Deutsch-Finnische Handelskammer
Saksalais-Suomalainen Kauppakamari
Tysk-Finska Handelskammaren

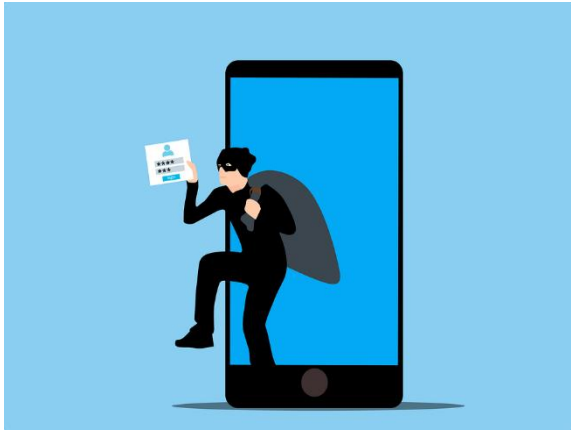
In the eyes of a hacker

@ Deutsch-Finnisches Businessforum
Cybersecurity – 28.09.2023 in Rostock

how companies can benefit from the internal view of hacking and how valuable this can be to have a better defense against hacking attacks

Agenda

1. Who is a Hacker?
2. How do Hackers act?
3. What threatens my company?
4. How to strengthen my defense?
5. 18 Basics to Cyber Security?



Who is a Hacker?

ECOVIS®

Hacker

- Skilled person with specific knowledge to overcome security measures and gain control to IT-systems & data (IT security expert)

Types of Hackers

- Good = help you to improve your security to avoid cyber attacks (white hat)
- Bad = take advantage of you poor security & execute cyber attacks (black hat)
- (imagine a housebreaker)

Motivation

- Different hackers have different goals
- Compare effort & benefit
- If your defense is weak it‘s more likely that you get hacked
- (ZA – if you look like food – you are food)

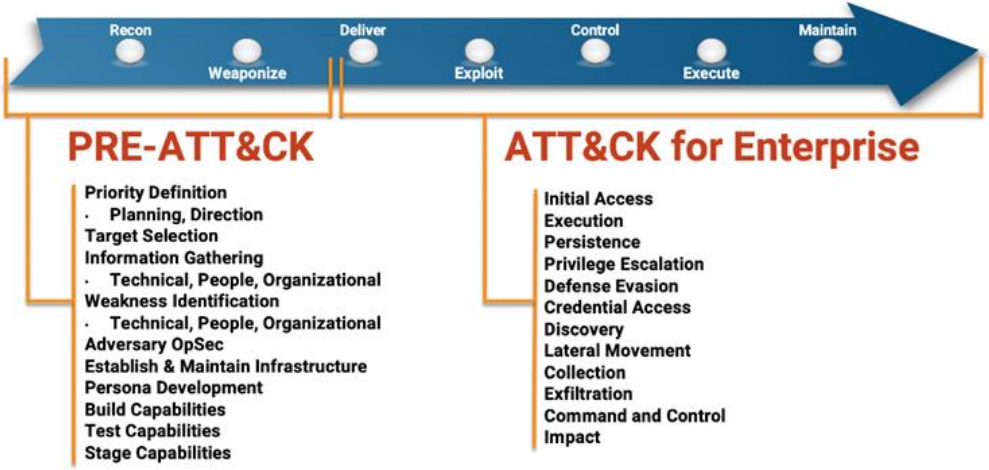
How do Hackers act?

Attack Framework

- structured and planned approach
- apply project management rules

Example

- Cyber Kill Chain
- Military origin
- 7 steps to capture an enemy target
- Know-How, Tactics, technics & tools
- Coorperation between specialists



What threatens my company?

It‘s a combination of….

1. Attack surface

- Endpoints & Servers
- Worldwide networks
- Mobile devices
- Cloud & SaaS
- Suppliers & Customers
- Service providers
- Users
- Internet of Things

2. Different threats

- Malware
- Ransomware
- Botnets & DoS
- Web based
- Social engineering
- Physical
- Phishing
- Etc.

3. Different attackers

- Cyber criminals
- Hacktivists
- Company
- Nation States
- Employee
- Script kiddies
- Cyber terrorists

Threat Landscape

My Company

How to strengthen my defense?

First… **Think if you want & can accept the impacts of cyber attacks**

- payment of damages and ransom, production downtime
- loss of reputation, infringement of law, bankruptcy

Second… **Ask yourself**

- How long am I able to act without my computers and digital data? (RTO)
- What do I do if it happens? (BCM)

Third… **Understand your threat landscape**

- Look through the eyes of a hacker and think as a hacker!
- analyse & reduce your attack surface
- enhance the effort for hacker to break into your company‘s IT

18 Basics to Cyber Security

Follow the Security Basics – Do IT! – it‘s not hard work

1. Know **all** your IT systems
2. Optimize security configuration
3. Use virus protection & firewalls
4. Update hard & software
5. Control access rights
6. Back up critical data
7. Disable macros
8. Enforce strong & fresh passwords
9. Segment network & secure transitions
10. Check home office access
11. Sensitize all employees
12. Pay extra attention to email
13. Define recovery time objective
14. Practice emergencies
15. Prepare replacement IT systems
16. Match insurance policy
17. Have the security level checked
18. Gradually reduce weak points

20% of the possible and correctly used cyber security measures provide **80%** protection against potential threats (Pareto).

Thank you!

NORMAN ESCHERICH

- M.Eng. Cyber Security & IT Forensic
- MBA Engineering Management
- Cyber Security Analyst (CySA+)
- Information Security Officer (ISO)
- Information Security Manager (ISM)
- Information Security Auditor (ISA)
- Forensic Scientist (OSSF)
- Lecturer & Trainer (ADA)

ECOVIS Europe AG

norman.escherich@ecovis.com