SONDERDRUCK
CHEManager
DIE ZEITUNG FÜR DIE MÄRKTE DER CHEMIE UND LIFE SCIENCES
33. Jahrgang · 3/2024, S. 28, Wiley-VCH, Weinheim, www.chemanager-online.com

Security bei der Fernwartung

Remote-Zugriffe auf interne Netzwerke sind immer kritisch

In der Industrie werden seit vielen Jahren Fernwartungslösungen eingesetzt. Allerdings ist der Umgang aus Perspektive der Internetsicherheit häufig sehr risikoreich. Welche Voraussetzungen für einen Fernzugriff müssen erfüllt sein, damit Betreiber ruhig schlafen können?

Laut BSI, dem Bundesamt für Sicherheit in der Informationstechnik, zählt der Einbruch von Cyberkriminellen über Fernwartungszugänge zu den besonders kritischen und am häufigsten auftretenden Bedrohungen für die Security von Industrial Control Systems, mit steigender Tendenz. Lässt sich Fernwartung überhaupt sicher betreiben?

Zugriffe auf interne Netzwerke von außen sind immer kritisch und sollten äußerst sensibel angegangen werden. In der Regel erfolgen Fernwartungszugriffe auf Level 2 oder 3 einer Anlage, teilweise aber auch auf SPS-Ebene oder eben auf IT-Systeme. Generell gilt: Für unterschiedliche Use Cases ergeben sich teilweise deutlich unterschiedliche Anforderungen und somit auch andere Varianten für einen sicheren Datenzugriff. In der reinen Ferndiagnose wird lediglich lesender Zugriff auf für eine Diagnose relevante Daten benötigt. Hier könnte ein temporärer Fernwartungszugriff passend sein, oder der Einsatz von Datendioden zur kontinuierlichen unidirektionalen Datenausleitung. Datendioden allein sind im Bereich des Monitorings, also der reinen Fernüberwachung, eine gute Lösung. Hier wird lediglich ein lesender Zugriff auf das überwachte System benötigt. Sie sind somit eine gute Möglichkeit, rückwirkungsfrei und hochsicher zyklisch oder permanent Daten auszuleiten.

Fernwartungsdienstleister dürfen nur Zugriff auf die benötigten Zielsystem-Applikationen erhalten.

Markus Maier, Genua

Grundlegende Anforderungen an die Cybersecurity bei Remote-Zugriffen

Aus Perspektive der IT-Sicherheit ist unbedingt darauf zu achten, dass Fernwartungsdienstleister nur Zugriff auf die benötigten Zielsystem-Applikationen erhalten, über verschlüsselte Verbindungen, über speziell gehärtete Komponenten und nach Multi-Faktor-Authentifizierung. Zusätzlich sollten Applikationsfilter oder auch Application Level Gateways zur weiteren Trennung vorhanden sein. Alle Zugriffe müssen protokollierbar sein und am besten durch ein SIEM-System (Security Information and Event Management) automatisiert überwacht werden. Im Betrieb ist aus Effizienz- und Sicherheitsgründen ein zentrales Management der erlaubten Fernwartungszugriffe unverzichtbar. Zur nahtlosen Integration sollten gängige Authentifizierungsdienste unterstützt werden. Einen guten Überblick über die wichtigsten Aspekte bieten die NAMUR-Empfehlungen NE 177 „NAMUR Open Architecture – NOA Security Zonen und NOA Security Gateway" sowie insbesondere die NE 135 „Fernzugriff (Remote Access) – Anforderungen an die IT-Sicherheit von Fernzugriffen". Erstere formuliert generelle Anforderungen an die sichere Datenausleitung für Überwachungs- bzw. Monitoringaufgaben, die NE 135 des NAMUR-Arbeitskreises „Automation Security" fasst die wichtigsten Anforderungen an die IT-Sicherheit von Fernzugriffen zusammen.

