Integrierte Sicherheit

Bei der Digitalisierung von Prozessen in Fertigung und Logistik müssen Safety und Security Hand in Hand gehen

Die zunehmende Vernetzung von industriellen Infrastrukturen stellt Anwender ebenso wie Hersteller vor neue Herausforderungen. Ganz oben auf der Agenda steht das Thema Sicherheit. Der folgende Beitrag zeigt, warum Industrie 4.0 ein integriertes Sicherheitskonzept verlangt: Bei der Absicherung von Produktionsumgebungen muss nicht nur der Schutz von Mensch und Umwelt vor Gefahren, die vom Betrieb eines Systems ausgehen (Safety), berücksichtigt werden, sondern ebenso der Schutz der Systeme selbst vor Angriffen aus ihrer Umwelt (Security) und die Wechselwirkungen beider Aspekte.

Dr. Michael Richter, *Leiter Text, unlimited communications berlin in Berlin*

Wie können Sie verhindern, dass weitgehend autonom agierende Maschinen ihre menschlichen Kollegen verletzen? Bei der funktionalen Sicherheit wird immer das ganze System betrachtet. Heute sind aber Maschinen oft Bestandteile von Produktionsnetzwerken. Die sie steuernden Systeme (Industrial Control Systems, ICS) sind mit einer zunehmenden Zahl von Komponenten verbunden, die aus dem Internet erreichbar sind. All das macht ICS zunehmend verwundbarer gegen Cyber-Angriffe – schlecht gesicherte IoT-Geräte gehören zu den populärsten Angriffsvektoren in Produktionsumgebungen.

Gelingt es einem Hacker, ins Produktionsnetzwerk einzudringen, kann er Sicherheitsmaßnahmen sabotieren oder gefährliche Zwischenfälle herbeiführen. Eine unabdingbare Voraussetzung für Safety – den Schutz der Menschen vor den Systemen – ist daher Security, der Schutz der Systeme vor Menschen. Die Digitalisierung der Produktion erfordert somit ein integriertes Konzept von Sicherheit, das Safety und Security gleichermaßen berücksichtigt.

Tatsächlich sehen Entscheider und IT-Verantwortliche in Industrieunternehmen den Schutz ihrer Mitarbeiter vor Verletzungen als die größte Herausforderung der Cyber-Sicherheit an, so die Kaspersky-Studie „The state of industrial cybersecurity in the era of digitalization“ von 2020. Auf den weiteren Plätzen folgen die Beeinträchtigung der Servicequalität, der Verlust vertraulicher Informationen durch Cyber-Angriffe sowie die Kosten für die Schadensbegrenzung.

Malware für industrielle Steuerungssysteme (ICS)

Besonders besorgniserregend: Die derzeit wichtigste Cyberbedrohung, Ransomware (Erpressungssoftware), ist mittlerweile auch ICS-fähig geworden. ICS verwalten nicht nur Daten, sie steuern auch physische Prozesse. Cyber-Angriffe auf ICS können physische Anlagen manipulieren oder sogar zerstören. Wie zuerst der Computerwurm Stuxnet demonstriert hat, der speicherprogrammierbare Steuerungen attackiert, kann moderne Malware heute tatsächlich Produktionsprozesse lahmlegen. Das macht betroffene Unternehmen erpressbar, denn jeder Ausfall in der Fertigung kostet viel Geld. Laut der Studie „Cyber Threat Perspective Manufacturing Sector“ des Security-Dienstleisters Dragos hat sich 2020 die Zahl der gemeldeten Ransomware-Angriffe auf Produktionsunternehmen gegenüber dem Vorjahr mehr als verdreifacht. Auch die Verschlüsselung geschäftskritischer Daten, beispielsweise von ERP-Daten, kann die Handlungsfähigkeit eines Unternehmens sabotieren. Zudem kann ein erfolgreicher Angriff auf ein Produktionsunternehmen Auswirkungen auf die gesamte Lieferkette haben, weil Anlagen und Prozesse immer enger miteinander verzahnt werden.

