Cybercrime

Aktuelle Lage & Phänomene / April 2024

KHK Borries, ZAC Berlin – Zentrale Ansprechstelle Cybercrime

LKA 724 Cybercrime im engeren Sinne

1. Vorstellung der Dienststelle
2. Aktuelle Phänomene
3. Wer wird angegriffen?
4. Wer greift an?
5. Was sind die Ziele von Angriffen?
6. Wie erfolgen die Angriffe?
7. Wie kann ich mich bzw. mein Unternehmen schützen?
8. Was sollte ich nach einem Schadensereignis tun?
9. Warum Polizei einschalten?

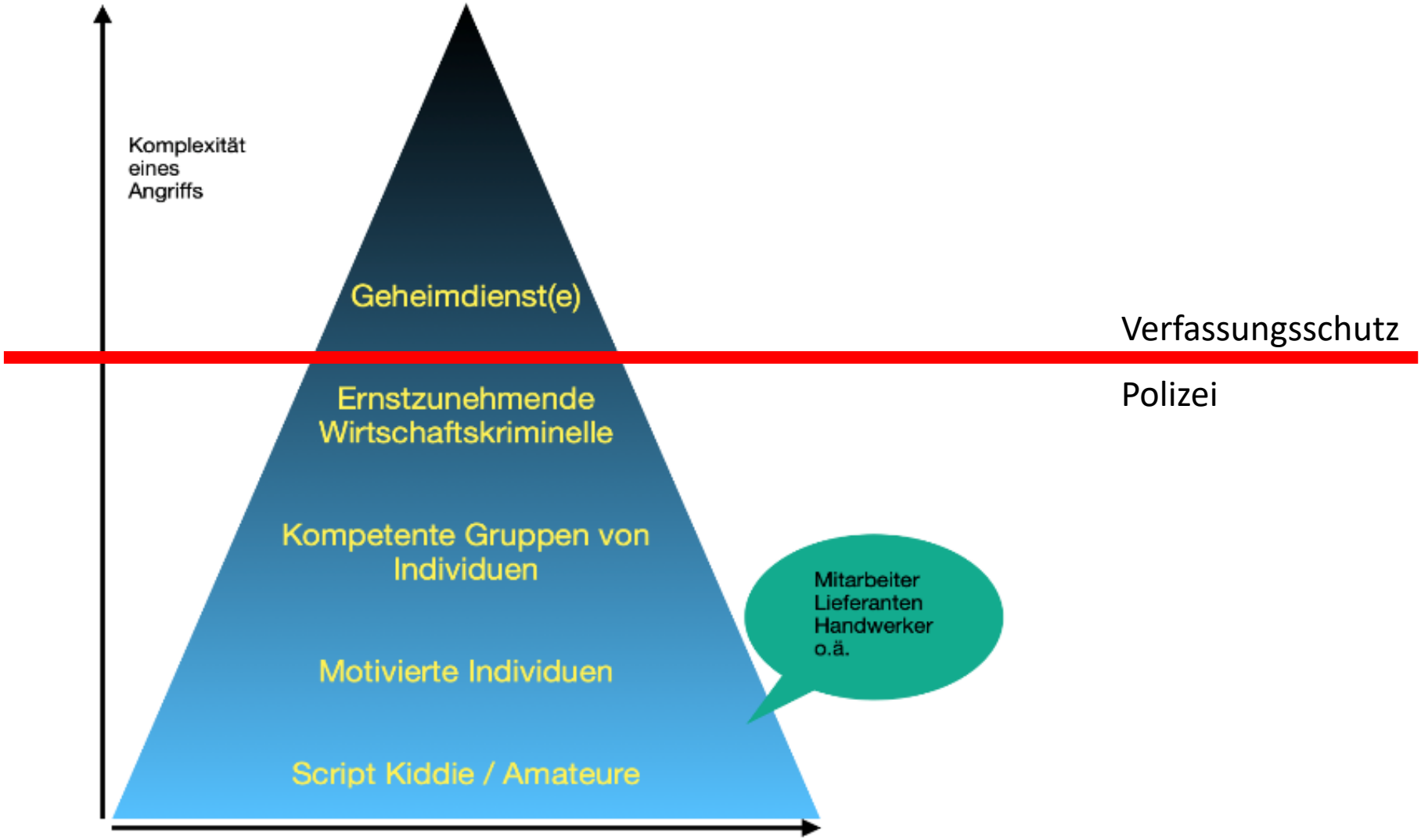
ZAC - Zentrale Ansprechstelle Cybercrime
für die Wirtschaft im LKA Berlin

