



Polizei
Hamburg
LKA 54 Cybercrime

ZENTRALE ANSPRECHSTELLE CYBERCRIME
Aktuelle Phänomene und Handlungsempfehlungen



- Sönke Rasmussen
- Seit 2011 bei der Hamburger Polizei
- 2017 Wechsel zur Kriminalpolizei
- Bachelorarbeit zum Thema Kryptowährungen und Geldwäsche
- 2019-2024 Cybercrime-Ermittler
- Seit 2024 Zentrale Ansprechstelle Cybercrime des LKA HH
- Blockchain Ermittlungen
- Verhandlungsgruppe des LKA



Agenda

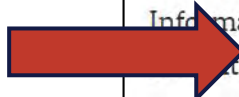
- Was ist die ZAC?
- „Cybercrime“ aktuell
- Tätergruppen und ihre Methoden
- Ablauf eines Ransomware Angriffs
- Wie können wir es den Tätern schwer machen?
- Was tun im Ernstfall?
- Was macht die Polizei und was macht sie nicht?
- Die wichtigsten Handlungsempfehlungen und Angebote





Was ist die ZAC?

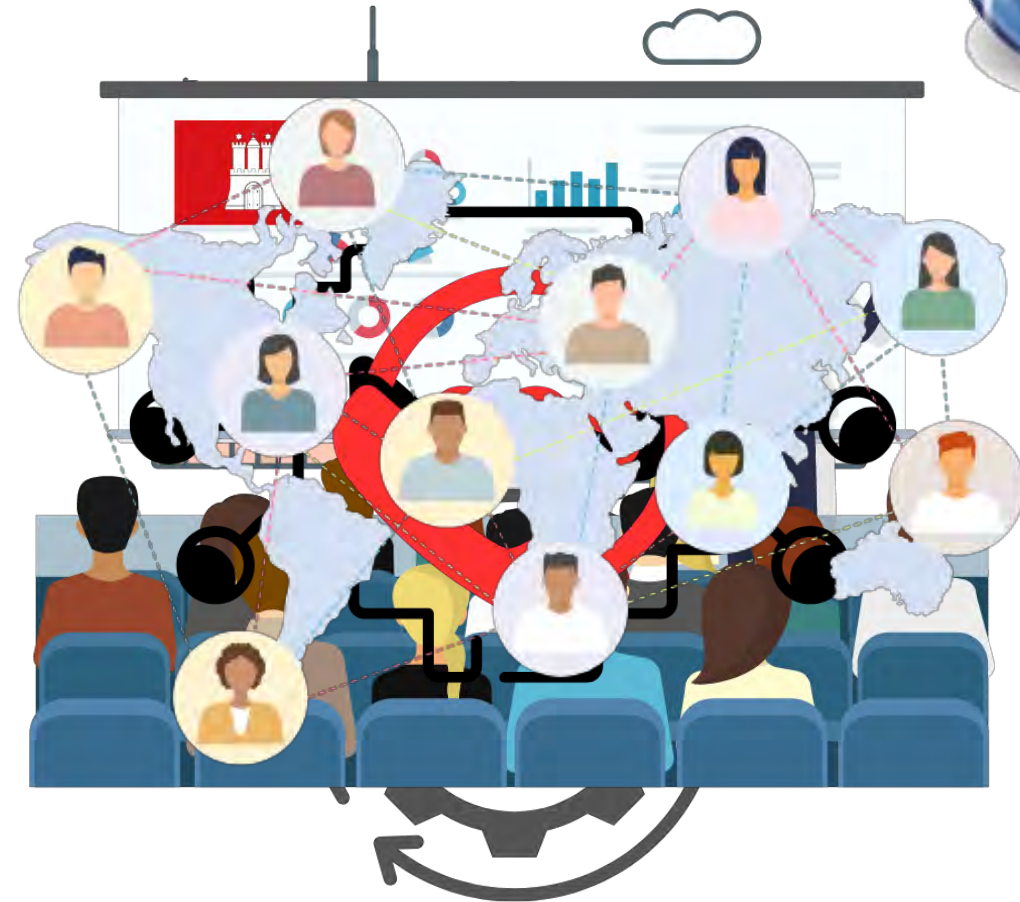
Erreichbarkeiten der Zentralen Ansprechstellen Cybercrime (NUR FÜR UNTERNEHMEN)			
Land/Bund	Telefonnummer	E-Mailadresse	Webseite
 Baden-Württemberg	+49 711 5401-2444		Zur Website ➔
 Bayern	+49 89 1212-3300		Zur Website ➔
 Berlin	+49 30 4664-972972	✉ zac@polizei.berlin.de	
 Brandenburg	+49 3334 388-8686	✉ zac@polizei.brandenburg.de	
 Bremen	+49 421 362-19820	✉ cybercrime@polizei.bremen.de	
 Hamburg	+49 40 4286-75455	✉ zac@polizei.hamburg.de	Zur Website ➔





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





„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*



„Cybercrime“ aktuell

Cybercrime im engeren Sinne

*qualifizierte
Cybercrime Delikte
(Hacking)*

- Ransomware
- DDoS-Attacken
- computergestützte Spionage und Sabotage
- scriptbasierte Zugriffsversuche und Accountübernahme
- *Erfordert ein hohes Know-How sowohl bei den Tätern als auch den Ermittlern*
- *Ver mehrt Angriffe staatlich geförderter Akteure und Hacktivist en*
- *automatisierte und durch KI-gesteuerte Scans und Angriffe*
- *Ver mehrt es Aufkommen und Ausnutzen von sog. „Zero-Day“ Schwachstellen*
- *Ransomware wird als Service angeboten „RaaS“*
- *Täter nutzen KI zur Programmierung, sog. „Vibe Coding“*
- *Hohes Dunkelfeld*



Tätergruppen

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





Wie gehen die Täter vor?

