Brownfield sicher vernetzen

Sicherheitsstrategien für die IT/OT-Konvergenz in der Prozessindustrie

Steffen Ullrich,
Genua

Die wenigsten industriellen Digitalisierungsprojekte werden auf der grünen Wiese geplant. Häufig gilt es, Bestandsanlagen (Brownfield) in der Fertigungs- und Prozessindustrie zu erweitern. Die gute Nachricht ist: Mit einem ganzheitlichen Ansatz können solche Umgebungen effizient gegen Risiken wie Cyberangriffe geschützt werden. Eine gute IT-OT-Security-Strategie legt außerdem den Grundstein, um Security Incidents frühzeitig zu identifizieren und hilft, die Verfügbarkeit und Effizienz von Anlagen zu steigern.

Wenn im Zuge von industriellen Digitalisierungsprojekten klassische Datenverarbeitung (IT) und Produktionsumgebung (OT) vernetzt werden sollen, liegt die Herausforderung für die Safety und Security darin, die unterschiedlichen Rahmenbedingungen und Zielsetzungen der beiden Domänen in einem gemeinsamen Sicherheitskonzept zu erfüllen. Insbesondere durch die Öffnung eines internen OT-Netzwerks für z.B. Fernwartungszugänge oder durch für Predictive Maintenance genutzte, nachträglich aufgesetzte Datenschnittstellen entstehen potenzielle Einfallstore für Angreifer.

Ansätze für die IT/OT-Sicherheitsstrategie

Mit einer ganzheitlichen, mehrstufigen Sicherheitsstrategie lässt sich aber auch in Brownfield-Anlagen hohe Sicherheit mit überschaubarem Aufwand realisieren. Um eine nachhaltig wirksame Sicherheitsstrategie aufzubauen, lassen sich folgende Ansätze aus der IT-Sicherheit heranziehen:

- Zones & Conduits und Defense in Depth
- Intelligente Netzwerküberwachung
- Zero Trust Networking Access
- Hochsichere Fernwartungsarchitekturen
- Hochsichere Datenausleitung

Zones & Conduits und Defense in Depth

Um einen Angreifer an der Fortbewegung in einem internen Netzwerk zu hindern, ist die statische Netzsegmentierung (Zones) ein klassisches und bewährtes Konzept. Solche Segmentierungen können physikalisch, logisch (Software, Protokoll) oder gemischt erfolgen. Mit entsprechenden „Wächtern“ an den wenigen Übergängen (Conduits) lassen sich die einzelnen Zonen entsprechend den jeweiligen Anforderungen gezielt absichern. Hierfür können unterschiedliche Methoden wie Filter oder Firewalls zum Einsatz kommen. Die Kombination mehrerer Sicherheits-

Abb.1: IT/OT-Referenzarchitektur für eine sichere digitalisierte Brownfield-Anlage. Implementierte Anwendungsszenarien sind hier u.a. die sichere Fernwartung, die Prozessoptimierung auf Basis von Edge Computing sowie die hochsichere Datenausleitung mittels Datendiode.

techniken in einer Defense-in-Depth-Strategie bietet eine robuste mehrstufige Verteidigung. So können z.B. an den Zonengrenzen verschiedene Arten von Firewalls zum Einsatz kommen (Applikation, Inhalte, Adressen) und innerhalb einer sicher abgeschirmten Zone auch problemlos unsichere alte, aber echtzeitfähige Feldbusse genutzt werden. In einem Brownfield-Szenario lassen sich auf diese Weise komplette Altsysteme als Ganzes sicherheitstechnisch kapseln bzw. nach außen isolieren.

Intelligente Überwachung in einem OT-Netz

In der IT sind das Monitoring und Überprüfen des Netzwerkverkehrs auf verdächtige Veränderungen (Anomalie-Erkennung) probate Mittel, um die interne Netzwerksicherheit zu erhöhen. Insbesondere bei der Absicherung von gewachsenen OT-Netzen empfiehlt sich dabei ein schrittweises, toolgestütztes Vorgehen. Der erste Schritt ist eine automatisierte Bestandsaufnahme (Asset Detection), welche Geräte im Netzwerk vorhanden sind. Es folgt eine Traffic-Analyse, wer im Normalfall mit wem wie viel kommuniziert. Mittels Machine-Learning-Algorithmen können moderne Tools nach einer kurzen Anlernzeit selbstständig zwischen Standardereignissen, spontanen, aber legitimen Ereignissen und Bedrohungen unterscheiden und den Datenverkehr in Echtzeit klassifizieren, Anomalien und potenzielle Brüche melden und automatisiert auf das jeweilige Ereignis reagieren. Das heißt in der Praxis, dass jeglicher Kommunikation definierte Regeln zugeordnet werden können. In einer Stabilisierungsphase werden das System bzw. dessen Policies praxisgerecht nachjustiert (Finetuning). In einem optional letzten Schritt legt der Nutzer fest, ob das System bei aktiv erkannten Bedrohungen oder bereits bei unbekannter Kommunikation nur Warnungen bzw. Alarme ausgibt oder den Datenverkehr tatsächlich unterbrechen darf. Wird dieses aktive Blocking des Datenverkehrs tatsächlich erlaubt, ist vorher OT-seitig zu gewährleisten,

