Ransomware:

Still Online Or Already Encrypted?

OpenRheinMain Conference 2022

September 2022

Ransomware: Still Online Or Already Encrypted?

Agenda

1 Speaker’s Introduction

2 PwC Cyber Security & Privacy

3 Evolution of Ransomware

4 Current Situation

5 Cyber Kill Chain – Ransomware

6 Effects of a ransomware attack

8 Ransomware on the example of Colonial Pipeline

9 Vulnerabilities

10 Questions & Answers

You don't have to be a hacker or programmer to work in cyber security

Speaker's Introduction

Philip Manthei

Cyber Security & Privacy | *Senior Associate*

- **At PwC since 2021**
- **M.Sc. in Business Administration (IT-Management/ Strategic Management)**
- **B.Sc. in Business Administration (IT-Management/ International Management)**

Domains

- Cyber Strategy
- Cyber Security in M&A
- BSI IT-Grundschutz
- Identity and Access Management (IAM)

Tools

- MS Azure
- Splunk
- CyberArk

Contact

E-Mail:
philip.manthei@pwc.com

LinkedIn:
/philip-manthei-12a443143

We help our clients to achieve their security goals in different fields

PwC Cyber Security & Privacy

Cyber Security & Privacy

> 400 CS&P colleagues

Frankfurt, Munich, Berlin, Düsseldorf, …

Cyber Strategy,

Cloud Security,

Identity & Access Management,

IoT/ OT- Security,

…

21
locations

>12.000
Employees
in Germany

Ransomware evolved towards an ecosystem

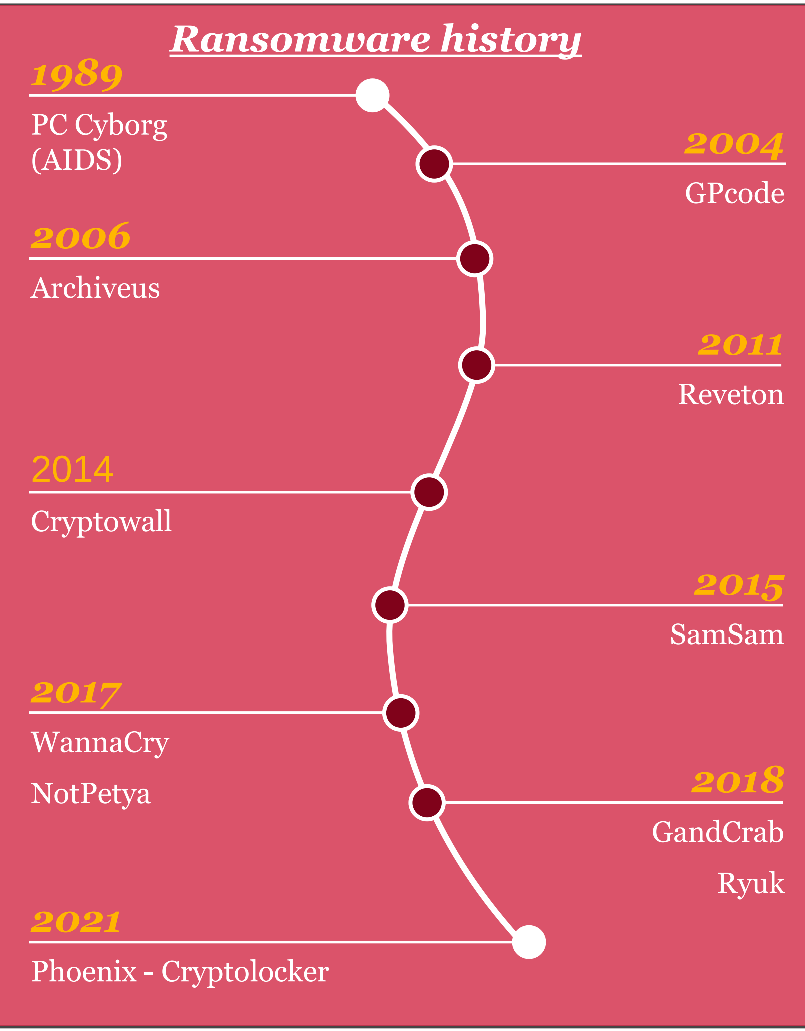
Evolution of Ransomware

The **ecosystem** of ransomware **professionalized**

The demanded **ransom raise** from **40 up to** more than **several million euros**

