FORTINET

WHITEPAPER

Erfolgreiche SD-WAN-Implementierung für Betriebstechnologie

Zusammenfassung

Für die Digitalisierung von Betriebstechnologie (OT) sind robuste, zuverlässige Verbindungen zum Internet und zur Cloud notwendig. Das softwaredefinierte Wide Area Networking (SD-WAN) wird zunehmend zu einer potentiellen Lösung, um langsame und kostspielige herkömmliche WAN-Infrastrukturen zu ersetzen. Da jedoch mit dem Internet verbundene Informationstechnologie (IT) immer mehr mit Betriebstechnologie vernetzt wird, benötigen Unternehmen mehr Transparenz über alle dezentralen Betriebsabläufe, die Möglichkeit von Implementierungen per Fernzugriff und ein einfacheres Management vorhandener Lösungen. Am wichtigsten dürfte jedoch eine stärkere Kontrolle über die Security sein, um sich vor steigenden Angriffen auf Betriebstechnologie zu schützen.

Die Konvergenz von IT und OT bringt neue Chancen – und neue Risiken

In der Industrie, der Fertigung und in kritischen Industriezweigen werden OT-Systeme zunehmend mit IT-Technologien konvergiert, um von mehr Effizienz und neuer Funktionalität zu profitieren. Dieses Zusammenwachsen von IT und OT erfordert jedoch neue Tools und Lösungen, die stärker vernetzte Betriebstechnologie richtig schützen können.

Die Digitalisierung erhöht die Komplexität und das Risiko für Unternehmen mit OT-Netzwerken. Daher brauchen OT-Verantwortliche heutzutage eine ganzheitliche Sicht auf die erweiterte Netzwerk-Infrastruktur. Tatsächlich besitzt der Großteil der Unternehmen (78 %) aber nur teilweise Einblick in OT-Umgebungen.[1] Das Problem: Ohne vollständige Transparenz lassen sich „unsichtbare“ Infrastrukturbereiche nicht schützen.

Infolge der weitverbreiteten IT-OT-Konvergenz ist das Air Gap – der schützende „Luftspalt“, der früher Betriebstechnologie vom Rest der Welt isolierte – weitgehend verschwunden. Das bedeutet, dass eine Sicherheitslücke oder ein erfolgreicher Angriff auf das IT-Netzwerk nun auch anfälliger, kritischer Betriebstechnologie gefährlich werden kann. Angreifer können im Unternehmen auf der Nord-Süd-Achse von außen in OT-Umgebungen eindringen oder sich auf der Ost-West-Achse lateral im Unternehmen bewegen. Fehlen Transparenz-Tools, bleiben Eindringlinge länger unentdeckt – und können so großen Schaden verursachen. Die Zeit von der ersten Aktion eines Angreifers in einer Ereigniskette bis zur ersten Infektion einer Ressource wird normalerweise in Minuten gemessen, während die Zeit bis zur Erkennung eher Monate beträgt.[2]

Unternehmen benötigen außerdem eine neue Infrastruktur für beide Bereiche: OT und IT. Nur so lassen sich redundante Aufgaben vermeiden, um Betriebsabläufe, Schulungen und Berichterstellung zu vereinfachen und gleichzeitig die Gesamtkosten zu senken. Komplexe Infrastrukturen – verursacht durch unzählige Einzelprodukte von verschiedenen Anbietern – führen jedoch nicht nur zu höheren Investitionskosten. Auch die Betriebskosten steigen erheblich, da der Implementierungs-, Management- und Überwachungsaufwand eine hohe Mehrbelastung für personell begrenzte Teams darstellt.

Herkömmliche WAN-Verbindungen verursachen hohe Kosten

Die Kosten sind in den meisten OT-Unternehmen ein Dauerproblem. Dabei gibt es oft Einsparungspotenzial bei der vorhandenen WAN-Infrastruktur. Ein herkömmliches WAN basiert hauptsächlich auf teuren MPLS-Leitungen (Multiprotocol Label Switching) oder Satellitenverbindungen. Um eine zentrale Kontrolle und Transparenz zu gewährleisten, läuft der gesamte Datenverkehr über ein On-Premises-Rechenzentrum. Dieses Backhauling kann die Leistung beeinträchtigen, wenn durch Sicherheitsfunktionen Engpässe entstehen.

