THE KILLCHAIN

MISCHA ROHLEDER

Cloud Security Consultant

Knowledge is of no value unless you put it into practice

LinkedIn

RALF SCHEDERECKER

Senior Consultant

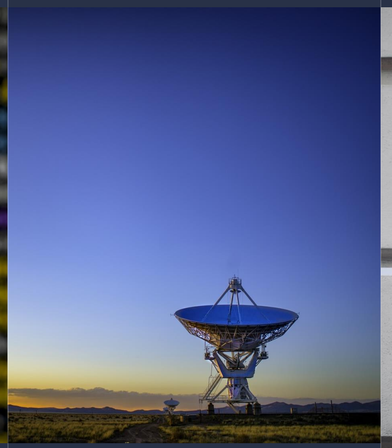
Get your mindset cloud ready!

LinkedIn

6 000 000 000 000 000 $_4$

Quelle: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Wer sind die Angreifer?

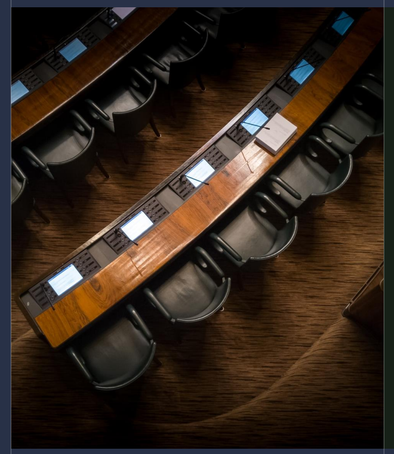
Cyber-Aktivisten	Cyber-Kriminelle	Wirtschafts-spionage	Staatliche Nachrichtendienste
			
01	02	03	04

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS_012.pdf

Previous
Next

Wer sind die Angreifer?

