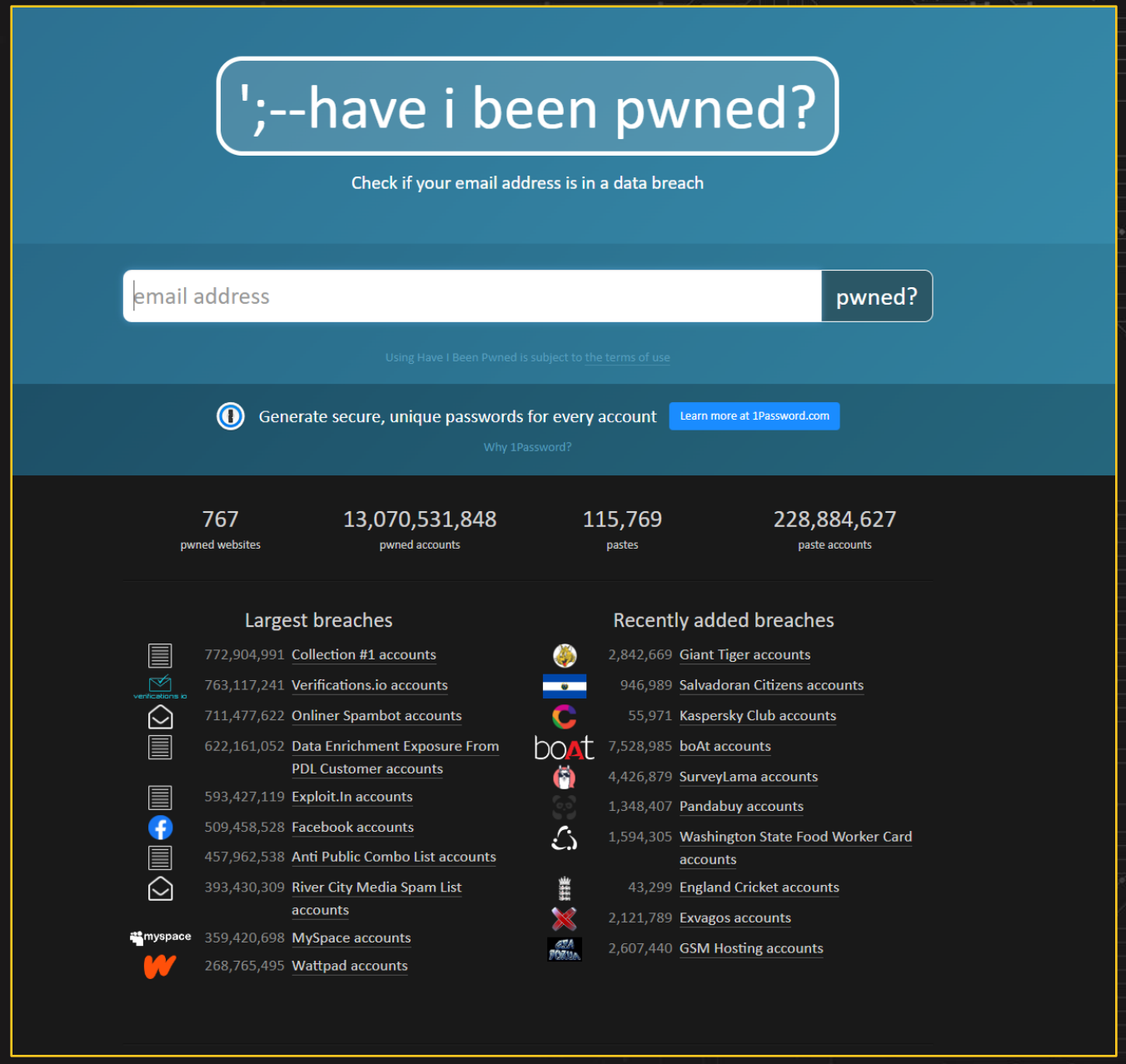
KROLL STRATEGIE

Cyberkriminalität in der Arztpraxis und Gegenmaßnahmen – eine reelle Bedrohung

Tobias Schemenewitz, Cyber Ermittler u. Leiter IT-Forensik
Kroll Strategieberatung GmbH

Ein Einstieg



- https://haveibeenpwned.com/

Tobias Schemenewitz
Cyber Ermittler / Leiter IT-Forensik
Kroll Strategieberatung GmbH

- **Bundeswehr**
  - Spezialkräfte
  - IT-Feldwebel
  - ISB
- **Studium IT-Sicherheit**
- **Kriminalpolizei**
  - IT-Forensik
  - Cyber-Ermittlungen
- **KROLL STRATEGIEBERATUNG**

