Einbruchschutz für smarte Fabriken

Vernetzte Fertigung braucht ganzheitlichen Schutz gegen Cyberattacken

Die Vorteile vollvernetzter, automatisierter und selbststeuernder Industrie-4.0-Prozesse sind in aller Munde. Dass sich neue Risiken und Angriffsflächen auftun, wenn Produktionsanlagen via Industrial Ethernet und Internet Protocol (IP) erreichbar sind, wird seltener thematisiert. Um cyberkriminelle Einbrecher und Erpresser abzuwehren, müssen ganzheitliche IT-Sicherheitskonzepte her.

Der Auftrag eilt. Rund um die Uhr läuft die Produktion auf Hochtouren. Dann fallen Touchscreens an mehreren Anlagen aus. Bei der Überprüfung fällt auf, dass auch der Zugriff auf zentrale Prozessdaten blockiert ist. Bald darauf geht eine Erpressermail ein.

Das Szenario ist nicht aus der Luft gegriffen. Allein seit 2016 rollten sechs große Cyberangriffswellen, die laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) teils mehrwöchige Betriebsausfälle und Millioneneinbußen in betroffenen Unternehmen verursachten. Angriffe auf Anlagensteuerungen und Industrial-PCs häufen sich laut BSI, weil zunehmend vernetzte Prozesse neue Angriffsflächen für Cyberkriminelle bieten. Entsprechend besorgt klingt BSI-Präsident Arne Schönbohm:

„Wir beobachten immer mehr IT-Sicherheitsvorfälle, die in immer kürzeren Abständen auftreten und eine neue Qualität aufweisen."

Eine beunruhigende Botschaft am Vorabend der Industrie 4.0.*

Industrial Ethernet: Mehr Performance, aber neue Risiken

Die Industrie 4.0 verspricht effizientere, transparentere und flexiblere Fertigungsprozesse. Doch auch die Risiken nehmen zu. Industrial Ethernet ersetzt bisherige Feldbusse. Fertigungssysteme lassen sich via Internet Protocol (IP) erreichen. Mit der Öffnung für die Außenwelt steigt die Gefahr unbefugter Zugriffe auf Steuerungssoftware und sensible Daten. Die zuletzt häufig erfolgreichen Angriffe zeigen, dass selbst global agierende Konzerne mit hochentwickelten IT-Systemen die Risiken unterschätzen.

Auch kleine und mittlere Betriebe sparen an der Cyber Security. Viele vermuten, ihre Produktion sei für Hacker uninteressant. Doch gerade weil IT-Systeme in der Fertigung pausenlos laufen und Updates dabei oft zu kurz kommen, sind sie besonders angreifbar; und das auch durch automatisierte Attacken. Selbst nicht vernetzte Anlagen sind bei Wartungen oder durch unkontrollierte USB-Schnittstellen in Gefahr. Hinzu kommt, dass Fertigungsbetriebe als Teil größerer Lieferketten erpressbar sind. Und nicht zuletzt wird Industrial IT-Security durch neue Regularien wie das IT-Sicherheitsgesetz zum Muss.

Umsetzung erfordert Expertise

Nur ganzheitliche Sicherheitskonzepte können vernetzte Produktionsanlagen zuverlässig schützen. Auf Basis detaillierter Status-quo-Analysen und mit fundiertem Systemverständnis für die heterogene IT im Produktionsumfeld gilt es, Risiken systematisch zu erfassen, zu bewerten und Sicherheitsziele zu definieren. Zu beachten ist, dass Wartungen und Updates umsetzbar sein müssen, wo Anlagen rund um die Uhr laufen und dass ein Passwortschutz wenig praktikabel ist, wo viele Bediener auf einzelne Systeme zugreifen. IT-Abteilungen, die sonst Büro-IT betreuen, können holistische Security-Konzepte für die Produktion kaum allein erstellen. Hier ist spezifische Expertise gefragt.

