VPN und Industrie 4.0

Ziemlich beste Freunde

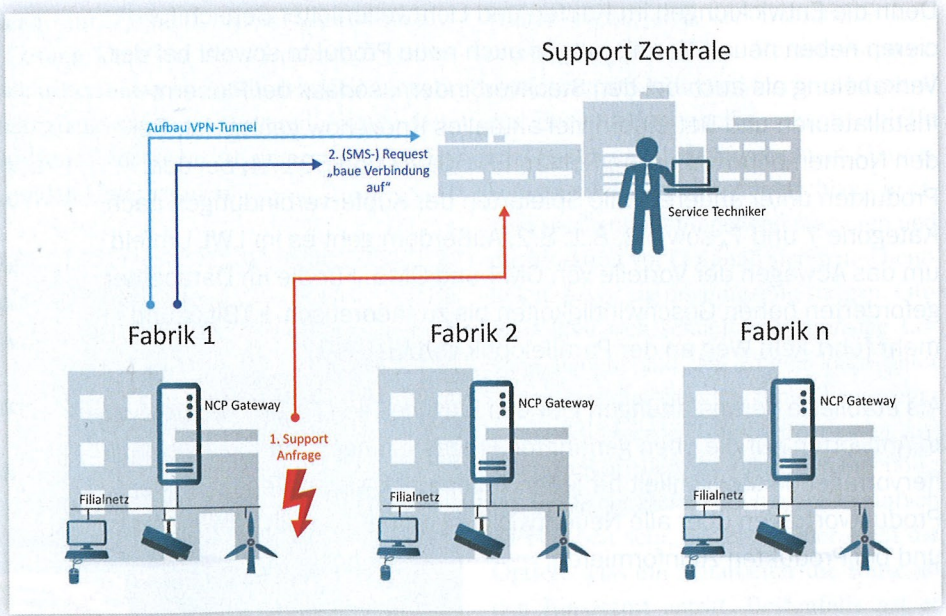
Fernwartung im industriellen Bereich verändert sich schnell von der früher üblichen, Modem-basierten direkten Verbindung hin zu einem IP- oder Cloud-Dienst. Die Anforderungen in der Industrie verlangen hohe Verfügbarkeit und Flexibilität, trotzdem darf die Sicherheit nicht zu kurz kommen. Die richtige Kombination aus Technik und Organisation sorgt für die perfekte Lösung.

Fernwartung von Industriemaschinen wird seit vielen Jahren praktiziert. Aber zunehmend verändern sich Art und Weise des Zugriffs. Während früher in der Regel ein Modem mit der Maschine verbunden war und den Zugang durch eine direkte Verbindung herstellte, setzen sich nun IP-basierte Lösungen durch. Die Gründe dafür sind sowohl niedrigere Kosten als auch höhere Durchsätze und mehr Funktionen. Allerdings entstehen durch den Wechsel auf IP auch neue Herausforderungen, was die Sicherheit der Verbindungen angeht. Ein Fernzugriff gilt als Angriffsvektor mit sehr hohem Schadenspotenzial, wenn Unternehmen die Verbindung und ihre Rahmenbedingungen nicht sehr sorgfältig absichern. Dabei geht es zum einen um die Verbindung selbst und alles was auf der Kundenseite zum Sicherheitskonzept gehört. Zum anderen sind auch Vorkehrungen zu treffen, um ein möglicherweise kompromittiertes Netz oder Endgerät auf Herstellerseite abzufangen.

