ICS Firing Range: Erfolgreiches Abwehren eines Hackerangriffes auf ein Wasserkraftwerk

Kukovic Christoph , Schwabel Tobias
St. Pölten
11. 10 2024

Verbund

Wer sind wir?

Christoph Kukovic

Chief Information Security Officer

Tobias Schwabel

Student für Energie- & Automatisierungstechnik

Projekt Vision

- **Herausforderungen** der Cybersecurity in der Welt der OT sichtbar machen
- **Funktionsweise** ergründen als Top-Priorität
- Erschaffen einer **realistischen Trainingsumgebung**

Es braucht einen greifbaren Prototypen - ICS Firing Range!

Entstehungsgeschichte - Vorstellung vs Realität

Das Ergebnis muss **Eindruck** hinterlassen!

- Angreifer soll **Chaos** auslösen
- Hacking eines Pumpspeicherkraftwerks
- Drücken des Buttons „Klappe Auf“
- **Wassermassen** sollen einen **Staudamm** herabströmen
- Das **Training** soll in Echtzeit den Angriff verhindern

Wissen wir eigentlich, wovon wir reden?

Richtige Fragen stellen

- Was sind potenzielle Gefahren?
- Welche Komponenten besitzt ein Kraftwerk?
- Was macht „die“ Steuerung?
- Wie könnte jemand eine Steuerung manipulieren?
- Wie kann gegengesteuert werden?

Teamfindung

- Projektleitung
- Red Team
- Blue Team
- Modelbauer
- Steuerungstechniker

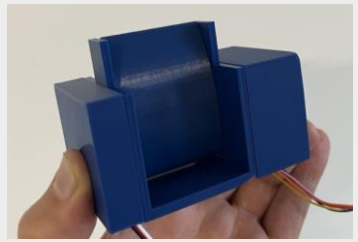
…
Sehr gestreute Kompetenzen

Wir benötigen weitere Hilfe – Masterarbeit?

Studienbegleitetes Arbeiten

- Anfrage
- Themenfindung
- Betreuerfindung
- Anpassen des Themas
- VERBUND – TU Wien Abstimmung

- **Auf geht’s!**



Aufgaben

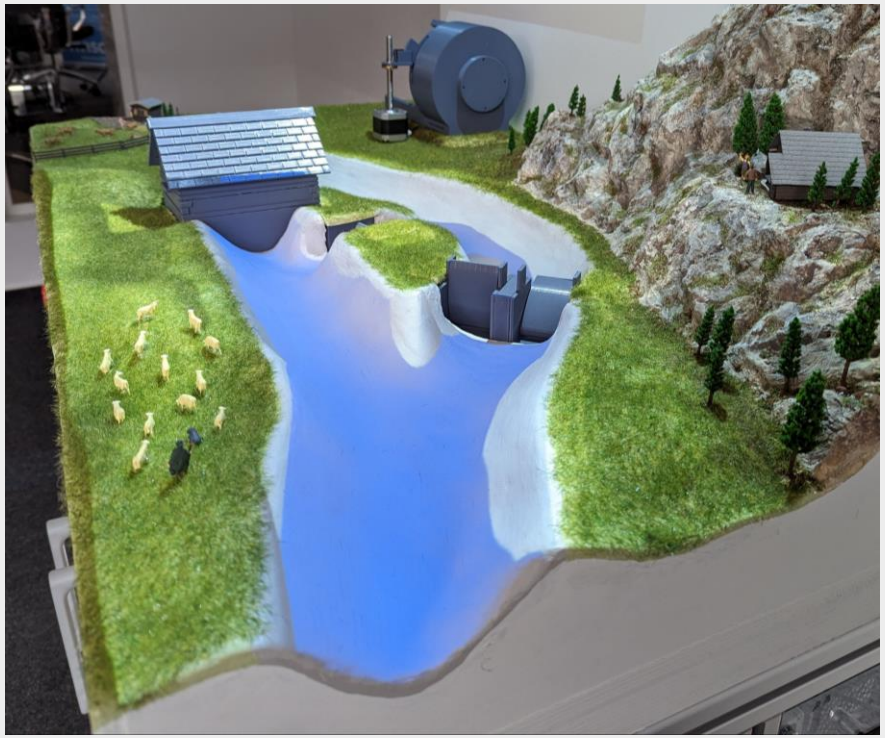
- Recherche – wie funktioniert ein Kraftwerk?
- Strategien, um Steuerungen von Grund auf modular auszulegen
- Kommunikation aufbauen
- Steuerung auslegen
- Steuerung in Betrieb nehmen
- Visualisierung erstellen und anbinden
- **Projektabschlusstermin**

