# Sichere Fernwartungszugriffe

Michael Sorg

Telekom Deutschland GmbH
PSSM Inhouse
Nauheimer Strasse 101
70372 Stuttgart
m.sorg@telekom.de

**Abstract:** Die folgende Arbeit befasst sich mit dem Thema der Fernwartungszugriffe. Welche Arten von Fernwartungszugängen sind in der Praxis zu finden und welche sicherheitstechnischen Gefahren ergeben sich daraus. Weiterhin wird ein Konzept vorgestellt, welches durch Einsatz eines Rendezvous-Servers eine Erhöhung des Security-Levels ermöglicht.

## 1 Einführung und Begriffserklärung zum Thema Fernwartung

### 1.1 Was ist Fernwartung?

Als Fernwartungen kann man alle Tätigkeiten bezeichnen, die ausgeführt werden, ohne das an dem zu wartenden System ein ausführender Techniker physisch vor Ort präsent sein muss. Eine Fernwartung kann „online“ oder „offline“ realisiert werden. Die Fernwartung eines Systems, die durch eine z.B. zugesande CD realisiert wird, welche ein selbstausführendes Updateprogramm enthält, entspricht einer „offline Fernwartung“. Eine „online Fernwartung“ entspricht dem Zugriff, eines aus LAN-Sicht externen Partners, welcher sich, im Regelfall, über das Internet und ein Zugangssystem auf das zu wartende System verbindet und die vorzunehmenden Wartungsarbeiten vornimmt. Die vorliegende Produktstudie befasst sich mit der Sicherung der „online Fernwartung“.

### 1.2 Wozu wird Fernwartung benötigt?

Gerade im Zeitalter der Globalisierung expandieren nationale Firmen in weit verstreute Standorte. Diese Globalisierung hat zur Folge, dass die Systeme vor Ort zu administrativen Zwecken nur unter erhöhten Aufwänden zur „direkten“ Konfiguration erreichbar sind. Auch Hersteller, welche ihren Abnehmern regelmäßige Updates und Wartungen, sowie Service- und Instandhaltungsarbeiten anbieten, benötigen eine Möglichkeit die dezentral aufgestellten Systeme zentral zu administrieren und auch zu steuern. Hierzu dient die Fernwartung. Durch einen Fernwartungszugriff ergeben sich folgende Vorteile:

- ermöglicht Administratoren und Herstellern einen zentralen Zugriff auf dezentral aufgestellte Systeme
- Zielsysteme sind 7x24h, rund um die Uhr, erreichbar
- Relevante und wichtige Daten können auf das System geladen werden
- Relevante und wichtige Daten können von dem System geladen werden
- Kein physikalischer Zugang zum System nötig

### 1.3 Wie realisiert man eine Fernwartung?

Wie bereits in 1.1 beschrieben werden im Regelfall die Fernwartungszugriffe über das Internet realisiert, denn über das Internet hat man die Möglichkeit eines weltumfassenden Netzes, welches bis auf die Einwahlkosten des Providers kostenlos zur Verfügung steht. Der Zugriff auf die zu wartenden Systeme wird in der Regel über ein von dem Hersteller vorgegebenes Verfahren bereitgestellt. Hierzu dient ein logisches Interface für den administrativen Zugang auf dem System. Der Zugriff auf dieses Interface ist dann von dem jeweiligen Netzbetreiber zu Wartungszwecken freizuschalten. Solche Zugriffe sind, aufgrund des Zugriffsweges über das Internet, meist verschlüsselte Verfahren, wie HTTPS-, SSH- oder VPN-Zugriffe. Durch diese Verfahren sind die in der Verbindung gesendeten Daten vor der Einsicht Dritter geschützt.

