Security für Produktionsanlagen

Industrial Security im Spannungsfeld zwischen Anlagenbauer und Betreiber

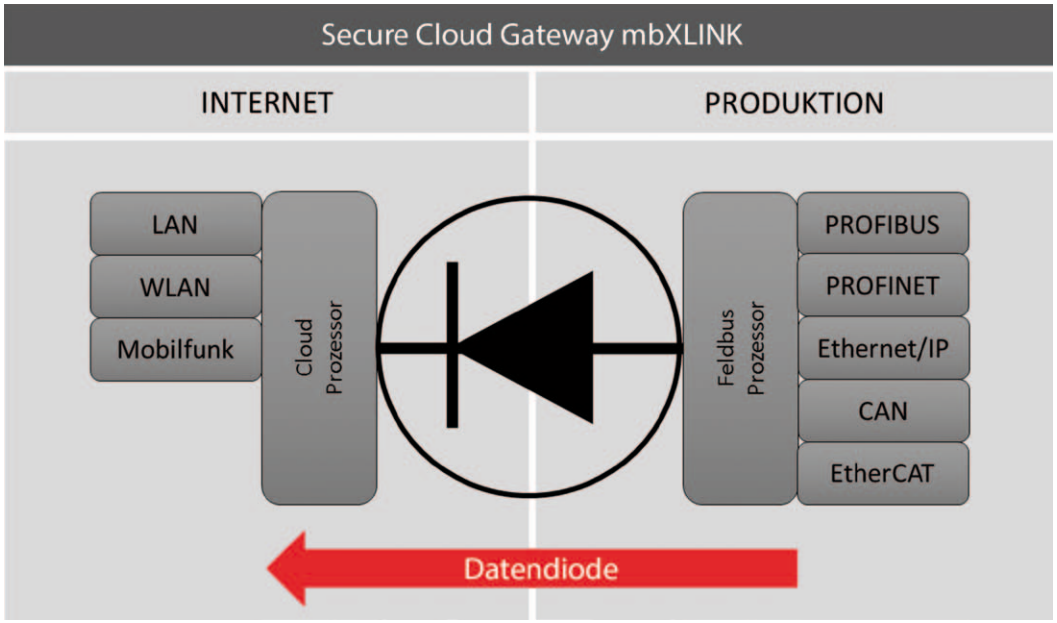
Security war lange Zeit nur ein Problem der klassischen IT. Spätestens seit Stuxnet ist klar, dass auch Produktionsanlagen und Automatisierungssysteme gefährdet sind. Allerdings sind die klassischen Security-Konzepte nicht mit der Automatisierungswelt kompatibel.

Die zunehmende Digitalisierung, auch im Hinblick auf Industrie 4.0, sorgt dafür, dass die Informations- und die Automatisierungstechnik immer mehr verschmelzen. Regelmäßige Meldungen über versuchte Denial-of-Service-Angriffe (DoS), gestohlene Kreditkartendaten oder manipulierte Finanztransaktionen treiben daher berechtigte Sorgenfalten auf die Stirn der Verantwortlichen.

Das Remote-Service-Portal für VMware läuft auf dem Server des Anwenders (Bilder: MB connect line GmbH)

Autor:

Siegfried Müller, Geschäftsführer der MB Connect Line



Das Secure Cloud Gateway verhindert das Eindringen von außen dank hardwaremäßiger Trennung

Nutzen steht im Vordergrund

Aus Sicht der Automatisierungstechnik sind die Vorteile und der Nutzen von Fernwartung und Zustandsüberwachung über Internet unbestritten. Unabhängig davon, ob es sich um eine Anlagenstörung, um eine Umrüstung oder schlicht um eine Frage zur Bedienung handelt, das Service-Personal des Maschinenbauers kann per Fernzugriff innerhalb von Minuten unterstützen. Was im Störungsfall eine tolle Sache ist, kann im Falle eines Missbrauchs zu großen Problemen führen. Verschafft sich jemand in böser Absicht Zugang zu technischen Anlagen, egal ob Produktionsanlagen, Gebäudetechnik oder Infrastruktur, können Schäden in bedeutender Höhe entstehen, beispielsweise durch die Ausspähung von Rezeptur- und Produktionsdaten oder durch eine Manipulation der Anlage, die zur Zerstörung führt – etwa durch Übertemperatur oder mechanische Überlastung.

