Investitionen in Konzepte als kritischer Faktor

Zukunftssichere Netze für unternehmenskritische Anwendungen auf dem Campus

ANDREAS ALBRECHT

Foto: Telent

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

Die IT und OT wachsen immer mehr zusammen, und immer mehr Unternehmen richten ihre Datennetze an Anforderungen aus, die man bislang eher aus den Kritischen Infrastrukturen kennt. Mit welchen Fähigkeiten und Technologien sie diese Aufgabe bewältigen, verrät Dr.-Ing. Reinhard Wegener, Director Technology Center bei der Telent GmbH im Gespräch.

Herr Dr. Wegener, warum ist das Zusammenwachsen von IT- und OT-Netzen so eine komplexe Aufgabe?

» Dr.-Ing. Reinhard Wegener: Einfach gesagt, weil zwei Technologiewelten aufeinanderprallen, die bislang strikt getrennt waren. Die IT dient dazu, Aufgaben im Büro zu erledigen. Sie ist mit dem Internet verbunden und nutzt allseits bekannte Umgebungen und Lösungen, wie Server, Clouds, Firewalls und Virenschutz. Zur Betriebstechnik, also der OT, gehören völlig andere Komponenten, wie Fertigungsmaschinen und Steuerungen. Sie kommunizieren über Industrieprotokolle miteinander, die in IT-Netzen unbekannt sind. Die OT kann nicht einfach die Sicherheitstools der IT verwenden, und das erschien in der Vergangenheit auch nicht als notwendig, da sie als ursprünglich in sich geschlossene Umgebung vor Cyberangriffen weitgehend abgeschirmt war.

Was ändert sich für die Betreiber?

» Dr.-Ing. Reinhard Wegener: Je weiter die digitale Vernetzung im Rahmen der Industrie 4.0 voranschreitet, umso stärker nimmt die Konvergenz von IT und OT zu. Damit Produktionsprozesse weiter zuverlässig und sicher laufen, sind in einer gemischten IT/OT-Umgebung höhere Anforderungen zu erfüllen. OT-Vernetzung wurde bislang oft in Einzelmaßnahmen und zu wenig in ganzheitlichen Konzepten gedacht. Für die betriebsinterne IT-Abteilung bedeutet das, ihre bisherigen Aufgaben bleiben bestehen, und es kommen neue hinzu.

Steigt nur die Menge an zusätzlichen Aufgaben?

» Dr.-Ing. Reinhard Wegener: Nein. Um ein Projekt mit OT-Charakter erfolgreich umzusetzen, braucht es vor allem mehr Kompetenzen, etwa zu infrastrukturellen und elektrotechnischen Themen oder der Softwareintegration. In der Konzeptphase müssen die netzwerktechnischen Anforderungen der prozessentscheidenden OT-Anwendungen analysiert werden und in das Netzdesign einfließen.

Unternehmen brauchen zudem Know-how in neuen Technologien, um hinsichtlich Funktionalität und Betreibbarkeit die richtige Auswahl zu treffen. Zudem wird Cyber-Security immer bedeutender. Um es auf den Punkt zu bringen: Unternehmen mit IT/OT-Landschaften benötigen mehr Fähigkeiten als bisher und müssen künftig mehr in die Konzeptionsschritte investieren, wie wir das als erfahrener Systemintegrator im Bereich der Kritischen Infrastrukturen seit jeher gewohnt sind.

Was ist im Kritis-Bereich anders?

» Dr.-Ing. Reinhard Wegener: Kritis bezeichnet ja Infrastrukturen, die für die Versorgung der Bevölkerung von hoher Bedeutung sind, wie die Energieversorgung oder der Schienenverkehr. In diesen Bereichen wurde die OT schon immer als prägende Anforderung mitberücksichtigt, da prozessgetriebene Anwendungen, etwa eine

Stellwerksvernetzung, essenziell für die Funktion der Betriebsmittel und somit die Sicherheit der Fahrgäste und des Personals sind.

Welche neuen Anforderungen stellen sich durch die IT-/OT-Konvergenz?

» Dr.-Ing. Reinhard Wegener: Eine wichtige Anforderung, die bislang typisch für Kritis war, ist die langfristige Systembetreibbarkeit. Sie resultiert aus den langen Investitionszyklen der Betriebstechnik, die eine entsprechend stabile und dennoch erweiterungsfähige Netzwerklösung erfordern. Das gilt aber auch für industrielle Produktionsanlagen. Deswegen sollten die gewählten Technikoptionen nicht nur aktuell passend, sondern so konzipiert sein, dass sie langfristig betreibbar sind, selbst wenn einzelne Elemente im Sinne des technischen Fortschrittes erneuert werden. Eine weitere permanente Anforderung ist die Cyber-Security. Damit technische Lösungen und Infrastrukturen dauerhaft höchsten Sicherheitsanforderungen genügen, ist ihre Betrachtung in einem Information Security Management System, kurz ISMS, notwendig, wie man es im Kritis-Umfeld als verpflichtend kennt.

Mit welche neuen Technikoptionen lassen sich betriebseigene Netze zukunftssicher gestalten?