Experten rechnen mit zunehmenden Angriffen auf kritische Infrastrukturen: Botnetze, die DDoS-Angriffe (Distributed Denial-of-Service) gegen OT-Netzwerke ausführen, Angriffe auf Fertigungssysteme, die Cloud-Dienste verwenden, und Supply-Chain-Angriffe, bei denen Drittanbieter von Bedrohungsakteuren kompromittiert werden, um über sie kritische Bereiche anzugreifen.[3]

Einzigartige physische Anforderungen von Betriebstechnologie

OT-Unternehmen betreiben unterschiedlichste Umgebungen an Standorten aller Größen – von großen Betriebsgeländen mit klimatisierten Gebäuden bis hin zu kleinen, abgelegenen Anlagen ohne Büro- oder Computerräume. Oft herrschen extreme Umgebungsbedingungen, die den Einsatz von normalen IT-Systemen verbieten. Dazu zählen:

- Umspannwerke
- Bohrinseln
- Fabriken
- Wasserkraftwerke
- Lager/Vertriebszentren
- Flughäfen
- Schiffe

SD-WANs erfreuen sich zunehmender Beliebtheit für Verbindungen zu unternehmenseigenen Remote-Standorten. Dabei werden unterschiedlichste Standard-Internet-Technologien wie LTE, DSL oder Kabelverbindungen verwendet, die MPLS-Leitungen und Satelliten-Links ersetzen und so die Kosten erheblich senken. Anwendungsleistung und Nutzererlebnis werden mit einer speziellen Verkehrslenkung (Traffic-Routing) gewährleistet. Das SD-WAN überträgt dabei den Datenverkehr nach den Kriterien Leistung (wie Latenz, Jitter) und Konnektivitätskosten, um eine zuverlässige, hochwertige Verbindung sicherzustellen.

Die breite Akzeptanz von SD-WANs in vielen Unternehmensbereichen deutet darauf hin, dass OT-Umgebungen als Nächstes folgen werden, sobald speziell auf Betriebstechnologie abgestimmte Hardware erhältlich ist. Benötigt werden robuste SD-WAN-Geräte, die für Industrie-, Fertigungs- und kritische Infrastrukturen ausgelegt sind – allesamt Umgebungen mit anspruchsvollen Bedingungen (wie Bohrinseln, Umspannwerke, Montagelinien oder Seefrachter).

Ein SD-WAN löst mehrere OT-Herausforderungen gleichzeitig: Es bietet z. B. eine rasche Implementierung, schnelle Verbindungen zu Cloud-Anwendungen und ein einheitliches Management, um das IT-Team zu entlasten.[4] Ein SD-WAN kann auch die Produktivität steigern. Beispielsweise können bei einer Multi-Cloud-Architektur die Benutzer direkt vom Standort auf Cloud-Dienste wie Microsoft 365, Oracle Cloud oder Anwendungen auf AWS zugreifen. Dies kann eine geringere Latenz und eine weitaus bessere Nutzererfahrung bieten als eine Internet-Verbindung, die über die Firewall eines zentralen Rechenzentrums läuft.[5]

SD-WANs und die Sicherheitsfrage

Der direkte Zugriff auf Cloud- und Internet-Ressourcen dürfte in einer OT-Umgebung noch größere Konsequenzen für die Sicherheit haben als bei einer typischen SD-WAN-Bereitstellung.[6] Die Umstellung von einem klassischen WAN auf ein SD-WAN erhöht das Risiko zusätzlich, da der Internet-Traffic nicht mehr per Backhauling über ein Rechenzentrum zur zentralen Sicherheitsüberprüfung läuft. Leider basieren die meisten SD-WAN-Produkte auf Routing-Technologien, die nur den besten Konnektivitätspfad für den Datenverkehr finden sollen. Eine integrierte Sicherheit ist dagegen bei den meisten SD-WAN-Lösungen Mangelware.

Jede Zunahme der Anfälligkeit von Betriebstechnologie stellt ein ernstes Problem dar, da OT-Unternehmen bereits massiven gezielten Angriffen ausgesetzt sind: Die überwiegende Mehrheit (90 %) erlebte im Vorjahr mindestens einen illegalen Zugriff auf OT-Systeme – bei 65 % waren es sogar drei oder mehr Sicherheitsvorfälle.[7]

Durch einen Angriff verursachte Ausfälle oder Störungen von Betriebstechnologie können einen enormen Einfluss auf die Produktivität, Effizienz und sogar die Sicherheit haben. Malware-Angriffe zielen jetzt speziell auf gefährdete Steuerungstechnik (ICS) sowie SCADA- und Schutzsysteme ab.[8] Dieses Risiko betrifft kritische Infrastrukturen (wie Staudämme, Kernkraftwerke, Öl- und Gas-Pipelines), bei denen ein erfolgreicher Angriff schwere Folgen für Mensch und Umwelt bis hin zur Lebensgefahr haben kann.