### 1.4 Welche Gefahren ergeben sich aus dem jetzigen Zugriffsverfahren?

Sollte ein Fernwartungszugriff nicht durch ein verschlüsseltes Zugriffsverfahren bereitgestellt werden, besteht die Möglichkeiten durch Man-in-the-Middle Attacks oder Snifferattacken, das sicherheitsrelevante Daten, wie z.B. Passwörter oder Ablaufprozesse, von Dritten im Internet, aber auch im LAN mitgelesen und ausgenutzt werden können. Bild 1.4.1 zeigt den unverschlüsselten Zugriff auf ein System

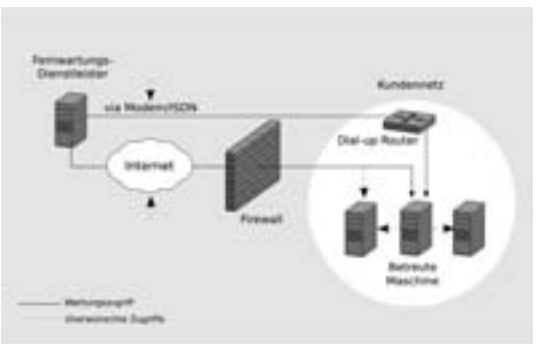


*Bild 1.4.1*

Der verschlüsselte Fernwartungszugriff verhindert zwar die Möglichkeiten Dritter im Netz, die Verbindung mitzulesen, der verschlüsselte Zugriff beschränkt aber auch den lokalen Administrator zu überprüfen, welche Verbindungen oder Handlungen durch die verschlüsselte Verbindung durchgeführt werden. Ein Fernwartungszugriff öffnet somit eine „Türe“ in das LAN der jeweiligen Firma und stellt somit ein Sicherheitsrisiko dar. Da sich zu wartende System oft in einem bestehenden Computernetzwerk befinden, besteht die Möglichkeit von einem zu wartenden System weiter auf andere Systeme zu „springen“ oder durch Spionagemaßnahmen weitere Informationen über die interne Netztopologie eines LANs zu erhalten, was zu weiteren Angriffsmaßnahmen genutzt werden kann. Die Möglichkeiten einen freigeschalteten Zugriff auf ein System boshaft auszunutzen sind groß. Es gilt somit den Zugriff so sicher wie möglich, aber auch so transparent wie möglich zu gestalten. *Bild 1.4.2* zeigt den verschlüsselten Fernwartungszugriff und noch bestehende Gefahren

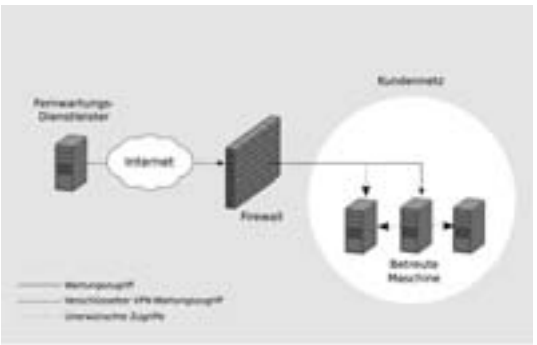


*Bild 1.4.2*

# 2 Realisierung einer sicheren Fernwartung

## 2.1 Allgemeine Konzeptbeschreibung

Das Konzept einer sicheren Fernwartung besteht aus dem logischen Separieren des zu wartenden Systems vom LAN. Bei einem Zugriff auf das System ist somit kein „Weiterspringen“ oder ein Sniffing auf andere bestehende Verbindungen möglich. Weiterhin lässt das vorliegende Konzept keine Verbindungen direkt vom Internet in das LAN, also auf das zu wartende System, zu. Man bringt durch das Zwischenschalten von sogenannten Rendezvous-Servern die internen Systeme in die Lage nach der Signalisierung eines Wartungswunsches die Verbindung auf das wartende System zu initialisieren. Durch dieses Konzept besteht die Möglichkeit eine verschlüsselte Verbindung über das Internet bereitzustellen, die Verbindungen aber auf den Rendezvous-Servern aber durch entschlüsseln, transparent und prüfbar zu machen (z.B auf Viren oder bekannte Angriffsverfahren). Weiterhin ist kein direkter Zugriff auf das System im LAN möglich, da dieses erst eine Verbindung zu Rendezvous-Server aufbauen muss, damit ein Fernwartungszugriff stattfinden kann. *Bild 2.1.1* zeigt eine Übersicht der Topologie mit integrierten Rendezvous-Servern.

