Sichere Fernwartung
mit GeNUBox und Rendezvous-Server

Zusammenfassung

In diesem Dokument wird eine Fernwartungslösung zur Wartung beliebiger Systeme in den IT-Netzwerken von Kunden vorgestellt. Ausgehend von einer Diskussion der Schwächen, die die üblichen Wartungszugänge aufweisen, werden schrittweise die deutlichen Verbesserungen beschrieben, die sich durch den Einsatz zunächst des GeNUBox-Systems von GeNUA und schließlich eines Rendezvous-Servers im Firewall-System ergeben.

1 Einführung

Die Fernwartung von Rechnersystemen ist ein Thema mit wachsender Bedeutung. Ein Grund dafür ist die steigenden Zahl von Betreibern, die die Pflege ihrer Systeme (bzw. eines Teils davon) im Rahmen eines Outsourcings an externe Dienstleister vergeben, um Kosten zu sparen.

Ein anderer Grund ist die Tatsache, dass fast alle Hersteller von komplexer Software, Hardware und computergestützten Industriesystemen von ihren Kunden einen netzbasierten Zugriff auf die gelieferten Systeme zu Wartungs- und Diagnosezwecken verlangen. Zu diesen Produkten gehören z.B. kundenspezifische Branchen-Softwarelösungen, Computer-Tomographen und Großgeräte wie Turbinen.

Für die Fernwartung muß das IT-Netz des Kunden partiell gegenüber dem Wartungsunternehmen geöffnet werden. Diese Öffnung ist grundsätzlich unvermeidlich, sollte aber aus Sicherheitsgründen so gering wie möglich gestaltet werden. An dieser Stelle stoßen die üblichen Implementierungen des Fernwartungszugriffs häufig auf Bedenken bei den Kunden, da sie unnötig große Teile des IT-Netzes offenlegen. Zudem sind Identifizierung und Authentisierung des zugreifenden Dienstleisters meist ungenügend gesichert.

Eine Verbesserung dieser Situation liegt offensichtlich im Interesse der Kunden, die Fernwartungs-Dienstleistung in Anspruch nehmen möchten (oder müssen), aber dabei keine wesentlichen Einschränkungen ihrer Netzwerksicherheit hinnehmen wollen. Aber auch auf Seiten der Fernwartungsdienstleister erhöht ein sicherheitstechnisch sauberes Zugriffskonzept die Akzeptanz ihrer Kunden.

In diesem Dokument wird ein solches Konzept schrittweise entwickelt. Dabei wird in Abschnitt 2 die typische Ausgangssituation des Kunden dargestellt, der sein IT-Netz gegenüber Fremdzugriffen abgesichert hat. Abschnitt 3 beschreibt die Risiken, die die üblichen Standardlösungen für Fernwartungszugriffe mit sich bringen. In Abschnitt 4 wird auf die gelegentlich vorgeschlagene Absicherung mittels IPSec und die damit verbundene Gefahr der unbeabsichtigten Kopplung mit anderen Kundennetzen eingegangen. Der Abschnitt 5 stellt schließlich den ersten Schritt des verbesserten Fernwartungskonzepts dar, in dem das Wartungsobjekt durch eine GeNUBox-Appliance von dem restlichen IT-Netz des Kunden isoliert wird. Schließlich beschreibt Abschnitt 6 den zweiten Schritt des Konzepts, in dem die gefährliche Öffnung der Firewall für Zugriffe von außen durch die Kopplung über einen Rendezvous-Server ersetzt wird.

Zur Verdeutlichung der Rollen wird im folgenden einheitlich vom *Fernwarter* und dem *Kunden* gesprochen. Als *Wartungsobjekt* wird das System (oder Ensemble von Systemen) bezeichnet, die durch den Fernwarter gepflegt werden sollen.

2 Ausgangssituation

Die Abbildung 1 zeigt die typische Netz-Topologie eines Kunden, der seine Verbindung zum Internet mit einer Firewall absichert. Diese Firewall läßt Zugriffe aus dem Kundennetz auf das Internet zu, blockiert aber Zugriffe aus dem Internet auf das Kundennetz.

