

**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](mailto: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?



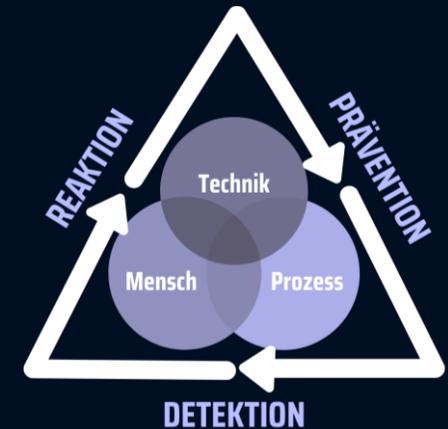
# Mythen rund um Cyber-Security

- „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“

Selling Network Full Access (Domain Admin)

3lv4n · Jul 15, 2020

Watch

Jul 15, 2020

  
**3lv4n**  
CyberPunk Hacker  
Premium

Joined: Jul 15, 2020  
Messages: 31  
Reaction score: 12  
Deposit: 0 B

**Electric Power Company - Amman - Employees:8.150 Revenue: \$719 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 3200\$**

**Hospitals - Saudi Arabia - Employees: 7.400 Revenue: \$1 Billion (Domain Admin+NTDS+Full internall netwrok info) Price: 3500\$**

**Insurance - Thailand - Employees: 520 Revenue: \$131 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 1000\$**

**insurance - Saudi Arabic - Full Network Access(Domain Admin+NTDS+ Full internall netwrok info) Price: 3000\$**

**Government - Kuwait - Full Network Access(Domain Admin+NTDS+Full internall netwrok info) Price: 3000\$**

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



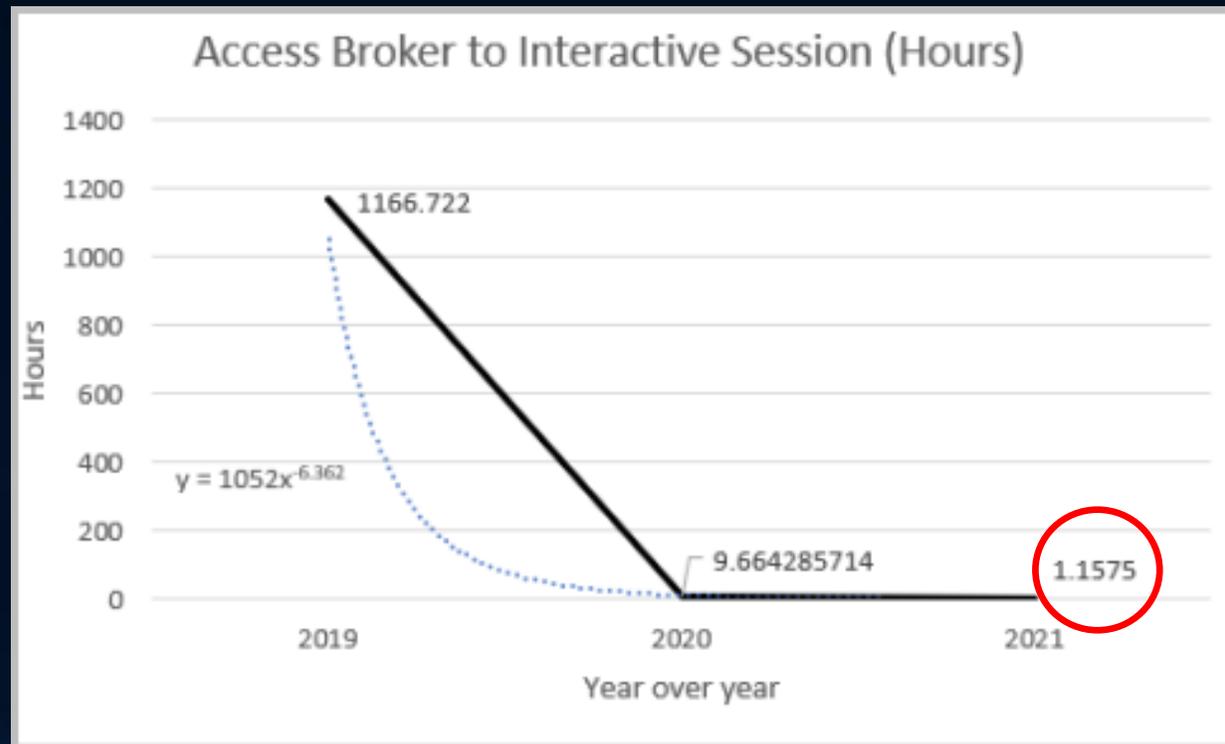
zielgerichtet





# Initiale Infektion – Patient 0

- Dauer bis zum ersten „bösen“ Login:



