txOne networks

The Leader of OT Zero Trust

How to **keep** your **operation running** with **OT Zero Trust**

Wie OT Zero Trust ihre Produktion schützen kann

IoT/OT Security Conference - Europe, Swiss, **Cham**

Pre-Sales Manager, DACH | Jasmin Steinhoff

Agenda

- Was ist der **Unterschied** zwischen **IT- und OT-Security?**
- Warum ist **IT-Security nicht für OT** Umgebungen **geeignet?**
- Warum ist **OT Zero Trust anders** als IT Zero Trust?
- Warum muss **OT-Security nicht kompliziert** sein?

txOne networks

Märchenstunde…

Maschinen in der Produktion sind „**air-gapped**“, **sicher gebaut** und sicher in der Nutzung!

…das klingt wie Science Fiction…

IT-OT Konvergenz mit **vernetzten Maschinen** in der ganzen Produktion, die in **hochgradig optimierten Prozessen** interagieren.

Industry4.0

… Realität sind Cyber Angriffe auf OT/IoT

Sehr lukrativ: **hohe „Gewinne, einfache Angriffe!**
Finanzielle Gewinne, Anerkennung und Erfolg, Insider-Bedrohungen, politisch motiviert, staatliche Akteure, Wirtschaftsspionage …

txOne networks

Was ist der **Unterschied** zwischen **IT- und OT-Security**?

Technisch

txOne networks

✓ Andere Protokolle

Organistorisch

✓ Verfügbarkeit
✓ Andere Normen
✓ Nachweisbarkeit

Betrieblich

✓ Verfügbarkeit
✓ Wartung
✓ Lebenszyklus

Unbekannter (Asset) Sicherheits-Status

Sicherheit & Gewährleistungen

Unbekannte Geräte & Verbindungen

flache Netzwerkinfrastrukturen

"air-gapped & isolierte Netzbereiche

Wartungen durch ext. Techniker

Einzel-Systeme

Alte Hardware, embedded Geräte

Geringe System Ressourcen

Fernzugriffe und Cloud-Verbindungen

OT spezifische Netzwerk Kommunikation (Protokolle)

Herausforderungen

- **Verfügbarkeit & Sicherheit (Mensch/Maschine) haben hohe Priorität in der OT**
- **Altsysteme (legacy) werden häufig eingesetzt**
- **Hochgradig verwundbare (vulnerable) Geräte/Maschinen**
- **Geringe Netzwerksicherheit in der Produktion**
- **Geringe Kenntnisse & Bewusstsein für Cyber-Sicherheit**

txOne networks

Warum ist **IT-Security nicht für OT** Umgebungen **geeignet?**

- **Verfügbarkeit & Sicherheit (Mensch/Maschine) haben hohe Priorität in der OT**
- **Altsysteme (legacy) werden häufig eingesetzt**
- **Hochgradig verwundbare (vulnerable) Geräte/Maschinen**
- **Geringe Netzwerksicherheit in der Produktion**
- **Geringe Kenntnisse & Bewusstsein für Cyber-Sicherheit**
- **Geringe Kenntnisse über Geräte & Risiken**

txOne networks

Warum ist **OT Zero Trust anders** als IT Zero Trust?

Keine wirksame Abgrenzung zwischen “Trusted” and “Untrusted”

IT Zero Trust schützt “USER und DATEN”

How do we authenticate the user based on informative context and grant the least privilege on App and Data?

OT Zero Trust schützt “Geräte/Maschinen”

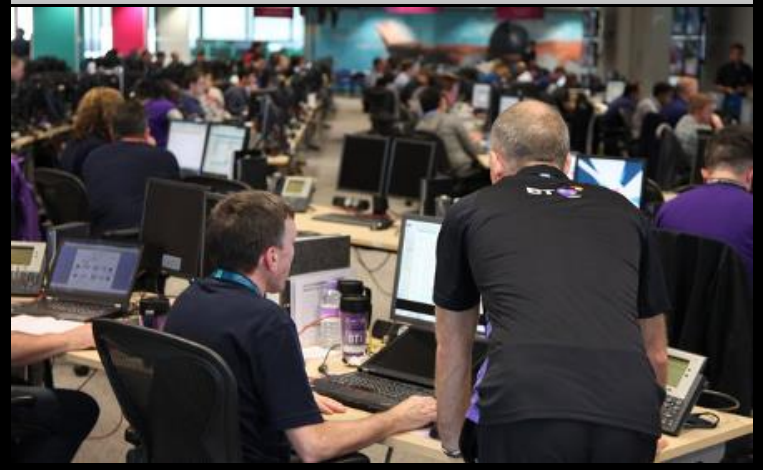
How do we verify the integrity when the asset arrives, preserve the critical processes, and grant the least privilege on network access?