Polizei Berlin
ZAC – Zentrale
Ansprechstelle Cybercrime
KHK Borries
KHK Huwald
Friesenstr. 16
10965 Berlin

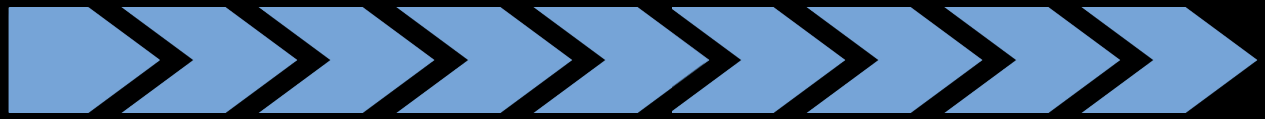
Tel.: 030 - 4664 / 972 972
E-Mail:
zac@polizei.berlin.de

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

Wer greift an?



kriminelle Wertschöpfung



Handel mit Exploits

Entwicklung von Software

Bereitstellen von Infrastruktur

Einsatz von „Hacking“ / Phishing

Zusammenführen von Daten

Weiterverwertung von Daten

- **Handel**
- **Betrug**
- **Erpressung**

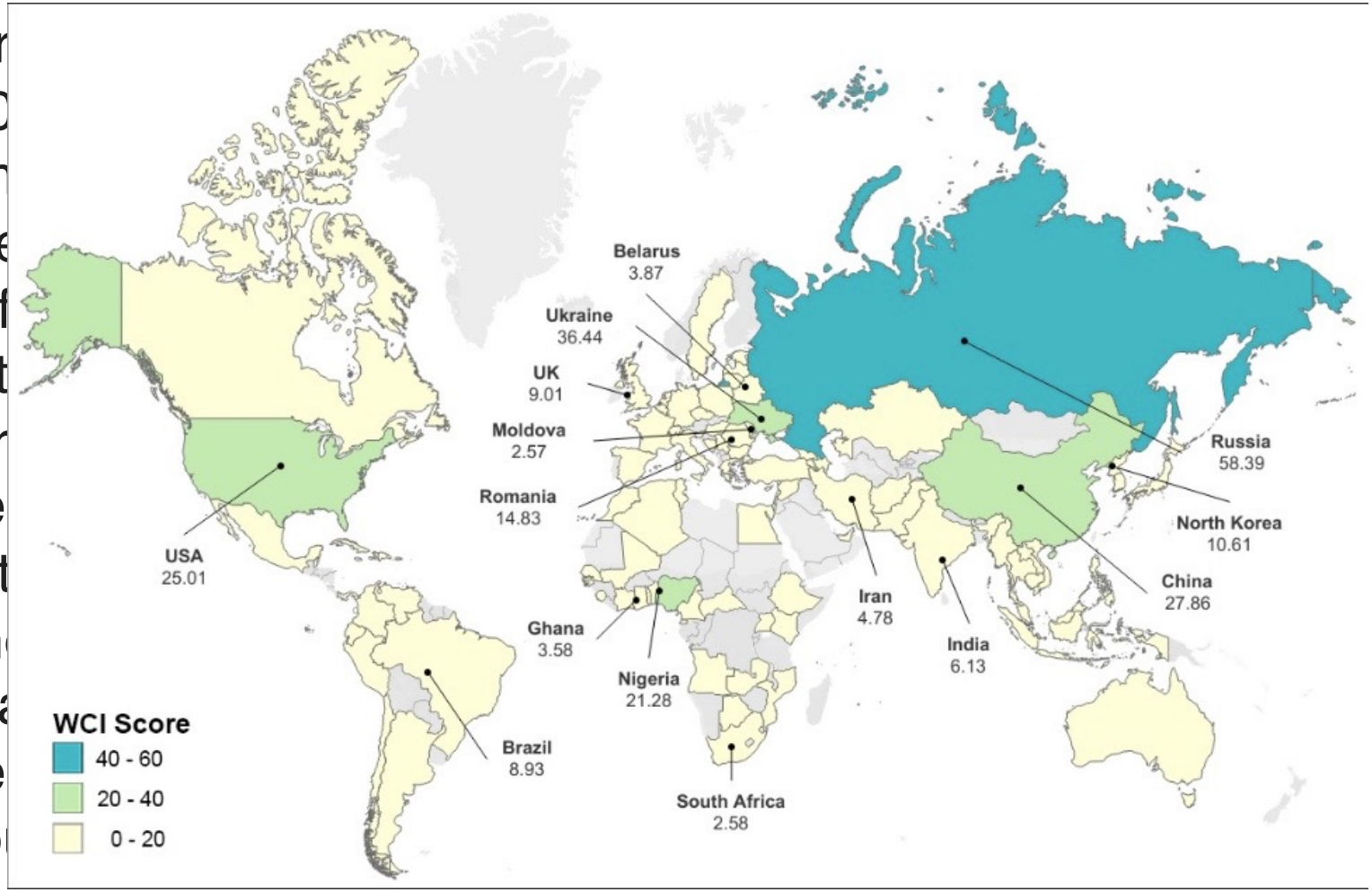
reale Wertschöpfung

Mapping the global geography of cybercrime with the World Cybercrime Index

Miranda Bruce, Jonathan Lusthaus, Ridhi Kashyap, Nigel Phair, Federico Varese

