LANline

10,– €
September 2021
26. August

IT Network Datacenter www.lanline.de

Hybrid/Multi-Cloud-Vernetzung

Secure Access Service Edge

Out-of-Band-Verwaltung für das SD-WAN

Cloud-basiertes Netzwerk-Management

Mit Marktübersicht SD-WAN-Lösungen

Cisco Meraki Go Set im Test
Wireless-Lösung für das KMU

Sicherheit beim Edge Computing
Größerer Blickwinkel gegen diffuse Sicht

Backup und Archivieru
Mit Mar
Back

Sonderdruck NTT Data

September 2021

Cybersecurity: OT und IT im Gleichschritt

Know-how bündeln

Cyberkriminelle haben die Operational Technology (OT) als lukratives Angriffsziel entdeckt. Viele Betriebe sind auf die Bedrohung nur wenig vorbereitet. Dies gilt vor allem, weil IT- und OT-Verantwortliche unterschiedliche Sichtweisen haben.

Es kann jeden treffen – im Mai war Colonial Pipeline dran, der Betreiber der größten Treibstoff-Pipeline in den USA. Hacker platzierten eine Schadsoftware, die die Computersysteme verschlüsselte und den Betrieb der Pipeline störte. Damit hatten sie Erfolg. Colonial zahlte fünf Millionen Dollar, damit die Angreifer das System wieder entsperrten.

Angriffe mit Ransomware oder anderen Strategien auf Industrieanlagen oder kritische Infrastrukturen passieren täglich, und sie dürften häufiger werden. Die Industrie 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.

Verfügbarkeit ist alles

Noch etwas spielt den Angreifern in die Hände: Zwischen den Verantwortlichen für IT und OT gibt es in vielen Unternehmen eine tiefe Kluft, der eine versteht nicht, was der andere sagt und umgekehrt. Dies beginnt damit, dass IT- und OT-Verantwortliche die drei Säulen von Cybersecurity – Verfügbarkeit, Integrität, Vertraulichkeit – unterschiedlich gewichten. Während für IT-Experten die Vertraulichkeit einen hohen Stellenwert genießt, ist sie den Verantwortlichen im Produktionsumfeld ziemlich gleichgültig. Für sie zählen nur drei Aspekte: Verfügbarkeit, Verfügbarkeit und Verfügbarkeit. Die Produktion darf niemals stillstehen, außer in geplanten Wartungsfenstern, die bei Anlagen in der Prozessindustrie, also bei der kontinuierlichen Fertigung etwa von Chemikalien, nur alle paar Jahre anstehen. Die Maxime aus der IT-Welt, Patches möglichst schnell innerhalb von Tagen einzuspielen, ist deshalb bei Produktionsleuten völlig unbekannt.

Dennoch ist den Beteiligten bewusst, dass dies nicht für immer so bleiben kann. Schließlich hat sich durch die Vernetzung von Maschinen untereinander und zunehmend über die Automatisierungspyramide hinweg mit der Office-IT die Angriffsfläche vergrößert, ebenso das Risiko, sich Malware einzufangen, die sich durch das Netzwerk gräbt. An dieser Stelle gibt es die nächste Diskrepanz. Wenn die IT von Vernetzung spricht, meint sie meist sternförmige Netzwerktopologien, die von Switches koordiniert werden. Dort sind Anbieter wie Cisco, HP oder Fortinet die Platzhirsche. Anders in der OT: Dort dominieren Ringtopologien, Feldbusse und Echtzeit-Netzwerke. Den Markt dominieren Siemens, Hirschmann, Phoenix-Contact und andere, mit denen die IT selten zu tun hat. Die Vorliebe für Ringtopologien in der OT rührt daher, dass dort Latenzen und natürlich die Verfügbarkeitsanforderungen sehr kritisch sind. Der Datenaustausch etwa mit einem Roboter muss auf Millisekunden genau sein, Laufzeitverzögerungen können ihn aus dem Takt bringen. IT- und OT-Experten sprechen also eine unterschiedliche Sprache und haben völlig unterschiedliche Vorstellungen von der Cybersecurity. Angesichts zunehmender Attacken etwa mit Ransomware fühlen sich die IT-Leute in Unternehmen in der Pflicht, ihren OT-Kollegen die Gefahren zu erklären und Lösungsvorschläge zu machen. Dies kann von ihnen jedoch schnell als oberlehrerhaft aufgefasst und abgeblockt werden. Das Totschlagargument der OT lautet dann: Die Produktion sorgt für den Umsatz des Unternehmens, nicht die IT.

