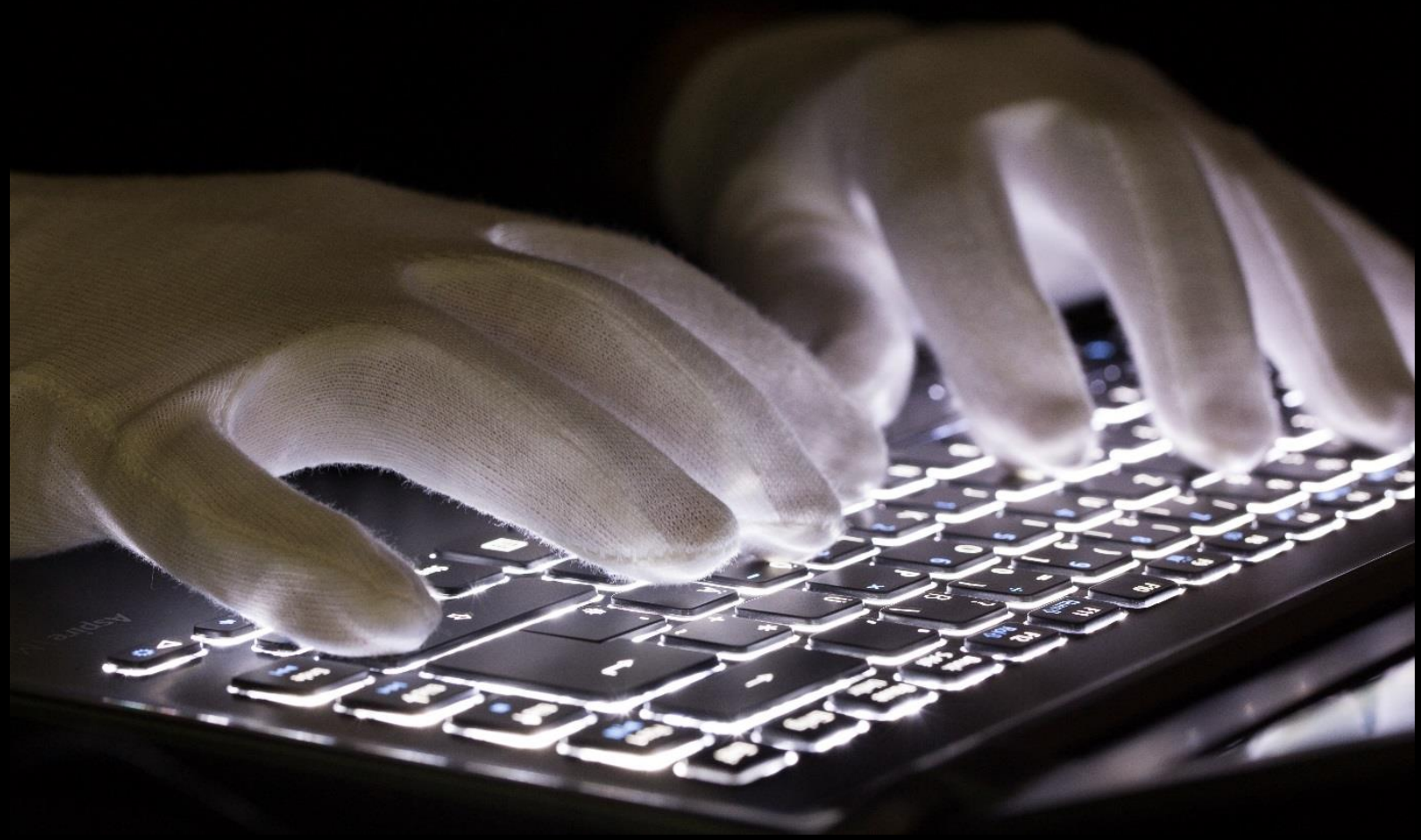
POLIZEI BERLIN

BERLIN

KHK Borries

ZAC Berlin – Zentrale Ansprechstelle Cybercrime



POLIZEI BERLIN

Opferseite

BERLIN

Basler Schulnetz gehackt, Schü… Darknet

Cyber-Angriff auf …

Cyber- … Partei

… Mail-Kon…

… IT der Deuts…

Cybersicherheit: ESA-Satellit im Orbit

heise online › Security › Cybergang AlphV bei internationalem Rüstungszulieferer Ultra eingedrungen

Cybergang AlphV bei internationalem Rüstungszulieferer Ultra eingedrungen

Die Cybergang AlphV ist weiter aktiv. Sie hat im Darknet Daten veröffentlicht, die vom Rüstungszulieferer Ultra stammen.