Published: April 10, 2024 • https://doi.org/10.1371/journal.pone.0297312

… This paper
to October 20
intelligence/in
an anonymize
cybercrime of
five major cat
they consider
types of cybe
according to t
offenders. Th
Index, a globa
types of cybe
number of co



https://doi.org/10.1371/journal.pone.0297312.t001

Was sind die Ziele der Angreifer?

1. finanzielle Interessen,
2. Informationsbeschaffung,
3. Sabotage,
4. Einflussnahme,
5. Durchsetzung politischer Interessen

Wie erfolgen Angriffe?

Angriffsmittel und –methoden

gestreut

Spam (-E-Mails)

Schadprogramme

Datendiebstahl

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

gezielt

Botnetze

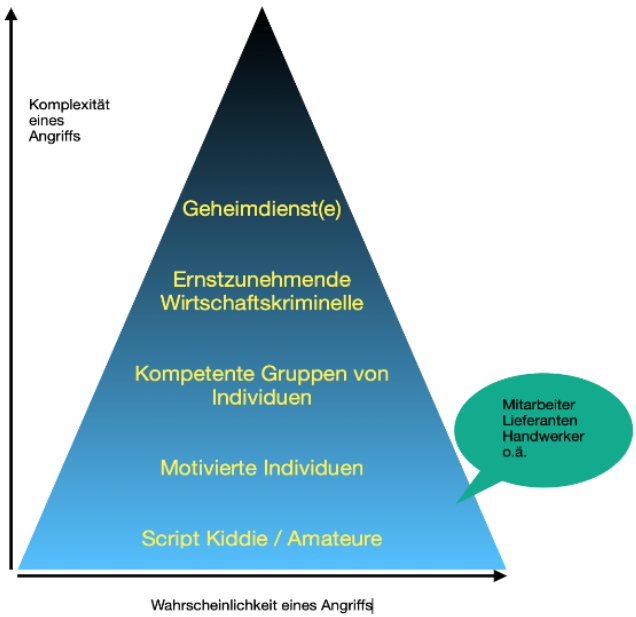
Social Engineering (!)