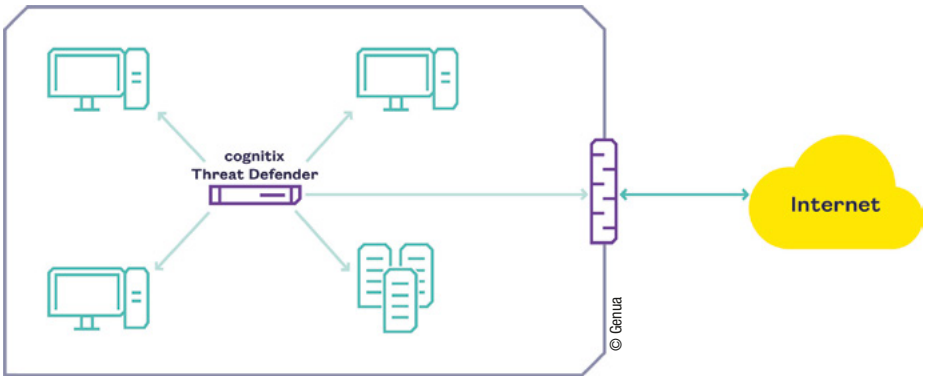

Abb. 2: Mikrosegmentierung nach Forrester. Einzelne Dienste oder Geräte werden voneinander abgetrennt und die Kommunikation zwischen ihnen reguliert und überwacht.

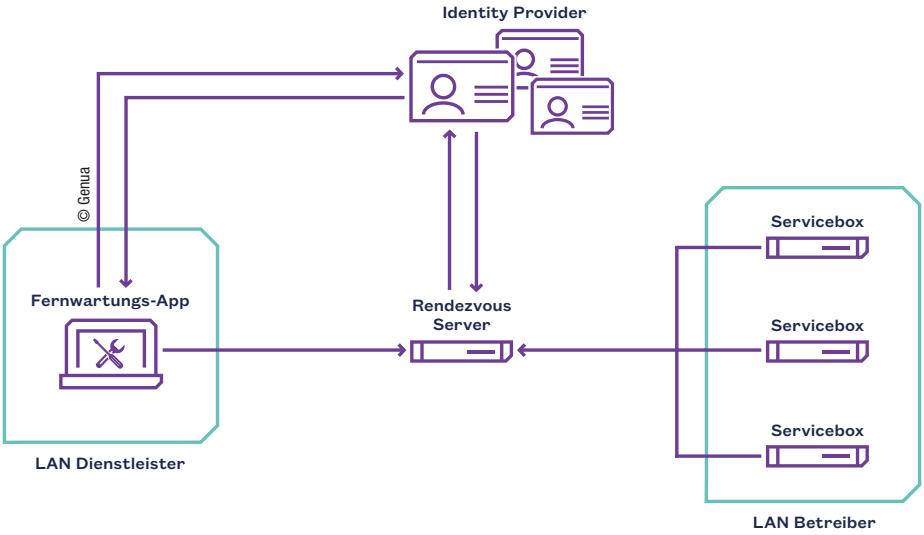

Abb. 3: Implementierung eines Software-Defined-Perimenters am Beispiel der Fernwartungslösung Genubox. Diese erlaubt die Anbindung an Identitäts- und Zugriffsmanagementsysteme.

dass dadurch die Betriebssicherheit der Produktionsanlagen (Safety) zu keinem Zeitpunkt gefährdet ist.

Zero-Trust-Architekturen für die Industrie

Der traditionelle Ansatz für das Management digitaler Infrastrukturen bestand bis dato in zentral verwalteten Netzen mit einem einheitlich hohen Sicherheitsniveau. Seit dem Aufkommen von Industrie 4.0 werden jedoch mehr und mehr Systeme durch externe Hersteller und Dienstleister fremd gemanagt bzw. haben Verbindungen zu fremd verwalteten Netzen, etwa für Cloud Computing. Für die Industrie bedeutet dies einen zunehmenden Kontrollverlust. Die in der IT seit Längerem etablierten Zero-Trust-Architekturen helfen Betreibern, die Netzwerkhoheit über ihre OT zu behalten. Im Paradigma des Zero-Trust-Networking wird das Vertrauen in die Sicherheit des Gesamtnetzes durch das Vertrauen in die Sicherheit spezifischer Kommunikationsendpunkte ersetzt, d.h. in Geräte, Dienste und Anwendungen. Eine Kompromittierung einzelner Endpunkte ist damit auf die erlaubten Kommunikationsbeziehungen beschränkt und gefährdet nicht mehr das Gesamtnetz.