Staatliche Akteure



05

Cyber-Terroristen

06

Skript-Kiddies

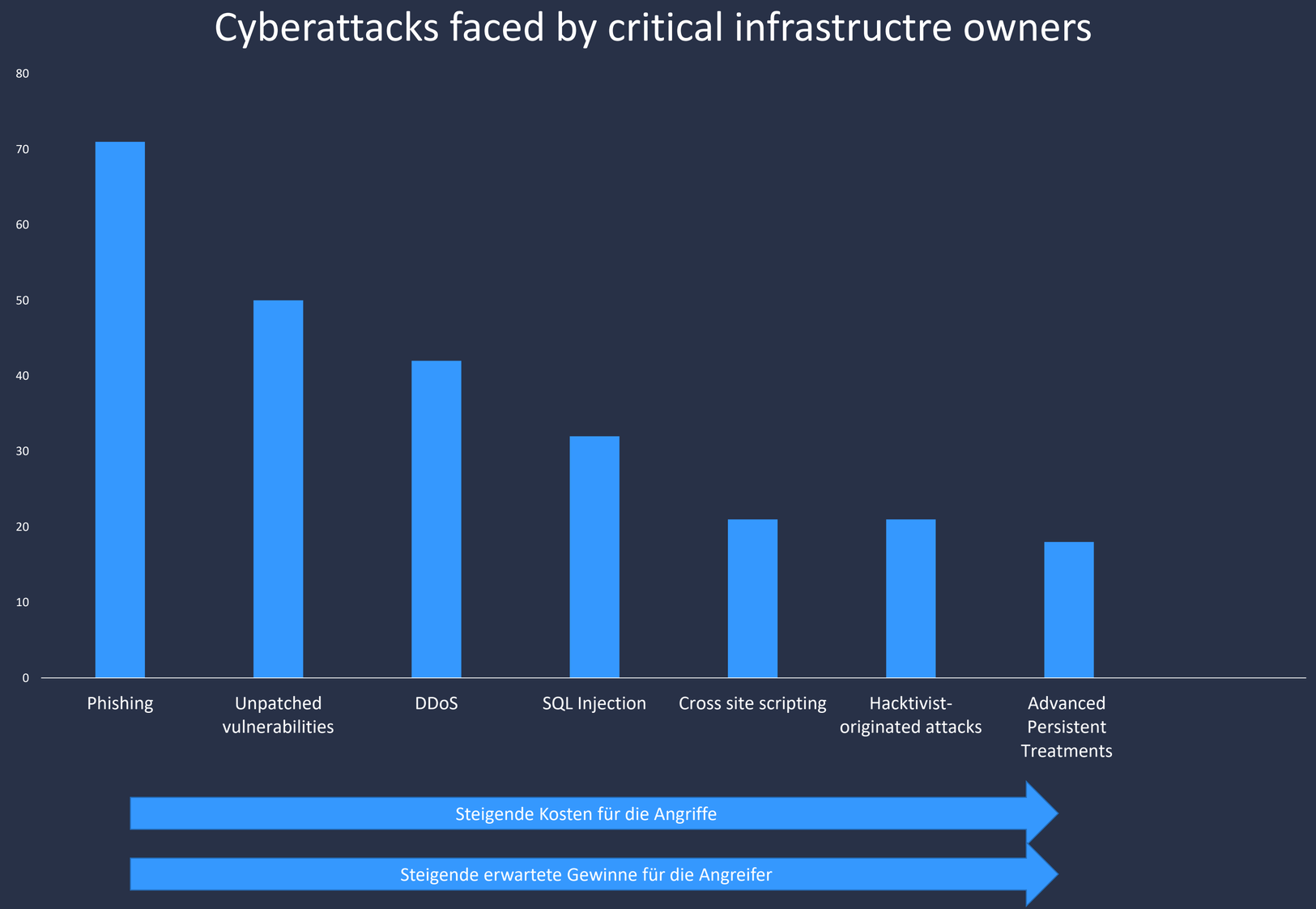
07

Ehemalige Mitarbeiter

08

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS_012.pdf

Arten von Angriffen



Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS_012.pdf

THE KILLIN

Was ist die Killchain?

- Begriff kommt aus dem Militär
- Modell zur Beschreibung von Angriffen auf IT Systeme
- Verteidigung von IT Systemen

Quelle: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf

1

External Reconnaissance

- Zielauswahl
- Sammeln von Informationen

2

Weaponization

- Auswahl des Angriffwegs
- Malware
- Ausnutzen von Schwachstellen

3

Delivery

- Übertragung von schädlichen Inhalten
- Malware, SQL Injection, …

4

External Exploitation

- Ausnutzen von **bekannten** Schwachstellen

5

Installation

- Erlangen von Kontrolle
- Agiert im Verborgenen

6

Command & Control

- Fernsteuerung der Opfer

7

Actions on Objectives

- Exfiltration
- Korruption

Quelle: https://pandanews.de/wp-content/uploads/Whitepaper-Cyberangriffe-verstehen-Die-Cyber-Kill-Chain.pdf

1

External Reconnaissance

- Zielauswahl
- Sammeln von Informationen

- **Wenige Informationen nach außen preisgeben**
- **Ports schließen / Private IPs verwenden**
- **Mitarbeiter Awareness**

Quelle: https://pandanews.de/wp-content/uploads/Whitepaper-Cyberangriffe-verstehen-Die-Cyber-Kill-Chain.pdf

2

Weaponization

- Auswahl des Angriffwegs
- Malware
- Ausnutzen von Schwachstellen

- **Kaum vorhandene Schwachstellen**
- **Regelmäßige Updates**
- **NIDS (Network-based Intrusion Detection System)**
- **NIPS (Network-based Intrusion Prevention System)**

Quelle: https://pandanews.de/wp-content/uploads/Whitepaper-Cyberangriffe-verstehen-Die-Cyber-Kill-Chain.pdf

3

Delivery

- Übertragung von schädlichen Inhalten
- Malware, SQL Injection, …

- **Mitarbeiter Awareness**
- **Proxy Filter**
- **Anti Virus**
- **Email Scanning**

Quelle: https://pandanews.de/wp-content/uploads/Whitepaper-Cyberangriffe-verstehen-Die-Cyber-Kill-Chain.pdf

4

External Exploitation

- Ausnutzen von **bekannten** Schwachstellen

- **Updates / Patches**
- **HIDS (Host-based Intrusion Detection System)**
- **DEP (Data Execution Prevention)**

Quelle: https://pandanews.de/wp-content/uploads/Whitepaper-Cyberangriffe-verstehen-Die-Cyber-Kill-Chain.pdf

5

Installation

- Erlangen von Kontrolle
- Agiert im Verborgenen

- **Anti Virus**
- **HIDS (Host-based Intrusion Detection System)**

Quelle: https://pandanews.de/wp-content/uploads/Whitepaper-Cyberangriffe-verstehen-Die-Cyber-Kill-Chain.pdf

6

Command & Control

- Fernsteuerung der Opfer

- **NIDS / NIPS**
- **Firewall**

Quelle: https://pandanews.de/wp-content/uploads/Whitepaper-Cyberangriffe-verstehen-Die-Cyber-Kill-Chain.pdf

7

Actions on Objectives

- Exfiltration
- Korruption

- **Audit Logs**
- **Honeypot**

Quelle: https://pandanews.de/wp-content/uploads/Whitepaper-Cyberangriffe-verstehen-Die-Cyber-Kill-Chain.pdf

Fragen?

Wie schützt ihr eure privaten Daten?

Vielen Dank!

LinkedIn

LinkedIn