Identitätsdiebstahl

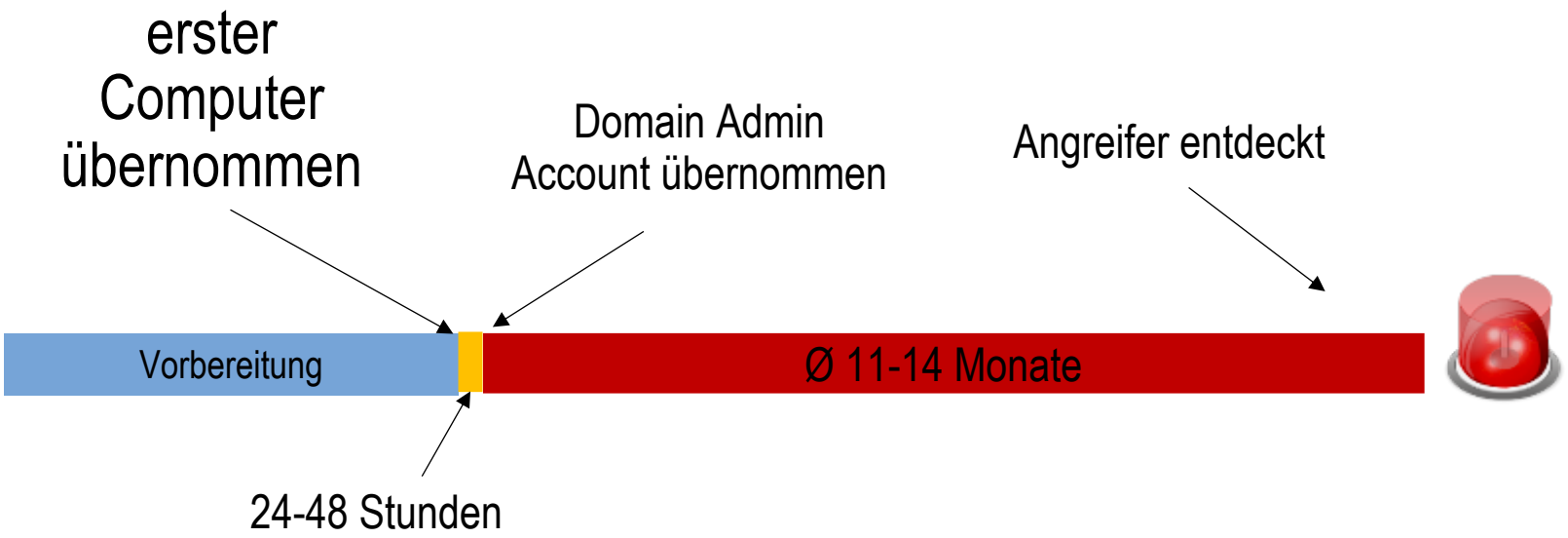
(Distributed) Denial of Service (DDoS)

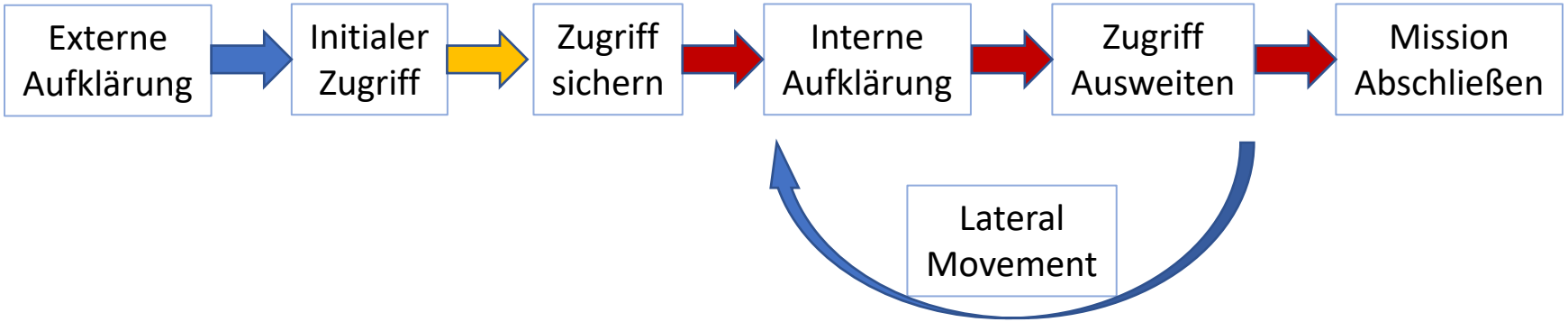
Advanced Persistent Threats (APT)

