

Von TIBER-EU zu DORA TLPT



Erfahrungen und Herausforderungen

Agenda

1. Überblick
2. Ablauf und Aufgaben
3. Erfahrungen



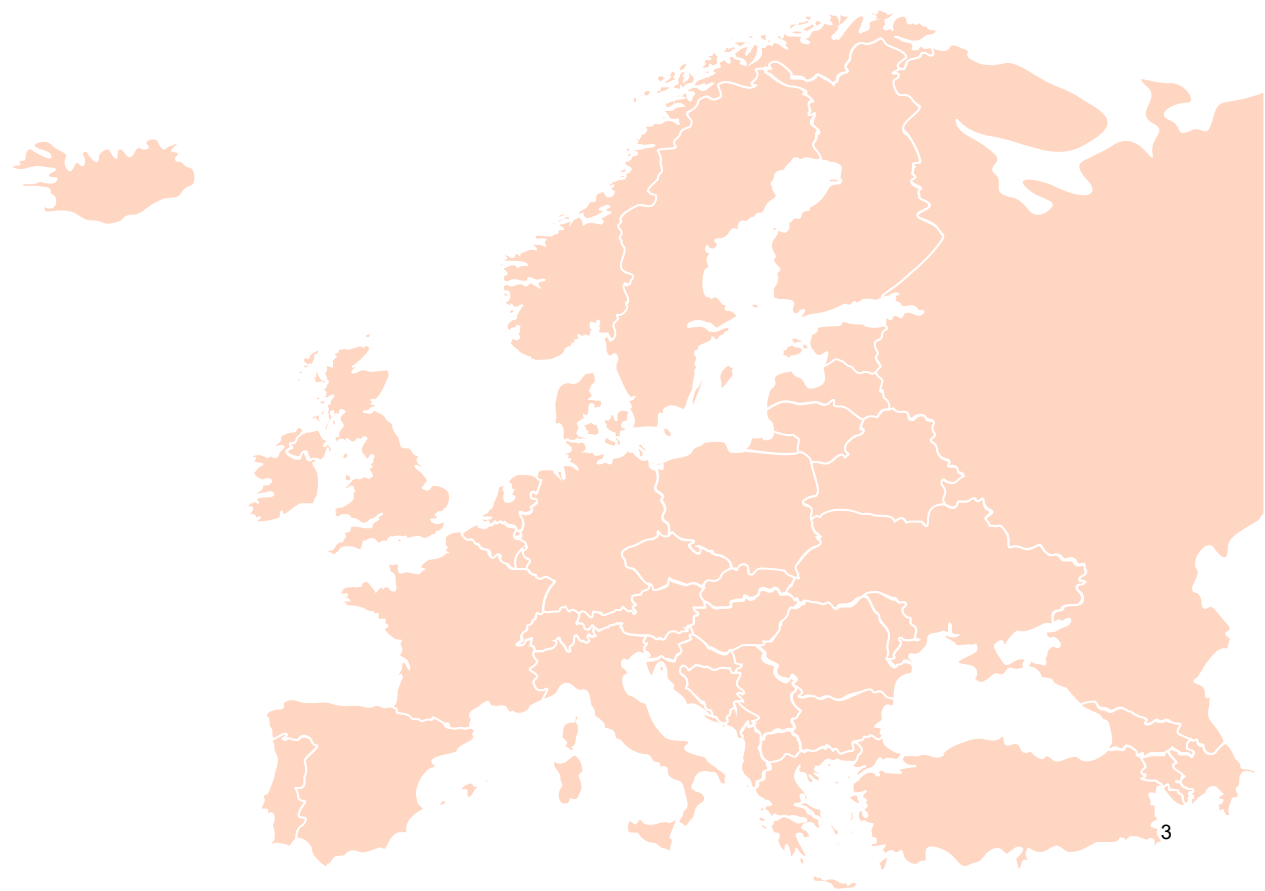
Ihre Vortragenden



Florian Hehenberger
Manager, PwC Cybersecurity & Privacy
Tel.: +43 699 16305004
E-Mail: florian.hehenberger@pwc.com
Hafenstrasse 2a, 4020 Linz



Akashpreet Wedech
Senior Assosicate, PwC Cybersecurity & Privacy
Tel.: +43 676 6870278
E-Mail: akashpreet.wedech@pwc.com
Donau-City-Straße 7, 1220 Wien



1

Überblick



Überblick Angriffssimulationen

Finden von Schwachstellen



Vulnerability Scan

Toolbasierter, automatisierter Scan nach Schwachstellen von zuvor definierten Zielsystemen.

