Sicherheit durch Zwiebelschichten

Mit Defense in Depth OT-Netze vor Cyberangriffen schützen

Smarte Produktionsmaschinen und intelligente Steuerungen in kritischen Infrastrukturen sind oft schlecht gerüstet gegen Cyberangriffe. Ob Systeme mit veralteter Firmware oder im Internet frei zugängliche Bedienoberflächen – es gibt immer mehr eklatante Schwachstellen, die Cyberkriminelle geschickt ausnutzen. Sind Hacker erst einmal in ein OT-Netz eingedrungen, ist die Gefahr groß, denn noch besitzen die wenigsten Betriebe moderne Sicherheitsarchitekturen wie Defense in Depth. Das wie eine Zwiebel aufgebaute Konzept schützt das Kernnetz mit mehreren spezialisierten Verteidigungsschichten.

Das Risiko ist vor allem kleinen und mittelständischen Unternehmen ohne schlagkräftige IT-Abteilung oft nicht bewusst: Ihre betrieblichen Steuerungssysteme könnten ungesichert mit dem Internet verbunden sein – so wie Hunderte, die „Shodan" bereits gefunden hat. Die IoT-Suchmaschine durchforstet das Netz nach offenen Ports von Geräten, die permanent mit dem Internet verbunden sind, und legt die Ergebnisse in einer Datenbank ab. Darin kann jeder gezielt nach Schlagworten suchen, z. B. nach einem bestimmten SPS-Typ, und erhält zusätzlich Details wie Standort, IP-Adresse, Bestellnummer und Firmware. Diese Informationen nutzen Experten, um die Sicherheit der Netze zu erhöhen, aber eben auch Hacker. In Kombination mit Daten aus der Common Vulnerabilities and Exposures Datenbank (CVE), die häufige Schwachstellen bei Soft- und Hardware auflistet, können Kriminelle Sicherheitslücken gezielt aufspüren, etwa zu einer ungesicherten SPS. Diese lässt sich dann beispielsweise mit einem einfachen DDoS-Angriff in den Stop-Zustand versetzen.

Bild: ©katrinshine/stock.adobe.com

Verfügbarkeit im Fokus

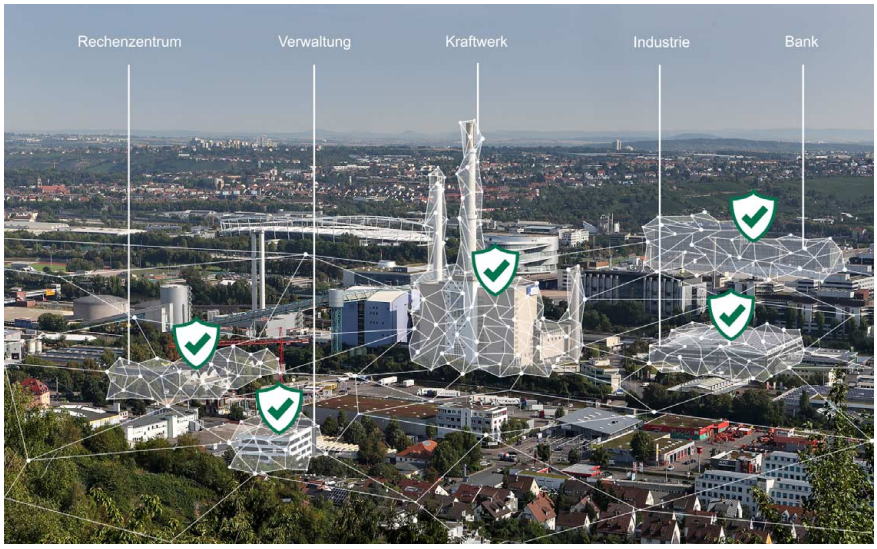
Durch die zunehmende IT/OT-Konvergenz verweben die Netze immer mehr miteinander. Darauf reagiert das Defense-in-Depth-Konzept, indem es weitere Sicherheitsschichten installiert – auch im OT-Bereich, der sich bisher bei der Sicherheit auf die physische räumliche Trennung seiner Komponenten verließ. Der erste Schritt, um Schwachstellen überhaupt zu entdecken, ist eine Gap-Analyse für einen transparenten Überblick über die technische Infrastruktur. Das ist kein leichtes Unterfangen in über Jahrzehnten gewachsenen Produktionslinien, die zumeist aus unterschiedlichen Technologiezeitaltern stammen. Hierin liegt auch die Ursache, warum viele Anlagen mit veralteter Firmware laufen.

