Von Null auf OT
Grundlagen, Gefahren, Schutzmöglichkeiten

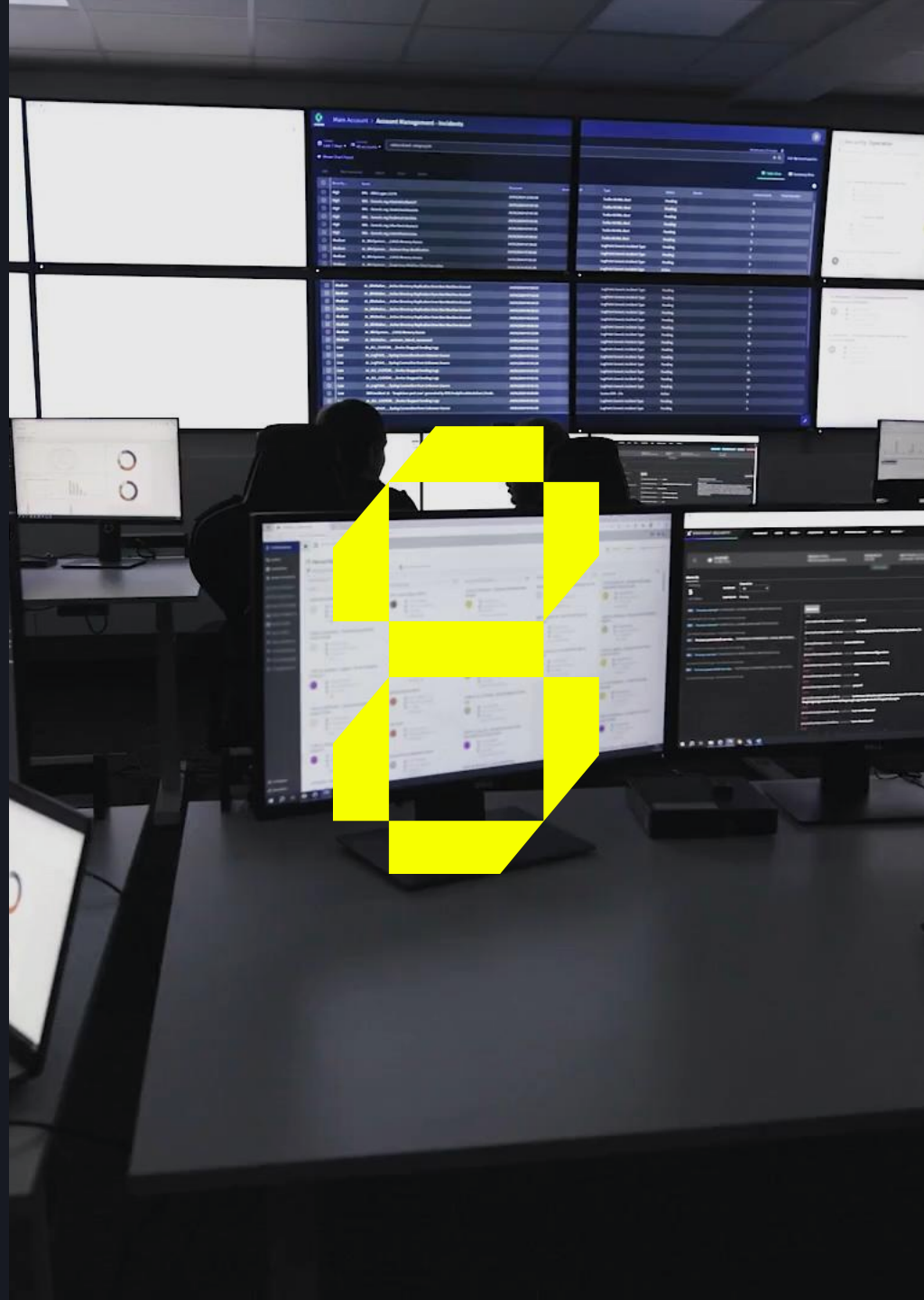
8COM
CYBER SECURITY

Keynote

Von Null auf OT
Grundlagen, Gefahren, Schutzmöglichkeiten

Richard Jaletzki
Teamlead OT Security

8COM
CYBER SECURITY



8COM

Grundlagen der OT

Unterschiede zwischen IT und OT

IT (Information Technology) „Computer bewegt Daten“	OT (Operational Technology) „Computer bewegt Dinge“
Datenverarbeitung und Kommunikation	Steuerung physischer Prozesse
E-Mail, Datenbanken, ERP, …	Industrieanlagen, Roboter, SCADA, HVAC, Zugangssteuerung, …
Updates und Patches regelmäßig möglich “Patch Tuesday”	Updates schwierig, planungsintensiv „Patch September“
Ausfälle sind i.d.R. nicht Geschäftskritisch	Ausfälle bedeuten Produktionsstopp, Umwelt- und Gesundheitsgefahren

