Vorteile der ViPNet Technologie

Symmetrische Verschlüsselung

infotecs

Vorteile der ViPNet Technologie

Symmetrische Verschlüsselung

ViPNet ist eine Technologie mit symmetrischer Verschlüsselung. Dieselbe spezielle Verschlüsselungsmethode verwenden das Militär und Spezialdienste auf der ganzen Welt. Der Einsatz symmetrischer Verschlüsselung ermöglicht dem Benutzer den Aufbau einer Umgebung, welche beim IPSec grundsätzlich nicht möglich ist: eine Umgebung mit absoluter Sicherheit vor Man-in-the-Middle-Angriffen.

UDP-Transport

Der Grundgedanke symmetrischer Verschlüsselung besteht darin, dass jede Seite bereits vor Beginn des Datenaustauschs über einen Schlüssel verfügt, mit dem die Verschlüsselung erfolgt. Dabei kann auf das TCP-Protokoll, also auf sog. Reliable Delivery verzichtet und die UDP-Kapselung für den gesamten Datenverkehr verwendet werden. Die Vorteile eines solchen Prozesses sind offensichtlich:

- UDP wird als Transportprotokoll von allen Echtzeitanwendungen benutzt, d. h. solche Anwendungen werden von ViPNet per se unterstützt (IP-Telefonie, Videokonferenz, Medien-Streaming u. ä.).
- Der Wechsel von einem Netzwerk in ein anderes Netzwerk (z. B. von 4G zu WiFi) läuft für den Benutzer (und die Anwendungen) transparent ab, ohne dass für die sichere Verbindung eine erneute Einwahl durchgeführt werden muss. (Bei IPSec wäre eine wiederholte Einwahl erforderlich.) Es erfolgt lediglich die automatische Änderung des Routings auf der Netzwerkschicht.

Übertragen in die Praxis bedeutet dies, dass ein mobiler Benutzer sich frei mit seinem VPN-Client bewegen kann und keinen Gedanken an die Wiedereinwahl in das VPN, nicht erreichbare Dienste oder übrige Verbindungsprobleme verschwenden muss.

Ständige Authentifizierung und Resistenz gegen Störungen

Bei symmetrischer Verschlüsselung besitzt jedes Knotenpaar des privaten Netzwerks seinen eigenen Schlüssel für den Informationsaustausch. Dieser Schlüssel selbst wird bei der Verschlüsselung jedoch nicht verwendet, stattdessen kommt eine Ableitung von ihm zum Einsatz. Dabei wird jedes neue ausgehende Paket im ViPNet Netzwerk durch eine neue Schlüsselableitung verschlüsselt. Auf diese Weise werden folgende Ziele erreicht:

- Die Teilnehmer authentifizieren sich gegenseitig mit jedem ankommenden IP-Paket.
- Der Schlüssel kann durch Abfangen von Daten nicht ermittelt werden.
- Verbindungen können durch Manipulation oder Beschädigung einzelner Pakete nicht beeinträchtigt werden – jedes Paket ist selbstständig. Um die Kommunikation zwischen den Knoten zu unterbrechen, müsste der Traffic komplett blockiert werden.

Resistenz gegen Kompromittierung

In IPSec verfügt jeder Knoten über lediglich einen privaten Schlüssel, der für den Verbindungsaufbau zu jedem beliebigen anderen Knoten verwendet wird. Bei ViPNet hingegen besitzt jeder Knoten mehrere separate Schlüssel, und zwar für die Verbindung zu jedem einzelnen der anderen Knoten des privaten Netzwerks. Ein Schlüssel existiert nur in dem Fall, wenn die entsprechende Verbindung durch den Administrator explizit erlaubt ist. Selbst bei Kompromittierung eines Schlüssels, welcher zum Schutz einer Punkt-zu-Punkt-Verbindung verwendet wird, hat dies keinen Einfluss auf die Sicherheit der Verbindungen mit allen anderen Knoten.

Gleichrangiges Netzwerk

ViPNet verfügt über Knoten mit gesonderten Funktionen. Mit diesen Knoten können neue Schlüssel generiert (ViPNet Network Manager) oder die zuverlässige Übermittlung von Schlüssel-Updates garantiert sowie die Informationen über den Zustand der einzelnen Knoten aktualisiert werden (ViPNet Coordinator). Dennoch handelt es sich bei diesem Netzwerk, im Hinblick auf den echten Benutzerdatenverkehr, um ein Peer-to-Peer-Netzwerk. Das bedeutet, jeder Knoten kann Daten an jeden anderen Knoten direkt übermitteln und dabei die Infrastruktur-Komponente umgehen. Der Austausch von verschlüsselten Daten zwischen zwei Computern findet unmittelbar innerhalb eines LANs und nicht über den Coordinator statt. In IPSec ist der Versand des gesamten Datenverkehrs über das Gateway unumgänglich, selbst wenn zwei nah beieinander stehende Computer Daten austauschen. Diese Notwendigkeit führt dazu, dass IPSec zum Datenschutz in lokalen Netzwerken nicht eingesetzt werden kann. Dabei lauert, statistisch gesehen, dort die größte Gefahr für Datendiebstahl.