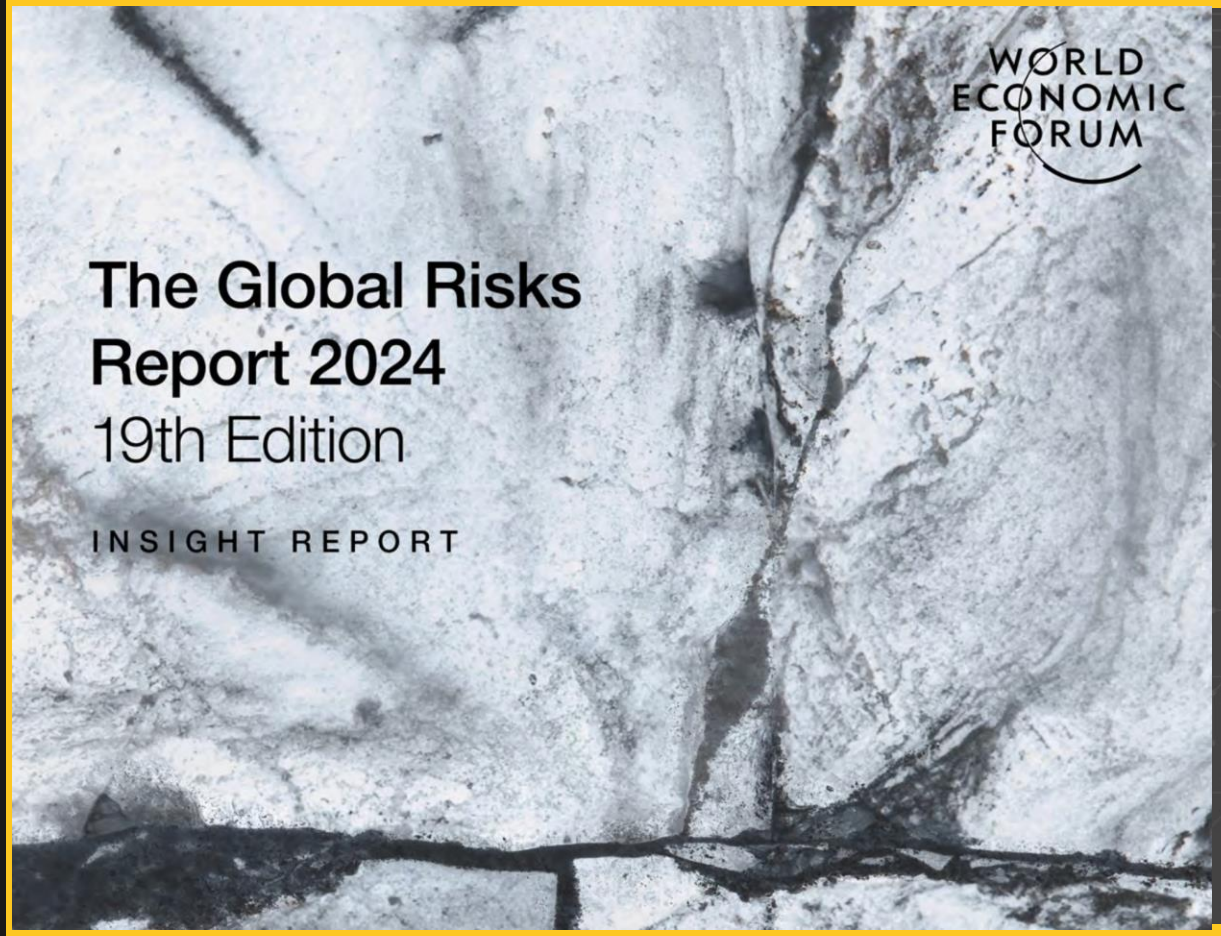
MEINE MISSION:

Durch proaktive Maßnahmen und innovative Strategien die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen schützen.

Agenda

- Einführung in die Cyberkriminalität
- Bundeslagebild CC BKA
- Top 8 Cyber Attacks 2024
- Phänomene / Risiken für Arztpraxen
- Beispiele von Phänomenen
- Ransomware
- Fallbeispiele
- Technische Maßnahmen
- Organisatorische Maßnahmen

Global Risk



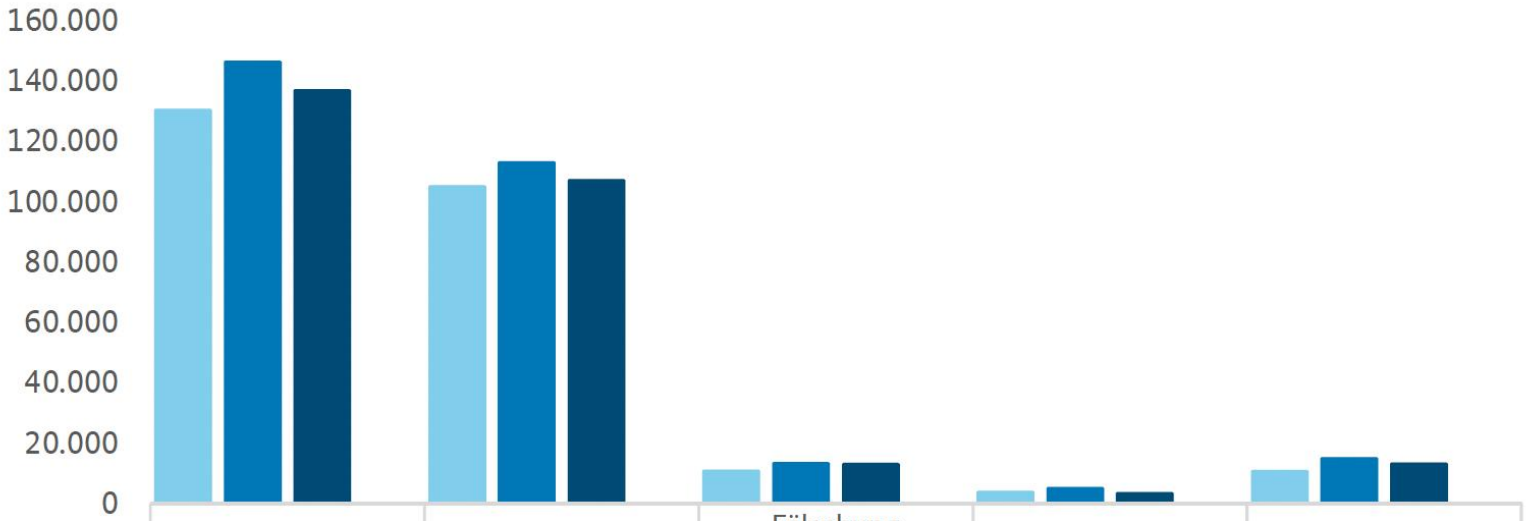
Der jüngst veröffentlichte Global Risks Report 2024 des World Economic Forum positioniert Cyber-Unsicherheit ganz weit vorn auf den 4. Platz

