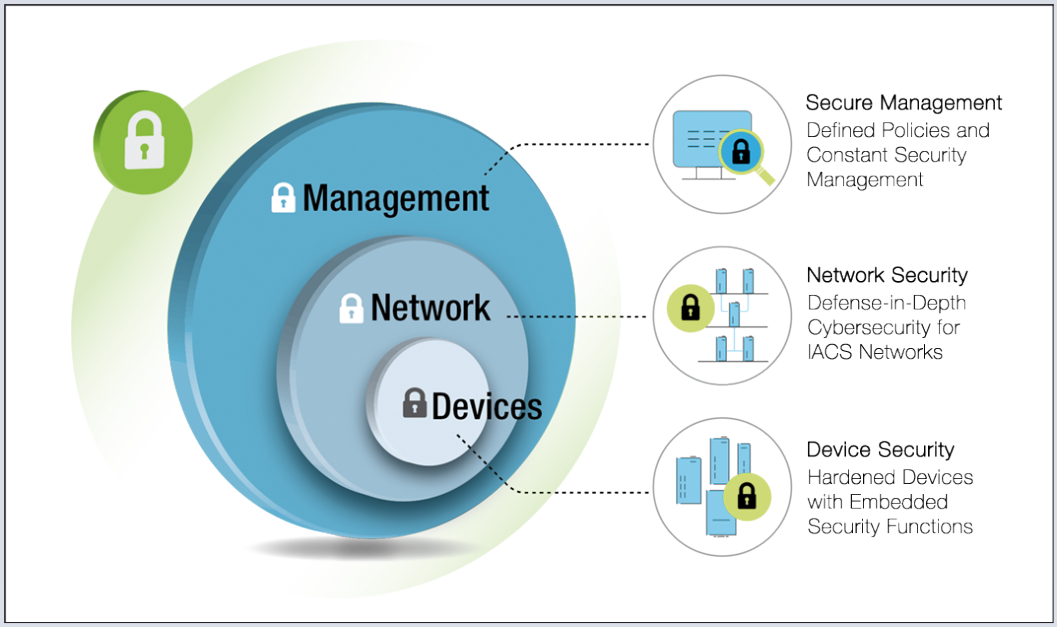
Ich glaube ich brauche IIoT…ist das auch sicher?



Das industrielle Internet der Dinge, kurz IIoT, ist der Begriff der Stunde, und viele große und kleine Unternehmen prüfen, wie diese neue Technologie ihrem Geschäft helfen kann. Wie der Name schon sagt, geht es darum, ein maximal miteinander verbundenes Netz industrieller „Dinge" zu schaffen. Aber worum handelt es sich bei diesen „Dingen"? In gewissem Sinne könnten dies die Geräte sein, welche die Datenansicht der realen Welt liefern, aber in Wirklichkeit sind es die eigentlichen Daten, die verarbeitet werden. In dieser Hinsicht sind die Gemeinsamkeiten zwischen IIoT und dem allgemein bekannten Internet einfach zu erkennen.

Application Platform as a Service

IIoT-Anwendungen können zum Beispiel eine so genannte APaaS-Instanz (Application Platform as a Service) verwenden. Unternehmen verkaufen kein Produkt mehr, sondern sie verkaufen oder vermieten sogar ein Gesamtpaket aus Produkt, Wartung und Überwachung. Automatisierungsstrukturen und -maschinen bilden die Unterschiede zwischen IIoT und dem allgemeinen Internet, wobei eine solche Anwendung effiziente betriebliche Prozesse ermöglicht. Die Begrenzung unerwünschter, nicht autorisierter Zugriffe, die sich negativ auf den reibungslosen Betrieb auswirken, ist dabei eine sehr wichtige Funktion.

Der tatsächliche Einsatz des IIoT sollte grundsätzlich durch zwei Fragen entschieden werden: Benötigt ein Unternehmen das IIoT überhaupt, und wenn ja, kann der Service als sicher angesehen werden? Wir betrachten diese Fragestellung im Folgenden aus drei verschiedenen Blickwinkeln: Ein Unternehmen denkt an das IIoT als mögliche Lösung, ein Lieferant berät das Unternehmen, und ein Hacker versucht auf ein IIoT-Netzwerk zuzugreifen.

Situation Lieferant-Unternehmen

Lieferant: Sind Sie sicher, dass Sie das IIoT brauchen? Wäre nicht auch ein einfaches Überwachungssystem gut genug?

Unternehmen: Ich habe davon gehört und ich habe eine Menge Dinge, die ich an vielen verschiedenen Orten überwachen muss, daher scheint es ein guter Weg zu sein.

