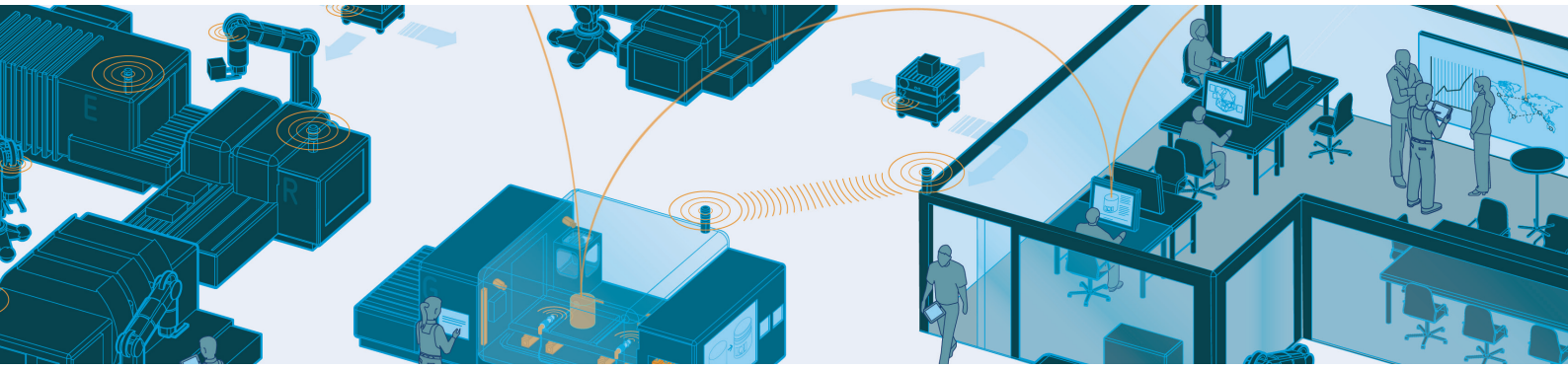
ZVEI:
Die Elektroindustrie

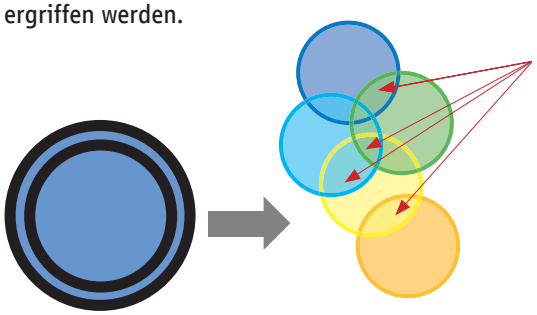


Industrie 4.0:
Industrial Security 4.0 als gemeinschaftliche Aufgabe

Bisherige Security-Konzepte für die Industrie zielen vorrangig auf die technische Absicherung der eigenen Unternehmensnetzwerke ab. Viele Vorteile von Industrie 4.0 erfordern allerdings mehr als einzelne, isolierte Maßnahmen. Übergreifende Sicherheitsarchitekturen sind notwendig.

Industrial Security – Der aktuelle Stand

In der Industrie stehen die Unternehmens- und Produktionsanlagen im Fokus. Nach dem Mantelprinzip richtet sich die Security an Zugriffs- und Produktschutz, Netzwerksicherheit und Werksschutz als Ganzes aus. Konzeptionell bildet das eigene Unternehmen als kontrollierbarer Verantwortungsbereich die Basis. Das Grundprinzip ist ein relativ freier, sicherer und kontrollierter Innenraum, bei dem alle Übergänge nach außen beispielsweise über Firewalls abzusichern sind. Hat ein Angreifer die Barrieren aber einmal überwunden, führt ein nur nach außen gerichtetes Sicherheitskonzept zu einem unkalkulierbaren Risiko, falls keine zusätzlichen Schutzmaßnahmen ergriffen werden.



