

VPN - Virtual Private Network

Sicherheit im Internet

Das Internet wurde von den US-Militärs auf Datensicherheit und nicht auf Datenschutz ausgerichtet. Dies bedeutet, dass die [Protokolle](#) des Internet sich auf die Übermittlung aller Datenpakete konzentrieren, so dass eine Nachricht (E-Mail etc.) immer vollständig den Adressaten erreicht.

Da ein Schutzmechanismus vor fremdem Mitlesen bisher nicht eingebaut wurde, kann bis heute jeder den gesamten Datenverkehr des Internets mitlesen. Mittels Hochleistungsrechnern lassen sich selbst die heute anfallenden riesigen Datenmengen der normalen Telekommunikationswege (Telefon, Telefax) teilweise durchforsten. Im Internet insbesondere bei elektronischer Mail ist sogar mit verhältnismäßig leistungsschwachen Rechnern ein beinahe hundertprozentiges Scannen fast aller Nachrichten möglich.

Geheimdienste selbst befreundeter Staaten führen dies im großen Stil in Deutschland durch. Publik werden zwar meist nur die großen Lauschangriffe, wie derjenige bei dem die deutschen Anbieter des ICE durch den französischen Geheimdienst abgehört wurden und der darauf erfolgten gezielten Unterbietung des Angebots durch die französische Firma.

Angesichts der zunehmenden Wichtigkeit der Wirtschaftsdaten in einer modernen Industriegesellschaft kann jedoch potentiell jede Firma von derartigen Lauschangriffen betroffen sein.

Hinweis

Das Risiko, abgehört zu werden, besteht nicht nur für das Internet, sondern für alle öffentlichen Kommunikationswege, insbesondere Funk- und Satellitenstrecken, die vor allem im internationalen Telefon- und Datenverkehr eingesetzt werden.

Datendiebstahl, Datenverfälschung, Datenmissbrauch etc. kann nicht nur zum Verlust von Aufträgen führen, sondern beim Ausspähen der eigenen Passwörter sogar bis zum Bankrott der Firma führen.

Da der Sicherheitsstandard des Versands jeglicher Daten (E-Mail etc.) in öffentlichen Netzen deutlich unter dem des Postversands eines Briefes in einem offenen Umschlag liegt, wurden seit langem Verbesserungen gesucht. Als Lösung werden heute diverse sichere Datenübertragungsmöglichkeiten in Netzwerken angeboten. Die insgesamt sicherste und für den Endanwender in der Praxis am einfachsten handhabbare Lösung wird durch ein VPN erreicht.

Vorteile des VPN

Ein Virtual Private Network ist eine Verbindung zwischen zwei Punkten über öffentliche Netzwerke, z. B. zwei Filialen. Dort kann entweder ein einzelner Rechner oder ein ganzes Netzwerk angeschlossen werden. Die Endpunkte der Verbindung bestehen aus speziellen Gateways / Routern. Diese kommunizieren miteinander über die in den öffentlichen Netzwerken benutzten Protokolle. Bei dieser Kommunikation besteht zunächst kein Unterschied zu normalen Routern. D. h. der Inhalt dieser normalen Kommunikation kann sehr einfach abgehört werden.

Das Besondere an VPN liegt in folgendem: In den versandten Datenpaketen befinden sich wiederum Datenpakete, die zwischen den zwei miteinander kommunizierenden Computern

ausgetauscht werden. Allerdings ist die so getunnelte Netzwerkverbindung ebenfalls mit nur wenig größerem Aufwand abhörbar.

Vorteil

Die speziellen Gateways des VPN verschlüsseln jedoch die getunnelte Verbindung. D. h., die Daten, die Sie von Ihrem PC aus über ein VPN mit einem anderen PC austauschen, werden verschlüsselt, ohne dass Sie auf Ihrem PC, File-Server, Mail-Server etc. Verschlüsselungssoftware installieren müssen. Die Verschlüsselung wird vom Gateway auf der Protokollebene durchgeführt. Damit ist sichergestellt, dass selbst bei Benutzerfehlern alle Daten sicher verschlüsselt übertragen werden.