Lesezeit: 2 Min. In Pocket speichern

(Bild: Pixels Hunter/Shutterstock.com)

08.01.2024 15:38 Uhr | Security

Von Dirk Knop

Cybercrime: Erpressergang greift Hotelkette MotelOne an

Terabytes interne Daten der Hotelkette MotelOne stehen offen im Darknet. Darunter befinden sich auch Buchungs- und Zahlungsinformationen und interne Zugänge.

87

Lesezeit: 1 Min. In Pocket speichern

(Bild: BeeBright/Shutterstock.com)

30.09.2023 16:47 Uhr | Security

Die Cyber-Erpresser …

https://www.heise.de/security/

https://eurepoc.eu/de/dashboard-de/

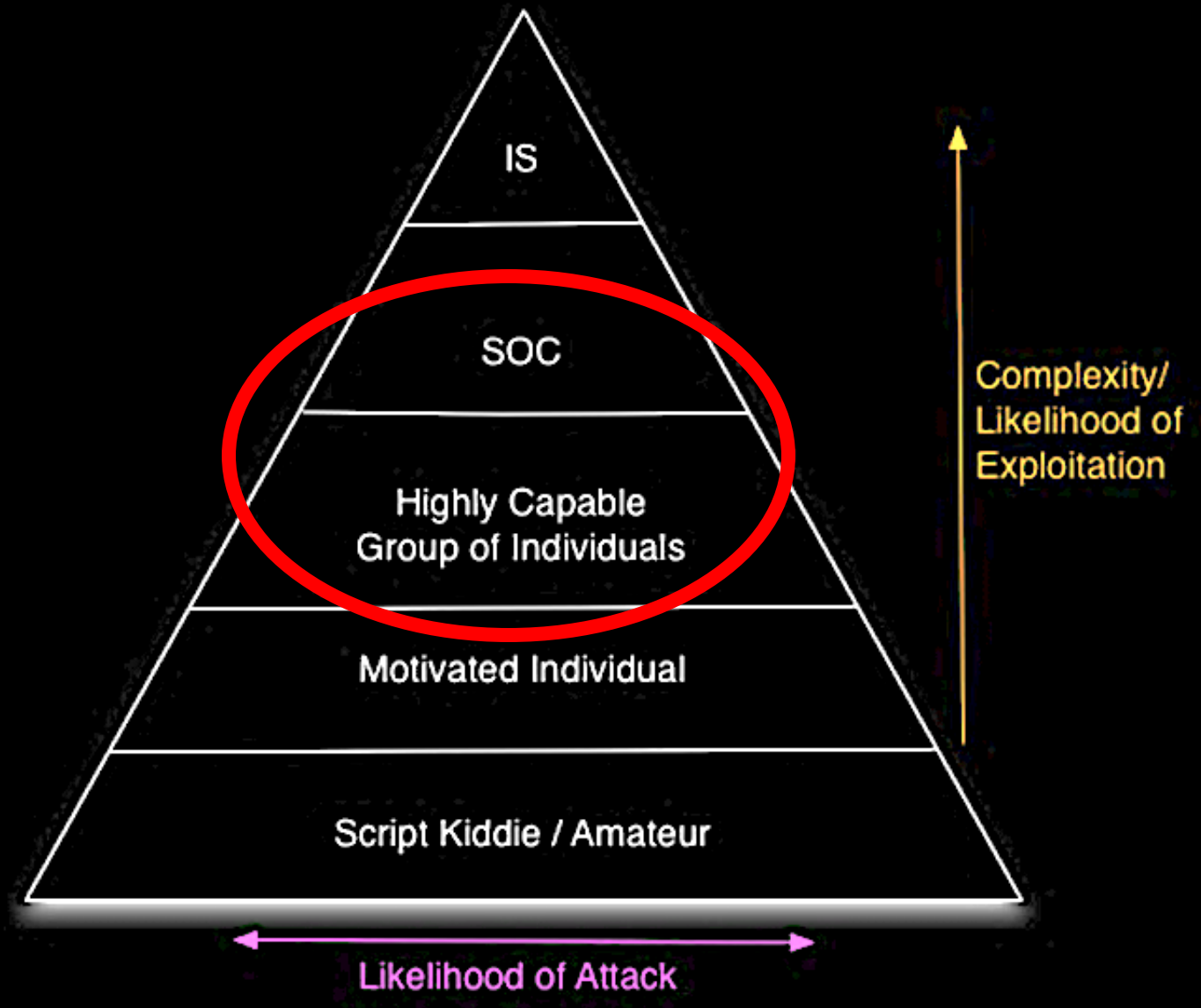
https://www.security-incidents.de/sicherheitsvorfall-datenbank/

