Disclaimer

Vertraulichkeit und Veröffentlichung

- Dieses PDF wurde exklusiv für die Besucher der IoT/OT Security Conference in Cham, März 2024 erstellt und steht diesen zum Download zur Verfügung.
- Die öffentliche Verwendung oder Weitergabe dieses PDFs und aller darin enthaltenen Informationen darüber hinaus ist nicht gestattet.
- Der Inhalt wurde auf Aktualität und Richtigkeit zum Zeitpunkt der Veranstaltung geprüft. Für Gültigkeit darüber hinaus kann keine Aussage gemacht werden.
- Das Copyright obliegt der terreActive AG sowie der an dieser Präsentation beteiligten Unternehmen.

Eigentumsrechte und Bildquellen: terreActive AG, Splunk, Presentationload, IStock

OT Security

Einfache Massnahmen zur Risikoreduktion

Agenda 2024

Übersicht

01 Wer wir sind

02 Was bisher geschah

03 DIE Schwachstellen

04 Vorhandene Tools nutzen

05 SIEM ausbauen

06 Fazit

Über terreActive

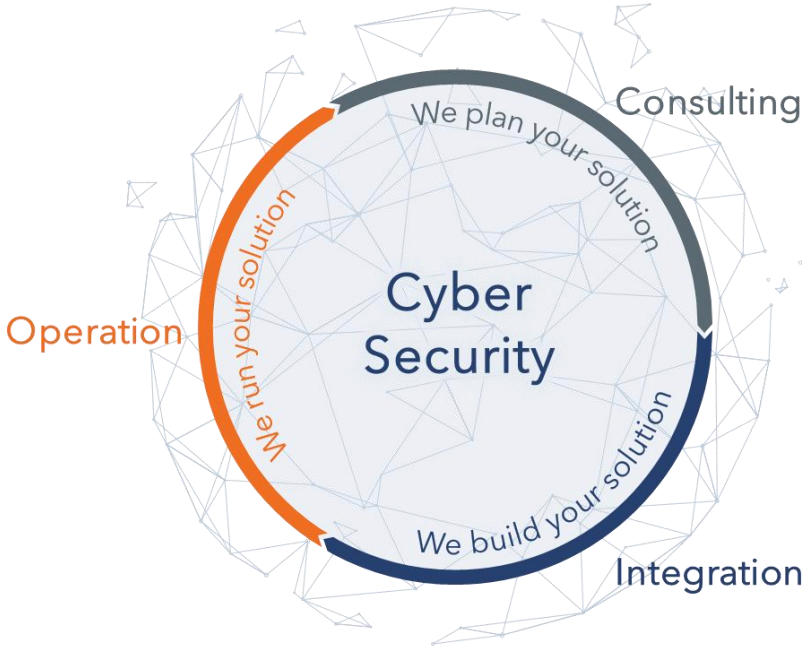
Security made in Switzerland

1996 gegründet – mehr als 25 Jahre Kompetenz in der Cyber Security

Schweizer Firma
Hauptsitz Aarau, alle Server in der Schweiz

90 Mitarbeitende (50 Ingenieure)

B2B-Kunden vom KMU bis Grosskonzern, Banken, Verwaltungen, Spitäler, Industrie. Mit branchenspezifischen Besonderheiten vertraut (FINMA).



terreActive ist Spezialist für die Überwachung und den Betrieb von IT-Sicherheitsinfrastrukturen.

Wir bieten den ganzen Zyklus an Cyber-Security-Dienstleistungen:

Von der Beratung über die Konzeption, die Integration bis zum Betrieb.

