Hacker in die Irre führen

Kernnetze mit „Defense in Depth“ schützen

Eine große Herausforderung ist der Schutz der Betriebstechnologie, deren bislang von der Außenwelt abgeschottete Netze sich im Zuge der Industrie 4.0 öffnen. Herkömmliche IT-Sicherheitsstrategien greifen hier nicht – stattdessen braucht es speziell auf die OT zugeschnittene Strategien, wie „Defense in Depth“ mit mehreren Sicherheitsschichten und fachmännisch konfigurierten Honeypots.

Von Andreas Baltes, KORAMIS – Cybersecurity by telent

Die Lage wird sich nicht entspannen. Im Gegenteil: Die Mehrheit der von der Bitkom befragten Unternehmen rechnet mit zunehmenden Cyberattacken. Besonders bedroht fühlen sich Betreiber kritscher Infrastrukturen und mittelgroße Unternehmen. Cyberkriminelle machen sich zunehmend den rasanten Fortschritt in der Digitalisierung zunutze, durch den die Betriebstechnologie (Operational Technology, OT) und die Informationstechnologie (IT) zusammenwachsen. In allen Branchen schreitet die digitale Transformation rapide voran und forciert damit die steigende IT/OT-Konvergenz. Immer mehr Geräte, Steuerungen und Industrieroboter sind mit Sensoren, Monitoren und weiteren digitalen Technologien ausgestattet, die Daten sammeln, auswerten und aufbereiten. Damit das gelingt, müssen sich die bislang in den Unternehmen separierten Netze der IT und OT verbinden. Über diese Schnittstelle öffnet sich das OT-Netz dem Internet, und damit steigen die Sicherheitsprobleme. Eine der Schwachstellen sind die vielen Endgeräte, die in OT-Umgebungen Daten unverschlüsselt über allgemein bekannte Industrieprotokolle austauschen. Sind Hacker erst einmal ins OT-Netz eingedrungen, macht die ungesicherte Kommunikation Manipulationen zum Kinderspiel. Die Folgen können weit über finanzielle Schäden hinausgehen. Denn die Hard- und Software der Betriebstechnologie steuert Abläufe etwa im Bereich des Verkehrsmanagements, der Wasserversorgung oder in den Fertigungen der Medizin- und Lebensmittelindustrie. Funktionieren diese Prozesse nicht mehr ordnungsgemäß, kann das sogar Menschenleben gefährden.

Die zunehmende IT/OT-Konvergenz eröffnet Cyberkrimiellen neue Schlupflöcher. Ganzheitliche Securitykonzepte minimieren die technischen Angriffsflächen und halten die Aufmerksamkeit für die Gefahren hoch.

Sorge vor Updates

Updates und Netzwerküberwachungen sind Bestandteil jeder IT-Sicherheitsstrategie. Doch diese Vorgehensweise lässt sich auf die Netzwerke der OT nicht so einfach übertragen. Das liegt vor allem daran, dass die Anlagenverfügbarkeit für Betreiber eine sehr hohe Priorität hat und sie deswegen im Bereich der Betriebstechnologie gern nach dem Motto verfahren: Never change a running system. Während sich bei der Büro-IT Updates regelmäßig automatisch aufpielen und sich Probleme relativ leicht beheben lassen, sieht das bei der oft jahrzehntealten Anlagentechnik anders aus. Hier existiert die nicht unberechtigte Sorge, dass ein Firmware-Update oder der Wechsel auf ein Übertragungsprotokoll mit höherer Datensicherheit, wie das feldbusbasierte Time-Triggered Protocol (TTP), zu größeren Beeinträchtigungen

führen kann. Würde beispielsweise nach einer Installation die Visualisierung auf einer Maschine nicht mehr reibungslos laufen, könnte sie nicht bedient werden und stünde im schlimmsten Fall still. Doch nichts zu tun ist angesichts der enormen Bedrohung durch kriminelle Attacken keine Alternative.

Schutz durch mehrere Schichten

Für eine effektive OT-Sicherheit müssen Sicherheitsverantwortliche andere Konzepte einsetzen, etwa „Defense in Depth“. Dieser bisher in der Praxis wenig genutzte Ansatz basiert auf der Idee, das Kernnetz durch mehrere spezialisierte Verteidigungsschichten zu schützen. In der ersten Ebene wird das Netz segmentiert; horizontal, indem das OT-Netz in mehrere Zonen unterteilt wird oder vertikal durch eine neutrale Zone zwischen OT- und IT-Netz. Dringen Cyberkrimielle ein, können sie nur auf einen Teilbereich zugreifen. Das kann Angriffe nicht hundertprozentig verhindern, aber da die Kommunikation der Segmente untereinander reglementiert ist, können Sicherheitsvorfälle eingedämmt und der Zugriff auf besonders schützenswerte, betriebskritische Assets bedeutend verringert werden.

