MODERNE SICHERHEITSARCHITEKTUREN SCHÜTZEN UNTERNEHMEN VOR HACKER-ANGRIFFEN

EINFALLSTOR SMART FACTORY

Ein Virus legt den Computer lahm. Nichts geht mehr. Cyberangriffe in industriellen Umgebungen können dramatische Folgen haben: Produktionsstillstand, Umsatzausfall, Image-Schaden. Denn durch die zunehmende Verschmelzung von klassischer IT und operativer OT erlangen Cyber-Kriminelle leichter Zugriff auf sensible Betriebs- und Prozessdaten. Konventionelle Firewalls helfen da längst nicht mehr weiter. Gefragt sind moderne Sicherheitsarchitekturen.

Rasend schnell vollzieht sich in nahezu allen Branchen die Entwicklung zur Smart Factory, zur intelligenten Produktionsstätte, die hochgradig digitalisiert und vernetzt ist und weitgehend autonom arbeitet. Neue Technologien verknüpfen nicht nur Anwendungen und Objekte über das Industrielle Internet of Things (IIoT) – sie befähigen Maschinen auch mittels Machine Learning und Künstlicher Intelligenz (KI), Daten zu analysieren, daraus zu „lernen“ und entsprechende Handlungsmuster abzuleiten.

Um den Produktions- bzw. Prozessverlauf steuern zu können, erfasst und bewertet die Smart Factory in Echtzeit Unmengen an Daten (Big Data), und zwar entlang der kompletten Prozesskette. In geschlossenen Systemen mit begrenzter Kapazität ist das kaum möglich, weshalb immer mehr Unternehmen in die Cloud umziehen. Die Cloud speichert wichtige Informationen wie Betriebsstunden, Fehlermeldungen oder Maschinenstatus, abrufbar über mobile Geräte zu jeder Zeit an jedem Ort.

DIE SMART FACTORY WIRD ZUM EINFALLSTOR

Während Verwaltungs- und Produktionsnetzwerke in der klassischen Fabrik voneinander getrennt operierten, verschmelzen IT und OT (Operational Technology) in der Smart Factory zu einem großen digitalen Netzwerk. Das erleichtert Hackern den Zugriff auf Produktionssysteme – mit fatalen Folgen, nicht nur für den Geschäftsbetrieb, sondern auch für die Reputation des Unternehmens. Herkömmlich Firewalls, wie sie in der IT-Welt üblich sind, stoßen in der OT an ihre Grenzen, und regelmäßige Updates, in Verwaltungsnetzwerken ein Routinevorgang, finden in den Produktionsnetzwerken häufig nicht statt – aus Sorge, die Maschinen könnten anschließend nicht mehr reibungslos funktionieren. Doch sind die Betriebsversionen von industriellen Steuerungen und Systemen veraltet, haben Hacker leichtes Spiel.

Vor allem kleinere und mittlere Unternehmen ohne schlagkräftige IT-Abteilung glauben häufig, ihre Produktion sei nicht mit dem Internet verbunden und deshalb sicher. Ein Trugschluss, den Hacker etwa für einen Distributed-Denial-of-Service-Angriff (DDoS), um eine speicherprogrammierbare Steuerung (SPS) zu stoppen und so eine ganze Fertigung lahmzulegen. SPSen finden sich beispielsweise in Roboterarmen. In Kombination mit IIoT-Sensoren, die über WiFi verbunden sind, steuern sie die Bewegungen des Roboterarms. Das Problem: Noch immer werden viele ungesicherte SPSen eingesetzt, die direkt mit dem Internet verbunden sind. Sie bieten Hackern ein gewaltiges Einfallstor, zumal sie über Datenbanken relativ leicht identifizierbar sind.

IT-SICHERHEITSGESETZ 2.0

Die Schäden, die der deutschen Wirtschaft durch Cyberangriffe entstehen, sind enorm. Sie beliefen sich im Jahr 2021 auf 220 Mrd. Euro, wie aus einer Studie des Branchenverbands Bitkom hervorgeht. Damit hat sich die Schadenssumme im Vergleich zu 2019 verdoppelt. Der Gesetzgeber hat die Gefahr erkannt und die Maßnahmen zum Schutz Kritischer Infrastruktur verschärft. Bisher galt das für die Bereiche Energie, Wasser, Ernährung sowie ITK. Mit dem im Juni vergangenen Jahres in Kraft getretenen neuen IT-Sicherheitsgesetzes 2.0 kommen Unternehmen aus der Abfallwirtschaft und solche von öffentlichem Interesse hinzu. Neben Rüstungsbetrieben sind das Firmen, die systemrelevant sind, sowie deren wichtigste Zulieferer. Dem Bundesamt für Sicherheit in der Informationstechnik erlaubt das Gesetz, Ports zu scannen, um bei Unternehmen Sicherheitslücken in der IT aufzuspüren.