Das optimale Zusammenspiel aller Beteiligten

Wie genau läuft aus Sicht der Security das optimale Zusammenspiel aus Fernzugreifendem, Betreiber sowie Hersteller und Integrator von Fernzugriffslösungen? Klar ist, dass zunächst der Betreiber entscheiden muss, über welche Wege der Fernwarter wann und worauf Zugriff bekommt. Viele Hersteller von Anlagenkomponenten haben eigene Fernwartungslösungen in ihre Komponenten integriert. Ob sie diese nutzen dürfen oder auf zentrale, einheitliche Systeme zurückgreifen müssen, – die Entscheidung liegt einzig beim Betreiber. Das Wesentliche ist die strikte Authentifizierung vor dem Zielsystem und der ausschließliche Zugriff auf die benötigten Zielsystemapplikationen. Darüber hinaus sind nicht alle VPN-Technologien gleich sicher. Aufgrund unserer Erfahrung setzen wir auf SSH- und IPSec-basierte Verbindungen. Durch den Tunnel kann der Fernwarter dann mit beliebigen TCP-basierten Anwendungen auf das Wartungsobjekt zugreifen. TLS/SSL-basierte VPNs empfehlen wir hingegen nicht, für sie werden regelmäßig gravierende Schwachstellen aufgedeckt.