Industrielle Netzwerke benötigen sichere, priorisierte Verbindungen zu Leitstellen und Cloud-Anwendungen. Intelligente Sensoren, die auf Kommunikationsprotokollen für das industrielle Internet der Dinge (IIoT) und das Internet der Dinge (IoT) basieren – wie OPC UA (Open Platform Communications Unified Architecture), MQTT (Message Queuing Telemetry Transport) und HTTP (Hypertext Transfer Protocol) – müssen geschützt werden. Gleiches gilt für Übertragungen von Telemetrie- und Steuerungsdaten vom Prozess-Steuernetz zum IT-Unternehmensnetzwerk oder über das Internet, die häufig unsichere Protokolle wie Modbus, BACnet oder SafetyNET verwenden. Diese müssen in verschiedenen Segmenten platziert, überprüft und priorisiert werden und benötigen zudem einen starken Schutz. Eine typische SD-WAN-Lösung bietet jedoch keine dieser kritischen Sicherheitsfunktionen.

Einzigartige physische Anforderungen von Betriebstechnologie (Forts.)

Standorte wie die zuvor genannten erfordern spezielle Elektronik, die problemlos unter den üblichen OT-Umgebungsbedingungen funktioniert, z. B. bei

- extremen Temperaturen,
- Feuchtigkeit,
- starker oder ständiger Vibration,
- elektromagnetischen Interferenzen (EMI),
- geringer Stellfläche,
- unterschiedlichen Stromanforderungen (über 110 V bzw. 220 V) oder für
- Zertifizierungen gemäß verschiedener OT-Branchenvorschriften.

Der weltweite SD-WAN-Markt wird voraussichtlich bis 2024 um 168 % auf ein Volumen von über 3,2 Mrd. USD wachsen.[10]

Cyber-Kriminelle maximieren ihre Chancen, indem sie gleichzeitig sowohl ältere als auch neue OT-Schwachstellen – bedingt durch die wachsende Angriffsfläche – attackieren.[11]

Implementierung, Management und Überwachung per Fernzugriff

Ein weiteres Hauptproblem bei der Anpassung eines SD-WAN an OT-Umgebungen besteht darin, dass diese Technologien meistens an Remote-Standorten implementiert werden müssen. Das kann problematisch sein, da oft nur begrenztes oder gar kein technisches Personal Ort ist.[9] Die SD-WAN-Lösung muss daher kohärente Sicherheitsrichtlinien für Remote-Implementierungen bieten, die den Standort sofort ab der ersten Inbetriebnahme eines Systems schützen.

Zudem benötigt das Security Operations Center (SOC) des Unternehmens zentrale Transparenz über jeden Standort. Das ist notwendig, um die aktuelle Bedrohungslage zu überwachen, Gateways zwischen IT- und OT-Netzwerken zu verwalten und infizierte Systeme in Quarantäne zu setzen, um die Verbreitung von Malware zu begrenzen.

Notwendigkeit eines zuverlässigen, sicheren und kostengünstigen SD-WAN für Betriebstechnologie

Da Cyber-Kriminelle aller Art (von Hacktivisten über feindliche Staaten bis hin zur organisierten Kriminalität) zunehmend versuchen, OT-Systeme zu stören oder zu beschädigen, müssen Unternehmen die Vorteile der Digitalisierung maximieren und zugleich neue Risiken minimieren, die diese Technologien für sensible Umgebungen mit sich bringen.

Produktivität und Kostensenkung sind kritische Erfolgsfaktoren in jedem Unternehmen. Von Betriebstechnologie abhängige Branchen können es sich jedoch nicht leisten, einen dieser Faktoren über die betriebliche Sicherheit zu stellen. Das erhöhte Risiko, das direkte Internet-Verbindungen für OT-Umgebungen bedeuten, erfordert ein SD-WAN mit integrierter Security, zentraler Transparenz und Funktionen für das Remote-Management. Um in modernen Industrieumgebungen von den Vorteilen eines SD-WAN zu profitieren, sind zudem robuste Lösungen nötig, die nativ für die einzigartigen physischen Anforderungen von OT-Implementierungen entwickelt wurden.

[1] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit". Fortinet, 30. Juni 2020.

[2] „2019 Data Breach Investigations Report". Verizon, April 2019.

[3] Bruce Sussman: „15 Cyber Threat Predictions for 2020". SecureWorld, 12. Dezember 2019.

[4] Nirav Shah: „SD-WAN: More Than A Retail Solution". Network World, 15. Juli 2020.

[5] Joe Robertson: „What Manufacturing CISOs Need to Know About SD-WAN". LinkedIn, 20. Dezember 2019.

[6] Nirav Shah: „SD-WAN: More Than A Retail Solution". Network World, 15. Juli 2020.

[7] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit". Fortinet, 10. September 2020.

[8] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems". Fortinet, 8. Mai 2019.

[9] „SD-WAN Isn't Just for Retail". Fortinet, 3. April 2020.

[10] „SD-WAN Market Expected to Increase 168 Percent by 2024". BBC Magazine, 8. Juli 2020.

[11] Derek Manky: „Operational Technology: Why Old Networks Need to Learn New Tricks". Dark Reading, 31. Dezember 2019.

FORTINET

www.fortinet.com/de

18. Februar 2021, 19:50 Uhr

839530-0-1-DE