Heute:
Sicherheit durch Isolation des Unternehmens

Zukunft:
Wertschöpfungsnetzwerke verbinden verschiedene Unternehmen

Quelle: ZVEI

Grundsätzliche Problematik

Unternehmen kommunizieren bereits heute automatisiert durch wenige Schnittstellen, z. B. bei Bestellprozessen. Um die Vorteile von Industrie 4.0 zu nutzen, müssen künftig Menschen, Maschinen, Feldgeräte usw. breiter (über mehrere Systeme) und tiefer (bis hin zu einzelnen Maschinenteilen einer Produktionsanlage) direkt miteinander kommunizieren. Die zahlreichen Kommunikationspunkte im Wertschöpfungsnetzwerk lassen sich aufgrund der Komplexität auf herkömmliche Art nicht mehr verwalten. Daher benötigt jede Instanz eine eigene Absicherung. Gefordert sind Sicherheitskonzepte, die auch nach einer dynamischen Änderung, z. B. der Umkonfiguration einer Produktionsanlage, weiterhin wirksam bleiben.

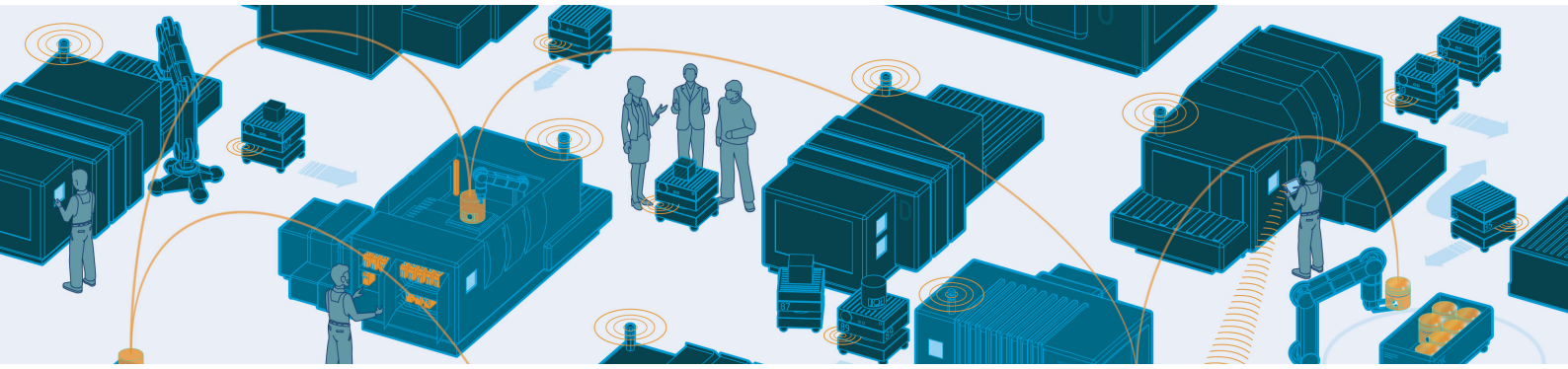
Hersteller, Integratoren und Betreiber müssen ein gemeinschaftliches Vorgehen definieren, um unternehmensübergreifende Wertschöpfungsnetzwerke, in denen verschiedene Unternehmen mit ggf. unterschiedlichen Sicherheitsniveaus kooperieren, zu definieren und zu etablieren.

