Foto: Telent GmbH

Auch kleine und mittelständische Unternehmen (KMU) verfügen inzwischen vielfach über IoT-basierte Systeme. Sie geraten so zunehmend in den Fokus von Cyberattacken.

IoT-Systeme in der Produktion

Auch in der industriellen Produktion werden IoT-Systeme zunehmend zu interessanten Zielen für kriminelle Hacker. Wie kann man die Fertigung und das Unternehmen schützen?

JAKOB SCHMIDT

Auch kleine und mittelständische Unternehmen (KMU) verfügen mittlerweile über IoT-Systeme, und in der Produktion über Know-how, welches sich lohnt auszuspähen. IoT-Geräte dienen Hackern dabei nicht selten als Hintertür, um auf das gesamte Netzwerk eines Unternehmens zuzugreifen. Direkt können die Angreifer nicht das System attackieren, da es durch ein Sicherheitssystem geschützt ist – bleibt also nur die Hintertür. Wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf seiner Website schreibt, wurden zum Beispiel Modelle von Überwachungskameras, die in Rechenzentren und Serverräumen eingesetzt werden, genutzt, um Bild- und Videodateien auszuspähen. Eine weitere Herausforderung für die Sicherheit von Netzwerken in Unternehmen sind sogenannte Distributed Denial of Service (DDoS)-Attacken. Dabei handelt es sich um eine absichtlich herbeigeführte Serverüberlastung. Bei einem DDoS-Angriff wird eine große Zahl infiltrierter Systeme, wie zum Beispiel IoT-Geräte, für einen Angriff auf ein einzelnes Ziel mobilisiert. Das Zielsystem kann diesen Ansturm meist nicht bewältigen, der Server bricht zusammen und Teile der Produktion kommen zum Stillstand.

Hinzu kommt die zunehmende Verschmelzung von IT- und OT-Umgebungen in Unternehmen. Klassische Informations-

„Die Auszüge aus dem ITSiG 2.0 zeigen, dass KMU einen strategischen Partner an ihrer Seite brauchen, der sie unterstützt und begleitet."

Jakob Schmidt, Coordinator Awareness, Koramis GmbH, ein Tochterunternehmen der Telent GmbH

technologien (Hard- und Software, Netzwerktechnik et cetera) und der OT-Bereich (Operational Technology, zum Beispiel zur Prozesssteuerung und Automatisierung) unterscheiden sich grundlegend in der Auslegung ihrer Kommunikation. Während sich herkömmliche IT auf Kommunikation und Vertraulichkeit fokussiert, sind in der Produktion insbesondere Verfügbarkeit und Safety wichtig. Durch die Vernetzung von Prozessen verschmelzen IT- und OT-Umgebungen miteinander, zum Beispiel. die Betriebs- und Steuertechnik.

Verglichen mit IT-Systemen für Bürokommunikation haben OT-Infrastrukturen eine längere Nutzungsdauer, müssen aber mit aktuellen Sicherheitsanforderungen kompatibel sein. So ist die Sicherheit von Hardware und Software längst ein wesentlicher Faktor bei der Entwicklung.
Zu den genannten Herausforderungen stellt auch der Gesetzgeber Anforderungen an die Absicherung von IoT-Komponenten. Das BSI hat im ITSiG 2.0 (Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) hierfür detaillierte Regulierungen festgelegt. Neben den Update-Funktionen, Authentisierung und der regelmäßigen Aktualisierung von Sensoren und Management-Systemen fordert er eine Einschränkung des Netzzugriffs durch ein eigenes Netzsegment. Bereits wenige Auszüge aus dem ITSiG 2.0 zeigen, dass kleine und mittelständische Unternehmen einen strategischen Partner an ihrer Seite brauchen, der sie bei der umfassenden Umsetzung unterstützt und begleitet.

Sicherheit als Managed Service

Managed Security ist der richtige Ansatz für eine kosteneffiziente, zukunftsorientierte Sicherheitsstrategie. Unter den Managed Services subsummieren sich Dienstleistungen aus dem IT-Bereich, die im Auftrag eines Unternehmens von einem Managed Services Provider (MSP) erbracht werden. Der große Vorteil hierbei: Der Provider kümmert sich um die wiederkehrenden IT-Services wie Netzwerkdienstleistungen, Anwendungen, Monitoring, Storage oder Security-Services, damit Unternehmen effizienter und wirtschaftlicher arbeiten können.

Mit der Unterstützung eines externen Spezialisten können mittelständische Unternehmen ein erweiterbares, bedarfsorientiertes Konzept aufstellen und sich als vertrauenswürdige Geschäftspartner positionieren. Der Systemintegrator Telent GmbH und seine auf Cybersecurity spezialisierte Tochter Koramis GmbH verfügen über umfangreiche Erfahrungen mit regulatorischen Verfahren und unterstützen ihre Kunden von der Schwachstellenanalyse über die Netzplanung mit Notfallkonzept bis zur Umsetzung von Managed-Security-Konzepten inklusive Echtzeitüberwachung.

Ihr Konzept von Managed Security umfasst verschiedene Maßnahmen wie Netzsegmentierung, Systemhärtung und Sandboxing. Sie wehren die tiefergehenden Gefahren von Hackerangriffen ab und schützen so vor Angriffsvektoren, die Sicherheitslücken bieten. Zur Netzsegmentierung werden die Netze des Unternehmens in Bereiche unterteilt, die so wenig wie möglich, und nur über klar definierte Zugänge, miteinander verbunden sind. Besonders kritische Anwendungen erhalten durch die Systemhärtung eine zusätzliche Stufe an Sicherheit. Beim sogenannten Sandboxing laufen Betriebssysteme und kritische Anwendungen komplett getrennt voneinander. Die getrennte Laufzeitumgebung ermöglicht den Weiterbetrieb einer Software oder eines Prozesses, auch wenn eine andere kritische Anwendung lahmgelegt wurde.

Überwachung mit SIEM und SOC

Die unternehmensspezifischen Lösungen für Managed Security umfassen Supportleistungen für den Schutz von IT-/OT-Umgebungen und individuelle Lösungen für Multi-Vendor-Umgebungen sowie SIEM-Tools. Dahinter verbergen sich die Konzepte von Security Information Management (SIM) und Security Event Management (SEM). Für die Echtzeitanalyse von Sicherheitsalarmen greifen SIEM-Tools auf Daten aus Anwendungen und Netzwerkkomponenten zurück, kombinieren sie und erhöhen so die Sicherheit. Für das unternehmensspezifische Managed Security System wählen die Spezialisten von Telent einen Technologiemix aus Hard- und Software, maschinellem Lernen und Künstlicher Intelligenz (KI), um den Datenfluss lückenlos zu überwachen. ■

telent GmbH:
www.telent.de

KORAMIS GmbH:
www.koramis.de