Beispiel

Angenommen Sie greifen auf den File-Server in der entfernten Filiale zu, um sich die Umsätze der letzten Tage anzeigen zu lassen. Dann sendet der File-Server diverse Datenpakete zum Gateway. Das Gateway nimmt jedes komplette Datenpaket, verschlüsselt es und packt es in ein weiteres Datenpaket des öffentlichen Netzwerkes ein (tunnelt es). Dies ist in etwa vergleichbar mit einem versiegelten Brief, der nochmals in dem üblichen offenen Briefumschlag eingetütet wird. Im Prinzip handelt es sich darum, in einem Netzwerk eine normale Nachricht mit einem 1.024-, 2048- oder sogar 4096-Bit-Schlüssel zu kodieren und anschließend nochmals in den üblichen Netzwerk-Datenpaketen (siehe ISO-OSI-Modell im ECP) "einzupacken". So ist eine Gesamtnachricht (die immer aus mehreren Datenpaketen besteht) doppelt geschützt und selbst für professionelle Lauscher zurzeit allenfalls mit immens hohem Zeit- und Geldaufwand zu dekodieren. Das Gateway des Empfängers packt aus dem öffentlichen Paket das verschlüsselte wieder aus, entschlüsselt es und schickt es über Ihr lokales Netzwerk zu Ihrem PC. Zusätzlich findet eine Authentifizierung statt. Hierbei wird mittels Verschlüsselungstechnik überprüft, ob die Daten tatsächlich vom richtigen Absender stammen.

Kostenvorteile

Die Kosten eines VPN liegen nicht wesentlich höher als bei einer unverschlüsselten Netzwerkverbindung.

Die wesentlichen Kosten einer Verbindung zwischen zwei Netzwerken entstehen durch die Verbindung über öffentliche Netze (z. B. eine Internet-Anbindung oder Telekom-Standleitung).

Auch die Funktionalität eines Gateways / Routers ist für die komfortable Datenübertragung zwischen Netzen erforderlich. Eine Firewall ist bei einer Internet-Anbindung sowieso unerlässlich, um Ihr firmeninternes Netzwerk vor externen Hacker-Angriffen zu schützen.

Es fallen bei einer hardware-mäßigen VPN somit nur Kosten für das zusätzliche Verschlüsselungsmodul an. Diese betragen etwa 30 % der Firewall-Kosten, fallen jedoch angesichts der monatlichen Leitungsgebühren nicht ins Gewicht.

Daneben existieren inzwischen Software-Lösungen, die samt PC, Firewall, Virens Scanner etc. nur 2.200 Euro kosten. Siehe hierzu die 2002 mit dem Cyber One Preis dotierte Software der Firma Intra2net:

- <http://www.intra2net.de>

Ein Virtual Private Network ist wesentlich schneller, sicherer und preiswerter als ein Kurier. Auch eventuelle Probleme mit den Zollbehörden kann man so geschickt umgehen.

Praxistipp

Vor allem die Bedienerfreundlichkeit und absolute Sicherheit geben den Ausschlag für den Normalanwender, der sich nicht mit technischen Details befassen möchte.

Hinweis

Wenn Sie mit einem herkömmlichen Verschlüsselungsprogramm Ihre E-Mails verschlüsseln, können Sie einen gleichwertigen Sicherheitsstandard der verschlüsselten Mail erhalten. Die Voraussetzung hierfür ist jedoch, dass Sie persönlich auf Ihrem PC und Ihr Kommunikationspartner auf seinem Rechner das gleiche Verschlüsselungsprogramm installiert haben, und dass nicht einer der beiden durch einen Bedienungsfehler die Verschlüsselung unsicher macht oder vergisst. Selbstverständlich können Sie sämtliche Daten verschlüsseln. Allerdings müssen Sie dies in jedem Einzelfall persönlich tun. VPN erledigt dies hingegen automatisch für Sie.

Nachteil

VPN verschlüsselt allerdings nur zwischen den am Virtual Private Network beteiligten Punkten. Dies bedeutet, dass Nachrichten an Kommunikationspartner, die nicht an das VPN angeschlossen sind, nicht von VPN verschlüsselt werden können. Die Verschlüsselung findet nur zwischen den beteiligten Gateways statt.

Aufgrund des heute eingesetzten IPSec muss es nicht mehr bei allen Beteiligten das gleiche Hardware-Gateway sein. Mit moderner VPN-Software gelingt dies auch mit Fast-Standard-Rechnern.

