Security an der Edge

Experten warnen: Es ist nicht die Frage ob, sondern wann ein Unternehmen beziehungsweise eine Produktion das Ziel einer Cyber-Attacke wird. Die sich verlagernde Angriffsoberfläche für Cyber-Attacken sorgt für einen wachsenden Bedarf an Security-Lösungen an der Edge.

Stellen Sie sich vor, Sie sind für die Nordamerika-Aktivitäten eines führenden Herstellers zuständig. An einem scheinbar normalen Arbeitstag erhalten Sie von einer ihrer größten Fabriken eine Liste von Produktdefekten. Der Trend scheint vor einiger Zeit begonnen zu haben und verstärkt sich weiter, jedoch lässt sich die Ursache des Defekts nicht lokalisieren. Dabei scheint alles in der Fabrik normal zu laufen.

Verzwickte Situation

Sie stehen vor der Entscheidung: Soll die betreffende Anlage für genauere Diagnosen abgeschaltet werden oder soll der Betrieb in der Hoffnung weiterlaufen, der Trend möge sich von allein umkehren und der Produktausstoß wieder ein normales Niveau erreichen? Sie entscheiden sich, die Anlage herunterzufahren und eine außerplanmäßige Wartung durchzuführen.

Nach mehrstündiger Diagnose scheint es einen Durchbruch zu geben: Obwohl oberflächlich alles normal wirkt, gibt es in der SPS-Software eine Anomalie. Im Laufe weiterer Diagnosen wird klar, dass die Fabrik Opfer eines Hackerangriffs wurde.

Warum hat man dies nicht früher entdeckt? Die Hacker müssen vorsichtig vorgegangen sein und den Schad-Code so verborgen gehalten haben, dass für die Bediener scheinbar alles normal lief.

Nachdem die Anlage außer Betrieb gesetzt werden musste, kann die Fabrik wieder ihren regulären Betrieb aufnehmen. Die Frage aber bleibt: Ist es gelungen, alle betroffenen Anlagen in Quarantäne zu nehmen?

Zum Glück sind sämtliche Geräte in der Fabrik einschließlich der Antriebe und Servos mit einer Hardware-Root-of-Trust ausgestattet, die es ermöglicht, ein Softwareupdate auf vertrauensvolle Weise an alle potenziell betroffenen Maschinen auf der Welt zu pushen. Vielleicht gelingt es mit diesem Update, das japanische Werk vor ähnlichen Problemen zu bewahren.

Security-Lösungen erlangen immer mehr Bedeutung

Das Beispiel zeigt: Weil sich die Angriffsoberfläche für Cyber-Attacken wandelt, gibt es ein erhöhtes Sicherheitsrisiko und einen gesteigerten Bedarf an Security-Lösungen an der Edge. Es ist unerlässlich, Fabriken auf belastbare Weise gegen Cyber-Angriffe zu wappnen.

Ein Unternehmen muss in der Lage sein, Angriffe zu erkennen und nach einer Attacke wieder zu einem geordneten Betrieb zurückzukehren. Daher bedarf es für den Aufbau einer vernetzten Fabrik intelligenter Edge Devices, die mit Attacken fertig werden können. Dies wiederum macht es notwendig, Security von der untersten Ebene an, also der Hardware, einzubauen. Wenn man den untersten Ebenen der Boot-Struktur eines Geräts vertrauen und entsprechende Software-Updates herausgeben kann, ist eine Fabrik in der Lage, sich rasch von einer Attacke zu erholen und ihren regulären Betrieb wieder aufzunehmen.

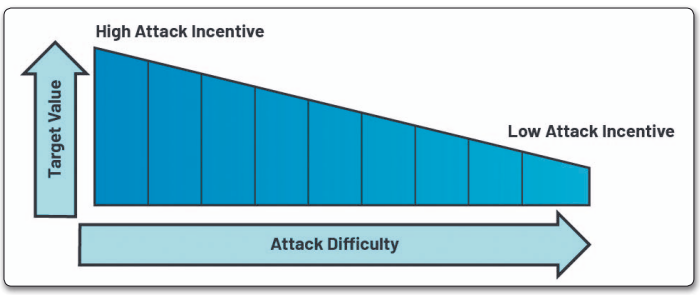
Sicherheitsrisiken verändern sich

Die Nachfrage nach Edge-Computing führt zur Vernetzung von immer mehr Geräten, die auf der Basis der von ihnen empfangenen Daten mit ihrer realen Umgebung interagieren. Diese intelligenten Geräte sind von entscheidender Bedeutung für die Resultate des heutigen digitalen Zeitalters. Je mehr Rechenleistung allgemein verfügbar wird, umso stärker wächst der Bedarf an Schutz vor den vermehrten Risiken aus dem Cyberspace. Es ist nur eine Frage der Zeit, bis die nächste intelligente Kaffeemaschine Schlagzeilen macht, weil sie von einer Cyber-Attacke als Geisel genommen wurde. Auch wenn das Lösegeld vernachlässigbar sein dürfte, gibt es durchaus Anreize für einen Angriff auf eine Kaffeemaschine, denn wegen der geringen Hürden ist das Durchführen einer solchen Attacke sehr wohl lohnend.

