Polizei
Hamburg
LKA 54 Cybercrime

ZENTRALE ANSPRECHSTELLE CYBERCRIME

Aktuelle Phänomene und Handlungsempfehlungen

Haftungsausschluss

Das LKA Hamburg übernimmt keine Haftung für Schäden, die aus der Anwendung der hier erörterten Maßnahmen resultieren.

Der Vortrag ist als Anregung zu verstehen, welche Maßnahmen zur Vorbereitung eines Cybersicherheitsvorfalls getroffen werden können.

Der Vortrag basiert auf den praktischen Erfahrungen der ZAC Hamburg.

Agenda

- Was ist die ZAC?
- „Cybercrime“ aktuell
- Tätergruppen
- Wie gehen die Täter vor?
- Ablauf eines Ransomware Angriffs
- Wie können wir es den Tätern schwer machen?
- Was tun im Ernstfall?
- Was macht die Polizei und was macht sie nicht?
- Die wichtigsten Handlungsempfehlungen

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Was ist die ZAC?

Alle ZAC Kontakte

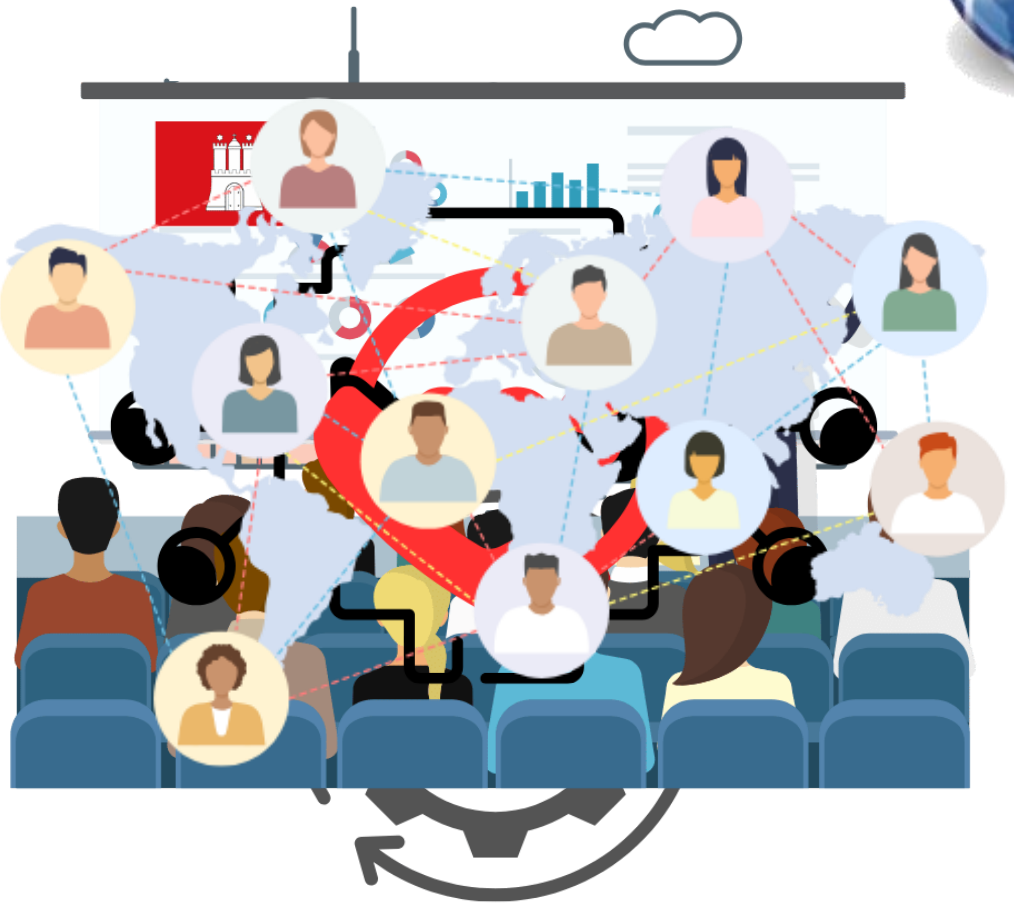
Erreichbarkeiten der Zentralen Ansprechstellen Cybercrime (NUR FÜR UNTERNEHMEN)

	Land/Bund	Telefonnummer	E-Mailadresse	Webseite
	Baden-Württemberg	+49 711 5401-2444		Zur Website
	Bayern	+49 89 1212-3300		Zur Website
	Berlin	+49 30 4664-972972	zac@polizei.berlin.de	
	Brandenburg	+49 3334 388-8686	zac@polizei.brandenburg.de	
	Bremen	+49 421 362-19820	cybercrime@polizei.bremen.de	
	Hamburg	+49 40 4286-75455	zac@polizei.hamburg.de	Zur Website

ZAC HH Kontakt

Was ist die ZAC?

- Die zentrale Ansprechstelle Cybercrime für die Hamburger Wirtschaft
- Beratungsangebote, präventive Awareness Schulungen und Incident Response Übungen
- Beratung in Ernstfällen
- Bindeglied zu den ermittlungsführenden Dienststellen in Hamburg und internationalen Fachdienststellen



KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

„Cybercrime“ aktuell

Cybercrime im weiteren Sinne *Straftaten im Internet*	• Betrug • Stalking • Hasskriminalität • Beleidigung • Kinderpornografie • u.v.m.	• *Findet auf allen bekannten Plattformen statt* • *Hochspezialisierte Tätergruppen* • *Unternehmensähnliche Täterstrukturen* • *KI-Stimmen und Videos* • *Stark ansteigende Fallzahlen* • *Kein Hacking*

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

„Cybercrime“ aktuell

Cybercrime im engeren Sinne *qualifizierte Cybercrime Delikte (Hacking)*	• Ransomware • DDoS-Attacken • Spionage • Sabotage • Scriptbasierte Angriffe	• *Erfordern ein hohes Know-How sowohl bei den Tätern als auch den Ermittlern* • *Vermehrt Angriffe staatlich geförderter Akteure und Hacktivisten* • *Automatisierte und durch KI-gesteuerte Scans und Angriffe* • *Neben Unternehmen gehören auch Schulen, Behörden und Gemeinden zu den Zielen* • *Neben herkömmlichen Sicherheitslücken vermehrtes Aufkommen von sog. Zero-Day Schwachstellen* • *Hohes Dunkelfeld*

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Tätergruppen

- Staatliche Akteure
- Jugendliche Hacker (sog. Scriptkiddies)
- Hacktivisten
- Innentäter
- Betrüger
- Ransomware-Gruppierungen

Wie gehen die Täter vor?