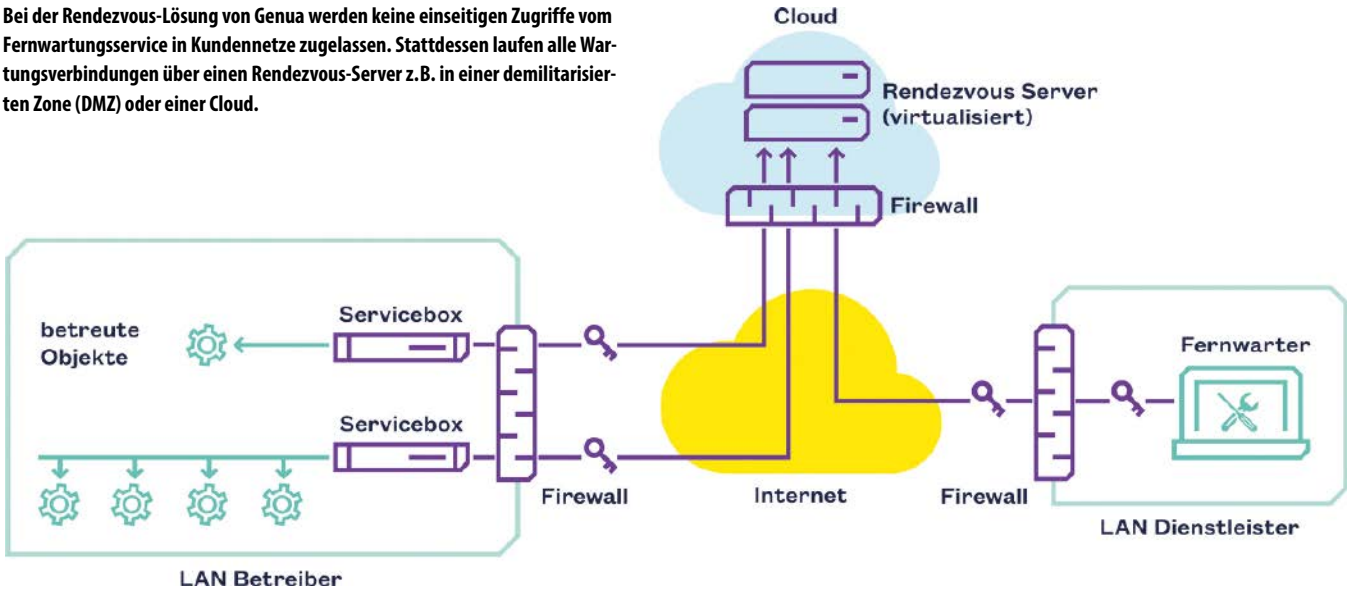
Risiken und Einfallstore

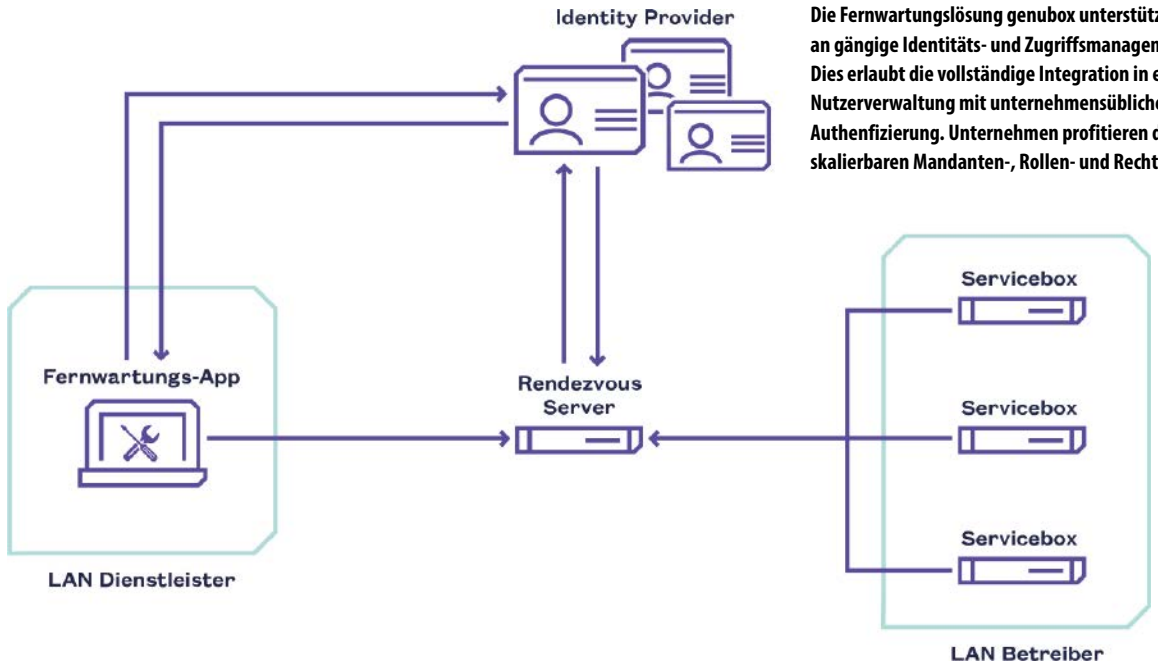
Dem Betreiber muss klar sein, dass diverse Angriffsvektoren vorhanden sind. Das beginnt mit der Bedrohung von Innen durch Fehlverhalten von Mitarbeitenden. Die Bandbreite reicht hier von der Beantwortung von Phishing-Mails über bewusste Sabotage bis hin zu kompromittierten Client-PCs. Extern lauert die Gefahr durch das Abgreifen von Zugangsdaten oder das Ausnutzen von Schwachstellen z.B. bei IoT-Geräten.

Im Rahmen seiner Analysen und Industriekooperationen zur Cyber-Sicherheit hat das BSI die Top10 der gefährlichsten Cyber-Bedrohungen für Industrieanlagen zusammengestellt:

- 1. Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme
- 2. Infektion mit Schadsoftware über Internet und Intranet
- 3. Menschliches Fehlverhalten und Sabotage
- 4. Kompromittierung von Extranet und Cloud-Komponenten
- 5. Social Engineering und Phishing
- 6. (D)DoS Angriffe
- 7. Internet-verbundene Steuerungskomponenten
- 8. Einbruch über Fernwartungszugänge
- 9. Technisches Fehlverhalten und höhere Gewalt
- 10. Soft- und Hardwareschwachstellen in der Lieferkette.

Bei der Rendezvous-Lösung von Genua werden keine einseitigen Zugriffe vom Fernwartungsservice in Kundennetze zugelassen. Stattdessen laufen alle Wartungsverbindungen über einen Rendezvous-Server z.B. in einer demilitarisierten Zone (DMZ) oder einer Cloud.





Die Fernwartungslösung genubox unterstützt die Anbindung an gängige Identitäts- und Zugriffsmanagementsysteme. Dies erlaubt die vollständige Integration in eine zentrale Nutzerverwaltung mit unternehmensüblicher Multifaktor-Authenfizierung. Unternehmen profitieren damit von skalierbaren Mandanten-, Rollen- und Rechte-Konzepten.