Innerhalb des Kundennetzes ist das Wartungsobjekt lokalisiert, das möglicherweise anderen Systemen innerhalb des Netzes Dienste anbietet und deshalb von diesen angesprochen wird.

Der Fernwarter kann in dieser Konfiguration das Wartungsobjekt nicht erreichen, da seine Zugriffe an der Firewall blockiert werden.

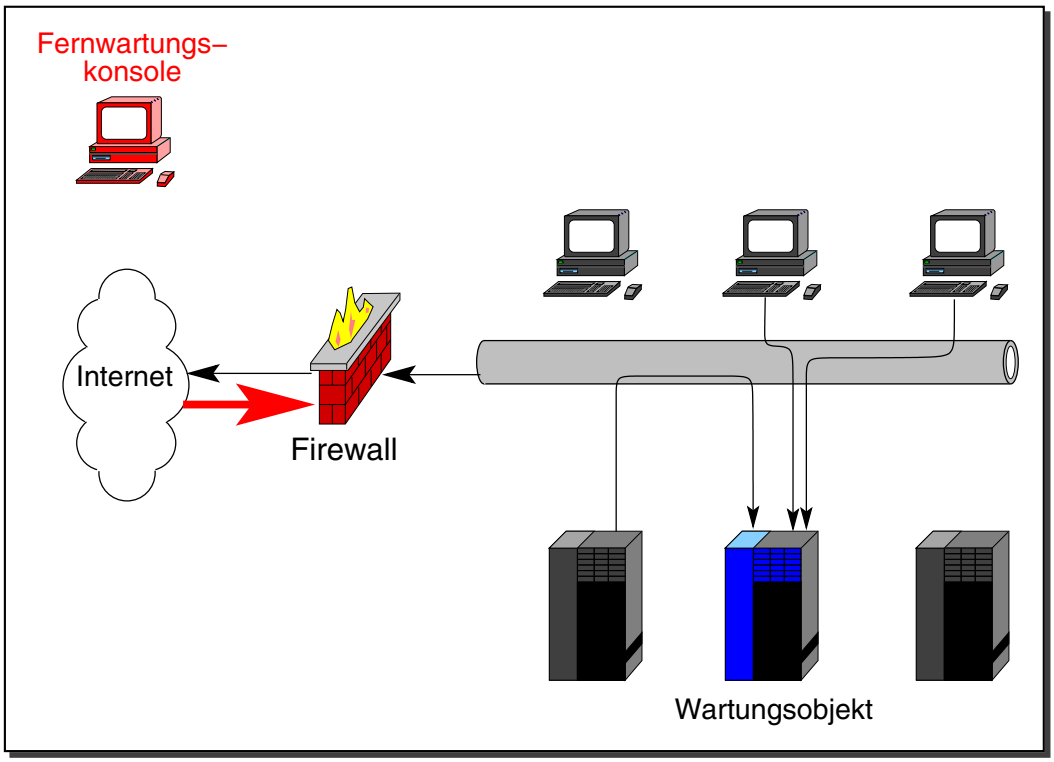

Abbildung 1: Ausgangssituation im Kundennetz

3 Die unbefriedigende Standardlösung

Um den Fernwartungszugriff zu ermöglichen, öffnet der Kunde in der Regel die Firewall für die Absender-IP-Adresse des Fernwarters und die Ziel-IP-Adresse des Wartungsobjektes. Diese Situation wird in der Abb. 2 dargestellt. Weitgehend analog dazu ist auch die Einrichtung eines weiteren Zugriffsweges per Modem oder ISDN an der Firewall vorbei.