Open-Source Intelligence - OSINT

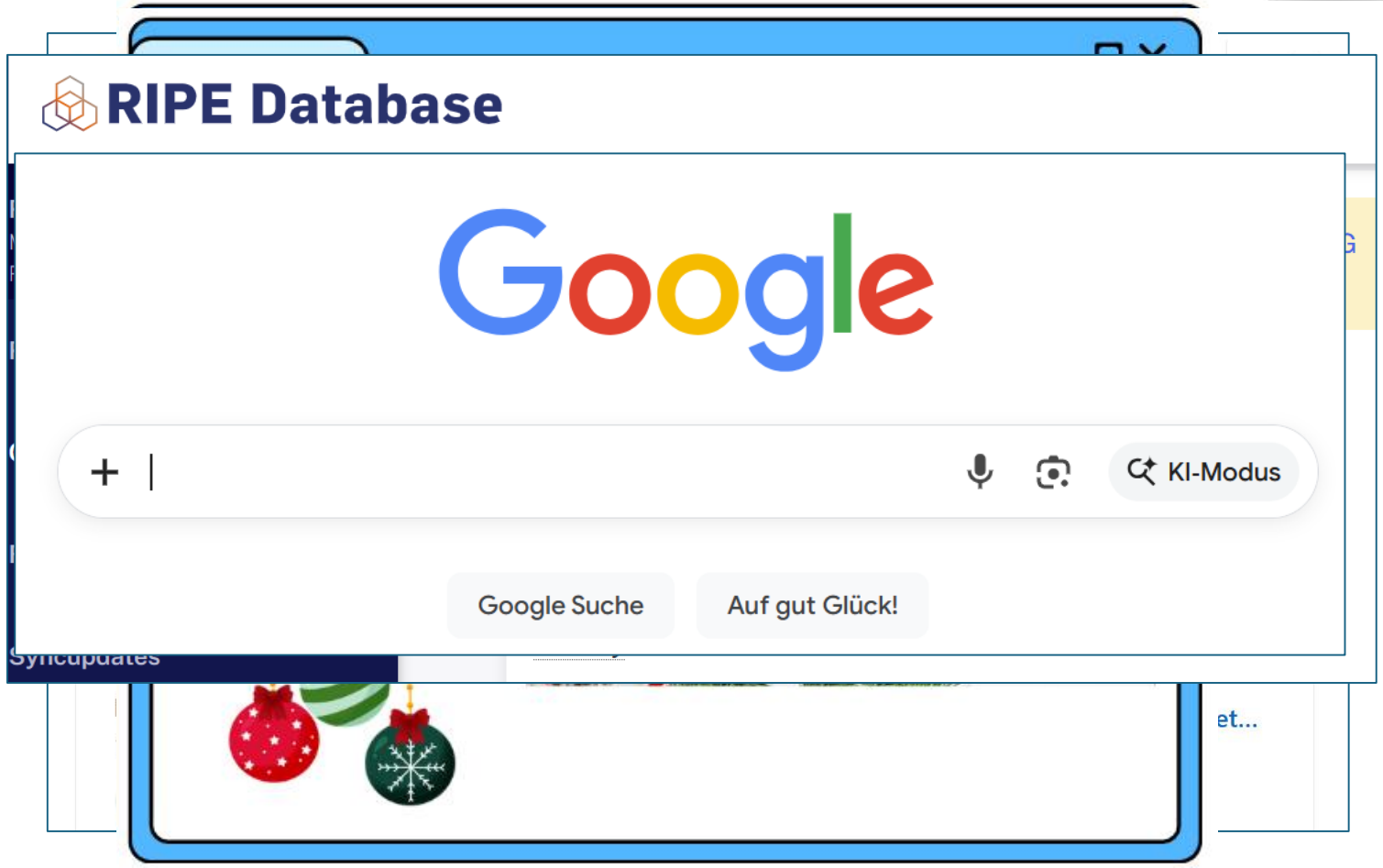
Sammeln von Informationen aus öffentlich zugänglichen Quellen.

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Wie gehen die Täter vor?

Open-Source Intelligence - OSINT

- Social Media
- Webseite des Unternehmens
- Öffentliche Datenbanken
- Google Dorking



Wie gehen die Täter vor?

Datenlecks und Datenhehler

Namen

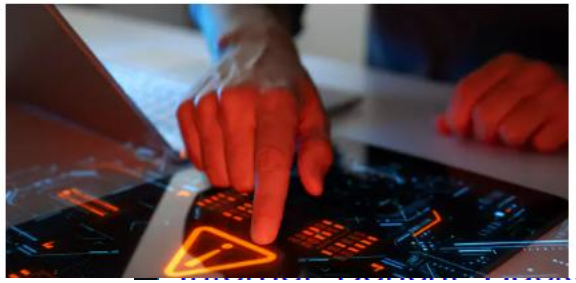
(E-Mail) Adressen

Telefonnummern

Kreditkartendaten

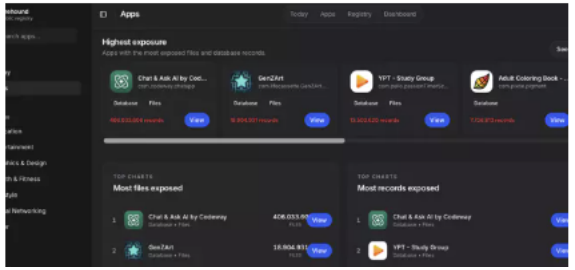
Passwörter

https://haveibeenpwned.com/



Datenleck: 72 Millionen Datensätze von Under Armour geleakt

Eine Ransomware-Bande ist bei Under Armour eingedrungen und hat Daten entwendet. 72 Millionen Datensätze sind nun bei Have I Been Pwned.



Millionenfache Datenlecks bei KI-Apps: Nutzerdaten öffentlich zugänglich

Sicherheitsforscher decken gravierende Datenschutzlücken auf: Einige KI-Apps im App Store exponieren Millionen Nutzerdaten.

Instagram-Datenleck: Daten von 6,2 Millionen Konten bei Have-I-Been-Pwned

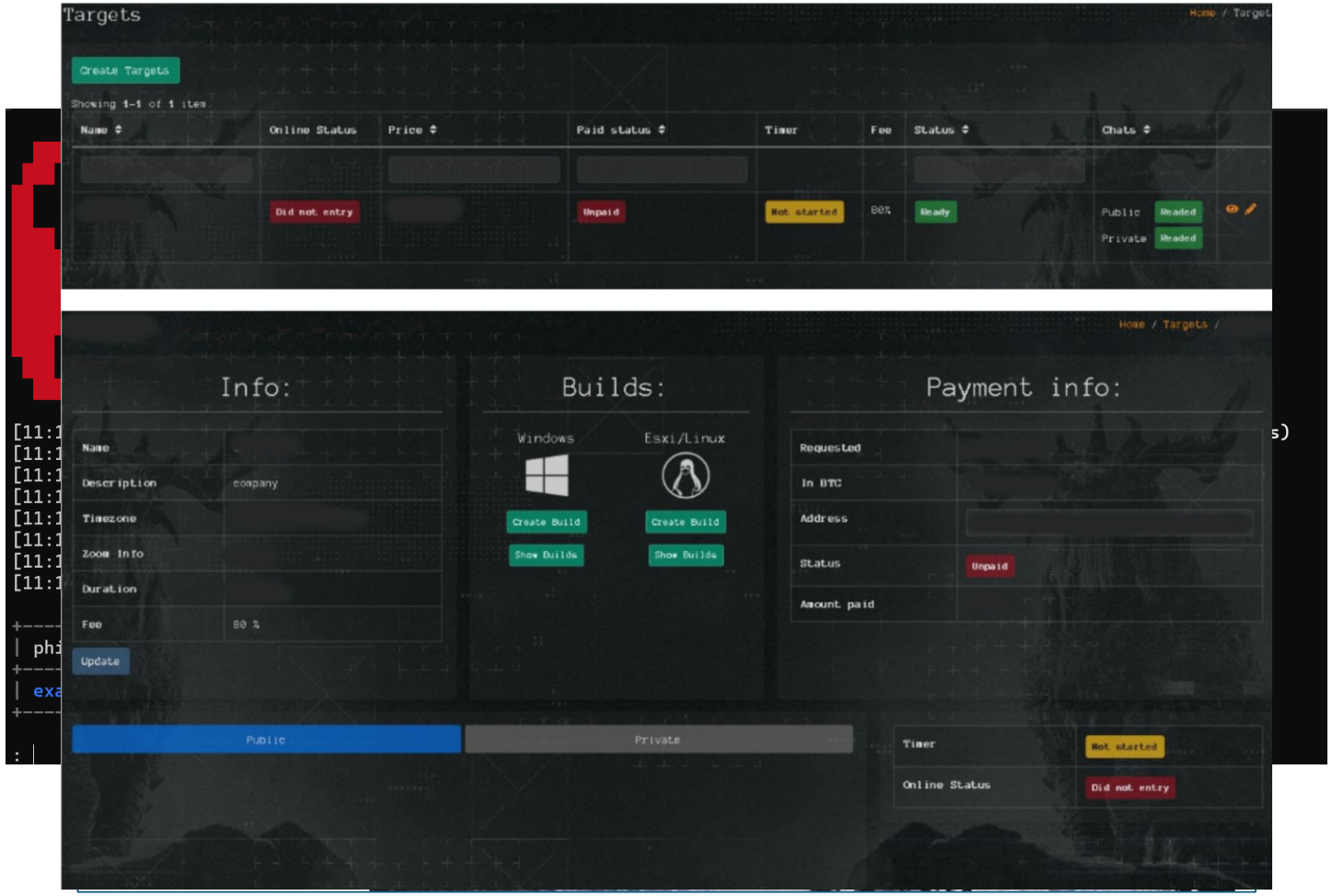
Daten von 6,2 Millionen Instagram-Nutzern sind beim Have-I-Been-Pwned-Projekt gelandet. Von BreachForums kamen zudem 672.000.

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Wie gehen die Täter vor?

