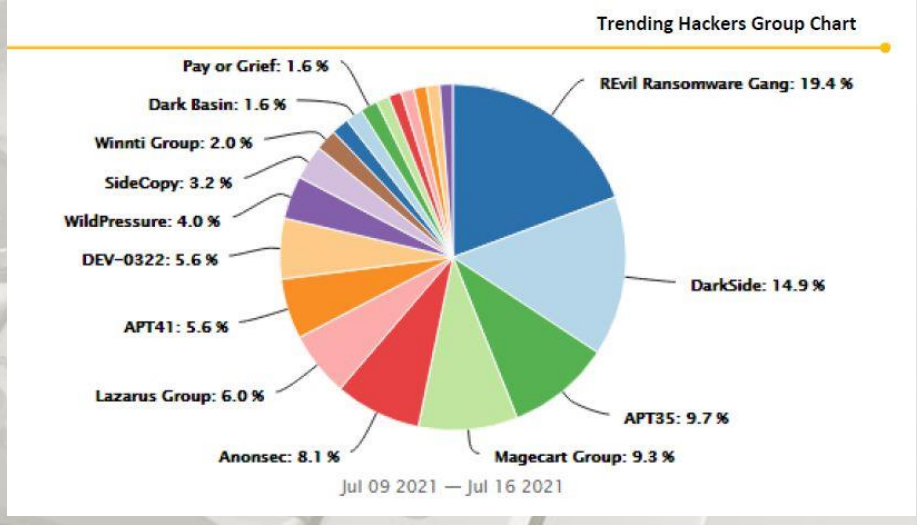


Quelle: Europol EC3 – OSINT Dashboard Week 28/2021

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Aktuelle Cybercrimetrends





Quelle: Europol EC3 – OSINT Dashboard Week 28/2021

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

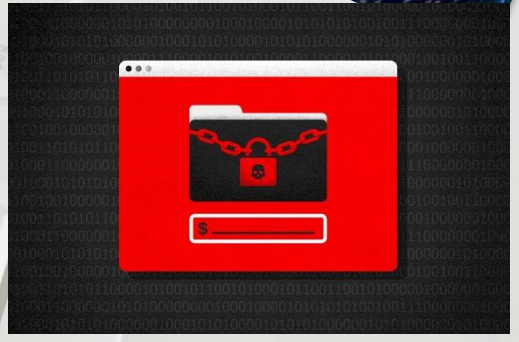
Lage- und Bedrohungspotential

- Botnetze/DDoS-Angriffe
- BEC – Bussiness E-Mail Compromise
- Diebstahl digitaler Identitäten
- Advanced Persistent Threats (APT)
- Angriffe auf kritische Infrastrukturen
- Underground Economy /Darknet
- Cybercrime-as-a-Service

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Lage- und Bedrohungspotential

Digitalisierung vs. Schutz des digitalen Goldes (Daten)



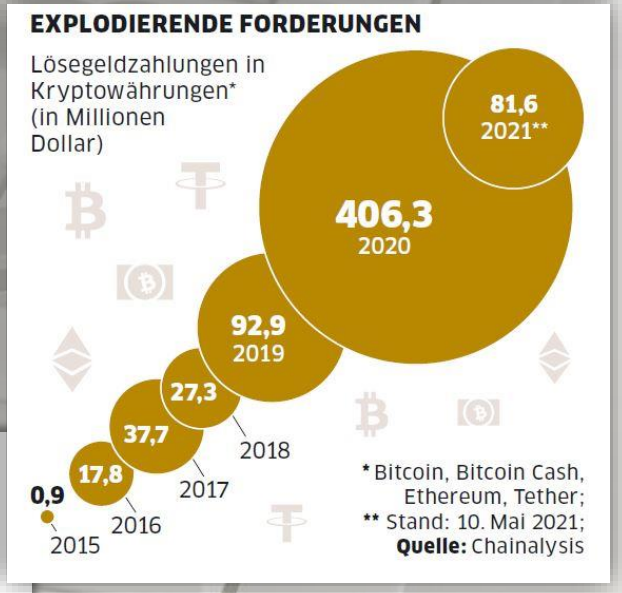
Aktuelle Cybercrime Phänomene

- Smishing (Fake Sendungsverfolgung per SMS)
- Phishing = Ausspähen von Daten (Joker)
- Hacking von Telefonanlagen (Blockieren oder Mehrwert)
- Nutzung von Botnetzen für Angriffe (Zhtrap)
- Schwachstellen MS Exchange (Hafnium), BIG-IQ von F5, MS Druckerspooler
- Malware (WannaCry, Sodinokibi, Phobos, REvil, CLOP, Trickbot, Cobalt Strike, Dridex, PayorGrief uvm.) durch Verschlüsselung + Erpressung (Ausspähen und Veröffentlichung) BigGame-Hunting
- CEO Fraud (Geschäftsführerbetrug)