Ziele :

Bekannte Schwachstellen identifizieren



Penetration Test

Teilautomatisierter und manueller Test auf Schwachstellen von zuvor definierten Zielsystemen und Applikationen.

Ziele :

Zielgerichtet dedizierte Schwachstellen identifizieren



Red Teaming & (Threat-Led) Penetration Test

Umfängliche Angreifer-Simulation mit zuvor festgelegten Szenarien und klar definierten Endzielen.

Ziele :

Verbesserung der Cyber Resilienz



Purple Teaming

Angreifer-Simulation mit teilautomatisierten und manuellen Testszenarien gemeinsam mit dem SOC Team (Blue Team).

Ziele :

Verbesserung der Cyber Resilienz

Base-Line Security Testing

Advanced Security Testing

Was ist das TIBER-Framework?

(TIBER = Threat Intelligence-Based Ehtical Red-Teaming)



TIBER ist ein standartisiertes Framework zur Durchführung von Red Team Simulationen (Branchen-unabhängig)

Simulation beinhaltet Threat Intelligence und Red Teaming

TIBER-AT wird veröffentlicht durch OeNB

TIBER-Frameworks werden als Grundlage für DORA TLPTs verwendet



Was ist DORA TLPT?

Durchführen von Threat-Led Penetration Tests (TLPT) basierend auf TIBER-EU / TIBER-AT (Threat Intelligence & Red Teaming)

Durchführen von drei Angriffssimulationen basierend auf Threat-Intelligence Informationen

Risikobasierter Ansatz auf kritischen Live Produktionssystemen

Durchführen von unabhängigen Tests (zumindest alle 3 Jahre)

