OT-Infrastrukturen – Wieviel Sicherheit ist genug?

Tec Forum Baden 2024, 12.03.24

Reto Amsler
ALSEC Cyber Security Consulting AG

AGENDA

- Was ist Operational Technologie
- Problemfelder der OT
- Bedrohungen im Überblick
- Können wir uns schützen?
- Wieviel Sicherheit ist genug?
- Zusammenfassung / Conclusion

About me

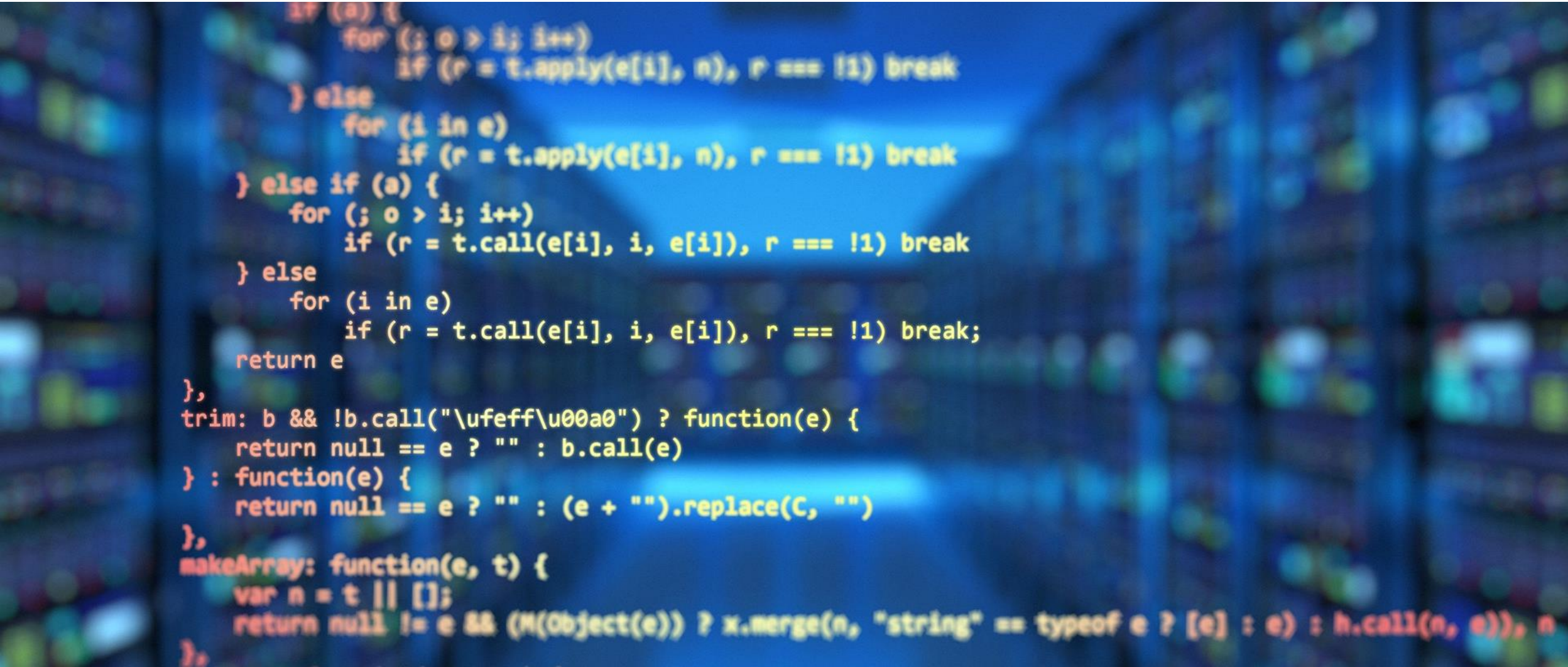
Reto Amsler Jetzt überprüfen

Protect Critical Infrastructure - not a job but a passion! ALSEC hat sich zur Mission gemacht die Resilienz "Kritischer Infrastrukturen" im Bereich Cyber Security zu erhöhen.

Was ist Operational Technology (OT)?

- Steuern, regeln und überwachen physische Prozesse
- Verteilte Systeme
- Hohe Anforderung an Verfügbarkeit
- Äusseren Einflüssen ausgesetzt
- Proprietäre Kommunikationsprotokolle

Problemfelder der OT



Purdue Model – Ist angezählt

Office Infrastructure (IT)

Critical Infrastructure (OT)

Purdue Model – Ist angezählt – Beispiel Strom

Kennen sie diesen Herrn?