Hacker-Tools und Suchmaschinen

- Shodan
- Metasploit
- Evilginx
- Ransomware-Dashboards



Wie gehen die Täter vor?

Automatisierte Angriffe

Brute-Force: Trial-and-Error-Methode, bei der ein Angreifer automatisiert alle theoretisch möglichen Kombinationen von Zeichen ausprobiert, um ein Passwort, einen kryptografischen Schlüssel oder einen Benutzernamen zu knacken.

Credential Stuffing: gestohlene Paare aus Benutzernamen/E-Mail-Adressen und den dazugehörigen Passwörtern werden verwenden, um sich unbefugten Zugang zu anderen Benutzerkonten zu verschaffen.

Wie gehen die Täter vor?

Automatisierte Angriffe

Ablauf

- Entdeckung: Ein Bot findet über Google Dorking oder Shodan eine Login-Maske (z. B. das Admin-Panel einer Kanzlei).
- Dauerfeuer (Brute Force): Ein Skript probiert im Sekundentakt hunderte Kombinationen aus. Es nutzt dabei "Wörterbücher" mit den häufigsten Passwörtern (Sommer2024!, Passwort123).
- Erfolg & Meldung: Sobald eine Kombination funktioniert, stoppt das Skript und sendet dem Täter eine Nachricht (z. B. via Telegram-Bot): "Zugriff erfolgreich: admin.beispiel-firma.de | User: admin | Pass: admin123".

Wie gehen die Täter vor?

Social Engineering

Denn der Mensch ist oft leichter zu hacken als ein Computer

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Betrüger
Caller-ID-Spoofing

Betrüger
E-Mail Manipulation

Sehr simpel: E-Mail-Spoofing

Von: CEO Peter Hansen <0815_Betrug@gmail.com>
Gesendet: Freitag, 15. März 2024 09:08
An: Buchhaltung XY Agentur<Buchhaltung@XY-Agentur.de>
Betreff: Bankkontoinformationen aktualisieren

> Sie erhalten nicht oft eine E-Mail von 0815_Betrug@gmail.com. Erfahren Sie, warum dies wichtig ist

Guten Morgen

Ich möchte meine Bankverbindung vor Abschluss der nächsten Lohn- und Gehaltsabrechnung ändern.
Was brauchst du von mir?

Grüße.
Peter Hansen
Managing Director

Betrüger
E-Mail Manipulation

Sehr simpel: E-Mail-Spoofing

Von: Henry Georges
Gesendet: Mittwoch
An: POL-persl <persl
Betreff: [EXTERN] Ge

Guten Morgen

Welche Informatio

Monat zu ändern?

Grüße
Henry Georges
Head of Digital Fo
Polizei Hamburg

Von: Henry Georges <fovertogood@gmail.com>
Gesendet: Donnerstag, 11. September 2025 09:27
An: POL-PERSL <persl@polizei.hamburg.de>
Betreff: [SPAM] [EXTERN] Kontoinformation aktualisieren

Guten Morgen

Ich möchte meine Bankdaten aktualisieren, bevor die nächste Gehaltsabrechnung abgeschlossen wird. Was brauchen Sie?

Grüße
Henry Georges
Head of Digital Forensics
Polizei Hamburg

Betrüger
E-Mail Manipulation

Simpel: durch den Austausch einzelner Buchstaben

- thomas.meier@meinewelten.de
- thomas.meier@meinewelten.com
- thomas.meier@meinewellen.de
- thomas.meier@rneinewelten.de

Betrüger
E-Mail Manipulation

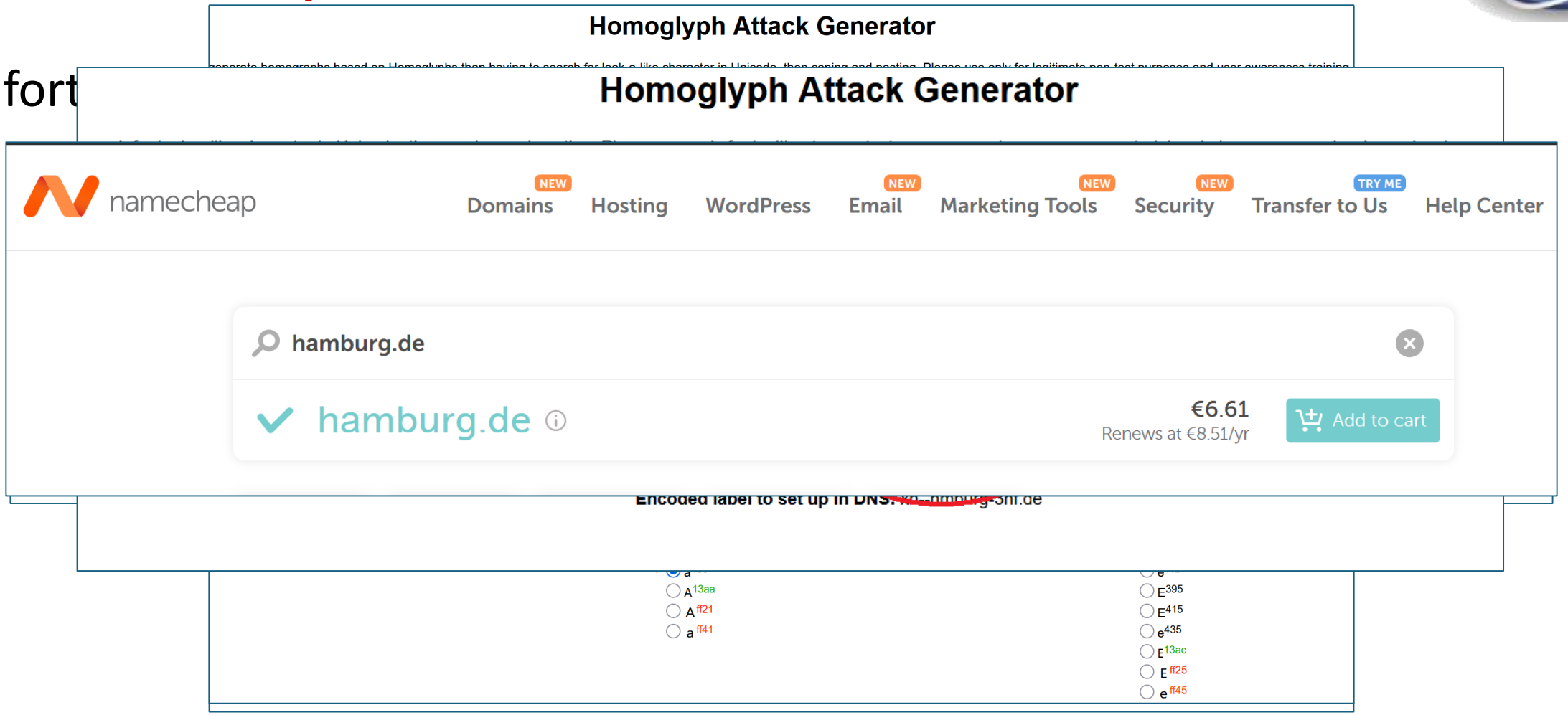
fortgeschritten: die sog. Homoglyphen-Attacke

- Homoglyphen sind ähnlich oder gleich aussehende Schriftzeichen

original	Homoglyph
a	a ạ ą ä à á ą
c	c ć ċ
d	d ď
e	e ẹ ė é è
g	ġ
h	ɦ
i	i í ï

Betrüger
E-Mail Manipulation

fort



Ransomware

Was ist Ransomware?