Nachrichtendienstliche Cyber-Angriffe



Typischer Ablauf eines Angriffs und Beobachtungen





Warum sind Angriffe erfolgreich?

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)

Notfall-Management

Prävention

- **Sicherheitskonzept**
- Kontakt zu Experten/ZAC
- **Awareness** für Mitarbeiter

(*regelmäßig, unregelmäßig und kreativ*)

Detektion

- Penetration-Tests
- Capture the Flag o.ä.
- Alarmierungslisten

Reaktion

- **Back-up Konzept**
- IT-Laufkarte oder z.B. Mauspad mit Rufnummer der IT-Abteilung

Notfall-Management

Prävention

Detektion

Reaktion

7 einfache Methoden für mehr Sicherheit

1. Nur Dienste mit Ende-zu-Ende-Verschlüsselung nutzen
2. genutzte Geräte aktuell halten -> Sicherheitsupdates
3. Passwörter und Entsperrcodes **geheim** halten
4. Jedes Passwort nur einmal verwenden -> Passwortmanager
5. Möglichst 2-Faktor-Authentifizierung nutzen
6. Sensibler Umgang mit Apps/Software und Daten
    1. Je weniger desto besser
    2. Auf die Quelle/Herkunft achten
7. Webcam(s) physisch abdecken

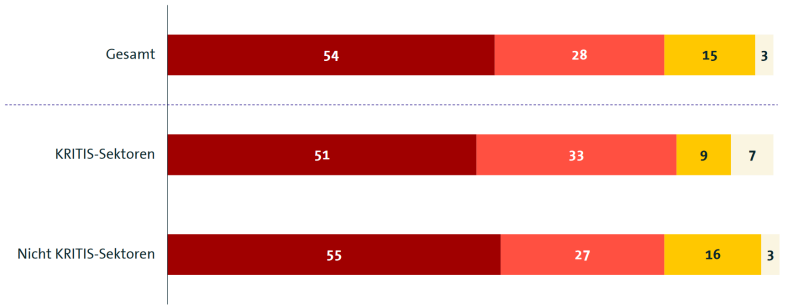
Siehe auch https://t3n.de/news/cybersecurity-experte-erklaert-einfache-methoden-schutz-vor-haeckern-1618295/

Studie des bitkom e.V.

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

Wirtschaft erwartet deutliche Zunahme von Cyberattacken

Wie wird sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den nächsten 12 Monaten im Vergleich zu den letzten 12 Monaten voraussichtlich entwickeln?

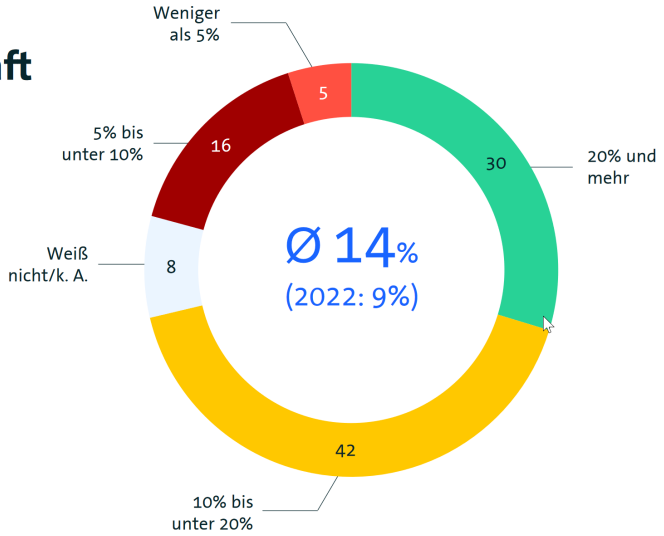


14 Basis: Alle Unternehmen (n=1.002) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen | Quelle: Bitkom Research 2023

bitkom

Cybersicherheit: Investitionsbereitschaft steigt

Wie hoch ist geschätzt der Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget Ihres Unternehmens?