Abgrenzung zum restlichen Projektteam finden

V

Erwartung

- **Ich**: Kein Informatiker / kein Security Spezialist
- Anforderung klingt machbar
- Arbeit mit Leuten aus dem Gebiet
- Sollte etwas nicht klappen – einfach Fragen
- Jeder kennt sich bei meinen Fragen aus, wenn nicht anderer Kollege
- Immer Zugriff auf alle Systeme
- Alle Informationen, die ich bekomme stimmen



Prozess

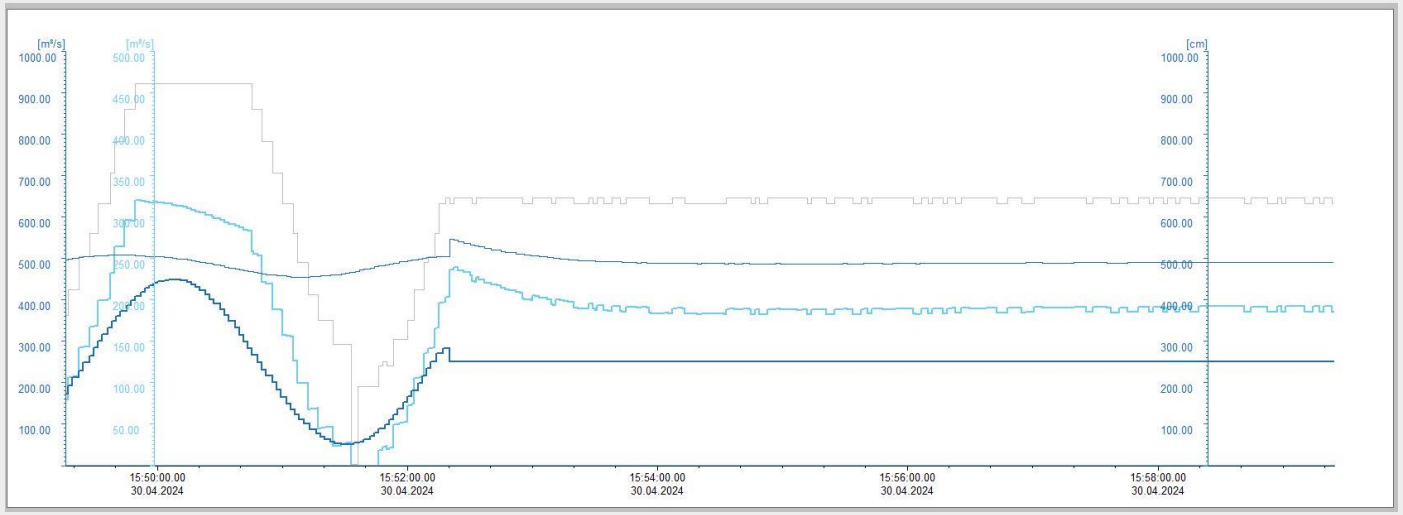
- Informationen sammeln
- „Passt das so, ja aber…“
- „Da bin ich nicht die Richtige Ansprechperson“

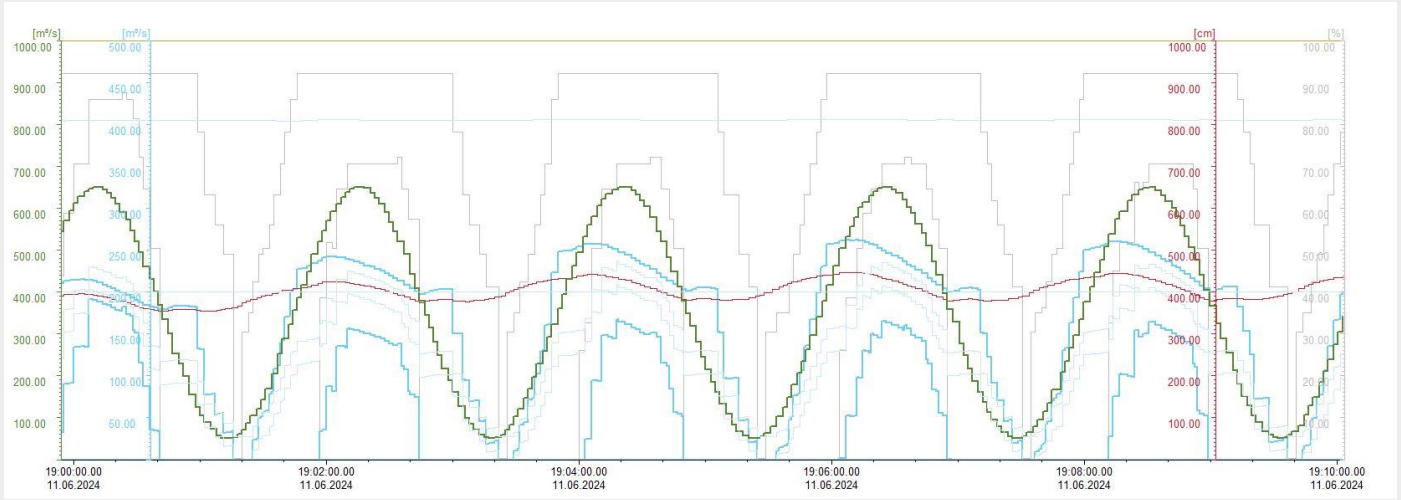
- Dann besten Gewissens
- Welche Einschränkungen damit Zeitplan realistisch?
- Laufende Schulung mit Herstellern ausmachen

