Hacking & Pentests iZm DORA & CRA

ADV-Rechtstag| 7.11.2024

RA MMag. Norbert Amlacher

Partner bei andréewitch & partner rechtsanwälte GmbH (Wien)

Übersicht

1. Was sind diese Abkürzungen auf der Titelfolie?
2. Was hat das Ganze mit Hacking & Pentests zu tun?
3. Und wie schaut das in der Praxis aus, Avi Kravitz?

Wie stellt sich die _KI_ das eigentlich vor?

Digital Operational Resilience Act

Cyber Resilience Act

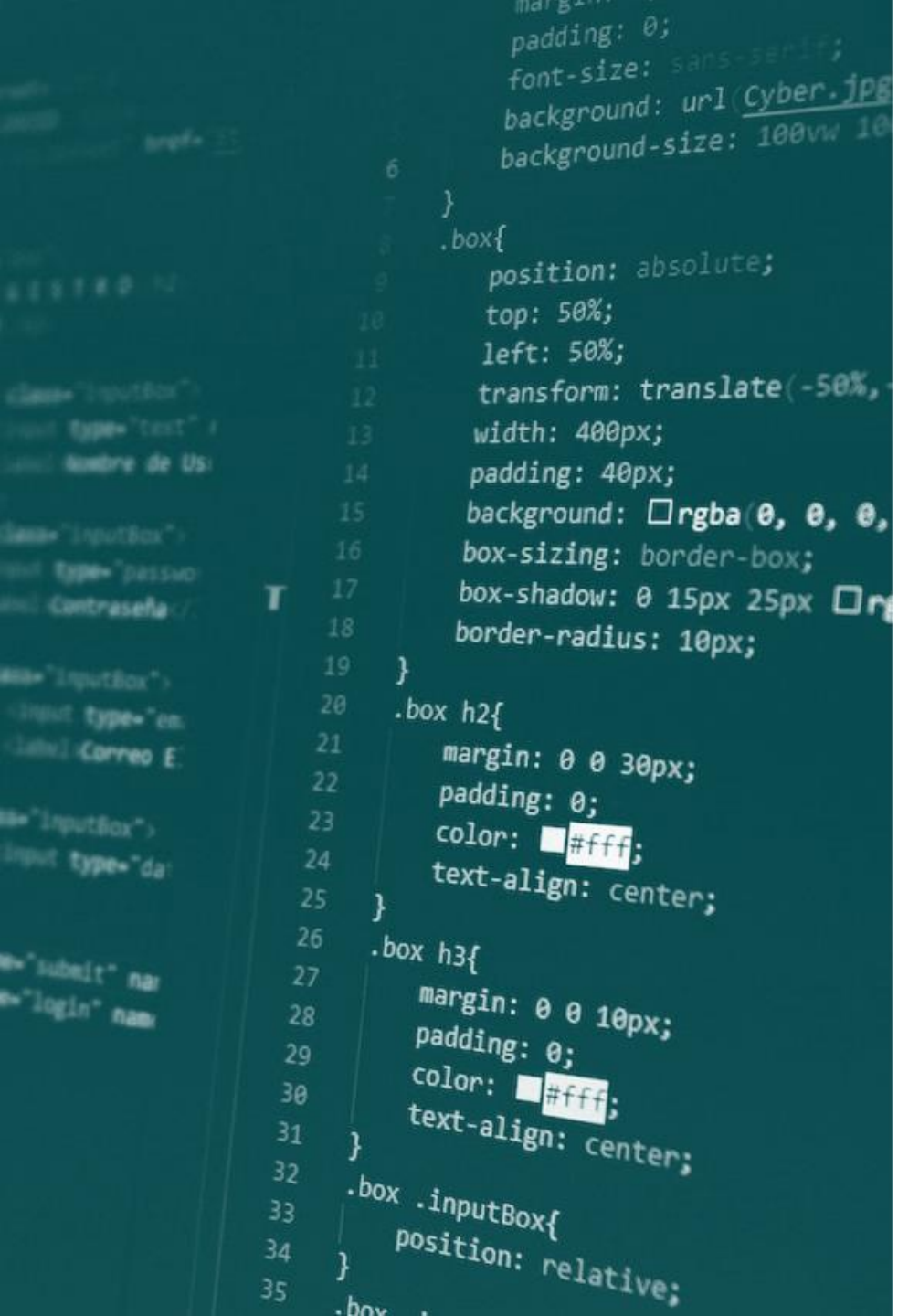

stablediffusionweb.com

1. Was sind diese Abkürzungen? (DORA)

- **VO (EU) 2022/2554** vom 14.12.2022 – digitale Resilienz im Finanzsektor
- gilt ab **17.1.2025** unmittelbar
- **Finanzunternehmen** = grds. Kreditinstitute & Versicherungsunternehmen
- **IKT-Drittdienstleister** mittelbar & tlw. unmittelbar erfasst
- Nationale Umsetzung im **DORA-Vollzugsgesetz** (BGBl. I Nr. 112/2024)
- **Schwerpunkte**:
  i. IKT-Risikomanagement (Governance-/Kontrollrahmen, Leitungsorgan)
  ii. Behandlung, Klassifizierung & Berichterstattung IKT-bezogener Vorfälle
  iii. Testen der digitalen operationalen Resilienz
  iv. Management des IKT-Drittparteienrisikos (Verträge, Informationsregister)
  v. Überwachungsrahmen für kritische IKT-Drittdienstleister
  vi. Zahlreiche delegierte Rechtsakte (technische Durchführungs- und Regulierungsstandards)
- **Strafen** bis zu **1% des jährlichen Nettoumsatzes** / EUR 500.000

1. Was sind diese Abkürzungen? (CRA)

- **Verordnung, gilt voraussichtlich ab 2027 (final schon beschlossen)**
- **Produkte, mit digitalen Elementen + Datenverbindung**
- **Hardware** (z.B. Handy, Router, Drohne), **Software** (embedded & stand alone)