Ransom **(Soft)ware**

Lösegeld **Computerprogramm**

Computerprogramme, die dazu dienen,

- sich Zugang zu geschützten Netzwerken zu verschaffen
- Netzwerke zu analysieren
- den Virenschutz zu deaktivieren
- verschlüsselte Passwörter auszulesen
- höhere Rechte im Netzwerk zu erlangen
- sich unbemerkt in Netzwerken auszubreiten
- die Kontrolle über Netzwerke zu übernehmen
- Daten aus Netzwerken auszuleiten
- Daten im Netzwerk zu verschlüsseln

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Ransomware

Tätergruppierungen, Strukturen und Zahlen

GROUP NAME	STATUS	LAST UPDATE	VICTIMS DETECTED	FIRST ACTIVITY	FIRST ACTIVITY (ASSESSED)	LAST VICTIM
lockbit3	🟢	2025-03-05 11:02	1995	2022-06-29	2021-12-26	gruppocogesi.org (2025-03-02)
clop	🟢	2025-03-05 11:01	1006	2020-03-13	2020-03-13	IOVATE.COM (2025-03-04)
lockbit2	🔴	N/A	1006	2021-09-09	2021-09-09	datalit.it (2022-06-28)
play	🟢	2025-03-05 11:02	787	2022-11-26	2022-11-26	Pre Con Industries (2025-03-02)
ransomhub	🟢	2025-03-05 10:31	760	2024-02-10	2023-03-09	goencon.com (2025-03-04)
alphv	🔴	N/A	731	2021-09-09	2021-09-09	ipmaltamira (2024-03-03)
akira	🟢	2025-03-05 10:01	643	2023-04-26	2023-04-12	Ray Fogg Corporate P (2025-03-04)

Quelle: https://www.ransomware.live/groups

Ransomware

Tätergruppierungen, Strukturen und Zahlen

Ransomware-Gruppierungen sind hierarchisch organisiert und strukturiert.

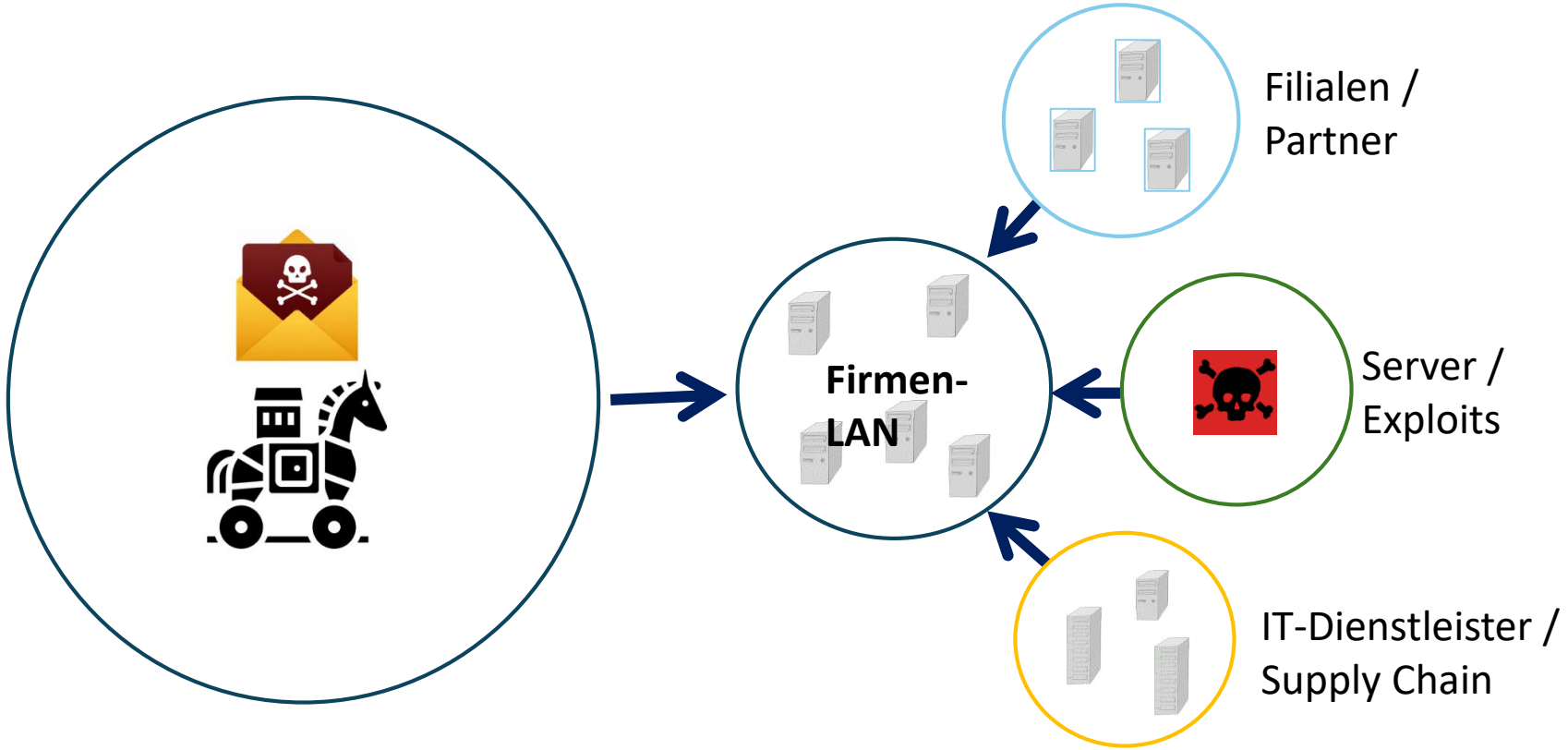
Innerhalb der Gruppierungen gibt es, wie in der herkömmlichen Geschäftswelt, verschiedene Rollen wie

- **Buchprüfer**
- **Kunden-Support**
- **Entwickler**
- **Vertriebler**
- **Verhandlungsführer**
- **usw.**