Klar sein muss sich der Anlagenbetreiber über die Priorisierung der unterschiedlichen Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Unbestreitbarkeit, denn sie benötigen unterschiedliche Sicherheitsmaßnahmen. Für den Schutz von Verfügbarkeit und Integrität helfen technische Maßnahmen wie Datendioden, Firewalls oder redundante Systeme. Vertraulichkeit und Authentizität werden mithilfe einer eindeutigen Authentifizierung beim Zugriff abgesichert. Hinzu kommen verschlüsselte Datenleitungen, sichere Protokolle, sowie Hashes und digitale Signaturen. Beim Thema Unbestreitbarkeit helfen sichere Audit-Logs und revisionssichere Lösungen. Sie halten konkret fest, wer was wann getan hat.

Schutz für IoT-Geräte

Um industriell genutzte IoT-Geräte zu schützen, empfehlen wir u.a. folgende Maßnahmen:

- Regelmäßige Sicherheitsprüfungen der Betriebstechnik, um mögliche Schwachstellen zu ermitteln.
- Nutzung von speziell auf die Industrie zugeschnittene Lösungen zur Überwachung, Analyse und Erkennung des Netzwerkverkehrs, um sich vor Angriffen zu schützen, die Prozesse und Anlagen bedrohen.
- Überprüfung der Sicherheit und Kontrolle vorhandener Zertifikate vor dem Einbau neuer IoT-Komponenten.
- Einschätzung des Herstellerumgangs mit Schwachstellen: Werden diese transparent gemeldet und umgehend behoben?
- Ersetzen der Standardpasswörter durch starke Zahlen/Buchstabenkombinationen oder Nutzung eines Passwort-Manager-Programms.
- Vertraulichkeit bei sensiblen Informationen wie Seriennummern, IP-Adressen, vor allem keine Verbreitung über soziale Medien etc.
- Dauerhaftes Informieren über den aktuellen Stand bzgl. Schwachstellen und Sicherheitslücken bei IoT-Geräten.

Services für Security

Wir nehmen am Markt nicht nur eine wachsende Sensibilität für die Risiken durch Fernwartungszugänge wahr, verbunden mit dem Wunsch nach vertrauenswürdigen Lösungen, sondern auch eine steigende Nachfrage nach begleitenden Managed Services, denn Expertise in der IT- und OT-Security ist angesichts des Fachkräftemangels ein rares Gut. Diese Bedarfe adressieren wir gemeinsam mit unserem Partner Deutsche Telekom Security. Das Unternehmen bietet ein flexibles Managed-Service-Paket für die sichere Fernwartung in der Industrie an, also für Industrial Remote Access Service (RAS). Die Architektur dieses Magenta Secure Industrial RAS (MSIRAS) hostet unseren Genubox Rendezvous-Server mit dem zugehörigen Central Management System Genucenter in einer Virtual Private Cloud (VPC) innerhalb der Open Telekom Cloud. Genubox wurde von uns speziell für industrielle Umgebungen entwickelt und erfüllt alle Empfehlungen des BSI an eine sichere Fernwartung. Die Open Telekom Cloud bietet ‚Infrastructure as a Service' aus einer Public Cloud aus deutschen Hochsicherheitsrechenzentren. Die Deutsche Telekom Security unterstützt darüber hinaus mit ihren mehr als 1.600 Sicherheitsexperten Kunden je nach Anforderungen bei der Realisierung des Fernzugriffs, von der Grobplanung der Architektur und Prüfung der Standortvoraussetzung über die Integrationsplanung und Migration bis hin zum Betrieb inklusiv CERT-Management und Überwachung.

Security ist ein Dauerlauf

Ein Vorteil cloudbasierter Lösungen für Fernwartungszugänge liegt sicher in der guten Skalierbarkeit. Aus IT-Security-Sicht ist die konkrete technische Umsetzung der Fernzugriffslösung maßgeblich und nicht die Frage, ob das System in einer Public Cloud gehostet wird. Entscheidend ist auch hier, dass ausschließlich authentisierte externe Anwender Zugriff auf vorher spezifizierte Dienste und Zielsysteme erhalten sowie ein feingranulares, ausgereiftes Rechte- und Rollensystem gemäß Zero-Trust-Prinzipien. Ganz wichtig: Sicherheit ist kein einmaliger Sprint, sondern ein Dauerlauf, der aufmerksame Anwender und Experten mit Fachwissen nach dem Stand der Technik benötigt.

Markus Maier,
Product Owner Industrieprodukte,
Genua, München

■ www.genua.de