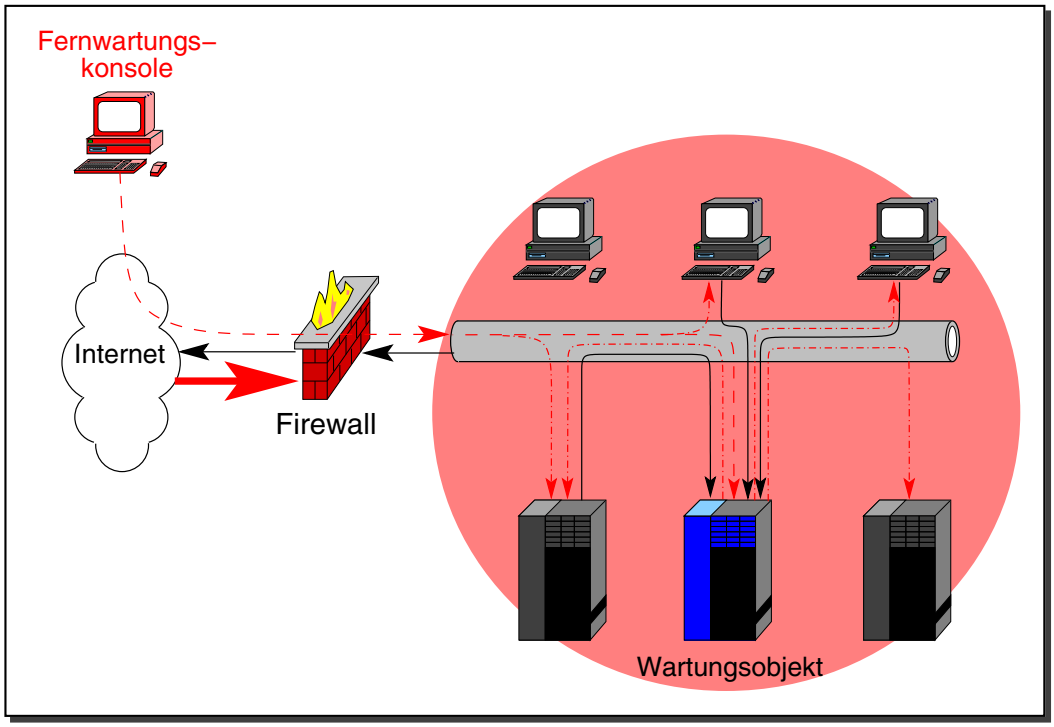

Abbildung 2: Unbefriedigende Standardlösung für Fernwartungszugriffe

In beiden Fällen kann der Fernwarter auf dem gestrichelt dargestellten Weg wie gewünscht auf das Wartungsobjekt zugreifen.

Diese Standardlösung eröffnet aber die folgenden Risiken:

1. Der Fernwarter wird nicht (oder ungenügend) identifiziert und für den Zugriff authentisiert. Damit besteht die Gefahr des Zugriffs durch Drittparteien.
2. Der Fernwartungszugriff kann abgehört und gegebenfalls durch Angreifer übernommen werden.
3. Nicht loyale Mitarbeiter der Herstellerfirma oder in deren Netz eingedrungene Eingreifer können von dem Wartungsobjekt aus auf andere Rechner des Kundennetzes zugreifen (strich-punktierte Linien).
4. Eventuell vorhandene Implementierungsfehler in der Firewall erlauben möglicherweise den direkten Zugriff auf andere Rechner des Kundennetzes ohne Benutzung des Wartungsobjekts.

Aufgrund dieser Risiken ist bei der Standardlösung das gesamte Kundennetz (schattiert unterlegter Bereich) gefährdet.

4 Gefährliche Scheinlösung: IPSec

Gelegentlich wird vorgeschlagen, den Fernwartungszugriff durch das VPN-Protokoll IPSec abzusichern, wie in Abb. 3 dargestellt. Dadurch werden tatsächlich die Risikofaktoren 1 und 2 aus der obigen Aufstellung behoben, die Faktoren 3 und 4 bleiben aber als fortbestehende Gefährdungen.