Open-Source Intelligence - OSINT

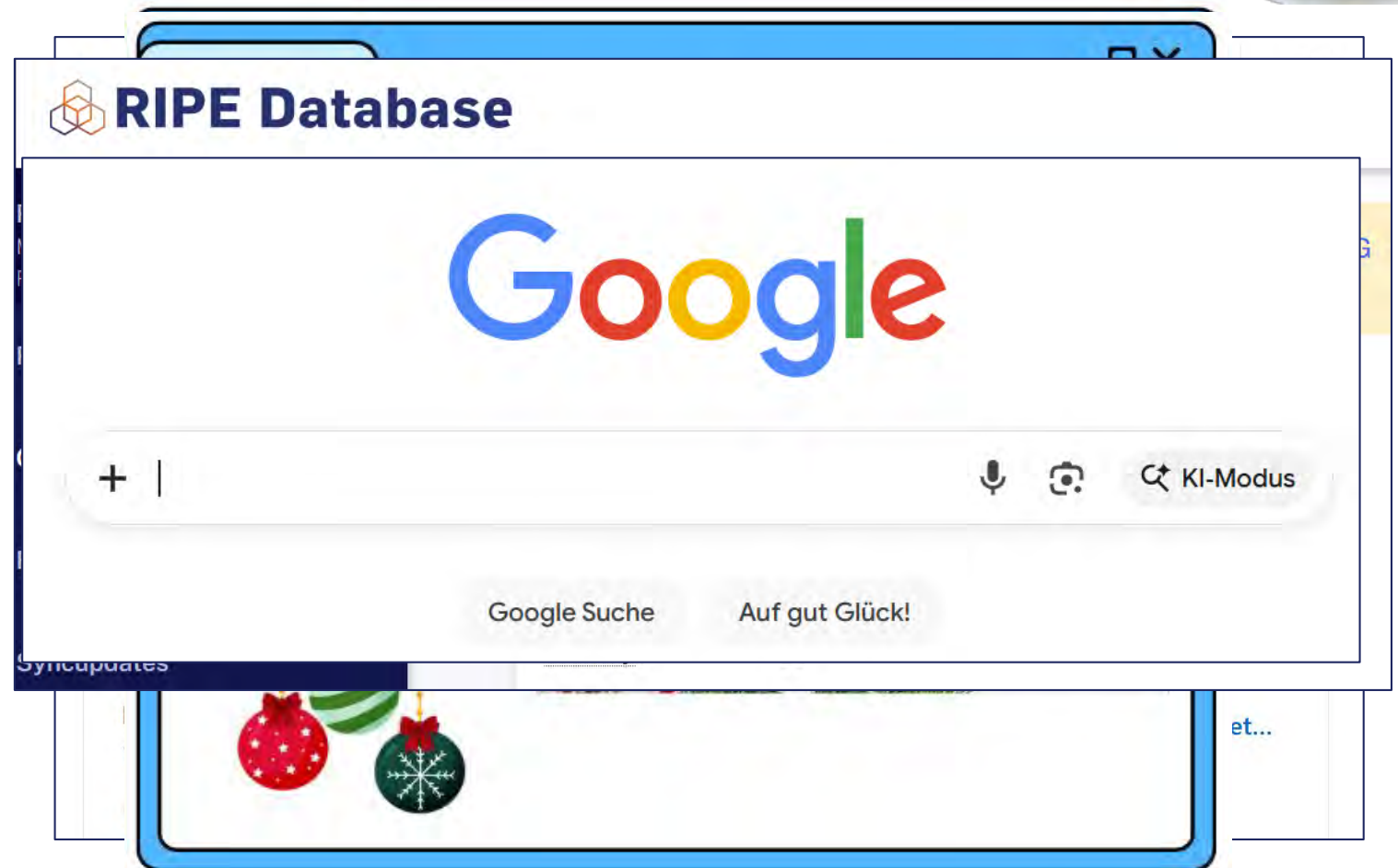
Sammeln von Informationen aus öffentlich zugänglichen Quellen.



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.



Wie gehen die Täter vor? **Social Engineering**

Denn der Mensch ist oft leichter zu hacken als ein Computer



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

<p>Von: Henry Georges Gesendet: Mittwoch An: POL-persl <persl@polizei.hamburg.de> Betreff: [EXTERNAL] Ge</p> <p>Guten Morgen</p> <p>Welche Information</p> <p>Grüße Henry Georges Head of Digital Fore Polizei Hamburg</p>	<p>Von: Henry Georges <fovertogood@gmail.com> Gesendet: Donnerstag, 11. September 2025 09:27 An: POL-PERSL <persl@polizei.hamburg.de> Betreff: [SPAM] [EXTERNAL] Kontoinformation aktualisieren</p> <p>Guten Morgen</p> <p>Ich möchte meine Bankdaten aktualisieren, bevor die nächste Gehaltsabrechnung abgeschlossen wird. Was brauchen Sie?</p> <p>Grüße Henry Georges Head of Digital Forensics Polizei Hamburg</p> 	<p>Monat zu ändern?</p>
--	---	-------------------------



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
- thomas.meier@meinewelten.de



Betrüger

CEO Fraud

2015/2016

Sehr geehrte Frau M.,

ich kann doch in einer streng vertraulichen Finanzangelegenheit auf Ihre Unterstützung zählen. Unser Unternehmen plant eine Expansion in den asiatischen Geschäftsraum und wird hierzu eine existierende Firma übernehmen. Wie Sie sicher verstehen können, ist diese Transaktion streng geheim. Aus diesem Grunde und zu Dokumentationszwecken für die Bafin darf die gesamte Kommunikation mit mir ausschließlich per Mail erfolgen.

Mit der Abwicklung wurde das Schweizer Notariat E. betraut. Der Rechtsanwalt und Notar Dr. E. wird sich morgen telefonisch bei Ihnen bezüglich der Details melden.

