Operational Technology (OT) und IoT richtig absichern

Cybersecurity

Cyberkriminelle haben OT und IoT als lukrative Angriffsziele entdeckt. Viele Betriebe sind auf die Bedrohung nur wenig vorbereitet. Ein strukturiertes Vorgehen hilft, Risiken zu minimieren.

Von Christian Koch, NTT Data

Angriffe auf Wasserversorgungssysteme, manipulierte Mischungsverhältnisse von Medikamenten bei Pharmaunternehmen, Ausfälle der Anzeigetafeln im öffentlichen Nahverkehr: Hacker entdecken zunehmend die Operational Technology (OT) und das Internet der Dinge (IoT) als lukratives Angriffsziel. Während den meisten Menschen inzwischen klar ist, dass sie nicht auf dubiose Mails voller Rechtschreibfehler klicken sollten, sind Maschinen und Anlagen oft ungeschützt.

Lange Zeit hatten Cyberkriminelle kein Interesse an OT, weil Produktionsanlagen oder Versorgungssysteme für Strom, Wasser und Gas nicht mit anderen IT-Systemen verbunden waren und sie so kaum Schäden anrichten konnten oder Angriffe sehr komplex waren.

Vernetzte Produktion lockt Kriminelle

Die Fertigungsindustrie digitalisiert ihre Geschäftsprozesse entlang der gesamten Wertschöpfungskette, von der Virtualisierung im Produktentstehungsprozess über flexiblere Service- und Geschäftsmodelle bis zu neuen Herstellungsverfahren wie Additive Manufacturing. Durch die Anbindung der Produktionsanlagen und Maschinen an interne Systeme zur Produktionssteuerung oder immer mehr auch an die Cloud steigt das Risiko für Malware und Cyberangriffe. Dabei versuchen die Cyberkriminellen, eine Anlage zu stören und Lösegeld zu erpressen oder im Auftrag von meist ausländischen Wettbewerbern oder Staaten an Betriebsgeheimnisse zu kommen. Dann tauchen Monate später Kopien von Autoersatzteilen auf, die nicht einmal ein Servicetechniker vom Original unterscheiden kann.

Dass die Sicherheit von OT dem Stand in der IT so weit hinterherhinkt, liegt daran, dass OT von Ingenieuren geplant wird, die fachliche Anforderungen der Produktion unter Kostendruck und in kurzer Zeit umsetzen müssen, für die aber in der Vergangenheit Cybersecurity nie ein Thema war. Sie entwickeln eine Anlage rein nach funktionalen Gesichtspunkten.

Bei neuen Risiken durch Cybersecurity müsste die Software der Anlagen eigentlich gepatcht werden. Doch das ist in der OT normalerweise nicht vorgesehen. Never touch a running system, gilt in der OT noch mehr als in der IT. Meist ist auch keine Zeit, um Patches aufzuspielen. Selbst wenn das Update vielleicht nur einige Minuten dauert, kann es zum Stillstand einer ganzen Produktion führen und ein langwieriges Wiederanfahren nach sich ziehen, insbesondere da meist auch Funktionstests nötig sind. Also muss man auf ohnehin geplante Wartungsfenster ausweichen, die aber selten sind. In Anlagen der chemischen Produktion etwa kann es mehrere Jahre dauern, bis sich einmal die Gelegenheit für ein Update inklusive aller funktionalen Tests ergibt.

Als Komplementärmaßnahme empfiehlt sich oft als Erstes eine Netzwerksegmentierung. Dabei trennt man Teile einer Anlage je nach Risikolevel und Kritikalität von anderen Systemen ab. Hierzu müssen der Detailaufbau und die Kommunikation der Anlage bekannt sein. Es empfiehlt sich, auch Altsysteme, die manchmal Jahrzehnte alt sein können und für die es keine Updates mehr gibt, von neuen Teilen zu trennen und separate Sicherheitsstrategien anzuwenden. Doch nicht nur Hersteller und Betreiber einer Anlage sind gefordert, für eine hohe Security müssen auch die Instandhalter mit im Boot sein. Bei Fernwartung greifen sie über eine VPN-Verbindung meist auf einen Jump-Server zu. Über solche Verbindungen gelingt es Hackern hin und wieder, Schad- und Spionagesoftware zu platzieren, die dann ganze Anlagen und Werke befallen kann, insbesondere wenn der Zugriff auf den Jump-Server oder die VPN-Authentifizierung nur schwach geschützt ist. Um solche Risiken zu vermindern, braucht es eine bessere Architektur. Manche Security-Dienstleister empfehlen dazu ein Audit mit einem Penetration Test, das Schwachstellen in der IT- und OT-Infrastruktur aufdecken soll. Vermutlich findet man jede Menge Schwachstellen, doch der Erkenntnisgewinn ist gering, insbesondere wenn keine Security in die OT-Systeme implementiert wurde. Viel besser ist es, erst einmal Maßnahmen umzusetzen und diese dann mit einem Audit zu prüfen. Startpunkt für eine bessere OT-Security ist eine höhere Sichtbarkeit in den OT-Netzen. Oft wissen die Unternehmen gar nicht, welche Detailkomponenten sie in den Anlagen haben, welche Softwareversionen sie nutzen, welche Daten sie austauschen und welche Verbindungen nach außen zu Drittfirmen bestehen. Doch was nicht bekannt ist, kann man auch nicht schützen. Die Kenntnis der eingesetzten Software-Versionen, Kommunikationsbeziehungen, externen Zugriffe, Zonierungen im Netzwerk und einiges mehr ist die Grundlage jeder Cybersecurity-Strategie.

Viele Unternehmen, die nach Unterstützung für OT-Security fragen, haben bereits einen Sicherheitsvorfall hinter sich oder kennen Unternehmen in ihrem Umfeld, die so einen Vorfall hatten. Das Bewusstsein ist in den vergangenen Jahren gestiegen und die Unternehmen sind motiviert, mehr für die Security zu tun. Die Unternehmen fühlen sich allerdings oft überfordert und wissen nicht, wo sie beginnen sollen. Hier ist ein strukturiertes Vorgehen gefragt, das dem Unternehmen Orientierung gibt.

Christian Koch, Vice President Cybersecurity und Lead für IoT/OT bei NTT Data.

Beachten Sie den Eintrag Community-Info – Seite 91