- Verbindliche **Cybersicherheitsanforderungen**, betroffen v.a. Hersteller
- **Schwerpunkte**:
  i. Security by Design / keine Schwachstellen
  ii. Sicherheitsaktualisierungen & laufendes Schwachstellenmanagement
  iii. Datenminimierung
  iv. Informations-, Dokumentations- und Meldepflichten (24 Stunden)
  v. CE-Kennzeichen (eigene oder externe Prüfung) + harmonisierte Normen
- **Strafen** bis zu **2,5% des weltweiten Jahresumsatzes**



2. Was hat das mit Hacking & Pentests zu tun?

- **CRA:** Annex I: „*apply **effective and regular tests** and reviews of the security*“
- **DORA:** viel umfassendere/spezifischere Regeln, u.a.:

i. **Digitale operationale Resilienz** ist zu testen (Art 24)

ii. **Testprogramm** hat Bewertungen, Tests, Methoden, Verfahren & Tools zu umfassen, die in Art 25 & 26 DORA genannt sind

iii. Tests sind grds. von **unabhängigen (internen oder externen) Parteien** durchzuführen

iv. **Umfang in Art 25 DORA**: „*Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests*“

v. **Erweiterte Tests nur von ausgewählten Finanzunternehmen (Art 26 DORA)**: **Bedrohungsorientierte Penetrationstests (threat-led penetration testing)** mindestens alle 3 Jahre, ggf. öfter/seltener, am Live-Produktionssystem >> Zusammenfassung der Ergebnisse an Behörde + Pläne mit Abhilfemaßnahmen & Unterlagen zum TLPT; Behörden bescheinigen Tests

vi. **Technische Regulierungsstandards** auf Basis von **TIBER-EU-Rahmen** (= „Threat Intelligence-Based Ethical Red Teaming“), in Österreich TIBER-AT

3. Und wie schaut das in der Praxis aus, Avi Kravitz?

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Anmerkungen?

