Fernwartung ja – aber bitte nur sicher

Ein Fernzugriff auf Anlagen hat viele Vorteile, muss aber gut geschützt sein

Maschinen und Anlagen in der Prozessindustrie müssen überwacht und gewartet werden. Fernwartung erleichtert diese Aufgaben, eröffnet jedoch zusätzliche Angriffsflächen. Wie sieht eine gute Sicherheitsarchitektur im Spannungsfeld zwischen Informationstechnik (IT) und operationaler Technik (OT) aus und wie kann sie implementiert und betrieben werden?

Keywords
- *Zustandüberwachung*
- *Fernwartung*
- *NOA Security Gateways*
- *IT/OT-Konvergenz*

Für die Industrie ist ein Fernzugriff auf Anlagen, Maschinen und Prozesse aufgrund seiner Vorteile gängige Praxis und daher nicht mehr wegzudenken. Denn damit ist eine Zustandsüberwachung zur Fehlererkennung und -analyse ebenso möglich, wie eine Wartung aus der Ferne oder der Datenaustausch für die Teilhabe an industriellen Ökosystemen. Dies erhöht nicht nur die Effizienz, sondern reduziert auch Kosten, da kein Techniker vor Ort erforderlich ist, und verbessert im Störfall die Reaktionsgeschwindigkeit.

Der dafür benötigte Remote-Zugang ist jedoch ein massiver Eingriff in die Sicherheitsarchitektur der operationellen Technologie (OT) vor Ort. Dadurch können potenzielle Einfallstore für Angreifer entstehen und Schadsoftware eingeschleust werden. Dies gilt umso mehr, wenn Zugriffe auf kritische (OT-)Steuerungssysteme über direkte VPN-Verbindungen erfolgen.

Wie aber können Betreiber den Fernzugriff so absichern, dass die Gefahren für die Verfügbarkeit und die Integrität der Anlagen und Maschinen so gering wie möglich sind?

Unterschiedliche Anforderungen bei Monitoring und Wartung

In der operationellen Technologie sind zwei Szenarien zu unterscheiden: Zum einen die reine Überwachung, zum anderen die Fernwartung. Beim Monitoring, wie sie etwa bei der vorausschauenden Wartung zum Einsatz kommt, besteht eine permanente Verbindung für die Datenausleitung aus der Steuerungs- und Feldebene. Dabei werden nur Daten ausgeleitet, es findet kein Schreibzugriff auf die Maschinen statt. Zur Absicherung derartiger Anbindungen sind Datendioden der beste Weg.

Datendioden lassen Transfers nur in eine Richtung zu, von der Anlage zum Monitoringsystem. Übertragungsversuche in der Gegenrichtung werden blockiert. Ein Beispiel für eine solche dem neuesten Stand der Technik entsprechende Lösung ist die cyber-diode von Genua[1], welche die Empfehlungen der NOA NE 177[2] bezüglich des NOA Security Gateways implementiert. Für die Übertragung werden dabei gängige Protokolle wie OPC UA (Open Platform Communications – Unified Architecture), FTP(S) oder Syslog (System Logging Protocol) verwendet. Derartige Datendioden schützen also die Integrität und die Verfügbarkeit der Maschinen und Anlagen.

Ein Zugang zur Fernwartung hingegen wird nur temporär zum Zweck der Wartung oder Störungsbeseitigung aufgebaut, erlaubt aber neben einem lesenden auch einen aktiven schreibenden Zugriff auf die Anlagen. Die Gefahr ist hier größer als bei der Überwachung, da die Möglichkeiten eines Angreifers, und damit die eventuell angerichteten Schäden höher sind. Derzeit noch häufig eingesetzt wird eine VPN-Anbindung direkt über das Betreibernetzwerk, die einen durchgehenden Zugang bis tief in die industrielle Ebene, bspw. auf die speicherprogrammierbare Steuerung (SPS) von Maschinen und Anlagen, erlaubt.

Die direkte Kopplung zweier Netzwerke per VPN stellt ein erhebliches IT-Sicherheitsrisiko dar. So bleibt etwa der Pfad zwischen der Unternehmensebene und der Steuerungsebene auch nach Abbau der VPN-Anbindung offen. Der VDMA rät daher in seinem Leitfaden „Sichere Fernwartung“[3] von dieser Architektur ab.

