TRAIN AS YOU FIGHT
AIT CYBER RANGE

Cyber Security Training und Übungen

Gregor Langner
AIT Austrian Institute of Technology
Center for Digital Safety & Security
gregor.langner@ait.ac.at

14. Juli 2023

MOTIVATION


Digitalisierung


Vernetzung


Faktor Mensch

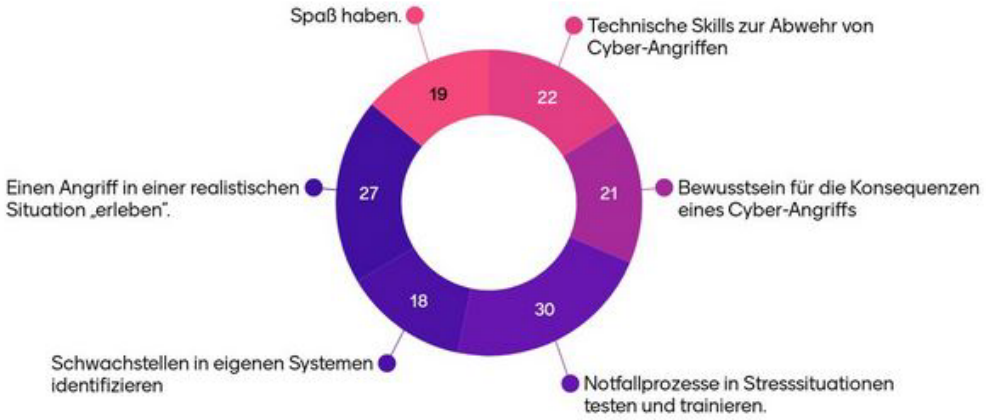

Neue Technologien


Neue Bedrohungen und Angriffe

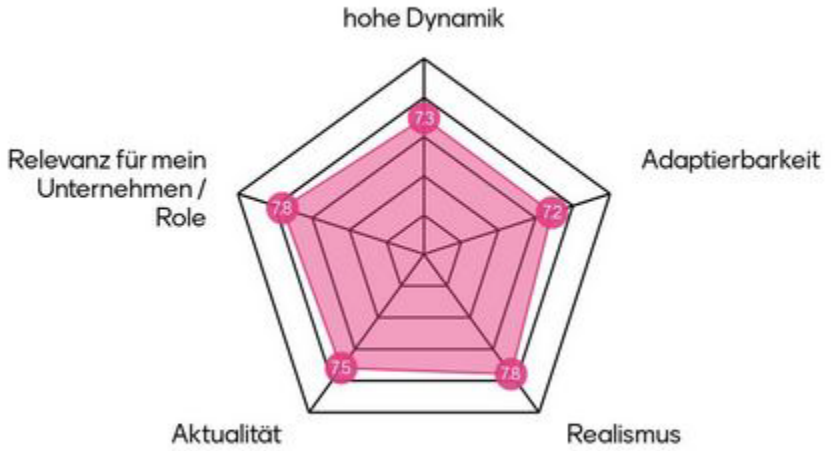

Rechtliche Anforderungen (z.B. NIS, DSGVO)

UMFRAGE ERGEBNISSE

Welche Resultate werden erwartet?