https://www.hackmageddon.com/2024/12/18/the-biggest-data-breaches-of-2024/

https://www.security-incidents.de/sicherheitsvorfall-datenbank/

https://www.berlin.de/polizei/aufgaben/praevention/cybercrime/artikel.1316711.php

die Gegenseite



IS = Intelligence services

SOC = Serious organized Crime

http://openstack.booktype.pro/security-guide/threat-classification-actors-and-attack-vectors/

POLIZEI BERLIN

Cybercrime: Angriffsvektoren

BERLIN

komplexe Netzwerktechnologien

unzureichende Absicherung industrieller Steuerungssysteme

„Digitale Sorglosigkeit“

Assume Breach

tech lash

Schwachstellen / Exploits

Innentäter

veraltete Software und ungepatchte Systeme

mobile Endgeräte (BYOD vs. COPE)

POLIZEI BERLIN

Cybercrime: aktuelle Bedrohungen

BERLIN

(gestreut)

Spam (-E-Mails)

Schadprogramme

Datendiebstahl

Drive-by-Exploits und Exploit-Kits („RDP“)

Botnetze

(gezielt)

Social Engineering (!)

Identitätsdiebstahl

(Distributed) Denial of Service (DDoS)

Advanced Persistent Threats (APT)

Nachrichtendienstliche Cyber-Angriffe

POLIZEI BERLIN

Typischer Ablauf eines Angriffs und Beobachtungen

BERLIN

Wie erfolgen die Angriffe?

Erpressen

1. Entschlüsselung d. Daten
2. Veröffentlichung d. Daten
3. Verkauf/Nutzung d. Daten

erster Computer übernommen

Domain Admin Account übernommen

Angreifer entdeckt

Vorbereitung

11-14 Monate

24-48 Stunden

Externe Aufklärung → Initialer Zugriff → Zugriff sichern → Interne Aufklärung → Zugriff Ausweiten

Zugriff Ausweiten → Daten ausleiten → **Erpressen**

Zugriff Ausweiten → Mission Abschließen → Daten verschlüsseln → **Erpressen**

Lateral Movement


LOCK FILE
ALL YOUR IMPORTANT FILES ARE ENCRYPTED!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
Restore you data posible only buying private key from us.
There is only one way to get your files back:
01.
contact us
UTox
Email
uTox ID:
https://utox.org/
Email: contact@contipauper.com
02.
Through a Tor Browser - recommended
Download Tor Browser - https://www.torproject.org/ and install it.
Open link in Tor Browser -
http://zqaflhty5hyz
This link only works in Tor Browser!
Follow the instructions on this page
ATTENTION!
Do not try to recover files yourself. this process can damage your data and recovery will become impossible
Do not rename encrypted files.
Do not waste time trying to find the solution on the Internet. The longer you wait, the higher will become the decryption key price
Decryption of your files with the help of third parties may cause increased price (they add their fee to our).
Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
Thanks to the warning wallpaper provided by lockbit, it's easy to use

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive-Crime-Gruppen/aktive-crime-gruppen_node.html

Cybercrime: Schäden

https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf

https://www.cyberagentur.de/programme/sck/#:~:text=Ziel%20des%20Programms%20SCK%20ist,die%20durch%20Cyberkriminalität%20verursacht%20werden.

