BELDEN
SENDING ALL THE RIGHT SIGNALS

HOPF
PARTNER | SOLUTIONS | COMPONENTS

Solution Guide

Fabrikautomatisierung: Leitfaden für Cybersicherheit

Dynamische Märkte prägen alle Bereiche der Fabrikautomatisierung

Wie können Hersteller wettbewerbsfähig und produktiv bleiben, ihre Kosten und Durchlaufzeiten reduzieren, die Erträge steigern und Marktanteile gewinnen? Durch die Digitalisierung. Digitalisierung bedeutet Vernetzung und Daten. Da immer mehr Geräte – von den E/As im Feld bis zu allen Ebenen der Lieferkette – mit Netzwerken verbunden sind, werden Inseln beseitigt, wodurch die Daten von jedem Gerät wertvolle Informationen liefern können. Diese digitale Revolution ist nichts anderes als Industrie 4.0 und sie ist nicht mehr nur eine Option – denn in der neuen, datenzentrierten, vernetzten Welt dreht sich alles um das wirtschaftliche Überleben.

Vernetzung stößt auf Bedenken

Vernetzung treibt die industrielle Automatisierung voran. Vernetzung treibt die Überwachung der Prozesse voran. Vernetzung treibt den Fernzugriff voran. Die Vernetzung verbindet die bisher durch den sogenannten Air Gap (Luftspalt) geschützten oder physisch isolierten Steuerungsnetzwerke aber auch mit der Cyberwelt. Dadurch können böswilliges, unbeabsichtigtes oder zufälliges menschliches Handeln – also alles, was aus der Ferne über ein Netzwerk möglich ist – negative Auswirkungen auf die Reputation von Unternehmen, die Sicherheit der Mitarbeiter, die Produktivität und die Qualität der Produkte haben.

Belden – Sending the Right Signals und zwar sicher

Belden ist ein strategischer Partner für Hersteller, der es Ihnen ermöglicht, Ihre Fertigungsprozesse auf Industrie 4.0 umzustellen und dann stetig zu optimieren. Die Lösungen von Belden ermöglichen eine durchgängige Vernetzung, von industriellen Kabeln über Steckverbinder und E/A Module bis hin zu Switches, Routern und industriellen Firewalls. Das sind die Komponenten für das Fundament von Industrie 4.0.

Schritt 1: **Transparenz**

Die Transparenz Ihrer Fertigungsprozesse ist der erste Schritt zur Cybersicherheit. Aber wie lässt sich etwas schützen, von dem Sie nicht wissen, dass es im Netzwerk vorhanden ist? **Tripwire Industrial Visibility** und **Tripwire Log Center** bieten diese Transparenz:

- Sie ermöglichen es Ihnen, alle Geräte in Ihrem Steuerungsnetzwerk zu erkennen und festzustellen, mit wem diese was kommunizieren und wann sich deren Konfigurationen ändern.
- Korrelieren Protokollereignisse aus mehreren Quellen und erstellen Regeln, um relevante Ereignisse zu markieren. Wenn beispielsweise eine fehlgeschlagene Anmeldung auf einem wichtigen Gerät fünfmal ausgeführt wird, sendet **Tripwire Log Center** eine automatische Benachrichtigung an den Netzwerkadministrator.

Schritt 2: **Schutzmaßnahmen**

Beginnen Sie mit zwei grundlegenden Maßnahmen: der Segmentierung des Netzwerks und dem Schutz der Geräte. **Industrielle Netzwerklösungen von Belden** und **Tripwire Enterprise** können beide eingesetzt werden, um wirkungsvolle Schutzmaßnahmen zu implementieren:

- Netzwerksegmentierung: **Eagle Firewalls von Hirschmann** und **Security Appliances von Tofino Security** ermöglichen eine zuverlässige Segmentierung des Netzwerks (Unterteilung in kleinere Teilbereiche oder Zonen), sodass Anwendungen oder Geräte voneinander getrennt werden können.
- Geräteschutz: Es muss gewährleistet sein, dass alle Geräte – HMIs (Human Machine Interface), Arbeitsstationen, Switches, Router etc. – gemäß den bewährten Vorgehensweisen (Best Practices) und Standards der Branche wie etwa IEC 62443 oder NIST SP 800-82 konfiguriert sind.

