Remote Access in der Industrie

Risiken und Lösungsansätze

Die Digitalisierung von Fertigungs- und Produktionsanlagen verspricht eine höhere Effizienz durch optimierte Prozesse. Die notwendige Öffnung der Betriebstechnologie nach außen bis hin zu Public Clouds schafft jedoch nicht zu vernachlässigende Risiken für die Security und Safety. Mit den richtigen Konzepten lassen sich Fernwartung, Predictive Maintenance und andere Services nutzen, ohne Hackern Tür und Tor zu öffnen.

Es gab Zeiten, da war der Shop Floor extrem sicher gegen externe Angreifer geschützt – nämlich als das OT-Netz noch autark war, streng abgeschirmt vom IT-Netz und ohne Verbindung zu externen Systemen. Doch die fortschreitende Automatisierung der Industrie hat die Trennung von IT und OT (Operational Technology) aufgeweicht. Moderne Maschinen und Anlagen erhalten Auftragsdaten vom ERP, bieten Zugriff auf Betriebsstatus und Fertigungsfortschritt per Dashboard auf Tablet und Smartphone, optimieren Prozesse mittels KI aus der Cloud und lassen sich aus der Ferne konfigurieren und warten. Die Kehrseite der Medaille: Auch Cyberkriminelle versuchen von außen auf die Systeme zuzugreifen, um wertvolle Kundendaten und geistiges Kapital zu stehlen, Fertigungsprozesse zu sabotieren oder die Anlage stillzulegen, um Lösegeld zu erpressen. Ein prominentes Beispiel ist der Rüstungshersteller Rheinmetall, treffen kann es aber jedes Unternehmen. Viele sind schlicht „Beifang" automatisierter Hackerangriffe. Ende vergangenen Jahres trugen Cyberkriminelle sogar zum Ende des Fahrradherstellers Prophete Group bei, der nach einem mehrwöchigen Produktionsausfall Insolvenz anmelden musste.

Autor:
Harry Jakob
freier Journalist und Autor
genua GmbH
www.genua.de

Hochsichere Datenausleitung mit OPC UA

Grundsätzlich ermöglicht der Industriestandard OPC UA eine plattformunabhängige Kommunikation und den standardisierten Austausch von Maschinendaten, sowohl horizontal (also die Vernetzung von Steuerungen, einzelner Maschinen, Anlagen oder Produktionseinheiten) als auch vertikal (vom Maschinensensor bis hin zur Cloud). Eine in der Industrie häufig anzutreffende Anwendung ist Predictive Maintenance. Hierfür ist häufig lediglich ein kontinuierlicher Datentransfer notwendig, bei dem Daten vom Shop-Floor nach außen geleitet werden. Eine Kommunikation in die Gegenrichtung ist in der Regel nicht notwendig. Solche Monitoringaufgaben können mit Datendioden recht sicher und zuverlässig umgesetzt werden. Durch den Einsatz der cyber-diode, beispielsweise zwischen OPC-UA-Servern von Maschinen und Zielen wie Datenbanken, Visualisierungs-Clients oder Clouddiensten, lassen sich Daten für die Zustandsüberwachung verschlüsselt und hochsicher ausleiten. Dabei lässt die Datendiode ausschließlich One-Way-Datentransfers zu. In Gegenrichtung blockt sie jeden Informationsfluss ab. Ein Transport von Schadcode oder andere Cyber-Risiken sind damit ausgeschlossen.

Mehr Angriffsfläche durch Fernwartungszugänge

Fernwartungszugänge beruhen hingegen auf einer Zwei-Wege-Kommunikation, die auch Schreibrechte für Anwender von außen umfasst. Damit ist das Risiko für Angriffe ungleich höher. Um dieses wirksam zu begrenzen, muss eine Reihe von Herausforderungen gemeistert werden. Für den Anlagenbetreiber ist es von elementarer Bedeutung, dass die Zugriffe kontrollierbar, steuerbar und nachvollziehbar sind sowie ein fehlerfreier und störungsfreier Produktionsprozess gewährleistet wird. Das bedeutet, dass nur autorisierte Personen Zugriff haben dürfen, ihre Aktivitäten begrenzt und überwacht werden müssen und diese keine unerwarteten Nebenwirkungen auslösen, die den Anlagenbetrieb beeinträchtigen.

Stand der Technik bei Architekturen für Remote Access

Der VDMA-Arbeitskreis „Sichere Fernwartung" hat im Jahr 2021 die am häufigsten eingesetzten Architekturen im Bereich Remote Access auf ihre Vor- und Nachteile hin bewertet. Sie lassen sich grob in drei Klassen einteilen:

- die Netzkoppelung von außen per VPN mit direktem Zugriff auf interne Ressourcen,
- die Netzkoppelung von außen mit einem „Zwischenstopp" über Jump Hosts,
- das Rendezvous-Konzept mit einem Verbindungsausbau von innen nach außen.