RA MMag. Norbert Amlacher

andréewitch & partner rechtsanwälte GmbH
Stallburggasse 4, 1010 Wien
www.andlaw.at
Telefon: +43 (1) 533 31 58
E-Mail: office@andlaw.at

a.team rocks
CONSULTING & MANAGED DEFENSE

Fortgeschrittene Penetration Tests / Red Teamings

AVI KRAVITZ

07.11.2024

Who am I?

Avi Kravitz | avi@a-team.rocks

Founder @ A-Team Rocks Consulting
Co-Founder @ Active Cyber Defense Center / ACDC
Co-Founder @ Founders of Europe

Advisory Board @ T3K Forensics
Advisory Board @ HTL-Spengergasse
Advisory Board & Partner @ Blue-Shield Security

Senior Security Consultant & Trainer

IT-Security seit 1999 (Offensive Security)

Spezialisierung seit 2011 auf Wirtschafts- und Industriespionage

Von 100 Unternehmen – wie viele kannst du hacken?

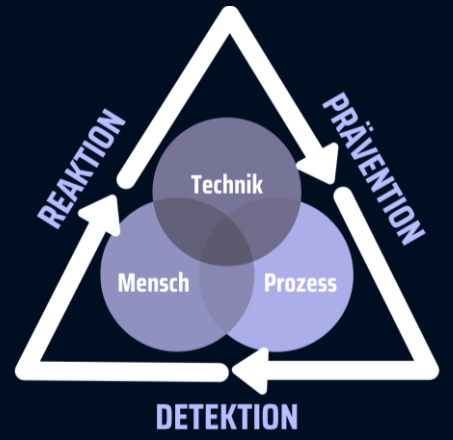
Mythen rund um Cyber-Security

- „Ich habe doch eine Firewall und ein Antivirenprogramm!“
- > 50% der erfolgreichen Angriffe verwenden neuartige Lücken

- „Wer will schon was von mir/uns?“
- > 90% aller Cyberangriffe sind opportunistisch

Mythen rund um Cyber-Security

- „Unsere IT kümmert sich darum.“
- Cyber-Security funktioniert nur ganzheitlich



- „Wir haben eh eine Cyber-Versicherung abgeschlossen“
- Reputation, Betriebsunterbrechung, Sorgfaltspflicht, vertragliche Ausschlussgründe, Strafen,…

Größten (sichtbaren) Bedrohungen 2024

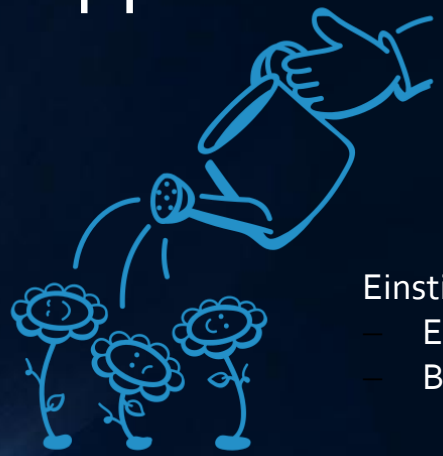
1. Identitätsdiebstahl
2. Erpressung (1.1 Mrd. USD in 2023)
3. Angriffe über die Lieferkette (seit 2021: +650%)

Cyber-Angriffe – die Akteure

opportunistisch VS zielgerichtet

Cyber-Angriffe – die Akteure

opportunistisch VS zielgerichtet



Einstieg meist:

- E-Mail (z.B. Phishing, Attachments,…)
- Browser (z.B. Malvertising)

Die (häufigsten) Eintrittsvektoren:

- E-Mail / Phishing (+76% zu 2021)
- Nicht aktuell gehaltene & exponierte Systeme/Software
- Unzureichend gesicherte Fernzugänge
- **Most Trending**: Angriffe über die Lieferketten
- **Hottest newcomer**: Malvertising


Wir haben initialen Zugang, was nun?

