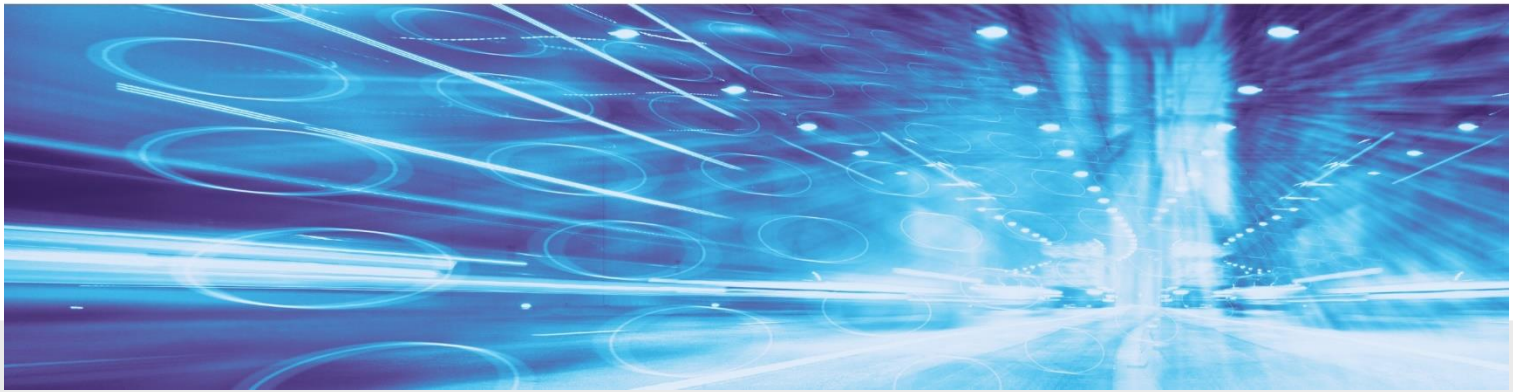
IT-/OT-Konvergente Netzwerke:

Zwei Welten mit dem gemeinsamen Ziel die OEE nicht zu gefährden …

Rolf Köpfli, VR
Hanspeter Weingartner, Geschäftsführer
Cham, 13. März 2024

DDS NETCOM



DDS NETCOM AG

Addresse: Allmendstrasse 8
CH-8320 Fehraltorf
+41 43 355 22 11
info@dds.ch

Gegründet: 1992

Mutterfirma USA: Seit 2023 eine 100%- Tochter der
Mc Naughton – Mc Kay Electric Corp. USA
www.mc-mc.com

Firmenverbund D: Service & Distribution GmbH, D-47809 Krefeld
www.sud-gmbh.de

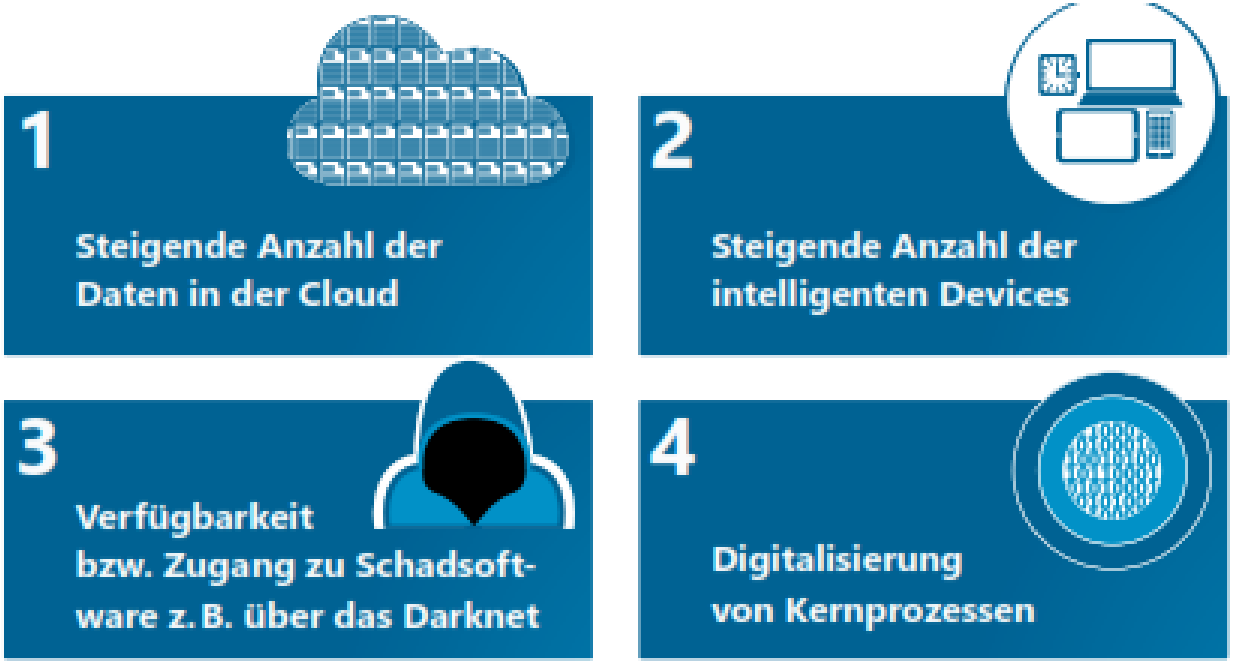
CINP Belden® Certified Industrial Network Provider
PDP Hirschmann™ Platinum Preferred Distribution Partner
PSP Hirschmann™ Platinum Preferred Solutions Partner

