

CeBIT Trend 2003



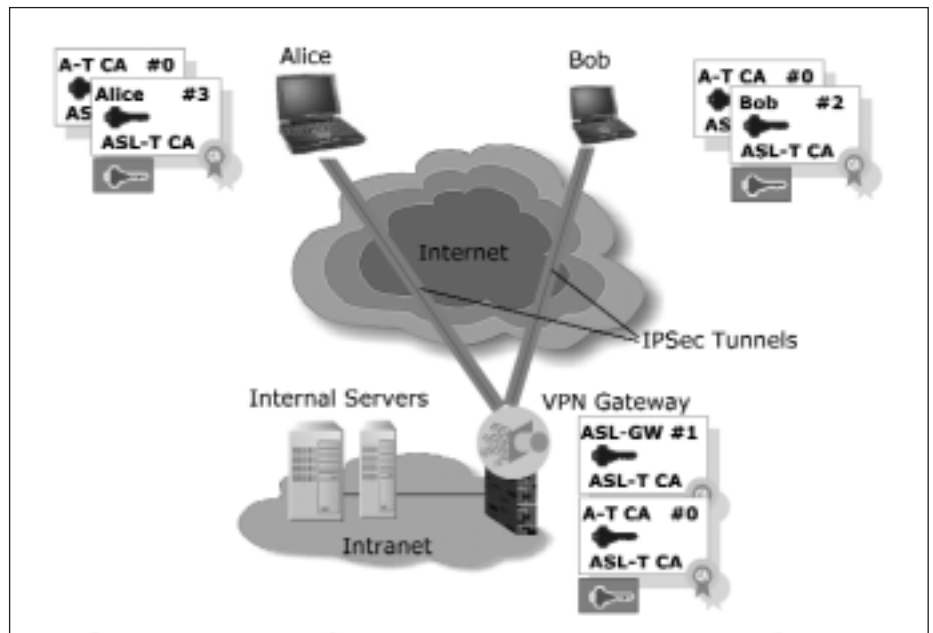
VPN
– sicherer Zugang über SSL

ANDREAS MERTZ*

Datensicherheit sollte in jedem Unternehmen absolute Priorität haben – wobei dies natürlich nicht zwingend bedeutet, dass eine hundertprozentige Absicherung des Unternehmensnetzwerks immer erreicht werden kann und muss. Für Unternehmen, die einen oder mehrere verteilte Standorte haben, müssen bei der Erstellung einer Sicherheitsstrategie verschiedene Faktoren berücksichtigt werden – einerseits der Aufbau eines wirksamen Schutzes vor ungewolltem Zugriff, andererseits leichte Administrierbarkeit.

Generell gilt, dass für den Aufbau gesicherter Verbindungen zweier oder mehrerer Niederlassungen mit der Unternehmenszentrale über – per Definition – unsichere Netze der Einsatz von IPsec sehr gut geeignet ist. Einen gesicherten Zugriff auf zentral gehostete Applikationen oder Datenbestände im Unternehmen von Client-Desktops der Außendienstmitarbeiter ist unter der Prämisse der Benutzerfreundlichkeit oft schwierig zu realisieren. Hier bedarf es einer Überprüfung, ob IPsec der Forderung nach einfacher Bedienbarkeit und Administrierbarkeit genügt. Denn wenn nicht für alle IPsec-Tunnel die gleichen Preshared Keys verwendet werden, muss notwendigerweise der Aufbau einer Certification Authority sowie die Ausstellung entsprechender Zertifikate erfolgen. Dadurch steigen die Komplexität und Fehleranfälligkeit des Systems zwangsläufig – neben dem erhöhten Aufwand ist auch mit signifikant hohen Kosten für die Orga-

* Andreas Mertz, Geschäftsführer, IT-CuBe GmbH, www.it-cube-gmbh.de. Das Beratungsunternehmen IT-CuBe hat als erstes Unternehmen in Deutschland die Partnerzertifizierung von Netilla Networks www.netilla.com erworben.