Initial Access Broker

- „Makler für den Erstzugang“

Quelle: Blueliv

Circassian March 24, 2023 01:32 PM

Hi,

RDP USA access
Revenue: $64.3M Zoominfo
Industry: Construction Zoominfo
139 employees. Zoominfo
rights: domain admins
Type access: RDP

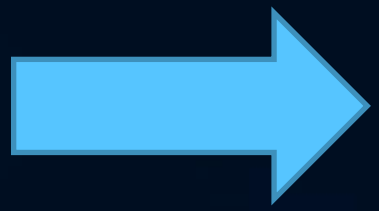
5 Hyper V| AV:Windows Defender | 130 computer Active Directory | 487 User Active Directory

Price : 3000 Usd

I agree to the guarantor.

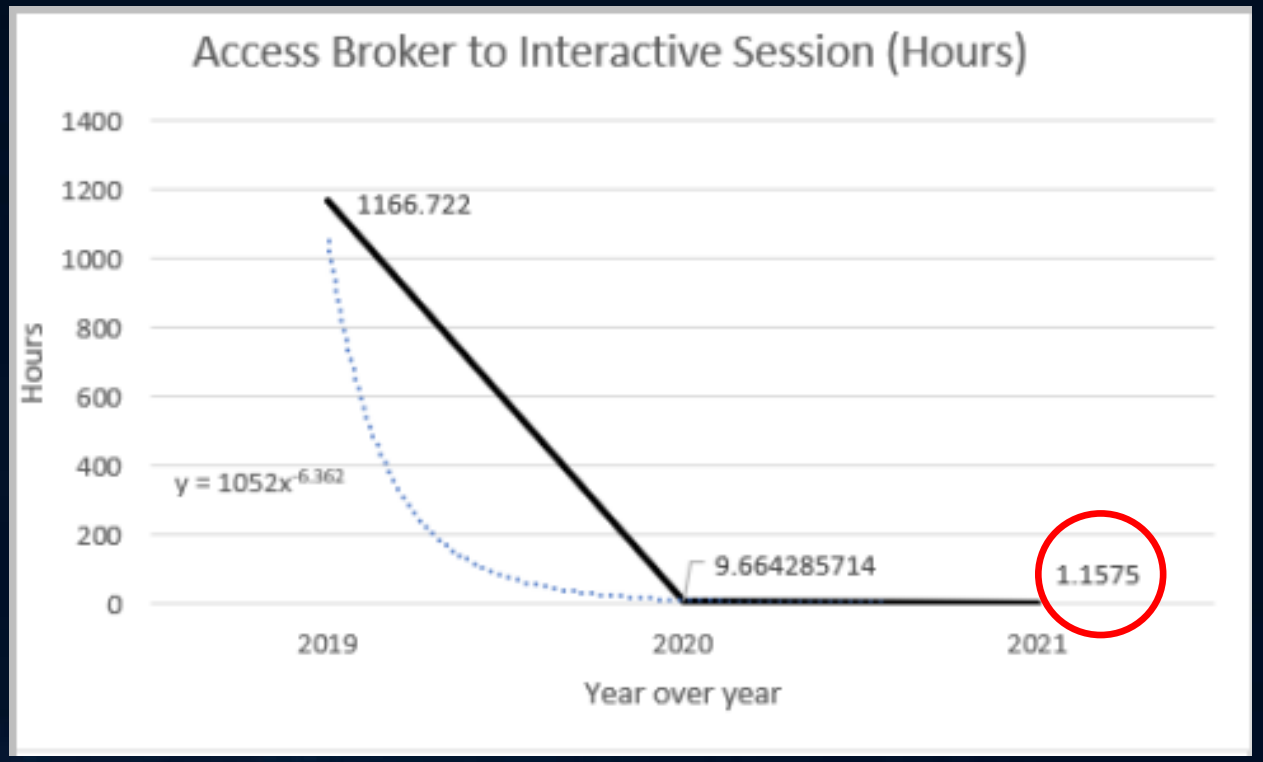
Cyber-Angriffe – die Akteure

opportunistisch wird zielgerichtet



Initiale Infektion – Patient 0

- Dauer bis zum ersten „bösen" Login:

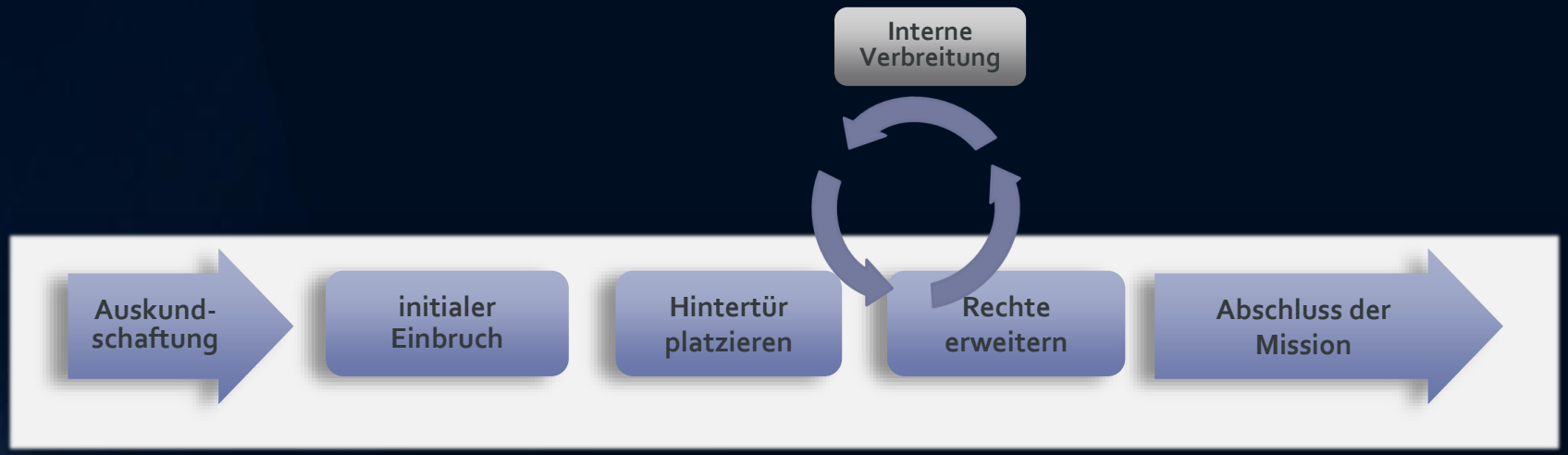


Quelle: IBM X-Force

Penetration Test VS Red Teaming

- Penetration Testing: Einzelne Schwachstellen finden, meist spezifisch (Black-, White-, Gray-Box)
- Red Teaming: Simulation umfassender, realistischer Angriffsszenarien, um die gesamte Verteidigung und Reaktionsfähigkeit zu testen
  - Threat Intelligence-based Red Teaming (z.B. TIBER)
  - Objective based Red-Teaming
  - Assumed Breach Testing

Die Anatomie eines fortgeschrittenen Angriffes



Quelle: Lockheed Martin & Mandiant

Was haben wir daraus gelernt?

- Ziel Prävention => draußen halten und/oder Zeit gewinnen
- Es gibt kein Schlangenöl um „sicher“ zu sein

“There are only two types of companies: Those that have been hacked and those that will be hacked.”

– Robert S. Mueller, III, former Director of the FBI

Was haben wir daraus gelernt?

- Ziel Prävention => draußen halten und/oder Zeit gewinnen
- Es gibt kein Schlangenöl um „sicher“ zu sein
- Hausaufgaben erledigen!