Auf dem ersten Rang steht Desinformation, das durch KI befeuerte zweite Risiko aus der Technologie-Kategorie.

Was ist Cyberkriminalität?

- **Cyberkriminalität** bezieht sich auf kriminelle Aktivitäten, die unter Verwendung von Computern, Netzwerken oder anderen Formen der Informationstechnologie durchgeführt werden
- **Relevanz für die Medizin:** Im Gesundheitswesen umfasst Cyberkriminalität den Diebstahl von Patientendaten, Ransomware-Angriffe auf medizinische Einrichtungen und das Eindringen in Gesundheitsnetzwerke
- **Besondere Verwundbarkeit:** Arztpraxen verarbeiten täglich sensible Patientendaten, was sie zu einem attraktiven Ziel für Cyberkriminelle macht

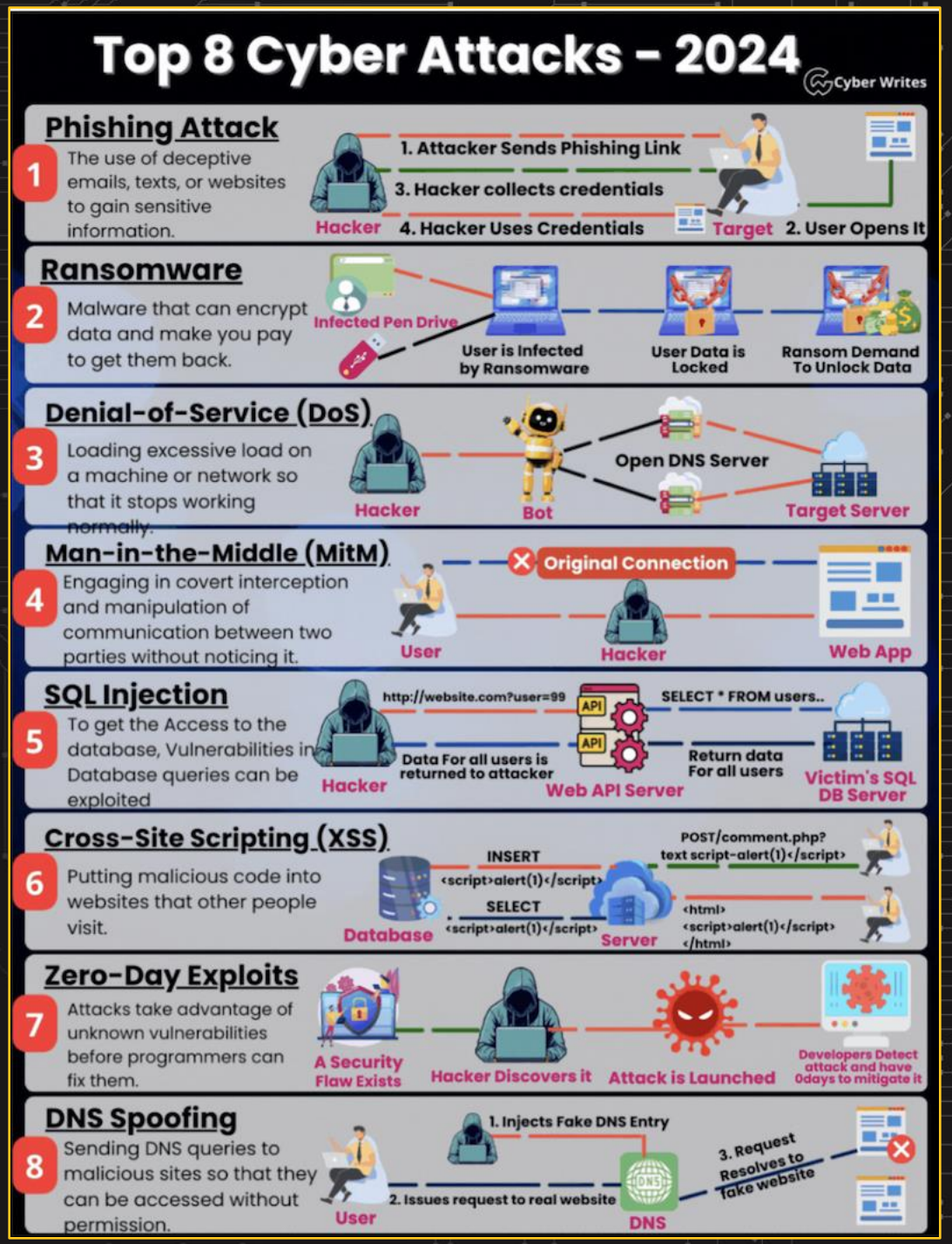
Bundeslagebild Cybercrime 2022



	CC gesamt	Computerbetrug	Fälschung beweiserheblicher Daten, Täuschungen im Rechtsverkehr bei Datenverarbeitung	Datenveränderung, Computersabotage	Ausspähen von Daten einschl. Vorbereitungs-handlungen und Datenhelerei
2020	130.477	105.049	10.895	3.770	10.763
2021	146.363	113.002	13.390	5.053	14.918
2022	136.865	107.165	13.043	3.451	13.206
Diff. zu 2021	-6,5%	-5,2%	-2,6%	-31,7%	-11,5%

Das "**Bundeslagebild Cybercrime**" ist ein Bericht des Bundeskriminalamtes (BKA), der die Entwicklungen und Trends in der Cyberkriminalität in Deutschland zusammenfasst. Es bietet eine Analyse der Bedrohungslage durch Delikte wie Phishing, Malware-Angriffe und Online-Betrug, um präventive Maßnahmen zu unterstützen und politische sowie sicherheitsrelevante Entscheidungen zu informieren.

Top 8 Cyber Attacks 2024



CC Phänomene & Risiken für Arztpraxen

- Phishing
- Ransomware
- Datenlecks und –diebstahl
- Advanced Persistent Threats (APT)
- Malware und Viren
- Man-in-the-Middle
- Denial-of-Service (DoS)

- Verlust von Patientendaten
- Reputationsschäden
- Betriebsunterbrechung
- Finanzielle Verluste
- Rechtliche Konsequenzen
- Verlust der medizinischen Datenintegrität
- Erhöhtes Risiko für Patienten

Beispiele Phishing

Phishing-Sparkasse

Sparkasse

Sehr geehrte/r [redacted]

Ihre persönlichen Daten bedürfen der Aktualisierung. Sie sind verpflichtet, Ihre Daten bei Aufforderung zu aktualisieren. Sollten Sie Ihre Daten nicht innerhalb der nächsten 14 Tage fristgerecht bis zum 01.08.2019 aktualisiert haben, werden wir Sie schriftlich per Einschreiben zur Aktualisierung auffordern. Hierbei kann ein Entgeld von 2,56 Euro enstehen.