Dem heutigen Stand der Technik entspricht ein hardwarebasiertes Rendezvous-System. Dieses setzt auf einen beim Betreiber innerhalb einer demilitarisierten Zone (DMZ) in der lokalen Betriebsebene angesiedelten VPN-Server auf. Ein Fernwartungszugriff erfolgt dabei in zwei Schritten: Zunächst stellt der Servicetechniker eine VPN-Anbindung zum Rendezvous-Server her, der die Authentifizierung und Autorisierung des Fernwarters sicherstellt. Anschließend wird ein Datenpfad zwischen Server und Maschine aufgebaut. Alle Wartungsverbindungen laufen also über den Server. Somit ist von außerhalb kein direkter Durchgriff auf die unterste Ebene möglich. Sobald die VPN-Verbindung zwischen dem VPN-Client vor dem Zielsystem und dem Rendezvous-Server durch den Operator abgebaut wird, besteht kein Zugriff auf die Steuerungs- und Feldebene mehr. Die Sicherheit ist damit gewährleistet. Derartige Rendezvous-Server sind kommerziell verfügbar, so beispielsweise die den BSI-Empfehlungen für eine sichere Fernwartung entsprechende genubox[4] von Genua.

Vielfältige Herausforderungen bei Fernzugriff

Neben der Sicherheit stehen die Betreiber von Fernwartungsnetzen vor weiteren Aufgaben. Zum einen muss eine einfache Bedienbarkeit gegeben sein – der Spezialist für eine Anlage soll sich mit deren Funktionalität beschäftigen

und nicht mit deren Schutz. Zum anderen sind derartige Netze hochkomplex, da unterschiedlichste Lösungen im Einsatz sind, etwa verschiedene Firewalls oder Personal mit voneinander abweichenden Zugriffsrechten. Deshalb sollten diese Geräte leicht integriert und kombiniert werden können. Dazu gehört auch, dass sich ein Netz einfach skalieren lässt, sobald zusätzliche Maschinen oder Zugriffspfade hinzukommen. Ein weiteres Thema ist die Verfügbarkeit. Hier muss sich der Betreiber Gedanken machen, wie diese auf Netzwerkebene immer gegeben ist.

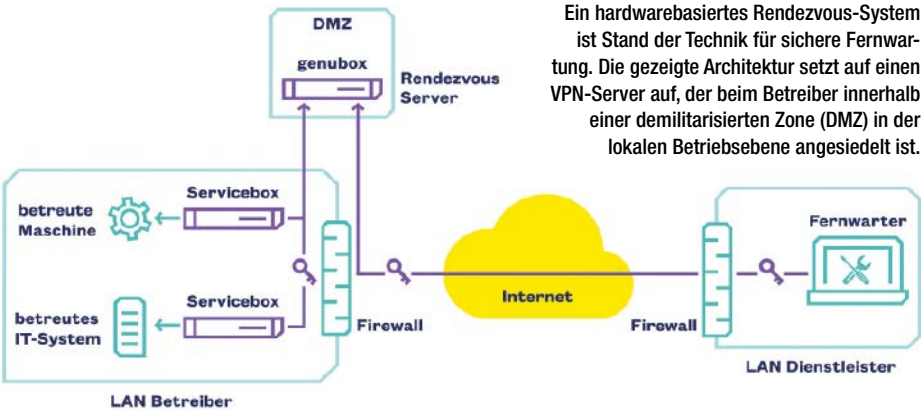
Größtes Problem ist derzeit die IT/OT-Konvergenz. Denn es sind Verantwortliche aus der OT und der IT beteiligt, also Domänen, die bisher eher weniger miteinander zu tun hatten und teilweise voneinander abweichende Fachbegriffe verwenden. Zudem sind Anforderungen und Schutzziele unterschiedlich. Hier gilt es, zeitgemäße Ansätze und Lösungen zu finden.

Zero-Trust ist die Zukunft

Eine neue Tendenz ist die Verlagerung der VPN-Server aus der industriellen DMZ heraus in die Cloud, um den Betrieb zu vereinfachen, die Verfügbarkeit zu erhöhen und die Skalierbarkeit zu verbessern. Dies birgt zusätzliche potenzielle Sicherheitsrisiken, die sich durch Zero-Trust-basierte Lösungen mit restriktiven, individuellen Zugriffsrechten und Identitäten, die auf starker Authentifizierung basieren, reduzieren lassen.

Zusätzlich sollte das Netzwerk weiter segmentiert werden. Stärker segmentierte Netze entstehen durch eine verstärkte Trennung der Maschinen und Anlagen untereinander. Ein Nutzer muss dann einzeln nachweisen, dass er darauf Zugriff erhalten darf. Damit diese Segmentierung wirksam ist, dürfen die Betreiber diese Rechte nur sehr eingeschränkt vergeben.

Eine Identitätsüberprüfung durch Passwörter ist dabei nicht ideal. Besser eignen sich Mehrfaktor-Authentifikation, kryptografische Methoden mit Verschlüsselung durch Public-Private-Schlüssel, der Einsatz von Hardwaretoken, Smartcards oder eine Authentifikation über externe Identity Provider wie Azure AD oder Okta. Wird dies beachtet, kommt ein Angreifer selbst mit erschlichenen Rechten im Netzwerk nur langsam vorwärts; er erhält also nicht sofort den Worst-Case-Zugriff auf die gesamte Steuerungs- und Feldebene.



