

Komfortable und sichere  
Fernwartungs-Zugriffe

# Rendezvous in der DMZ



Wer große Anlagen wie Druckmaschinen, Fertigungsroboter, Stromgeneratoren oder Computertomografen für viel Geld beschafft, verlangt vom Hersteller die Zusicherung des störungsfreien Betriebs.

Sollte durch den Ausfall eines Systems beispielsweise eine ganze Fertigungsstraße stillstehen, summieren sich die Kosten schnell auf beträchtliche Summen – den Image-Verlust durch verspätete Lieferungen und verärgerte Kunden noch gar nicht mitgerechnet. Die geforderte, hohe Betriebszuverlässigkeit können Hersteller nur durch ständige Betreuung ihrer Anlagen via Fernwartung garantieren. Solche 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 Unternehmen, die Fernwartungs-Services von mehreren Herstellern nutzen, die zahlreichen Zugriffsmöglichkeiten in ihre Netzwerke hinein 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 zuverlässige IT-Sicherheit. Gelöst werden kann diese Aufgabe mit Fernwartungs-Lösungen, die auf bewährten Standards und durchdachten Sicherheits-Konzepten basieren.

## Die Basis: durchdachte Sicherheitskonzepte

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 diesem Grund werden immer

Foto: Siemens Pressebild

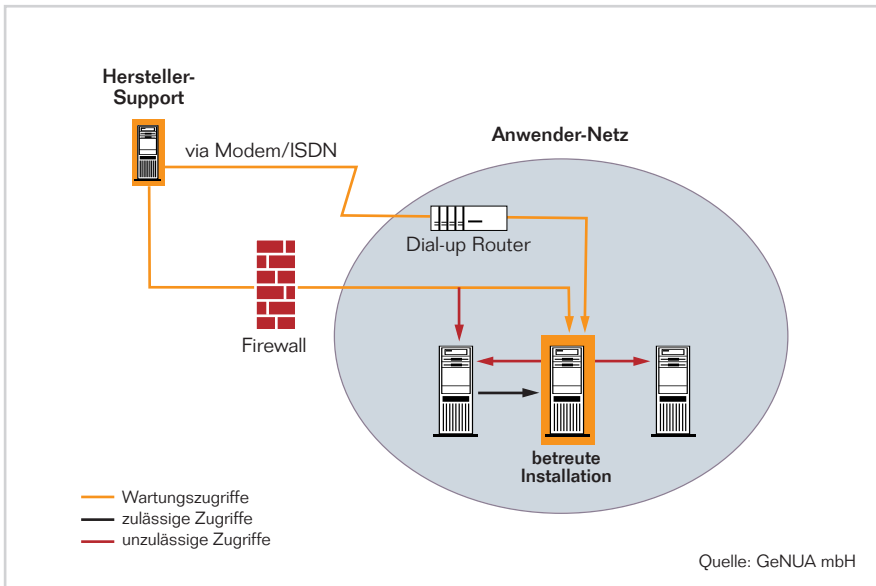


Bild 1: Der unverschlüsselte Fernwartungszugang.

meist 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 auf-

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 Bereich 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 die meisten Unternehmen betreiben nur ein flaches Netz, an das alle Systeme angebunden werden. Wer einen Zugang hat, kann somit leicht im gesamten Kunden-LAN „herumsurfen“ und zum Beispiel auf Produktionsanlagen von Wettbewerbern oder die Server der Entwicklungsabteilung zugreifen – also äußerst sensible Systeme und Daten.