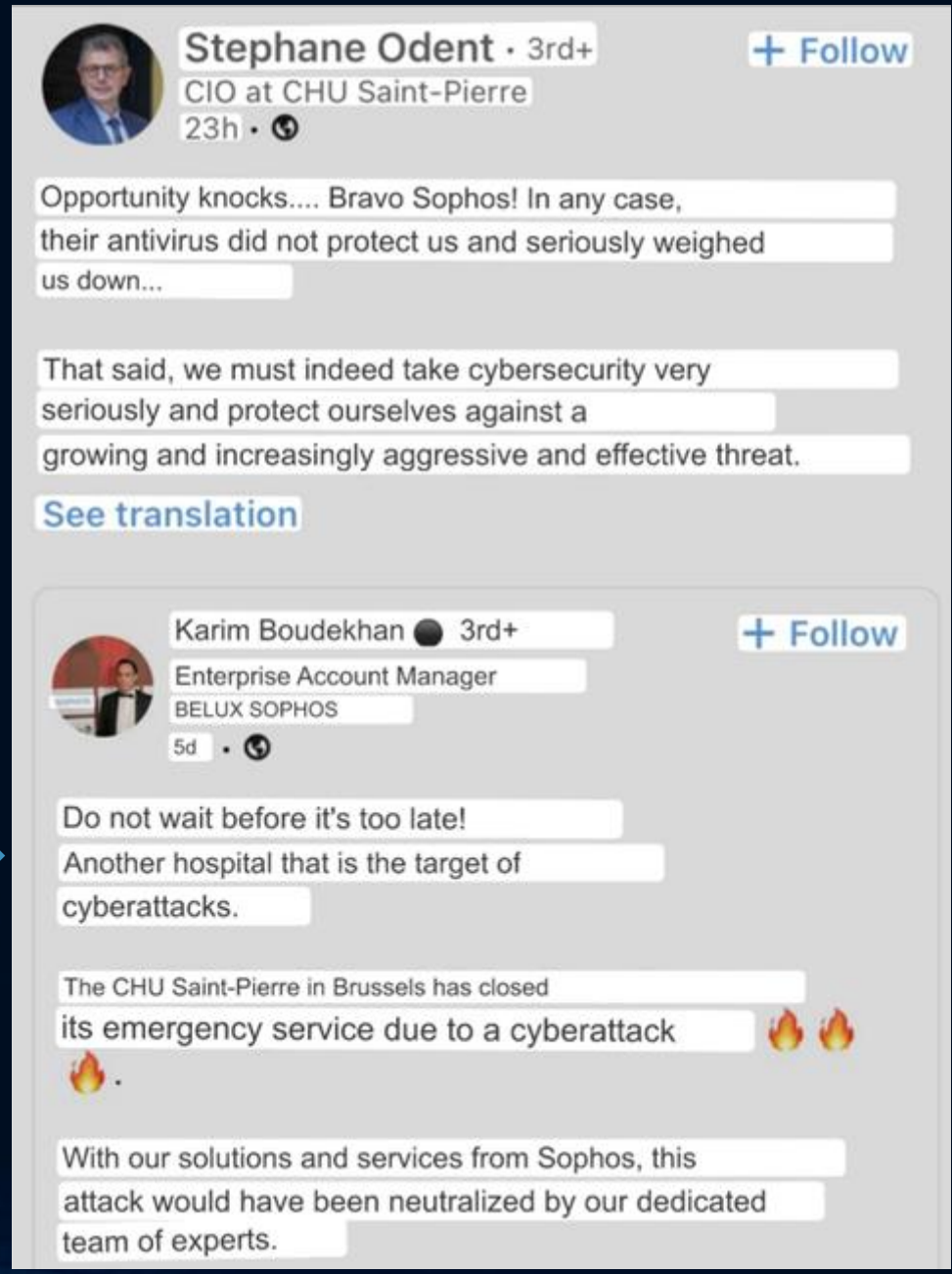
“There are only two types of companies: Those that have been hacked and those that will be hacked.”