Beispielhafte TLPT Roadmap

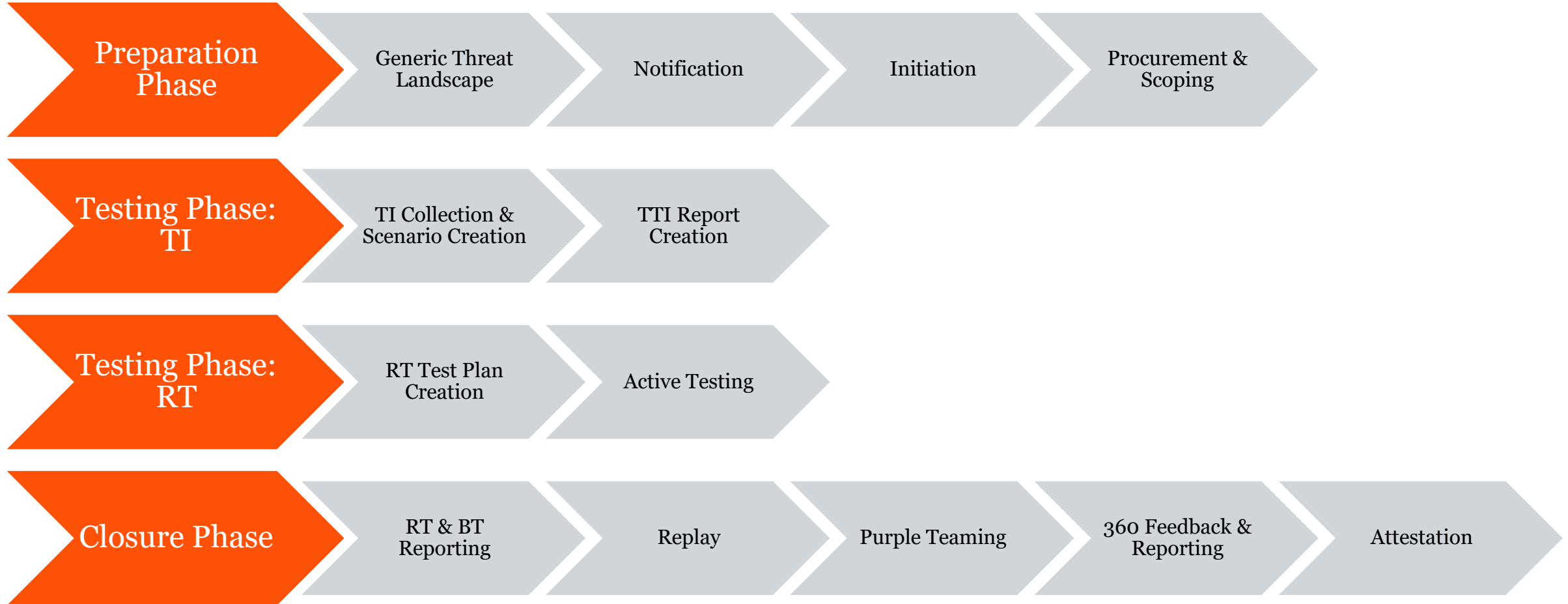


2

Ablauf und Aufgaben

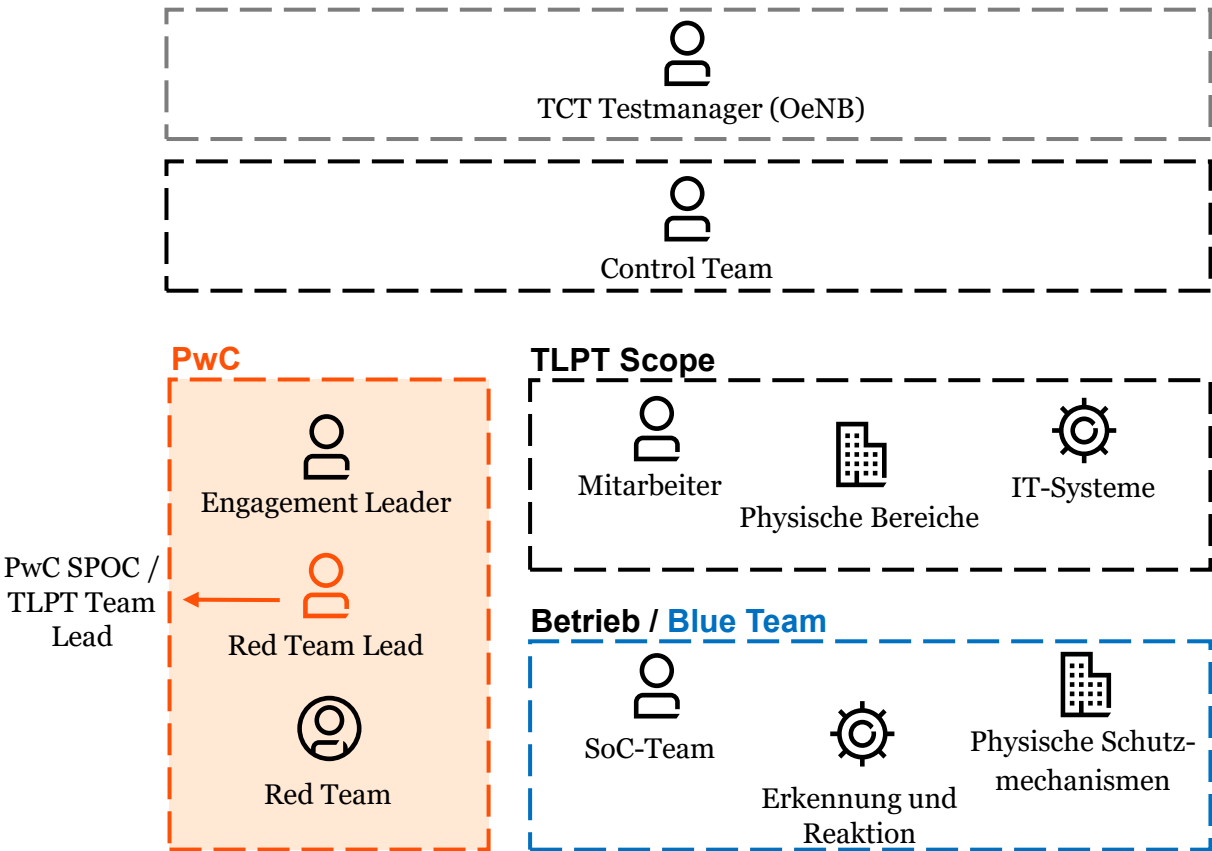


Wie ist der Ablauf einer TIBER basierten Red Team Simulation?