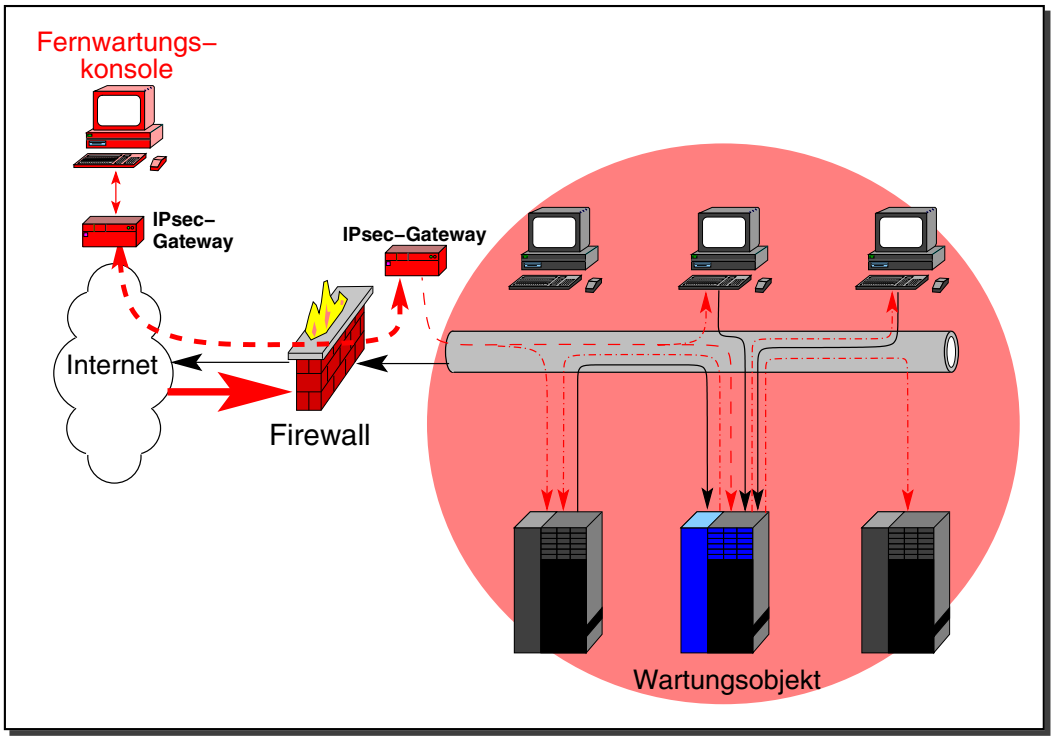

Abbildung 3: Fernwartungszugriff über IPSec-Tunnel

Darüberhinaus eröffnet dieser Lösungsversuch ein weiteres Risiko. Da IPSec einen vollkommen transparenten und **gerouteten** Netzzugriff implementiert, besteht nunmehr die Möglichkeit, daß die IT-Netze verschiedener Kunden, die gleichzeitig über IPSec gewartet werden, unbeabsichtigt miteinander kommunizieren können. Angesichts der Spezialisierung der Fremdwarter auf Wartungsobjekte, die wiederum häufig branchentypisch sind, besteht die reelle Möglichkeit, dass dabei Netze miteinander konkurrierender Unternehmen miteinander in Kontakt geraten. Dieses Szenario ist in Abb. 4 dargestellt.

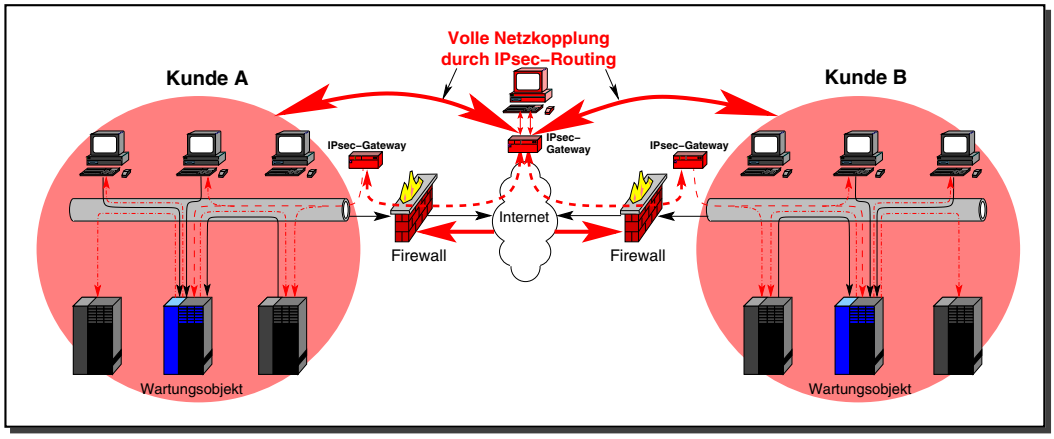

Abbildung 4: Kopplung von Kundennetzen durch IPSec-Routing

5 Erster Lösungsschritt: Einsatz der GeNUBox

Zwei Maßnahmen sind notwendig, um die in Abschnitt 3 aufgezeigten Hauptrisiken zu vermeiden.