txOne networks

Warum ist **OT Zero Trust anders** als IT Zero Trust?

Was ist mit SecOps?

IT SecOps



Phishing → Email opened → Word doc opened → PowerShell launched → Command & Control check-in

OT SecOps ???

File is copied → New process Launched On HMI → PLC Configuration Change

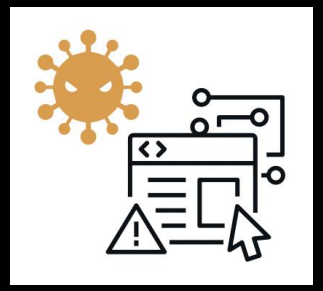
Blinder Fleck

Produktion

txOne networks

How to keep your operation running with OT Zero Trust

Wie OT Zero Trust ihre Produktion schützen kann



Inspect

Scan all inbound devices brought on site by personnel to stop insider threat, and scan assets before onboarding to prevent supply chain attacks.

Lock Down

Trustlists secure endpoint and networks alike by specifying what is allowed, blocking everything else.

Segment

Network segmentation groups vulnerable assets into operations friendly safe zones, preventing attackers from moving and malware from spreading.

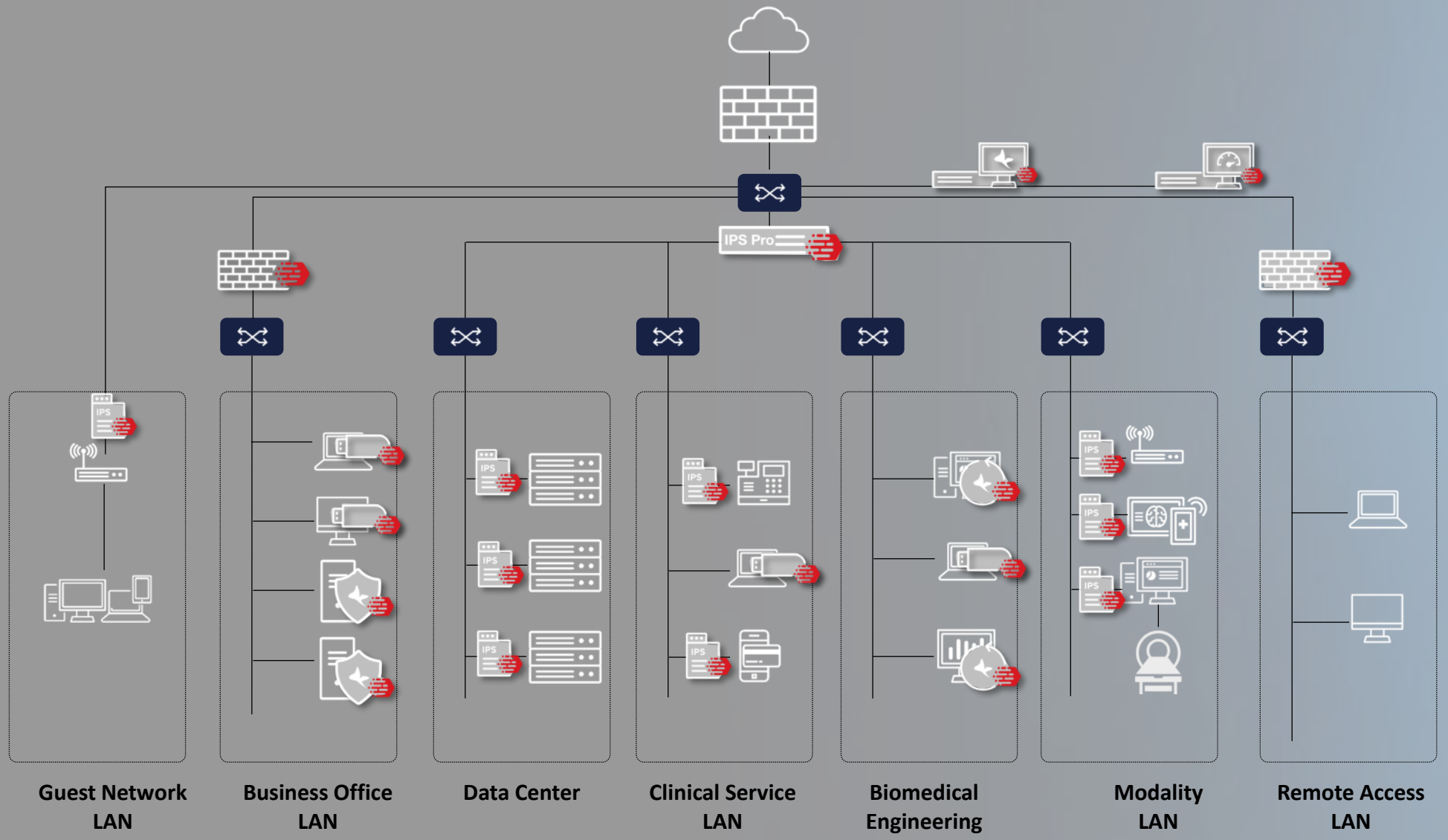
Reinforce

Shield assets at a network level to secure vulnerabilities in legacy and other unpatched assets without interrupting their work.

Complete Shopfloor Security

txOne networks

Solutions Deployment



Network Defense

- EdgeIPS Pro
- EdgeIPS
- EdgeFire
- ODC/ EdgeOne

Endpoint Protection

- StellarOne
- StellarProtect
- StellarProtect *Legacy Mode*

Security Inspection

- Portable Inspector

txOne networks

Warum muss **OT-Security nicht kompliziert** sein?

Herausfoderungen…

- Verfügbarkeit
- Altsysteme (legacy)
- Verwundbare Maschinen
- Netzwerksicherheit
- Geringe Kenntnisse über Geräte & Risiken

Zero Trust…