Dieses Vorgehen senkt proaktiv die Angriffsfläche, erlaubt reaktiv auch eine schnellere Detektion und Begrenzung von Schäden sowie eine rasche und gezielte Recovery. Das Resultat sind robustere und resiliente Netze, passend zur höheren Kritikalität und den damit einhergehenden Anforderungen an Zuverlässigkeit und Kontrolle. Es gibt mehrere Ansätze, Zero-Trust-Networking zu implementieren. Beim Zero-Trust-Networking nach Forrester (Abb. 2) wird ein Netz in sich selbst durch den Einsatz von Firewalls an strategischen Stellen in Mikrosegmente unterteilt, zwischen denen die Kommunikation reguliert wird. Im Extremfall befindet sich jedes Gerät in einem eigenen Mikrosegment. Dieser Ansatz eignet sich besonders für eine nachträgliche Härtung bestehender Netze und arbeitet gut mit Legacy-Anwendungen zusammen. Es wird jedoch ein eventuell dynamisches Mapping zwischen Identitäten und IP-Adressen benötigt, da nur diese zuverlässig als Entscheidungskriterium im Datenverkehr sichtbar sind.

Alle Zero-Trust-Ansätze unterscheiden sich primär durch den Ort der Durchsetzung in der Netzwerkinfrastruktur und die damit einhergehenden Möglichkeiten bzw. Limitierungen. Ihnen ist gemein, dass die Entscheidungen basierend auf den Identitäten von Geräten, Anwendungen, Nutzern bzw. Diensten erfolgen, die nicht notwendigerweise an eine spezifische physische Ausprägung gekoppelt sind. Typische Identitäten sind in diesem Umfeld z.B. kryptografische Zertifikate oder Nutzer-Accounts. In eher statischen, kontrollierten Netzen können aber auch klar zugeordnete physische Merkmale wie die MAC- oder IP-Adresse als Identitäten in den Entscheidungen genutzt werden.

Hochsichere Fernwartung mittels Software-Defined Perimeter

Das Zero-Trust-Networking-Konzept der Cloud Security Alliance (CSA) wiederum ist ein Software-Defined-Perimeter (SDP), der externen Clients nach einer Authentisierung Zugriff in eine interne Infrastruktur erlaubt. Im Gegensatz zu einem klassischen Virtual Private Network findet hier jedoch keine komplette Netzkopplung statt, sondern der Zugriff ist auf einzelne Dienste beschränkt. Eine an das Konzept des Software-Defined-Perimeters angelehnte Lösung Implementierung einer Fernwartungslösung ist auf Abb. 3 zu sehen. Dabei übernimmt ein Rendezvous-Server die Rolle des Software-Defined-Perimeters und erlaubt authentisierten externen Anwendern den Zugriff nur auf spezifische Dienste. Hierhin verbindet sich das Zielsystem von innen. Der Fernwarter wiederum baut ebenfalls eine verschlüsselte Kommunikation zu diesem Perimeter auf. Nach erfolgreicher Authentisierung wird ein Zugriff ausschließlich auf spezifisch benötigte Dienste ermöglicht, wie z.B. auf den Desktop der zu wartenden Maschine, das Terminal oder auf ausgewählte Ports. Das geschieht nach dem Principle-of-Least-Privilege: Nur das gewünschte Protokoll der Software bestimmt also die Verbindung. Alle anderen Anwendungen oder gar beide Netze werden nicht gekoppelt. Eine Schnittstelle zu Identitäts- und Zugriffsmanagementsystemen ermöglicht die flexible Anbindung der Fernwartung an eine zentrale Benutzer- und Rechteverwaltung.

Hochsichere Datenausleitung

Anwendungen mit höchster Schutzklasse stellen Industrieanlagen im Bereich kritischer Infrastruktur (KRITIS) dar. Hierzu gehören bspw. viele teils jahrzehntealte IACS-Systeme in der Energie- und Wasserversorgung sowie in Kernkraftwerken. Diese basieren oft noch auf veralteten Betriebssystemen, die schon seit vielen Jahren nicht mehr aktualisiert und gepatcht werden können. Da deren Schwachstellen aber schon sehr lange öffentlich bekannt sind, stellt ein externer Zugriff auf diese Systeme ein vollkommen unkalkulierbares, nicht vertretbares Risiko dar. Trotzdem wird auch hier für eine effiziente Überwachung und Steuerung oftmals ein (Fern-)Zugriff auf die Daten des laufenden Betriebs benötigt. Abhilfe schaffen sichere Datendioden. Sie stellen eine besonders sichere und performante Lösung dar, bei der Daten nur in eine Richtung fließen können. Dabei sind die jeweiligen Netzwerke auch physikalisch völlig entkoppelt, was quasi eine unüberwindbare, absolut sichere Einbahnstraße in Richtung Außenwelt darstellt.

Der Autor

Steffen Ullrich, Technology Fellow, Genua GmbH

Diesen Beitrag können Sie auch in der Wiley Online Library als pdf lesen und abspeichern:

https://dx.doi.org/10.1002/citp.202201115

Kontakt

genua GmbH, Kirchheim bei München
Tel.: +49 89 991950 - 0
info@genua.de · www.genua.de/digitale-industrie