Gerade bei älteren Installationen findet sich noch häufig eine einfache VPN-Verbindung von außen auf einen VPN-Server direkt auf die OT-Ebene, so dass Netzwerksegmentierungen und Demilitarisierungszonen (DMZ), also Sicherheitszonen, die sich zwischen öffentlichem Internet und privatem Intranet befinden, keine Wirkung entfalten können. Diese Konstellation bietet den geringsten Schutz unter den betrachteten Konzepten und

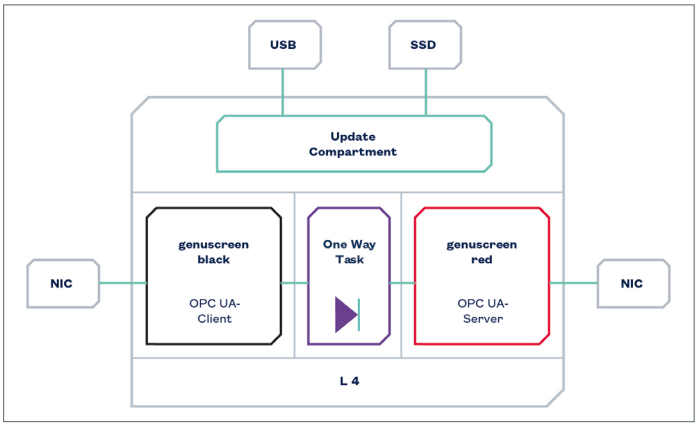

Bild 1: Aufbau der cyber-diode für den Datentransfer von einem vertrauenswürdigen Netzwerk (schwarz), z. B. einem Produktionsbereich, in ein unsicheres Netzwerk (rot), z. B. das Internet. Das Design der Datendiode ermöglicht eine gesicherte, rückwirkungsfreie Ausleitung von Maschinen- und Anlagendaten z. B. für die vorausschauende Wartung.

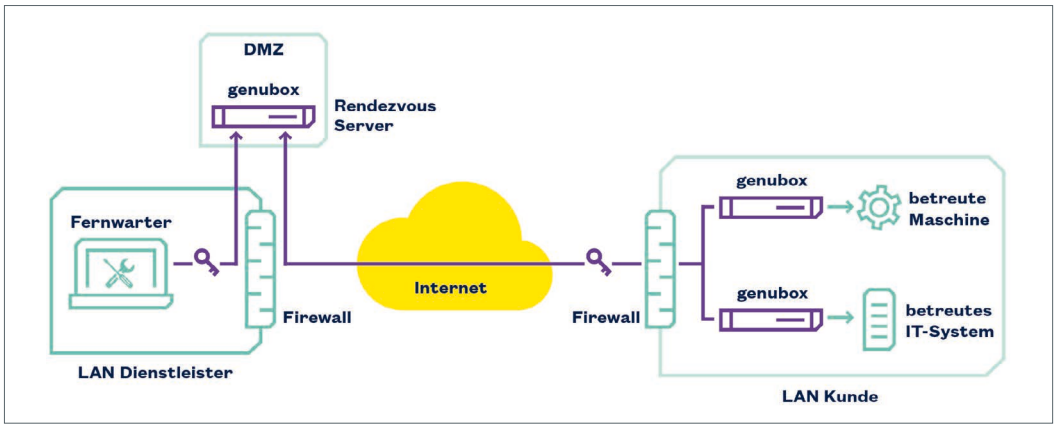

Bild 2: Ein hardwarebasiertes Rendezvous-System ist Stand der Technik für sichere Fernwartung. Die gezeigte Architektur setzt auf einem VPN-Server auf, der beim Betreiber innerhalb einer demilitarisierten Zone (DMZ) in der lokalen Betriebsebene angesiedelt ist.

sollte schnellstmöglich auf zeitgemäße Lösungen umgerüstet werden.

Jump Host

Einen etwas besseren Schutz bietet die Variante, bei der eine VPN-Verbindung von außen auf einen sogenannten Jump Host aufgebaut wird, der sich in einem relativ unkritischen und gut geschützten Netzwerksegment befindet. Von diesem aus kann sich der Dienstleister weiter durch die Netzwerksegmente arbeiten, indem er sich jeweils autorisiert, bis er beim Zielsystem angelangt ist. Das Risiko dieser Architektur ist zwar geringer, das Verfahren erfordert jedoch einen hohen Wartungsaufwand und ist nur schlecht skalierbar.

Rendezvous-Konzept

Als „Stand der Technik" wird vom VDMA das Rendezvous-Konzept bewertet. Dieses beruht darauf, dass sich ein Dienstleister von außen zu einem sogenannten Rendezvous-VPN-Server verbindet. Die Verbindung zwischen Rendezvous-Server und Maschine bzw. Anlage kann dann allerdings nur von innen her aufgebaut werden. Für die Positionierung des VPN-Servers gibt es eine ganze Reihe unterschiedlicher Möglichkeiten: zum Beispiel in der Industrial Zone des Unternehmens, beim Dienstleister oder in der Cloud – jedoch nicht im OT-Netzwerk. Das Angriffsrisiko für diese Varianten unterscheidet sich kaum. Die Sicherheit hängt in erster Linie von der konkreten technischen Umsetzung ab. Den höchsten Angriffsschutz bietet die Rendezvous-Architektur Betreibern in Kombination mit anderen Sicherheitskonzepten. So ist es grundsätzlich sinnvoll, den gesamten Netzwerkverkehr auf ungewöhnliche oder unerwünschte Kommunikation zu überwachen. Weitere Ansätze, um die Sicherheit zu erhöhen, sind:

- der Einsatz von Applikationsfiltern bzw. Application Level Gateways,
- das Protokollieren aller Zugriffe,
- die automatisierte Überwachung durch ein SIEM (Security Information and Event Management) System,
- die Nutzung eines zentralen Managements der erlaubten Fernwartungszugriffe,
- die Unterstützung gängiger Authentifizierungsdienste zur nahtlosen Integration.