Aktuelle Versandadresse:

[redacted]

Zur Aktualisierung

Wichtiger Hinweis:

Sollte Ihre aktuelle Versandadresse abweichen, können Sie zu Ihrer nächstgelegenen Filiale gehen und dort ein Formblatt zusammen mit einem dortigen Mitarbeiter ausfüllen.

Freundlich grüßt

Phishing-Paypal

Hallo [redacted]

Ihre Mithilfe ist erforderlich!

Die neuen Datenschutzgesetze verpflichten uns nun dazu, in regelmäßigen Abständen die Konten unserer Kunden zu überprüfen. Dies dient ausschließlich zu Ihrer eigenen Sicherheit, da in der Vergangerheit immer mehr Vorfälle von Benutzung verschiedener Kundenkonten durch unbefugte Personen entstanden sind.

Um daher wie gewohnt weiterhin Ihr Konto bei uns nutzen zu können, ist Ihre aktive Mitwirkung erforderlich. Dies wird vom Gesetzgeber so verlangt.

Nachdem Sie sich über den Bestätigungsbutton angemeldet haben, werden Ihnen detailiert alle weiteren notwendigen Schritte erklärt.

Bestätigen

Bei Misachtung oder Verweigerung ist ganz klar eine Schließung des Kundenkontos vorgesehen. Der Gesetzgeber fordert in so einem Fall dazu auf.

Vielen Dank im voraus für Ihre Mitwirkung und Ihr Verständnis!

Mit freundlichen Grüßen
Ihr PayPal Kundensupport

Phishing-Volksbank

Volksbanken Raiffeisenbanken

Sehr geehrte Damen und Herren,

leider kam es in letzter Zeit vermehrt zu Problemen mit den hinterlegten Kontaktdaten unserer Kunden, daher bitten wir sie ihre bereits hinterlegten angaben in unserem Kundencenter abzugleichen.

Um einer vorsorglichen Abgleichs Sperrung ihres Kontos unsererseits entgegenzuwirken, empfehlen wir ihnen den Abgleich schnellstmöglich selbst durchzuführen.

Klicken Sie dafür einfach auf »Zum Formular« und folgen anschließend den Anweisungen die ihnen im Kundencenter angezeigt werden.

Mit freundlichen Grüßen,
Ihre **»Volksbanken-Raiffeisenbanken«**

»Zum Abgleich«

Datum: 17.07.2019

amazon

Sehr geehrt [redacted]

wir, das Kundenservice-Team, nehmen Ihre Sicherheit sehr ernst.
Aus diesem Grund ist es vonnöten eine routinemäßige Sicherheitskontrolle durchzuführen.

Der Datenabgleich dient dazu, dass Ihre persönlichen Daten fortdauernd aktuell sind.
So können wir Sie unter anderem vor Missbrauch durch Dritte schützen.