- Koordinierung mit den Teams
- Telefonate, Abstimmung

Schnittstellen!!! Wenn nichts redet funktioniert nichts …

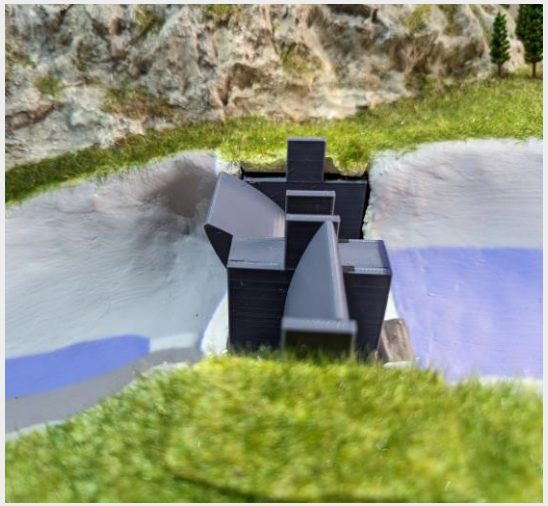
Verlängerung
Schreiben an der Arbeit

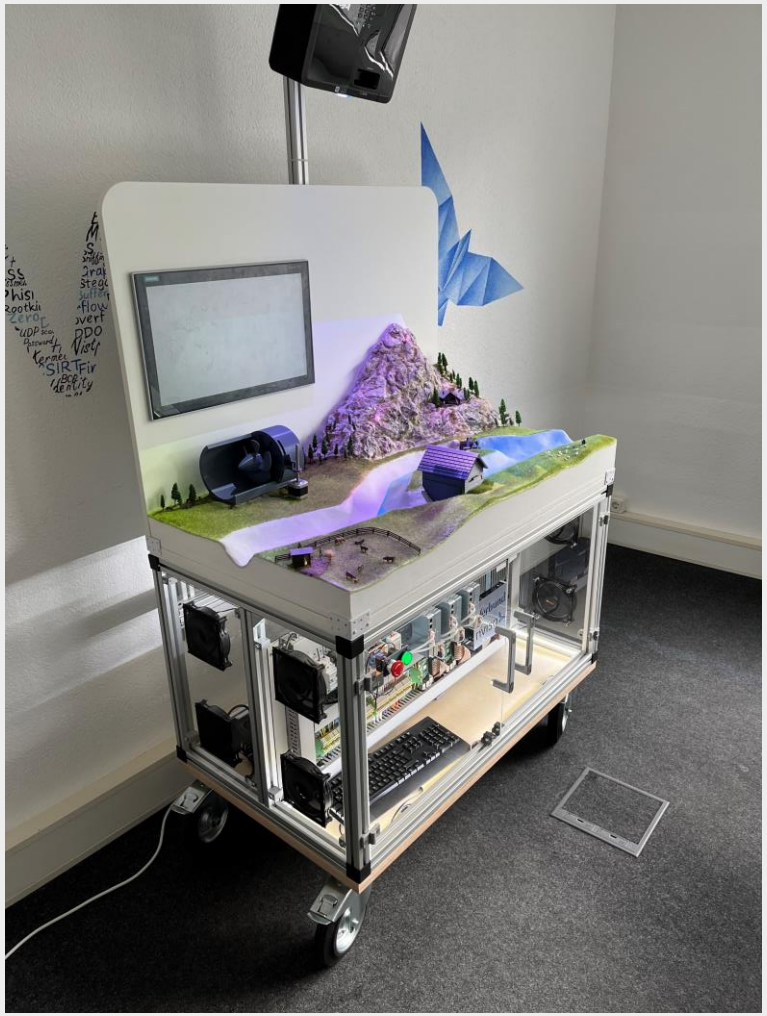




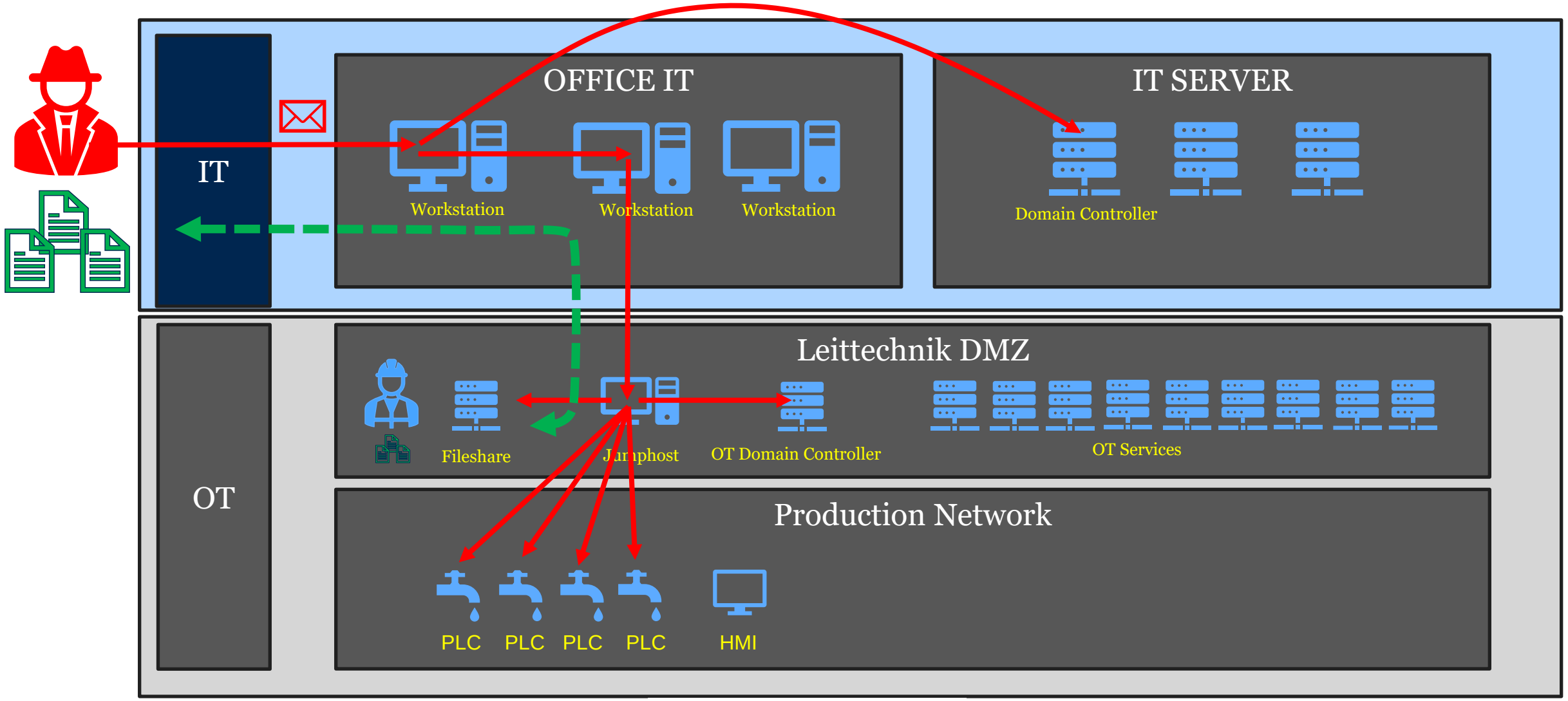
Funktionen

- Automatischer Betrieb
- Manueller Betrieb
- Automatische/Manuelle Ansteuerung Notablass
- Verstellen der Zufluss-Funktion
- Notabschaltung der Turbine
- Wiedergeben betriebsnotwendiger Zustandsgrößen
- Signal und Fehleraufzeichnung





Walktrough


IT
OFFICE IT
Workstation
Workstation
Workstation
IT SERVER
Domain Controller
OT
Leittechnik DMZ
Fileshare
Jumphost
OT Domain Controller
OT Services
Production Network
PLC
PLC
PLC
PLC
HMI

Ergebnis

- **Model** um Awareness und Wissen im Gebiet der **Cyberangriffe** auf **IT** und **OT Umgebungen** zu sammeln
- Vorbereitung auf OT Cyber Security Range
- Angriff wird analysiert und nachgestellt
- **15 hands-on Lab Exercises**, in denen der Angriff forensisch untersucht wird.

Vielen Dank!