Ransomware-as-a-Service:

Subscription Business Modell that offers ransomware tools to attack a customer's target



Ransomware history

1989 PC Cyborg (AIDS)

2004 GPcode

2006 Archiveus

2011 Reveton

2014 Cryptowall

2015 SamSam

2017 WannaCry, NotPetya

2018 GandCrab, Ryuk

2021 Phoenix - Cryptolocker

During the last years, the number of ransomware attacks soared

Current Situation

⚠ **66 %** of the responders **experienced** a **ransomware attack**

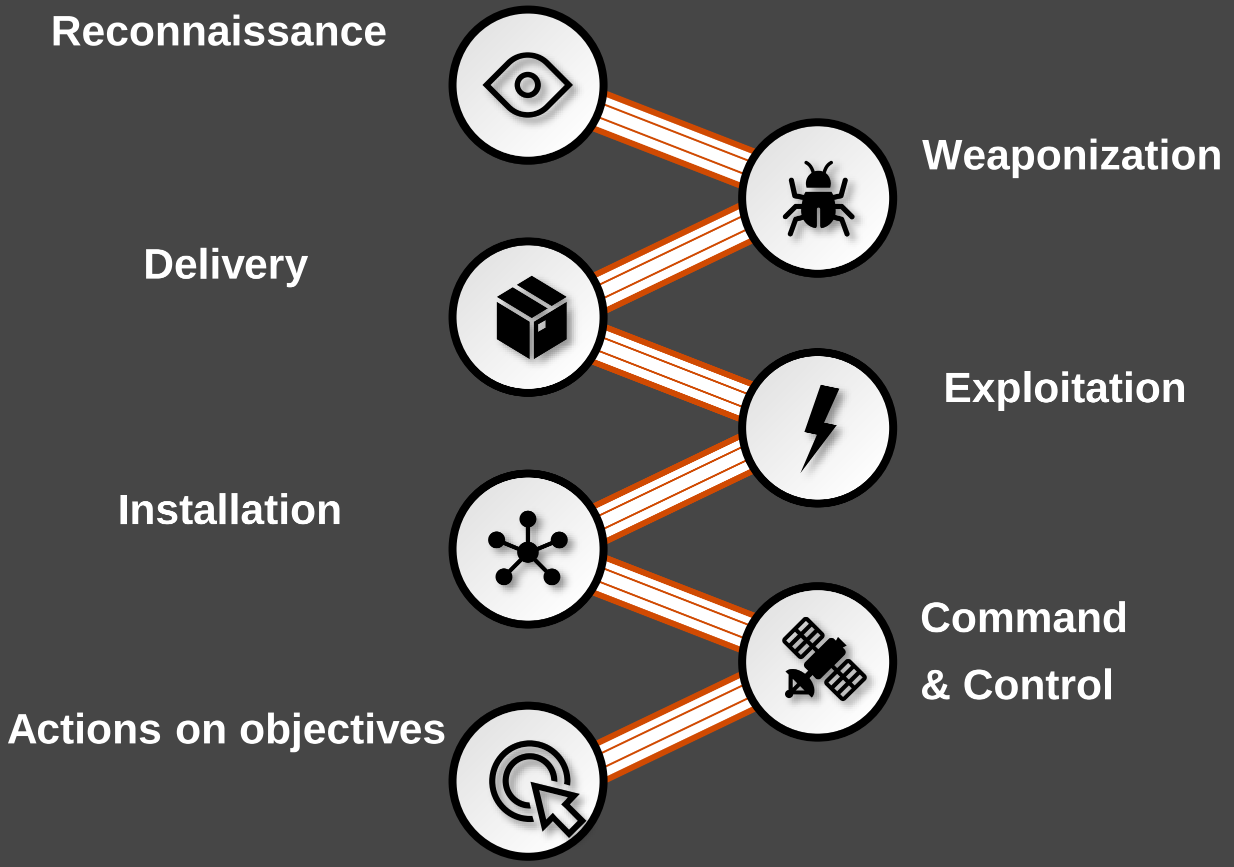
€ **46 %** of the responders **paid** the **ransom**