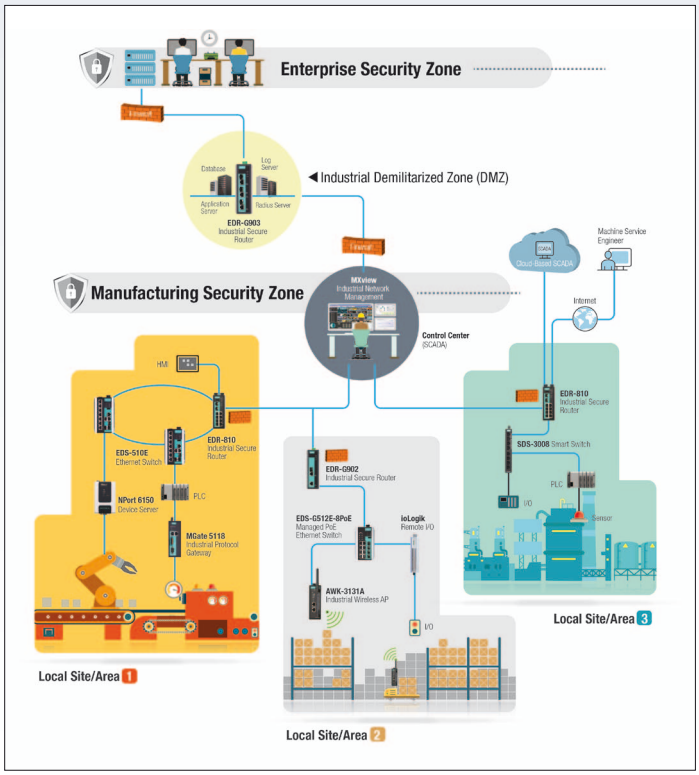
Lieferant: Lassen Sie uns Ihre Erwartungen betrachten. Möchten Sie nur wissen, was in der Werkstatt passiert oder auch, wie die Betriebskosten aufgeschlüsselt werden?

Unternehmen: Ich muss den Produktionsprozess verwalten und meine Gewinne maximieren können.

Lieferant: Wie schaffen Sie das heute?

Unternehmen: Ich habe eine Reihe von Prozessen, die jeder befolgt, und ich mache intelligente Annahmen über den Ablauf der Dinge.

Lieferant: Sie haben zwei Säulen. Eine effiziente Unterbrechung des Fertigungsprozesses ist die eine und



Autor:
Alan Harris, Moxa Field Application Engineer

Moxa
www.moxa.com

die andere ist, dass Sie die Kosten der Angestellten, der Produktionsstätte selbst und des Maschinenparks kennen und dann Annahmen treffen, wie z. B. regelmäßige Wartung und Urlaubszeiten. Aber wie genau sind Ihre Annahmen? Sehen Sie sich heute die Kosten für Probleme an und prüfen Sie, ob Sie Ihre Annahme ändern sollten?

Unternehmen: Wir tun es aber nur, wenn wir Zeit haben, es zu tun. Vielleicht einmal im Jahr.

Lieferant: Was ist, wenn wir eine Ihrer Annahmen bezüglich der regelmäßigen Wartung nehmen, zum Beispiel die Kosten für das Ersetzen dieser Vorrichtung in den Schneidegeräten auf allen Maschinen? Durch die Anwendung der IIoT-Technologie müssen Sie die regelmäßige Wartung nicht mehr durchführen, sondern das Teil nur austauschen, wenn es tatsächlich erforderlich ist, und den Austausch so planen, dass er zur kostengünstigsten Zeit für das Herunterfahren der Maschinen stattfindet.

Unternehmen: Hört sich gut an, aber es gibt noch etwas, worüber ich mir Sorgen mache: alle diese Daten werden über das Internet übertragen. Das bedeutet, dass andere es sehen können und Hacker in meine Systeme eindringen können.

Daten als Lebensader

Die Lebensader eines Unternehmens sind seine Daten. Beschafft sich jemand die Daten, analysiert oder ändert sie, dann besitzet er das Unternehmen. Wenn Daten in falsche Hände geraten, kann ein Unternehmen bestenfalls wertlos sein und im schlimmsten Fall sind die Kunden des Unternehmens, bei denen die Integration in andere Prozessbestandteile stattfindet, noch schlechter dran.

Ohne Daten ins Internet zu stellen, besteht auch heute noch die Notwendigkeit, Sicherheitsrisiken zu bewerten. Gibt es beispielsweise die Möglichkeit, einen Virus von außen in das Netzwerk einzubringen? Gibt es einen verärgerten Mitarbeiter, der dem Unternehmen schaden will? Auf dem Markt gibt es verschiedene Produkte mit den notwendigen Funktionen zur Sicherstellung, dass Daten dauerhaft abgesichert sind. Der allgemeine Rat hierfür lautet, Zonen mit Sicherheitsebenen auf IIoT-Gateways, Industrial Secure Routern und Industrial Network Switches bereitzustellen. Gateways, Router und Switches unterschiedlicher Hersteller führen diese Funktionen aus.