IPSec

Bei IPSec handelt es sich um einen relativ jungen internationalen Standard, mit dem durch die Erstellung Virtueller Privater Netzwerke (VPN) lokale Netzwerke über das Internet miteinander verbunden werden können (Tunnel-Modus). Es können auch zwei einzelne PCs auf diese Weise miteinander verbunden werden (so genannter Transport-Modus). Wie der Name bereits andeutet, arbeitet IPSec auf der IP-Ebene, so dass keine Veränderungen an den von Ihnen benutzten Standardanwendungen vorgenommen werden müssen.

Zum Verbindungsaufbau müssen sich die beteiligten Rechner zuerst gegenseitig authentifizieren und die Verbindungsschlüssel austauschen. Ein Verfahren heißt Pre-Shared-Key (PSK), wobei Sie das gemeinsame Passwort dem Benutzer der Gegenstelle vorher mitteilen müssen (z. B. per Telefon). Das zweite Verfahren setzt auf "öffentliche Schlüssel", (PKC - Public Key Cryptography). Hierbei wird von jedem Rechner ein Schlüsselpaar aus "privatem Schlüssel" und "öffentlichem Schlüssel" erzeugt, wobei der private nicht aus dem öffentlichen errechnet werden kann. Dies erlaubt, den öffentlichen Schlüssel bei einer Zertifizierungsstelle (CA - Certifying Authority) tatsächlich allen im Internet zur Verfügung zu stellen. Die anderen Nutzer benutzen Ihren öffentlichen Schlüssel und schicken Ihnen - z. B. per E-Mail - die Nachricht, die nur Sie mit dem privaten Schlüssel lesen können. Für das heute oft verwendete DynIP-Verfahren hat sich der Public-Key durchgesetzt.

Um zu verhindern, dass sich jemand als Dritter dazwischen schaltet, wird bei diesem Verfahren zusätzlich noch die Signatur (fingerprint) ausgetauscht. Die gängigsten Fingerprint-Verfahren sind MD5 und SHA-1.

Eine weitere Optimierung lässt sich mittels PFS (Perfect Forward Secrecy) erzielen. Dies muss auf allen Gegenstellen identisch eingestellt sein, um sicherzustellen, dass ein Sitzungsschlüssel nicht aus dem vorhergehenden errechnet werden kann.

Software-Gateways sehen hierfür ein komplettes Schlüsselmanagement vor. Auf Linux-Systemen wird oft ein RSA-Schlüssel nach RFC 2537 verwendet. Dies erlaubt, einen so genannten Self-Signed-Key zu exportieren. Hierbei benötigt man für den Verbindungsaufbau keine dritte Stelle,

wie die Zertifizierungs-Behörde, sondern kann selbst das eigene Zertifikat erstellen und an die Gegenstelle exportieren. Man ist somit selbst gleichzeitig Inhaber (Subject) und Zertifikatsaussteller (Issuer). Dies ist preiswerter und macht einen erheblich flexibler, da die Beantragung und Einrichtung von Zertifikaten bei einer CA auch zeitaufwendig ist.

Die meisten anderen IPSec-Implementierungen benutzen den wesentlich komplexeren X.509-Standard, der auch für SSL/TLS (z. B. bei den oft zu sehenden HTTPS-Verbindungen) oder bei der modernen Verschlüsselung der E-Mails gemäß S/MIME eingesetzt wird. Da die Sicherheit der Verbindung u. a. von der Schlüssellänge abhängt, werden heute immer längere Schlüssel (bis zu 4096) eingesetzt. Allerdings ergeben sich oft Überlastprobleme bei Schlüsseln größer 2048-bit. Der tatsächliche Verbindungsaufbau erfolgt bei IPSec mit dem Protokoll IKE (Internet Key Exchange) in zwei Stufen. Zuerst wird eine gesicherte Verbindung aufgebaut, um dann im Quick Mode die eigentlichen Sitzungsdaten (IPSec SA - Security Association) und Sitzungsschlüssel auszutauschen. Damit auf beiden Rechnern die Verbindung überprüft werden kann, müssen beide Seiten identische Werte für Start- und Zielnetz des gemeinsam aufgebauten Tunnels angeben.