Sollte einer Abweichung der hinterlegten Daten vom System erkannt werden, werden Sie temporär gesperrt und von einem Mitarbeiter schriftlich informiert.

Wir bitten Sie Ihre Daten binnen 48 Stunden vollständig zu verifizieren.

Weiter zur Verifizierung

mit freundlichen Grüßen,
Ihr Amazon-Kundenservice

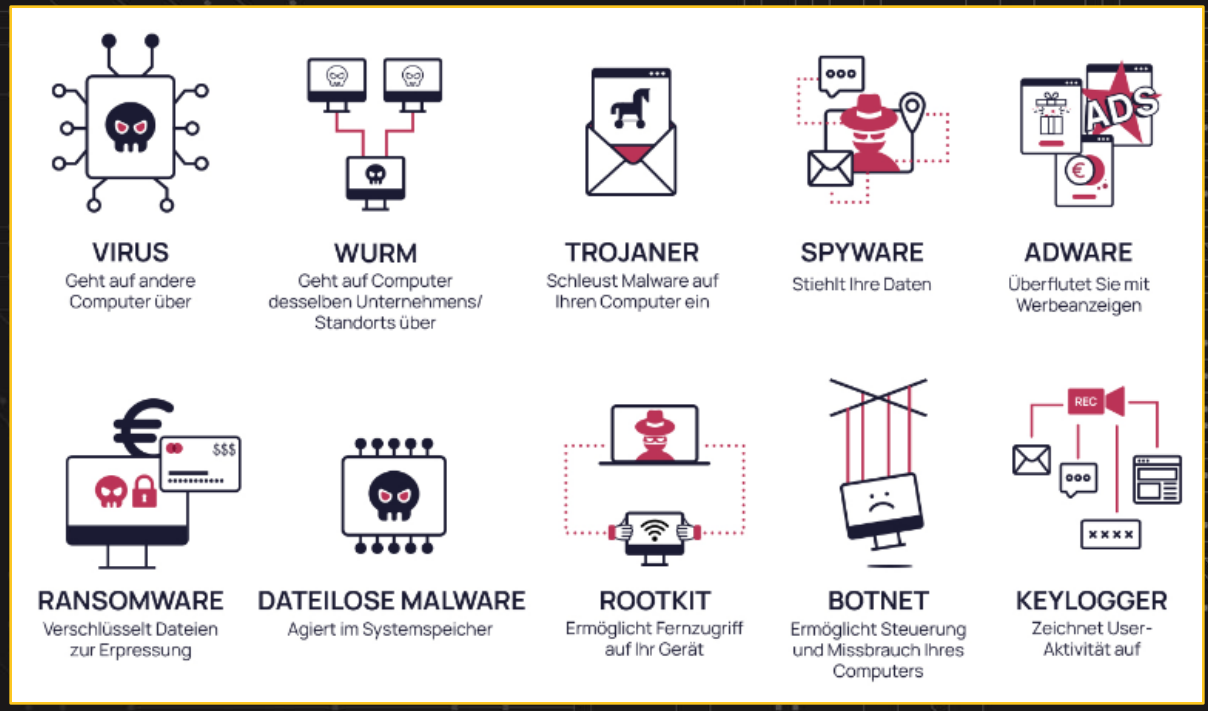
Dies ist eine automatisch versendete Nachricht. Bitte antworten Sie nicht auf dieses Schreiben, da die Adresse nur zur Versendung von E-Mails eingerichtet ist.

Prime Day ist Montag, 15. Juli & Dienstag, 16. Juli
Ein zweitägiges Feuerwerk voller toller Angebote, Entertainment-Events und vieles mehr
Machen Sie sich bereit

prime day

Beispiele Malware

Art	Verhalten	Reales Beispiel
Ransomware	Deaktiviert den Datenzugriff des Opfers, bis Lösegeld gezahlt wird	RYUK
Dateilose Malware	Nimmt Änderungen an Dateien vor, die zum Betriebssystem gehören	Astaroth
Spyware	Erfasst ohne Wissen der Benutzer Daten zu ihren Aktivitäten	DarkHotel
Adware	Präsentiert unerwünschte Werbung	Fireball
Trojaner	Tarnt sich als erwünschter Code	Emotet
Wurm	Breitet sich in einem Netzwerk aus, indem er sich selbst kopiert	Stuxnet
Rootkit	Ermöglicht Hackern die Fernsteuerung des angegriffenen Geräts	Zacinlo
Keylogger	Überwacht die Tastatureingaben von Benutzern	Olympic Vision
Bot	Startet eine Flut von Angriffen	Echobot
Mobilgeräte-Malware	Infiziert mobile Geräte	Triada



Ransomware-Angriffe auf deutsche Krankenhäuser im Überblick

17.09.2020

IT-Ausfall an der Uniklinik Düsseldorf

Update (17. September 2020, 10.00 Uhr): Cyberangriff bestätigt – Sicherheitslücke in verbreiteter Software ermöglichte Zugang – Wiederherstellung geht Schritt für Schritt voran

Seit Donnerstag letzter Woche (10.9.) ist das IT-System des Universitätsklinikums Düsseldorf (UKD) weitreichend gestört. Daher ist das UKD weiterhin von der Notfallversorgung abgemeldet und Patienten mit Terminen sollten zur Abstimmung Kontakt mit der behandelnden Abteilung aufnehmen.