Bitte bereiten Sie alles für eine entsprechende Auslandsüberweisung vor.

Ich weiß, dass ich mich auf Sie verlassen kann.

Mit freundlichen Grüßen

Dr. W., CEO





Betrüger

CEO Fraud

heute

Guten Marion,

Was ist unser Bankguthaben?

Können wir heute 70T bezahlen?

Gruß

Thomas Meier

Geschrieben von iPad

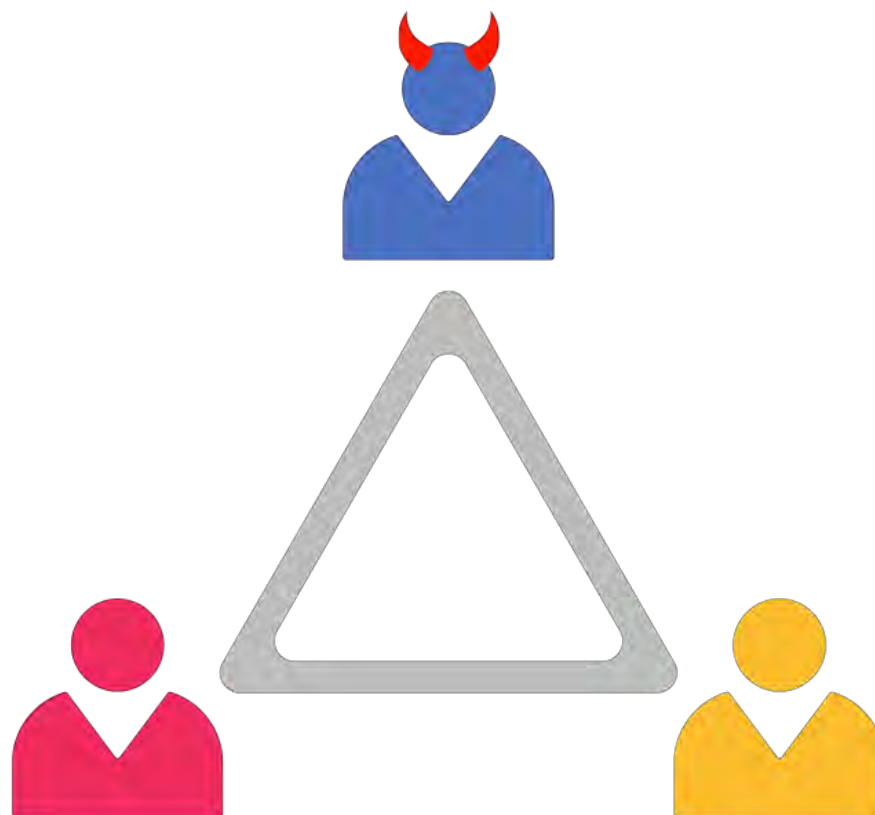




Betrüger

BEC Fraud (Business E-Mail Compromise)

„Man-in-the-Middle-attack“





Betrüger

BEC Fraud (Business E-Mail Compromise)

„Man-in-the-Middle-attack“



Frau Meier von dem Unternehmen
Werkstattbedarf XY
Ulla.meier@werkstattbedarfxy.de

Lieferant

Rechnung

Bestellung



Herr Hansen von dem Unternehmen
KFZ Service GmbH
Mike.hansen@kfzservice.de

Kunde

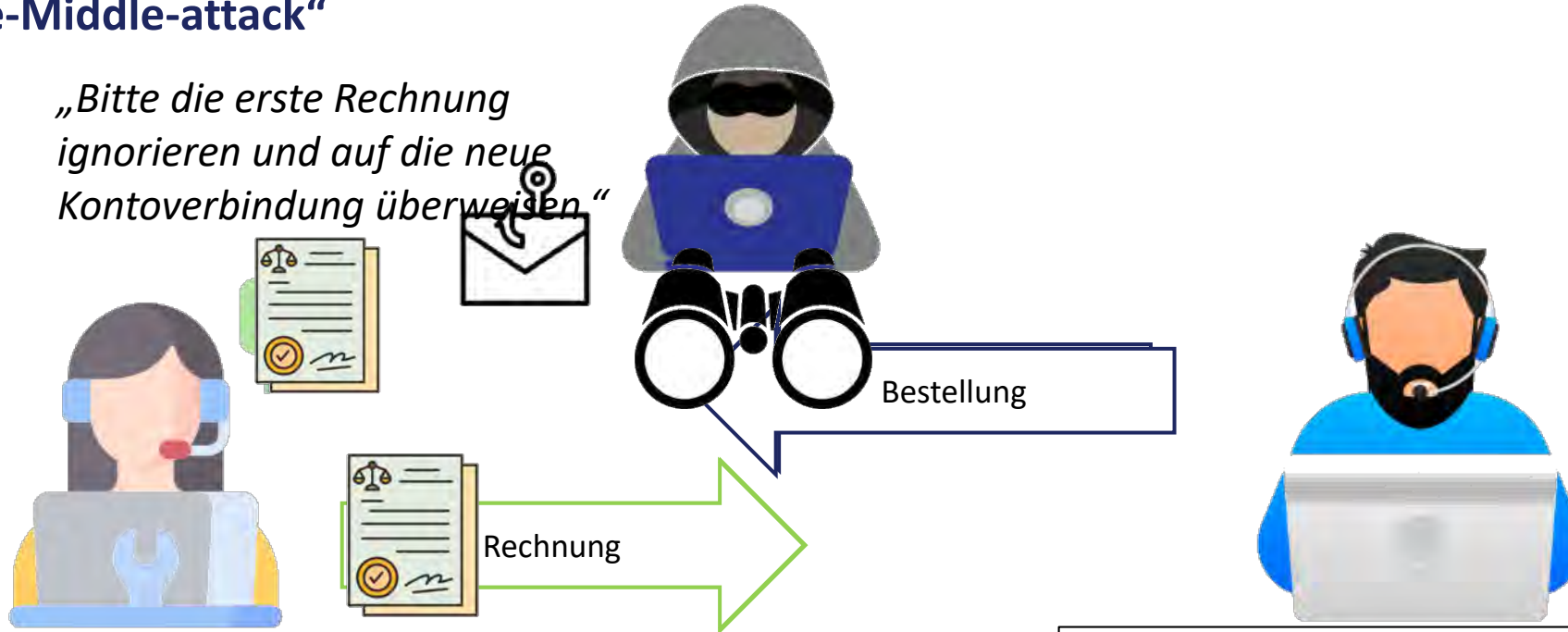


Betrüger

BEC Fraud (Business E-Mail Compromise)