15 Basis: Alle Unternehmen (n=1.002) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen | Quelle: Bitkom Research 2023

bitkom

Notfall-Management
Sicherheitsschulungen / Awareness

- *Sensibilisierung* für Informationssicherheit
- *Mitarbeiter*bezogene Sicherheitsmaßnahmen
- *Produkt*bezogene Sicherheitsmaßnahmen
- Bedeutung der *Datensicherung* (Backup) und deren Durchführung
- Verhalten bei Auftreten von Schadsoftware (*Handlungsleitfäden*)
- Umgang mit *personenbezogenen Daten*
- Einweisung in *Notfallmaßnahmen*
- *Notfallübungen*
- Vorbeugung gegen *Social Engineering*
- *Fehlerkultur im Unternehmen*

Notfall-Management

Prävention

- Ganzheitliches Sicherheitskonzept realisieren und permanent fortschreiben (PDCA – Plan/Do/Check/Act)
- Sicherheitsstandards regelmäßig analysieren
- Sicherheitsvorkehrungen kontrollieren, Verstöße sanktionieren
- Frühwarnsystem zur Erkennung von Know-How-Verlusten

Detektion

Assume Breach

- *Antiviren-Software / Firewall /* Intrusion-Detektion / Sandbox / Security Information und Event Management (SIEM) / Anti-Krypto-Programme / Whitelisting v. Exe. / Security Orchestration, Automation and Response (SOAR)
- Security-Monitoring-Konzept (was darf wann von wem protokolliert und ggfs. eingesehen werden?) und Netzwerk-(Traffic)-Analyse

Reaktion

Notfall-Management

Prävention

Detektion

Reaktion

Lessons learned?

- Abarbeitung gemäß zuvor erstellter Handlungsketten („Notfallhandbuch“)
- Alarmierung(en) z.B. **Krisenstab**
- IT-Abteilung / ext. IT-Dienstleister
- Rechtsabteilung / ext. Jurist
- Firmenleitung / Geschäftsführung
- Datenschutz- bzw. Informationssicherheitsbeauftragter
- Betriebsrat o.ä.
- ggfs. Hinzuziehung von externen Spezialisten
- Einschaltung von Strafermittlungsbehörden
- Mit dem Zwecke
1. (weiteren) Schaden vom Unternehmen (und deren Kunden) abzuwenden
2. als Unternehmen wieder handlungsfähig zu werden
3. gerichtsverwertbare Beweise zu sichern um den Täter ermitteln und bestrafen zu können