» Dr.-Ing. Reinhard Wegener: IT/OT-Organisationen können neben der im Campusbereich üblicherweise eingesetzten Netzwerktechnik – die sich ihrerseits weiterentwickelt in Richtung Software Defined Networking, abgekürzt SDN – solche Technologien einsetzen, die bisher in öffentlichen Netzen anzutreffen sind. Insofern sind sie nicht grundsätzlich neu, aber ihr Einsatz auf einem Firmencampus, in privaten Gebäuden und Anlagen ist bisher eher selten. Zu diesen Optionen gehören Passive Optical LANs, kurz POL, und private 5G-Campusnetze sowie die Bereitstellung von Funkdiensten Dritter auf dem Campus.

Sie würden SDN als Option für einen sicheren Netzzugang einsetzen?

» Dr.-Ing. Reinhard Wegener: Ja, denn im Gegensatz zur traditionellen Netzwerkarchitektur, bei der einzelne Geräte Entscheidungen über den Datenverkehr treffen, wird ein SDN durch eine zentral und intelligent agierende Softwareplattform gesteuert. Sie überblickt das gesamte Netz, setzt Konfigurations- und Sicherheitsregeln automatisiert mit höherer Nachvollziehbarkeit um und unterstützt beispielsweise ein Zero-Trust-Konzept, wonach sich intern wie extern jeder, der auf Daten zugreift, authentifizieren muss.

Passive optische LAN kennt man vor allem aus öffentlichen Netzen …

» Dr.-Ing. Reinhard Wegener: Genau, die für Internetanbieter optimierte Glasfasertechnologie mit passiven optischen Verteilpunkten kann aber auch in einem ausgedehnten privaten Netz wirtschaftlich attraktiv sein, wenn dadurch der aufwendige Aufbau von Verteilerebenen mit Kupferkabel entfällt. Anhaltspunkte, ob sich ein passives optisches LAN Glasfaser lohnt, sind eine große Fläche mit vielen Anschlusspunkten für IT-, aber eben auch OT-Dienste wie Überwachungskameras oder Messstationen oder die Eigennutzung durch den Facility-Betreiber. Über eine Rentabilitätsberechnung können wir das genauer ermitteln.

runzelkorn - fotolia.com

Funkdienste auf dem Campus sind immer auch ein infrastrukturelles Thema. Dabei gilt es, in Sachen Sicherheit jedoch einiges zu beachten.

Neu sind privatbetriebene 5G-Campusnetze. Für wen ist das sinnvoll?

» Dr.-Ing. Reinhard Wegener: Lokale 5G-Mobilfunknetze bieten Unternehmen die Chance, ihre Digitalisierung massiv voranzutreiben. Das liegt an den Schlüsselmerkmalen von 5G: Neben einer hohen Bandbreite und der Möglichkeit, enorme Mengen an IoT-Geräten zu vernetzen, sind an dieser Stelle die kurzen Latenzzeiten von weniger als einer Millisekunde zu nennen. Damit können etwa industrielle Anlagen selbst mit sicherheitsrelevanten Bestandteilen drahtlos vernetzt und wechselnden Anforderungen ohne Verkabelungsaufwand angepasst werden. Auch für die Abdeckung ausgedehnter oder komplexer Firmengelände kann ein 5G-Campusnetz die beste Lösung sein.

Funkdienste auf dem Campus sind immer auch ein infrastrukturelles Thema. Was gilt es dabei zu beachten?

» Dr.-Ing. Reinhard Wegener: Ob Neubau oder Modernisierung, eine frühzeitige Planung ist entscheidend, um etwa Sicherheitsfunkdienste wie für die Feuerwehr im Einsatzfall in Gebäuden optimal zu gewährleisten. Hierfür sind qualifizierte Planunungstools erforderlich, die eine dreidimensionale Funkversorgung auf einem Campus innerhalb und außerhalb von Gebäuden berechnen kann. Daraus ergeben sich dann individuell abgestimmte Kabel- und Antennen-Infrastrukturen. Umfangreiche behördliche Richtlinien und Verfahren sind zu beachten. Die zugehörige aktive Technik benötigt wiederum Integration in das ISMS.

Wie können Unternehmen diese Systemvielfalt im Griff behalten?

» Dr.-Ing. Reinhard Wegener: Die meisten betriebsinternen IT-Teams werden personell und kompetenzmäßig an ihre Grenzen stoßen. Wollen sie ihre Netze zukunftsfähig halten, sollten sie Verantwortung für bestimmte Bereiche, zum Beispiel die Cyber-Security oder die 5G-Funkinfrastruktur, abgeben. Unserer Erfahrung nach funktioniert das reibungslos, wenn die Arbeitsweise eines Dienstleisters maßgeschneidert zu seinen Kunden passt.

Wir haben unsere Prozesse in diesen Fällen eng mit unseren Auftraggebern vernetzt. Von der Supportanfrage über aktuelle Zwischenstände bis zu Ergebnisberichten läuft alles elektronisch und in gemeinsam definierten Prozessen ab. Das ist so effektiv, dass wir über unser 24/7-Servicecenter einige zehntausend Tickets jährlich bearbeiten. Dadurch gewährleisten wir, dass die IT- und OT-Umgebungen unserer Kunden sicher laufen und den hohen Anforderungen aus der Kritis-Welt gerecht werden. ■

telent GmbH:
www.telent.de