Unterschiedliche Anforderungen

Die Themen Zugriffsschutz und Security fallen in der Regel in die Zuständigkeit der IT (Informationstechnik). Dort steht die Sicherheit an erster Stelle und damit über der Funktionalität und der Verfügbarkeit. Im Gegensatz dazu steht an einer Produktionsanlage die Verfügbarkeit über allem. Das lässt sich an einem einfachen Vergleich verdeutlichen: Eine Papiermaschine, in der das Papier mit fast 2.000 m/s durch die Anlage läuft, muss innerhalb von Millisekunden reagieren können. An einem Büro-PC spielt es dagegen keine Rolle, wenn der Benutzer mal fünf Sekunden auf einen Virenscan warten muss.

Auch in einem weiteren Punkt unterscheiden sich die IT und die Automatisierungstechnik gravierend: bestehende Steuerungen und andere Automatisierungskomponenten wie Umrichter oder Regler haben in der Regel keine eigenen Sicherheitsfunktionen. Wer auf ein Gerät Zugriff hat, kann dort Daten auslesen und Programme oder Parameter ändern, ohne dass er sich authentifizieren muss und ohne dass dies protokolliert wird. Das hat historische Gründe. In den Anfangszeiten der Automatisierung war jede Steuerung eine autarke Insel und die äußere Sicherheit war durch einen aufmerksamen Werkschutz garantiert.

Kein Zugriff von außen

Soll nun jedoch eine Vernetzung und Fernwartung stattfinden, ist eine Lösung gefordert, welche sowohl den Anforderungen der IT als auch der Automatisierungstechnik entspricht. Als nicht akzeptabel gelten Konzepte, bei denen über das Internet von außen auf Maschinen oder Anlagen zugegriffen werden soll. Dieser Ansatz würde zu einem erheblichen technisch-administrativen Aufwand führen. Für jedes zusätzlich installierte Gerät müsste die Konfiguration der Firewall manuell angepasst werden. Neben dem Arbeitsaufwand muss auch das Sicherheitsrisiko betrachtet werden. Bei der manuellen Konfiguration der Firewall ist schnell ein Fehler passiert, der die Schutzfunktion beeinträchtigen kann.

Zentrale Plattform

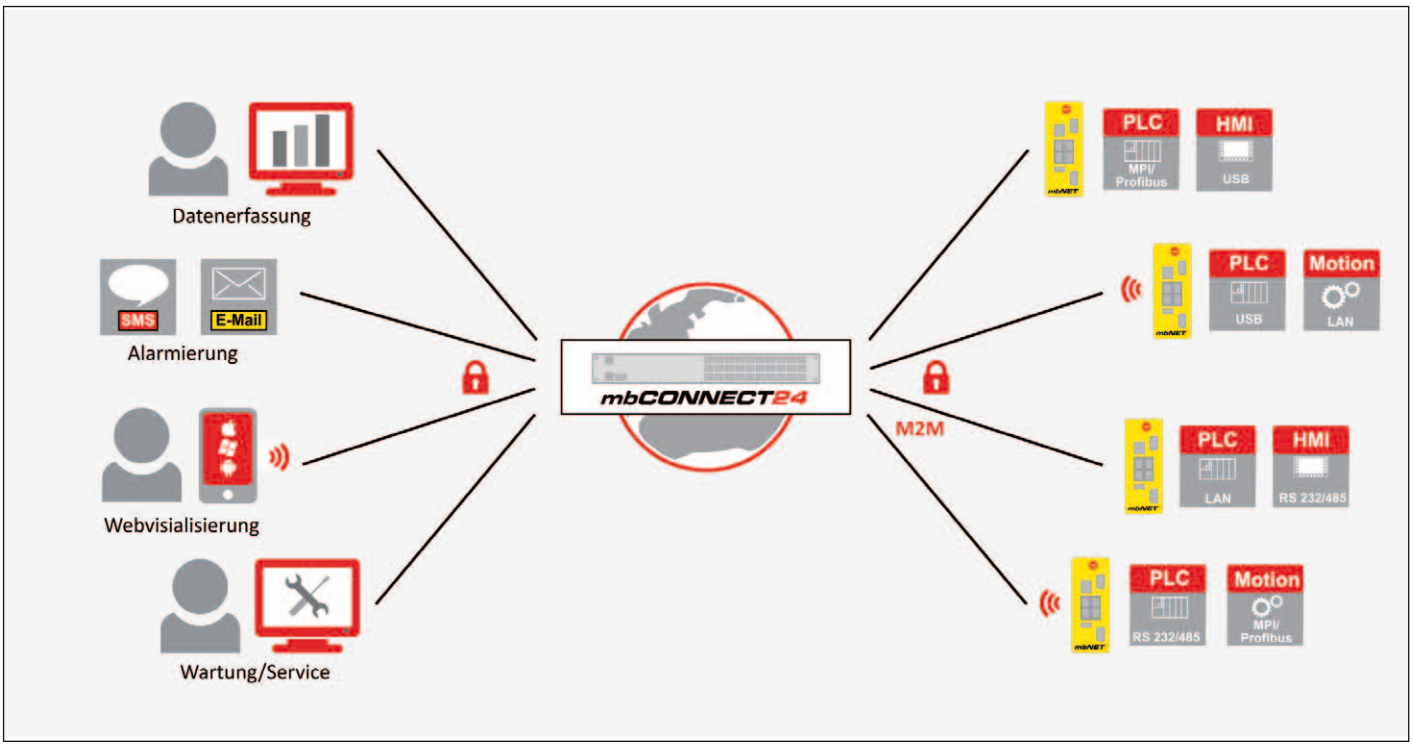
In der Praxis haben sich Lösungen bewährt, die auf einer zentralen Remote-Service-Plattform basieren. Sowohl das Service-Personal als auch die Maschinen und Anlagen verbinden sich mit der Remote-Service-Plattform. Der große Vorteil ist, dass Verbindungen von innen nach außen ohne Änderungen an bereits vorhandenen Firewalls funktionieren. Eingehende Verbindungsanfragen an den Maschinen kommen prinzipbedingt nicht vor. Bei den Kunden bereits eingeführte Sicherheitsstrategien bleiben unberührt. Die Übertragung der Daten sollte verschlüsselt erfolgen, beispielsweise über gesicherte VPN-Verbindungen. Als Verschlüsselungsprotokoll hat sich TSL (SSL) bewährt. Diese hohen Sicherheitsstandards ermöglichen den Einsatz auch in geschäftskritischen Anwendungen.

