Cybersecurity für IT-kritische Infrastrukturen

Artikel vom **15. Juni 2021**
Wissenstransfer

In kleinen und mittelständischen Unternehmen (KMU) übernehmen IoT-Systeme in der Fabrik mittlerweile wichtige Aufgaben in der Steuerung, Überwachung und Datenverarbeitung. Als entscheidender Baustein der Produktion werden sie so zu interessanten Zielen für kriminelle Hacker. Wie kann man die Fertigung und das Unternehmen schützen?

Cybersecurity dient dem Schutz von industriellen Systemen und Infrastrukturen vor aktuellen und zukünftigen Bedrohungen (Bild: Koramis by telent GmbH).

Auch KMU verfügen 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 das System nicht 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 beschreibt, 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 Informationstechnologien (Hard- und Software, Netzwerktechnik etc.) und der OT-Bereich (Operational Technology, z. B. 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 Sicherheit wichtig. Durch die Vernetzung von Prozessen verschmelzen IT- und OT-Umgebungen wie die Betriebs- und Steuertechnik miteinander. 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. **Update-Funktion und Netzsegmente sind rechtliche Vorgaben** Zu den genannten Herausforderungen setzt 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 Managementsystemen fordert er eine Einschränkung des Netzzugriffs durch ein eigenes Netzsegment. Dezidierte Sicherheitsrichtlinien als Arbeitsanweisung für Mitarbeiter gehören für das BSI ebenso zu den Schutzmaßnahmen, wie eine verschlüsselte Datenübertragung, Netzwerküberwachung, die Protokollierung sicherheitsrelevanter Ereignisse sowie der Schutz der Administrationsschnittstelle. Bereits diese 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 Auf-trag 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. Besonders für kleine und mittelständische Firmen ist das eine passende Lösung, da es dort häufig an Ressourcen und Fachkräften für spezifische Sicherheitsmaßnahmen fehlt. 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 Betriebssystem und kritische Anwendungen komplett getrennt voneinander. Die getrennte Laufzeitumgebung ermöglicht den Weiterbetrieb einer Software oder eines Prozesses, auch wenn eine andere kritische Anwendung durch Angreifer vorübergehend lahmgelegt wurde. Zudem schützt Sandboxing vor Zero-Day-Exploit-Attacken. Awareness-Trainings und -Kampagnen

ergänzen die technischen Maßnahmen, da sie die organisatorische Sicherheit bezüglich des Faktors Mensch erhöhen. **Kontinuierliche Sicherheitsüberwachung** 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 fortschrittlichen Technologiemix aus Hard- und Software, maschinellem Lernen und Künstlicher Intelligenz (KI), um den Datenfluss lückenlos zu überwachen. Zahlreiche detaillierte Korrelationsinformationen und Algorithmen lösen Alarme aus und weisen dank Echtzeitanalysen auf potenzielle Gefahren hin. Einen integrierten Schutz vor Bedrohungen während und nach einem Angriff bietet beispielsweise Cisco Firepower, die erste vollständig integrierte Next-Generation Firewall (NGFW) mit Unified Management. Firepower-Geräte unterstützen die Integration mit SIEM-Tools von Drittanbietern. Neben den technischen Lösungen empfiehlt sich ein Security Operation Center (SOC) – ein Expertenteam, das Netzwerke kontinuierlich überwacht, aktiv nach Bedrohungen sucht und diese ausschaltet. Das Managed-Security-Portfolio von telent beinhaltet üblicherweise die 24/7-Netzwerküberwachung mit Echtzeit-Alarmierung. Der integrierte Incident-Management-Workflow sorgt für die umgehende Behebung von Angriffen und Ausfällen. Ergänzt wird das individuelle Sicherheitskonzept für die KMU durch Netzwerkplattformen, die Analytics-Funktionen bereits in ihrer Architektur implementiert haben, wie etwa Cisco DNA (Distributed Network Architecture) und Cisco ISE (Identity Services Engine). Mit einer umfangreichen Umbrella-Funktion erlaubt Cisco ISE u. a. die richtliniengesteuerte Zugriffskontrolle in der gesamten Infrastruktur, was für maximale Sicherheit vom Kabel- über das Wireless- bis hin zum VPN-Netzwerk sorgt. Das zentrale Management bringt einen transparenten Überblick über Benutzer und Geräte im Netzwerk und erhöht die Systemsicherheit.

Hersteller aus dieser Kategorie