Cyber-Security-Spezialistin von

Der Auditor

Christian Fichera

- Teamleiter Audit, Risk & Compliance
- White Hat Hacker
- 8 Jahre Erfahrung in Cyber Security
- 15 Jahre Erfahrung in IT
- Focus: Penetrationstest und Ethical Hacking

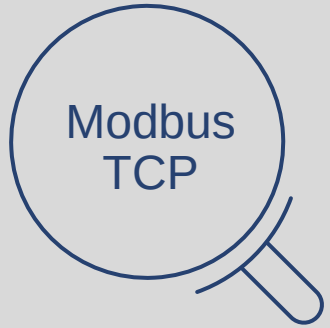
Der Pen-Tester

Raphael Ruf

- Cyber Security Consultant
- eigentlich Polymechaniker EFZ
- 15 Jahre Erfahrung in IT und OT
- Vulnerability Management und Breach & Attack Simulation
- Focus: Penetrationstest und Ethical Hacking

Was bisher geschah

Zuviel Zucker im Getränk



So einfach kommt der Hacker rein

Ein Beispiel aus der Praxis

Abfüllanlage

Angriff auf Abfüllanlage via ModbusTCP

Abfrage und Veränderung der Rezeptur

→ Keine Authentisierung

→ Verwendung von unverschlüsseltem Protokoll

Tages-Anzeiger

Aargauer Zeitung

14.02.2023

Weil zu viel Zucker krank macht:

Getränkehersteller verpflichten sich zur Zuckerreduktion

Die häufigste Schwachstellen

«einfach» Patchen

Die häufigste Schwachstellen

Nach über 30 OT Pentests in 2023

- «Unbekannte» Assets (Shadow IT)
- Kein Passwort oder default Passwort
- Veraltete Systeme (OS und App)
- Ungenügende Segmentierung
- Unverschlüsselte Protokolle

Low Hanging Fruits First

Massnahmen

• «Unbekannte» Assets (Shadow IT)	➢ Know your assets! (Inventory)
• Kein Passwort oder default Passwort	➢ Passwörter setzen
• Veraltete Systeme (OS und App)	➢ Patching
• Ungenügende Segementierung	➢ Netz-Segmentierung
• Unverschlüsselte Protokolle	➢ Upgrade auf sicheres Protokoll

Nicht immer einfach umzusetzen

→ Protection & Detection

Cyber Security
since 1996

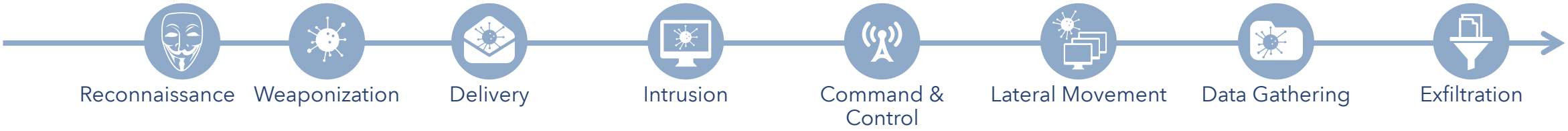
terreActive
terreActive
terreActive
terreActive

Einfache Massnahmen zur Risikoreduktion

Use Low Hanging Fruits

Cyber Defense Platform

Attack Phases (Cyber Kill Chain)



NIST	SOLUTIONS & TOOLS
Identify	Asset & Identity Inventory (CMDB)
	Threat Intelligence
Protect	FW, Gateways, Sandboxing, NIPS
	AV, HIPS, NAC
	NIPS
	DLP/DAM
	EPP/EDR
Detect	Vulnerability Management
	DLP/DAM
	Cyber Deception
	NDR, IDS
	NDR, IDS
	EPP/EDR
	SIEM
Respond	EPP/EDR, NAC
	SOAR
Recover	SOAR

Identify

Know your Assets

- «Was läuft auf diesem Gerät?»
  «Dieses Gerät kennen wir gar nicht!?»
- Was man nicht kennt, kann auch nicht geschützt werden
- Bestehende Prozesse für IT auch für OT anwenden
- OT-Geräte genau so inventarisieren wie IT
- Aktive oder passive Scanner

Protect

EDR Endpoint Detection Response

→ Angreifer stoppen bevor er in der OT landet

EDR in der OT

- Bestehende EDR-Lösung auf OT-Geräten deployen
- Kompatibilität mit Legacy OS
- Support für Legacy OS
- Speziell für OT (wenig Belastung auf dem System) z. B. TXOne Stellar