IPsec mit zertifikatsbasierter Authentisierung

nisation und einer geringen Akzeptanz seitens der Nutzer zu rechnen.

Alternativ zur Verwendung von IPsec – wodurch nur Sicherheit auf der Netzwerk-Schicht geschaffen wird, Client- und Anwendungsprogramme müssen zusätzlich gekauft, installiert und implementiert werden – können, abhängig vom Sicherheitsbedarf im Unternehmen, andere Verfahren zum Einsatz kommen. Steht in erster Linie die Nutzung von Anwendungen und Dateien im Vordergrund sollte SSL (Secure Socket Layer) als Alternative in Betracht gezogen werden, um die Übertragung von Daten über das Internet gegen fremdes Abhören zu sichern. Die Nutzung von SSL hat sich mittlerweile bei Applikationen wie Online-Banking als vertrauenswürdig erwiesen und ist im Bezug auf Nutzerfreundlichkeit kaum zu übertreffen: ein https-fähiger Browser ist alles, was der Anwender benötigt. So stellt sich folgerichtig die Frage, ob SSL-basierte

VPNs zum sicheren Zugriff von unterwegs auf zentrale Serverdaten und Anwendungen eingesetzt werden kann.

■ HTTPS-basierter Zugriff auf zentrale Server-Applikationen

Server-basierte Anwendungen eliminieren die Limitierungen von IPsec im Bezug auf verteilte Anwendungen. In diesem Ansatz wird berücksichtigt, dass es für die meisten Arbeitsprozesse nicht notwendig ist, einen Zugriff auf das gesamte Netzwerk zur Verfügung zu stellen, sondern nur auf einzelne Server-basierte Anwendungen

INHALT:

- HTTPS-basierter Zugriff auf zentrale Server-Applikationen
- Fazit

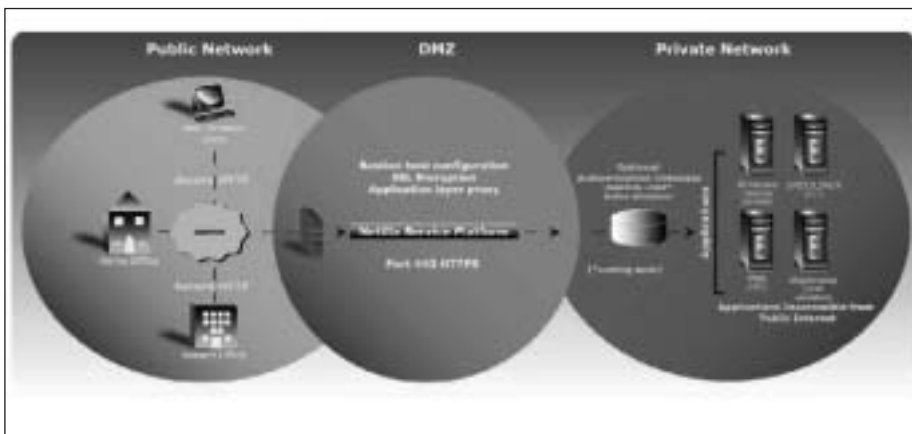
oder Dateien. Der Anwender kann jederzeit, auch von einem Standort außerhalb des Unternehmens, zum Beispiel auf seine gewohnten Desktop-Applikationen per Browser zugreifen. Diese Abfragen erfolgen, ohne dass die gesamten Anwendungsdaten über die Leitung geschickt werden müssen: Das alte Prinzip, nur die Tastatureingaben und Bildschirmaktualisierungen zwischen Terminal und Host über das Netzwerk zu schicken, ist wieder stark im Kommen; mit der Konsequenz, dass Produkte wie Citrix® Metaframe®, welche Windows-Systemen zu erweiterter Multi-User-Fähigkeit verhelfen, heute gut am Markt etabliert sind. Um jedoch einen sicheren Remote Access für Server-basierte Anwendungen zu ermöglichen bedarf es im Citrix-Modell geeigneter Sicherheitsvorkehrungen, wie der Implementierung eines Webservers, zum Beispiel MS Internet Information Server (IIS), und dem Einsatz von NFuse® für den https-basierten Zugriff auf Serverapplikationen. Ein solches Szenario weist einige Problemstellen auf, allein unter dem Aspekt der Sicherheitslücken bei dem Microsoft Server IIS. Weitere Anforderungen in diesem Citrix/NFuse-Ansatz sind, die Notwendigkeit eine Reihe von Ports an der Firewall öffnen zu müssen und das aufwändige Zertifikatshandling bei der Authentisierung von Verbindungen zwischen dem NFuse-Server und der MetaFrame Middleware.