Quelle: IBM X-Force

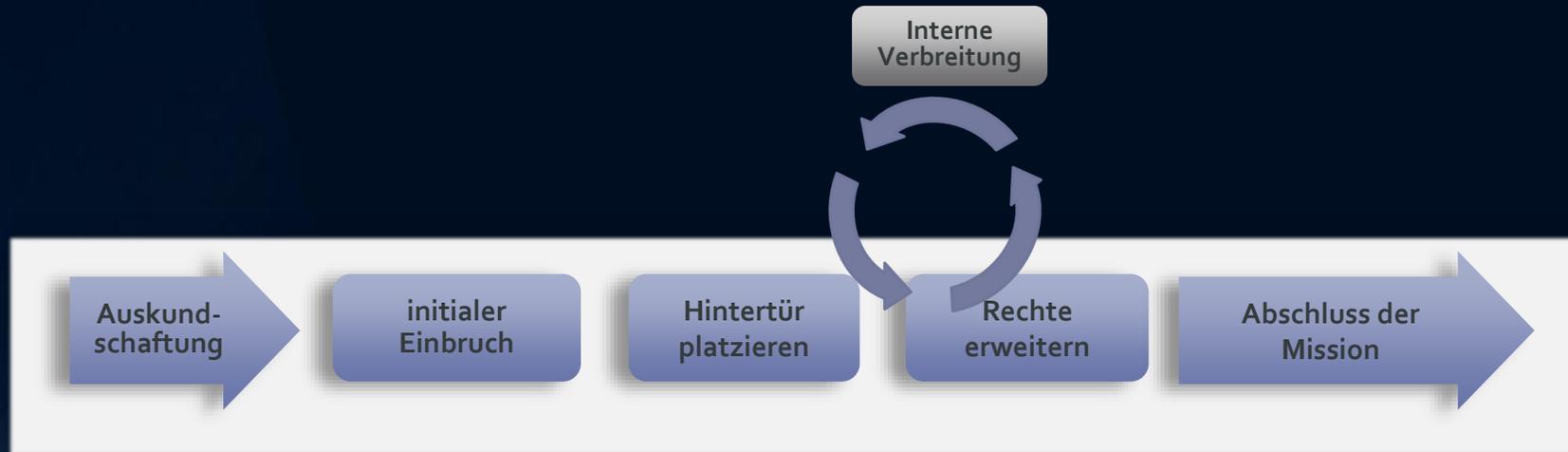


# Penetration Test VS Red Teaming

- 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: [noticemercia](#)  
12.03.2023: [BRF](#)



Stephane Odent · 3rd+

+ Follow

CIO at CHU Saint-Pierre

23h ·

Opportunity knocks.... Bravo Sophos! In any case, their antivirus did not protect us and seriously weighed us down...

That said, we must indeed take cybersecurity very seriously and protect ourselves against a growing and increasingly aggressive and effective threat.

[See translation](#)



Karim Boudekhan ● 3rd+

+ Follow

Enterprise Account Manager

BELUX SOPHOS

5d ·

Do not wait before it's too late!  
Another hospital that is the target of cyberattacks.

The CHU Saint-Pierre in Brussels has closed its emergency service due to a cyberattack



With our solutions and services from Sophos, this attack would have been neutralized by our dedicated team of experts.



# Wohin geht die Reise?

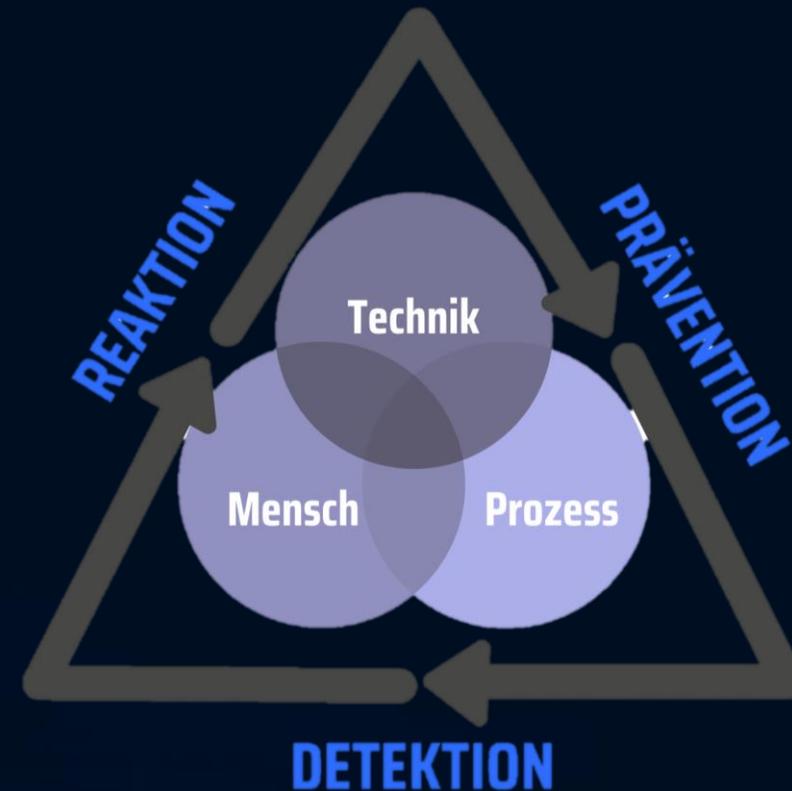
- Cyber-Crime gekommen um zu bleiben!
- Angriffe werden immer schneller
- ...und dank KI auch immer besser
  
- Messlatte für Cyber-Versicherungen steigt

*"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?

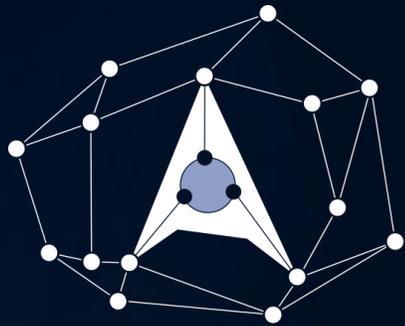
And I told them "Once you pass the compliance you will be secure"





Cybersecurity controls  
**Ineffective Vs Missing**

Vielen Dank!



**a-team rocks**  
CONSULTING & MANAGED DEFENSE

avi@a-team.rocks

