Blick über den Tellerrand

Technikalternativen für sichere Firmennetze

Reinhard Wegener

Gemischte IT/OT-Architekturen, der Mangel an Fachkräften insbesondere für Security-Themen und die verschärfte Bedrohungslage machen es immer anspruchsvoller, industrielle Datennetze und ihre Anwendungen sicher zu betreiben. Deswegen lohnt ein Blick über den Tellerrand auf Techniken, die bislang in Firmennetzen noch selten eingesetzt werden, wie SDN oder 5G. Sie helfen, viele der Herausforderungen zu meistern, erfordern jedoch auch die Bereitschaft, neue Wege in Planung und Betrieb zu gehen.

Systeme der OT sind der entscheidende Treiber für den Aufbau privater 5G-Campusnetze: Jedoch dürfen OT-Vernetzungen nicht länger als isolierte, automatisierungstechnische Einzelmaßnahme betrachtet werden

Vernetzte Produktionsanlagen, Echtzeitkommunikation zwischen Maschinen, intelligente Roboter: 55 % der Industrieunternehmen mit mehr als hundert Beschäftigten nutzten im vergangenen Jahr spezielle Industrie-4.0-Anwendungen, weitere 25 % planten laut Bitkom-Studie, sie einzusetzen. Das hat zur Folge, dass immer mehr Geräte der Betriebstechnik (Operational Technology – OT) vernetzt und an das betriebliche IT-Netz einschließlich der Cloud angeschlossen werden. Somit begegnen sich zwei Technikwelten, deren Sicherheitsarchitektur im Fall der OT nicht selten noch im Entstehen ist. Neben einzelnen Industriebranchen sind vor allem Betreiber kritischer Infrastrukturen (Kritis) bereits seit vielen Jahren gezwungen, ganzheitlich auch die OT als prägende Anforderung zu berücksichtigen.

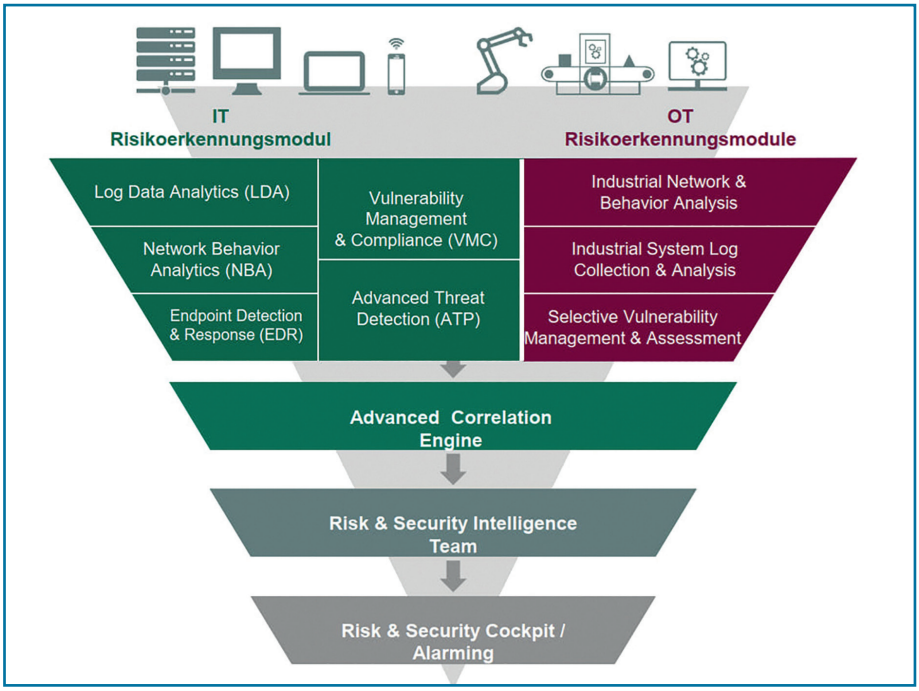
In Zeiten von Industrie 4.0 gilt nicht nur für Kritis, sondern für alle Produktionsbetriebe: Sichere, leistungsfähige Datennetze sind die Grundlage für erfolgreiche Digitalisierung und unternehmerische Wettbewerbsfähigkeit. Wenn in Smart Factories Verwaltungs- und Produktionsnetze zu einer digitalen Plattform verschmelzen, müssen die ursprünglich in sich geschlossenen Netze der sensiblen Fertigungsbereiche anders geschützt werden. Klassische Netzsegmentierung mit Firewalls ist weiterhin eine notwendige, aber keine hinreichende Maßnahme mehr und die Grundanforderung regelmäßiger Sicherheitsupdates – sofern noch erhältlich – findet in Produktionsnetzen häufig nicht statt aus Sorge, die Maschinen könnten anschließend nicht mehr reibungslos funktionieren. Doch mit veralteten Softwareversionen haben Cyberkriminelle leichtes Spiel, sobald sie ins Netz eingedrungen sind.