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

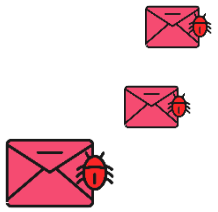
Professionelle Hackergruppierungen

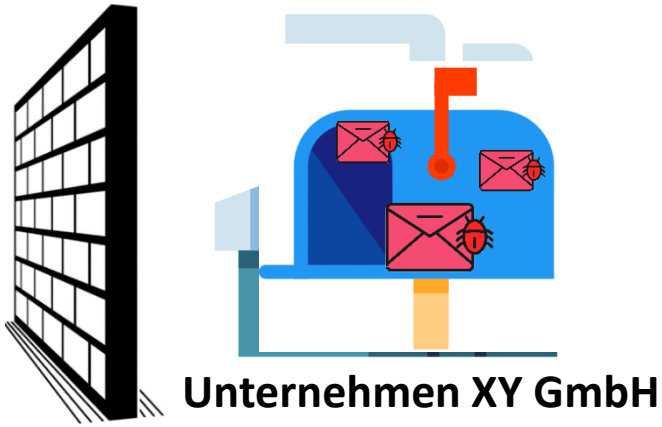
Ablauf eines Ransomware Angriffs



Professionelle Hackergruppierungen

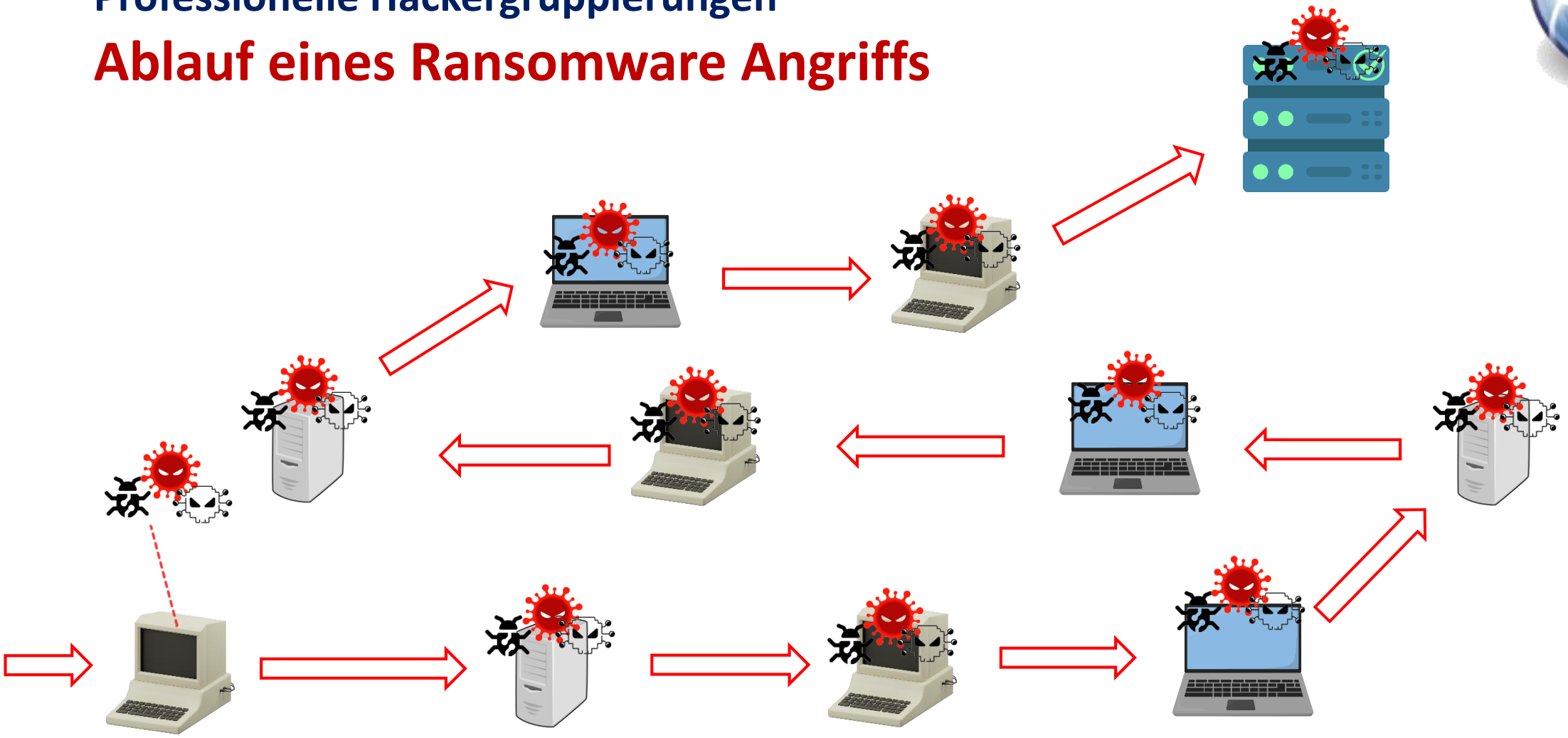
Ablauf eines Ransomware Angriffs





Professionelle Hackergruppierungen

Ablauf eines Ransomware Angriffs



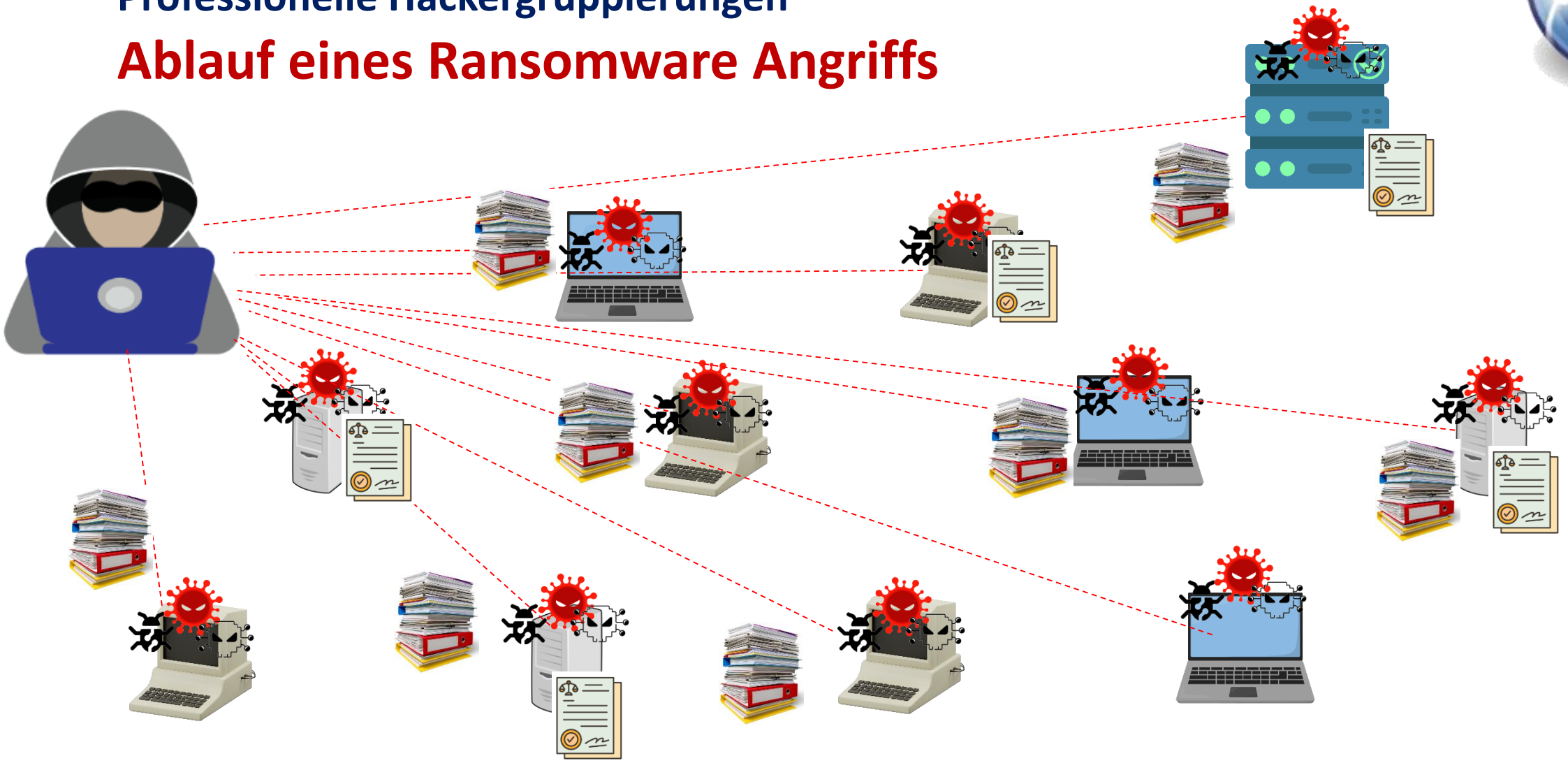
KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Professionelle Hackergruppierungen

Ablauf eines Ransomware Angriffs

Professionelle Hackergruppierungen

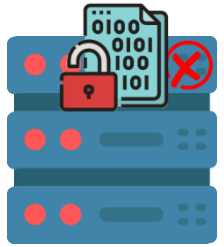
Ablauf eines Ransomware Angriffs



KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Professionelle Hackergruppierungen