- Durch den Einsatz von VPN-Techniken werden die Risikofaktoren 1 und 2 eliminiert. Dafür ist das SSH-Protokoll ausgezeichnet geeignet. Gegenüber dem im vorstehenden Abschnitt genannten IPSec-Verfahrens bietet es den Vorteil einer flexibleren und individuelleren Identifizierung des Fernwarters (Ausschaltung von Risikofaktor 1), während die starke Verschlüsselung das Abhören und Verändern der Kommunikation bzw. die Übernahme der Sitzung durch einen Angreifer verhindert (Ausschaltung von Risikofaktor 2).
- Durch eine weitere Filterfunktion wird das Kundennetz in zwei Bereiche unterteilt. Dabei ist der eine Bereich, der das Wartungsobjekt enthält, vom Fernwarter erreichbar, während der andere, größere Bereich ihm nicht zugänglich ist. Es ist sehr vorteilhaft, wenn die Filterung auf OSI-Schicht 2 (im *bridging mode*) erfolgen kann. Bei der üblichen Filterung auf OSI-Schicht 3 (im *routing mode*) wäre zusätzlich eine Restrukturierung des Kundennetzes in zwei eigenständige Subnetze erforderlich, die durch den *bridging mode* vermieden wird.

Die beiden Funktionen eines VPN-Gateways auf der Basis von SSH und eines Paketfilters als zusätzliche Firewall im *bridging mode* sind in dem System GeNUBox von GeNUA miteinander vereint (siehe [1]). Die GeNUBox wird – wie in der Abb. 5 gezeigt – an der Schnittstelle der beiden oben erwähnten Bereiche des Kundennetzes platziert.

Der Fernwarter baut zunächst einen VPN-Tunnel zur GeNUBox auf (breite gestrichelte Linie) und wird dort authentisiert. Durch den Tunnel kann er dann (mittels des *Local-Forward*-Mechanismus von SSH) mit beliebigen TCP-basierten Anwendungen auf das Wartungsobjekt zugreifen (dünne gestrichelte Linie).

Die Paketfilter-Funktion der GeNUBox wird so konfiguriert, dass bestehende Zugriffsmöglichkeiten anderer Kundensysteme auf das Wartungsobjekt nicht beeinträchtigt werden (durchgehende Linien). Dagegen unterbindet der Filter unerlaubte Verbindungen,