Grundlagen der OT

Geräte

- Embedded Systems / Field Controllers:
  - PLC (Programmable Logic Controller)
    bzw. SPS (Speicherprogrammierbare Steuerung)
  - RTU (Remote Terminal Units)
  - HMI (Human Machine Interface)

- Netzwerk-Technik, Firewalls, Drucker, ...

Unterschiede zwischen IT und OT

Schutzbedarfe in der IT „Daten schützen“	Schutzbedarfe in der OT „Betrieb sichern“
	0. Sicherheit (Safety)
1. Vertraulichkeit	1. Verfügbarkeit
2. Integrität	2. Integrität
3. Verfügbarkeit	3. Vertraulichkeit

Patch Management & Technologie-Support

- Patches haben geringe Priorität
  - “Patch september” muss teilweise Jahre im Voraus geplant werden
- Technologie-Support bis zu 30 Jahre
- Cybersicherheit ist selten ein Thema
  - Beeinträchtigt Echtzeit-Anwendungen
  - War beim Bau der Anlage noch irrelevant

Patch Management & Technologie-Support

- diverse Bus-Systeme, Fokus für Security: Netzwerk (TCP/IP)
- Anforderung: Echtzeit, z.B. unter 7ms für einen Schaltbefehl
- viele proprietäre Implementierungen
- wenige bis keine Sicherheits-Features

DNP3

BACNet

Modbus

MQTT

EtherCAT

Siemens S7

Teamviewer

OPC, OPC/UA

DHCP
DNS
FTP
HTTP
IMAP
LDAP
NTP
RDP
SMB
SNMP
SSH
Syslog
Telnet
VNC

OT-Gebote und -Verbote

- Safety priorisieren
- eine Asset-Datenbank pflegen
- passive Netzwerk-Überwachung
- physische Begehungen durchführen

- keine pauschalen Netzwerk-Scans
- keine aktuelle Asset-Datenbank erwarten
- kein kooperatives Personal erwarten

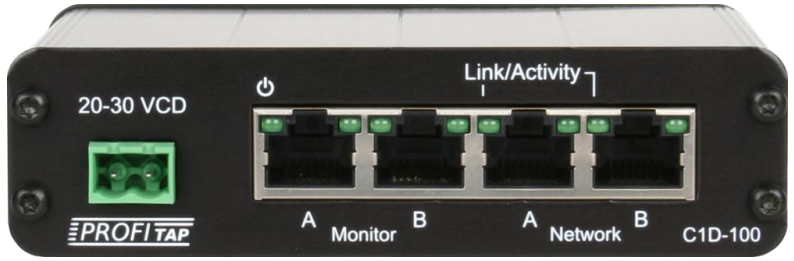
8COM

- OT-Security Monitoring

Netzwerk-Überwachung

- Überwachung des Datenverkehrs
- TAP-Device, SPAN- oder Mirror-Port
- Daten-Diode möglich – garantiert Rückwirkungsfrei

- Baselining für Anomalieerkennung
- Threat Intelligence für Angriffserkennung



Gefahren erkennen

- i.d.R. keine direkten Maßnahmen
- Abstimmung mit OT-Fachpersonal vor Ort
- gemeinsame Analyse: legitimes Verhalten, technische Fehlfunktion oder Cyberangriff?

Analyse

- Netzwerk-Verkehr verstehen:
  Welche Befehle wurden ausgeführt?
- Effekte verstehen:
  Wofür ist das betroffene Gerät verantwortlich?
- Ursache verstehen: Warum ist das passiert?

8COM
CYBER SECURITY

Fehlfunktion oder Cyberangriff?

Hauptfrage der OT-Security

Sie haben noch Fragen?

Sprechen Sie mich gerne an!

8COM
CYBER SECURITY

Richard Jaletzki
Teamlead OT Security

richard.jaletzki@8com.de
+49 6321 48 446 – 2095
+49 151 72457327

8com.de/newsletter