Dr.-Ing. Reinhard Wegener ist Director Technology Center bei der Telent GmbH

Zusätzliches Fachwissen nötig

Um Projekte in gemischten IT/OT-Umgebungen erfolgreich umzusetzen, dürfen OT-Vernetzungen nicht länger als isolierte, automatisierungstechnische Einzelmaßnahme betrachtet werden, sondern im Verbund mit allen funktionskritischen Systemen, Komponenten und Prozessen. Dafür braucht es Transparenz, die eine Inventarisierung aller IT/OT-Assets mit Eigenschaften wie Firmware-Version, Protokolle und Kommunikationsverbindungen liefert. Eine umfassende Erhebung ist die Voraussetzung, um geeignete Systeme, etwa zur Angriffserkennung und -abwehr, auswählen zu können. Für unternehmensinterne IT-Abteilungen ist die zunehmende IT/OT-Konvergenz herausfordernd, denn sie brauchen Know-how in neuen Techniken, um hinsichtlich Funktionalität, Betreibbarkeit und Cybersecurity die richtigen Konzepte und Maßnahmen zu wählen, ohne dass die IT-bezogenen Aufgaben zurückgehen. Mehr Fachwissen ist auch bei den vermeintlich separaten infrastrukturellen und elektrotechnischen Themen sowie der Softwareintegration gefragt, da bei einer ganzheitlichen Herangehensweise bereits in der Konzeptphase die netztechnischen Anforderungen der prozessentscheidenden OT-Anwendungen analysiert werden und in das Netzdesign einfließen. Auf den Punkt gebracht: Unternehmen mit IT/OT-Landschaften benötigen mehr Fähigkeiten als bisher und müssen künftig mehr in Konzeptionsschritte investieren, so wie es Betreiber bzw. erfahrene Systemintegratoren im Bereich der kritischen Infrastrukturen seit jeher kennen.

Nicht zwangsläufig braucht es den großen Schnitt, um IT/OT-Netze sicherer und leistungsfähiger zu gestalten. Die technische Weiterentwicklung zu Software Defined Networking (SDN) ist eine bislang auf dem Firmencampus noch selten eingesetzte Option, die alte Paradigmen durch ein neues Konzept ersetzt. Im Gegensatz zur traditionellen Netzarchitektur, bei der einzelne Geräte Entscheidungen über den Datenverkehr treffen, zentralisiert SDN die Intelligenz in einer Komponente, dem sogenannten SDN-Controller. Das Netzmanagement wird damit einfacher, da Administratoren das gesamte Netz von einem Punkt aus überblicken und verwalten können. Zudem lassen sich wiederkehrende Aufgaben, wie Konfigurationen und Updates, automatisieren. Das spart Zeit, Kosten und minimiert das Risiko menschlicher Fehler. Mehr Schutz gewährleistet ein SDN-Controller auch, indem er Sicherheitsregeln (Policies) konsistent über die gesamte Infrastruktur ausrollt und das Gesamtnetz feingranular segmentiert mithilfe von virtuellen Netzen, die eine uni- oder bidirektionale Kommunikation in verschiedene Bereichen erlauben oder unterbinden. Das ist relevant beispielsweise für die Sicherheit eines Flughafens, bei dem OT-Systeme wie Gepäckkontrolle, Enteisungsanlagen oder Kraftstoffpumpen über die IT-Architektur verwaltet werden. Dass etwa ein mit Malware befallenes Tablet eines Passagiers keinesfalls mit der kritischen Infrastruktur kommunizieren kann, ist selbstverständlich, aber der Anspruch geht viel weiter. Wie sieht es mit dem Laptop eines Servicetechnikers aus? Hier trennt und steuert SDN über die zentrale Instanz kritische von unkritischen Datenströmen. Cyberrisiken können durch permanentes Monitoring des Netzes frühzeitig erkannt und Gegenmaßnahmen eingeleitet werden.