„Man-in-the-Middle-attack“

„Bitte die erste Rechnung ignorieren und auf die neue Kontoverbindung überweisen.“



Frau Meier von dem Unternehmen
Werkstattbedarf XY
Ulla.meier@werkstattbedarfxy.de

Lieferant

Herr Hansen von dem Unternehmen
KFZ Service GmbH
Mike.hansen@kfzservice.de

Kunde



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





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 <i>(2025-03-02)</i>
clop ⓘ	●	2025-03-05 11:01	1006	2020-03-13	2020-03-13	IOVATE.COM <i>(2025-03-04)</i>
lockbit2	●	N/A	1006	2021-09-09	2021-09-09	datalit.it <i>(2022-06-28)</i>
play ⓘ	●	2025-03-05 11:02	787	2022-11-26	2022-11-26	Pre Con Industries <i>(2025-03-02)</i>
ransomhub ⓘ	●	2025-03-05 10:31	760	2024-02-10	2023-03-09	goencon.com <i>(2025-03-04)</i>
alphv ⓘ	●	N/A	731	2021-09-09	2021-09-09	ipmaltamira <i>(2024-03-03)</i>
akira ⓘ	●	2025-03-05 10:01	643	2023-04-26	2023-04-12	Ray Fogg Corporate P <i>(2025-03-04)</i>

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



Ransomware

Tätergruppierungen, Strukturen und Zahlen

Ransomware-Gruppierungen sind hierarchisch organisiert und strukturiert.

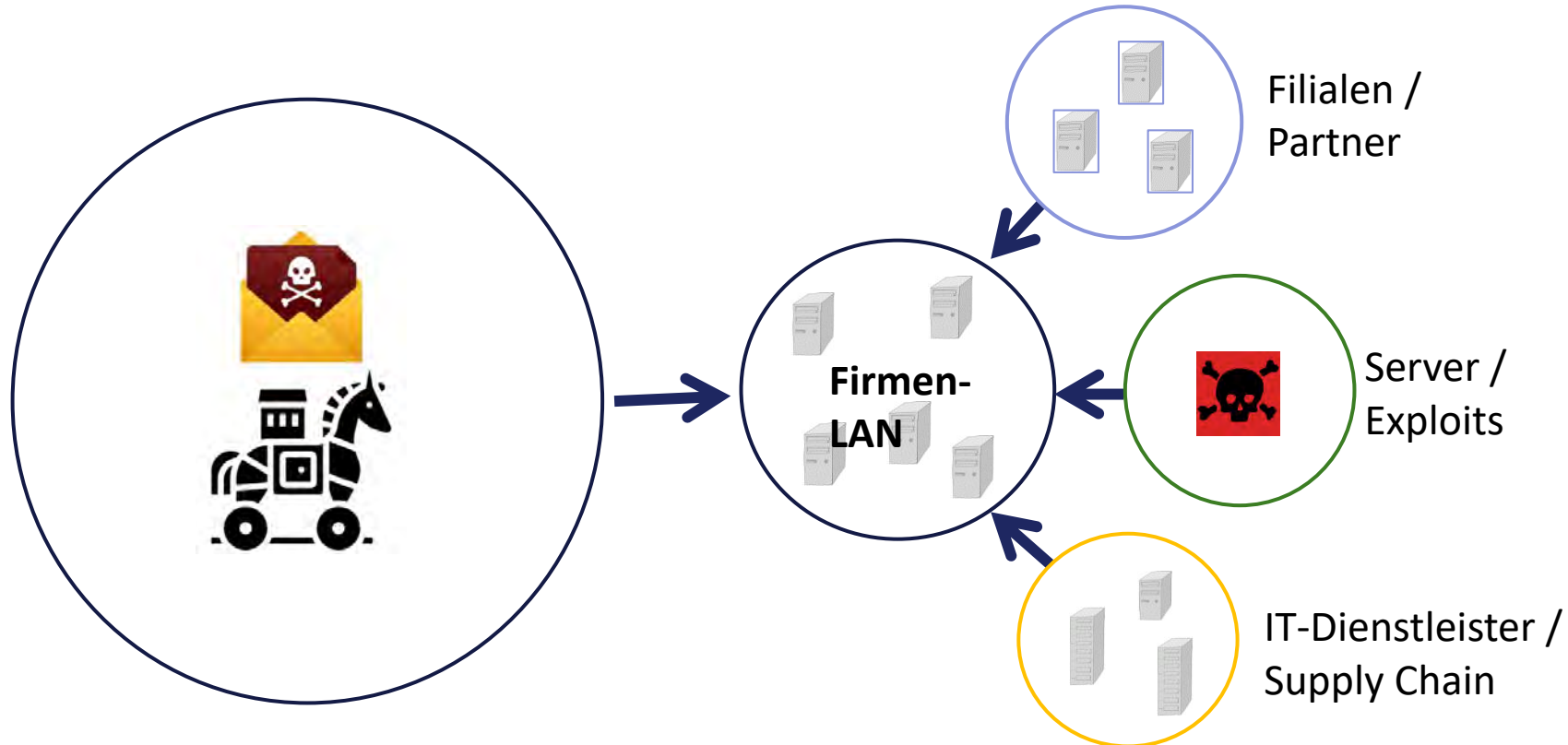
Innerhalb der Gruppierungen gibt es, wie in der herkömmlichen Geschäftswelt, verschiedene Rollen wie