Involvierte Teams und Kommunikationswege

- OeNB – Begleitet die Simulation aktiv
- Unternehmen – Bildet ein Control Team
- Unternehmen – Blue Team (BT) ist nicht informiert
- Red Team (RT) und Threat Intelligence (TI) Provider führen die Tests durch



Lessons Learned aus TIBER / TLPT basierten Red Team Simulationen?

Geheimhaltung ist eine große Herausforderung

Simulation für das gesamte Unternehmen (insb. Blue Team, Incident Response Prozesse, etc.)

Insbesondere die abschließenden Purple Teaming Workshops bieten viel Mehrwert

Teilweise etwas aufwändig aufgrund des Formalismus



3

Erfahrungen & Praxisbeispiele



Threat-Led Penetration Testing

Praxiserfahrung: Physischer Zutritt



Threat-Led Penetration Testing

Praxiserfahrung: Deep Fake

Florian



DORA TLPT & TIBER-AT

Roland

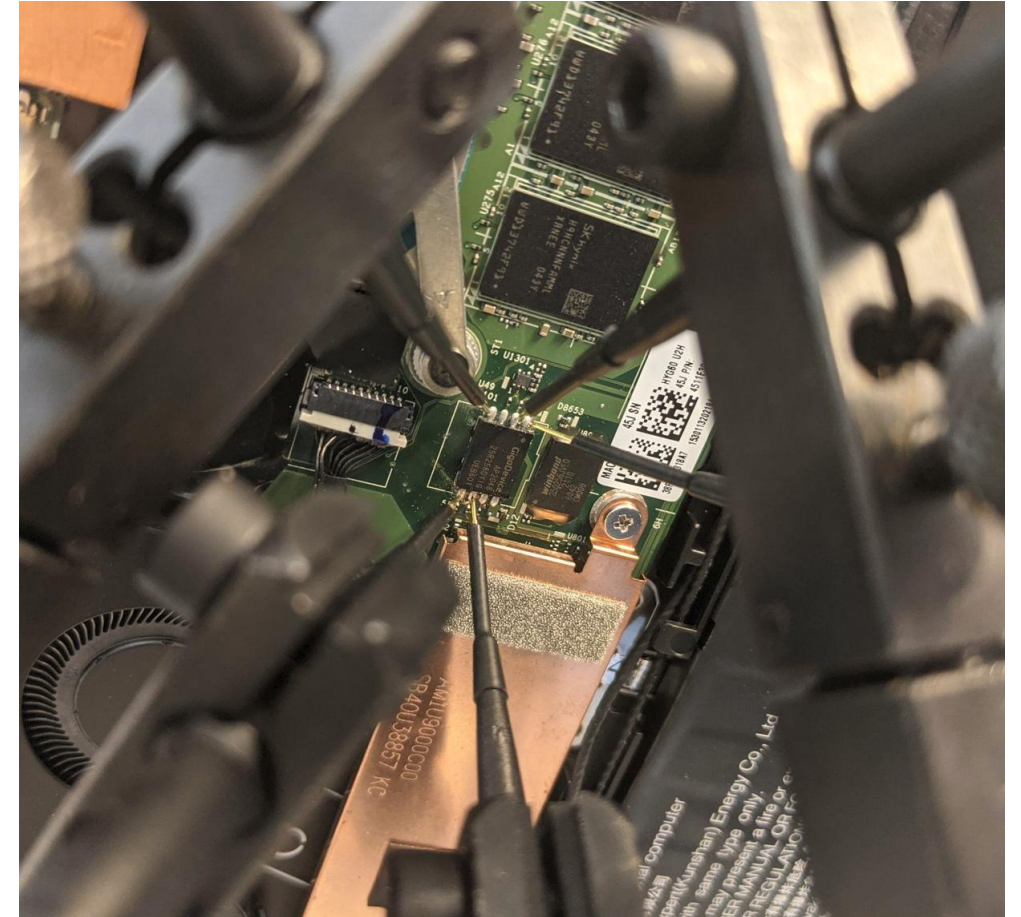
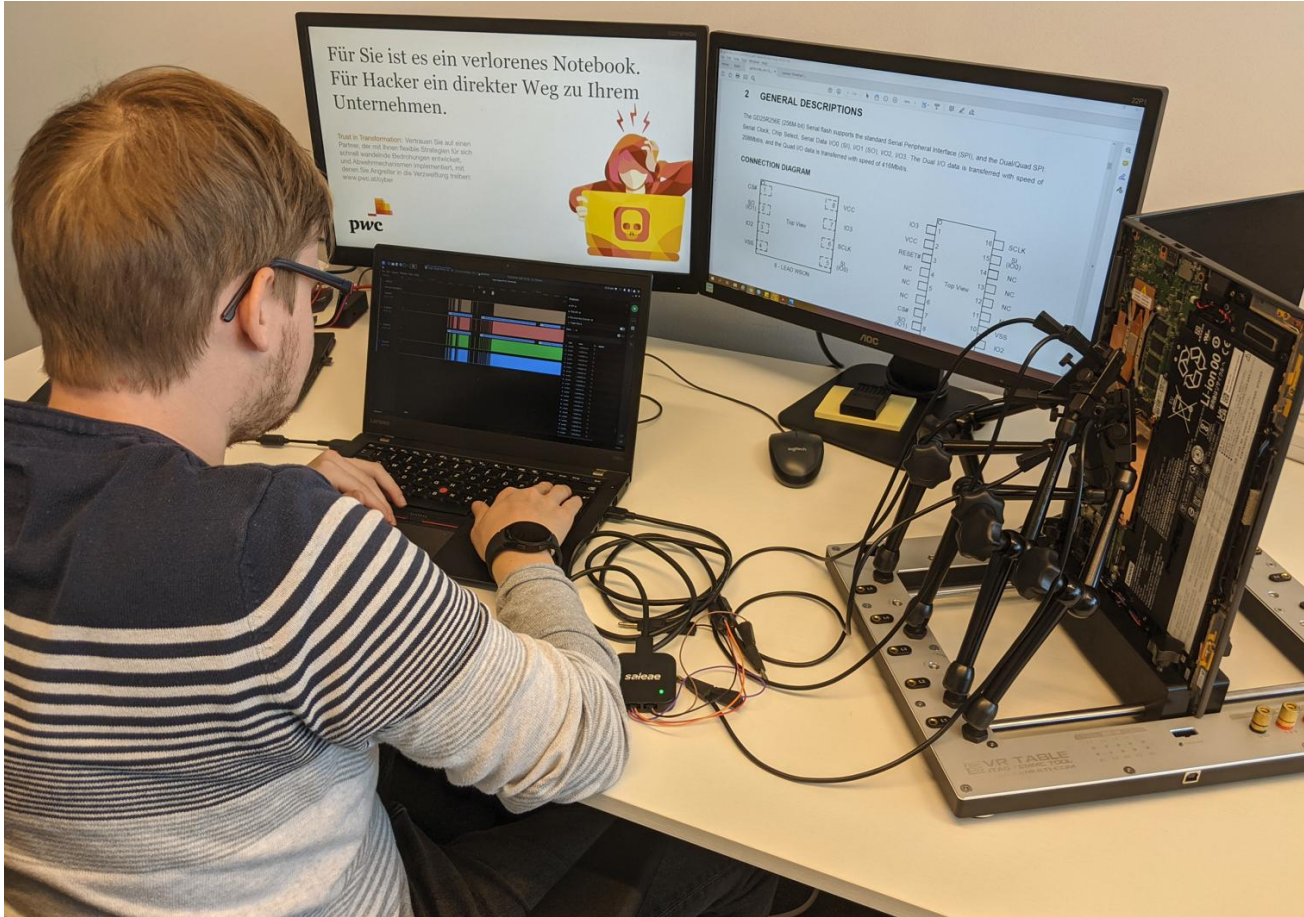