Detect

NDR & IDS / IPS & Defender OT Sensor

- Initial Compromise typischerweise in der IT
- Angreifer auf dem Weg von IT zur OT erkennen
- Reconnaissance
- Lateral Movement

Erkenntnis aus PoC:

Kunde hat bereits die nötige Funktionalität in der Firewall

Vulnerability Scanning

Tenable Vuln, Tenable OT, MS Defender for OT / IoT

- OT-Geräte können sehr sensitiv sein
- **Passives** Vulnerability Scanning mit Netzwerkverkehr
- **Klassisches** Vulnerability Scanning
- **Spezifisches** OT Vulnerability Scanning

  (z. B. Medigate, Tenable OT)

Cyber Security
since 1996

terreActive
terreActive
terreActive
terreActive

SIEM ausbauen

Integration ins SIEM

Beispielsweise mit Splunk

- Anreicherung des SIEM mit Logs aus der OT
- Anpassung und Tuning von bestehenden Use Cases auf OT

- **Typische Use Cases:**
  - Default Account Usage
  - Potential Port Scan Detected by Internal System
  - Network Intrusion Internal – Attack
  - Malware Infection on High Or Critical Priority Host
  - Malicious Operation Detected on Endpoint by EDR/EPP Solution
  - Incident Reported by Security System

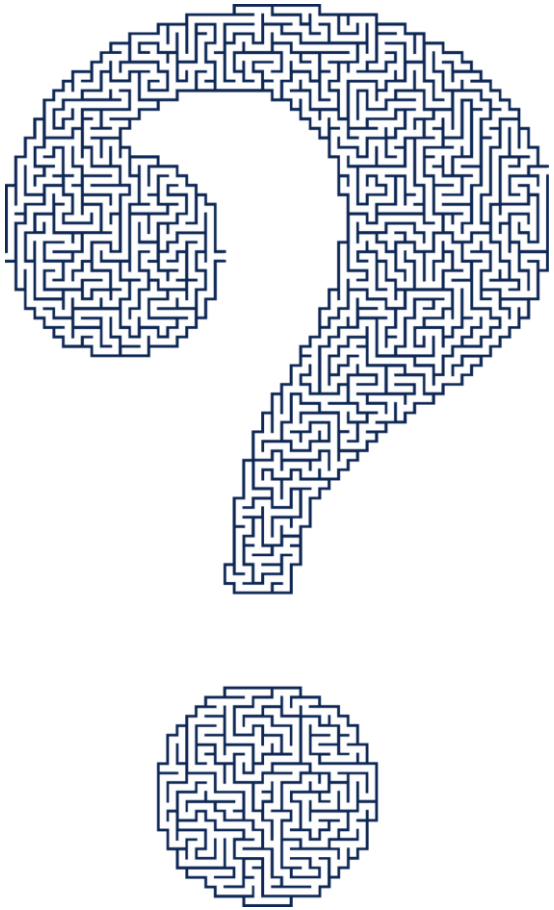
Fazit

Abwägen und entscheiden. Worauf Sie achten müssen.

- OT rückt näher an die IT → Synergien nutzen
- Themen sind verwandt, IT einbeziehen → Ressourcen effizient nutzen
- Nutzen Sie ein OT-Audit um Schwachstellen aufzudecken
- Ein Workshop zur *Cyber Defense Platform* hilft bei der Standortbestimmung

Schützen Sie sich!

Machen Sie Ihre Schwachstellen mit einem OT-Pentest sichtbar



Kontakt

Wir sichern Ihren Erfolg

Christian Fichera

Raphael Ruf

christian.fichera@terreActive.ch

raphael.ruf@terreActive.ch

terreActive AG
Kasinostrasse 30
CH-5001 Aarau

www.security.ch

+41 62 834 00 55
info@terreActive.ch