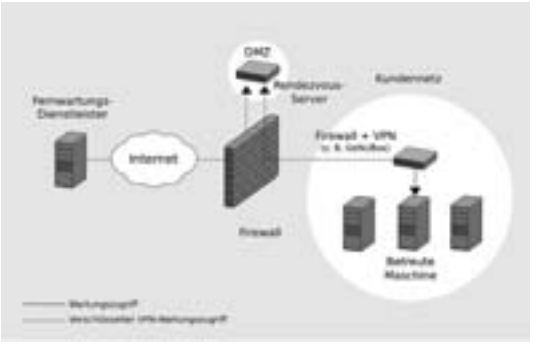


*Bild 2.1.1*

## 2.2 Technische Hintergründe

Der Rendezvous-Server wird, wie in Bild 2.2.1 zu sehen, in einer DMZ (demilitarisierte Zone) platziert. Das System ist somit physikalisch und logisch vom internen Netz getrennt. Eine weitere Firewall+VPN-Box wird im LAN platziert. An diesem System befindet sich auch ein Zugang zu dem zu wartenden System. Der externe Partner verbindet sich via SSH auf den Rendezvous-Server. Die Verbindung über das Internet ist somit verschlüsselt und nicht mitlesbar. Der Rendezvous-Server ist durch eine geeignet Authentifizierung und Authoriziering, vorzugsweise mittels Zertifikaten, in der Lage die Gegenstelle zu identifizieren. Der SSH-Tunnel endet auf dem Rendezvous-Server und wird hier auch entschlüsselt. Der Rendezvous-Server kann nun sehen, auf welches interne System eine Wartungsverbindung erstellt werden soll. Durch die Zuordnung des gesuchten Systems zu einer internen Firewall+VPN-Box wird hier ein Signal für einen Verbindungswünsch übermittelt. Dieses Signal ist ein administratives Protokoll, welches die vom Absender übermittelten Daten enthält. Dieses Protokoll wird über einen IPSEC-VPN verschlüsselt und ist somit auch nicht von Dritten im internen Netz mitlesbar. Wenn das zu wartende System das Signal für einen Verbindungswunsch erhält, überprüft es die Absenderdaten. Es besteht bis hierhin noch keine direkte Verbindung von dem Fernwarter auf das zu wartende System. Stimmen die gesendeten Parameter mit der internen Policy des Systems überein, baut das zu wartende System eine verschlüsselte Verbindung zu dem Rendezvous-Server auf. Gleichzeitig wird das System von den GenuBoxen durch die Zuweisung in ein eigens generiertes VLAN logisch aus dem internen Netz getrennt und in eine eigene Zone „geschoben“. Ist die geschehen, verbindet der Rendezvous-Server in der DMZ die externe Verbindung und die interne Verbindung miteinander. Der externe Techniker kann nun so verschlüsselt über das Internet und durch das LAN des jeweiligen Kunden auf ein zu wartendes System zugreifen. Die logische Umgebung gestaltet sich so, als ob sich das zu wartende System in einem eigenen Wartungsnetz befindet und so isoliert ist.

## 2.3 Vorteile des Zugriffsverfahrens

Diese Lösung eliminiert alle genannten Risiken und bietet folgende Vorteile:

- Der Einfluss des Fernwarters und alle damit verbundenen Gefährdungen beschränken sich auf den kleinstmöglichen Bereich um das Wartungsobjekt herum.
- Ein FernwartungsZugriff ist ohne Mitwirkung oder Zustimmung des KundennetzAdministrators unmöglich.
- Außer auf dem Wartungsobjekt selber können die Aktionen des Fernwarters auch auf der GeNUBox und dem RendezvousServer im Klartext protokolliert werden.
- Der externe VPN-Tunnel schützt den FernwartungsZugriff vor Abhören, Verändern oder Übernahme der Sitzung.
- Der interne VPN-Tunnel verhindert einen direkten Zugriff des Fernwarters auf Kundensysteme, die sich nicht im Bereich des Wartungsobjektes befinden.

- Die Filterfunktion der GeNUBox verhindert einen Zugriff des Fernwarters vom Wartungsobjekt aus auf Kundensysteme, die sich nicht im Bereich des Wartungsobjektes befinden.
- Diese Fernwartungslösung ist unabhängig vom Typ der bereits vorhandenen Firewall des Kunden.

## Literaturverzeichnis

[Bilder] www.genua.de