Rollenbasierte Rechteverwaltung

Die zentrale Plattform hat auch den Vorteil, dass der Anlagenbetreiber weder externem Service-Personal noch den eigenen Mitarbeiten einen direkten Zugriff auf das Produktionsnetzwerk erlauben muss. Direkten Zugriff auf alle Maschinen hat nur die Plattform, die eine rollenbasierte Rechteverwaltung für alle Beteiligten bietet. Sie erlaubt eine feine Abstufung der Rechte der einzelnen Benutzer – bis hin zur Beschränkung der Zugriffsrechte auf einzelne Ports oder Protokolle. Damit sind verschiedene Sichtweisen auf die Maschinen und Anlagen möglich. Den Produktionsleiter interessieren beispielsweise nur die wesentlichen Zahlen einer Anlage, während für den Bediener wichtig ist, ob die Anlage richtig läuft und alle Parameter im grünen Bereich sind. Für das Service-Personal sind die Produktionsdaten und Rezepturen tabu, sie können jedoch eingreifen, wenn Anlagenparameter oder SPS-Programme angepasst werden müssen.

Cloud oder nicht?

Seit Snowden und der NSA-Affäre überlegt man genau, wem man seine Daten anvertraut: Wo steht der Server? Wie ist dieser gesichert? Welche nationalen Gesetze gelten am Serverstandort? Zu empfehlen ist daher eine Lösung, die auf der Server-Infrastruktur des Anwenders betrieben wird, beispielsweise auf Basis von VMware vSphere. Kein Tunnel-Endpunkt befindet sich damit außerhalb des eigenen Hoheitsgebiets. Es sind alle Vorteile einer virtualisierten Umgebung wie Skalierbarkeit, Verfügbarkeit, Performance, Datensicherung und schnelle Wiederherstellung nutzbar. Über verschiedene Lizenzmodelle kann die Leistungsfähigkeit der Plattform mit den Kundenanforderungen wachsen. Dank regelmäßiger Sicherheitsupdates des Herstellers ist die Kundenplattform stets auf dem aktuellen Stand. Die Antwort zu der Frage oben ist deshalb: Ja, aber auf der eigenen Infrastruktur.



Die Remote-Service-Plattform als universelle Lösung für die Datenerfassung, Fernwartung und M2M-Kommunikation