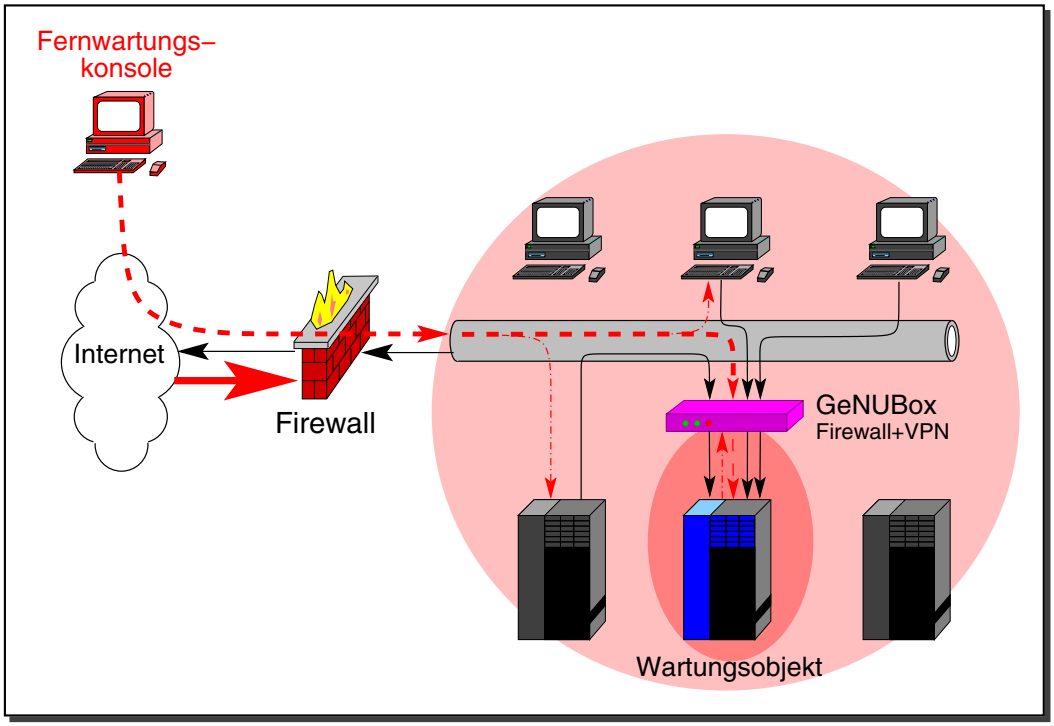

Abbildung 5: Isolation des Wartungsobjekts durch GeNUBox

die der Fernwarter wissentlich oder unwissentlich vom Wartungsobjekt zu anderen Kundensystemen aufzubauen versucht. Damit beschränkt sich die Gefährdung durch den Fernwartungszugriff im wesentlichen auf den Bereich des Wartungsobjekts (dunkel unterlegte Fläche).

Als Restrisiko bleibt der oben genannten Faktor 4, der eine Gefährdung des Kundennetzes nur beim Vorliegen einer Fehlfunktion der Haupt-Firewall ermöglichlicht. Diese Gefährdung erstreckt sich auf den hell unterlegten Netzbereich in Abb. 5.

6 Zweiter Lösungsschritt: Einsatz eines Rendezvous-Servers

Das im vorstehenden Abschnitt genannten Restrisiko kann schließlich vermieden werden, indem die direkte Einwahl des Fernwarters in das Kundenetz unterbunden wird. Stattdessen wird ihm lediglich die Verbindung zu einem Rendezvous-Server erlaubt, der in einer *Demilitarisierten Zone* (DMZ) der Haupt-Firewall angeordnet ist. Dieser Server kann vorteilhaft ebenfalls mit einem GeNUBoxCompact-System realisiert werden. Diese Situation ist in Abb. 6 dargestellt.

Für den Fernwartungszugriff baut der Fernwarter zunächst einen SSH-Tunnel zum Rendezvous-Server auf. Von dort aus darf er allerdings keine Verbindung zum Kundennetz aufbauen, entsprechende Verbindungswünsche werden von der Firewall unterbunden. Erst wenn durch den Administrator des Kundennetzes ein weiterer Tunnel von der