POL-SO: Cyberangriff auf die IT-Infrastruktur des Dreifaltigkeits-Hospitals in Lippstadt

Lippstadt/Erwitte/Geseke (ots)

Information über den Cyberangriff bei der Klinikum Lippe GmbH

Nachdem die erforderlichen Untersuchungen abgeschlossen sind, möchten wir Sie darüber informieren, dass wir im vergangenen Jahr leider Ziel eines Cyberangriffs geworden sind. In der Folge können wir zum derzeitigen Stand nicht ausschließen, dass sich Dritte unberechtigten Zugang zu personenbezogenen Daten verschafft haben.

PRESSEMITTEILUNG

Caritas-Klinik Dominikus von Cyberangriff betroffen

Berlin, 31. Januar 2024 | Die Caritas-Klinik Dominikus wurde Opfer eines Hacker-Angriffs auf die IT-Infrastruktur.

5 Schritte eines Ransomware-Angriffs auf ein mittelständisches Unternehmen

AUFKLÄRUNG

Ihre Infrastruktur wird kompromittiert, erforscht und der Zugang verkauft

DATENRAUB

Ihre sensiblen Daten werden gestohlen

SABOTAGE

Verschlüsselung Ihrer Systeme, Produktionsausfall

ERPRESSUNG

Druckmittel werden gegen Sie eingesetzt

FINALE

Drohungen werden wahrgemacht

Server per RDP von außen erreichbar → Admin-Zugang per Phishing gestohlen → Übernahme der IT-Umgebung um 3:00h nachts → Diebstahl von Kundendaten (100GB) → Verschlüsselung der Server → Erpressung

IT-Totalschaden, Arbeit aller Angestellten von 4 Wochen vernichtet

Schaden:

150.000 €

Ein Klassischer Ransomware-Angriff

CYBER KILL CHAIN

Erkundung der Infrastruktur | **Auswahl der Werkzeuge** | **Transport der Werkzeuge** | **Ausnutzung von Schwachstellen** | **Brückenkopf schaffen** | **Ferngesteuerte Aktivitäten** | **Datendiebstahl und Sabotage**

1

- Bereitstellung des verseuchten Softwarepaketes
- Mitarbeiter lädt verseuchte Datei auf seinen PC
- Mitarbeiter führt die Datei auf einem PC aus
- Schadcode stiehlt Zugangsdaten + Verkauf im Darknet

2

- 2. Angreifer kauft Zugangsdaten im Darknet
- Zugriff auf das Unternehmen (Fernzugang)
- Einrichtung einer Persistenz
- Angreifer ergaunert sich weitreichende Rechte in der Infrastruktur
- Sabotage durch Verschlüsselung + Erpressung
- Datendiebstahl

Folgen für das Opfer (reales Beispiel)

Beschäftigte
können nicht arbeiten,
sind verunsichert

Cyber-Versicherung
prüft, ob der Sachverhalt
abgedeckt ist

IT-Dienstleister
Wiederherstellung der
Datensicherung

Bank
Gespräche wegen möglicher
Lösegeldzahlung

Mandanten
können uns nicht erreichen, Termine und
Fristen können nicht eingehalten werden

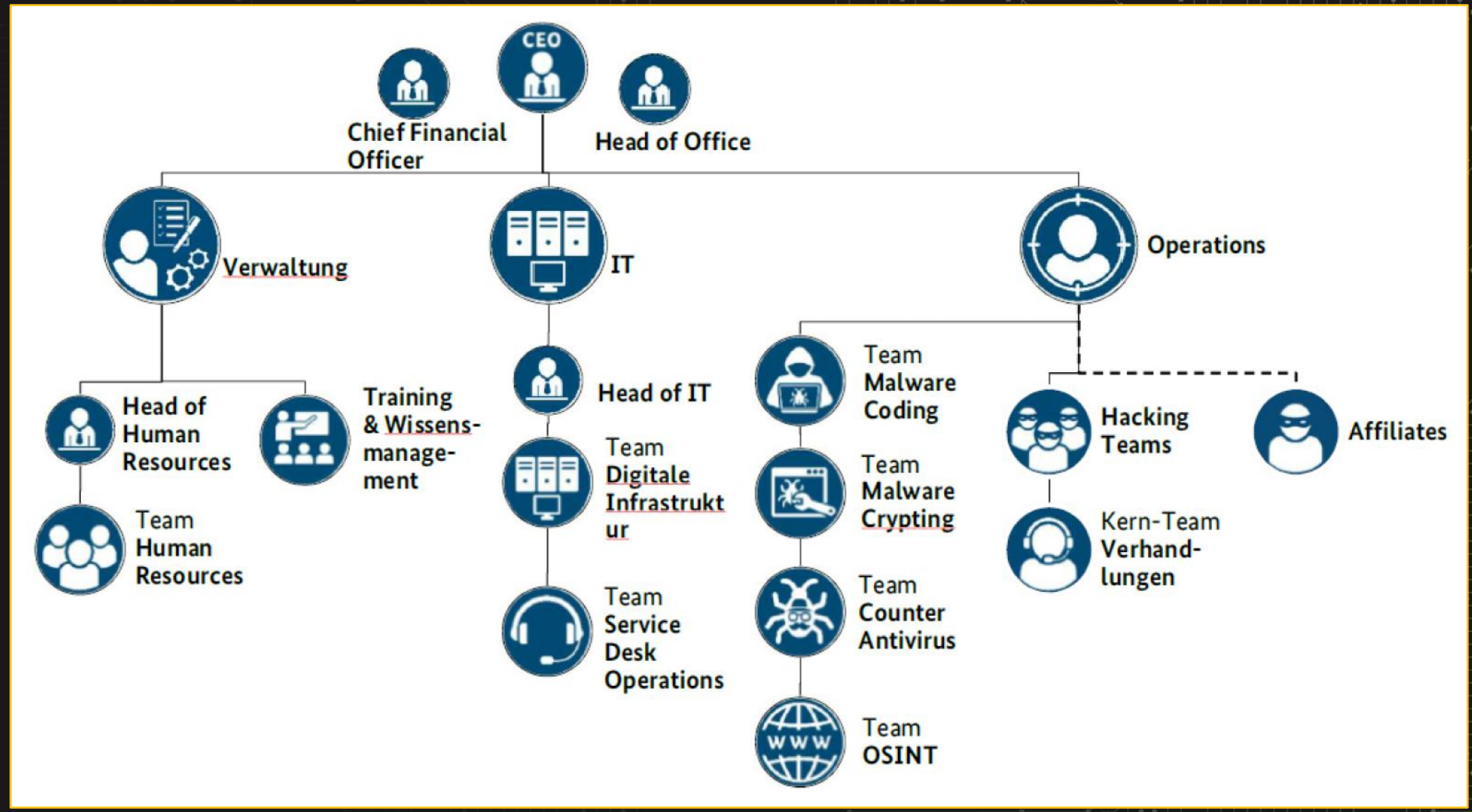
Forensiker
Ermittlung des Tathergangs und
welche Daten betroffen sind