Gefahrenabwehr

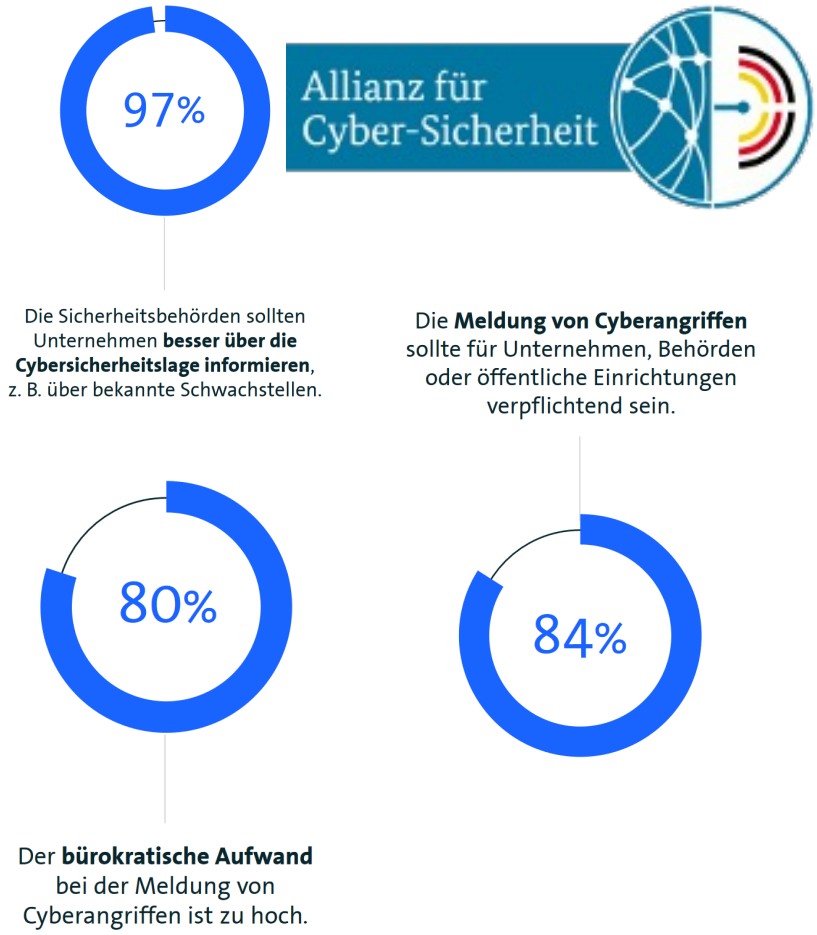
Strafverfolgung

ZACs sind

- **Single Point of Contact für die jeweilige Landespolizei**
- **Unabhängige Informationsquelle zu aktuellen Cybercrime-Phänomenen**
- **Bieten technische Informationen und kriminalistische Bewertung im Schadensfall**
- **Leisten Unterstützung bei Sensibilisierung / Awareness**

Zu wenige Informationen, zu viel Bürokratie

Inwieweit stimmen Sie den folgenden Aussagen zu?



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

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.

Foto: KVK Huwald

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

Erfolge der Cybercrime Bekämpfung!

Januar 2021	Emotet
April 2022	Hydra Market
März 2023	ChipMixer
April 2023	Genesis Market
August 2023	QakBot
Februar 2024	Crimenetmarket