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



Professionelle Hackergruppierungen

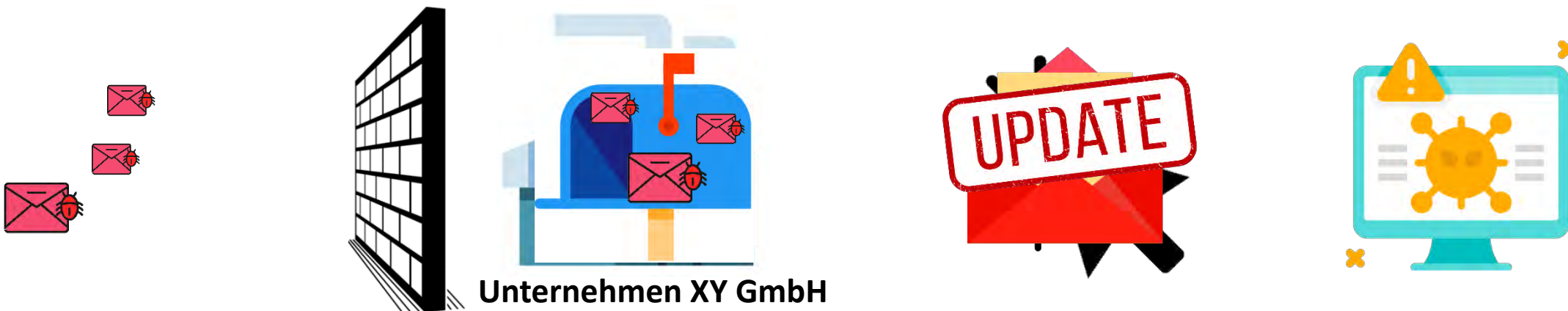
Ablauf eines Ransomware Angriffs





Professionelle Hackergruppierungen

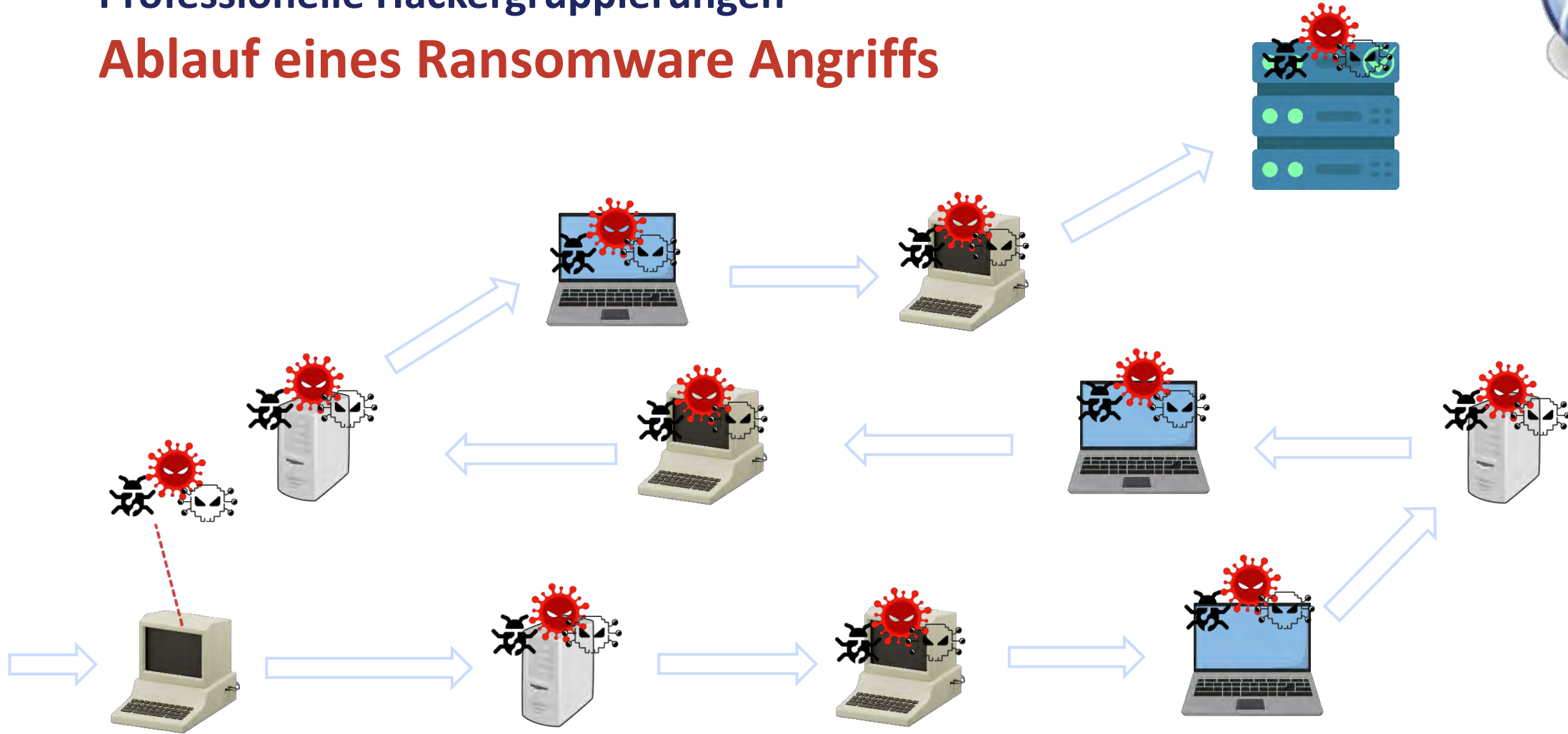
Ablauf eines Ransomware Angriffs





Professionelle Hackergruppierungen

Ablauf eines Ransomware Angriffs





Professionelle Hackergruppierungen

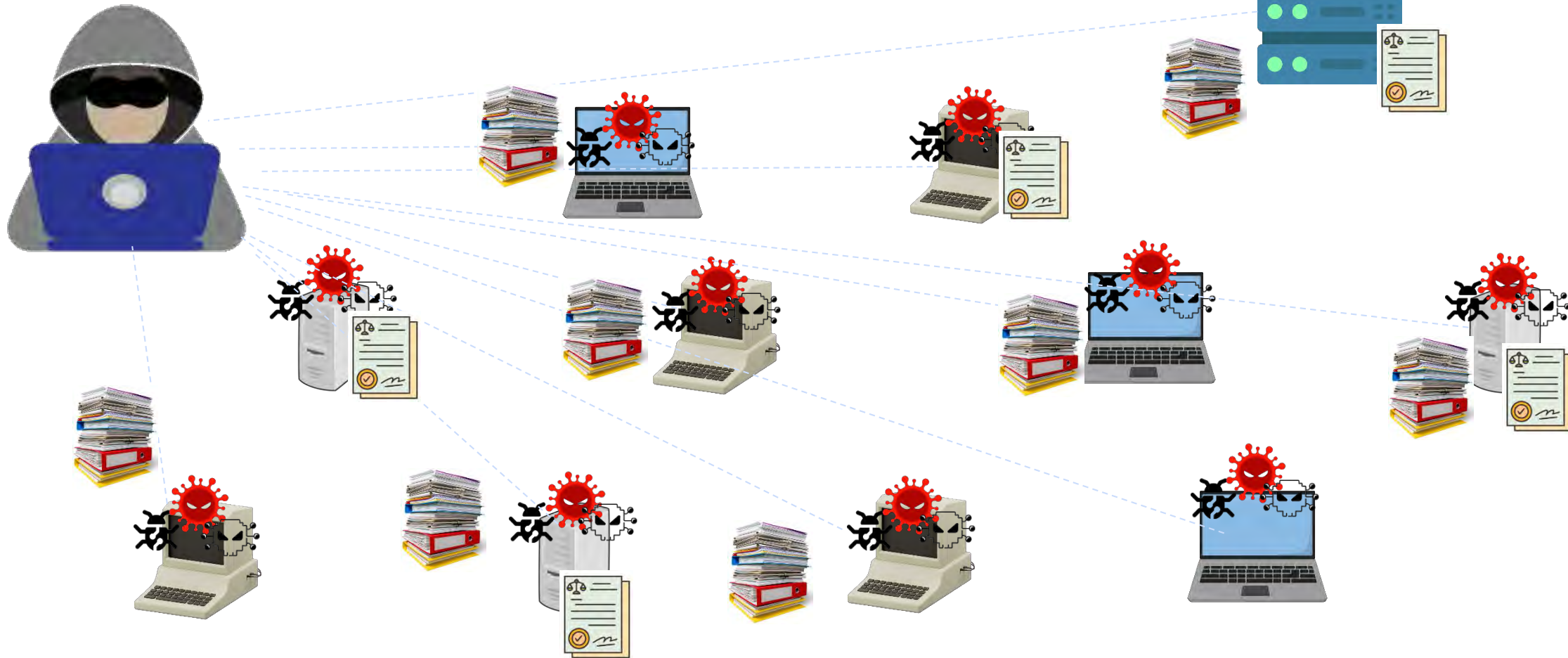
Ablauf eines Ransomware Angriffs





Professionelle Hackergruppierungen

Ablauf eines Ransomware Angriffs





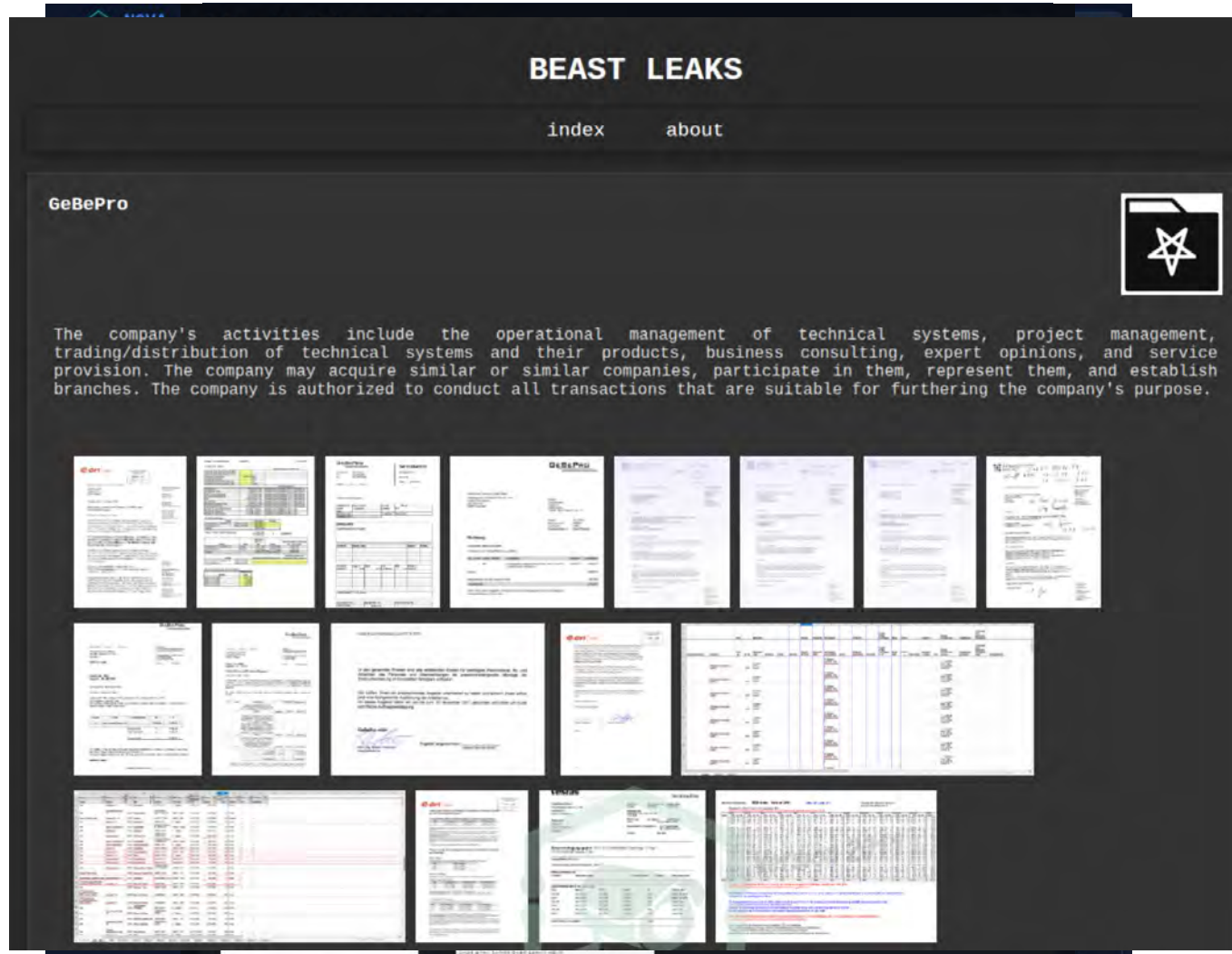
Professionelle Hackergruppierungen

Ablauf eines Ransomware Angriffs





Ransomware - Krisenstab























Verhandlungen

The screenshot shows a Hive live chat interface. On the left, a dark sidebar displays the company profile for XY GmbH: Headquarter: Hamburg, Founded: 1974, Employees: 1821, Revenue: 54 Mill \$, Profit 2024: 8.9 Mill \$. Below this is an 'Uploaded Files' section with an 'Upload' button. The main chat area is titled 'Live Chat Sales dept.' and contains a