BELDEN 2020 Distributor Value Award Winner

Unser Mehrwert für Ihr Unternehmen

- **Netzwerk Infrastruktur**
  Netzwerk segmentieren | Zonen und Verbindungen festlegen | Unterstützung bei der Projektierung und Installation ¦ Geräte und Zugänge sichern | Netzwerk dokumentieren
- **Daten sammeln und verwalten**
  Daten sammeln (Syslog & Sensoren) | Log-Daten filtern & verwalten | Untersuchung, Analyse & Reporting
- **Schwachstellen analysieren**
  Sicherheitsschwachstellen bewerten | Best Practice- & Policy-Tests
- **Integrität sicherstellen**
  In Echtzeit Änderungen feststellen | Sicherheitslücken beheben | Reporting & Analysen zur Einhaltung der Vorschriften

Vier Gründe für einen nachhaltigen Sicherheitsansatz in OT-Netzwerken



Hauptgründe für das exponentielle Wachstum von IT / OT Sicherheitsvorfällen:

1. Die Cloud – Daten liegen längst nicht mehr geschützt und von der Außenwelt abgeschirmt im Rechenzentrum eines Unternehmens, sondern fließen zwischen dem Unternehmen, externen Partnern und Kunden und Mitarbeitern, die darauf von überall auf der Welt zugreifen.

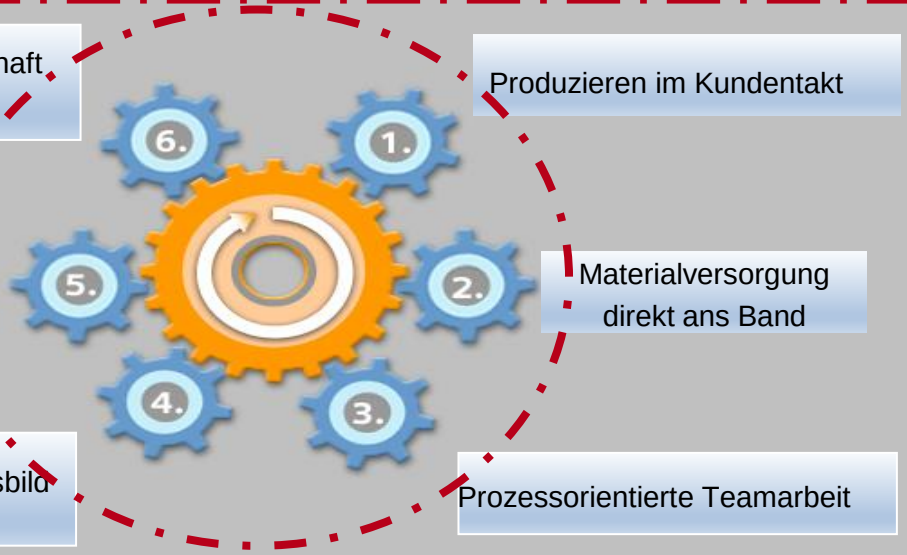
2. Mobile Geräte – Nicht nur Unternehmen des Internet-Zeitalters sind geradezu darauf angewiesen, jederzeit Zugriff auf relevante Daten zu gewähren. Mitarbeiter arbeiten außerhalb des Büros und greifen während Konferenzen oder von Cafés aus auf die Unternehmensdaten zu.

3. Darknet – Ähnlich wie Unternehmen, die ihre Dienste in die Cloud verlagern, agieren auch die Hacker, die ihre Dienstleistungen auf Untergrund-Marktplätzen anbieten.