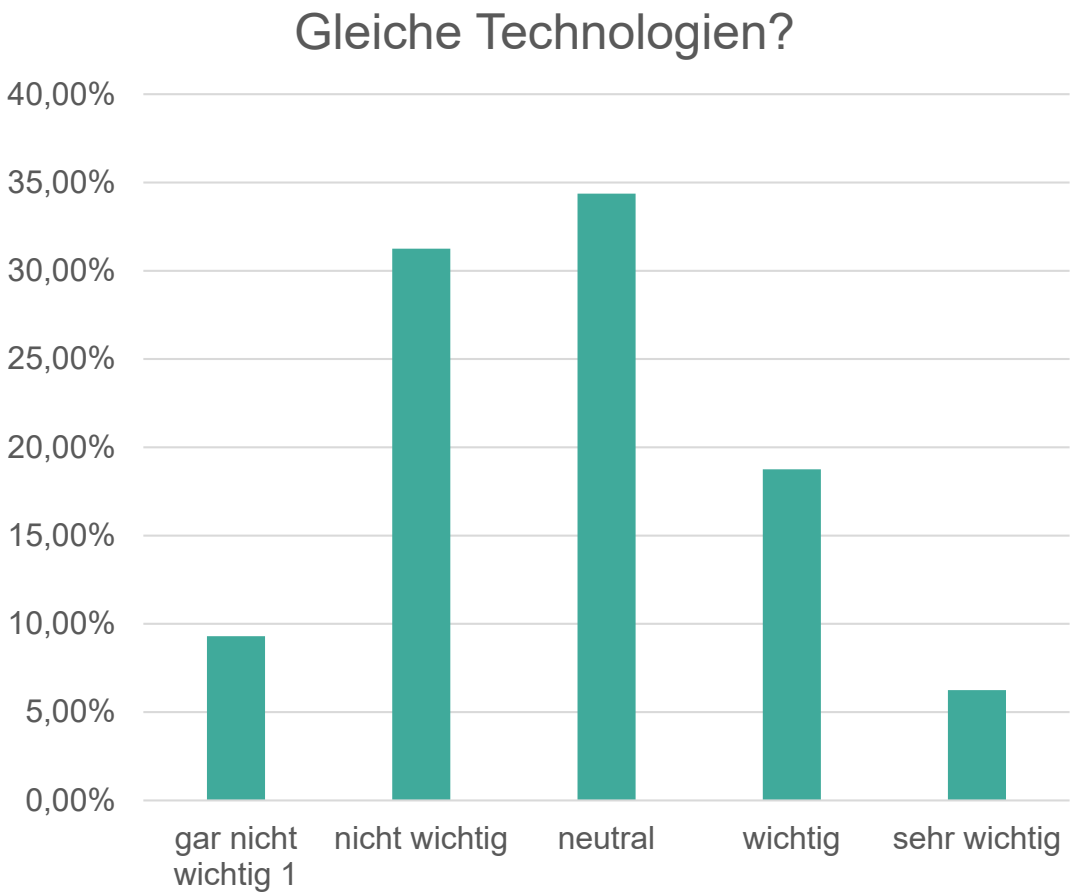


Was macht ein Szenario aus?

