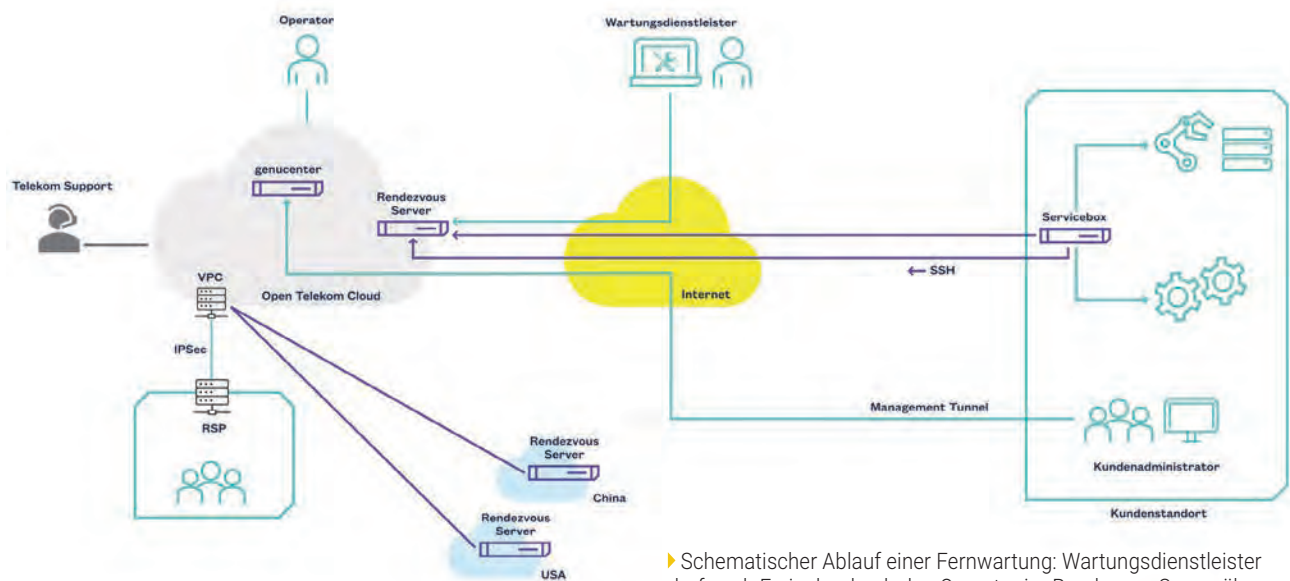


Sichere Fernwartung – leicht gemacht

Keine Chance für Cyber-Brechstangen



► Schematischer Ablauf einer Fernwartung: Wartungsdienstleister darf nach Freigabe durch den Operator im Rendezvous-Server über die Servicebox auf die zu wartende Maschine zugreifen.



Artikel
anhören!



Online-Kriminelle haben die OT für sich entdeckt – das zeigen u.a. rasant steigende Zahlen von Ransomware-Vorfällen. Einfallstore sind meist unzureichend überwachte oder mangelhaft implementierte Fernwartungszugänge. Eine Kooperation der Deutschen Telekom Security und der Firma Genua stellt jetzt sicher, dass auch Unternehmen ohne große IT-Abteilungen auf sie zugeschnittene Fernwartungssysteme nutzen können. Die MSIRAS genannte Lösung vereint in Deutschland entwickelte und gefertigte Sicherheitsprodukte mit quantenresistenter Verschlüsselung mit dem professionellen 7x24-Management eines nationalen Netzbetreibers in dessen deutschen Rechenzentrum. Anwender erhalten alle Leistungen für sichere industrielle Fernwartung aus einer Hand – von der Planung über die Installation bis hin zum Betrieb und Service.