WirtschaftsWoche

HACKER UNTER DRUCK

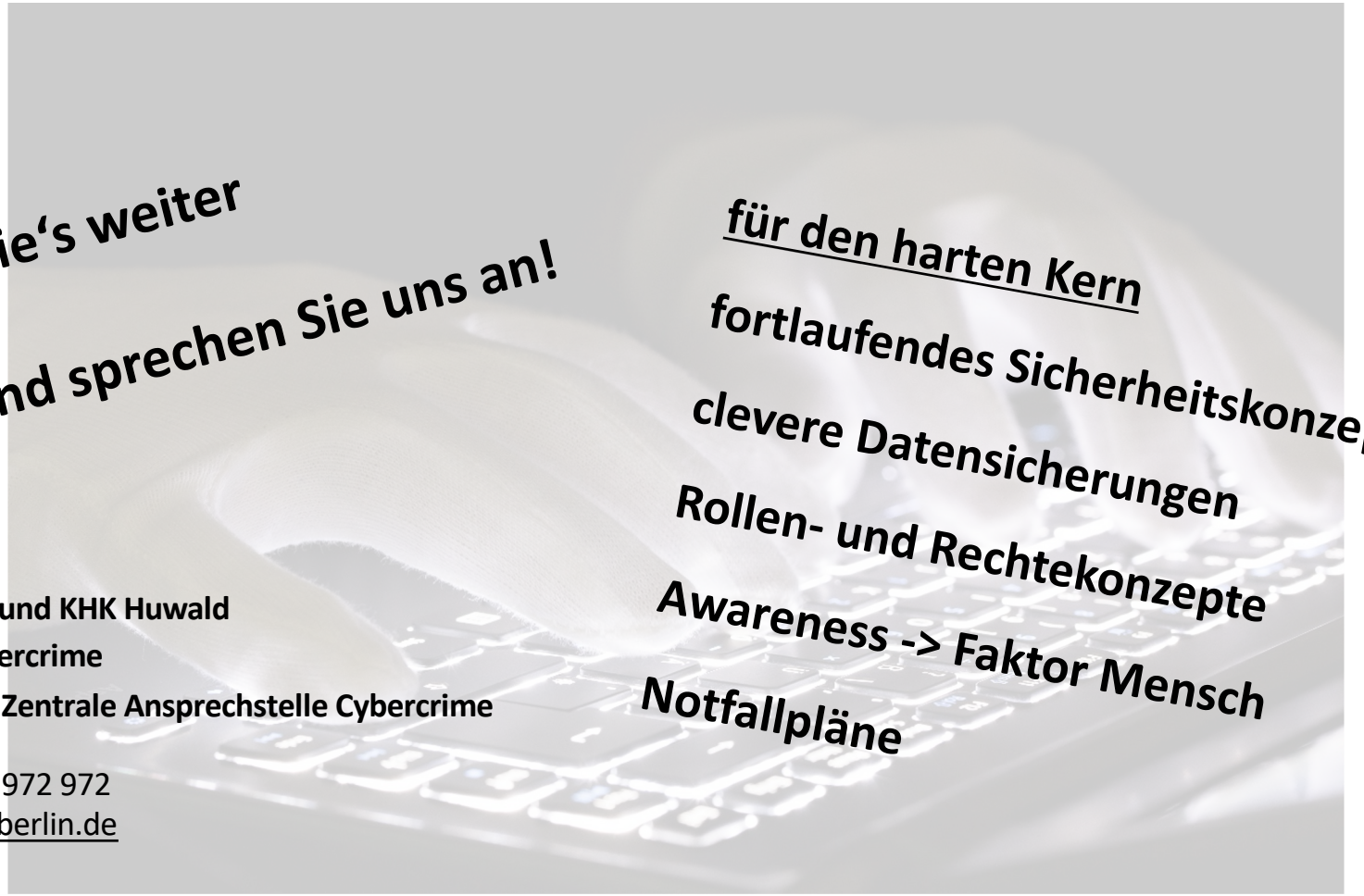
Was hinter den jüngsten Erfolgen der Cybercrime-Jäger steckt

Interview von Thomas Kuhn
09. April 2024

Bild: imago images

Emotet, Hive, Qakbot und nun LockBit – gleich mehrfach konnten Strafverfolger zuletzt große Hackernetzwerke ausschalten. Doch wie nachhaltig sind diese Erfolge?

https://www.wiwo.de/technologie/digitale-welt/hacker-unter-druck-was-hinter-den-juengsten-erfolgen-der-cybercrime-jaeger-steckt/29746126.html



Sagen Sie‘s weiter

… und sprechen Sie uns an!

für den harten Kern

fortlaufendes Sicherheitskonzept

clevere Datensicherungen

Rollen- und Rechtekonzepte

Awareness -> Faktor Mensch

Notfallpläne

KHK Borries und KHK Huwald
LKA 724 Cybercrime
ZAC Berlin – Zentrale Ansprechstelle Cybercrime

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

ZAC - Zentrale Ansprechstelle Cybercrime
für die Wirtschaft im LKA Berlin

Polizei Berlin
ZAC – Zentrale
Ansprechstelle Cybercrime
KHK Borries
KHK Huwald
Friesenstr. 16
10965 Berlin

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

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

Broschüren der ZACs

POLIZEI BERLIN

https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/Wirtschaftsunternehmen/wirtschaftsunternehmen_node.html

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

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=6

Weitere nützliche Informationen zum IT-Grundschutz und zur Sicherheit in Unternehmen erhalten Sie hier

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Deutschland sicher im Netz (DsiN)
- Allianz für Cybersicherheit
- Empfehlungen für Sicherheit im Internet des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) und des Bundeskriminalamtes
- Bundesministerium für Wirtschaft und Energie
- Akademie für Sicherheit und Wirtschaft GmbH
- DsiN-Sicherheitscheck
- NoMoreRansom