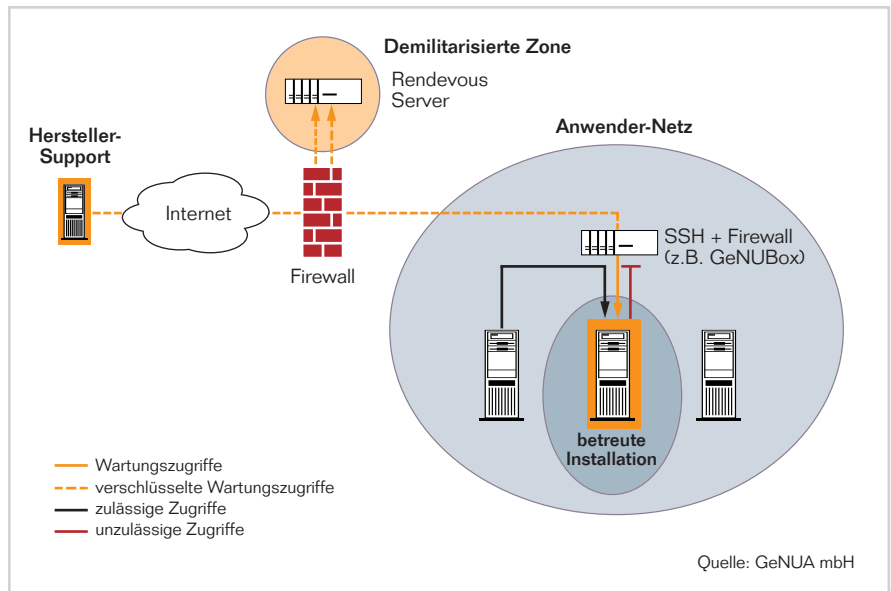


Bild 2: Die Fernwartung über einen Rendezvous-Server.

### 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. Firmen mit einem größeren Maschinenpark verfügen zu-

grund 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 zu meist vor ähnlichen Problemen: Auch hier ist ein vielfältiges Portfolio an Fernwartungs-Systemen gewachsen, das umständlich zu bedienen ist und großen Aufwand bei der Administra-

tion 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 Fernwartungslösung, die diese Kriterien erfüllt:

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

### Sichere Lösung für alle Zugriffe

Das deutsche IT-Sicherheitsunternehmen GeNUA bietet Lösungen für dieses Anforderungsprofil. Im Mittelpunkt dieser Lösung steht ein Rendezvous-Server. Das Konzept: Es werden keine einseitigen Zugriffe von Wartungsdienstleistern in das Netz des Kunden zugelassen. Stattdessen führen alle Fernwartungszugriffe auf einen Rendezvous-Server, der in einem speziellen Bereich neben der Firewall, der so genannten demilitarisierten Zone (DMZ), installiert ist. Hierhin kommt der Kunde

dem Dienstleister mit einer Verbindung von innen aus dem Wartungsbereich entgegen. Erst wenn es auf dieser zentralen Wartungsplattform zum Rendezvous kommt, kann der Dienstleister 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.

Die Verbindungen zu dem Rendezvous-Server werden über öffentliche Netze wie das Internet mit einem VPN-Gateway aufgebaut. Dabei wird das VPN-Standardprotokoll SSH verwendet, das starke Verschlüsselungs- und Authentifizierungsverfahren bietet. So ist sichergestellt, dass die Datenkommunikation nicht abgehört werden kann und nur berechnete Teilnehmer Zugang zur zentralen Wartungs-Plattform in der DMZ bekommen.

### Sicherheit im Kundennetz

Innerhalb des Kundennetzes sorgt zusätzlich die Fernwartungs-Appliance GeNUBox für Sicherheit. Sie wird an der betreuten Anlagen installiert und erzeugt die SSH-Verbindung zum Rendezvous-Server. Darüber hinaus separiert sie mit einer integrierten Firewall-Funktion den Wartungsbereich

vom restlichen Netzwerk. So führt die SSH-Verbindung ausschließlich zum Wartungsobjekt – Zugriffe auf andere Systeme im Netz des Kunden sind nicht möglich. Ein weiteres nützliches Merkmal ist die Applikationsplattform. Hier können Anwendungen installiert werden, um die GeNUBox als intelligentes Tool vor Ort bei der Anlage einzusetzen: Sie kann komplexe Aufgaben erledigen wie etwa die Steuerung und Wartung von Maschinen oder aufwändige Datenanalysen. Aufgrund der robusten und wartungsfreien Konstruktion ist die Appliance auch für den Einsatz in rauen Industrieumgebungen geeignet.

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 Fernwartungssystem mit vielen Teilnehmer aufgebaut und betrieben werden. Um neue Teilnehmer in die Lösung einzubinden, wird an der jeweiligen Gegenstelle lediglich eine Fernwartungs-Appliance installiert.



Dr. Michaela Harlander