message bubble that says 'He said ok' with a small flame icon. At the bottom of the chat area is a text input field and a 'Send' button. On the right, a yellow webpage is displayed with the heading 'Decryption Software', a key icon, and a 'Download' button. Text on the page reads 'CONTACT our sales department FIRST via Live chat to get an offer please!'.



 <p>ssp-ce.de </p> <p>Dragonforce</p> <p>Discovered: 2026-03-26</p> <p>SSP Airport Gastronomiegesellschaft mbH operates in the air transport, airport, and aviation service...</p> <p></p>	 <p>Schmiede </p> <p>Akira</p> <p>Discovered: 2026-03-23</p> <p>Schmiede Corporation specializes in high-precision contract machining, focusing on complex and diff...</p> <p></p>
 <p>Resch Maschinenbau </p> <p>Kairos</p> <p>Discovered: 2026-03-21</p> <p>Wir setzen in unserer Position als Fertigungsspezialist neben einer qualitativ hochwertigen Fertigung...</p> <p></p>	 <p>bdtronic </p> <p>Akira</p> <p>Discovered: 2026-03-20</p> <p>bdtronic provides innovative solutions for dispensing, impregnation, hot riveting, and plasma appli...</p> <p></p>
 <p>HLF Heizung-Sanitär GmbH </p> <p>Nightspire</p> <p>Discovered: 2026-03-25 Attack est.: 2026-03-19</p> <p>Data is not available now...</p> <p></p>	 <p>gasteiger.design </p> <p>Dragonforce</p> <p>Discovered: 2026-03-18</p> <p>Gasteiger specializes in creating unforgettable living designs that reflect individual personalities...</p> <p></p>



Weitere Angriffe





Weitere Angriffe

schädliche Apps und Browser Extensions



Oct 02, 2024

**Fake Trading Apps Target
Victims Globally via Apple App
Store and Google Play**

Sicherh
Apps in

seuchte
gesamt



Weitere Angriffe

BadUSB und Hacking Gadgets





Weitere Angriffe

BadUSB und Hacking Gadgets





Weitere Angriffe

BadUSB und Hacking Gadgets



I+f: Grüne Welle mit Hacker-Tool

Stop-and-go im Feierabendverkehr, aber die Pizza wird auf dem Beifahrersitz kalt? Das Hacking-Gadget Flipper Zero schafft (illegale!) Abhilfe.



WLAN-Netzwerke scannen und kopieren
 Bluetooth-Verbindungen kappen
 Smart-TV-Apps öffnen
 Smart-TV-Menüs auslesen (ohne PIN)
 Smart-TV-Geräte steuern (z.B. TV Geräte steuern)