DynIP und DynDNS

Beim DynIP-Verfahren kann eine Seite (Road-Warrior) oder beide Seiten (bei Sternverbindungen auch alle Teilnehmer) eine dynamische IP verwenden. Dies erspart die teure Standleitung, hat allerdings den Nachteil, dass der Road-Warrior die Verbindung aufbauen muss. Oder man bedient sich des DynDNS (Dynamic Domain Name Serving), wobei mindestens eine Stelle eine DynDNS besitzen muss. Dies entspricht im Prinzip dem üblichen Eintrag einer Domain `www.hau-mich-blau.de`, die auf einem Domain-Name-Server in die im Internet verwendete IP-Zahl umgerechnet und dem richtigen Rechner zugeordnet wird. Um auch während der Tunnel-Verbindung z. B. zur anderen Filiale nicht ständig online sein zu müssen, benutzt man heute den Lockruf, der bei Bedarf die Gegenstelle aktiviert. Aus Sicherheitsgründen besitzen die Tunnelverbindungen bei IPSec nur eine beschränkte und individuell einstellbare "Lebenszeit". Um sicher zu stellen, dass die Verbindung noch aufrechterhalten ist, bzw. um sie wieder zu aktivieren, benutzt man das Ping-Verfahren.

Bei der individuellen Verschlüsselung einzelner Daten mit Standardsoftware, z. B. PGP (Pretty Good Privacy), können Sie problemlos plattformübergreifend kommunizieren. D. h. es ist belanglos, ob Sie oder Ihre Kommunikationspartner Windows-, Macintosh-, Unix- oder Novell-Betriebssysteme einsetzen. Die Verschlüsselung ist zwischen den Systemen kompatibel. Beim VPN hingegen müssen i.d.R. die benutzten speziellen Gateways oder die Software vom gleichen Hersteller stammen, um alle Möglichkeiten auszunutzen. Bei unterschiedlichen Systemen steht aus dem großen Angebot an Möglichkeiten oft nur eine kleine Auswahl zur Verfügung.

Allgemeine Netzwerkprobleme

Kleinere Anpassungsprobleme ergeben sich nicht nur bei VPN, sondern in jedem größerem Netzwerk im Bereich der Anwendersoftware. Zwar können Sie plattformübergreifend auf z. B. Unix-, NT- oder Novell-Server von Windows-, Macintosh-, OS/2-Clients zugreifen. Ferner können Sie z. B. zwischen Word für Macintosh, Word Perfect für Windows, Star-Office für Linux und den meisten anderen gebräuchlichen Textverarbeitungsprogrammen Texte austauschen. Hingegen sind unter Umständen nicht unerhebliche Datenbank Anpassungen erforderlich, wenn Sie Daten zwischen einem Oracle- und einem Access-Server abgleichen wollen.

Der Datenaustausch zwischen inkompatiblen Finanz-, Buchhaltungs- oder CAD-Systemen ist entweder nicht oder nur mit hohem finanziellem und programmiertechnischem Aufwand möglich. Bei derartigen Inkompatibilitäten kann auch kein VPN helfen.

Zielgruppen

VPN ist die Technologie der Wahl, wenn Sie

- als Firma mit Niederlassungen, Zweigstellen / Filialen, Außendienststellen oder Außendienstmitarbeitern kommunizieren wollen,
- mit Produktionsstätten, Lagern etc. kommunizieren wollen,
- externe Abteilungen führen,
- Logistikzentren unterhalten,
- Warenumschnlagplätze besitzen,
- als Konsortium untereinander sensible Daten über Netzwerke jeglicher Art austauschen,
- enge Beziehungen zu Lieferanten bzw. Subunternehmern unterhalten,
- sensible Daten über Netzwerke jeglicher Art zu festen Partnern (Fusionspartner) außerhalb des Mutterhauses senden müssen.

Technischer Aufwand

Ein derart hochsicheres Netzwerk ist relativ einfach zu konzipieren und aufzubauen. Dies soll anhand eines Beispielnetzes einer Spedition mit diversen Verbindungen zur Außenwelt und Niederlassungen im Ausland erläutert werden.

Beispiel: Spedition

Die Beispielspedition hat ihren Geschäftssitz in Süddeutschland und besitzt je eine Niederlassung in Österreich und Italien. Ferner unterhält die Spedition einen Warenumschnlagplatz in einem Freihafen in Norddeutschland und einen in Österreich.