Trend zur Cloud, hin zu Zero Trust

Nicht zuletzt durch die zunehmende Verlagerung von Diensten in die Cloud gewinnt außerdem Zero Trust erheblich an Bedeutung. Die Verlagerung des Rendezvous-Servers in die Cloud erlaubt es Betreibern und Maschinenbauern zum Beispiel, den Betrieb zu vereinfachen, die Verfügbarkeit zu erhöhen und die Skalierbarkeit zu verbessern. Gleichzeitig erhöhen sich jedoch die Ansprüche an die IT-Sicherheit weiter. Gemäß dem Motto „Vertraue niemals, verifiziere immer!" basiert das Zero-Trust-Paradigma auf der Idee restriktiver, individueller Zugriffsrechte und Identitäten, die auf starker Authentifizierung basieren. In der Konsequenz muss sich jeder Anwender und jeder Dienst einzeln authentifizieren und es werden nur die absolut nötigen Zugriffsrechte vergeben. Im Fall von Remote Access heißt das etwa, dass jeder Fernwarter nur jeweils für „seine" Zielsysteme und Applikationen eine explizite Freischaltung erhält. Um die Sicherheit weiter zu erhöhen, sollte das Netzwerk außerdem 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 Rechte nur sehr eingeschränkt vergeben werden.

Cloud-Identity-Provider

Für derlei Cloud-Szenarien liegt es außerdem nahe, auch den Dienst zur Verwaltung der Identitäten zu einem Cloud-Identity-Provider zu verlegen und Cloud-Identity-Provider wie OKTA oder Azure Active Directory zu nutzen. Dies erlaubt die vollständige Integration der Fernwartung in eine zentrale Nutzerverwaltung mit unternehmensüblicher Multifaktor-Authenfizierung. Unternehmen profitieren damit von skalierbaren Mandanten-, Rollen- und Rechte-Konzepten und Nutzer können sich über ihr gewohntes Verfahren authentifizieren.

Fazit

Die Ansprüche an die sichere Umsetzung von Remote Monitoring, Predictive Maintenance oder Fernwartung sind also ziemlich umfangreich. Mit der richtigen Security-Strategie sind diese jedoch durchaus zu erfüllen. Mittels einer integrierten Plattformlösung, die Security-by-Design realisiert, lassen sich umfangreiche Security-Maßnahmen mit vergleichsweise geringem Aufwand integrieren und das Sicherheitsniveau deutlich erhöhen. ◄

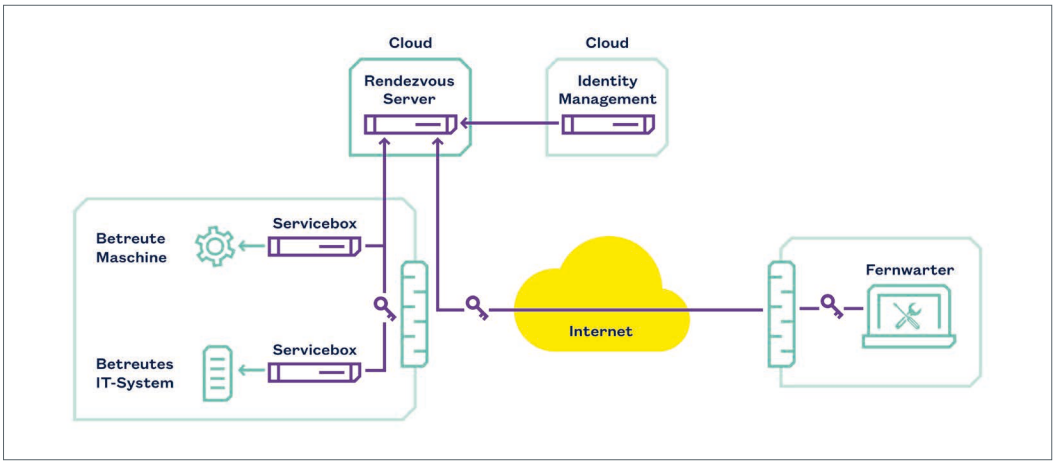

Bild 3: Ein Trend ist die Verlagerung des Rendezvous-Servers in die Cloud. Vorteile ergeben sich für Betrieb, Skalierbarkeit und Verfügbarkeit. Gleichzeitig steigen die Ansprüche an die IT-Sicherheit.