Pandemie erschwert Absicherung

Der Sicherheitsdienstleister Kaspersky rechnet in seinen Prognosen für ICS-Bedrohungen 2021 mit noch ausgefeilteren Ransomware-Kompromittierungen, mehr zielgerichteten Angriffen auf Industrieeinrichtungen, neuen Taktiken zur Monetarisierung von Attacken und auch zunehmenden Spionageversuchen über OT (Operational Technology). Zu allem Überfluss wird die Arbeit der Security-Verantwortlichen noch durch die Auswirkungen der Covid-19-Pandemie erschwert.

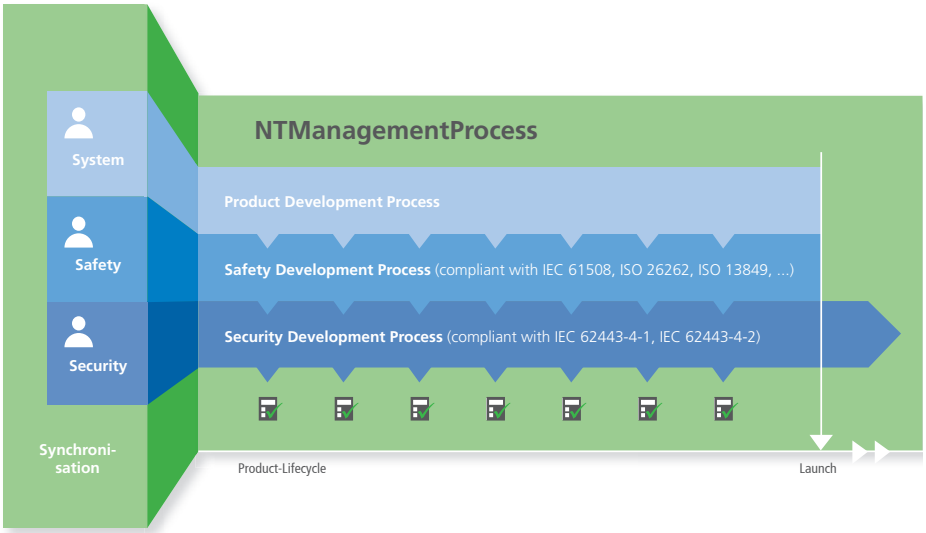
Denn als Reaktion auf die Pandemie haben viele Unternehmen ihre Arbeitsweise geändert und Arbeitsplätze ins Homeoffice verlegt. Häufig kommen dabei persönliche Geräte der Mitarbeiter zum Einsatz. Diese sind zwar per VPN (Virtual Private Network) ans Firmennetz angebunden, unterliegen aber in der Regel weniger strengen Sicherheitsstandards als Firmengeräte. Wie die bereits erwähnte Kasperski-Studie zur industriellen Cyber-Sicherheit ergab, nahmen dadurch unerwünschte Netzwerk-Scans auf Produktionsnetzwerke weltweit zu. Auch die Zahl von Phishing-Attacken und Malware-Angriffen steigt: Die Cyberkriminellen nutzen die Angst der Menschen vor dem Virus, um Zugangsdaten abzugreifen und die Kontrolle über die privaten Systeme zu übernehmen.

> In vernetzten Umgebungen kommen zu Safety-Risiken wie Bedienfehlern oder Ausfällen noch Security-Risiken für die System- und Datensicherheit hinzu, die ebenfalls regelmäßig analysiert und bewertet werden müssen.