Ablauf eines Ransomware Angriffs



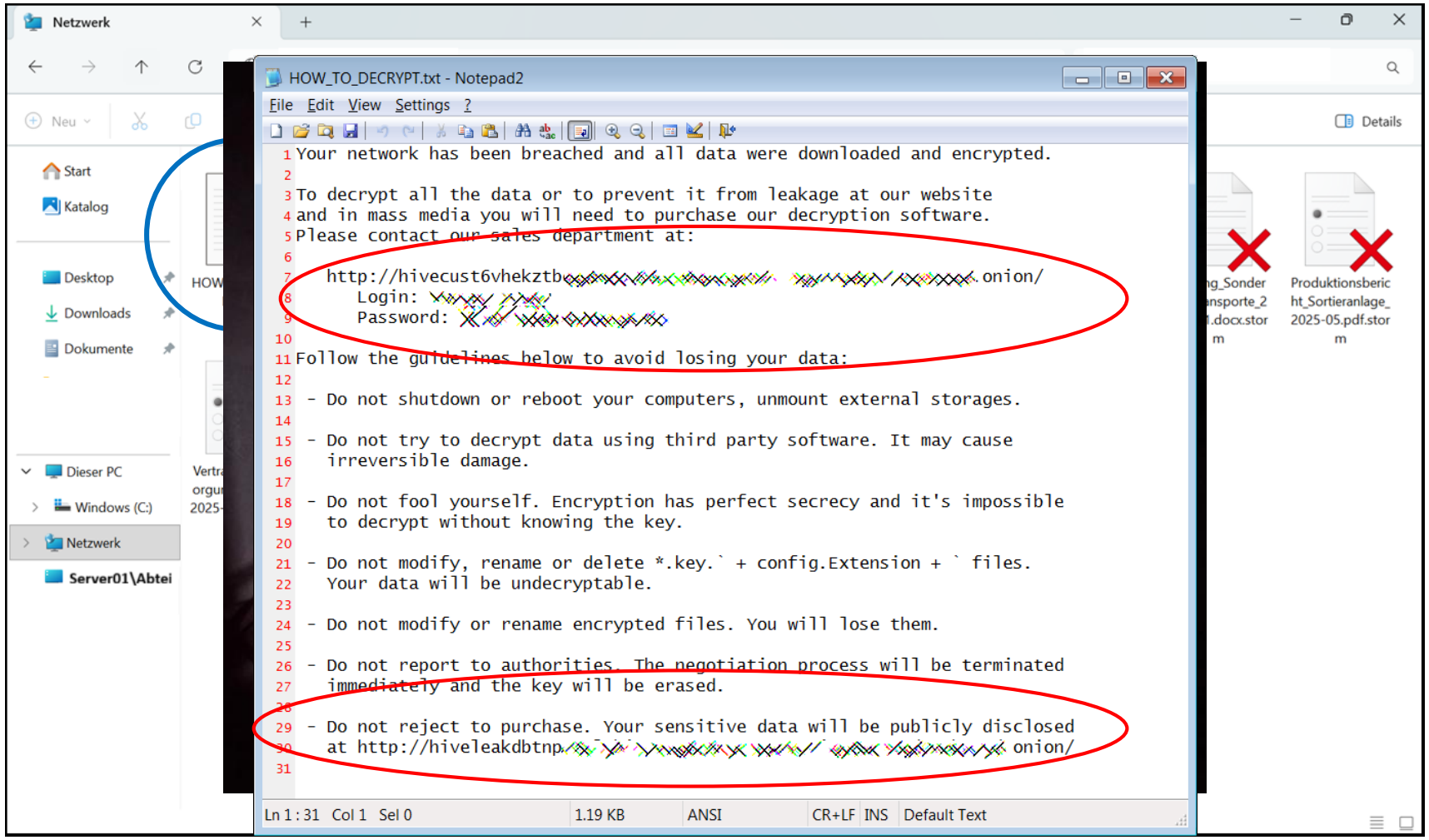






KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Ablauf eines Ransomware-Angriffs



Ablauf eines Ransomware-Angriffs

Mitarbeitende › **IT-Support** › **Leiter IT** › **Geschäftsführung**

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Ransomware - Krisenstab

Rollen im Krisenstab

- Krisenstabsleiter
- Dokumentation
- IT & Cybersicherheit
- (Geschäftsführung)
- Recht & Compliance
- Kommunikation & PR
- Finanzabteilung
- Personalabteilung (HR)
- ggf. externe Berater

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

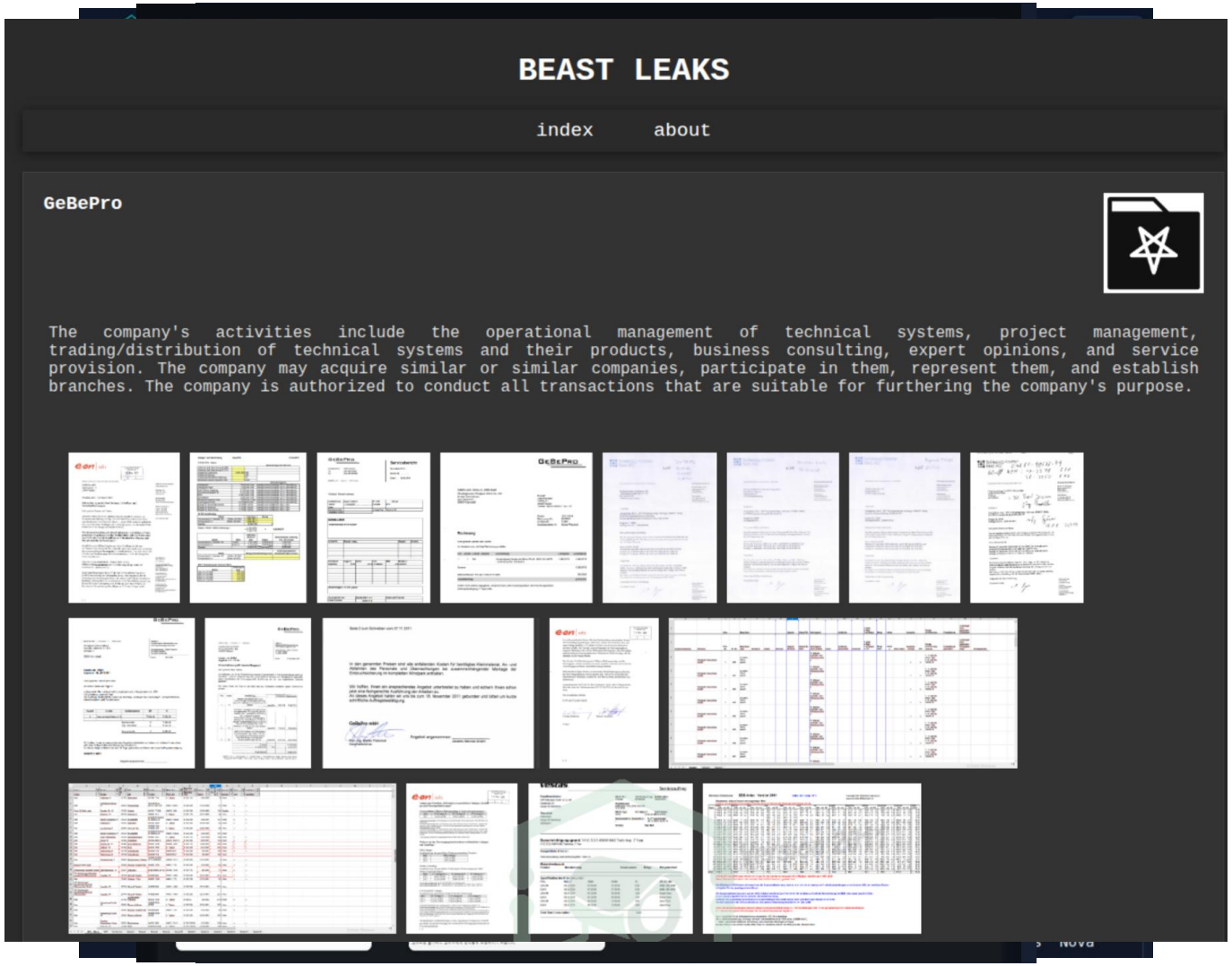
Ransomware - Krisenstab

Ist-Stand-Erhebung

- Was ist passiert?
- Welche Systeme/Daten sind betroffen?
- Haben wir Backups und sind diese auch betroffen?
- Können wir die Systeme zeitnah wiederherstellen?
- Können wir auf einen Notbetrieb umstellen?
- Sind Daten abgeflossen?
- Was für Daten sind abgeflossen?
- Wer weiß bereits davon?
- Wen müssen wir in welcher Form informieren?
- Was wollen die Täter?
- Ist die Drohung der Täter ernst zu nehmen?

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Ransomware - Krisenstab



Krisenstab und finanzielle Herausforderungen

Fragen an die Finanzabteilung

- Wie hoch ist der finanzielle Schaden pro Tag?
- Wie hoch ist der finanzielle Schaden insgesamt?
- Welche Ausfallzeiten kann das Unternehmen tragen?
- Wie sollen die Mitarbeitenden ihr Gehalt erhalten?
- Welche Rechnungen müssen wir priorisiert begleichen?
  - Liegen Rechnungs- und Bankdaten in Papierform vor?
- Wie viel kostet es, die IT wiederherzustellen?
  - Neue Hardware?
  - Durch die IT Abteilung?
  - Mit Hilfe eines ext. Dienstleisters?
- Wie viel Lösegeld könnten wir zahlen?
- Wie schnell und wo können wir Bitcoin beschaffen?

Bitcoin?