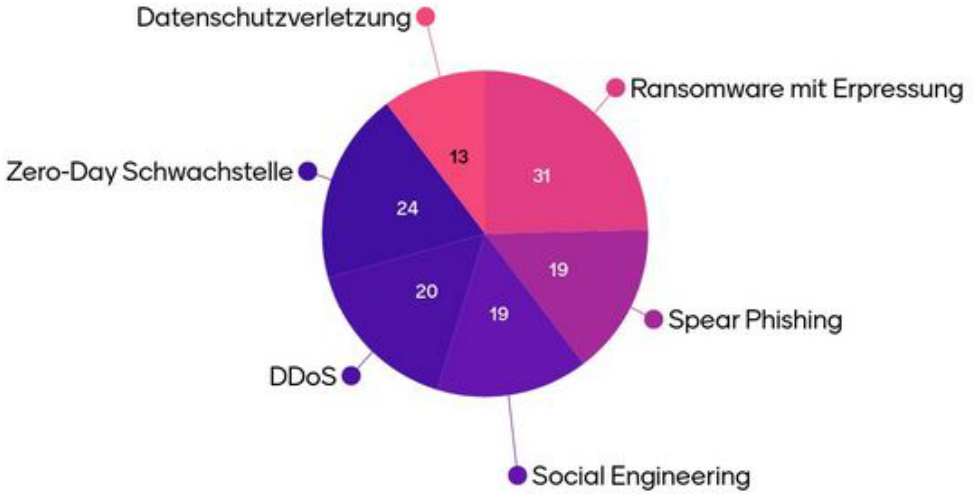


N=2000

UMFRAGE ERGEBNISSE



Interessante Themen für ein Szenario

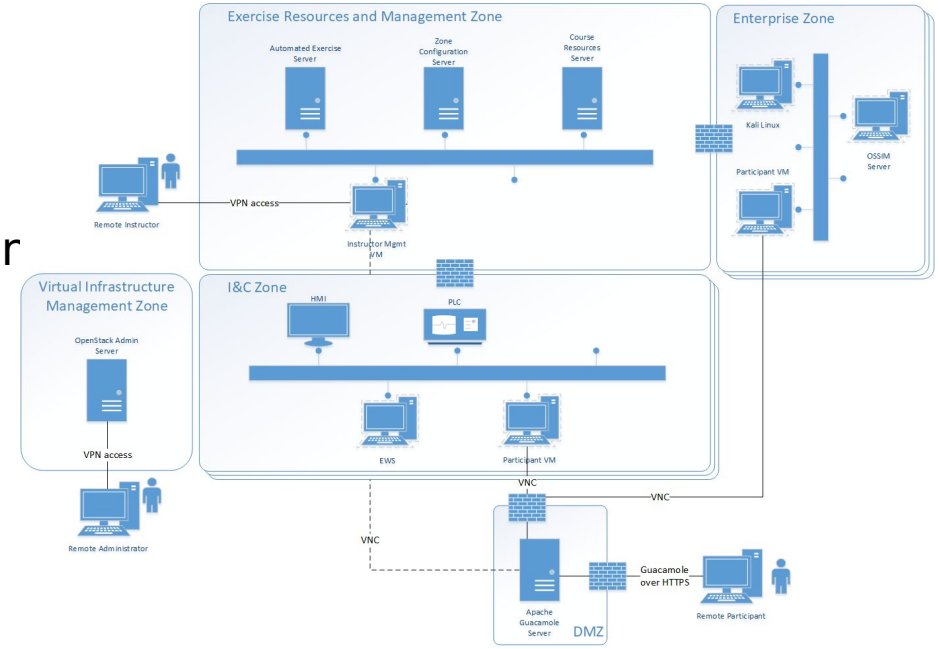


N=2000

CYBER RANGE

Virtuelle Umgebung um IKT Infrastrukturen zu simulieren

- ermöglicht die Simulation oder Emulation **großer und komplexer Netzwerke** mit unterschiedlichen (flexiblen) Systemkomponenten, Netzwerken und Benutzern
- eine sichere, realistische Umgebung zum Testen, Untersucher und Analysieren von Incidents in verschiedenen, skalierbaren Bedrohungsszenarien **ohne Verwendung der eigentlichen Produktionssysteme**
- für verschiedene **Anwendungsdomänen** (Informationstechnologie, Operational Technology, etc.)



TEILNEHMER:INNEN

- Managing **board**
- **Management / Führungskräfte**
- **Operatives Personal**
  (e.g., Admins, CERTs, CSIRTs)
- **Angestellte**

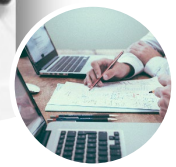
AIT CYBER RANGE

Modellierung und Simulation von vielfältigen Systemen

IT Netzwerke und Systeme

Industrial Control Systems (ICS)

Individuelle Bedrohungsszenarien



Forschung & Entwicklung

https://cyberrange.at

SZENARIO

Entscheidungen

- Krisenstäbe & -management

Prozesse

- Notfallpläne & Prozesse
- Kommunikationswege

Technik

- Infrastruktur (SW, HW, Netzwerke)
- Werkzeuge

ANGRIFFSSZENARIEN

Advanced Persistent Threat (APT)

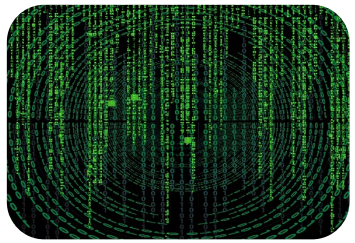
Ransomware

Trojaner / Remote Access Trojaner

Botnets

Data breach (DSGVO)

Phishing

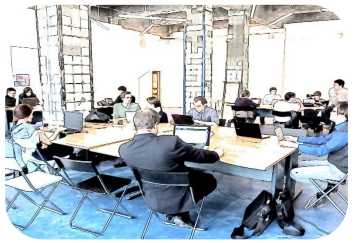


Vulnerability

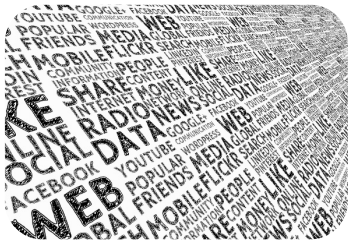
DDoS

Fehlkonfiguration

Nachrichten



Simulation von Akteuren (z.B. CERT, Trust Circle)