Stephan Strohmeier ist Bereichsleiter Safety & Security Solutions bei der NewTec GmbH in Mannheim

Vernetzte Produktionsumgebungen effektiv schützen

„Wer vernetzte Maschinen und Anlagen anschafft oder bereits einsetzt, sollte für jeden konkreten Anwendungsfall regelmäßig eine strukturierte Bedrohungs- und Risikoanalyse durchführen“, empfiehlt Stephan Strohmeier, Bereichsleiter Safety & Security Solutions beim süddeutschen Sicherheitsspezialisten Newtec GmbH. „Dabei können die internationalen Security- und Safety-Normen und die Anleitungen des BSI eine große Hilfe sein. Allerdings sollten bei der Absicherung von Produktionsumgebungen Safety- und Security-Experten stets Hand in Hand arbeiten, denn Sicherheit ist immer eine Eigenschaft des Gesamtsystems, in dem sich Safety- und Security-Aspekte gegenseitig beeinflussen. Das wird leider in den aktuellen Standards und Anleitungen noch nicht genügend reflektiert.“



Ein strukturierter Security-Management-Prozess synchronisiert alle Bereiche der Produktentwicklung (System-, Security- & Safety-Entwicklung) nach den Vorgaben der einschlägigen Normen IEC 62443 und IEC 61508

Beispielsweise berücksichtigt das BSI in seinem ICS-Security-Kompendium keine Safety-Aspekte, sondern verweist auf die Safety-Basisnorm IEC 61508. Diese und die Security-Norm IEC 62443 verweisen wiederum aufeinander. Für den Anwender erzeugt das ein Henne-Ei-Problem. Um Unternehmen in dieser Situation zu unterstützen, hat Newtec einen strukturierten Prozess für die integrierte Sicherheit industrieller Anwendungen über ihren kompletten Lebenszyklus hinweg entwickelt.

In der Risikoanalyse auf bewährte Best Practices setzen

„Risikoanalysen in Bezug auf die funktionale Sicherheit berücksichtigen Eintrittswahrscheinlichkeiten und Auswirkungen möglicher Fehler, um zu beurteilen, welche Anstrengungen für deren Verhinderung bzw. Beherrschung notwendig und angemessen sind“, erklärt Stephan Strohmeier von Newtec. „In vernetzten Umgebungen kommen zu Safety-Risiken wie Bedienfehlern oder Ausfällen noch Security-Risiken für die System- und Datensicherheit hinzu. Sie können auf vergleichbare Weise analysiert werden, um potenzielle Bedrohungen und Angriffsvektoren in typischen Einsatzkontexten zu identifizieren, zu bewerten und mit praktikablen Maßnahmen abzuwehren.“

Newtec stützt sich dabei nicht nur auf die Methoden der genannten Normen und den BSI-Katalog, sondern auch auf bewährte Best Practices und umfangreiche Erfahrung. Bei Bedarf prüft Newtec Security-Konzepte und Systeme auf Schwachstellen (Penetration Tests) und bietet auch Hardware- und Softwarelösungen für die sichere Vernetzung und Cloud-Anbindung an, z. B. Sensorknoten und IIoT-Gateways.

Sicherheit und Pandemie

Und welchen Einfluss hat nun die Covid-19-Pandemie auf ein solches Vorgehen? Was beobachtet Newtec? Stephan Strohmeier schmunzelt: „In der Tat höre ich diese Frage in letzter Zeit häufig. Am grundsätzlichen Vorgehen der Risikoanalyse ändert sich durch die Pandemie erst einmal nichts. Aber natürlich erbringt die Analyse zusätzliche Resultate vor allem in Bezug auf Homeoffice und mobiles Arbeiten mit Fernzugriff auf das Firmennetzwerk. Somit sind weitere Bedrohungsszenarien in der Risikoanalyse zu berücksichtigen. Wir sehen aber auch, dass die Awareness der Unternehmen für Security-Aspekte durch die Remote-Arbeitsplätze gestiegen ist. Dieses gewachsene Bewusstsein strahlt hoffentlich auch in die Entwicklung neuer vernetzter Produkte aus.“

Bilder: *Aufmacher Pugun & Photo Studio – stock.adobe.com, sonstige NewTec*

www.newtec.de