Fachliche Unterstützung durch Behörden

Die wachsende Bedeutung des Themas erkennt man an der Verfügbarkeit von Richtlinien und Guidelines. Sowohl das amerikanische US-CERT (United States Computer Emergency Readiness Team) als auch das deutsche BSI (Bundesamt für Sicherheit in der Informationstechnik) haben jeweils Anleitungen zur Absicherung von Fernwartungszugängen veröffentlicht. Während sich das BSI auf die wichtigsten Hinweise und Empfehlungen konzentriert, gibt das Dokument des US-CERTs eine umfassende Einführung in das Thema, beschreibt die Herausforderungen und erklärt an einem Fallbeispiel die schrittweise Absicherung der Fernzugänge mit den vorgeschlagenen Maßnahmen. Es wird schnell klar, warum die Anwender nicht nur die Verbindung zwischen Service-Techniker und Maschine im Auge haben sollten, sondern auch die Umgebung und die organisatorische Seite. Fällt der Hersteller und damit auch das Ausgangsnetz und das Endgerät des Technikers einem Cyberangriff zum Opfer, hat der Angreifer einen direkten Zugang zum Netz des Maschinenanwenders. Im Prinzip erweitert sich der Perimeter des Kunden um das Endgerät und das Netzsegment des Service-anbietenden Herstellers. Verschiedene Maßnahmen können verhindern oder zumindest einschränken, dass das Kundennetz dann ebenfalls kompromittiert wird.

Viele der Hinweise, die beide Sicherheitsbehörden anführen, sind klassische IT-Sicherheitsmaßnahmen. Allerdings ist der Reifegrad der industriellen Umgebung aufgrund der bisher oft praktizierten Trennung von IT und Operational Technology (OT) häufig niedriger als gewünscht. So ist der klassische Weg, um die Sicherheit von Gütern zu gewährleisten, eine Bedrohungs- und Risikoanalyse. Es muss zunächst klar sein, welche schützenswerten Elemente in der Umgebung vorhanden sind und welche Angriffsvektoren auf sie wirken können. Daraus ergibt sich ein Risiko, das sich durch die entsprechenden technischen, prozeduralen oder organisatorischen Maßnahmen einschränken lässt.



Spezialisierte Gateways für IoT- und IIoT-Umgebungen bieten meist einen flexiblen Verbindungsaufbau. Die Insel/Maschine kann unter anderem ein Dial-up-Medium nutzen oder direkt über das IIoT-Gateway eine Verbindung initiieren, die normalerweise inaktiv ist (Entnetzung). Benötigt der Service-Techniker Zugang zur Insel/Maschine, sendet er beispielsweise eine SMS zum Gateway oder Router im Inselsystem und veranlasst es zum Aufbau einer Verbindung. Genauso kann im Gegenzug eine Maschine eine Fernwartungssession – gerade im Hinblick auf Predictive Maintenance (vorausschauende Wartung) – selbst initiieren. Bild: NCP

Weitere Sicherheitsmaßnahmen lassen sich durch die Architektur umsetzen. Segmentierung, One-Way-Gateways, Firewalls und DMZ sind probate Mittel, um zu verhindern, dass sich Angreifer Zugang zu Ressourcen im Produktionsbereich verschaffen können. In die gleiche Richtung zielt die Forderung nach einer sinnvollen Rechtevergabe. Mit den heute für IP-Remote-Zugänge verfügbaren Lösungen können Verantwortliche erlaubte Zielsysteme ebenso definieren wie die Endgeräte, von denen der Zugriff erfolgt. In größeren Umgebungen kann auch der Einsatz einer Privileged-Access-Management-Lösung (PAM) sinnvoll sein. Damit sind die tatsächlichen Zugangsdaten für das Zielsystem nicht bekannt, der Administrator oder Service-Techniker meldet sich an der PAM-Lösung an, die seine Aktivitäten überwacht.