Während in der IT-Welt regelmäßige Updates von Computern, Speicher oder Netzwerkgeräten eine Selbstverständlichkeit sind, stehen dieser bislang in der OT andere Prioritäten entgegen. Maschinenverfügbarkeit und Gesamtanlageneffektivität führen zu dem Motto: Never change a runnig system. Dahinter steht die nicht unberechtigte Sorge, dass Firmware-Updates oder der Wechsel auf ein Übertragungsprotokoll mit höherer Datensicherheit, wie das feldbusbasierte TTP (Time Triggerd Protocol), die Funktion älterer Anlagen beeinträchtigen oder sogar zum Stillstand bringen. Doch nichts zu tun ist angesichts der enormen Bedrohung keine Alternative. Es reicht eine über einen DDoS-Angriff gestoppte SPS, um eine Linie über Stunden lahmzulegen. Denn weder für Bediener, Techniker oder IT-Verantwortliche ist ein Hackerangriff auf Anhieb erkennbar, da die Ursache (bspw. DDoS) in der Meldungsanzeige oder der Diagnose in der SPS nicht aufgezeichnet wird. So muss erst einmal herausgefunden werden, warum die Technik nicht mehr läuft.

Kontrolliert bis ins Detail

Cyberangriffe können die Zwiebelschichten von Defense in Depth nicht hundertprozentig verhindern, aber sie erhöhen das Schutzniveau deutlich, etwa durch vertikale Netzwerksegmentierung.

Auszug aus dem SPS-MAGAZIN, Fachzeitschrift für Automatisierungstechnik, Ausgabe 05/2022.



Die fortschreitende IT/OT-Konvergenz eröffnet immer mehr Zugangspunkte für Cyberattacken.

Durch eine neutrale Zone, die das OT- vom IT-Netz trennt, erhalten eingedrungene Cyberkriminelle nur Zugriff auf einen Teilbereich. Industrielle Firewalls auf dem Stand der Technik übernehmen wie in IT-Netzen die Aufgabe, unerwünschten Datenverkehr außen vor zu halten, verschließen offene Ports und steuern gezielt den Datenverkehr.

Firewalls für Betriebstechnologien müssen allerdings mehr können als im Bereich der IT, z.B. auf einer bestimmten Maschine Lesefunktionen für Daten zulassen, die mit einem bestimmten Protokoll übertragen werden, jedoch alle Schreibfunktionen für dasselbe Protokoll blockieren. Eine derart detaillierte Kontrolle ermöglicht Deep Packet Inspection (DPI), indem sie den Inhalt von Datenpaketen vom Kopf bis zur Nutzlast untersucht und dadurch das verwendete Protokoll und die damit einhergehenden Funktionen ermittelt. Da Protokolle innerhalb der Netzwerke unverschlüsselt sind, können eingedrungene Hacker sie über einen Paket Sniffer wie Wireshark mitlesen, kopieren und etwa Boolsche Operanden oder Zahlenwerte einfach verändern. Ohne DPI bliebe das unentdeckt.

Hacker und Honeypots

Eine DPI ist zudem die Voraussetzung für die speziell auf OT zugeschnittene Cybersecurity-Strategien Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS). Ein IDS ist ein Netzüberwachungs- und Benachrichtigungs-Tool, das nach zuvor definierten Parametern einen Alarm auslöst. Ein IPS geht einen Schritt weiter und blockiert aktiv nicht autorisierte Datenpakte oder unterbricht Verbindungen. In den allermeisten Systemen sind IDS und IPS miteinander kombiniert und lassen sich wirksam von Honeypots flankieren. Die Honeypots sollen im Gegensatz zu IDS/IPS Hacker nicht abwehren, sondern bewusst anlocken. Sie täuschen ein attraktives Ziel vor, etwa eine SPS oder einen Server, werden als virtuelle Maschine in die Infrastruktur integriert und so konfiguriert, dass sie zwar leicht zu knacken sind, aber das echte OT-Netz keinesfalls in Mitleidenschaft ziehen. Da jegliche Kommunikation überwacht wird, kann im Fall eines Angriffs dieser zum Ursprung zurückverfolgt werden, etwa über die IP-Adresse, welche umgehend von der Firewall gesperrt wird. Die Überwachung liefert zudem Erkenntnisse über die Vorgehensweise von Cyberkriminellen. Dieses Wissen hilft Sicherheitsexperten dabei, Systeme besser zu schützen. Während Firewalls das Netzwerk nur nach außen absichern, eignen sich Honeypots auch dazu, interne Schwachstellen aufzudecken. In der Summe gelingt es durch die Vielzahl möglicher Schichten, ein für jedes Unternehmen maßgeschneidertes Security-Konzept für den OT- und den IT-Bereich aufzubauen, das Produktionsanlagen und die mit ihnen verbundenen Netze vor Sabotage, Spionage und Datendiebstahl wesentlich wirksamer schützt. ■

Andreas Baltes,
Security Solutions Consultant,
Koramis / Telent
www.telent.de