Und viele weitere

TECHNOLOGISCHER AUFBAU

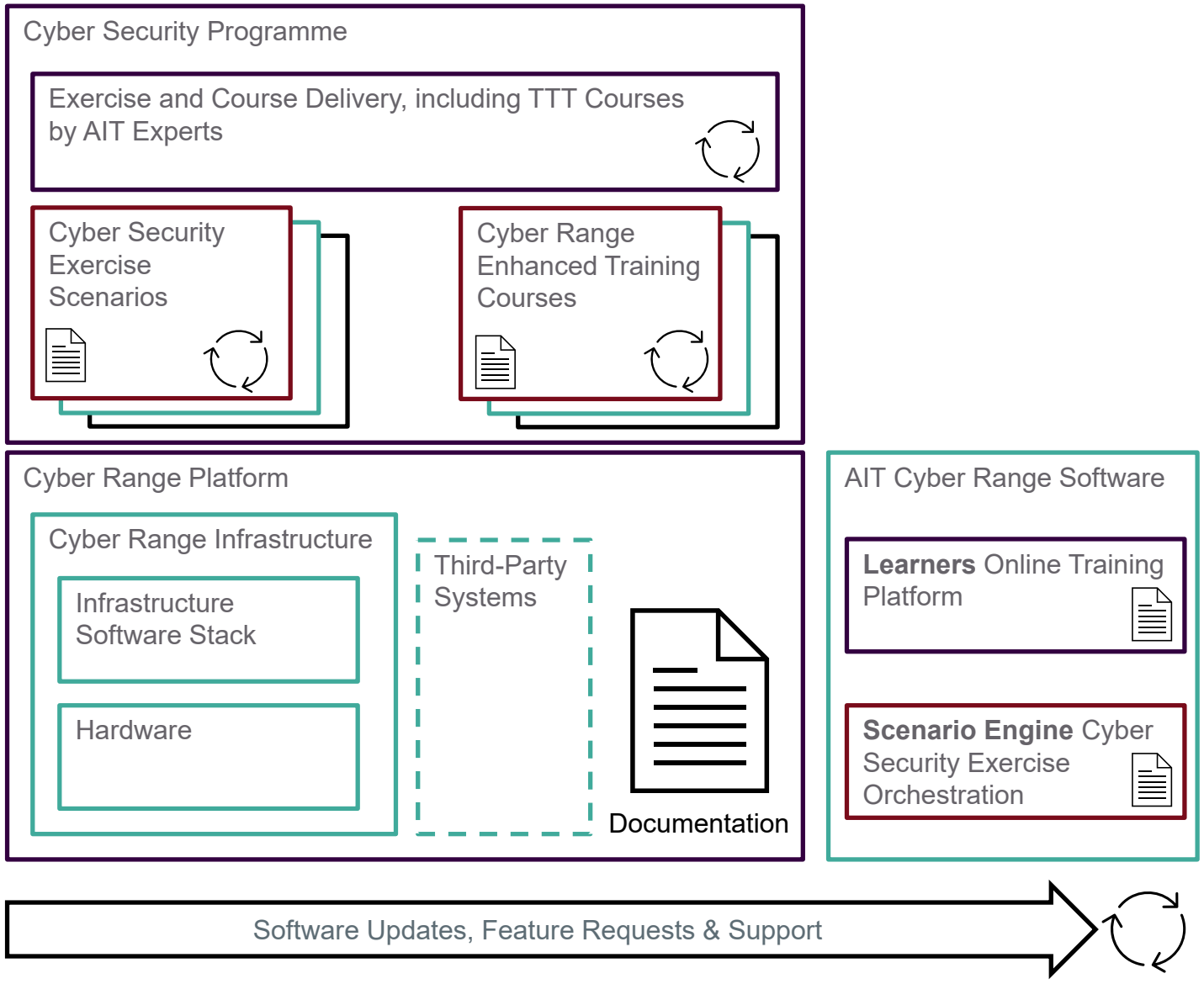
Building Blocks	Technologien
Scenario Engine	CyberRange
Software Provisioning	ANSIBLE, HashiCorp Packer
Infrastructure Provisioning	Terragrunt, HashiCorp Consul, HashiCorp Terraform
Computing Platform	KVM, openstack