Datenschutz-Aufsichtsbehörde
Meldung einer Datenpanne

LKA
Anzeige erstattet und
Ermittlungen eingeleitet

ANGST
KONTROLLVERLUST
EXISTENZSORGEN
HILFLOSIGKEIT
SCHAM
WUT
VERZWEIFLUNG
SCHULDGEFÜHLE

Arbeitsteilung | Organisation einer RaaS-Gruppierung



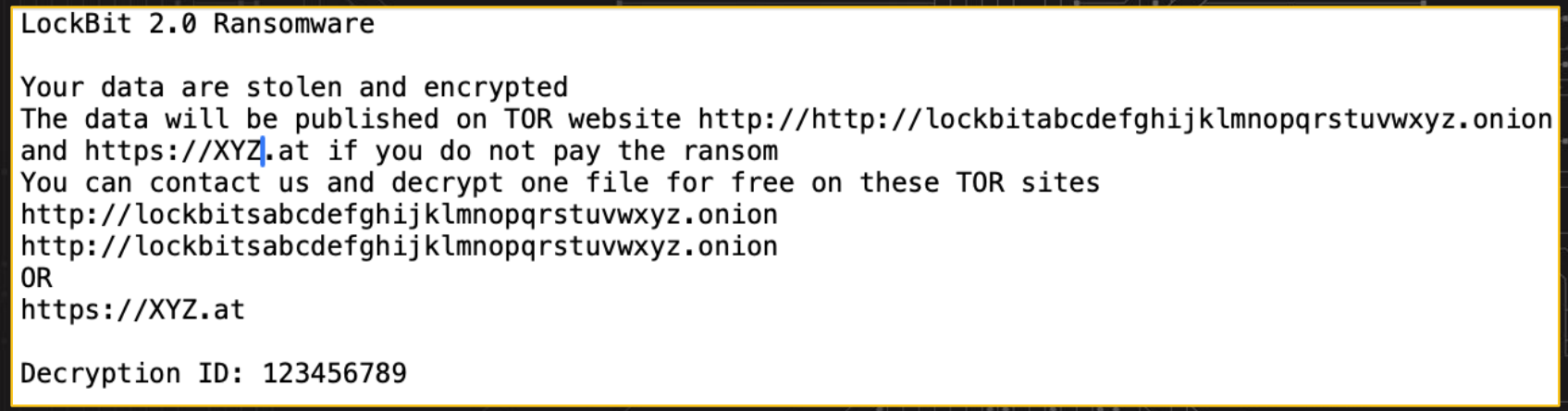
Fallbeispiele

- Praxis
- Ransomware (Verschlüsselung)
- Kein Zugriff auf Terminkalender, Patienten- und Verwaltungsdaten
- 836.258 Dateien verschlüsselt
- 369 GB
- Keine Firewall
- Keine Auslagerung von Backups
- Veraltete Virensignaturen

```
>> What has occurred?

   We have securely encrypted and taken possession of all your files.
   Your files are inaccessible without availing our decryption service.

>> How can you reach us?

   To initiate the decryption process, please exclusively send messages to the email addresses provided below.
   We do not take responsibility for communication through other email addresses.
   Write your personal ID in the subject of the email.


   Personal ID: 123456789
   Primary Email: XXXX
   Secondary Email: XXXX

>> What assurances do you have?

   To demonstrate the decryption procedure, we will open a small, inconsequential file less than 1MB in size (e.g., an image, text, PDF, etc.).
   This will allow you to witness the decryption process. Please refrain from sending important or backup files.

>> Cautions!

   1- Decryption can only be accomplished through us, so any attempts to decrypt through other means or individuals will prove futile.
   2- Please avoid manipulating the file formats with unnecessary methods, as this can corrupt the file structure, and such an error is irreversible.
   3- We have retained all your data, and it has been encrypted solely on your computer.
   4- A secure backup copy of all your data is stored in our company's cloud space. Failure to make payment may result in data exposure on the dark web.
   5- We have no interest in keeping your files, and upon payment, you will receive all of them.
```