4 % of the responders who **paid** the **ransom got** their **full data back**

The State Of Ransomware – Sophos (2022)
https://www.sophos.com/en-us/whitepaper/state-of-ransomware

The Cyber Kill Chain helps to model attacks such as Ransomware

Cyber Kill Chain - Ransomware



Ransomware - Facts

- **Business decisions** are primary **drivers of** becoming a potential **target**
- **Multiple actors** are **involved** in a ransomware attack
- Ransomware actors **utilize different vulnerabilities** to intrude a system
- Often **Supplier** became **initial targets** of ransomware **to distribute** it **to** their **clients**

The impact of ransomware on an organizations is vast

Effects of a ransomware attack

- Loss in Business
- Loss in sensitive Data
- Partner’s Trust
- Customer’s Trust
- Fines

The entire business of U.S. Colonial Pipeline was forced to shut down

Ransomware on the example of Colonial Pipeline (1/3)

Headlines Colonial Pipeline

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

- New York Times

Hackers Breached Colonial Pipeline Using Compromised Password

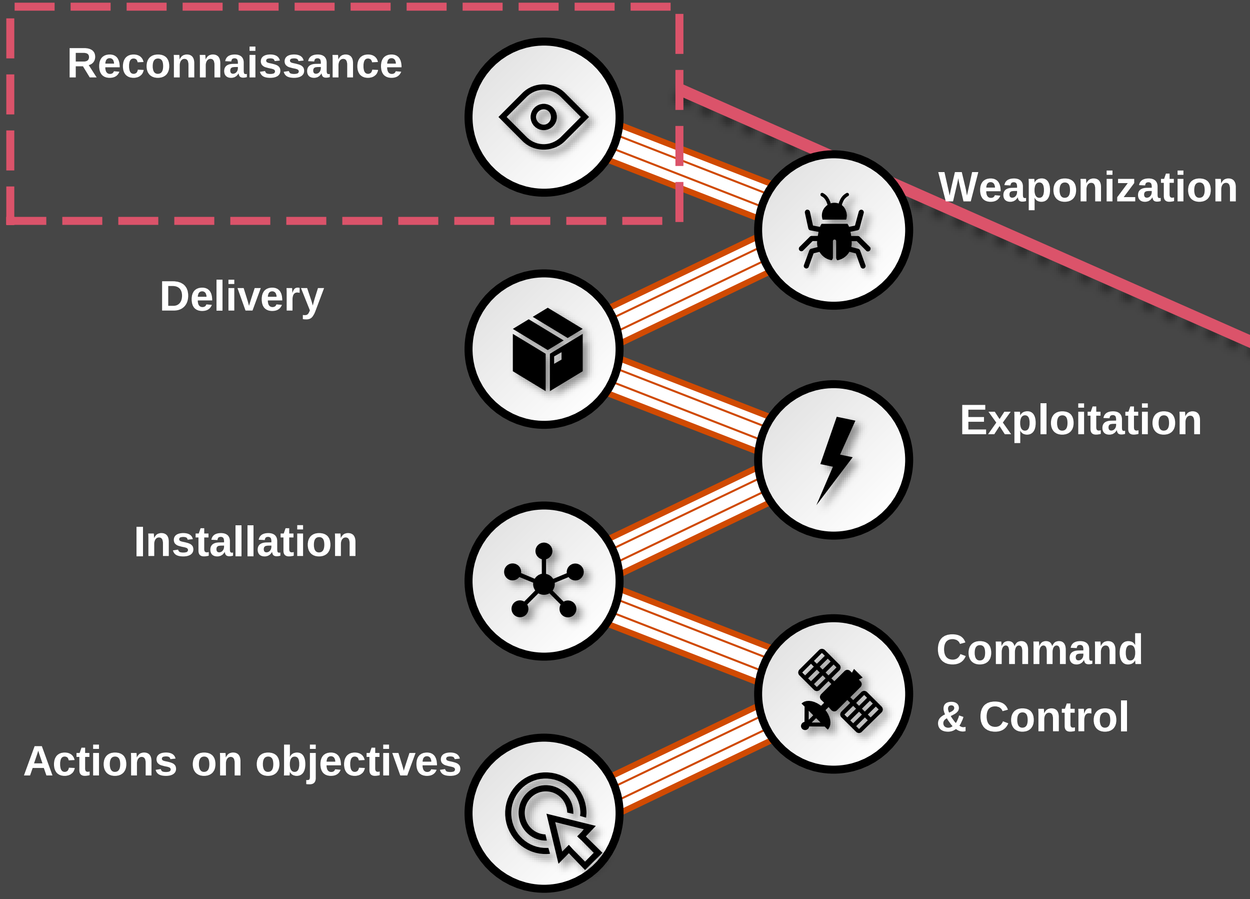
- Bloomberg

Facts

Suspect:	DarkSide
Ransom:	75 Bitcoins
Impact:	Shutdown (6 Days)
	100 GB Data Stolen

A compromised password unlocked access to the network

Ransomware on the example of Colonial Pipeline (2/3)



Details

- A **single stolen password** allowed to intrude the network of the Colonial Pipeline
- Perpetrators **accessed** the network via the **legacy VPN** of the company
- They remain **hidden** for approximately **1 week** to **scout** the network and systems

The ransomware attack could have been avoided

Ransomware on the example of Colonial Pipeline (3/3)

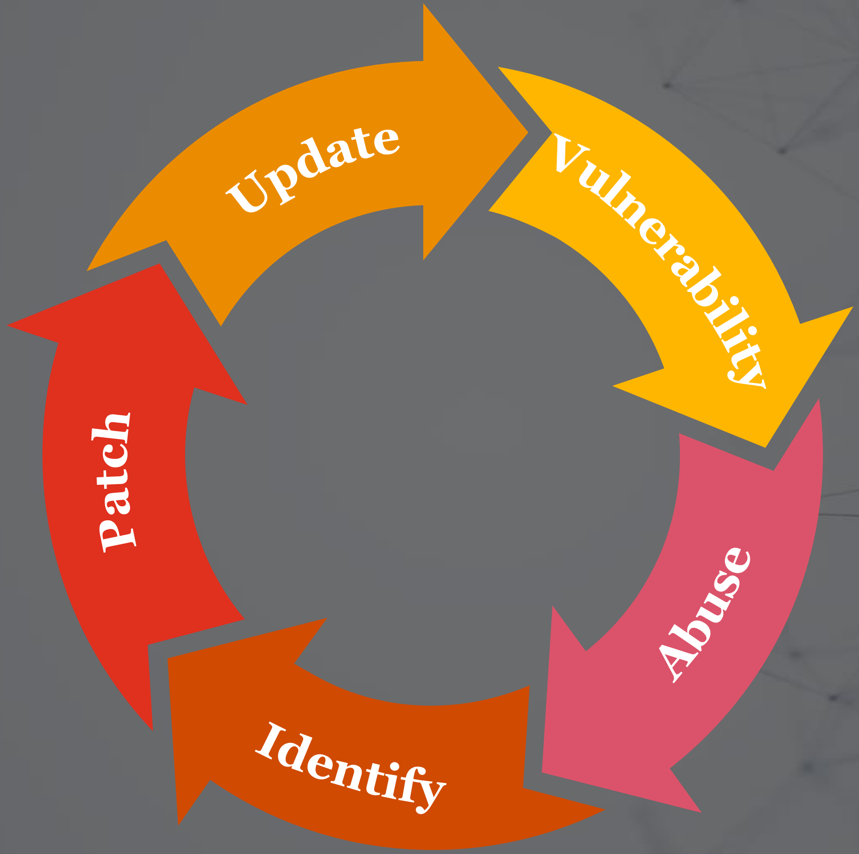
- **Multi-Factors Authentication**
- **Emergency Plan for Ransomware-Attacks**
- **Employee awareness**
- **Monitoring**

Vulnerabilities are a never ending story!