CYBER RANGE OVERVIEW

AUSTRIAN INSTITUTE OF TECHNOLOGY

CYBER RANGE

AUSTRIAN INSTITUTE OF TECHNOLOGY



NATIONAL CYBER SECURITY EXERCISE 2021

Exercises

Die Übung verfolgte eine Reihe von Zielen

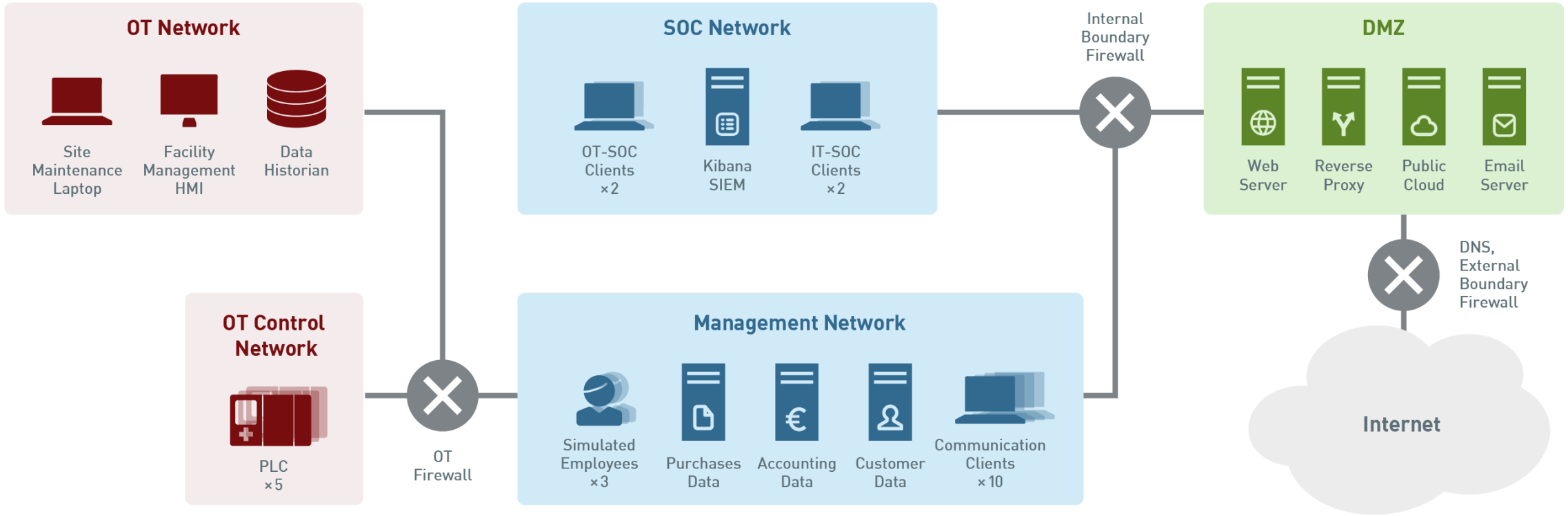
- Nationale Meldeverfahren für Cybersicherheit zu üben
- Einbindung nationaler Akteure, einschließlich kritischer Infrastrukturen, durch ein realistisches Cyberangriffsszenario
- Einbindung der Cybersicherheitsgemeinschaft in Österreich
- Sensibilisierung der Öffentlichkeit für Cybersicherheit

- Betreiber kritischer Infrastrukturen spielen als CSIRT-Teams und reagieren auf einen größeren Cybervorfall

- Nationale Stakeholder unterstützen die Teams, entwickeln ein nationales Cyber-Risiko-Bild und koordinieren die Reaktionsaktivitäten

EXERCISE NETWORK INFRASTRUCTURE

Exercises



EXERCISE ROLES AND INFRASTRUCTURE

Exercises

AIT Cyber Range Team

Provide technical and narrative injects with support from the Game Maker

Support teams during the exercise with technical questions

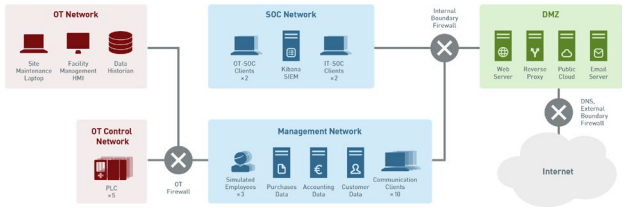
National CERT(s)

Support CSIRT teams, provide interface to authorities, distribute threat intelligence to stakeholders, information sharing hub

National Authorities

Develop national situation awareness and risk posture, coordination of state-level actors, handle reporting obligations

CSIRT Teams



Detect, analyse and contain technical threats, assess risk, communicate with stakeholders, fulfil reporting obligations, …

Observers & VIPs

VORTEILE

- Skalierbare und **individuelle Bedrohungsszenarien**
  - Z.B. Phishing, Data breach, Fehlkonfigurationen, DDoS, Advanced Persistent Threat, etc.
- Individuelle und **flexible Gestaltung der Infrastruktur**
  - Digitale Netzwerke und Systeme von kritischen Infrastrukturen
  - Digitale industrielle Steuerungsanlagen
  - Anwendungen in unterschiedlichsten Konfigurationen
- **Langjährige Erfahrung** im Bereich Cybersicherheit und Cyber-Übungen
- **Umfangreiches Wissen über nationale (unter internationale) Prozesse und Abläufe**

THANK YOU!

Gregor Langner
Research Engineer
Security & Communication Technologies
Center for Digital Safety & Security

AIT Austrian Institute of Technology GmbH
Giefinggasse, 1210 Wien, Austria
gregor.langner@ait.ac.at | www.ait.ac.at

https://cyberrange.at