Fallbeispiele

- Fa. XY Produktherstellung
- Ransomware (Verschlüsselung)
- Kein Zugriff auf Datenserver, E-Mail und Verwaltungsdaten
- mehr als 1.000.000 Dateien verschlüsselt
- mehrere TB
- Unzureichend geschützte Firewall
- Keine Überprüfung auf Backupkompromittierung
- Keine Endpoint-Security



Weitere

```
---------- [ Welcome to buhtiRansom ] ------------>

What happend?
-------------------------------------------------
Your files are encrypted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your files.
Follow our instructions below and you will recover all your data.

What guarantees?
-------------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data.

How to get access?
-------------------------------------------------
Using a browser:
1) Open website: https://abcdefgh.com/pay/efgh
2) Enter valid email to receive download link after payment.
3) Pay amount to Bitcoin address.
4) Receive email link to the download page.
5) Decrypt instruction included.

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. It WILL NOT be able to RESTORE.
!!! DANGER !!!
```

```
**************************************************************************************************************************

                                                HELLO Dear Customer !

If you reading this message, it means your network was PENETRATED and all your files has been ENCRYPTED

                                                ------------------------------------------------
                                                |                                              |
                                                | by   R A G N A R   L O C K E R !             |
                                                |                                              |
                                                ------------------------------------------------

**************************************************************************************************************************
                        [ YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL ]
                                (contact information you will find at the bottom of this notes)

                                                **** WARNING ****
DO NOT Hire any THIRD-PARTY NEGOTIATORS (RECOVERY Groups/FBI/Police and etc), otherwise we will close chat immediately and Publish all your
Data.
DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
                                or public Decryption software, it also may DAMAGE files.
                                ur system, it can DAMAGE files.
```

READ__ME_TO_RECOVER_YOUR_DATA.README

Documents | Aggregations | Schema | Explain Plan | Indexes | Validation

Filter | Type a query: { field: 'value' }

ADD DATA | EXPORT COLLECTION

```
_id: ObjectId('650a95dcf55f5adb9d48afd1')
content: "All your data is backed up. You must pay 0.0125 BTC to 14B8iRn9k76fTmg…"
```

All your data is ba
data will be public
us: rambler+1avsa

Gegenmaßnahmen | aktuelle Technologien und Methoden in der IT-Sicherheit

Endpoint Detection and Response (EDR)

Security Information and Event Management (SIEM)

Extended Detection and Response (XDR)

MFA

Threat Intelligence

Next-Generation Firewalls (NGFW)

Managed Detection and Response (MDR)

Machine Learning und Künstliche Intelligenz (KI) in der Sicherheit

Backups

Der STAND DER TECHNIK (kritisch betrachtet)

ANTIVIRUS

Online-
BACKUP

IDS/IPS

Intrusion Detection/Prevention System
einer gewöhnlichen KMU-Firewall

2FA

Zwei-Faktor-Authentifizierung

Der STAND DER TECHNIK (kritisch betrachtet)

MEDR
Mobile Endpoint Detection & Response

NDR
Network Detection & Response

THREATHUNTING
Anlasslose Suche nach Angreifern (Jagd)

Offline BACKUP
Mindesten eine aktuelle Sicherungskopie ohne Verbindung zur IT-Infrastruktur

Fortlaufendes PENTESTING
Regelmäßige Angriffe auf die eigenen Systeme, um Sicherheit zu prüfen

MFA
Mehrfach-Authentifizierung bei Anmeldungen aus der Ferne & Cloud

Organisatorische Sicherheit

- **Kompetente Menschen mit Unterstützung der Geschäftführung:** IT-Sicherheitsbeauftragter, CISO
- **Richtlinien und Verfahren**: Implementierung von Sicherheitsrichtlinien, und - Leitlinie
- **Schulung und Bewusstsein**: Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter für Sicherheitsrisiken und -praktiken.
- **Zugriffskontrolle**: Festlegung von Berechtigungen und Verantwortlichkeiten für den Zugriff auf Daten und Systeme.
- **Notfallpläne**: Erstellung von Plänen für Notfälle, wie z.B. Datenverluste oder Sicherheitsverletzungen.
- **Compliance und Audits**: Überwachung der Einhaltung von gesetzlichen und branchenspezifischen Standards, Durchführung von internen und externen Audits.
- **Risikomanagement**: Bewertung und Management von Sicherheitsrisiken, einschließlich der Durchführung von Risikoanalysen und -bewertungen.

Question & Answer

KROLL STRATEGIE

„Technik allein löst kein einziges Sicherheitsproblem. Menschen lösen Probleme.”

schemenewitz@kroll-strategie.de

0231 / 226 19765

Kroll Strategieberatung GmbH

Freie-Vogel-Straße 369 / 44269 Dortmund