Die Aufgaben eines Security Operation Center (SOC) reichen von der Risikoerkennung über erweiterte Korrelation der verschiedenen Analyseergebnisse bis hin zur adäquaten Reaktion auf Sicherheitsbedrohungen (Bilder: Telent)

Sicherheit der Gesamtlösung

5G ist ein weiteres Beispiel einer nicht grundsätzlich neuen, aber in privaten Gebäuden und Anlagen noch kaum in Produktivumgebungen eingesetzten Technik. Die typischen Schlüsselmerkmale des Mobilfunkstandards – hohe Bandbreite, große Endgerätedichte und besonders die kurze Latenz – bieten Unternehmen die Chance, ihre Digitalisierung massiv voranzutreiben. Industrielle Anlagen, selbst mit sicherheitsrelevanten Bestandteilen, lassen sich mit 5G drahtlos vernetzen und ohne Verkabelungsaufwand an wechselnde Anforderungen anpassen. Seine Spezifikationen machen 5G zum derzeit sichersten Mobilfunkstandard, kombiniert mit der Option der vollständigen „Funktionsherr-

schaft“, unter der Produktionsdaten das eigene Firmengelände nicht verlassen. Zu Recht verweist die Mobilfunktechnik auf über viele Generationen immer wieder verbesserte Sicherheitsmerkmale bei der Funkübertragung. Doch eine Kette ist nur so stark wie ihr schwächstes Glied.

Es können sich für Kriminelle auch Einfallstore öffnen, wenn unzureichend abgesicherte IoT-Endgeräte über 5G-Technik vernetzt werden. Ob Man-in-the-Middle-Attacken unverschlüsselte Kommunikation abgefangen, Denial-of-Service-Angriffe die Infrastruktur mit Anfragen überlasten oder bösartiger Datenverkehr Geräte infiziert – Cyberaktivitäten, die im weltweiten Netz funktionieren, gelingen ebenso auf Campusebene. Im Gegensatz zu den Anforderungen an die öffentlichen Netze der großen Telekommunikationsanbieter hat der Gesetzgeber keine vergleichbare Regulierung für private Campusnetze vorgegeben. Das verschafft den Betreibern bzw. Nutzern einen größeren Gestaltungsspielraum bei Technik und betrieblichen Prozessen, erhöht andererseits ihre eigene Verantwortung. Um dem gerecht zu werden, braucht es gleichermaßen hohen Sachverstand und viel Erfahrung im Bereich der Netztechnik wie der IT/OT-Sicherheit.

In puncto Sicherheit hat aus Unternehmenssicht die Integration des 5G-Netzes in die bestehenden IT/OT-Netze hohe Priorität. Um Angriffen vorzubeugen, müssen von Anfang an Sicherheitsstrategien etabliert und Maßnahmen wie das Absichern der Teilnehmer, Ende-zu-Ende-Verschlüsselungen und Netzsegmentierungen zuverlässig umgesetzt werden. Je höher die Messlatte gelegt wird, desto arbeitsintensiver wird die Konfiguration. Denn ein 5G-Campusnetz lässt sich sehr sicher gestalten, aber es ist mit Aufwand verbunden. Ein Beispiel für einen bewährten Sicherheitsmechanismus des Mobilfunks, der so im LAN bzw. WLAN nicht existiert, ist die eindeutige Authentifizierung durch SIM-Karten bzw. eSIM. Das funktioniert aber nur, wenn zuvor alle Komponenten und Endgeräte sauber zertifiziert und ein sicherer Provisionierungsprozess etabliert wurde. Zu beachten ist, ob die oft Jahrzehnte alten Maschinen und Steuerungen leistungsfähig genug sind, um z.B. moderne Ende-zu-Ende-Verschlüsselungen abzuarbeiten. Die dafür erforderlichen Operationen benötigen ein Mindestmaß an Rechenleistung, das viele OT-Geräte nicht besitzen. Damit die Endgeräte als Quelle der Daten, die über 5G transportiert werden, nicht einfach für Cyberkriminelle zu knacken sind, müssen sie vor dem Anschluss gehärtet werden. Das wiederum erfordert individuelle Maßnahmen, wie etwa ein abgeschottetes Mininetz, das eine Steuerung einhegt.