Schritt 3: **Kontinuierliche Überwachung**

Sobald die Grundlagen für Transparenz und Schutzmaßnahmen geschaffen worden sind, können Sie die Prozesse kontinuierlich überwachen, um sich ständig der Situation bewusst zu sein. Dadurch ist gewährleistet, dass Ihre Prozesse wie geplant laufen und unnötige oder ungeplante Stillstandzeiten vermieden werden. Systeme von **Tripwire** können durch eine kontinuierliche Überwachungslösung das Situationsbewusstsein stärken:

- Erkennen, wann der Modus von Steuerungen geändert wurde.
- Feststellen, ob ein neu installiertes E/A-Modul Schwachstellen hat.
- Überwachung von Arbeitsstationen, um sicherzustellen, dass deren Spezifikationen oder Standards für die Cybersicherheit korrekt konfiguriert sind.

Kundenreferenzen

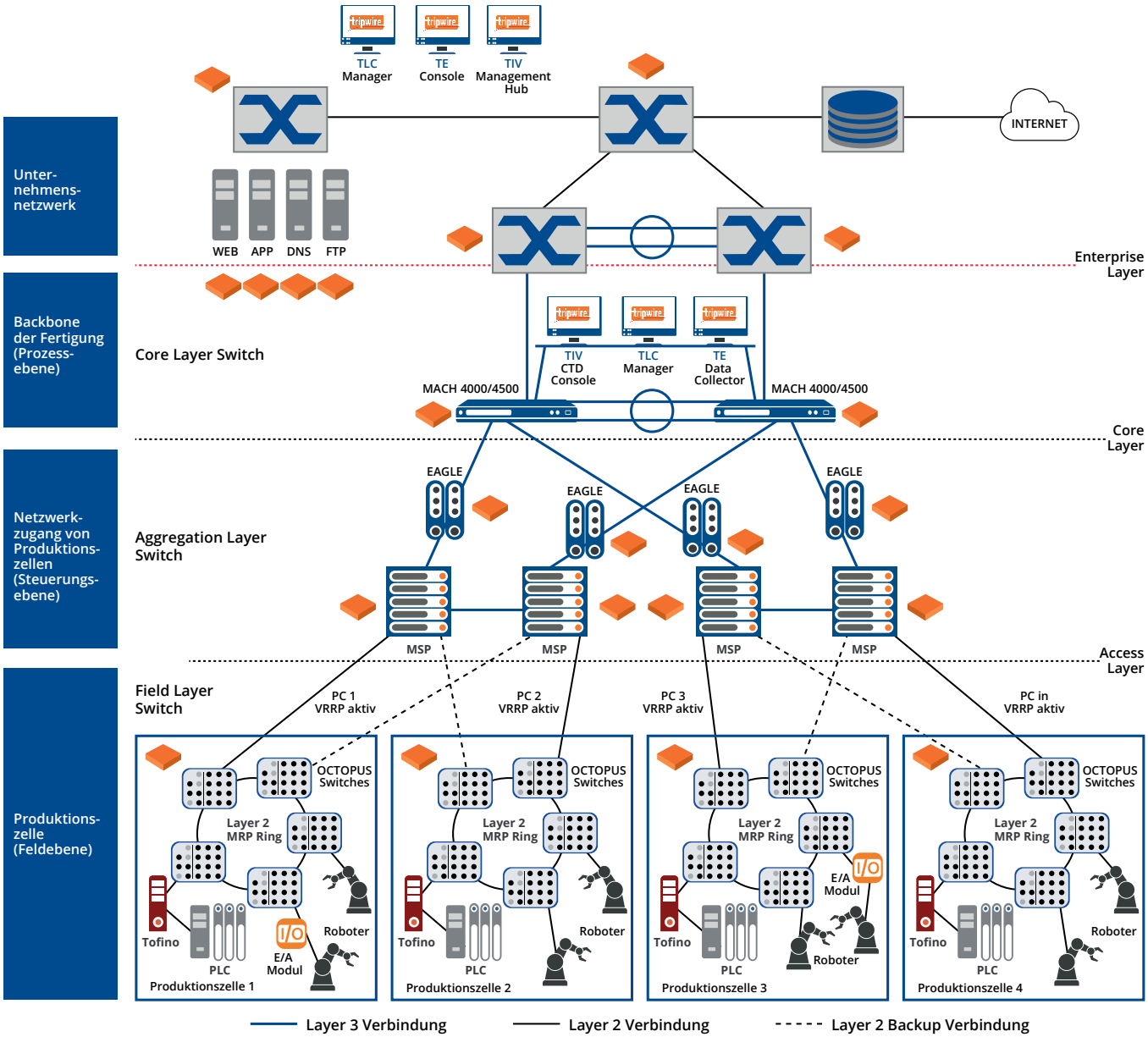
- **Internationaler Automobilhersteller:** Mit Lösungen von Belden können alle Geräte in deren jeweiligen Netzwerken durch eine Abfrage über ihr lokales Industrieprotokoll (Ethernet/IP) automatisch erkannt und Informationen zu Schwachstellen dieser Geräte bereitgestellt werden.
- **Hersteller von Nahrungsmitteln und Getränken:** Dank der hervorragenden Transparenz und Kohärenz der Protokollmanagementlösung von Tripwire konnte ein bevorstehender Kabelausfall rechtzeitig festgestellt werden: Der angeschlossene Switch sendete eine große Anzahl von CRC Fehlern an unser System, die von syslog erkannt wurden.
- **Hersteller von Konsumgütern:** Hunderte Arbeitsstunden eingespart bei der Bewertung der Gerätekonfiguration gemäß IEC 62443 durch Einsatz von Tripwire Lösungen, die diesen Prozess automatisiert haben.