- Insider-Bedrohungen
- Angriffe auf die Lieferkette
- Systemhärtung
- Segmentierung
- Abschirmen von Verwundbarkeiten

… WIR MACHEN OT SECURITY EINFACH!

Automatisierter Ansatz:
LERNEN von Vorgängen, **AUFBAU** einer Basislinie und **DURCHSETZEN** von Regeln

Device Onboard

- Überwachung der Integrität
- Überwachung der Konfiguration
- Inventarisieren von Geräte-Informationen

Application Activation

- Schutz wichtiger Anwendungen & Dienste
- Schutz vor Malware und Vermeidung von Unterbrechungen
- Erlernen neuer OT Anwendungen & Dienste

Network Communi-cation

- Mikro-Segmentierunge
- Abschirmen von Geräteschwachstellen
- Schutz vor unerlaubten Netzwerkzugriffen
- Erlernen des “normalen” OT-Netzwerkverhalten

Herausforderung Endgerät

- Installation & Neustart nicht erlaubt
  -> einfaches Scannen zur Laufzeit!
- Keine Unterstützung für Altsysteme
  -> Win2K bis Windows 11 möglich
- Heterogene Systeme & Geräte
  -> Individuelle, automatische Regeln

Herausforderung Netzwerk

- Netzwerk Umstellung
  -> L2-Integration & L3+ Security
- Verbindungsunterbrechung
  -> Hardware-Bypass

Herausforderung akzeptiert!

txOne networks

IT/OT convergence & Industry needs

- **Tailored OT Security** Solutions

and txOne networks deliver

- **OT Zero Trust**
- **Legacy** systems **life-time protection**
- **Rapid & Easy deployment** capabilities
- High **Visibility & Protection** for **Assets & Vulnerabilities**
- **Individual, automated Asset Policies** for heterogal Infrastructures
- Helps to **identify Risks**

Keep Your Operations Running!

txOne networks