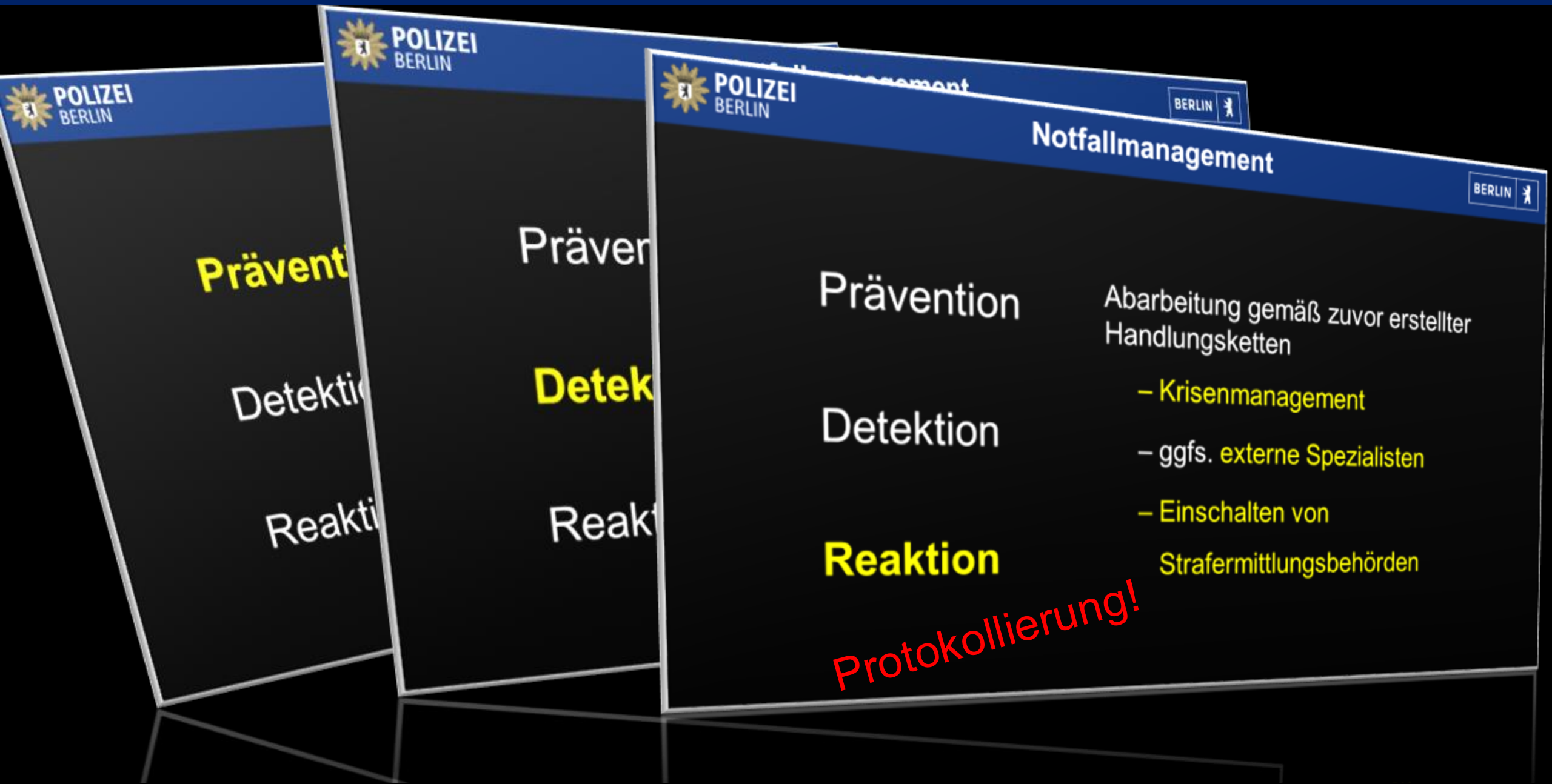
Best practice aus einem Unternehmen mit 70 Mitarbeitern