Rolian

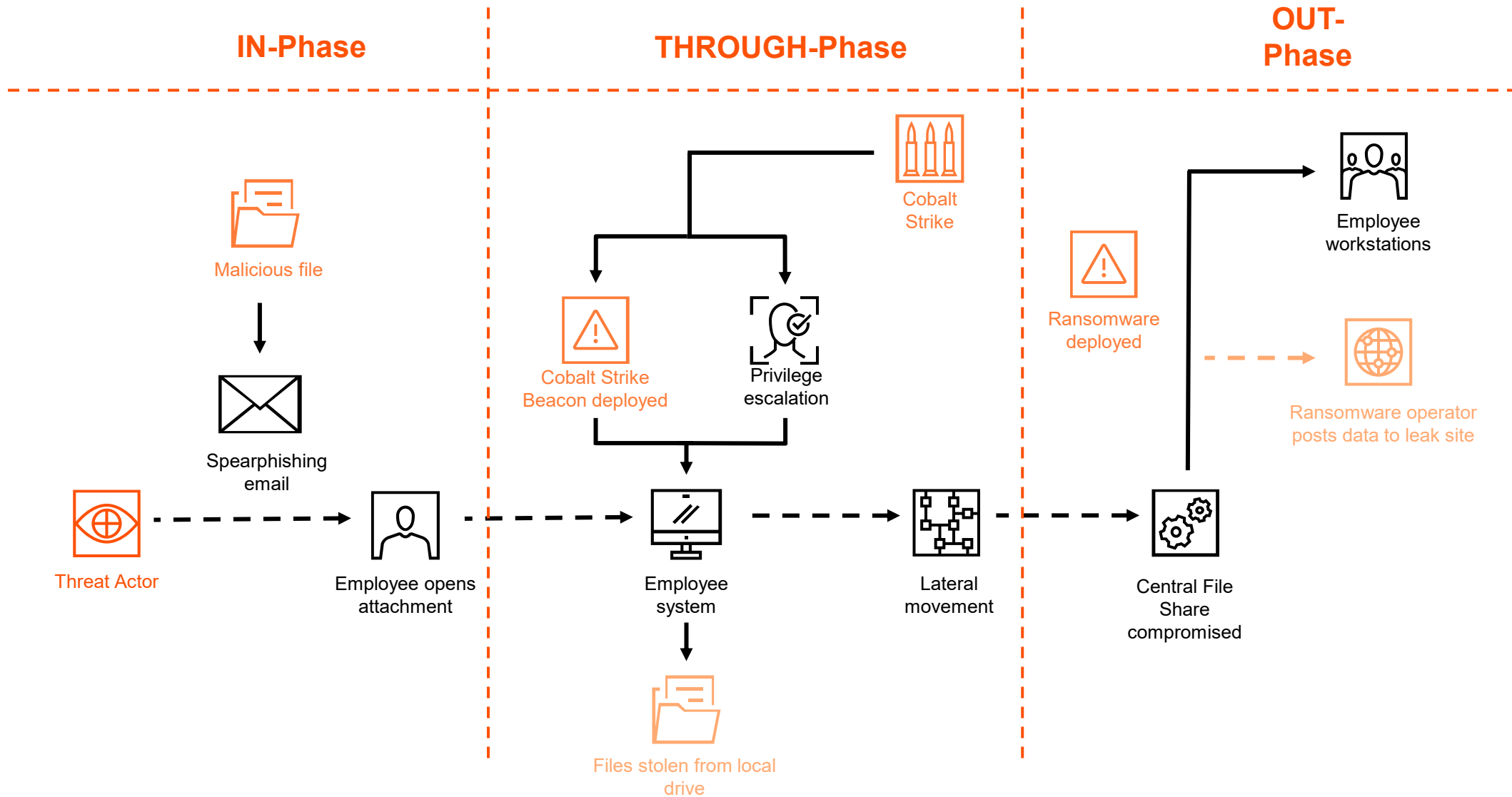


Threat-Led Penetration Testing

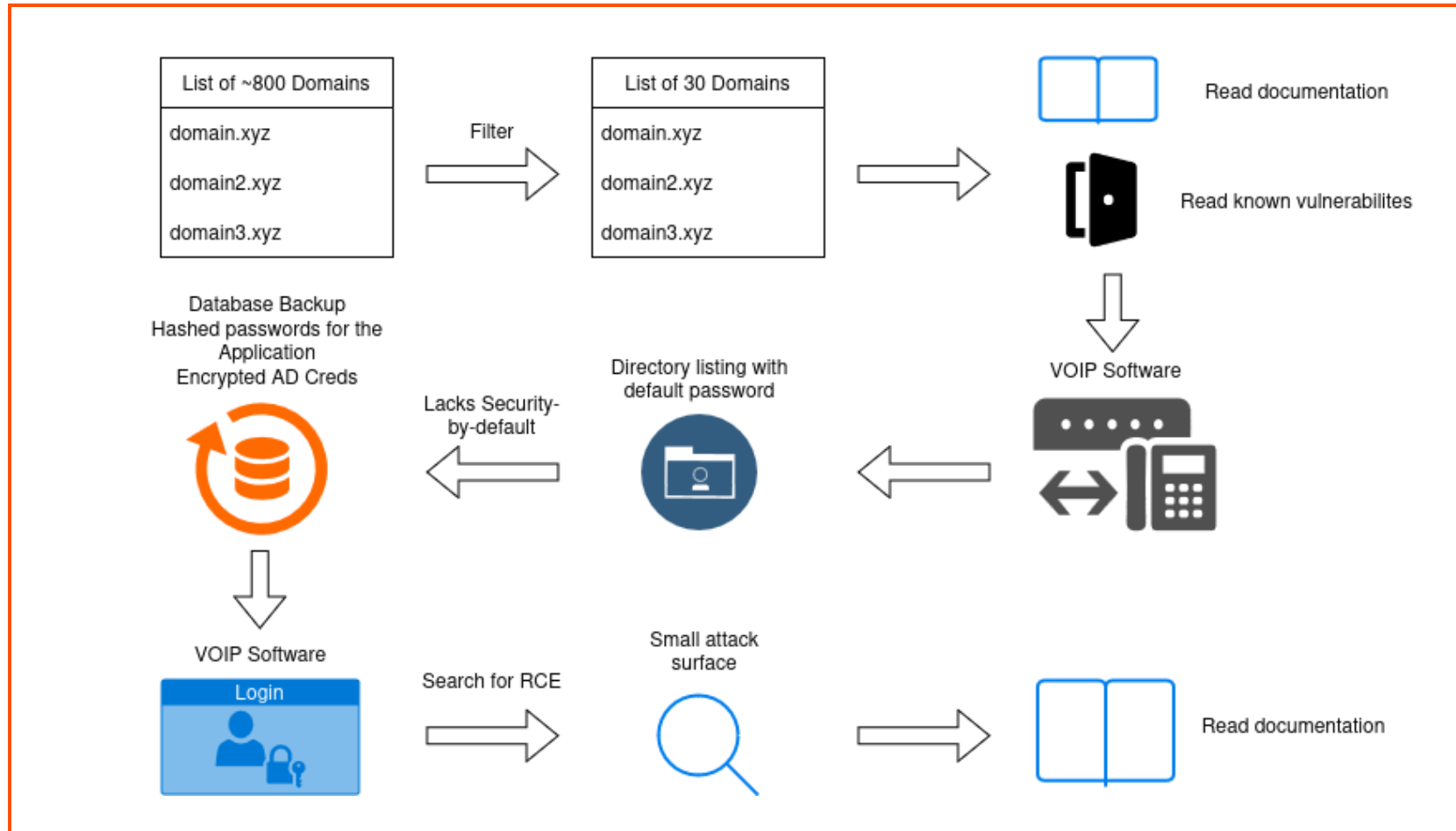
Praxiserfahrung: Hardware Angriffe



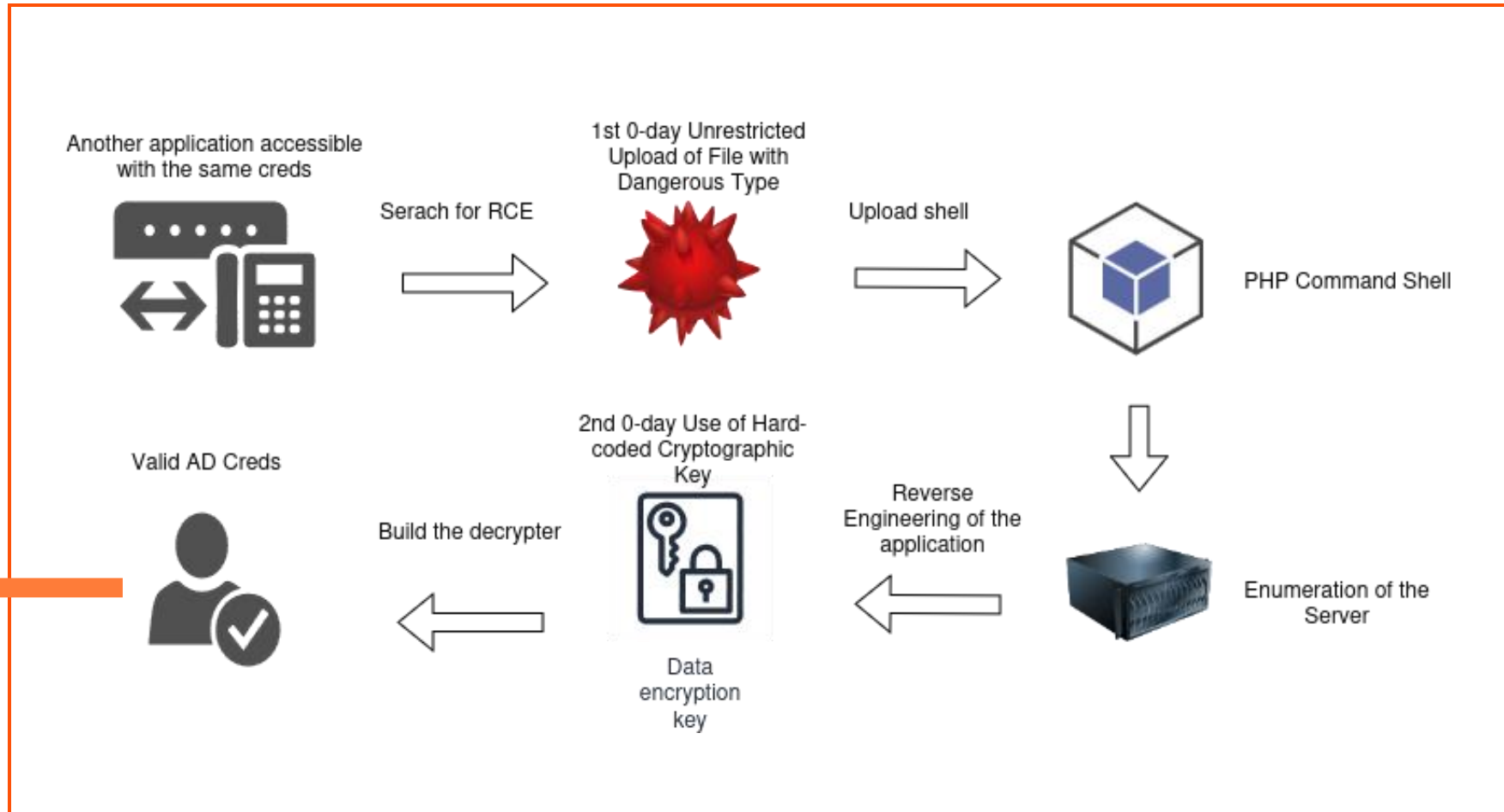
Wie könnte ein TLTP-Angriffsszenario aussehen?



Mögliches Angriffsszenario TLPT – IN Phase



Angriffsszenario TLPT – IN Phase



Diskussion & Fragen

Diese Präsentation dient ausschließlich als allgemeine Information über ausgewählte Themen und stellt keine fachliche Stellungnahme dar. Sie ersetzt insbesondere keine fachliche Beratung. Wir übernehmen keine (explizite oder implizite) Haftung für die Richtigkeit und Vollständigkeit der in dieser dargestellten Informationen und lehnen – im Rahmen der gesetzlichen Möglichkeiten – die Haftung und Verantwortung für Konsequenzen aus Handlungen, die ausschließlich auf der Verwendung oder Nichtverwendung von darin enthaltenen Informationen basieren, ab.

© 2025 PwC Österreich. „PwC“ bezeichnet das PwC-Netzwerk und/oder eine oder mehrere seiner Mitgliedsfirmen. Jedes Mitglied dieses Netzwerks ist ein selbstständiges Rechtssubjekt. Weitere Informationen finden Sie unter [pwc.com/structure](https://www.pwc.com/structure).