Weitere Angriffe

Fake Wifi

The screenshot shows a Wireshark interface with a packet list table and a detailed view of a selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.025749	172.16.0.122	200.121.1.131	TCP	1400	Window Update [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
5	0.076967	200.121.1.131	172.16.0.122	TCP	1400	Previous segment not captured [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
6	0.076978	172.16.0.122	200.121.1.131	TCP	1400	up ACK #2#1 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
7	0.102939	200.121.1.131	172.16.0.122	TCP	1400	Spurious Retransmission] 10554 → 80 [ACK] Seq=5601 Ack=1 Win=65535 Len=1400 [TCP segment of a reassembled PDU] Len=0
8	0.102946	172.16.0.122	200.121.1.131	TCP	1400	up ACK #2#2 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
9	0.128285	200.121.1.131	172.16.0.122	TCP	1400	Spurious Retransmission] 10554 → 80 [ACK] Seq=7001 Ack=1 Win=65535 Len=1400 [TCP segment of a reassembled PDU] Len=0
10	0.128319	172.16.0.122	200.121.1.131	TCP	1400	up ACK #2#3 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
11	0.154162	200.121.1.131	172.16.0.122	TCP	1400	Spurious Retransmission] 10554 → 80 [ACK] Seq=8401 Ack=1 Win=65535 Len=1400 [TCP segment of a reassembled PDU] Len=0
12	0.154169	172.16.0.122	200.121.1.131	TCP	1400	up ACK #2#4 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
13	0.179906	200.121.1.131	172.16.0.122	TCP	1400	Spurious Retransmission] 10554 → 80 [ACK] Seq=9801 Ack=1 Win=65535 Len=1400 [TCP segment of a reassembled PDU] Len=0
14	0.179915	172.16.0.122	200.121.1.131	TCP	1400	up ACK #2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
15	0.207145	200.121.1.131	172.16.0.122	TCP	1400	80 [ACK] Seq=11201 Ack=1 Win=65535 Len=1400 [TCP segment of a reassembled PDU] Len=0
16	0.207156	172.16.0.122	200.121.1.131	TCP	1400	9554 [ACK] Seq=1 Ack=12601 Win=63000 Len=0
17	0.232621	200.121.1.131	172.16.0.122	TCP	1400	80 [ACK] Seq=12601 Ack=1 Win=65535 Len=1400 [TCP segment of a reassembled PDU] Len=0
18	0.232629	172.16.0.122	200.121.1.131	TCP	1400	9554 [ACK] Seq=1 Ack=14001 Win=63000 Len=0
19	0.258365	200.121.1.131	172.16.0.122	TCP	1400	80 [ACK] Seq=14001 Ack=1 Win=65535 Len=1400 [TCP segment of a reassembled PDU] Len=0

Detailed View of Packet 15:

- Frame 15: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
- Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
- Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
- Transmission Control Protocol, Src Port: 10554, Dst Port: 80, Seq: 11201, Ack: 1, Len: 1400
 - Source Port: 10554
 - Destination Port: 80
 - [Stream index: 0]
 - [TCP Segment Len: 1400]
 - Sequence number: 11201 (relative sequence number)
 - [Next sequence number: 12601 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - 0101 = Header Length: 20 bytes (5)

Packet Bytes:

```

0020  00 7a 29 3a 00 50 a7 5c 30 08 e2 e2 ee bf 50 10  :z]P\ 0....P-
0030  ff ff bc 5e 00 00 42 4f 78 42 56 35 6a 45 52 52  :...^..BO xBV5JERR
0040  71 5a 69 63 39 34 54 77 48 4c 71 46 51 34 78 35  :qZic94Tw HlqFQ4X5
0050  61 62 46 30 77 55 6e 59 73 46 2b 67 6c 44 47 4c  :abF0wUnY sF+g1DGL
0060  33 56 75 35 65 61 33 4d 44 59 77 49 70 63 32 44  :3VuSea3M DYwIpc2D
0070  78 4c 44 4d 74 38 6b 2f 75 42 68 38 6a 48 6d 30  :xLDmt8k/ uBh8jHm0
0080  63 66 54 63 69 35 6a 77 77 4c 2f 56 4c 6f 6c 41  :cFTci5jw wL/VL01A
0090  57 4c 6c 35 63 43 79 4e 6d 63 36 52 70 58 57 7a  :WL15cCyN mc6RpXWz
    
```



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
- 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



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?

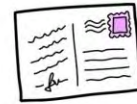
- Der richtige Umgang mit den eigenen Daten im Internet und KI
- Gesunde Skepsis bei E-Mails und Anrufen
- **Sichere Zugänge und MFA**
- Verschlüsselte und signierte E-Mails
- Klar definierte Prozesse bei Überweisungen
- Regelmäßige Schulungen und Übungen
- positive Fehlerkultur
- Technische Lösungen
- 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



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?



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





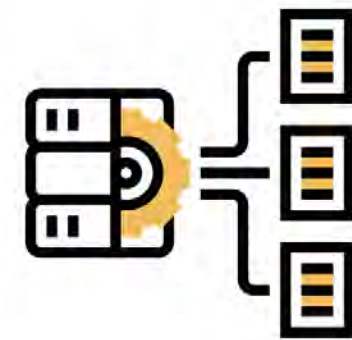
Wie können wir es den Tätern schwer machen?

- 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 (Zero Trust)
- Erkennen und Protokollierung 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



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?



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



Was tun im Ernstfall?

Ruhe bewahren und Überblick verschaffen	
IT / Cyberversicherung / externe Hilfe informieren	
Sofortmaßnahmen	Netzwerke trennen, Backups prüfen, alle aktiven Sessions beenden und VPN Zugänge sperren
ZAC informieren und telefonisch beraten lassen	040 4286 75455 zac@polizei.hamburg.de (bei akuten Notfällen auch 110 möglich)
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

CRIME SCENE - DO NOT CROSS

CRIME SCENE - DO NOT CROSS



Die wichtigsten Handlungsempfehlungen

- **Setzen Sie sich frühzeitig (vor dem Ernstfall) mit dem Thema auseinander**
- **Verschaffen Sie sich einen Überblick über Ihren Daten und Systeme**
- **Suchen Sie ggf. jetzt schon Kontakt zu Unternehmen und Stellen, die Sie im Notfall unterstützen könnten.**
- **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



Phishen Impossible

- Erklärvideos
- Quiz
- Aktuelle Phishing-Phänomene

Transferstelle Cybersicherheit

- Der CYBERSicher Check
- Workshops & Veranstaltungen
- Notfallhilfe





Vielen Dank für Ihre Aufmerksamkeit



ZAC Kontakt



PowerPoint