Erleichterte Vernetzung birgt steigende Angriffsrisiken

Nicht erst seit dem massiven Push, den die industrielle Kommunikation durch das Protokoll OPC UA erfahren hat, sprechen Maschinen mit Maschinen und wird nach immer höheren Graden der Interoperabilität gestrebt.

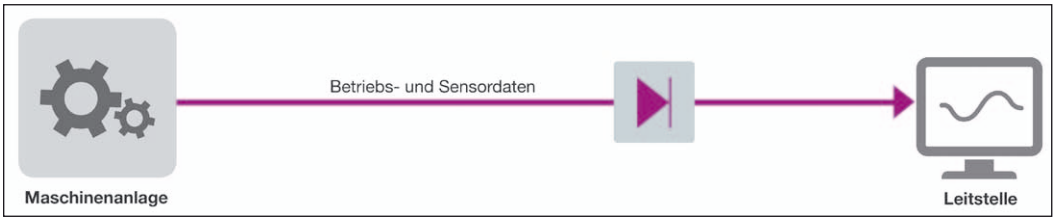
Schon seit langem und weit vor dem Industrie-4.0-Zeitalter wurden die Netzwerke ausgedehnt, Schnittstellen geschaffen und untereinander kommuniziert – weit über das lokale Netz hinaus. Aber jetzt erleichtert OPC UA die Verbindung von vorher isolierten Welten, der geschaffene Brückenschlag wird die Vernetzung von bisher voneinander getrennten Kommunikationspartnern deutlich beschleunigen.

Risiken bei zunehmender Vernetzung

Das Anbinden der Managementebene an die Produktion, die Vernetzung verschiedener Standorte, die Ausleitung von Daten zu Analysezwecken, der Zugriff von außen auf die Anlage per Fernzugriff und nicht zuletzt der durch alle diese Maßnahmen erreichte Grad der Interaktion und Automatisierung führen zu größeren Risiken für den Betrieb. Denn sollten Angreifer an einer Stelle einen Schwachpunkt ausnutzen und Daten stehlen oder den vollvernetzen Produktionsbereich lahmlegen, entstehen hohe Kosten und ein erheblicher Imageschaden. Noch schlimmer sind die Folgen, wenn durch Manipulationen bspw. Produktionsmaschinen außer Kontrolle geraten und Menschenleben gefährdet werden – gravierende Folgen also, die vermieden werden müssen. Dies macht deutlich, dass Industrie 4.0 eine hochwertige Absicherung erfordert, in kritischen Bereichen liegt die Fehlertoleranz bei null. Dies ist eine große Herausforderung für die IT-Sicherheit. Denn viele Einflussquellen bieten Spielraum für die unterschiedlichsten Angriffsszenarien. Und alle Branchen sind von steigenden Angriffszahlen betroffen.

Was tun?

Der Staat greift bereits ein und reguliert zum Beispiel im KRITIS-Umfeld das IT-Sicherheitsniveau. Das kann jedoch nur ein Anfang sein. Schon aus Selbstschutz und um die störungsfreie Produktion zu gewährleisten, sind viele Anlagenbetreiber gezwungen, rigorose Sicherungsstufen in ihre Netzwerke einzuziehen. Ganz zu schweigen von denen, die durch externe Einflüsse wie z. B. Branchen-Regularien oder Kundenanforderungen gezwungen



Interne Sicherheitszonen verhindern, dass sich Angreifer ungehindert im gesamten Netzwerk bewegen können

Autor:

Steve Schoner,
Product Marketing Manager,
genua gmbh

sind, ihre Maßnahmen durch Audits nachzuweisen. Doch was sind die ersten Schritte zu einem höheren Sicherheitsniveau? Hier helfen Institutionen wie der VDMA, und spezialisierte Beratungsdienstleister liefern fundierte Informationen und Empfehlungen. Im Folgenden beleuchten wir drei dieser Empfehlungen für Sie.