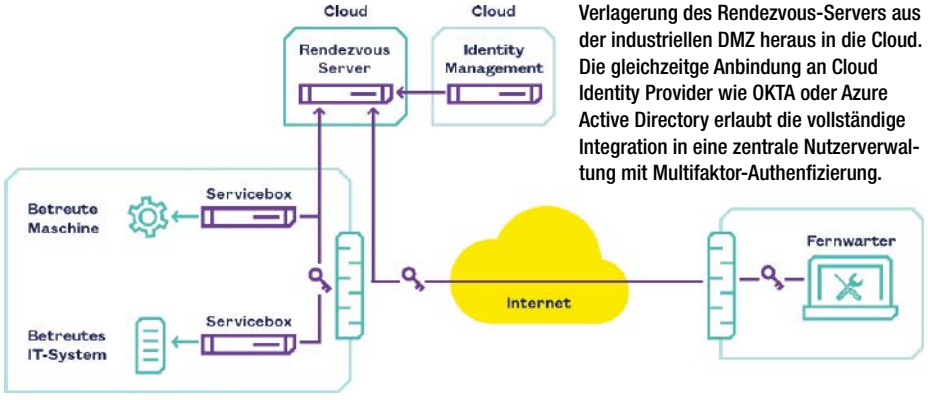
Ein hardwarebasiertes Rendezvous-System ist Stand der Technik für sichere Fernwartung. Die gezeigte Architektur setzt auf einen VPN-Server auf, der beim Betreiber innerhalb einer demilitarisierten Zone (DMZ) in der lokalen Betriebsebene angesiedelt ist.

Für Anwendungsfälle, in denen sich der Rendezvous-Dienst in der Cloud befindet, liegt es nahe, auch den Dienst zur Verwaltung der Identitäten zu einem Cloud-Identity-Provider zu verlegen. Dies ist mit einem gewissen Risiko behaftet, denn hier können sich Sicherheitslücken katastrophal auswirken. Allerdings sind Dienste in der Cloud skalierbar, die Auslagerung gewinnt daher immer mehr an Bedeutung. Die Absicherung ist also besonders wichtig. Betreiber solcher Fernwartungsnetze sollten sich bei der Umsetzung von einem erfahrenen Sicherheitsexperten für IT- und OT-Netzwerke beraten lassen.

Neue Brücken bauen

Wie verändern sich nun die Anforderungen durch die Verlagerung hin zu Rendezvous-Diensten in der Cloud? Zum einen werden die Ansprüche an die Sicherheit höher. Diese sollte in den Händen von ausgewiesenen Experten liegen und nicht durch eine „Schatten-IT“ sichergestellt werden. Zum anderen wird die Konvergenz weiter zunehmen, etwa durch den steigenden Bedarf an OT-Daten. Damit wird auch das Gap zwischen IT und OT weiter wachsen. Dies betrifft nicht nur die Fachtermini und das Fach-Knowhow, sondern auch die Schutzziele, die unterschiedlich ausfallen. Durch die Verlagerung in die Cloud vergrößert sich dieser Abstand weiter. Der Grad der Abstraktion wird höher und die Diskrepanz bei den Begriffen größer. Die Welten „Cloud“ und „OT“ liegen also nochmals weiter auseinander als die der IT und der OT.

Zugleich soll in allen Bereichen die Effizienz zusätzlich gesteigert werden. Gelingen kann das nur, wenn zwischen den beiden Fraktionen Brücken geschlagen werden, die groß und sehr breit sind. Nur indem alle Beteiligten an einem Strang ziehen und vorhandene Probleme gemeinsame angehen, lassen sich die erheblichen Vorteile des Fernzugriffs sicher nutzbar machen.



Verlagerung des Rendezvous-Servers aus der industriellen DMZ heraus in die Cloud. Die gleichzeitge Anbindung an Cloud Identity Provider wie OKTA oder Azure Active Directory erlaubt die vollständige Integration in eine zentrale Nutzerverwaltung mit Multifaktor-Authenfizierung.

Literaturangaben:

[1] https://www.genua.de/it-sicherheitsloesungen/datendiode-cyber-diode.

[2] NE 177: NAMUR Opern Architecture – NOA Security Zonen und NOA Security Gateway. Ausgabe 2021-04-08. Empfehlung der Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V

[3] VDMA: Sichere Fernwartung – Beispiele von Fernwartungsarchitekturen für einen sicheren Remote Service. Frankfurt Dezember 2021.

[4] www.genua.de/it-sicherheitsloesungen/fernwartungs-appliance-genubox.

Der Autor
Richard Oed,
freier Autor für Genua

Wiley Online Library

Genua GmbH, Kirchheim bei München
Tel.: + 49 89 991950 - 0
vertrieb@genua.de · www.genua.de