Die größten Krypto-Handelsplätze:

- **Binance**
- **Kraken**
- **Coinbase**

Deutsche Krypto-Handelsplätze:

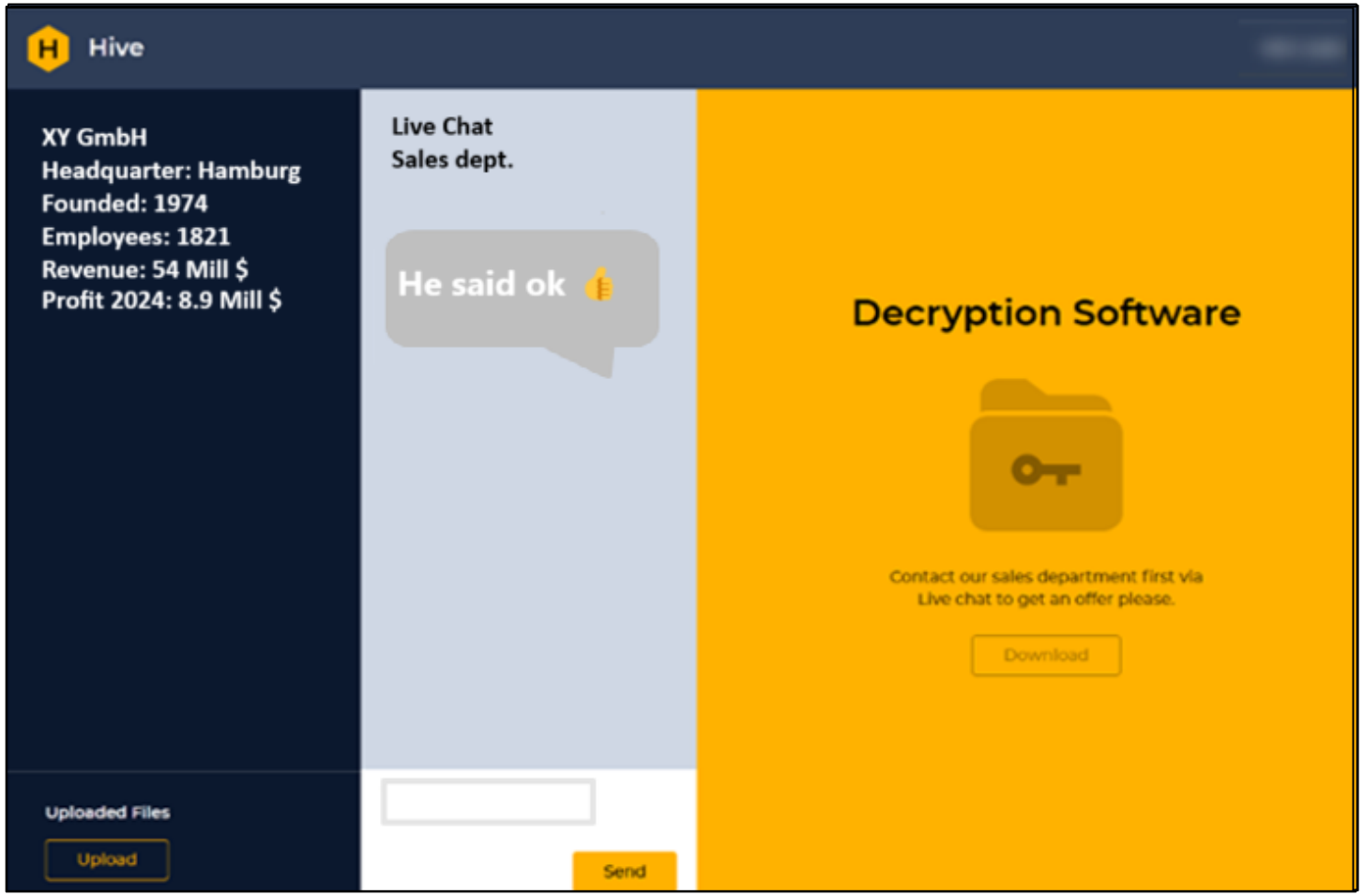
- **Bitcoin.de**
- **eToro**
- **Trade Republic**
- **Bitpanda (Österreich)**
- **usw.**

Dauer von KYC Prozessen beachten!

Überweisungen von Fiat-Währungen hinzu Handelsplätzen benötigen meist mehrere Stunden oder Tage.

Handelsplätze können sich weigern, direkt an Tätergruppierungen zu überweisen.

Verhandlungen



RANSOMWARE .LIVE

KRÜSS

Qilin

Discovery Date: 2026-01-28

N/A...

Centrotherm International

Qilin

Discovery Date: 2026-01-25

N/A...

TOMLLAWYERS.COM

Clop

Discovery Date: 2026-01-25

[AI generated] N/A...

HARTE-BAVENDAMM Rechtsanwlte PartG mbB

Qilin

Discovery Date: 2026-01-24

N/A...

www.hansemerkurintl.com

Dragonforce

Discovery Date: 2026-01-24

HanseMerkur, founded in 1875 and headquartered in Germany, is an insurance company specializing in h...

wohnverbund-st-gertrud.de

Safepay

Discovery Date: 2026-01-19

Wohnverbund St. Gertrud is a German social care and residential support organisation located in Mors...

Wie können wir es den Tätern schwer machen?

- **Der richtige Umgang mit den eigenen Daten im Internet und KI**
  - Privat und geschäftlich
  - Keine direkten Erreichbarkeiten oder Positionen angeben
  - Keine Unterschriften online stellen
  - Prüfen, ob KI unbedingt notwendig ist und welche möglichen Angriffsvektoren durch ihren Einsatz entstehen
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Wie können wir es den Tätern schwer machen?

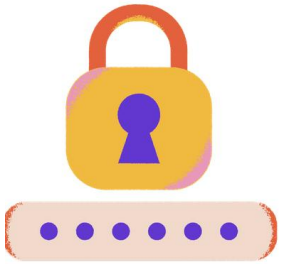
- Der richtige Umgang mit den eigenen Daten im Internet und KI
- **Gesunde Skepsis bei E-Mails und Anrufen**
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

- E-Mail-Absender genau prüfen
- Rückruf über hinterlegte Rufnummer
- Misstrauen bei unerwarteten und eiligen E-Mails
- Pfad hinter Verlinkungen mit der Maus anzeigen und auf Plausibilität prüfen
- Office Dokumente können gefährliche Makros enthalten
- Antivirensoftware
- E-Mail-Filter
- Sandboxing

Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- **Sichere Zugänge und MFA**
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

- Sichere Passwörter
  - mind. 12 Zeichen
  - Groß- und Kleinschreibung
  - Sonderzeichen und Zahlen
  - keine Namen oder Geburtstage
- Für jeden Dienst ein eigenes Passwort
- Passwörter in regelmäßigen Abständen ändern und nicht mit anderen Personen teilen
- Passwortsätze, Passwort-Manager, MFA und Passkeys nutzen



Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- **Verschlüsselte und signierte E-Mails**
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

- E-Mails ohne Verschlüsselung sind so (un)sicher, wie eine Postkarte

Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- **Klar definierte Prozesse bei Überweisungen**
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

- Vier-Augen-Prinzip und telefonische Rückversicherung bei geänderten Bankverbindungen oder ungewöhnlichen Überweisungsanordnungen

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- **Regelmäßige Schulungen und Übungen**
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

Wissen die Mitarbeitenden,

- wie sie mit Spam-Mails umgehen sollen?
- wo sie Hilfe bekommen?
- was sie tun dürfen/müssen, wenn ihr PC infiziert wurde?
- wie mit Überweisungsanordnungen und geänderten Bankverbindungen umzugehen ist?

Nutzen die Mitarbeitenden Firmen-Hardware (Laptops, Smartphones etc.) auch im privaten Bereich? (oder umgekehrt)

Nutzen die Mitarbeitenden sichere Passwörter und 2-Faktor-Authentifizierungen?

Werden einzelne Passwörter von mehreren Personen oder ganzen Abteilungen genutzt?