Unterschiedliche Sprachen

Um den Knoten zu durchschlagen, richten einige Unternehmen Schnittstelleneinheiten ein, die zwischen IT und OT vermitteln. Erfahrungsgemäß funktioniert dies meist gut. In solchen Zirkeln müssen beide Seiten aufeinander zugehen. Die OT muss sich öffnen und ihr Know-how preisgeben. Die IT muss die funktionale Sichtweise der OT akzeptieren und ihr Know-how entsprechend anpassen. Wenn die OT zum Beispiel einen Server aufsetzt, sollte sie die IT dazu holen und ein Sicherheitskonzept erstellen, das für beide passt und bei dem die IT-Kollegen nicht die Hände über dem Kopf zusammenschlagen.

Die IT und die Security-Abteilungen können auch ein wichtiger Partner sein bei Verhandlungen mit den Lieferanten von Steuerungen und Anlagen. Fragt man OT-Leute, warum sie eine Anlage so und nicht anders vernetzen, kommt als Antwort meist: Weil es der Hersteller so vorgibt oder man es immer schon so gemacht hat. Angesichts neuer Bedrohungen ist dies jedoch unbefriedigend. Die IT kann kritisch hinterfragen und die Hersteller zusammen mit dem Einkauf dazu verpflichten, mehr für eine moderne Cybersicherheit zu tun, damit sich die OT-Kollegen nichts aufzwingen lassen.

Malware schon bei Auslieferung

Dies gelingt allerdings leider nicht immer. Bei Spezialanlagen gibt es mitunter nur einen Anbieter und der Betreiber hat keine Wahl, was gefährlich sein kann. Es gab

Fälle, bei denen sich Malware bereits vor Auslieferung in einer Maschine eingenistet hatte. Abhilfe schaffen Lösungen, die Anlagen vor Inbetriebnahme überprüfen und die das Normalverhalten der Anlage überwachen und Alarm schlagen, wenn es zu verdächtigen Abweichungen kommt.

Dies greift dann jedoch nur bei neuen Anlagen. Was macht man mit den alten Maschinen, die oft 20 Jahre oder länger ihren Dienst tun und nun plötzlich zur Vernetzung nachgerüstet werden? Dann empfiehlt sich eine Netzwerksegmentierung. Dabei trennt man Teile einer Produktion je nach Risikolevel, Kritikalität und Betriebsmodell von anderen Systemen ab und wendet separate Sicherheitsstrategien an. Dazu müssen der Aufbau im Detail und die Kommunikation der Anlage bekannt sein.

Nicht nur Hersteller und Betreiber einer Anlage sind gefordert. Für eine hohe Security müssen vielmehr auch die Instandhalter mit ins Boot. Bei Fernwartung greifen sie über eine VPN-Verbindung meist auf einen Jump-Server zu. Über solche Verbindungen gelingt es Hackern bisweilen, 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, ist eine bessere Architektur nötig. Aber wie könnte die aussehen? Manche Security-Dienstleister empfehlen dazu ein Audit mit einem Penetrationstest, der 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 ist. Viel besser ist es, erst einmal Basismaßnahmen umzusetzen und diese dann mit einem Audit zu prüfen.

Nur schützen, was man kennt

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 Softwareversionen, Kommunikationsbeziehungen, externen Zugriffe, Zonierungen im Netzwerk und einiges mehr ist die Grundlage jeder Cybersecurity-Strategie. NTT Data empfiehlt zum Beispiel ein Cybersecurity-Framework, das aus vier Schritten besteht: technische Analyse, Bewertung, Umsetzung und Sicherung.

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 letzten 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. Dann ist ein strukturiertes Vorgehen gefragt, das dem Unternehmen Orientierung gibt. NTT Data erarbeitet mit dem Anwender zusammen ein Sicherheitskonzept, technische und organisatorische Lösungen und begleitet ihn später bei der Umsetzung und beim Betreiben der Sicherheitsmaßnahmen. Dabei geht es nicht um maximale Sicherheit, sondern um die für dieses Unternehmen passende Sicherheit. Viele Unternehmen denken dabei nur an Ransomware, die in den Medien großes Echo findet, vergessen jedoch, dass sie jede Menge Know-how haben, das für Wettbewerber interessant sein könnte. Vor allem das Wissen, wie man ein Produkt herstellt, ist mehr wert als viele denken. Dieses Wissen steckt in der OT, zum Beispiel in den Steuerungen.

Das Fazit lautet also: Cybersecurity in Produktionsanlagen ist kein optionales Feature, sondern ein absolutes Muss – und zum Glück auch kein Hexenwerk, wenn man sich an Grundregeln hält und mit kompetenten Partnern zusammenarbeitet.

Christian Koch/jos

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