Eine Reihe von Herstellern wie Netilla, uRoam, Neoteris, Safeweb, Aspelle

haben die Nachteile der existierenden Architekturen erkannt und bringen jetzt brauchbare preiswertere SLL-basierte Lösungen auf den Markt. So bietet beispielsweise Netilla eine vorkonfigurierte Software-/Hardware-Appliance, mit der ein sicherer Zugriff via Browser auf die unternehmensinternen Applikationen vorgenommen werden kann. Das allgemeine Grundprinzip dieser Lösungen besteht darin, dass ein Nutzer an seinem Client problemlos arbeiten kann und jederzeit der Zugriff – vor Ort im Unternehmen oder von außerhalb – auf Drucker und Dateien gegeben ist. Auch die Verwaltung der Appliance kann Web-basiert problemlos von jedem beliebigen Standort durchgeführt werden.

Fazit

Eine Flexibilisierung der Arbeitsprozesse ist in der gegebenen Wettbewerbssituation unabdingbar, so muss auch der verteilte Zugriff auf zentrale Ressourcen über per se unsichere Netze akzeptiert werden. Aufgabe der IT-Sicherheitsspezialisten ist es, mit kleineren Budgets den Sicherheitsstandard bei steigenden Anforderungen konstant zu halten. Der Einsatz von SSL-basierter VPN Technologie kann hier Unternehmen den richtigen Lösungsansatz bieten, da unter anderem auf Grund der geringeren Komplexität der Architektur die Total Costs of Ownership erheblich niedriger sind verglichen mit den TCO von IPSec. □



SSL-gesicherter Zugriff auf zentrale Applikationen, Quelle Netilla Inc.

Das Angebot zur CeBIT:

Profitieren Sie kostenlos von unseren Erfahrungen!

Die HiSolutions AG veranstaltet in Halle 17 im Rahmen des Sicherheitsforums DEFIS eine kostenlose Vortragsserie zum Thema Informationssicherheit. Profitieren Sie von unseren Projekterfahrungen und informieren Sie sich über aktuelle Trends!



Unser Vortragsprogramm:

Mi 12.3.	12:00	Security Management
Do 13.3.	12:00	Security Policies
Fr 14.3.	12:00	HiMessenger Sichere eMail For All! Sofort!
14.3.	16:00	HiScout SME Unterstützung für die Aufgaben des Security Managers
Sa 15.3.	12:00	Security Awareness
15.3.	15:00	PKI mit HiSecure
So 16.3.	12:00	Etablierung eines IDS
16.3.	15:00	Security Audits
Mo 17.3.	12:00	Sicherheitsstandards im Vergleich
17.3.	16:30	SAP-Sicherheit
Di 18.3.	12:00	IT-Grundschutzzertifikat
18.3.	15:30	Digitale Forensik
Mi 19.3.	12:00	Notfallplanung
19.3.	15:30	Content Security für SSL

Gerne beraten wir Sie auch an unserem Stand Halle 17/C31-9 oder senden Ihnen Vortragsunterlagen!

HiSolutions

www.hisolutions.com
it-security@hisolutions.com
Tel: 030-633288-0