Verantwortung übertragen

Kritis-Betreiber sind ab Mai 2023 gesetzlich verpflichtet, ihre IT/OT-Umgebung mit einer wirksamen Angriffserkennung gegen Cyberkriminalität zu schützen, z.B. mit einer Kombination von Intrusion Detection System (IDS) und Intrusion Prevention System (IPS). Zu deren wesentlichen Aufgaben gehören die Protokollierung, Detektion und Reaktion. Ein auf die OT spezialisiertes IDS/IPS versteht die Sprache der proprietären Protokolle der Anlagen und Steuerungen. Dadurch ist es in der Lage, sowohl Angriffe als auch Fehlkonfigurationen aufgrund menschlichen Versagens zu erkennen, im Verdachtsfall zu alarmieren oder nicht autorisierte Datenpakete zu blockieren.

Angesichts der steigenden Cyberkriminalität ist auch für Unternehmen außerhalb von Kritis eine ganzheitliche IT/OT-Sicherheitsstrategie gegen externe und interne Bedrohungen unbedingt ratsam. Diese zusätzliche Aufgabe werden in mittelständischen Unternehmen viele betriebsinterne IT-Teams personell und kompetenzmäßig kaum stemmen können. Wollen sie ihre Netze zukunftsfähig halten, können sie Verantwortung für bestimmte Bereiche, z.B. die OT-Netzbetreuung, die 5G-Funkinfrastruktur oder eben Elemente der Cybersecurity, abgeben.

In einem Security Operation Center (SOC) laufen alle Fäden zur Cybersecurity zusammen. Die leistungsfähige Einheit vereint Prozesse, Techniken und Experten zu einem integrierten Angebot. Ein effektives Überwachungs-Tool, das im SOC tätige Experten einsetzen, ist ein Security-Incident-Event-Management-System (SIEM). Es erhält von zahlreichen Datenkollektoren Informationen, bereinigt diese zu einem sogenannten normalisierten Stream und alarmiert bei Auffälligkeiten, wie Systemanomalien und Anzeichen eines Hackerangriffs. In der Praxis gibt es zahlreiche Fehlermeldungen, die das SOC-Team dezidiert auswerten und verifizieren muss, um zielgerichtet reagieren zu können. Ein optimales Schutzniveau lässt sich auch über ein externes SOC-as-a-Service eines spezialisierten Dienstleisters erreichen.

Erfahrungsgemäß funktioniert die Zusammenarbeit am besten, wenn die Arbeitsweise des externen Anbieters maßgeschneidert für den Kunden ist. Dazu gehört u.a., die Prozesse gemeinsam zu definieren, im Zuge der Zusammenarbeit eine enge prozessuale Vernetzung und Informationsbasis herzustellen sowie sie vom auslösenden Event bzw. der geplanten Maßnahme über aktuelle Zwischenstände bis zu Ergebnisberichten elektronisch abzubilden. Denn: Verantwortung übertragen soll im Ergebnis zu besserer Transparenz der betreuten Infrastruktur für alle verantwortlichen Beteiligen führen.

Der Blick über den Tellerrand zeigt: In der Summe gibt es viele technische und prozessuale Möglichkeiten, mit denen Unternehmen trotz immer komplexerer IT/OT-Landschaften, fehlendem Security-Personal und steigender Cyberkriminalität ihre Netzumgebungen sicherer gestalten können.