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- **Regelmäßige Schulungen und Übungen**
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet 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

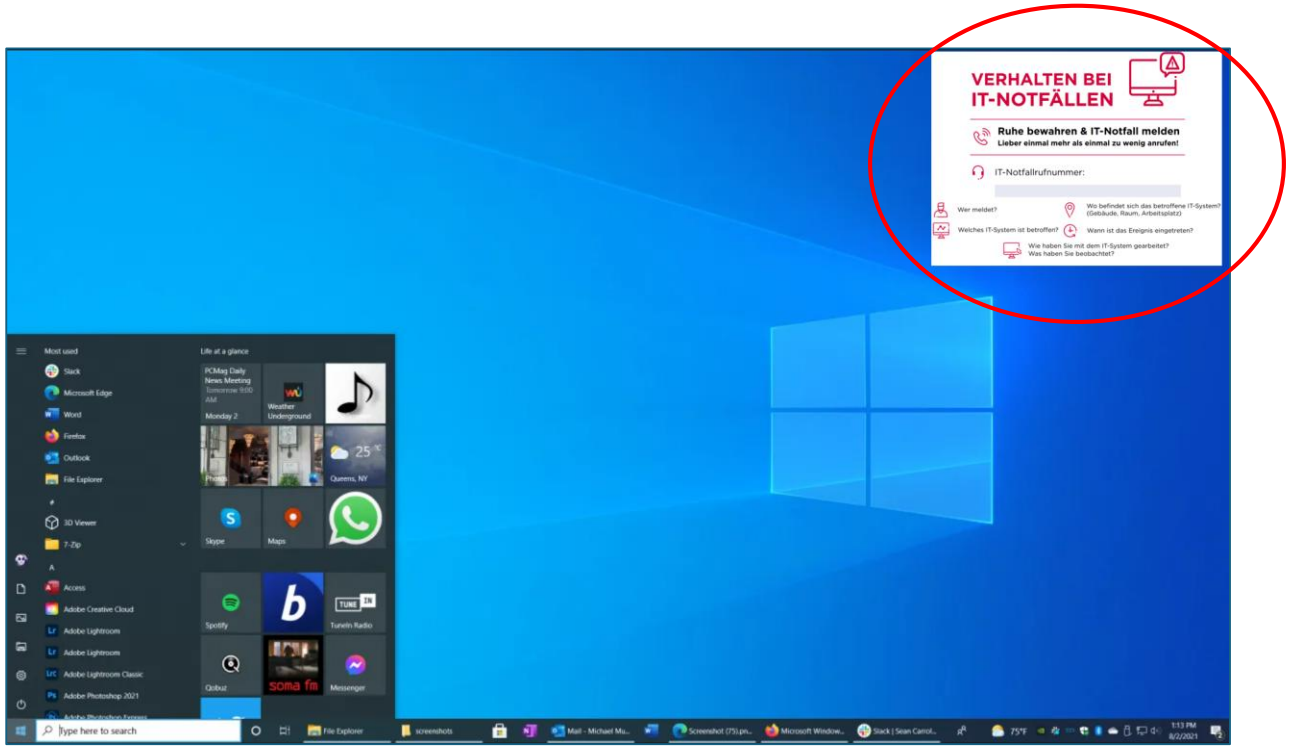
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- **Regelmäßige Schulungen und Übungen**
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- **Regelmäßige Schulungen und Übungen**
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein



Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- **positive Fehlerkultur**
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

- Jeder macht Fehler (Chefs inklusive)
- Niemand sollte Angst davor haben, einen falschen Klick zu melden
- Das rechtzeitige Wissen um einen falschen Klick mindert die Gefahr drastisch

Wie können wir es den Tätern schwer machen?

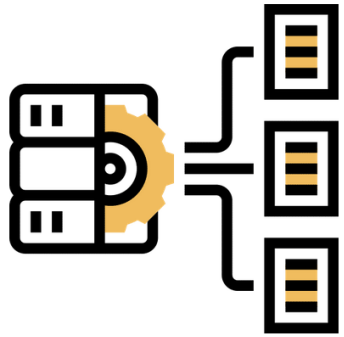
- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- **Technische Lösungen**
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

- Mail-Gateways, Sandboxing, URL-Filter
- MFA
- Automatische Updates
- Passwortkontrolle und Rotation
- Ausländischen IP-Adressen blockieren
- Rechtemanagement (Least Privilege-Prinzip)
- Erkennen und Protkollierung von Scans und Zugriffsversuchen
- Alarm und automatische Reaktionen bei ungewöhnlichen Aktivitäten wie großen Datenabflüssen
- Cloud oder nicht Cloud?

Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- **Krisensichere Backups**
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

- 3-2-1-Prinzip
  - 3 Kopien der Daten auf
  - 2 unterschiedliche Medien +
  - 1 extern aufbewahrte Kopie
- Backups vom Netzwerk trennen
- Das Wiedereinspielen von Backups testen



Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- **Zeitnahe Updates**
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- Trotzdem auf den Ernstfall vorbereitet sein

- Mit jedem Update wird die damit geschlossene Sicherheitslücke bekanntgegeben
- Täter wissen anhand der Bekanntgabe, welche Angriffe möglich sind
- Verzögerte oder ausbleibende Updates machen es den Angreifern sehr leicht

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- **Vor dem Ernstfall der IT die richtigen Fragen stellen**
- Trotzdem auf den Ernstfall vorbereitet sein

- Welche Systeme und Geräte haben wir im Unternehmen? (Schatten-IT)
- Gibt es ungenutzte oder ungeschützte Admin-Konten?
- Welche Daten besitzen wir?
- Welche sind unsere wichtigsten Daten und Systeme?
- Wo liegen diese Daten und wer hat Zugriff darauf?
- Wer hat welche Berechtigungen im Netzwerk?
- Wie können wir besonders sensible Daten vor einer Veröffentlichung schützen?
- Werden große Datenabflüsse überwacht?
- Werden verdächtige Zugriffsversuche und Anomalien im Netzwerk erkannt und gemeldet?
- Wie reagieren wir auf Angriffe zur Nachtzeit / an Feiertagen / am Wochenende?
- Wie schnell können die Systeme mit Hilfe der Backups oder ohne Backups wiederhergestellt werden?
- Wie zeitnah werden Updates eingespielt?

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Wie können wir es den Tätern schwer machen?

- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- Sichere Zugänge und MFA
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- Krisensichere Backups
- Zeitnahe Updates
- Vor dem Ernstfall der IT die richtigen Fragen stellen
- **Trotzdem auf den Ernstfall vorbereitet sein**
- Notfallprozesse erarbeiten, testen und ausgedruckt bereitlegen
- Krisenstabsübungen
- Presse-Statement in die Schublade legen
- Mit dem Thema „Bitcoin“ befassen (nicht gleich kaufen)
- Mit den gängigen Meldepflichten vertraut machen
  - **DSGVO (alle Unternehmen):**
    max. 72 Stunden
  - **Kritis Unternehmen:**
    sofort an das BSI melden
  - **NIS2-Unternehmen:**
    24 Stunden=Erstmeldung, 72 Stunden= Detailbericht, max. 1 Monat=Abschlussbericht an das BSI
  - **Banken, Versicherungen, Zahlungsinstitute:**
    sofort an die BaFin

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

Was tun im Ernstfall?

Ruhe bewahren und Überblick verschaffen	
IT hinzuziehen	
ZAC informieren und telefonisch beraten lassen	**040 4286 75455** **zac@polizei.hamburg.de** **(bei akuten Notfällen auch 110 möglich)**
Schäden begrenzen	**Zugangsdaten ändern + MFA einrichten** **ggf. Netzwerke trennen, Backups prüfen**
Vorgehen dokumentieren	
Digitale Spuren sichern	
Weitere Stellen informieren	**Datenschutzbehörde** **ggf. Hausbank, Kunden, Lieferanten etc.**
Auf weitere Einschläge vorbereiten	**z.B. Anfragen von Kunden und der Presse**

Was macht die Polizei und was macht sie nicht?

- Awareness-Maßnahmen vor dem Ernstfall
  - Geschäftsleitung
  - Mitarbeitende
- Incident Response Übung
- Unterstützung während des Ernstfalls
- Ermittlung der Täter

- Tatort absperren und alle Geräte beschlagnahmen
- Systeme wieder aufsetzen
- Geld sofort wiederbeschaffen
- Ein individuelles Sicherheitskonzept für Ihr Unternehmen erstellen

Die wichtigsten Handlungsempfehlungen

- Setzen Sie sich frühzeitig (vor dem Ernstfall) mit dem Thema auseinander
- Verschaffen Sie sich einen Überblick über Ihren Daten und Systeme
- Investieren Sie in Ihre IT-Sicherheit
- Machen Sie Ihre Backups krisensicher
- Schulen Sie Ihre Mitarbeitenden (fortlaufend)
- Nutzen Sie die kostenlosen Angebote

Nutzen Sie die kostenlosen Angebote

BSI – Bundesamt für Sicherheit in der Informationstechnik
- Leitfäden
- Kontakte
- Broschüren

Transferstelle Cybersicherheit
- Der CYBERsicher Check
- Workshops & Veranstaltungen
- Notfallhilfe

Phishen Impossible
- Erklärvideos
- Quiz
- Aktuelle Phishing-Phänomene

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455

ZAC Kontakt

https://lkahh.de/files/Rasmussen/allgemein_60min.zip

Vielen Dank für Ihre Aufmerksamkeit

KOK Rasmussen zac@polizei.hamburg.de 040 4286 75455