Situation Hacker

Was passiert, wenn ein Hacker in ein derart gesichertes Netzwerk eindringen möchte?

Hacker: Hier ist etwas. Eine große Menge an Daten wird von diesem Punkt aus in die Cloud übertragen. Kann ich hier reinkommen? Hm. Stark verschlüsselt und sogar die Verbindung selbst ist gut gesichert. Mal sehen, ob es einen anderen Weg gibt.

Hacker: Ah! Der physische Verbindungspunkt hat einen offenen Port. Jetzt kann ich mich hier genauer umsehen. Was ist das? Dieses Format habe ich schon einmal gesehen. Ich kann mein Modbus-Skript verwenden, um eine Anforderung zum Abrufen der Nachrichtendaten zu senden.

Hacker: Seltsam, ich bekomme die Antwort „Keine Verbindung". Sie müssen den Nachrichtenstrom anscheinend auf Anforderungen außerhalb des Gültigkeitsbereichs hin überwachen. Mal sehen, ob ich am Verteilungs-Switch vorbeikomme. Nein, meine IP-Adresse ist nicht zulässig. Ich bin jetzt von der Topologie abgeschnitten. Die Firewall wurde irgendwo aktualisiert, um meine Modbus-Abfrage zu stoppen.

IIoT-Gateways spielen in den meisten modernen IIoT-Anwendungen eine wesentliche Rolle. Es ist daher wichtig, ein IIoT-Gateway zu wählen, das Daten und Verbindungen vom Netzwerkrand, dem so genannten Edge, hin zur Cloud schützen kann. Durch die Verwendung von Industrial Secure Routern innerhalb des lokalen Netzwerks, werden Funktionen eingesetzt, die zum Einschränken und Stoppen unerwünschter Verbindungen und zum Spoofing von Daten erforderlich sind. Die IIoT-Gateways, die den Trusted Platform Module (TPM) -Standard unterstützen, entsprechen dem Sicherheitsstandard EAL4 +. Verbindungen zwischen dem Gateway und der Cloud sollten VPN mit seiner inhärent expliziten Kapselung und Verschlüsselung für jeden gebildeten Tunnel verwenden. Ein Authentifizierungssystem wie das API-Token-Management muss unbedingt verwendet werden. Dadurch wird sichergestellt, dass nur autorisierte Benutzer oder externe Systeme die API (Programmierschnittstelle) des IIoT-Gateways verwenden können.

Hohe Sicherheit aufrechterhalten

Eine weitere Überlegung ist es, Eindringlinge nicht nur zu erkennen und dann auf das Ereignis zu reagieren, sondern auch sicherzustellen, dass das konfigurierte Topologiesystem von Anfang an eine gute Sicherheit bietet und die hohe Sicherheit konsequent aufrechterhält. Ein Bestandteil der MxStudio-Software von Moxa ist ein Teil zum Anzeigen und Überwachen der Topologie namens MxView, der eine Sicherheitsansicht der Topologie bietet. Die Software scannt automatisch die IEC 62443-4-2-bezogenen Konfigurationen der Netzwerkgeräte von Moxa und stellt fest, ob das Gerät die Anforderungen der IEC 62443-4-2 Level 2, Level 1 oder der Grundstufe erfüllt. Die Software ist sehr einfach zu bedienen und informiert die Bediener schnell über den aktuellen Sicherheitsstatus der einzelnen Geräte im Netzwerk. Durch die fortlaufende automatische Überprüfung der Sicherheitseinstellungen der Geräte wird sichergestellt, dass alle Geräte, selbst in großen Netzwerken, über die entsprechenden Sicherheitseinstellungen verfügen, und der Netzwerkbetreiber muss die Geräte nicht zeitaufwändig manuell scannen.

Haben wir das gewünschte Ergebnis erzielt und eine sichere IIoT-Lösung bereitgestellt? Die Verbindung zur Cloud wird auf sehr sichere Weise hergestellt, und die Überwachung zur Erkennung von Eingriffen und die Möglichkeit zur Reaktion darauf stehen zur Verfügung. Schon die Gestaltung der lokalen Topologie ist von Anfang an auf Sicherheit ausgerichtet.

Die Wartung der Cyber-Sicherheit ist wichtig und für das IIoT obligatorisch. Es ist keine „Fire-and-forget"-Lösung. Wäre die Anfrage des Hackers unbemerkt geblieben, hätte er nicht nur Zugriff auf die Maschinen erhalten, sondern auch Einfluss auf das gesamte Geschäftsmodell des Unternehmens. ◄