Cyberkriminelle haben oft leichtes Spiel

Die Cybersecuritybedrohungen für Smart Factories sind vielfältig. Funktionierende Sicherheitsmechanismen unterscheiden sich teils fundamental von der klassischen Unternehmens-IT, essenziell ist aber auch hier ein risikobasierter Ansatz. **Text** Dr. Dr. Florian Skopik

FOTO: AIT/JOHANNES ZINNER

Dr. Dr. Florian Skopik
Thematic Coordinator Cyber Security, Security & Communication Technologies, Center for Digital Safety & Security, AIT Austrian Institute of Technology GmbH

Erfolgreiche Cybersecurityangriffe auf nicht-klassische IT-Systeme nahmen in den letzten Jahren rasant zu. Neben vereinzelten aufsehenerregenden Fällen, wie dem Angriff auf die Colonial Pipeline in den USA im Mai 2021, gibt es de facto wöchentlich Berichte über erfolgreiche Angriffe auf Firmen im produzierenden Gewerbe und Anbieter von kritischer Infrastruktur. Die Akteure sind so vielfältig wie ihre Ziele. Von sogenannten Insider Threats (typischerweise unzufriedene, bestechliche oder erpressbare Mitarbeiter:innen mit Insiderwissen) über Hacktivisten, die aus ideologischen Motiven handeln, oder Cyberkriminellen, die rein finanzielle Motive verfolgen, bis hin zu staatlich finanzierter Wirtschaftsspionage ist alles nicht nur denkbar, sondern bereits da gewesen.

Die Ziele der Angreifer können sehr unterschiedlich sein

Angreifer versuchen dabei, Zugriff auf interne Systeme zu erlangen, um geistiges Eigentum, wie Produktionspläne oder Maschineneinstellungen, zu entwenden, oder aber haben das Ziel, den Betrieb zu stören. Dabei muss nicht immer gleich ein Totalausfall die Folge sein. Auch die Manipulation einzelner Maschinen mit dem Ziel, die Produktqualität zu verringern, konnte bereits beobachtet werden – was sehr schwer für den Betreiber zu entdecken ist. Verbreitet ist auch, mittels Ransomware (Verschlüsselungstrojaner) Systeme zu verschlüsseln und Lösegeld zu erpressen.

Die eigenen Schwächen kennen

Hierbei gehen die Angreifer ganz unterschiedlich vor, jedoch in der Regel so, dass sie mit dem geringstmöglichen Aufwand die größte Wirkung im Sinne ihrer Ziele erreichen. Daher ist es für Betreiber essenziell, die eigenen Schwächen genau zu kennen, um dort gezielt nachzubessern. Neben technischen Lücken steht bei vielen erfolgreichen Angriffen auch der Mensch im Fokus. Mittels Social Engineering, also der Anwendung ausgefeilter Täuschungsmanöver, werden Mitarbeiter dazu gebracht, im Sinne der Angreifer zu handeln – die sich beispielsweise als Geschäftspartner oder Dienstleister ausgeben. Dahingehend bergen insbesondere der unachtsame Umgang mit sensitiven Informationen, wie Passwörtern, gepaart mit mangelndem Risikobewusstsein, große Gefahren.

Der Druck auf die Unternehmens-IT wächst

Die klassische Unternehmens-IT hat in den letzten Jahren teils unter großem Leidensdruck lernen müssen, mit diesen Bedrohungen umzugehen. Die Betriebsleittechnik, auch Operational Technology (OT) genannt, die auch Steuersysteme in Smart Factories umfasst, hinkt aber oft aus unterschiedlichen Gründen deutlich hinterher. Ein breiter Mix an eingesetzten Technologien und Geräten mit wenig Rechenleistung und schlechter Netzwerkanbindung verhindert oft anspruchsvolle Schutzmechanismen, wie fortschrittliche Kryptografie und feingranulares Monitoring. Geräte in der OT unterliegen auch einem sehr hohen Lebenszyklus von oft 20 Jahren und mehr – neue Sicherheitstechnologien setzen sich daher nur langsam durch. Darüber hinaus sind Updates und das Einspielen von Patches in Steuergeräten nicht so einfach umsetzbar wie in Bürogeräten.

Ein risikobasiertes Informationssicherheitsmanagementsystem (ISMS), das diese Faktoren berücksichtigt und den Umgang mit verbleibenden Risiken wirksam steuert, ist daher auch für Smart-Factory-Betreiber unumgänglich. ■

FOTO: MILAN MALKOMES