Bedenken Sie einmal, wieviel Aufwand man wohl treiben würde, um für eine ganze Fabrik Lösegeld zu erpressen. Die potenziellen Einnahmen sind hier deutlich höher – und damit steigt auch der Anreiz für etwaige Angreifer. infolge der zusammengewachsenen IT- und OT-Netzwerke (Operational Technology) ist es nicht mehr effektiv, beim Schutz kritischer Infrastrukturen ausschließlich auf Firewalls zu setzen. Man sollte vielmehr die Annahme zugrundlegen, dass sich jemand bereits Zugang zum Fabriknetzwerk verschafft hat, weshalb Integrität und robuste Authentifizierungs-Protokolle für sämtliche vernetzten Geräte vonnöten sind.

Darauf kommt es an

In einem Netzwerk zusammengeschlossener Geräte müssen diese die Fähigkeit haben, sich bei anderen Geräten im Netzwerk zu authentifizieren, Daten mit Signaturen zu



Ein Cyber-Angriff folgt ökonomischen Aspekten. Je höher der Schwierigkeitsgrad eines Angriffs, desto geringer ist der Anreiz für eine Attacke

Autor:
Erik Halthen ist Product Development Manager bei Analog Devices. Als Mitglied des Cyber Security Center of Excellence von ADI hat Halthen die Funktion des Security Systems Managers für Industrielösungen übernommen.

Analog Devices
www.analog.com

versehen und empfangene Daten zu validieren. Zwar gibt es hierfür standardisierte Verfahren, aber eine Fabrik bringt stets bestimmte Restriktionen mit sich, die das Anpassen der Security-Maßnahmen in einigen Anwendungsfällen zu einer Herausforderung werden lassen. Die Abhängigkeit von der Zeit in Motion-Control-Anwendungen etwa kann zu Latenz-Toleranzen führen, die traditionelle Arten der gegenseitigen Authentifizierung zwischen Geräten ungeeignet machen.

Bei der Verwendung der standardmäßigen Public-Key-Infrastruktur senden sich die Geräte gegenseitig Challenges zum Feststellen der Authentizität, und tauschen dann mit einer Methode wie etwa TLS (Transport Layer Security) einen gemeinsamen Session Key aus. Auch wenn diese Methode bereits in vielen Fabriken zur Anwendungen kommt, verbietet sich ihr Einsatz in schnellen Motion-Control-Anwendungen, da hier eine große Zahl von Geräten in einem bestimmten Zeitrahmen zusammenarbeiten muss.

Sobald Latenzen im Mikrosekundenbereich gefordert werden, muss das Verfahren zum Authentifizieren von Nachrichten so gewählt werden, dass das geforderte Geschwindigkeits- und Sicherheitsniveau erreicht wird. Der Fluss der Daten vom Controller zu sämtlichen Komponenten der Regelschleife muss unbedingt auf kongruente Weise empfangen werden.

Eine Möglichkeit, diese Art von Datenfluss zu erreichen, ist die Verwendung ein und desselben gemeinsamen Session Keys durch alle Geräte. Dies jedoch setzt eine ganz spezielle Netzwerk-Konfiguration voraus, die den Geräten die Authentifizierung bei einem Security Manager erlaubt, der sämtlichen Geräten einer bestimmten Security-Gruppe denselben Session Key zur Verfügung stellt. Diese Schlüssel werden mit dem standardmäßigen TSL-Verfahren ausgetauscht, während bei zeitkritischen Abläufen auf alternative Protokolle zurückgegriffen wird.

Ausweitung von Identität und Integrität bis an die Edge

Die Konnektivitätslösungen für Industrial-Ethernet der Reihe ADI Chronous ermöglichen eine geschützte Kommunikation an der Edge, das heißt an den Außengrenzen der Regelschleife. Die Lösungen sind an den Kommunikations-Endpunkten angesiedelt und können die Netzwerk-Kommunikation an jedem Knotenpunkt innerhalb des Systems absichern. Diese skalierbaren Ethernet-Lösungen ermöglichen das Ausweiten der Security in hochgradig zeitsensiblen Anwendungen, um mit wechselnden Sicherheitsrisiken fertig zu werden. Dazu zählen folgende Aspekte:

- Absicherung der Außengrenzen des Fabriksteuerungs-Netzwerks mit dem Ziel, eine belastbare und verlässliche Architektur aufzubauen
- Ermöglichen einer geschützten Konnektivität von Robotern, Antrieben und Produktionsmaschinen in einem integrierten OT/IT-ISN
- Schaffung der Möglichkeit für Authentifizierung und Verschlüsselung (je nach Bedarf) in einer hochgradig zeitkritischen Umgebung