- Backup-Strategie
  - Auf Band und USB-Festplatten rollierend, an unterschiedlichen Orten
  - Spiegelung der Daten auf zweiten Standort
- Firewall, gemanaged und regelmäßig angepasst, KI geplant
- Fernzugriffe
  - via VPN und 2-Faktor-Authentifizierung
  - Geräte COPE
- Passwörter: kompliziert, einmalig für jeden Account, werden verschlüsselt in der Cloud abgelegt, einmal pro Monat ausgedruckt im Safe abgelegt
- Positive Fehlerkultur, familiäre Firmenatmosphäre
- Auch digitales On-Boarding / Off-Boarding für Mitarbeiter
- Chefs gehen mit gutem Beispiel voran
- „Probesterben“ (oder auch „Übungen“)

POLIZEI BERLIN

Gegenmaßnahmen

BERLIN



https://www.computerweekly.com/de/definition/Attribution-von-Cyberangriffen

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive-Crime-Gruppen/aktive-crime-gruppen_node.html

Cybercrime: Polizei übernimmt IT-Infrastruktur der Ransomware-Gruppe "Hive"

Deutsche Ermittler haben in Zusammenarbeit mit den Behörden in den Niederlanden und den USA die Kontrolle über das Ransomware-Netzwerk "Hive" übernommen.

Die Behörden haben auch die Darknet-Sites der Hive-Gruppe übernommen. (Bild: Polizeipräsidium Reutlingen)

UPDATE **26.01.2023, 17:21 Uhr** **Lesezeit: 3 Min.**

Von Volker Briegleb

Die Behörden haben auch die Darknet-Sites der Hive-Gruppe übernommen. (Bild: Polizeipräsidium Reutlingen)

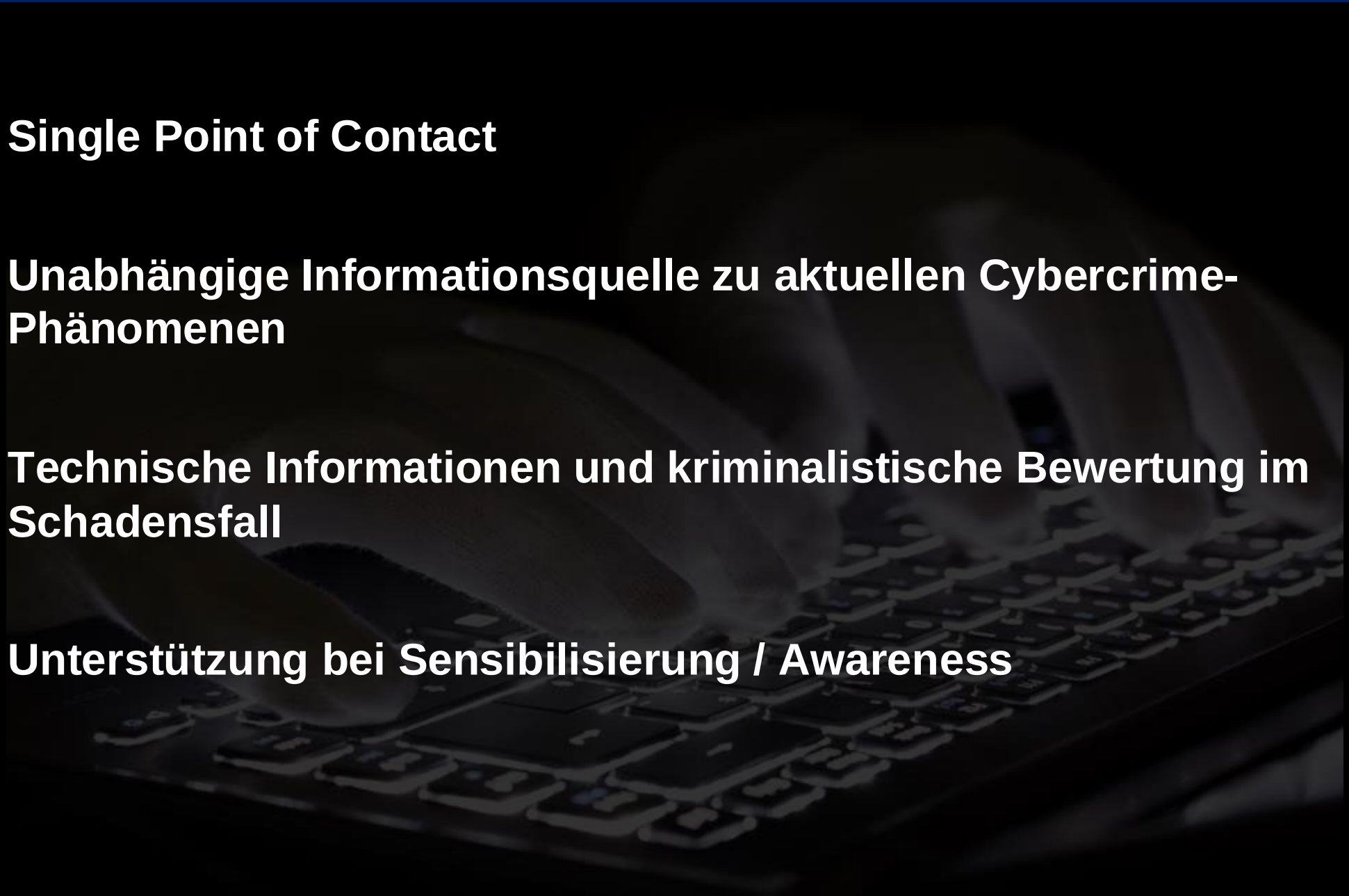
https://www.heise.de/news/Cybercrime-Polizei-zerschlaegt-Ransomware-Gruppe-Hive-7472192.html