Cyberattacken kosten die deutsche Wirtschaft durch Datendiebstahl, Sabotage und Industriespionage mehr als 200 Mrd. Euro pro Jahr. Eines der empfindlichsten Einfallstore ist der Fernwartungszugang. Da Reparaturen ohne aufwändige Anreise bei den Betreibern durch Automatisierung und Digitalisierung immer einfacher geworden sind, erfolgen Wartung und Programmierung von Komponenten zum Beispiel in der Energieversorgung, Fabrikautomation oder Verkehrsleittechnik immer häufiger aus der Ferne – und öffnen so kriminellen Kräften Tür und Tor. Laut BSI zählt der Einbruch von Cyberkriminellen

über diesen Weg zu den besonders kritischen und am häufigsten auftretenden Bedrohungen für die Anlagensicherheit – mit steigender Tendenz.

Ein Beispiel: Ransomware-Agenten nutzen schlecht abgesicherte Remote-Zugänge, um sich Zugang zu OT-Netzen zu verschaffen. Das Risiko für die OT steigt derzeit überproportional, da die Angreifer die häufig noch veralteten OT-Netze ohne Schutz für sich entdeckt haben. Mit dem Druck, die Produktion schnellstmöglich wieder zum Laufen zu bekommen, steigen schnell die Chancen für eine Ransom-Zahlung.

Handlungsbedarf ist offensichtlich

Dass diese Einfallstore gesichert werden müssen, ohne ins analoge Zeitalter zurückfallen zu müssen, zeigt auch ein Blick in die täglichen Nachrichtensendungen: Laut Bundesamt für Verfassungsschutz zeigen Cyber-Attacken eine neue Qualität. Sie werden von internationalen Geheimdiensten mit Personal und Ressourcen unterstützt. Hinzu kommt, dass die Angriffe immer ausgefeilter werden.

Dass die Dringlichkeit beim Thema Cybersicherheit stetig zu nimmt, hat auch

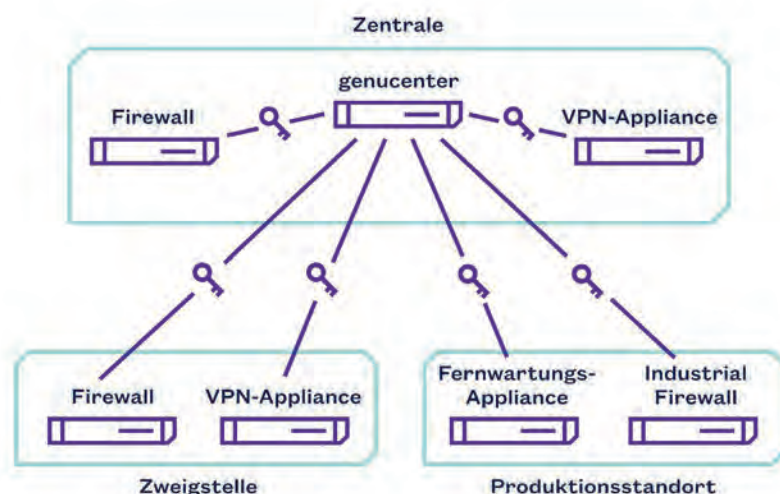


die Europäische Union erkennt und in ihrer zweiten Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2) den verpflichtenden Schutz kritischer Infrastrukturen angeordnet. Unternehmen und Organisationen aus den Bereichen Energie, Wasser, Verkehr, Gesundheit, Banken sowie digitale Infrastruktur müssen seit Oktober 2024 auch in Deutschland Mindeststandards einhalten. Bei Verstößen drohen empfindliche Strafen: Bußgelder bis zu zehn Millionen Euro oder 2 Prozent des Jahresumsatzes und sogar die persönliche Haftung der Geschäftsleitung stehen auf dem Spiel.

Sichere Konzepte für den Fernzugriff

Angesichts der drohenden Schäden durch Cyberangriffe und der möglichen Strafen wählen immer mehr Unternehmen die hochsichere Fernwartungslösung Genubox von Genua. Seit einigen Jahren gehört das Unternehmen zur Bundesdruckerei-Gruppe und entwickelt seine Lösungen speziell für industrielle Umgebungen stetig weiter. Zusammen mit dem Genucenter, das wie eine Leitstelle für ein Netzwerk aus Sicherheitsgeräten fungiert, erfüllt Genubox alle Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) an eine sichere Fernwartung. Mit ihr erhalten nur befugte Personen Zugriff auf sensible industrielle Netze.