Um den Waren- und Lkw-Fluss optimal abzuwickeln, hat sich die Firma vor einigen Jahren bereits zum Aufbau eines Kommunikationsnetzwerkes entschieden.

Da sich in der täglich zwischen den verschiedenen Niederlassungen und Warenumschnlagplätzen großen Datenmenge ein nicht unerheblicher Anteil an sensiblen Details befindet, entschloss sich die Spedition die Datenübermittlung sicher zu gestalten. Gleichzeitig wurde aus Kosteneinsparungsgründen die internationale Datenkommunikation von Telefonleitungen auf Internet umgestellt.

Hierzu waren folgende Änderungen am Netzwerk erforderlich:

Die Zentrale erhielt eine Standleitung zum Internet, eine Firewall und einen VPN-Router, der die Kommunikation zu den anderen Niederlassungen verschlüsselt. Aufgrund der besonders hohen Sicherheitsanforderung in der Zentrale entschloss man sich, neben dem VPN-Gateway eine separate Firewall auf einem eigenen Rechner zu installieren. Eine noch höhere Sicherheit hätte man mit einem zweistufigen Firewall-Konzept erhalten, das eine Firewall auf einem separaten Rechner und die zweite Firewall im VPN-Router enthielte. Dahinter befindet sich das firmeninterne LAN. Auf diesem internen Netz verwaltet die Firma ihre Buchhaltung, das gesamte Auftragsmanagement und ihr Logistik-Management. Ferner werden die geplanten Fahrzeug- und Warenbewegungen sowie freie Kapazitäten in der Zentrale verwaltet.

Jede Niederlassung erhielt eine Wählleitung mit Call-Back-Funktion. Dies ist bei geringen Online-Zeiten preiswerter als eine Standleitung, erlaubt aber einen Verbindungsaufbau von beiden Seiten. Wenn somit eine Person aus der Zentrale die Datenbestände der Filiale bearbeiten möchte, kann die Zentrale die Verbindung automatisch aufbauen.

Jede Niederlassung erhielt ferner ebenfalls einen VPN-Router mit integrierter Firewall. Die Filialen bearbeiten auf ihrem eigenen geschützten Firmennetz ihre eigenen Aufträge und die eigene Buchhaltung, deren Daten in regelmäßigen Abständen an die Zentrale übermittelt werden. Ferner erfassen die Niederlassungen dezentral die geplanten Fahrzeug- und Warenbewegung sowie die freien Kapazitäten und übermittelt sie regelmäßig an die Zentrale.

Die beiden Warenumschatlagplätze erhielten eine Wählleitung ohne Call-Back-Funktion sowie einen VPN-Router mit integrierter Firewall.

Die Warenumschatlagplätze erfassen dezentral alle umgeschlagenen Warenein- und -ausgänge sowie Fahrzeugbewegungen. Diese Daten werden an die Zentrale übermittelt.

Die Zentrale erhält somit den Überblick über Art, Menge und Ort, Absender und Empfänger aller Waren sowie die Zahl der an jedem Ort befindlichen Transportkapazitäten. Ferner führt die Zentrale alle Buchhaltungsdaten zur Monats-, Quartals- und Jahresabschlussrechnung zusammen. Derartig hochsensible Daten würden nicht nur die Konkurrenz, sondern auch die Auftraggeber der Spedition interessieren, weshalb sie mittels VPN geschützt wurden.

Um die Effizienz des Speditionsunternehmens zu erhöhen, entschloss sich die Firma in der Zentrale eine Unternehmensberatung einzuschalten, die ebenfalls über VPN Einsicht in alle Firmendaten erhielt.

Die Unternehmensberatung erhielt eine Wählleitung sowie einen VPN-Router mit integrierter Firewall. Zwar ist der Zugriff der Unternehmensberatung auf das Lesen beschränkt, ein Schreibzugriff auf die Speditionsdaten ist nicht möglich. Dennoch erstellt sie auf ihren eigenen Computern eine Analyse der Speditionsdaten mit sensiblen Daten und benötigt deshalb ebenfalls eine Firewall.