Denn es gilt, Security auf allen Ebenen zu adressieren und eine Governance zu entwickeln, um die IT-Security in Organisation, Prozessen und Köpfen zu verankern. Wirksamkeitsprüfungen im PDCA-Zyklus (Plan, Do, Check, Act) sind ebenso wichtig wie ein Informationssicherheits-Managementsystem (ISMS). Der ganzheitliche Schutz muss Gefahren vorbeugen, kritische Vorfälle erkennen, sie zügig abwehren – und in der Lage sein, Schlüsse für künftige Gefahren daraus zu ziehen. Nur so ist die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sämtlicher IT-Komponenten und -Systeme in der vernetzten Produktion dauerhaft sicherzustellen.

Konkrete Schutzmaßnahmen

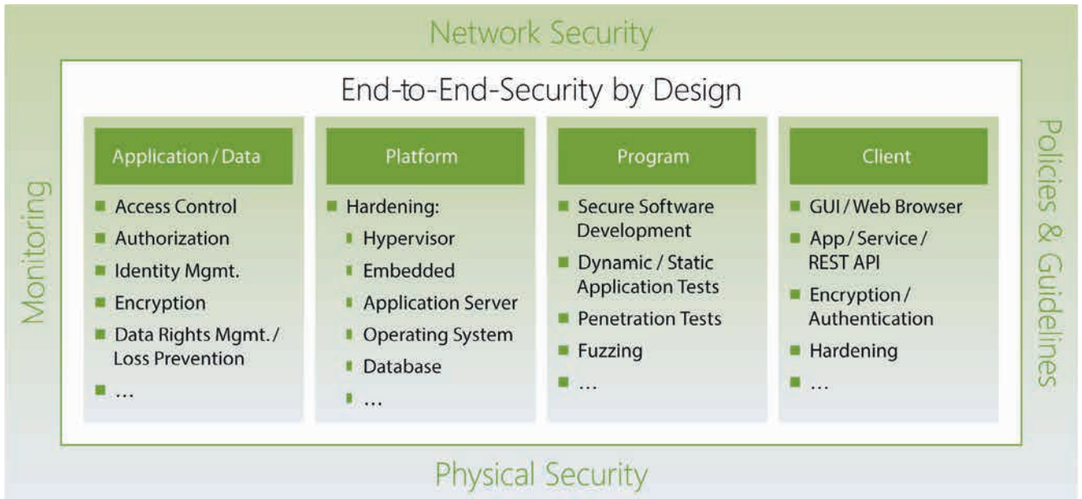
Aufgrund der heterogenen IT-Systeme sind bestehende Fertigungslinien schwer zu schützen. Es ist ratsam, den Schutz einzelner Maschinen oder Sicherheitszonen in vorgeschaltete Systeme zu verlagern. Diese schirmen die Prozesskommunikation von außen ab und filtern verdächtigen Netzverkehr heraus. Die Auslagerung erlaubt es zudem, Antivirensoftware, Angriffsabwehrfunktionen oder Applikations- und Benutzererkennungen bei laufender Fertigung zu aktualisieren. Schutz bieten auch Zonenmodelle, in denen Firewalls die Kommunikation zwischen einzelnen Fertigungszonen überwachen. Sie entscheiden anhand von Quell- und Zielinformationen, ob und welcher Netzverkehr zulässig ist. Beim Einrichten der Zonen sollten IT- und Fertigungsverantwortliche eng kooperieren. Zudem ist darauf zu achten, dass eine solche unterteilte Security-Umgebung mit Blick auf leichte Updates, Änderungen oder gesetzkonformes Reporting administrierbar bleibt.

Best Practice: End-to-End-Security by Design

Bei neu geplanten Smart Factories lässt sich Industrial Cyber Security dagegen direkt in die Soft- und Hardwaresteuerungen der Fertigungslinien integrieren. Security-Organisation, das fortlaufende IT-Sicherheitsmanagement und die Absicherung der Komponenten und Systeme können von Beginn an in Gleichklang gebracht und auf den Gesamtlebenszyklus der Anlagen ausgelegt werden. Mit dem Ansatz „End-to-End-Security by Design" entsprechen Fertigungsanlagen vernetzten IT-Systemen, deren Schutz zu einem Kernelement der Industrie 4.0 wird. ■

Autor

Norman Wenk ist Gruppenleiter Enterprise IT Security Consulting bei **ESCRYPT**.



Best Practice – End-to-End-Security by Design

*) Quelle: BSI-Magazin 2018/1