https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/241203_Festnahme_Crimenetwork.html

POLIZEI BERLIN

im Zweifel … ZAC der Polizei

BERLIN



Single Point of Contact

Unabhängige Informationsquelle zu aktuellen Cybercrime-Phänomenen

Technische Informationen und kriminalistische Bewertung im Schadensfall

Unterstützung bei Sensibilisierung / Awareness

Cybercrime

Interview mit Olaf Borries

„Es wird Tätern viel zu häufig leicht gemacht“

Olaf Borries, Kriminalhauptkommissar bei der ZAC – Zentrale Ansprechstelle Cybercrime für die Wirtschaft im Landeskriminalamt Berlin – ist Experte beim Thema Cybercrime. Im Gespräch mit dem KV-Blatt erzählt er, welche Präventionsmaßnahmen Praxen treffen sollten.

Warum sind gerade Arztpraxen beliebte Angriffsziele von Cybercrime? Welche Motivation steckt hinter einem solchen Angriff?

In Arztpraxen werden sehr viele sensible Daten erzeugt und verwaltet, ohne die eine Praxis nicht arbeiten kann und die auch ein hohes Schadenspotential besitzen. Sollten Daten hier abgeflossen oder verschlüsselt sein, so ist der Handlungsdruck entsprechend hoch. Als Motiv sind sehr häufig, besonders im Bereich der Erpressung – Stichwort ‚Ransomware‘ –, finanzielle Interessen zu nennen.

Wo sehen Sie vor allem kritische Angriffspunkte in Arztpraxen?

praxis aufzubauen; zum Beispiel durch die Verschlüsselung der Daten. Eine Entschlüsselung erfolgt dann erst gegen die Zahlung eines Lösegeldes. Als Polizei raten wir grundsätzlich davon ab, zu zahlen. In der letzten Zeit kam es immer häufiger dazu, dass die Daten der geschädigten Institution vorher heruntergeladen wurden und es im Falle der Nichtbezahlung zur Drohung der Veröffentlichung der Daten führte. Ein weiterer Bereich – nach unserer Erfahrung nicht so im Fokus bei Arztpraxen – sind so genannte DDos-Angriffe. Darunter versteht man eine Überlastung von Internetseiten durch massive Anfragen, sodass ein Aufrufen der Seite nicht möglich ist. Dies wird dann ebenfalls mit Erpressung verbunden.