Bilder: *Aufmacher Funtap – stock.adobe.com, Porträt telent*

»Cyberangriffe gehören mittlerweile zu den größten Risiken für das operative Geschäft. Um diese Gefahr mit aktuellen Sicherheitskonzepten zu minimieren, fehlt in vielen Unternehmen die notwendige Manpower. Diese Lücke füllen wir mit dem neuen Dienstleistungsangebot SOC-as-a-Service, in das unsere jahrzehntelange Erfahrung in Netztechnologien einfließt.“

Nico Werner, Head of Cybersecurity, telent GmbH

HACKER-ANGRIFFE ERKENNEN UND AUTOMATISCH ABWEHREN

Unternehmen sollten das Thema Cybersicherheit deshalb zur Chefsache machen und auf Nummer sicher gehen. Zum Beispiel, indem sie ihre OT-Netzwerke oder Netzwerkkomponenten wie Server oder Switches durch spezielle Security-Lösungen überwachen lassen. Deep Packet Inspection (DPI) ist eine solche Lösung, die die in einem Netzwerk übertragenen Datenpakete inspiziert und filtert, und zwar nicht nur deren Header, sondern auch die Nutzlast. In Kombination mit den Systemen Intrusion-Detection (IDS) und Intrusion-Prevention (IPS) kann DPI Hacker-Angriffe erkennen und automatisch abwehren. Während IDS verdächtige Aktivitäten und Vorfälle feststellt und meldet, ergreift IPS aktiv Gegenmaßnahmen, beispielsweise indem es Firewall-Regeln ändert und so den Zugriff auf das Unternehmensnetz blockiert. Die Funktionsweise von IDS basiert auf Signaturen, die bestimmte Muster erkennen, zum Beispiel Bytefolgen oder bekannte bösartige Befehlssequenzen, die von Malware verwendet werden. Eine weitere Möglichkeit, Cyberangriffe zu erkennen, ist das Anomalie-basierte IDS. Dabei werden mit Hilfe von Machine Learning vertrauenswürdige Aktivitäten protokolliert und davon abweichende Muster blockiert.

»IM JAHR 2021 BETRUGEN DIE SCHÄDEN DER DEUTSCHEN WIRTSCHAFT DURCH CYBERANGRIFFE RUND 220 MILLIARDEN EURO

SICHERHEITSRELEVANTE EREIGNISSE IM BLICK

IDS und IPS entsprechen den Vorgaben des neuen Sicherheitsgesetzes. Doch damit ist es nicht getan. Denn KRITIS-Betreiber müssen künftig auch sicherheitsrelevante Ereignisse überwachen, etwa mithilfe von Security-Incident-Event-Management-Systemen (SIEM). Das Software-Tool mit dem sperrigen Namen gibt bei Auffälligkeiten Fehlermeldungen ab. Voraussetzung ist, dass es richtig implementiert und betrieben wird. Kleineren und mittelständischen Betrieben fehlen aber häufig Personal und Expertenwissen, um Fehlermeldungen zu prüfen und daraus die richtigen Schlüsse zu ziehen. Unterstützung erhalten sie von Dienstleistern wie der telent GmbH, die mit eigenen Security Operation Center (SOC) Netzwerke von Unternehmen überwacht und aktiv nach Bedrohungen sucht. Ein SOC übernimmt dabei die Funktion einer „Kommandozentrale“, in der alle relevanten Informationen zusammenlaufen, um Sicherheitsvorfälle in IT- und OT-Umgebungen schnell zu erkennen und effektiv darauf zu reagieren. Hochspezialisierte Sicherheitsanalysten erkennen Bedrohungen nicht nur, sondern setzen ihr Know-how auch ein, um den Vorfall zu bewerten und im Falle eines Alarms die geeigneten Gegenmaßnahmen einzuleiten. So lassen sich IT und OT des betroffenen Unternehmens effektiv schützen.

www.telent.de

UNTERNEHMEN

telent GmbH
Gerberstraße 34, 71522 Backnang
Telefon: 07191 900-0
E-Mail: info.germany@telent.de

AUTOR

Nico Werner, Head of Cybersecurity bei der telent GmbH in Backnang