Auf die Netzwerksegmentierung folgen industrielle Firewalls. Sie müssen allerdings funktional mehr leisten als in IT-Netzen. Die OT erfordert eine detailliertere Kontrolle, die beispielsweise Lesefunktionen für Daten zulässt, die mit einem bestimmten Protokoll übertragen werden, jedoch alle Schreibfunktionen für dasselbe Protokoll blockiert. Möglich ist das mit Deep Packet Inspection (DPI). Diese Methode, die in einer Firewall integriert oder separat laufen kann, untersucht den Inhalt von Datenpaketen vom Kopf bis zur Nutzlast und ermittelt auf diesem Weg das verwendete Protokoll und die damit einhergehenden Funktionen. Das ist die Basis für eine speziell auf OT zugeschnitte Cybersecurity-Strategie, die sich auf Eindringlinge im Netz fokussiert. Dabei deckt sie ein breites Spektrum ab von neu angeschlossenen Geräten über Malware-Verhalten bis hin zu unerwarteten SPS-Programmierungen. Die Strategie gibt es in zwei Varianten: Als Intrusion-Detection-System (IDS) löst es nach fest definierten Paramentern einen Einbruchalarm aus, wenn es annomale Daten erkennt. Ein Intrusion-Prevention-System (IPS) geht über die Angriffserkennung hinaus, indem es versucht Angriffe automatisiert und aktiv zu verhindern. Dazu kann es nicht autorisierte Datenpakete blockieren, Verbindungen unterbrechen oder übertragenene Daten abändern.

Gezielt attraktive Köder auslegen

Den immer ausgefeilteren Angriffsmethoden der Cyberkriminellen setzen Security-Experten intelligente Lösungen entgegen, wie „Honeypots“. Honigtöpfe sind Köder, die Angreifer gezielt anlocken, um sie in die Irre zu leiten. Konfiguriert werden sie als Hardware oder virtuelle Maschine, die absichtlich Sicherheitslücken aufweist. Denn erfahrungsgemäß scannen Hacker Netzwerke nach den anfälligsten Geräten, um darüber einzudringen. Da jeder Honeypot überwacht wird, lassen sich die IP-Adressen der Angreifer identifizieren und für das gesamte System blockieren. Daneben liefert jeder entdeckte Angriff wichtige Daten, wie Cyberangriffe verlaufen. Dieses Wissen ist Gold wert, um IT- und OT-Systeme zukünftig sicherer zu machen.

Mit einer mehr als 20-jährigen Erfahrung in der Automatisierungs-, Prozess- und Netzleittechnik sowie Industrial-Security und als zertifizierter Partner führender Anbieter von Sicherheitslösungen, wie Cisco und Fortinet, konzipiert telent Sicherheitslösungen für die speziellen Anforderungen in der OT-Welt. Ein maßgeschneidertes Konzept beginnt grundsätzlich mit dem Blick auf die Netzübersicht des Betreibers, die aufzeigt, ob es Segmentierungen gibt oder wo nachgebessert werden muss. Für alle systemrelevanten Anlagenbereiche, die über nicht sichere Protokolle miteinander kommunizieren, empfiehlt sich eine Firewall, die mit Bausteinen aus dem Konzept „Defense in Depth“ flankiert wird. Die Ausgestaltung ist letztlich immer individuell abhängig von den spezifischen Bedürfnissen eines Unternehmens und der vorhandenen Netzarchitektur.

Den Mensch in den Blick nehmen

Angesichts der digitalen Innovationen, durch die IT und OT immer mehr verschmelzen, und der permanent steigenden Cyberkriminalität, ist eines sicher: Eine ganzheitliche IT-/OT-Sicherheitsstrategie gegen externe und interne Bedrohungen ist zwingend notwendig. Dazu gehört auch, Cybersecurity nicht nur technisch zu denken, sondern den Faktor Mensch in den Blick zu nehmen. Diese „Angriffsfläche“ wird oft sträflich vernachlässigt. Dabei werden auch hier die Methoden der Angreifer immer versierter. Sie ziehen alle Register des Social Engineering und nutzen typisch menschliche Verhaltensmuster, wie Hilfsbereitschaft oder Ängste, aus. Regelmäßige Schulungen können die Aufmerksamkeit für derartige Gefahren trainieren.

Die Awareness beim Personal hochzuhalten, die Angriffsflächen technisch erheblich verringern und im Fall einer erfolgreichen Cyberattacke dafür Sorge tragen, dass diese erst einmal nur begrenzt wirksam ist – das sind Erfolg versprechende Faktoren, die in der Summe das Security-Niveau bedeutend heben, auch wenn IT und OT immer mehr zusammenwachsen.