Bernd Schäfer (74J)
Elektroingenieur (1972)

Sprecher + Schuh AG
Schweizer EVU

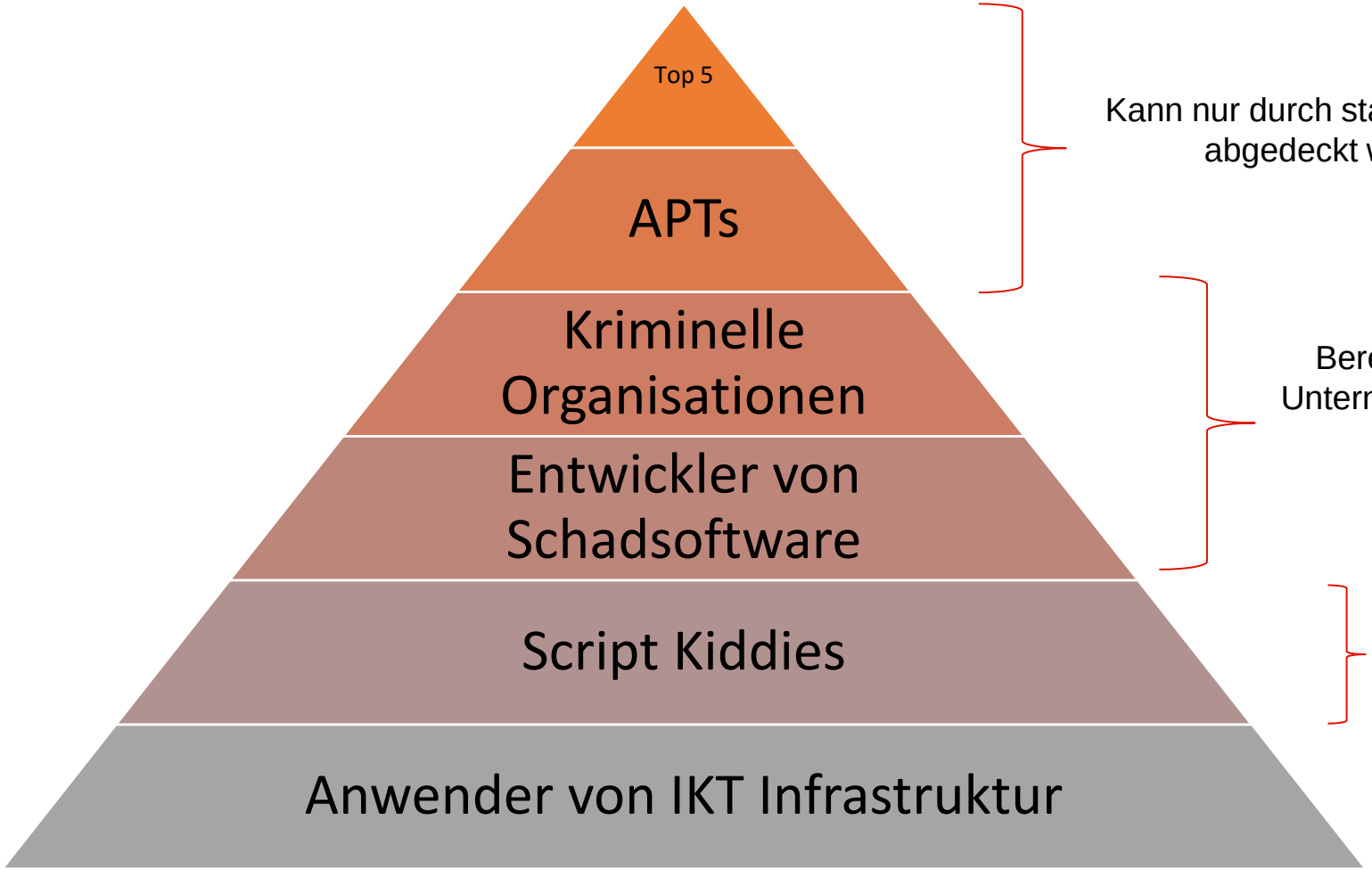
- Knowhow Träger der SCADA Applikationen
- 3th Level Supporter

IT ist anders…. OT auch:

IT	OT
Standard IP-Protokolle	Non-Standard Protokolle (Bus, Verkabelung etc.)
Aktuelles OS (Windows, Linux etc.)	Legacy / Embeded OS
Standardisierte Wartungsfenster für regelmässiges Patching/Upgrade	Ausserbetriebnahmen für Patching/Upgrade
Aktives Security Scanning	Passives Monitoring
Life Cycle 5 Jahre	Life Cycle 15 Jahre und mehr
Generelles IT-Wissen (Commodity)	Spezifisches Fachwissen
M2H (Mensch ist auch Sensor)	M2M (Maschine kommuniziert mit Maschine)

Bedrohungen im Überblick

Akteure im Cyberraum



Kann nur durch staatliche Stellen abgedeckt werden

Bereich, in welchem viele Unternehmen Verbesserungs-bedarf haben

Wird durch Unternehmen heute grossteils gut beherrscht

Top 10 Bedrohungen für ICS Infrastrukturen

Rang	2022	2019
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Top 10 Bedrohungen für ICS Infrastrukturen

Rang	2022	2019
1	Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	→
2	Infektion mit Schadsoftware über Internet und Intranet	↑
3	Menschliches Fehlverhalten und Sabotage	→
4	Kompromittierung von Extranet und Cloud-Komponenten	↗
5	Social Engineering und Phishing	→
6	(D)DoS Angriffe	→
7	Internet-verbundene Steuerungskomponenten	↗
8	Einbruch über Fernwartungszugänge	↗
9	Technisches Fehlverhalten und höhere Gewalt	→
10	Soft- und Hardwareschwachstellen in der Lieferkette	↑

https://www.allianz-fuer-cybersicherheit.de/

In Zahlen? – Schwierig zu nennen

- Indirekte Angriffe – eigentliches Ziel ist nicht erkennbar
- Angriffe werden nicht erkannt
- Tabu Thema

In Zahlen? – Schwierig zu nennen

Forescout ruft in seinem 2023 Global Threat Roundup Report nach verstärkten Massnahmen zum Schutz kritischer Infrastrukturen vor Cyberangreifern

13

13 Angriffe pro Sekunde gegen kritische Infrastrukturen

Können wir uns schützen?

Ja wir können! Aber…

- Wir müssen verstehen, was wir schützen müssen
- Wir müssen anerkennen, dass neue Technologien neue Anforderungen an den Schutz des Gesamtsystems stellen können (Industrie 4.0)
- Sicherheit ist Chefsache und nicht freiwillig!
- Sicherheit ist ein Prozess

- **100% Sicherheit gibt es nicht**

Wieviel Sicherheit ist genug?

Gesetzliche Anforderungen

- Energiesektor:
  - Strom Juli 2024: IKT-Minimalstandard in vorgegebener Maturität
  - Gas 2025: IKT-Minimalstandard in vorgegebener Maturität
- Branchenstandards
- IKT-Minimalstandards (kritische Teilsektoren)

- DSG / DSV, OR sowie sektorspezifische Regulatorien

Wie packe ich es an?

Sicherheitsbedürfnis festlegen

Sicherheitspolitik
Strategische Ausrichtung
Schutzlevel definiert
Verantwortlichkeiten geregelt
Stossrichtungen / Leitplanken definiert

Standortbestimmung

Ist-Analyse (Assessment) durchführen
Umfang: Prozesse; Technologie, Mensch
Anerkannter Standard

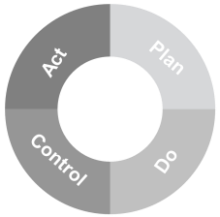
z.B.: IKT-Minimalstandard (BWL)

