FactSheet

Sicherung Ihrer Datentransportwege mittels OpenVPN

Branche IT / Infrastructure Management

Beschreibung

Um eine Sicherung Ihrer Datentransportwege zu gewährleisten, setzt die Dynamic Software GmbH auf die OpenSource-Software OpenVPN, welche unter anderem folgende Einsatzszenarien abdeckt:

- Sichere Übertragung des Netzverkehrs über ein unsicheres Medium (z.B. Internet, oder Telefonleitungen)
- Anbindung an das Firmennetz für Homeoffice- oder Aussendienst-Mitarbeiter
- Anbindung von Filialen an die Zentrale ohne teure Standleitungen mieten zu müssen
- Absicherung von WLAN gegen Missbrauch oder Ausspähen der Daten
- bei Bedarf können auch kleine Gateway-Rechner eingesetzt werden, mit denen der Zugriff für die User vollkommen transparent erfolgen kann – der User merkt nichts von der Verschlüsselung der Daten.
- Ein solcher Gateway-Rechner kann bei Bedarf auch die Rolle eines DSL-Routers übernehmen
- alles unabhängig vom Standort der „entfernten" Seite - egal ob über WLAN im Nachbargebäude oder über Internet aus Australien

Clients sind für Windows, Mac OS X und Linux verfügbar und sehr einfach zu bedienen.

Eine gute VPN-Software wie OpenVPN setzt nicht nur auf **Verschlüsselung**, mit der etwa unternehmenskritische Daten während der Übertragung vor der Ausspähung durch Unbefugte gesichert werden kann. Ungleich wichtiger ist die **kryptographische Absicherung** (Authentifizierung) des Datenverkehrs. Hiermit stellen beide Kommunikationspartner sicher, dass die Datenpakete auch wirklich von der Gegenseite kommen und nicht von einem Angreifer gefälscht wurden.

Die **Identifizierung** und **Authentifizierung** geschieht bei OpenVPN entweder über vorab vereinbarte „**Passwörter**" (sog. Pre-Shared Keys), oder über **SSL-Zertifikate**. Das gleiche Schema, das schon bei https (für sichere Webserver) zum Einsatz kommt, wird auch hier verwendet. Eine zentrale Stelle (sogenannte Certification Authority, welche auch unter Ihrer Kontrolle stehen kann) erstellt für den öffentlichen Schlüssel jedes VPN-Teilnehmers (auch für das zentrale Gateway) ein Zertifikat. Mit diesem Zertifikat weist sich der VPN-Teilnehmer beim zentralen Gateway aus, welches auf Grund dieses Zertifikats in der Lage ist, die Vertrauenswürdigkeit des VPN-Teilnehmers zu überprüfen ohne ihn vorher zu kennen. Das VPN-Gateway muss dazu lediglich das **Root-Zertifikat** der zentralen Stelle kennen.

Der Einsatz von OpenSource-Software (OSS) bietet eine Sicherheit, mit der nur wenige kommerzielle Softwareanbieter mithalten können. Da bei OSS der Quellcode von jedermann einsehbar ist, können Fehler und Sicherheitslöcher viel schneller gefunden werden. Gerade bei einer VPN-Software ist ein solcher Vorteil von entscheidender Bedeutung. „Sicherheit durch Verschleierung" (Security by Obscurity) ist ein Ansatz, den viele Anbieter von kommerzieller Sicherheitssoftware bevorzugen. Wenn man aber den eben genannten OSS-Aspekt betrachtet, ist ein öffentlicher Review des Quellcodes ein wesentlich besserer Ansatz, da so Sicherheitslöcher schneller behoben werden können.

Welche Leistungen im Zusammenhang mit OpenVPN bietet Ihnen Dynamic Software?

- Planung Ihrer VPN-Infrastruktur
- Installation und Inbetriebnahme der OpenVPN-Server bzw. -Gateways
- Durchführung der OpenVPN-Konfiguration für Ihre Infrastruktur
- Optional übernehmen wir die Betriebsverantwortung mit definierten Service Level für Ihre Infrastruktur.

Technologien

Einsatzgebiet	Intranet, Internet
Server Komponenten	Open Source OpenVPN