Letztendlich wurde in jedem Land ein Steuerberatungsunternehmen an das Speditionsnetzwerk angeschlossen. Die Steuerberater werden nicht über das Internet an das Netz gekoppelt, sondern greifen über eine direkte ISDN-Wählverbindung auf die Buchhaltungsdaten der jeweiligen nationalen Niederlassung zu. Hierzu benötigen sie einen VPN-Router. Da die Steuerberater nicht an das Internet angeschlossen sind, kann bei ihnen die Firewall entfallen.

Vergleich mit dem Anschluss über ein herkömmliches Netz

In der Bedienung für den Endanwender unterscheiden sich die beiden Netzwerk-Varianten nicht. Allerdings ist die Sicherheit des VPN wesentlich höher.

Die übertragene Datenmenge wird durch die Verschlüsselung und das Tunnelling nur unwesentlich größer. Ferner beinhalten moderne Verschlüsselungsverfahren die Möglichkeit leistungsfähiger Datenkompression. Deshalb kann es je nach Art der übermittelten Daten sein, dass die Datenübermittlung über ein VPN sogar schneller von statten geht als über ein herkömmliches Netzwerk.

Beispiel: Produzierendes Gewerbe

Bei einer Firma des produzierenden Gewerbes kommen unter Umständen noch weitere Möglichkeiten des VPN-Einsatzes hinzu:

Falls Sie längere Zeit mit derselben Werbeagentur zusammenarbeiten, empfiehlt es sich auch hier auf VPN für die sichere Datenübermittlung zurückzugreifen. Hierfür sollte auf Seiten der Werbeagentur ein VPN-Router installiert werden. Es wird hierbei vorausgesetzt, dass die Werbeagentur ihr internes Netzwerk bereits für die Kommunikation mit der Außenwelt durch eine Firewall gesichert hat. Ferner muss die Werbeagentur mit dem Internet verbunden sein. Sinnvoll kann es auch sein, die Kommunikation zur externen Druckerei durch VPN zu schützen. Hierbei sollte die Verbindung sowohl von der Werbeagentur als auch Ihrer eigenen Firma möglich sein. Hierbei ist darauf zu achten, dass alle anderen Kommunikationswege der Druckerei mindestens durch eine Firewall geschützt sind. Auch hier fallen die Installationskosten eines VPN-Routers an. Es ist auch möglich, dass die Druckerei zwei verschiedenartige VPN-Router (Hard- oder Software) installiert, über die sie mit zwei verschiedenen Auftraggebern kommuniziert.

Hinweis

Besitzt die Druckerei mehrere Kunden, die ihre Druckdaten über VPN übermitteln wollen, so muss man entweder je einen Router für jeden Auftraggeber in der Druckerei installieren, oder alle Firmen müssen von derselben Computerfirma mit der gleichen Router-Technik (Hard- oder Software) ausgerüstet werden. Außerdem ist dann noch durch geeignete Firewall-Maßnahmen sicherzustellen, dass die verschiedenen Kunden nicht auf die anderen Netze zugreifen können.

Kosten

Die Kosten sind somit abhängig von der Anzahl der angeschlossenen Systeme der Einheiten (Niederlassungen etc.).

Es ergibt sich eine extrem hohe Sicherheit zu relativ geringem Preis, da man nun nicht mehr eigene Netzwerke verlegen muss, sondern mittels Elektronik ein virtuelles privates Netzwerk in jedem öffentlichen Netz oder sogar dem Verbund von Netzen errichten kann.

Anwendungsaufwand für den Endbenutzer

Erstaunlicherweise entsteht dem Endanwender kein Aufwand! Der Endanwender bemerkt nicht, dass er über ein extrem sicheres Netzwerk kommuniziert. Der Aufwand für eine sichere Datenübermittlung sinkt auch insgesamt, weil man keine Disketten, Zips, CDs oder Kuriere mehr benötigt.

Rechtliche Aspekte

Leider ist eine derartige Verschlüsselung nicht in allen Ländern der Erde erlaubt. Vor allem Diktaturen aber auch demokratische Länder schränken die Benutzung hochsicherer Verschlüsselungssysteme ein oder verbieten jede sichere Verschlüsselung.

Allerdings gehen einige Länder aufgrund der kaum durchführbaren Umsetzung des Kodierverbotes und massiven öffentlichen Drucks langsam wieder zu einer etwas liberaleren Haltung über.