Alle Verbindungen in die Anlage zur Analyse oder Wartung werden im Fall von MSIRAS über einen Rendezvous-Server im deutschen Rechenzentrum der Telekom in Bielefeld abgewickelt. Zu diesem Treffpunkt bauen der externe Instandhalter und ein Verantwortlicher auf Betreiberseite zu einem fest verabredeten Zeitpunkt eine Verbindung auf. Erst mit diesem aktiven Schritt des Anwenders entsteht die durchgängige Verbindung, die zum Informationsfluss der Wartungszwecke notwendig ist. Maschinenwerte und Fehlermeldungen können anschließend ausgelesen und bearbeitet werden. Dabei werden Zero-Trust-Prinzipien konsequent umgesetzt. Der externe Service bewegt sich nur im zuvor definierten Zielsystem und Rollenbild, und der Zugriff bleibt zeitlich und räumlich beschränkt. Hierzu nutzt



► Struktur des Genucenters: Firewalls und Zugriffe auch komplexer Strukturen können zentral verwaltet werden.

Genua das robuste, offene und anwendungsgenaue SSH-Protokoll.

Komplexe Sicherungskonzepte mit MSIRAS meistern

Allerdings erfordert Planung, Einrichtung und Installation der genua-Lösung entsprechendes Knowhow und IT-Kapazitäten. Und auch im laufenden Betrieb wollen Fragen beantwortet, Updates durchgeführt und Erweiterungen vorgenommen werden. Für diejenigen Betriebe, die hier Unterstützung von Sicherheitsexpertinnen und -experten nutzen möchten, hat die Deutsche Telekom Security gemeinsam mit Genua den 'Magenta Secure Industrial Remote Access Service' – kurz MSIRAS – für die sichere Fernwartung in der Industrie entwickelt. MSIRAS kombiniert die sicheren Fernwartungslösungen von Genua, sicher implementiert und betrieben in einem deutschen Rechenzentrum, mit begleitenden Managed Services der Deutschen Telekom Security.

Das Managed-Services-Paket nutzt eine vertrauenswürdige, in Deutschland gehostete Cloudplattform um die virtuellen Maschinen von genua zu betreiben. Die VPC (Virtual Private Cloud) erfüllt höchste Datenschutzstandards und garantiert DSGVO-konforme Sicherheit – frei von außereuropäischen Einflüssen. Durch georedundante Rechenzentren, höchste Verfügbarkeitsstandards und regelmäßige unabhängige Prüfungen bietet sie eine sehr hohe Betriebssicherheit.

Zum Managed Service MSIRAS gehören zwei Service-Level, die die Verfügbarkeit absichern:

- S72 bietet eine Terminvereinbarung innerhalb von acht Stunden und eine Entstörfrist innerhalb 72 Stunden. Das entspricht 99,17 Prozent Verfügbarkeit im Jahr.
- Noch schneller ist der S24-Service-Level, der 24/7 eine Terminvereinbarung innerhalb von zwei Stunden und eine Entstörfrist innerhalb 24 Stunden bietet. Das entspricht 99,72 Prozent Verfügbarkeit im Jahr.

Die Rollen beim neuen Angebot MSIRAS sind also klar verteilt: Die Deutsche Telekom Security unterstützt mit ihren mehr als 1.600 Sicherheitsexperten und realisiert die Fernzugriffe. Sie plant die Architektur, prüft die Standortvoraussetzungen und migriert bestehende Systeme. Im Betrieb überwacht sie die Nutzung und hilft bei Problemen. Genua stellt für dieses Angebot den technischen Kern zur Verfügung und sorgt dafür, dass mit Genubox und Genucenter sowohl Hard- als auch Software höchsten Standards genügen und aktuell gehalten werden.

Gemeinsam helfen Deutsche Telekom Security und Genua IT- und OT-Verantwortlichen den Überblick zu behalten und die Fernwartung effizient und sicher zu verwalten. So können sich Anwender auf ihre Kernkompetenz konzentrieren, die Resilienz ihrer Produktion stärken und gemeinsam mit ihren Zulieferern und Dienstleistern dafür sorgen, dass die Anlagen produktiv bleiben. ■

Genua GmbH
www.genua.de