ViPNet: eine andere Art VPN

Symmetrische Verschlüsselung

infotecs

ViPNet: eine andere Art VPN

Symmetrische Verschlüsselung

ViPNet bietet prinzipiell eine völlig neue Herangehensweise für den Aufbau der VPN-Infrastruktur: Die IT-Sicherheitslösung basiert auf symmetrischer Verschlüsselung. Klassische VPN-Lösungen hingegen verwenden asymmetrische Verschlüsselung auf Grundlage von IPSec. Im Gegensatz zu asymmetrischer Verschlüsselung benötigt symmetrische Verschlüsselung deutlich **weniger Rechnerleistung** und verfügt über eine **höhere Resistenz gegenüber Störungen** bei gleicher Widerstandsfähigkeit der Schlüssel. Aus diesem Grund setzen militärische Datenschutzsysteme und staatliche Behörden weltweit symmetrische Verschlüsselung für besonders vertrauliche Daten ein.

Ein weiterer wichtiger Vorteil von ViPNet gegenüber dem traditionellen IPSec liegt in der **Benutzerfreundlichkeit** der Technologie. Während bei ViPNet von Beginn an die einfache Bedienung für den Nutzer im Vordergrund stand, richtete sich IPSec historisch bedingt an die Belange einzelner Hersteller von Netzwerktechnik und berücksichtigte dabei die vorhandene Hardware. Die Technologie sollte zwar möglichst unkompliziert umgesetzt werden, die Konfiguration erforderte jedoch eine Fülle von herstellerspezifischen Fach- und Produktkenntnissen.

Als den virtuellen privaten Netzwerken schließlich der Marktdurchbruch gelang, wurde eine „benutzerfreundliche" Variante notwendig: VPN auf Basis von SSL (heutzutage TLS). Diese Technologie erfordert von Administratoren und Benutzern keine speziellen Fachkenntnisse. VPN mit SSL verlangsamt jedoch beachtlich den Datenaustausch und nimmt mehr Rechnerleistung in Anspruch. Für den Aufbau einer vollwertigen Sicherheitsumgebung unter Verwendung von IPSec- und SSL-VPN muss eine komplette PKI-Infrastruktur mit höchster Sicherheitsstufe aufgebaut und verwaltet werden. Die dafür benötigten Komponenten werden allerdings von den Hardware-Herstellern entweder nicht angeboten oder erfordern den Erwerb separater Lizenzen für Soft- und/oder Hardware. Für den Anwender, hinter welchem sich nicht in jedem Fall ein Technikexperte verbirgt, werden unnötige Hürden aufgebaut. Daraus resultiert oftmals eine mangelnde Sicherheit – obwohl dies der Hauptgrund für den Einsatz einer Sicherheitslösung ist.

Infotecs setzt seit Beginn der Entwicklung von ViPNet auf maximale Benutzerfreundlichkeit und Einfachheit für den Endbenutzer verbunden mit **zuverlässigem Schutz und hoher Geschwindigkeit**.

Zentralisierte Verwaltung

Datenschutz bedeutet nicht nur die Notwendigkeit widerstandsfähiger Kryptografie, sondern erfordert darüber hinaus die hochqualitative Administration der Sicherheitsinfrastruktur. ViPNet bietet eine einheitliche Herangehensweise zur Verwaltung von Schlüsselinformationen. Schlüssel können jederzeit ausgewechselt werden. Dies geschieht für den Benutzer vollkommen transparent, ohne dass die Verbindung unterbrochen oder eine zusätzliche Handlung seitens des Benutzers erforderlich wird.

Der Aktualisierungsvorgang für die ViPNet Software funktioniert in ähnlicher Form – **neue Versionen werden zentral verteilt und automatisch installiert**. Die integrierten Mechanismen für den Versand der Updates können auch für eine geschützte Verteilung der Software von Drittanbietern auf die Knoten oder den Austausch anderer sensibler Daten verwendet werden. Beispielsweise kann ViPNet der Aktualisierung von spezialisierten Anwendungen auf mobilen Geräten mit eingeschränkten Benutzerrechten dienen.

Die ViPNet Technologie ermöglicht die **Kontrolle des gesamten Netzwerkes von einem Verwaltungspunkt aus**, was über die reine Statistiksammlung hinausgeht. Administratoren und IT-Verantwortliche können alle geschützten Verbindungen der einzelnen Netzwerkknoten verwalten, die Sicherheitsrichtlinien werden dabei maximal flexibel definiert. Auf diese Weise können z. B. zwei Computer desselben LAN-Segmentes auf der Netzwerkebene voneinander isoliert werden.

Zuverlässigkeit

Die Verwendung symmetrischer Verschlüsselung ermöglicht einen **„On-the-Fly"-Verbindungsaufbau** zwischen einzelnen Knoten, ohne die Erforderlichkeit zusätzlicher Authentisierungssitzungen oder anderer Prozesse. Das Risiko für einen Angriff oder die Beschädigung der Daten wird damit ausgeschlossen. Der Prozess der Verbindungsherstellung läuft eigenständig im Hintergrund, die Knoten tauschen augenblicklich Benutzerdaten aus. Aufgrund der Verwendung der UDP-Kapselung können im Falle eines Verbindungsabbruches ausschließlich verlorene Fragmente übermittelt werden, ohne dass der gesamte Traffic wiederhergestellt werden muss. Dies garantiert **maximale Geschwindigkeit** für den Informationsaustausch.

Sicherheit

ViPNet verfügt über ein **mehrstufiges Sicherheitssystem** für die Schlüsselinformationen. Hinter der scheinbar einfachen Handhabung der Knoten steckt eine ausgereifte Technologie für die **sichere Zustellung, Aktualisierung und Speicherung von Schlüsseln**. Unabhängige (auf Basis unterschiedlicher Masterschlüssel erzeugte) Schlüssel werden für die Speicherung der Schlüsselinformationen auf den Computern und für den Schutz des Datenaustauschs verwendet.

Im ViPNet Netzwerk authentisieren sich die Benutzer gegenseitig mit jedem von ihnen ankommenden IP-Paket, denn jedes einzelne übermittelte IP-Paket wird durch einen neuen Schlüssel verschlüsselt. So können die Daten weder manipuliert noch entschlüsselt werden, selbst wenn ein relativ großer Teil davon abgefangen wird. Die Verschlüsselung erfolgt mit dem als sicher geltendem und weltweit eingesetztem AES-256-Verfahren. Die Möglichkeiten für Angriffe wie z. B. Man-in-the-Middle sind grundsätzlich ausgeschlossen, da ein Austausch von öffentlichen Schlüsseln und Zertifikaten über einen unsicheren Kanal bei ViPNet nicht notwendig ist.

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