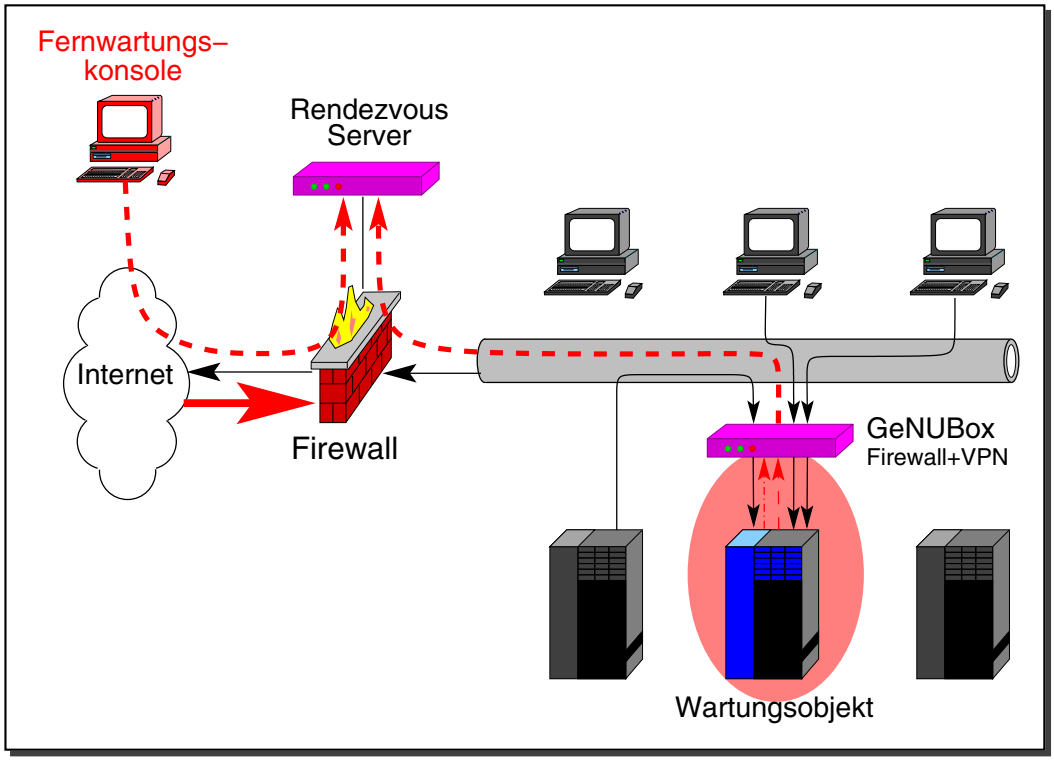

Abbildung 6: Rendezvous-Verfahren am Server in der Firewall-DMZ

GeNUBox zum Rendezvous-Server aufgebaut wird, öffnet sich dem Fernwarter ein gangbarer Weg zum Wartungsobjekt. Im einzelnen enthält der gesamte Vorgang die folgenden Schritte:

(a) Der Fernwarter startet lokal eine SSH-Client-Anwendung und baut eine Verbindung zum Rendezvous-Server auf. Dabei werden für alle von der Wartungssoftware benötigten TCP-Ports entsprechende *local forwarding*-Einträge auf den Rendezvous-Server konfiguriert.

(b) Der Fernwarter identifiziert sich am Rendezvous-Server, bei erfolgreicher Authentisierung wird der VPN-Tunnel zwischen dem Rechner des Fernwarters und dem Rendezvous-Server aufgebaut.

(c) Der Administrator des Kundennetzes startet eine SSH-Client-Anwendung auf der GeNUBox und baut eine Verbindung von innen auf den Rendezvous-Server auf. Für alle von der Wartungssoftware benötigten TCP-Ports werden dabei *remote forwarding*-Einträge auf das Wartungsobjekt konfiguriert. Vor Aufbau des Tunnels wird außerdem auf der GeNUBox vor dem Wartungsobjekt der Filtersatz für den Produktiveinsatz durch einen **Wartungsfiltersatz** ersetzt, welcher im Extremfall das Wartungsssytem vollkommen vom Restnetz isoliert.

(d) Sofern eine Authentisierung bei Verbindungsaufbauten von innen konfiguriert wurde, muss sich der Administrator identifizieren. Im Erfolgsfall wird der VPN-Tunnel zwischen GeNUBox und Rendezvous-Server aufgebaut.

(e) Der Fernwarter startet seine Wartungssoftware, die sich durch den externen VPN-Tunnel, den Rendezvous-Server und den internen VPN-Tunnel mit dem Wartungsobjekt verbindet. Nach erfolgreicher Authentisierung des Fernwarters auf dem Wartungsobjekt können die Arbeiten beginnen.

(f) Nach Abschluss der Wartungsarbeiten beendet der Fernwarter erst die getunnelte Verbindung zum Wartungsobjekt und anschließend den externen VPN-Tunnel zwischen seinem lokalen Rechner und dem Rendezvous-Server. Der Administrator löscht den internen VPN-Tunnel zwischen GeNUBox und Rendezvous-Server.

Diese Lösung eliminiert alle im Abschnitt 3 genannten Risiken und bietet die folgenden 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 Kundennetz-Administrators unmöglich.
- Außer auf dem Wartungsobjekt selber können die Aktionen des Fernwarters auch auf der GeNUBox und dem Rendezvous-Server 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.

Literatur

[1] *GeNUBox Technische Beschreibung*, GeNUA, 2005

© 2005 GeNUA mbH Revision: 0.1