BELDEN
SENDING ALL THE RIGHT SIGNALS

Beispiel einer Referenzarchitektur für Netzwerke in der Fabrikautomatisierung

In diesem Beispiel einer Referenzarchitektur können die Lösungen von Belden:

- Eine vollständige Bestandsaufnahme der Geräte und industriellen Kommunikationsprotokolle vornehmen
- Schwachstellen aller Geräte identifizieren
- Änderungen bei Steuerungen – Konfiguration, Modus und Firmware – erkennen
- Die Konfiguration von HMIs, SCADA Systemen, Arbeitsstationen und der Netzwerkinfrastruktur gemäß IEC 62443 bewerten
- Transparenz für alle Protokollinformationen von Steuerungen, SCADA Systemen, HMIs, Maschinenbetrieb und Netzwerkinfrastruktur herstellen
- Das Produktions- und das IT-Netzwerk eines Unternehmens segmentieren, die Kommunikation zwischen Zonen/Zellen ermöglichen und Regeln für die Kommunikation aller industriellen Protokolle mit Steuerungen durchsetzen



TLC = Tripwire Log Center | TE = Tripwire Enterprise | TIV = Tripwire Industrial Visibility
Industrielle Transparenz, Schutzmaßnahmen sowie Überwachung durch aktive und passive Lösungen: Tripwire Enterprise, Tripwire Log Center und Tripwire Industrial Visibility

Rufen Sie Ihren Vertriebsmitarbeiter von Belden oder Tripwire an, um einen Termin zu vereinbaren oder besuchen Sie unsere Webseite unter www.beldensolutions.com und www.tripwire.com

Belden US 1-855-400-9071 ■ Tripwire US 1-503-276-7500
Belden EMEA +49 (0) 7127 14 1809 ■ Tripwire EMEA +44 (0) 16 2877 5850

Belden, Belden Sending All The Right Signals, GarrettCom, Hirschmann, Lumberg Automation, Tofino Security, Tripwire und das Belden-Logo sind Handelsmarken oder eingetragene Handelsmarken der Belden Inc. oder verbundener Unternehmen in den USA und anderen Regionen der Welt. Sonstige hierin verwendete Marken und Bezeichnungen können das Eigentum von Belden und anderer Unternehmen sein.

©Copyright 2019, Belden Inc.

CYBER-SECURITY-DISCRETE-SELLING-GUIDE_SF_INET_BDC_0419_DEU