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Aktuelle Cybercrimetrends

Quelle: Europol EC3 – OSINT Dashboard Week 28/2021



Quelle: 16.07.2021 / Wirtschaftswoche 29

406

Millionen Dollar
Lösegeld wurden laut Chainalysis allein 2020 nach Hackerangriffen gezahlt

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

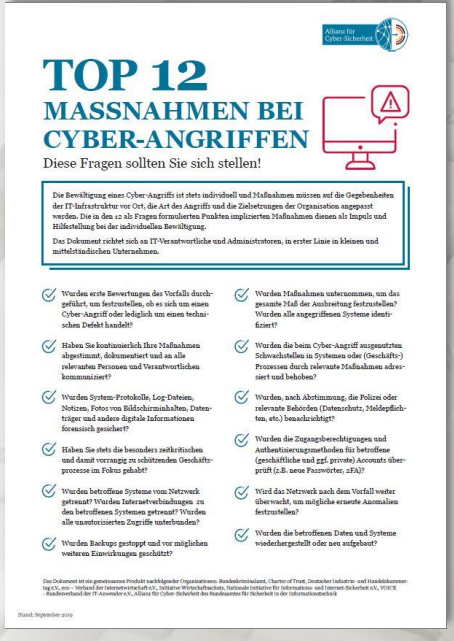
Jeder ist für sich und seine Daten, sowie für die eigene Sicherheit selbst verantwortlich!

Cybercrime kann jeden treffen und jederzeit!

Deshalb ist nicht die Frage, ob es Sie irgendwann trifft, sondern vielmehr wann und ob Sie es dann bemerken?

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Incident- und Notfallmanagement



TOP 12
MASSNAHMEN BEI CYBER-ANGRIFFEN
Diese Fragen sollten Sie sich stellen!

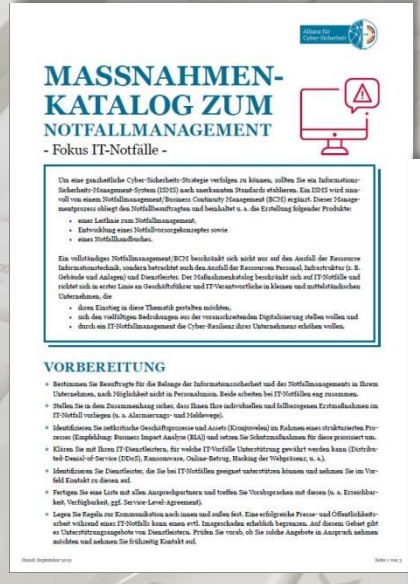
Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.

Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.

- Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, zFA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

Das Dokument ist ein gemeinsames Produkt nachfolgender Organisationen: Bundeskriminalamt, Charter of Trust, Deutscher Industrie- und Handelskammertag eV, eco – Verband der Internetwirtschaft e.V., Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit eV, VOICE – Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik

Stand: September 2019



MASSNAHMEN-KATALOG ZUM NOTFALLMANAGEMENT
- Fokus IT-Notfälle -

Um eine ganzheitliche Cyber-Sicherheits-Strategie verfolgen zu können, sollten Sie ein Informations-Sicherheits-Management-System (ISMS) nach anerkannten Standards etablieren. Ein ISMS wird normalerweise um einen Notfallmanagement/Business Continuity Management (BCM) ergänzt. Dieser Managementprozess obliegt den Notfallbeauftragten und beinhaltet u. a. die Erstellung folgender Produkte:

- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- einen Notfallhandbuches.

