

COMPUTER ZEITUNG

Die Wochenzeitung für die Informationsgesellschaft

Sonderdruck Nr. 24 / 2003, S. 21

SSL-Technik ist gegenüber der Quasinorm IPSec um bis zu 40 Prozent billiger

Webverschlüsselung schafft kostengünstigen Fernzugriff

Die SSL-basierte Absicherung des Remote Access aufs Unternehmensnetz gewinnt an Bedeutung. Diese Alternative benötigt keine Client-Software und ist dadurch weniger komplex.

Statt bei der Absicherung von Virtual Private Networks auf den De-facto-Standard IPSec zu setzen, wird häufig das aus dem Web bekannte Verfahren Secure Socket Layer (SSL) verwendet. Dieser Ansatz berücksichtigt, dass es für die meisten Arbeitsprozesse nicht nötig ist, einen Fernzugriff auf das gesamte Netzwerk zur Verfügung zu stellen, sondern nur auf einzelne Serveranwendungen.

Eine SSL-basierte Lösung erfordert keinen Support-Aufwand für IPSec-Clients, da jeder moderne Browser das SSL-Protokoll versteht, das sich bei Anwendungen wie Onlinebanking bereits als vertrauenswürdig erwiesen hat. Eine sichere Zugriffsmöglichkeit auf Firmenapplikationen kann also auf jedem beliebigen PC oder Laptop eingerichtet werden.

Die Prognosen der Marktforscher für SSL-VPNs sehen gut aus: Bis 2004 wird etwa ein Drittel der Unternehmen SSL-basierte Remote-Access-Technologien in Verbindung mit IPSec-VPNs nutzen, schätzt David Thompson, Analyst der Meta Group. Die Zahl derer, die SSL als Remote-Access-Technologie bevorzugen werden, soll laut Thompson

bis 2005/2006 auf 80 Prozent ansteigen. Laut Tolly Group glauben mehr als 75 Prozent der Unternehmen, dass SSL-VPNs traditionelle IPSec-VPNs – zumindest für den Remote Access – in den kommenden zwei Jahren vollständig verdrängen wird.



Spezielle Appliances regeln den SSL-geschützten Zugang zu bestimmten Anwendungen im Firmennetz. Foto: Netilla

Im Gegensatz zu IPSec-VPNs, die bei der Datensicherung auf Netzwerkebene (Schicht 3) arbeiten und den entfernten Benutzer im LAN darstellen, wird bei einem SSL-VPN ein Tunnel auf Transportebene (Schicht 4) etabliert, wofür zunächst bestimmte Authentisierungsmechanismen eingesetzt werden. Anschließend erfolgt ein benutzerabhängiger Zugriff auf die zugewiesene Applikation.

Ein weiterer Vorteil von SSL ist, dass Firewall-seitig die Öffnung von lediglich einem Port (443) erforderlich ist, was ein wesentlich geringeres Sicherheitsrisiko darstellt.

Administration ist deutlich einfacher

Mit einem SSL-VPN lässt sich also eine lückenlose Verschlüsselung und eine nahtlose Integration in Authentifizierungstechniken erzielen, ohne dass bestehende Applikationen zu modifi-

Durch den Einsatz von SSL-basierten Remote-Access-Lösungen können die IT-Verantwortlichen also auch mit kleineren Budgets den Sicherheitsstandard konstant halten. Die Einsparungen, die Firmen durch den Wegfall der IPSec-notwendigen Client-Software inklusive dem Aufwand für deren Installation, Administration und Updates winken, liegen bei rund 30 bis 40 Prozent gegenüber einem IPSec-VPN.

*Calum MacLeod,
European Sales Executive,
Netilla Networks/ab*

zieren sind oder Anpassungen an vorhandenen Netz- und Security-Devices vorgenommen werden müssen.

Zweiteiliges Vorgehen

Das Protokoll SSL wurde Mitte der 90er-Jahre vom Browser-Pionier Netscape entwickelt und wird heute beim Aufbau von sicheren Internetverbindungen (Https) von vielen Webapplikationen eingesetzt. „Es hat zwei Bestandteile“, erklärt Secaron-Expertin Helia Hollmann: Beim Handshake-Protokoll gibt sich zunächst der Server gegenüber dem Client mittels einem Zertifikat zu erkennen, optional auch umgekehrt. Beide verständigen sich dann auf symmetrische Schlüssel und Algorithmen, die zur Absicherung der Nutzdaten im Rahmen des Record Protocol eingesetzt werden.

ab