Mitgliederbereich der Website der KV Berlin noch einmal anschauen.

oder benötigen Informationen zum Thema? Kontaktieren Sie die Zentrale Ansprechstelle für Cy-

Lars Huwald

Astrid Frohloff

Rainer Stock

BERLIN

Gedanken zum Schluss

1. Cybercrime funktioniert seit Jahren hervorragend – größtenteils unverändert!
2. Die Phänomene werden nur in Nuancen und in relativ langen Zeiträumen angepasst

   – das Alte funktioniert ja … aber KI nimmt langsam Einzug
3. Medienkompetenz lässt bei vielen Mitbürgern sehr zu wünschen übrig
4. Gesundes Misstrauen beendet die meisten Taten bei Cybercrime („Betrug“)
5. Sichere digitale Authentifizierung (Forschung bei der Cyberagentur)
6. **jede Art von Vorbeugung / Sensibilisierung / Prävention / Vorbereitung hilft!**

Vishing-Attacken explodieren: Wenn dein Chef anruft, aber es gar nicht dein Chef ist
https://www.business-punk.com/2025/03/vishing-attacken-explodieren-wenn-dein-chef-anruft-aber-es-gar-nicht-dein-chef-ist/?utm_source=flipboard&utm_content=topic%2Fde-technologie

Phishing	„konventionell“ per E-Mail
Vishing	per Anruf
Smishing	als Textnachricht

Ebenenbruch / Medienwechsel / Codewörter

Mögliche Bedrohungsszenarien

Mittels der beschriebenen Verfahren ist es heute auch teilweise für technisch versierte Laien möglich, mediale Identitäten zu manipulieren, wodurch sich zahlreiche Bedrohungsszenarien ergeben:

[…]

•**Social Engineering**: Deepfake-Verfahren können außerdem dazu verwendet werden, gezielte Phishing-Angriffe („Spear-Phishing“) durchzuführen, um Informationen und Daten zu gewinnen.

Auch kann ein Angreifer diese Technologie zur Durchführung von Betrug und zur Abschöpfung finanzieller Mittel nutzen. **Beispielsweise könnte er eine Person mit der Stimme von deren Führungskraft anrufen, um eine Geldtransaktion auszulösen („CEO-Fraud“).**

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Gesetzliche Grundlagen

Regelungen für Organisationen zur IT-Sicherheit u.a.

- IT-Sicherheitsgesetz
- Cybersecurity Act
- Cyber Resiliance Act
- Critical Entities Resilience Directive
- Definition KRITIS
- KRITIS-Dachgesetz
- KRITIS-Verordnung
- Digital Operational Resilience Act kurz DORA
- NIS-Richtlinie
- NIS-2-Richtlinie
- ISO/IEC 27001
- BSI IT-Grundschutz
- DIN SPEC 27076
- DSGVO (bzw. EKD-DSG, KDG)
- GmbH-Gesetz (GmbHG)
- Aktiengesetz (AktG)
- DORA (Digital Operational Resilience Act)

Keine Garantie auf Vollständigkeit

POLIZEI BERLIN

BERLIN

ZAC Zentrale Ansprechstellen Cybercrime
für die Wirtschaft der Länder und des Bundes

„Standard“-Fragen
- Tatütataa
- Mitnahme Hardware
- Presse
- Cyberversicherung

für den harten Kern

fortlaufendes Sicherheitskonzept

clevere Datensicherungen

Rollen- und Rechtekonzepte

Awareness -> Faktor Mensch

Notfallpläne

KHK Borries, KHK Huwald & POK Wende
LKA 724 Cybercrime
ZAC Berlin – Zentrale Ansprechstelle Cybercrime

+49 30 4664 972 972
zac@polizei.berlin.de

POLIZEI
BERLIN

BERLIN

Polizei Berlin - Landeskriminalamt

ZAC – Zentrale Ansprechstelle Cybercrime für die Wirtschaft, Behörden und Verbände

Friesenstr. 16
10965 Berlin

Tel.: 030 - 4664 / 972 972
E-Mail: zac@polizei.berlin.de

www.polizei.de
/ Polizeiliche Einrichtungen
/ Zentrale Ansprechstellen Cybercrime der Polizeien