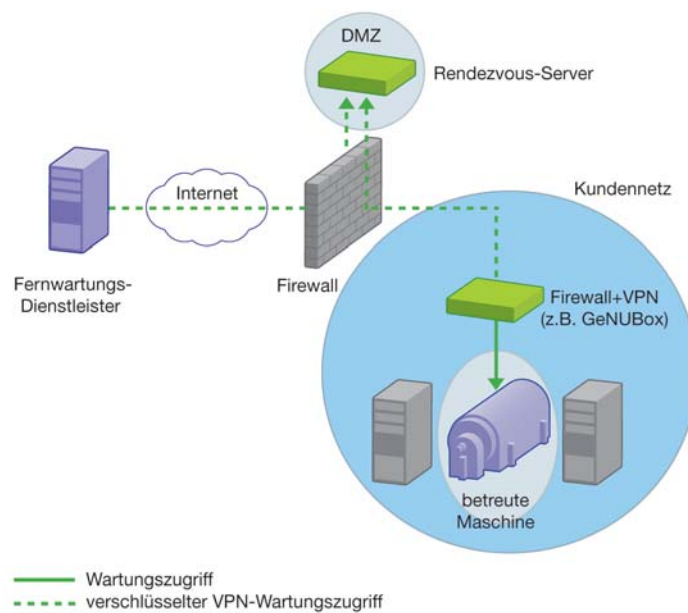


## Fernwartung über Rendezvous-Server



### Verabredung in der DMZ

# Sichere Fernwartung über zentralen Rendezvous-Server

Fernwartungs-Lösungen sind dank moderner IT-Technologie, weltweiter Vernetzung und schneller Datenübertragung problemlos zu realisieren. Die Herausforderung stellt sich an anderer Stelle: Wie behalten große Industrieunternehmen, die Fernwartungs-Services von mehreren Herstellern nutzen, die zahlreichen Zugriffsmöglichkeiten in ihre Netzwerke im Blick? Auf der anderen Seite stehen die Anlagen-Hersteller vor der Aufgabe, eine Vielzahl von Fernwartungs-Verbindungen zu ihren verschiedenen Kunden zu betreiben. Die zentralen Anforderungen sind hier: einfache Anwendung, flexible Einsatzmöglichkeiten, einheitliche Administration und vor allem auch zuverlässige IT-Sicherheit. Stuxnet hat gerade aufgezeigt, wie Produktionsanlagen weltweit massenhaft infiziert werden können, wenn diese komplett vernetzt, aber nicht ausreichend gesichert sind. Wir zeigen, wie diese Aufgabe sicher gelöst werden kann.

Die Vorteile einer Fernwartungs-Lösung liegen auf der Hand: Die Anlagen werden von erfahrenen Spezialisten des Herstellers fortlaufend überwacht und gewartet, ohne dass diese vor Ort sein müssen. Sollte trotz regelmäßiger Pflege eine Störung auftreten, können die Spezialisten via Wartungsverbindung zugreifen und die meisten Probleme umgehend lösen. Die erforderliche IT-Technologie ist ausgereift, schnelle Datenleitungen nahezu überall kostengünstig vorhanden. Fernwartungs-Lösungen sparen somit Zeit und Geld – davon profitieren sowohl der Wartungs-Dienstleister als auch der Anlagen-Anwender. Aus die-

sem Grund werden immer mehr Fernwartungs-Lösungen in der Industrie, dem Gesundheitswesen und anderen Bereichen eingesetzt.

### Fernwartung mit Nebenwirkungen

Diese Vorteile sind überzeugend, der zunehmende Einsatz von Fernwartungs-Lösungen ist aber mit erheblichen Nebenwirkungen verbunden. Denn die Anlagen, die betreut werden sollen, sind bei den Anwendern in die lokalen Netze (LAN) eingebunden. Für den Fernzugriff muss dem Dienstleister also ein Zugang in das LAN des Anwenders eingeräumt werden. Damit ist direkt der sensible Be-

reich der IT-Sicherheit bei der Anwenderfirma betroffen. Hier muss sichergestellt werden, dass über den Wartungszugang tatsächlich nur der Dienstleister in das LAN gelangt und keine unbefugten Dritten. Als weitere Sicherheitsstufe sollte der externe Zugriff auf das betreute Objekt begrenzt sein. Denn viele Unternehmen betreiben im Produktionsbereich ein flaches Netz, an das alle Systeme angebunden werden. Wer einmal Zugang erlangt hat, kann somit ungehindert im gesamten Kunden-LAN 'herumsurfen'. So konnte z. B. zuletzt der Schadcode Stuxnet innerhalb kurzer Zeit eine große Anzahl von Steuerungssystemen für Maschinenanlagen infizieren.

## Vielfalt an Lösungen erschwert Absicherung

Je mehr Wartungszugänge in ein LAN geführt werden, desto schwieriger ist die Absicherung. Denn es werden eine Vielzahl von Fernwartungs-Lösungen verwendet, die über unterschiedliche Wege eine Verbindung zur betreuten Anlage aufbauen: über Modem, ISDN, DSL oder Internet sowie mit verschiedenen VPN-Standards (Virtual Private Network) zur verschlüsselten Datenübertragung. Industrieunternehmen mit größeren Maschinenparks verfügen zumeist über ein gewachsenes Konglomerat solcher Lösungen. Für dieses Sammelsurium unterschiedlicher Lösungen müssen auf der Firewall wiederum eine Vielzahl an Ports freigeschaltet werden. Manchmal wird die Firewall sogar umgangen und die Verbindung direkt an die betreute Anlage im LAN gelegt. Mit jedem offenen Port und besonders natürlich durch die Umgehung der Firewall steigt die Gefährdung durch unberechtigte Zugriffe, Hacker-Attacken und Viren, die ganze Produktionsstraßen lahm legen können. Zu regelrechten Löchern werden diese Schwachstellen, wenn bei der Administration der diversen Zugänge Fehler unterlaufen oder die regelmäßige Pflege aufgrund des hohen Aufwands vernachlässigt wird. Dies kann schnell passieren, da jedes Fernwartungs-System andere Anforderungen stellt und einzeln betreut werden muss.