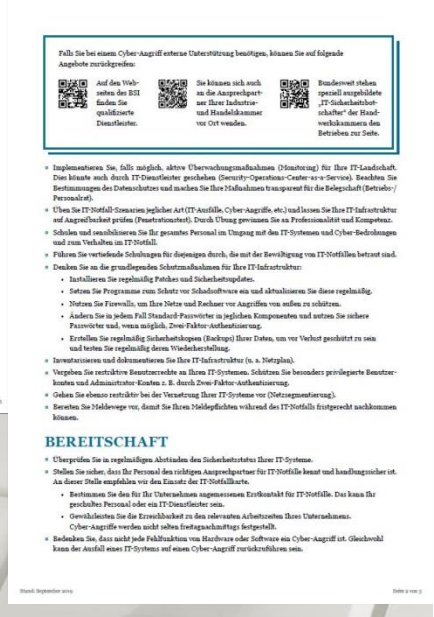
Ein vollständiges Notfallmanagement/BCM beschränkt sich nicht nur auf den Ausfall der Ressource Informationstechnik, sondern betrachtet auch den Ausfall der Ressourcen Personal, Infrastruktur (z. B. Gebäude und Anlagen) und Dienstleister. Der Maßnahmenkatalog beschränkt sich auf IT-Notfälle und richtet sich in erster Linie an Geschäftsführer und IT-Verantwortliche in kleinen und mittelständischen Unternehmen, die

- ihren Einstieg in diese Thematik gestalten möchten,
- sich den vielfältigen Bedrohungen aus der voranschreitenden Digitalisierung stellen wollen und
- durch ein IT-Notfallmanagement der Cyber-Resilienz ihres Unternehmens erhöhen wollen.

VORBEREITUNG

- Bestimmen Sie Beauftragte für die Belange der Informationssicherheit und der Notfallmanagements in Ihrem Unternehmen, nach Möglichkeit nicht in Personalunion. Beide arbeiten bei IT-Notfällen eng zusammen.
- Stellen Sie in den Zusammenhang sicher, dass Ihnen Ihre individuellen und fallbezogenen Erstmaßnahmen im IT-Notfall vorliegen (u. a. Alarmierungs- und Meldewege).
- Identifizieren Sie zeitkritische Geschäftsprozesse und Assets (Kronjuwelen) im Rahmen eines strukturierten Prozesses (Empfehlung: Business Impact Analyse (BIA)) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, für welche IT-Vorfälle Unterstützung gewährt werden kann (Distributed-Denial-of-Service (DDoS), Ransomware, Online-Betrug, Hacking der Webpräsenz, u. a.).
- Identifizieren Sie Dienstleister, die Sie bei IT-Notfällen geeignet unterstützen können und nehmen Sie im Vorfeld Kontakt zu diesen auf.
- Fertigen Sie eine Liste mit allen Ansprechpartnern und treffen Sie Vorabsprachen mit diesen (u. a. Erreichbarkeit, Verfügbarkeit, ggf. Service-Level-Agreement).
- Legen Sie Regeln zur Kommunikation nach innen und außen fest. Eine erfolgreiche Presse- und Öffentlichkeitsarbeit während einer IT-Notfalls kann einen evtl. Imageschaden erheblich begrenzen. Auf diesem Gebiet gibt es Unterstützungsangebote von Dienstleistern. Prüfen Sie vorab, ob Sie solche Angebote in Anspruch nehmen möchten und nehmen Sie frühzeitig Kontakt auf.

Stand: September 2019 Seite 1 von 3



Falls Sie bei einem Cyber-Angriff externe Unterstützung benötigen, können Sie auf folgende Angebote zurückgreifen:

Auf den Webseiten des BSI finden Sie qualifizierte Dienstleister.

Sie können sich auch an die Ansprechpartner Ihrer Industrie- und Handelskammer vor Ort wenden.

Bundesweit stehen speziell ausgebildete „IT-Sicherheitsbotschafter" der Handwerkskammern den Betrieben zur Seite.