4. Digitalisierung – Durch die Vernetzung von Maschinen, Sensoren und unterschiedlichen Geräten werden auch die Kernprozesse des Unternehmens digitalisiert.

Wieso brauchen wir stabile und sichere OT-Netzwerke?..

..weil die Leistungstreiber von guten Produktionssystemen alle miteinander vernetzt sind (sowohl IT, wie auch OT) und unsere OEE nachhaltig beeinflussen!



Warum nachhaltige Netzwerksicherheit?

- Gesetzliche Vorgaben D/CH
  - KRITIS Verordnung
  - IKT Leitlinien
  - NIS 2
- Voraussetzung für Geschäftsbeziehungen
- Vertrauensgewinn zwischen Geschäftspartnern
- **Absicherung der eigenen Vermögenswerte → OEE!**
- Sicherung von sensiblen Daten
- **Vermeidung von Stillständen in der Produktion → OEE!**
- Prävention vor Cyberangriffen
- Voraussetzung für bestehende und künftige Cyber Security Versicherungsabschlüsse

OEE (Overall Equipment Effectiveness)
Die Kennzahl wird berechnet aus der theoretischen Laufzeit einer Anlage abzüglich der Zeiten für technische Störungen, geplante Unterbrechungen, längere Bearbeitungszeiten sowie durch fehlerhafte Teile. Mit OEE bilden Sie die Leistungsfähigkeit einer Produktionsanlage komprimiert ab.

Prioritäten

Grundsätzliche Unterschiede IT und OT

Details

Grundsätzliche Unterschiede IT und OT

Art	Enterprise- Netzwerk	Industrie- Netzwerk
Installation	▪ Feste Grund-installation im Gebäude (UKV) ▪ Variabler Geräteanschluss an Standardarbeitsplätzen ▪ Überwiegend sternförmige Verkabelung	▪ Anlageabhängige Verkabelung und Kabelführung ▪ Feldkonfektionierbare Steckverbinder bis IP 67 ▪ Redundante Verkabelung, häufig Ringstrukturen
Daten	▪ Grosse Datenpakete ▪ Mittlere Netzverfügbarkeit (STP/RSTP) ▪ Hauptsächlich azyklische Datenübertragung ▪ Kein Echtzeitverhalten notwendig	▪ Kleine Datenpakete ▪ Sehr hohe Netzwerkverfügbarkeit (MRP) ▪ Hauptsächlich zyklische Datenübertragung ▪ Echtzeitverhalten z.T. notwendig
Umwelt	▪ Normaler Temperaturbereich ▪ Wenig Staub, Feuchtigkeit und Erschütterungen ▪ Kaum mechanische und chemische Belastungen ▪ Geringe EMV-Belastung	▪ Erweiterter Temperaturbereich ▪ Staub, Feuchtigkeit und Erschütterungen möglich ▪ Gefahr durch mechanische Beschädigung oder chemische Belastung ▪ Hohe EMV-Belastung

Vorgehensweise

Sicherheitskonzept

Netzwerk Infrastruktur

- Netzwerk segmentieren
- Zonen und Verbindungen festlegen
- Geräte und Zugänge sichern

Daten sammeln und verwalten

- Daten sammeln (Syslog & Sensoren)
- Log-Daten filtern & verwalten
- Untersuchung, Analyse & Reporting

Schwachstellen analysieren

- Sicherheitsschwach-stellen bewerten
- Best Practice & Policy-Tests

Integrität sicherstellen

- In Echtzeit Änderungen feststellen
- Sicherheitslücken beheben
- Reporting & Analysen zur Einhaltung der Vorschriften

Was immer wir im Zusammenhang mit CyberSecurity sowohl in der IT, wie auch in der OT tun, beeinflusst die Gesamteffizienz (OEE) unserer Unternehmung

Die OEE von Fertigungs- und Prozessanlagen hochzuhalten, ist eine technische und organisatorische Herausforderung.

Teams aus OT und IT müssen an einem Strang ziehen und ein Betriebskonzept realisieren, das die Bedürfnisse aller Seiten berücksichtigt.

Die Basis für das automatisierte Überwachen, Steuern und Optimieren von Industrieanlagen bilden sichere und stabile Netzwerke!

Die letzte Kontrollinstanz im Zusammenspiel von OT und IT bleibt jedoch der Mensch, der den Status des Risikofaktors nicht los wird!

Wir freuen uns auf die folgenden Gespräche mit Ihnen!