Anbindung von Bestandsanlagen

In Maschinen und Anlagen findet man häufig Steuerungen und Komponenten, die mit dem Internet verbunden sind, obwohl sie dafür gar nicht vorgesehen waren. Als viele der heute eingesetzten Geräte und Feldbusse entwickelt wurden, waren Internet, Industrie 4.0, Big Data und IIot (Industrial Internet of Things) noch unbekannt. Diesen Systemen fehlen daher jegliche Sicherheitsmerkmale für eine direkte Vernetzung, wie Zugangsschutz mit Passwort oder signierte Firmware-Updates. Jeder, der Zugriff auf die Geräte hat, kann Daten abziehen oder Programme ändern. Eine Barriere, entsprechend einer Firewall, an der sich der Benutzer erst einmal ausweisen muss, gibt es nicht. Das war auch kein Problem, solange die Anlagen als Inseln in der Halle standen. Der Werkschutz hatte dafür gesorgt, dass keine unberechtigten Personen an die Anlagen kamen. Heute sind diese autarken Inseln immer seltener zu finden, denn die durchgehende Digitalisierung schreitet in großen Schritten voran. Das umfasst auch die Kommunikation über Unternehmensgrenzen hinweg, so dass zwangsläufig der IP-basierte Datenaustausch über Internet ins Spiel kommt. Dabei geht es nicht nur um „Notfälle“ wie Fernwartung, sondern auch um viele andere Anwendungen: das Überwachen von Maschinenzuständen, das Erfassen von Verbrauchswerten, die Alarmierung bei Störung oder Materialmangel, das Fernauslesen von Messwerten oder das Protokollieren von Betriebsdaten. Mit der Vernetzung steigen auch die Risiken hinsichtlich Sabotage, Erpressung und Spionage. Mögliche Folgen können Produktionsausfall oder schlechte Qualität, Schäden an Maschinen und Anlagen, Gefährdung der Betriebs- und Arbeitssicherheit, Verlust von Image und Reputation, Umweltschäden sowie Diebstahl von Informationen und Know-how sein.

Sicher in die Cloud

Um Bestandsanlagen „Industrie 4.0-tauglich“ zu machen, eigenen sich Secure Cloud Gateways, welche hardware-technisch die Kommunikation nur in eine Richtung zulassen – vom Feld ins sichere Netz. Es sollte technisch unmöglich sein, sich von außen mit der Anlage zu verbinden, um Daten zu stehlen oder zu manipulieren. Möglich ist das, indem der Rückkanal elektrisch getrennt ist und nur per Schlüsselschalter zu Konfigurationszwecken aktiviert werden kann. Durch die echte hardware-basierte Trennung sind auch die üblichen Schwachstellen von Security-Hardware ausgeschlossen: fehlerhafte Konfiguration durch den Anwender oder Sicherheitslücken in der Geräte-Software. Neben der Nachrüstung eignen sich die Secure Cloud Gateways auch für Neuinstallationen. Der große Vorteil ist dabei, dass bestehende Sensoren und Bussysteme weiter verwendet werden können – der Anwender muss nicht auf neue Standards für IIoT-Sensoren warten, die es in Zukunft vielleicht einmal geben wird. Ein wichtiger Punkt ist die Unterstützung der vielfältigen Kommunikationsmöglichkeiten in der Feldebene (MPI, Profinet, Modbus, …) und in der Kommunikationsebene (Netzwerk, Mobilfunk, WiFi). Das lässt sich mit einem modularen Aufbau solcher Gateways umsetzen.

Sicherheitsrisiko Mitarbeiter

Industrielle Sicherheit umfasst nicht nur den sicheren Betrieb von Maschinen und Anlagen im Sinne von gefährdungs- und unfallfrei, sondern auch den Schutz von Know-how und die Sicherstellung der Systemintegrität. Das beginnt mit einer Segmentierung der Netzwerke in einzelne Automatisierungszellen und setzt sich darin fort, die Datenzugriffe nur einem begrenzten Teilnehmerkreis zugänglich zu machen. Was in diesem Zusammenhang oft unterschätzt wird, ist die Bedrohung von innen. Etwa dadurch, dass Mitarbeiter Downloads von kompromittierten Internetseiten oder E-Mails machen – oder Schadsoftware von USB-Sticks mit unklarer Herkunft einschleusen. Industrial Security ist keine rein technische Angelegenheit. Auch organisatorische Umstände und der Faktor Mensch spielen eine wichtige Rolle. Allgemein bekannte Abteilungspasswörter müssen ebenso der Vergangenheit angehören wie die kleinen gelben Haftnotizen, welche die Passwörter für jedermann zugänglich machen. Die Anforderungen an Qualifikationen und Ausbildung der Mitarbeiter werden steigen. Während im Produktionsumfeld und in der Automatisierungstechnik grundlegende Kenntnisse in Sachen Security erforderlich sind, werden sich Verantwortliche der IT-Sicherheit, wie der Chief Information Security Officer (CISO), mit den Anforderungen der Produktionstechnik befassen müssen. Und nicht zuletzt muss dem Management klar sein, dass es Industrial Security nicht zum Nulltarif geben kann.

■ *MB Connect Line*
www.mbconnectline.com