Segmentierung

Neben der Analyse des eigenen Unternehmens zur Ermittlung des IST-Standes, um sich einen Überblick zu verschaffen, stellt der VDMA in seinem Leitfaden für Industrie 4.0 die Segmentierung an vorderste Stelle. Das heißt: Netzwerke werden durch technische Maßnahmen aufgeteilt. Mit Firewalls werden Barrieren zwischen Maschinen und Komponenten eingezogen, wenn diese nicht den gleichen Schutzbedarf haben. Solche internen Sicherheitszonen verhindern, dass sich Angreifer ungehindert im gesamten Netzwerk bewegen können. Sollte dann ein Teil kompromittiert sein, wird die Ausbreitung des Angriffs zumindest erschwert und verlangsamt.

Datenverkehr ohne Rückkanal

Daneben können für ganz besonders gefährdete Netzsegmente Dioden sicherstellen, dass Daten ausschließlich in eine Richtung fließen. Das ist zum Beispiel der Fall, wenn zu Analyse- und Auswertungszwecken für Predictive Maintenance Daten von einer Anlage nach extern geleitet werden. In diesen Fällen muss jegliche Daten-Rückflussmöglichkeit unterbunden werden. Die Datendiode löst noch ein weiteres Sicherheitsproblem: Werden in einem abgeschotteten Hochsicherheits-Netzwerk Informationen aus anderen Bereichen benötigt, z. B. E-Mails, Videodaten oder Software-Updates, kann eine Schnittstelle für Einbahn-Transfers implementiert werden. So lassen sich Daten in Hochsicherheits-Netze übertragen, ohne in Gegenrichtung den Abfluss sensibler Informationen in ungeschützte Bereiche zu riskieren. Dioden haben den weiteren Vorteil, dass sie kaum verkonfiguriert werden können. Denn Dioden bieten im Vergleich zu Firewalls, die viele Anforderungen erfüllen müssen, nur wenige Optionen, da die Richtung des Datenflusses bereits fest einprogrammiert ist. Mehr Security by Design geht nicht.

Sichere Fernwartung

Was aber, wenn mittels oben beschriebener Predictive Maintenance bei einer Maschine Wartungsbedarf festgestellt wird? Eine Störung oder gar ein Ausfall muss vermieden werden. Denn ein Stopp der Produktion und der damit verbundene finanzielle Verlust ist für kaum ein Unternehmen tragbar. Daher ist es inzwischen gängige Praxis, dem Hersteller Zugriff auf Industrieanlagen per Teleservice einzuräumen, um eine schnelle und effiziente Wartung zu ermöglichen - Verschlüsselt, versteht sich.

Es empfiehlt sich auch hier, äußerst restriktiv mit den Zugriffsrechten umzugehen: Der Fernwartungs-Service muss sich eindeutig authentifizieren und erhält dann auch nur Zugriff auf das zur Wartung vorgesehene Objekt, nicht etwa das ganze Netz. Der Zugriff sollte immer von innen heraus bestätigt, also nicht automatisch zugelassen werden. Natürlich sollte es auch einen „Notaus"-Knopf geben, um im Zweifel den Zugriff zu unterbinden. In jedem Fall sind Logs oder noch besser Videoaufzeichnungen des Fernwartungszugriffs für eventuelle nachgelagerte Betrachtungen unerlässlich. Dem Fernwarter auf die Finger zu schauen, ist kein Zeichen von Misstrauen, sondern der Standardprozess zur Sicherung der Produktion.

Neben weiteren Faktoren zur Erhöhung des IT-Sicherheitsniveaus wie zum Beispiel Verschlüsselung oder einem Wiederherstellungsplan, gibt es noch eine Vielzahl an Möglichkeiten. Eines sollten alle gemeinsam haben: Einfache Konfiguration und Administration – auch bei einer Vielzahl unterschiedlicher Lösungen. Wer ein zentrales Management hat, ist hier klar im Vorteil. Dadurch werden die Folgeaufwände beim Betrieb der verschiedenen Sicherheitsprodukte gering gehalten. Zudem verschaffen diese Administrations-Zentralen eine solide Übersicht über alle betriebenen Komponenten und vereinfachen das Ausrollen von Updates und Patches. Denn bei allen Sicherheitsmaßnahmen gilt: Sie sind nur sicher, wenn sie auf dem aktuellen Stand gehalten werden. ◄