## Viele Wege führen zum Kunden

Am anderen Ende der Verbindung stehen die Wartungs-Dienstleister zumeist vor ähnlichen Problemen: Auch hier ist ein vielfältiges Portfolio an Fernwartungs-Systemen gewachsen, das umständlich zu bedienen ist und großen Aufwand bei der Administration erfordert. „Mit welcher Software und welchem Modem ist die Anlage beim Kunden XY zu erreichen“, ist eine häufig gestellte Frage in Service Centern. Auch für den Dienstleister ist es wichtig, dass sein Zugang in das Kundennetz zuverlässig gesichert ist. Denn sollte sich herausstellen, dass über diesen Weg beispielsweise ein Virus in das Netz gelangt ist und Schäden angerichtet hat, würde sich dies mit Sicherheit auf die weitere Beziehung zu dem Kunden auswirken.

Beide Seiten – Anwender und Dienstleister – haben somit ein großes Interesse an einer Fernwartungs-Lösung, die diese Kriterien erfüllt:

- Einfache Bedienung
- Komfortable Administration
- Hochwertige IT-Sicherheit
- Flexible Einsatzmöglichkeiten

## Sichere Lösung für alle Zugriffe: Rendezvous in der DMZ

Zur Fernwartung von Maschinenanlagen in sensiblen Produktionsbereichen bietet das deutsche IT-Sicherheitsunternehmen GeNUA eine Lösung, in dessen Mittelpunkt ein Rendezvous-Server steht. Das Konzept: Es werden keine einseitigen Wartungszugriffe von Herstellern in das Netz des Industrieunternehmens zugelassen. Stattdessen führen alle Fernwartungs-Zugriffe auf einen Rendezvous-Server, der in einem speziellen Bereich neben der Firewall, der so genannten demilitarisierten Zone (DMZ), installiert ist. Hierhin kommt das Industrieunternehmen dem Hersteller mit einer Verbindung von innen aus dem Produktionsbereich entgegen. Erst wenn es auf dieser zentralen Wartungsplattform zum Rendezvous kommt, kann der Hersteller die jetzt durchgängige Verbindung zum Zugriff auf die betreute Anlage nutzen. Der Rendezvous-Server kann sowohl in der DMZ des Dienstleisters oder auch des Kunden eingerichtet werden. Da der Kunde zu einem verabredeten Zeitpunkt selbst aktiv werden muss, hat er stets den Überblick, wer wann in seinem Netz unterwegs ist.

## VPN-Verfahren SSH verhindert Verbreitung von Schadcode

Die Verbindungen zu dem Rendezvous-Server werden mit dem VPN-Verfahren (Virtual Private Network) SSH aufgebaut, das starke Verschlüsselungs- und Authentifizierungs-Methoden bietet. So kann die Datenkommunikation nicht abgehört werden, und nur berechnete Teilnehmer erhalten Zugang zur Wartungsplattform in der DMZ. Das Protokoll SSH unterscheidet sich zudem in einem wesentlichen Punkt vom dem VPN-Verfahren IPsec, das andere Herstellern häufig zum Aufbau von Fernwartungs-Verbindungen verwenden: IPsec erzeugt immer eine vollständige Koppelung zwischen den verbundenen Netzen. Sollte ein Rechner in einem Netz mit Schadcode infiziert sein, kann er in allen via IPsec an-



Appliance GeNUBox für sichere Fernwartung

gebundenen Netzwerken ungeschützte Systeme befallen und sich rasant ausbreiten. Mit SSH werden dagegen nur die tatsächlich notwendigen Verbindungen zwischen einzelnen Rechnern erzeugt, so dass Schadcode keine schnellen Verbreitungswege findet.

## Kein Weiterkommen: Firewall isoliert Wartungsbereich

Bei der Lösung von GeNUA sorgt im Produktionsbereich zusätzlich die Fernwartungs-Appliance GeNUBox für Sicherheit. Sie wird an der per Fernzugriff betreuten Anlage installiert und separiert mit einer Firewall-Funktion den Wartungsbereich vom den anderen Systemen in diesem Netzbereich. So führt die SSH-Verbindung ausschließlich zum Wartungsobjekt – Zugriffe auf andere Systeme im Netz der Produktionsabteilung sind nicht möglich. Selbst wenn Schadcode bis hierhin vordringen sollte, kann er von dieser isolierten Anlage aus keine weiteren Systeme infizieren. Über den Rendezvous-Server können beliebig viele Fernwartungs-Verbindungen zusammengeführt werden. Da Bedienung und Administration über einheitliche Oberflächen erfolgen, kann mit geringem Aufwand ein sicheres Fernwartungs-System mit vielen Teilnehmern aufgebaut und betrieben werden. Um neue Teilnehmer in die Lösung einzubinden, wird an der jeweiligen Gegenstelle lediglich eine Fernwartungs-Appliance installiert. Zahlreiche große Maschinenbau-Unternehmen wie der Motorenhersteller MAN Diesel und der Druckmaschinen-Spezialist manroland nutzen diese komfortable Lösung von GeNUA, um ihre weltweit installierten Anlagen per Fernzugriff zu betreiben und ihren Kunden somit guten Service zu bieten. ■

[www.genua.de](http://www.genua.de)



Autorin: Dr. Michaela Harlander, Geschäftsführerin GeNUA mbH