- Implementieren Sie, falls möglich, aktive Überwachungsmaßnahmen (Monitoring) für Ihre IT-Landschaft. Dies könnte auch durch IT-Dienstleister geschehen (Security-Operations-Center-as-a-Service). Beachten Sie Bestimmungen des Datenschutzes und machen Sie Ihre Maßnahmen transparent für die Belegschaft (Betriebs-/Personalrat).
- Üben Sie IT-Notfall-Szenarien jeglicher Art (IT-Ausfälle, Cyber-Angriffe, etc.) und lassen Sie Ihre IT-Infrastruktur auf Angreifbarkeit prüfen (Penetrationstest). Durch Übung gewinnen Sie an Professionalität und Kompetenz.
- Schulen und sensibilisieren Sie Ihr gesamtes Personal im Umgang mit den IT-Systemen und Cyber-Bedrohungen und zum Verhalten im IT-Notfall.
- Führen Sie verteilende Schulungen für diejenigen durch, die mit der Bewältigung von IT-Notfällen betraut sind.
- Denken Sie an die grundlegenden Schutzmaßnahmen für Ihre IT-Infrastruktur:
  - Installieren Sie regelmäßig Patches und Sicherheitsupdates.
  - Setzen Sie Programme zum Schutz vor Schadsoftware ein und aktualisieren Sie diese regelmäßig.
  - Nutzen Sie Firewalls, um Ihre Netze und Rechner vor Angriffen von außen zu schützen.
  - Ändern Sie in jedem Fall Standard-Passwörter in jeglichen Komponenten und nutzen Sie sichere Passwörter und, wenn möglich, Zwei-Faktor-Authentisierung.
  - Erstellen Sie regelmäßig Sicherheitskopien (Backup) Ihrer Daten, um vor Verlust geschützt zu sein und testen Sie regelmäßig deren Wiederherstellung.
- Inventarisieren und dokumentieren Sie Ihre IT-Infrastruktur (u. a. Netzplan).
- Vergeben Sie restriktive Benutzerrechte an Ihren IT-Systemen. Schützen Sie besonders privilegierte Benutzerkonten und Administrator-Konten z. B. durch Zwei-Faktor-Authentisierung.
- Gehen Sie ebenso restriktiv bei der Verwetzung Ihrer IT-Systeme vor (Netzsegmentierung).
- Bereiten Sie Meldewege vor, damit Sie Ihren Meldepflichten während des IT-Notfalls fristgerecht nachkommen können.

BEREITSCHAFT

- Überprüfen Sie in regelmäßigen Abständen den Sicherheitsstatus Ihrer IT-Systeme.
- Stellen Sie sicher, dass Ihr Personal den richtigen Ansprechpartner für IT-Notfälle kennt und handlungssicher ist. An dieser Stelle empfehlen wir den Einsatz der IT-Notfallkarte.
  - Bestimmen Sie den für Ihr Unternehmen angemessenen Erstkontakt für IT-Notfälle. Das kann Ihr geschultes Personal oder ein IT-Dienstleister sein.
  - Gewährleisten Sie die Erreichbarkeit zu den relevanten Arbeitszeiten Ihres Unternehmens. Cyber-Angriffe werden nicht selten freitagnachmittags festgestellt.
- Bedenken Sie, dass nicht jede Fehlfunktion von Hardware oder Software ein Cyber-Angriff ist. Gleichwohl kann der Ausfall eines IT-Systems auf einen Cyber-Angriff zurückzuführen sein.

VERHALTEN BEI IT-NOTFÄLLEN

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

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

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

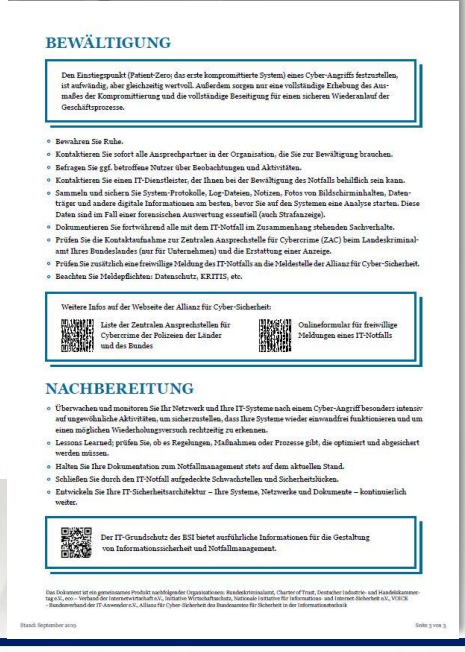
Wann ist das Ereignis eingetreten?