Sicherheitsstrategie

Gap-Analyse
Sicherheitsprogramm
Massnahmenplan

Sicherheits-Betrieb

Sicherheitsprojekte
(Abarbeiten Massnahmen)
Aufbau Sicherheitsorganisation



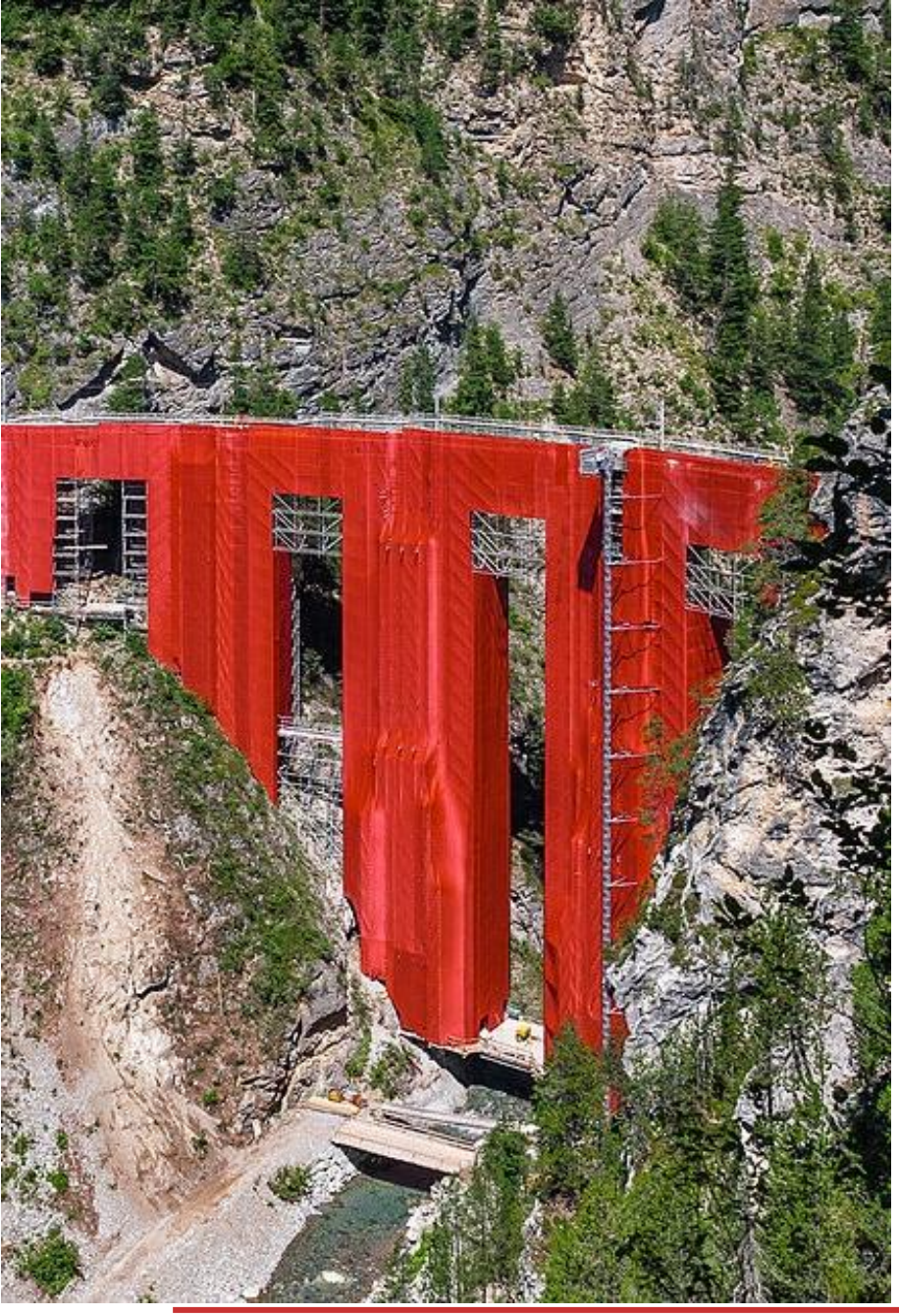
Monitoring & kontinuierliche Verbesserung

Zusammenfassung

Zusammenfassung

- OT regelt physikalische Prozesse und kann darum unser aller Wohlstand betreffen
- Der rasante technologische Wandel und neue Businessanforderungen beeinflussen die stabilen und trägen OT-Infrastrukturen stark
- Angriffe auf OT-Infrastrukturen sind real und nehmen zu
- Sicherheit ist Chefsache, ein Prozess und eine Frage der Unternehmenskultur
- Gesetzliche Anforderungen werden zunehmen, insbesondere auch durch die heutige geopolitische Lage

Nichts tun ist keine Option… packen wir’s an!!



ALSEC
CYBERSECURITY CONSULTING AG

„Building the Bridge“ zwischen IT und OT

Diskussion / Fragerunde

Ihre Expertin für die Gestaltung von Sicherheitsstandards für kritische Infrastrukturen.

«Unsere Cybersicherheits-Experten unterstützen Ihr Unternehmen mit fachmännischen und individuellen Services: Angefangen bei Schulungen, über die Erarbeitung von Prozessen sowie der Evaluation von Produkten bis hin zu deren Implementierung.»