Sicheres Benutzer-Management gefordert

Dass die Anmeldung am System durch starke Passwörter und Zwei- oder Mehrfaktor-Authentifizierung abgesichert sein muss, ist heute selbstverständlich. Zahlreiche Verfahren, ob Token oder Passcode auf einem weiteren Kommunikationsweg, stehen für 2FA und MFA zur Verfügung und müssen bei sensiblen Zugängen ins Netz unbedingt genutzt werden. Ebenso wichtig ist es, Default-Benutzer und Passwörter zu ändern oder stillzulegen. Leider finden Administratoren immer wieder heraus, dass Hersteller von industriellen Steuerungssystemen verborgene Benutzer-Accounts in ihren Systemen hinterlegen, von deren Existenz die Benutzer nicht oder nur durch Zufall erfahren. Und was bei normalem IT-Equipment zum Standard gehört, ist bei industriellen Anwendungen weniger verbreitet: die Ausgabe von Logs sowie Schnittstellen, um alle Vorgänge zu überwachen, am besten in einem SIEM-System (Security-Information- und Event-Management).
Generell sollten Verantwortliche reguläre Verbindungsanforderungen überwachen und nur auf Anmeldung freigeben. Es liegt allerdings in der Natur der Dinge, dass diese Vorgehensweise bei Notfällen nicht funktioniert. Allerdings gibt es technische Lösungen, die in diesem Fall eigenständig eine Verbindung zum Hersteller aufbauen und so den Wartungskanal aktivieren. Ein Weg dafür ist beispielsweise das Versenden einer SMS; diese wird aus dem Gateway mit inkludiertem Passcode über ein Mobilfunknetz an den Hersteller geschickt, der dadurch schließlich eine Verbindung initiieren kann. Dieser Ansatz funktioniert auch bei abgelegenen Standorten wie Pumpenstationen, die autark arbeiten und über keine durchgehende Datenverbindung verfügen.

Verschlüsselte Verbindungen sind Pflicht

Das Kernstück sicherer Fernwartung ist trotz aller Maßnahmen und Regelungen im Umfeld eine geschützte Verbindung zwischen Techniker und Maschine. Die notwendige Verschlüsselung dafür übernimmt heute fast immer ein Virtual Private Network (VPN), auch wenn es unterschiedliche Ausprägungen davon gibt. So ist neben dem klassischen Weg mit VPN-Gateway beim Kunden und VPN-Client auf der Maschine auch eine Cloud- oder Managed-Lösung möglich, in der beide Seiten per Client mit einem Gateway in der Cloud verbunden sind. Dieses Gateway kann der Hersteller oder ein Drittanbieter betreiben, sodass der operative Aufwand für beide Seiten minimal ist.
Eine VPN-Verbindung aus der klassischen IT hat normalerweise eine von zwei Ausprägungen. Entweder verbinden sich viele Clients mit einem zentralen Gateway, oder zwei Gateways stellen eine Verbindung miteinander her, über die der Datenverkehr verschlüsselt ausgetauscht wird. Alle Akteure, also Clients und Gateways, unterliegen der Hoheit eines Unternehmens. Der typische Anwendungsfall bei einem Hersteller, der die Maschinen bei seinen Kunden warten will, sieht anders aus. Dort sollen sich einer oder mehrere Techniker aus einem LAN heraus mit sehr vielen Geräten und Netzen verbinden, die nicht im Hoheitsbereich des Herstellers sind. Der Hersteller hat keine Kontrolle über die IP-Konfiguration der Zielsysteme und findet mit hoher Wahrscheinlichkeit identisch konfigurierte Netze vor – ein No-Go für herkömmliche VPN-Verbindungen.

So könnte die Systemumgebung zur Pumpenansteuerung an mehreren Standorten aus einer weitgehend identischen Konfiguration mit Server, Gateway, einem DCS für die Aktoren und der Pumpe selbst bestehen. Anwender sparen durch die „geklonte" Konfiguration zeitlichen Aufwand, vermeiden Fehler und halten das Ersatzteillager klein. Diese typische IoT-Systeminsel funktioniert zwar im Regelbetrieb autark, trotzdem muss der Service-Techniker immer mal wieder darauf zugreifen und bei Problemen eine Verbindung herstellen können. Doch wenn alle Inseln die gleiche Netzmaske, IP-Adresse und Gateway nutzen, kommt es zu Routing-Fehlern, wenn mehr als eine Insel mit dem zentralen LAN verbunden ist.

Organisieren oder automatisieren?