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

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik



BEWÄLTIGUNG

Den Einstiegspunkt (Patient-Zero) das erste kompromittierte System) eines Cyber-Angriffs festzustellen, ist aufwändig, aber gleichzeitig wertvoll. Außerdem sorgen nur eine vollständige Erhebung des Ausmaßes der Kompromittierung und die vollständige Beseitigung für einen sicheren Wiederanlauf der Geschäftsprozesse.

- Bewahren Sie Ruhe.
- Kontaktieren Sie sofort alle Ansprechpartner in der Organisation, die Sie zur Bewältigung brauchen.
- Befragen Sie ggf. betroffene Nutzer über Beobachtungen und Aktivitäten.
- Kontaktieren Sie einen IT-Dienstleister, der Ihnen bei der Bewältigung des Notfalls behilflich sein kann.
- Sammeln und sichern Sie System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen am besten, bevor Sie auf den Systemen eine Analyse starten. Diese Daten sind im Fall einer forensischen Auswertung essentiell (auch Strafanzeige).
- Dokumentieren Sie fortwährend alle mit dem IT-Notfall im Zusammenhang stehenden Sachverhalte.
- Prüfen Sie die Kontaktaufnahme zur Zentralen Ansprechstelle für Cybercrime (ZAC) beim Landeskriminalamt Ihres Bundeslandes (nur für Unternehmen) und die Erstattung einer Anzeige.
- Prüfen Sie zusätzlich eine freiwillige Meldung des IT-Notfalls an die Meldestelle der Allianz für Cyber-Sicherheit.
- Beachten Sie Meldepflichten: Datenschutz, KRITIS, etc.

Weitere Infos auf der Webseite der Allianz für Cyber-Sicherheit:

Liste der Zentralen Ansprechstellen für Cybercrime der Polizeien der Länder und des Bundes

Onlineformular für freiwillige Meldungen eines IT-Notfalls

NACHBEREITUNG

- Überwachen und monitoren Sie Ihr Netzwerk und Ihre IT-Systeme nach einem Cyber-Angriff besonders intensiv auf ungewöhnliche Aktivitäten, um sicherzustellen, dass Ihre Systeme wieder einwandfrei funktionieren und um einen möglichen Wiederholungsversuch rechtzeitig zu erkennen.
- Lessons Learned: prüfen Sie, ob es Regelungen, Maßnahmen oder Prozesse gibt, die optimiert und abgesichert werden müssen.
- Halten Sie Ihre Dokumentation zum Notfallmanagement stets auf dem aktuellen Stand.
- Schließen Sie durch den IT-Notfall aufgedeckte Schwachstellen und Sicherheitslücken.
- Entwickeln Sie Ihre IT-Sicherheitsarchitektur – Ihre Systeme, Netzwerke und Dokumente – kontinuierlich weiter.

Der IT-Grundschutz des BSI bietet ausführliche Informationen für die Gestaltung von Informationssicherheit und Notfallmanagement.

Das Dokument ist ein gemeinsames Produkt nachfolgender Organisationen: Bundeskriminalamt, Charter of Trust, Deutscher Industrie- und Handelskammertag eV, eco – Verband der Internetwirtschaft e.V., Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit eV, VOICE – Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik

Stand: September 2019 Seite 3 von 3

Allianz für Cyber-Sicherheit

https://www.allianz-fuer-cybersicherheit.de

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Blick in die Glaskugel

Wo drohen zukünftige Gefahren?

- Hausautomatisierungen (smart homes / smart grids / smart meter) und das „Internet der Dinge“ (IoT)
- Wearables (Fitnessarmbänder etc.)
- Botnetze aus netzwerkfähigen Haushaltsgeräten
- Elektromobilität / Autonomes Fahren (smart cars)

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Weiterführende Informationen

- ProPK
- https://haveibeenpwned.com/
- BSI für Bürger
- Klicksafe
- ZDDK (mimikama.at)
- Virus Total
- https://sec.hpi.de/ilc/

POLIZEI
SACHSEN-ANHALT
Landeskriminalamt

Zeit für Fragen


POLIZEI
SACHSEN-ANHALT
Landeskriminalamt
Merci !
Thank you!
Köszönöm !
Danke !
Dankon !
Gracias !
Vala !
GRAZIE !
Spascibo !
Terima kasih !