Vulnerabilities

Updates are released

Attack becomes public and gets patched

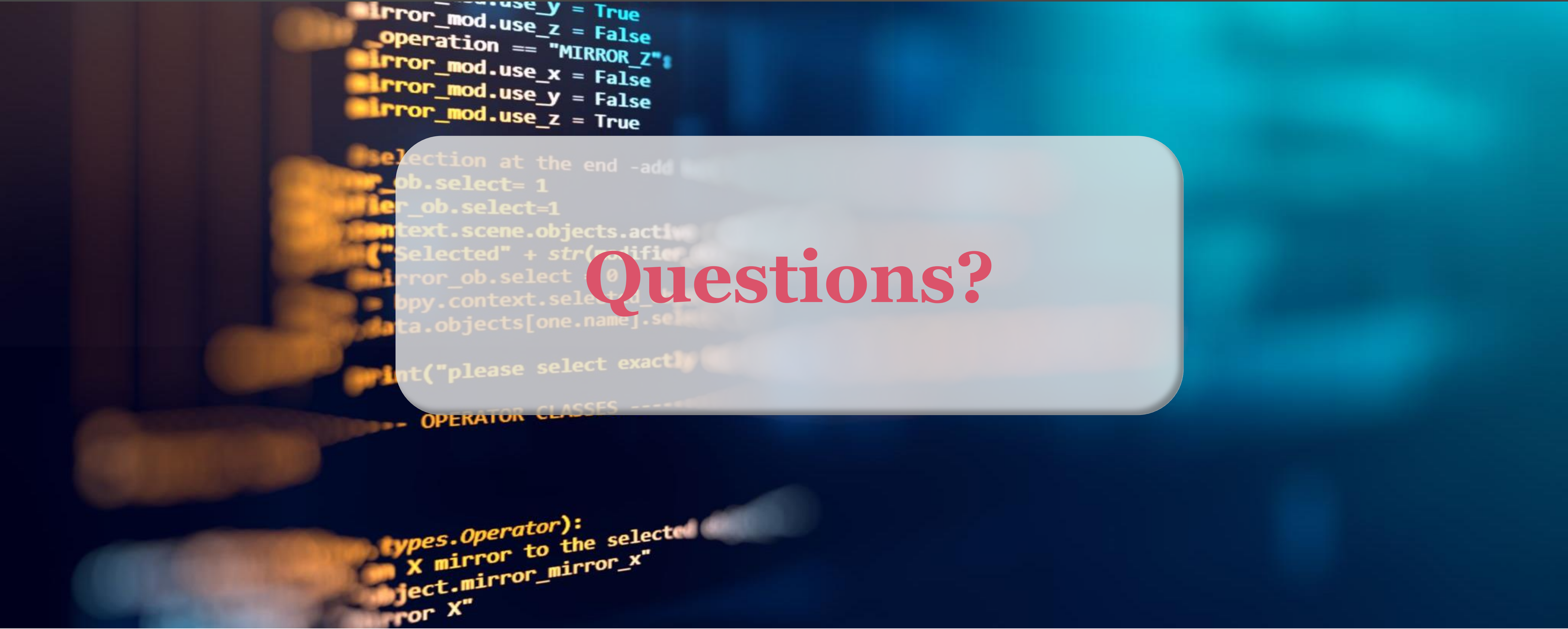


Hackers identify vulnerabilities

Hackers abuse the vulnerability to intrude the target network/ system

Please raise your questions

Q&A



```
.use_y = True
irror_mod.use_z = False
operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.acti
("Selected" + str(modifie
irror_ob.select = 0
bpy.context.selected_
ta.objects[one.name].se

int("please select exactly

OPERATOR CLASSES ----

types.Operator):
X mirror to the selected
ject.mirror_mirror_x"
ror X"
```

Questions?

Visit our booth and talk with us about your opportunities in cyber!

Booth

Andrea Fleuter

Monique Christoph

Philip Manthei

Gregory Schenk

Are you interested?

Let’s talk about your opportunity at PwC Cyber as intern, working student or associate!

Thank you for your attention!

pwc.de

Reach out to us!

Social Media

Social Media

INSTAGRAM

FACEBOOK

LINKEDIN

XING

Versprochen.

PODCAST