– Robert S. Mueller, III, former Director of the FBI

Details zum Sicherheitsvorfall

Ausfall | Einbruch

Betr. (Organisation)	CHU Saint-Pierre
Datum (Veröffent.)	13.03.2023
Land	Belgien
Vorfall	Am 11. März 2023 kam es zu einem Cyberangriff auf das Saint-Pierre Universitätskrankenhaus in Brüssel. Der Angriff wurde entdeckt, nachdem IT-Experten eine Verlangsamung interner Server feststellten. Aufgrund der Attacke wurden interne Server und die Notaufnahme für mehrere Stunden heruntergefahren und eintreffende Patienten wurden an andere Krankenhäuser umgeleitet.
Quellen	11.03.2023: Brussels Times 12.03.2023: noticemerica 12.03.2023: BRF



Wohin geht die Reise?

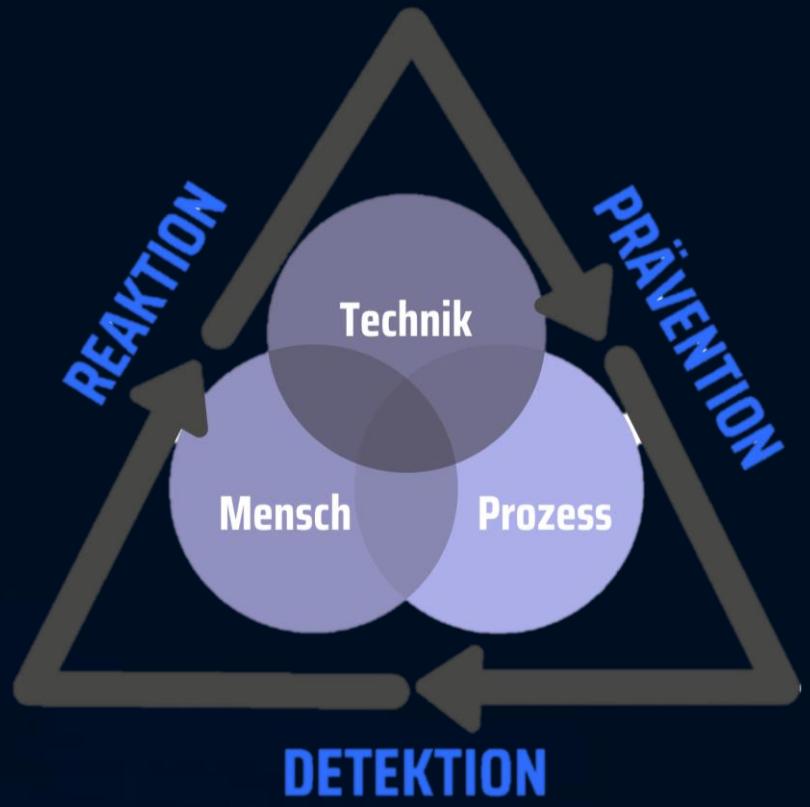
- Cyber-Crime gekommen um zu bleiben!
- Angriffe werden immer schneller
- …und dank KI auch immer besser

- Messlatte für Cyber-Versicherungen steigt

*"Cybersecurity Ventures also reports that cybercrime represents the **greatest transfer of economic wealth in history**. 15% growth every year." (Intrusion, 2021)*

State-of-the-Art Cyber-Security 2024ff

- Cyber-Security ist ein Prozess & kein Projekt
- Multi Vendor Strategie
- Monitoring & schnelle Reaktion ist und wird kriegsentscheidend
- Jede Security-Lösung braucht aktives Monitoring (Threat Hunting)



Jedes Unternehmen ist einzigartig!

Von 100 Unternehmen – wie viele kannst du hacken?

And I told them "Once you pass the compliance you will be secure"

Cybersecurity controls

Ineffective Vs Missing

Vielen Dank!

a-team rocks
CONSULTING & MANAGED DEFENSE

avi@a-team.rocks