Beispiel einer Industrial-Ethernet-Lösung

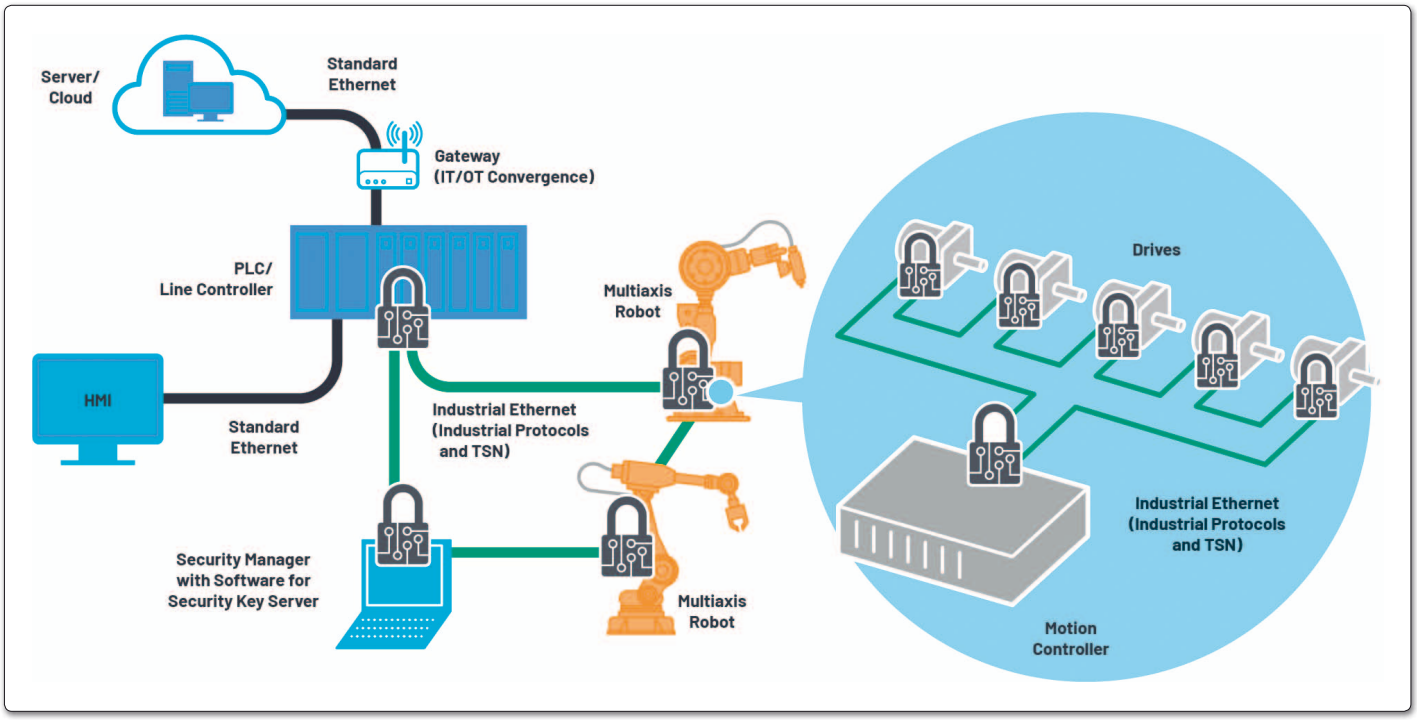
Die Security-Lösungen von Analog Devices für ADI Chronous Industrial Ethernet ermöglichen eine rasche Umstellung auf die vernetzte Fabrik. Auf der Basis der geschützten Entwicklungsprozesse bieten die Industrial-Ethernet-Lösungen die Gewähr dafür, dass das Security Design die Systemapplikation möglich macht, gleichzeitig aber ein Risikomanagement über den gesamten Produktlebenszyklus hinweg erlaubt.

Zu den Security Features zählen das Generieren und Verwalten der Schlüssel sowie Schutz für Bootvorgänge, Updates und Speicherzugriffe.

Die Einbindung von Security in die Geräte an den Außengrenzen eines industriellen Regelkreises schafft jenes Vertrauen in die Daten, das zum Skalieren von Lösungen nötig ist, die für Echtzeitentscheidungen in der Fabrik benötigt werden.

Zusammenfassung

Entscheidend für Unternehmen ist, sich den wandelnden Cyber-Risiken anzupassen. Haben es die Angreifer auf die Software des jeweiligen Geräts abgesehen oder wird es sich beim nächsten Cyber-Angriff um eine Netzwerkattacke handeln, die verfälschte Daten einschleust? Unabhängig hiervon müssen die verwendeten Geräte geschützt kommunizieren und sich vom nächsten Angriff erholen zu können. Dazu ist es notwendig, die Security von Anfang an, nämlich bereits in der Hardware, zu implementieren. Wenn man sich auf einer ganz elementaren Ebene auf den Bootvorgang eines Geräts verlassen und Software-Updates herausgeben kann, ist die Fabrik in der Lage, sich von einer Attacke zu erholen und den normalen Betrieb wiederaufzunehmen. ◄



Der Schaden durch einen Cyber-Angriff ist in einer vernetzten Produktion besonders hoch. Wichtig ist daher, die Betriebsumgebung sicher zu machen