Nahtlose Integration

Für den Anschluss an das ViPNet Netzwerk werden spezielle ViPNet Clients verwendet, welche für die am meisten verbreiteten Plattformen (Windows, Android, Mac OS) verfügbar sind. Die Clients werden in das Betriebssystem so eingebettet, dass der Benutzer den Zugang zum privaten Netzwerk erhält, ohne dabei die Netzwerkeinstellungen des Betriebssystems neu konfigurieren zu müssen. Im privaten Netzwerk werden lediglich die Daten verschlüsselt versendet, welche für die anderen VPN-Teilnehmer bestimmt sind. Andere Systemeinstellungen sind nicht erforderlich.

Schlüsselstruktur

Im ViPNet Netzwerk basiert das symmetrische Verschlüsselungsverfahren auf speziell erstellten Schlüsseln. Der Austausch von Zertifikaten und Signaturen ist nicht notwendig. Man-in-the-Middle-Angriffe sind unmöglich, weil keine Schlüsselinformationen über öffentliche, ungesicherte Wege übermittelt werden müssen. Alle übertragenen Daten sind ab dem ersten Byte zuverlässig geschützt.

Das verschachtelte Schlüsselsystem von ViPNet besteht aus vier unabhängigen Schlüsseldistributionen:

- Austausch-Schlüssel: Durch Ableitungen dieser Schlüssel wird der Datenaustausch zwischen den Netzwerkknoten verschlüsselt.
- Knoten-Schutzschlüssel: Durch diese Schlüssel werden Austauschschlüssel eines bestimmten Netzwerkknotens verschlüsselt.
- Benutzer-Schutzschlüssel: Durch diese Schlüssel werden Knoten-Schutzschlüssel verschlüsselt.
- Passwortschlüssel: Durch diese Schlüssel werden Benutzer-Schutzschlüssel verschlüsselt.

Für eine höhere Widerstandsfähigkeit basieren die ersten drei Schlüsseldistributionen auf einem separaten Masterschlüssel und der Passwortschlüssel wird auf Basis des Benutzerpassworts generiert.

Die Knoten- und die Benutzer-Schutzschlüssel sind dafür vorgesehen, Austausch-Schlüssel zu schützen und diese im Falle einer Kompromittierung zu ersetzen. Die Verschlüsselung des Datenverkehrs erfolgt paketweise. Für jedes einzelne Paket wird anhand des Austausch-Schlüssels ein eigener Schlüssel generiert, der für das jeweilige Absender-Empfänger-Paar vorgesehen ist. So kann der eingesetzte Schlüssel auch durch Abfangen des verschlüsselten Datenverkehrs nicht ermittelt werden. Ebenso können keine Schlüsselcontainer missbraucht werden, wenn das Benutzerpasswort nicht bekannt ist.

Die Anzahl der Austausch-Schlüssel auf jedem Client ist gleich der Anzahl der Verbindungen dieses Clients zu anderen Clients des ViPNet Netzwerks. Jeder „Client-to-Client"-Schlüssel ist einmalig. Das Hinzufügen von Verbindungen und die Aktualisierung der Schlüssel erfolgen für Benutzer absolut transparent.

Technologie der virtuellen Adressen

Die ViPNet Clients bieten abgesehen von der Verschlüsselung noch eine Reihe weiterer Funktionen. Eine dieser Funktionen ist die Unterstützung virtueller Adressen. Eine virtuelle Adresse ist eine gewöhnliche IP-Adresse, die ausschließlich innerhalb des ViPNet Netzwerks und nur auf der Anwendungsschicht existiert, d. h. das Betriebssystem kennt diese Adressen nicht. Virtuelle Adressen werden jedem Knoten automatisch zugewiesen und zwar so, dass innerhalb eines Netzwerks keine Adressen doppelt vorkommen. Diese Technologie ermöglicht eine „Out-of-the-Box"-Verbindung von einem privaten Netzwerk zu anderen Netzen mit gleichen IP-Adressenbereichen, ohne dass dabei IP-Adressen-Konflikte entstehen. Möchte ein Unternehmen seine Mitarbeiter im Home-Office an das Unternehmensnetzwerk anbinden und die Kommunikation zwischen diesen Mitarbeitern ermöglichen, erweist sich die ViPNet Technologie als sehr einfach in der Handhabung – obwohl die meisten privat verwendeten Router standardmäßig gleiche IP-Adressenbereiche vergeben.

Kontakt

Infotecs Internet Security Software GmbH
Oberwallstraße 24
10117 Berlin
Tel +49 30 206 43 66-0
Fax +49 30 206 43 66-66
Web www.infotecs.de
Mail info@infotecs.de

Marketing und Presse

Anja Müller
Tel +49 30 206 43 66-52
Mail presse@infotecs.de

Vertrieb

Josef Waclaw
Tel +49 30 206 43 66-14
Mail vertrieb@infotecs.de