Kontakt:
Gunther Koschnick
Geschäftsführer
Fachverband Automation
Telefon: +49 69 6302-318
E-Mail: koschnick@zvei.org

Stand: April 2016

Autor:
ZVEI-Führungskreis Industrie 4.0, Spiegelgremium Sicherheit

ZVEI:
Die Elektroindustrie



• Sicherheitsketten als Ziel

Wichtig ist eine durchgängige Security im gesamten Produkt- und Anlagenzyklus, d. h. von der Entwicklung und Herstellung eines Produkts über Entwurf, Auslieferung, Betrieb und Wartung der Anlagen bis zu ihrer Außerbetriebnahme. Hierbei stellen vertrauenswürdige Hardware-Plattformen, wie Feldgeräte und Maschinen, die Basis für sichere Softwareprogramme dar, das wiederum als Voraussetzung für sichere Dienste und Prozesse dient. Security-Prozesse müssen daher bei allen Beteiligten etabliert und miteinander verzahnt werden und in der Lage sein, sich fortwährend der aktuellen Bedrohungslage anpassen.

• Ein wichtiger Schritt: Sichere Identitäten

Die Industrie benötigt ein System, das Kommunikation und ein geeignetes Identitätsmanagement über unterschiedliche, frei wählbare Plattformen und Provider ermöglicht. Jede Anlage und jede Komponente tragen selbst Sicherheitseigenschaften und benötigte Schutzmaßnahmen. Komponenten verhandeln in einem Wertschöpfungsnetzwerk untereinander angemessene Sicherheitsniveaus, je nach der Schutzwürdigkeit der Daten und Dienste.

Für diesen Austausch ist Vertrauen die Grundlage. Sichere und eindeutige Identitäten sind hier ein erster von mehreren Schritten. Identitäten für alle Elemente des Wertschöpfungsnetzwerks müssen sich unternehmensübergreifend gegenüber einer Plattform authentifizieren lassen und die jeweiligen Plattformen eine Vertrauensbeziehung untereinander haben. Die Verwaltung der Identitäten stellt jedoch zukünftig eine Herausforderung dar, erst recht, wenn die Prozesse automatisiert in Echtzeit erfolgen. Aktuell sind diese Identitäten und Plattformen jedoch nicht flächendeckend vorhanden.

Beherrschbare Restrisiken

Sicherheit kann sich nicht auf technisch-vorbeugende Maßnahmen beschränken. Gefordert ist vor allem der Mensch, der die Security adaptiv und kontinuierlich umsetzen muss. Zusätzlich müssen daher zuverlässige Fähigkeiten bzgl. der Präventions-, Detektions- und Reaktionsfähigkeiten im Unternehmen gestärkt werden. Mittels dieser drei Fähigkeiten lassen sich Risiken frühzeitig und gezielt bewerten und aufwandsgerechte Maßnahmen festlegen. Das bewusste und kontrollierte Eingehen von Restrisiken ist dann – ähnlich wie bei der Maschinensicherheit (Safety) – ein normaler und beherrschbarer Vorgang.

Was gilt es für Unternehmen zu tun?

- Kontakt zu den Integratoren und Endkunden suchen, um spezifische Sicherheitsanforderungen zu identifizieren.
- Definition eines gemeinschaftlichen, unternehmensübergreifenden Security-Vorgehens mit den Wertschöpfungspartnern.
- Anpassung des Vorgehens an die aktuelle Bedrohungslage.
- Informationen über sichere Identitäten z. B. über die Plattform Industrie 4.0 einholen.
- Feststellen, für welche Prozesse ein unternehmensübergreifendes, eindeutiges Identitäten- und Rechtemanagement für Menschen und Maschinen besteht oder künftig relevant wird.
- Prozesse zur frühzeitigen Risikobewertung im Unternehmen etablieren.

Weitere Informationen rund um Industrie 4.0 in der Elektroindustrie liefern

· ZVEI-Positionspapier „Industrie 4.0: Auf dem Weg zur smarten Fabrik – die Elektroindustrie geht voran“
· Faktenblatt Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0)
· Faktenblatt Industrie 4.0-Komponente

online auf www.zvei.org.

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Lyoner Straße 9 • 60528 Frankfurt am Main • Telefon: +49 69 6302-0 • Fax:+49 69 6302-317 • E-Mail: zvei@zvei.org • www.zvei.org