Das Problem lässt sich durch organisatorische Maßnahmen mildern, beispielsweise indem die Service-Techniker untereinander klären, wer wann eine aktive Verbindung nutzen darf. Das ist aber nur in kleinen Umgebungen mit wenigen Mitarbeitern praktikabel und in einem Notfall mit mehreren betroffenen Inseln zum Scheitern verurteilt. Die Alternative, jeweils individuelle Parameter zu vergeben, bedeutet dagegen mehr Aufwand bei der Konfiguration und bei der Verwaltung der Parameter. So sind schnelle Ortswechsel mobiler Einheiten, beispielsweise bei einem Inselsystem mit mehreren Kameras und einem Gateway zur Überwachung von Baustellen, nicht mehr so unkompliziert durchführbar.
Ein speziell für industrielle oder IoT-Anwendungen ausgelegtes VPN-Gateway löst das Problem durch einen technischen Trick. Dieses Gateway nutzt Network Address Translation, um die tatsächlich genutzten IP-Adressen der Inselsysteme vor dem Rest des Netzwerks zu verbergen. So sind Dutzende, Hunderte oder Tausende Inselnetze mit den gleichen IP-Parametern möglich, ohne dass es zu Konflikten kommt. Verwendet wird eine automatisch vergebene, eindeutige aber temporäre IP-Adresse. Das zentrale IIoT-Gateway (Industrial Internet of Things) sorgt beim Zugriff dafür, dass über diese Adressen trotzdem die immer gleichen Systeminseln er-

reicht werden (Destination-NAT). Um die Inselsysteme eindeutig zu authentifizieren, kommen Merkmale der Gateways oder der Client-Software auf Seiten des Zielsystems zum Einsatz. Unterstützt das Gateway Mechanismen wie SmartCards oder Zertifikate, werden diese herangezogen. Einfacher und universeller sind Hardwaremerkmale wie Prozessor-ID oder eine Seriennummer des Motherboards. Normalerweise reicht es, wenn sich das gewünschte Merkmal über eine Systemfunktion und ein Shellscript auslesen lässt.

Verbindungen asynchron einleiten

Der Vorteil einer solchen Lösung, die speziell für den Einsatz im IoT- und IIoT-Umfeld ausgelegt ist, liegt auch im flexiblen Verbindungsaufbau. Die Insel/Maschine kann unter anderem ein Dial-up-Medium nutzen oder direkt über das IIoT-Gateway eine Verbindung initiieren, die normalerweise inaktiv ist (Entnetzung). Benötigt der Service-Techniker Zugang zur Insel/Maschine, sendet er beispielsweise eine SMS zum Gateway oder Router im Inselsystem und veranlasst es zum Aufbau einer Verbindung. Genauso kann im Gegenzug eine Maschine eine Fernwartungssession – gerade im Hinblick auf Predictive Maintenance (vorausschauende Wartung) – selbst initiieren. Das spart nicht nur Kosten, weil die Verbindung nur On-Demand zustande kommt, es sorgt auch für mehr Sicherheit, weil die Verbindung, wie von US-CERT und BSI empfohlen, im Regelfall nicht aktiv und damit nicht von einem Angreifer erreichbar ist. Als integrierter Bestandteil einer VPN-Lösung bedeutet die asynchrone Verbindung für den Service-Techniker keine Mehrarbeit und verzögert die Verbindung lediglich um einige Sekunden.

IP-basierte Fernwartungszugänge werden über kurz oder lang den Löwenanteil in industriellen Umgebungen ausmachen. Dedizierte Wählverbindungen mit (Funk-)Modems sind nur noch in besonders sensiblen Bereichen und an entlegenen Standorten notwendig. Durch IP sind schnellere Verbindungen mit mehr Funktionen möglich, sie eröffnen aber auch einen weiteren Angriffsvektor. Um Fernwartung trotzdem sicher durchzuführen, müssen Anwender ihre Umgebung sowohl in organisatorischer Hinsicht als auch durch die passenden technischen Maßnahmen absichern. Spezialisierte VPN-Gateways für IoT und Industrial IoT können mit den Besonderheiten der industriellen Umgebung sehr gut umgehen und bieten die notwendige Flexibilität und Sicherheit, die ein geschützter Zugang in das eigene Netz erfordert.

Jürgen Hönig/ts

Jürgen Hönig ist Chief Marketing Officer bei NCP Engineering, www.ncp-e.com.