Dennoch müssen Sie grundsätzlich vor dem Einsatz eines VPNs im Ausland überprüfen, ob seine Benutzung erlaubt wird. Falls nicht, sollten Sie selbst Ihre Schlüsse ziehen und keine sensiblen Daten über öffentliche Netze dorthin versenden, bzw. Personen und Niederlassungen aus diesem Land keinen netzwerkgebundenen Zugriff auf Daten der Zentrale einräumen.

Alternativen

Die Spedition hat einen eigenen Web-Server bei sich in der Firma stehen. Auf diesem Web-Server befindet sich neben der Firmenpräsentation eine Schnittstelle zu der Datenbank mit den Auftragsdaten und den Warenbewegungen. Kunden können auf Wunsch per Internet Aufträge erteilen und den Bearbeitungsstand Ihrer Aufträge abfragen bzw. erfahren, an welchem Ort sich die Ware momentan befindet. Hierzu benötigt der Kunde nicht unbedingt einen VPN-Anschluss.

Um dennoch einen gewissen Sicherheitsstandard zu garantieren, erfolgt eine Verschlüsselung der Daten per SSL. Secure Socket Layer bewirkt eine Verschlüsselung der Datenkommunikation zwischen dem Web-Browser des Anwenders und dem Web-Server in Ihrer Firma. Der Anwender muss hierbei allerdings das Zertifikat des Web-Servers manuell authentifizieren, oder Sie hinterlegen Ihr Zertifikat bei einer anerkannten Zertifizierungsstelle (z. B. Very Sign). Dies geschieht mittels Bestätigung durch Mausklick.

Der Hauptnachteil liegt allerdings in der Schlüssellängenbeschränkung der amerikanischen Browser, die aufgrund der US-Exportregulierungen nicht absolut sicher sein dürfen. Diese Exportbeschränkungen lassen sich inzwischen auf mehreren Wegen umgehen. Es obliegt allerdings

dem einzelnen Anwender, sich mit sicherer Verschlüsselungstechnik zu versorgen. Hierzu sind jedoch Fachkenntnisse erforderlich.

SSL-E-Mails?

Ein weiterer Nachteil liegt darin, dass die Verschlüsselung auf der Ebene der Applikationen stattfindet. D. h., dass jede Applikation, die SSL benutzen möchte, selbst die Verschlüsselung durchführen muss. Das hat Folgen etwa für E-Mails: Wollten Sie eine E-Mail per SSL verschlüsseln, so müsste Ihr Mail-Programm sowie Ihr Mail-Server SSL-Verschlüsselung für E-Mail implementieren. Die verschickte E-Mail wäre dann zwar während der Übermittlung verschlüsselt, würde jedoch auf dem Mail-Server sofort automatisch ausgepackt und entschlüsselt werden müssen, um überhaupt an die richtige Adresse weiterversandt werden zu können. Denn die Adresse ist im verschlüsselten Zustand auch für den Mail-Server nicht lesbar. Dies führt dazu, dass ein SSL-verschlüsselter E-Mail-Versand nicht praktikabel ist. Aus den gleichen Gründen ist es nicht sinnvoll, die Übertragungsprotokolle von File-Servern SSL zu verschlüsseln.

PGP

Außendienstmitarbeiter sind lediglich mit Internet-Zugängen und E-Mail-Adressen ausgestattet und kommunizieren mit der Zentrale und den Niederlassungen der Spedition mittels E-Mail. Um dort eine höhere Sicherheit zu erhalten, wird die E-Mail mittels PGP (Pretty Good Privacy von Phil Zimmermann) verschlüsselt. Das Programm benutzt mit einem 1024- bis 4096-Bit-Schlüssel die zurzeit sicherste Verschlüsselungsmethode. Dies bedeutet, dass die Mail während der gesamten Übertragung über das Internet mit der größtmöglichen Sicherheit verschlüsselt ist. Die so genannten Header-Daten (Adresse und Empfänger sowie die Betreffzeile) werden von PGP allerdings nicht verschlüsselt und sind somit für jeden einsichtig.

Ferner ist zu beachten, dass sowohl die Außendienstmitarbeiter als auch Ihre Kommunikationspartner in den Niederlassungen und der Zentrale peinlich genau darauf achten müssen, dass sie die E-Mail jedes Mal vor dem Absenden auch tatsächlich verschlüsseln.

Resümee

Mit einer einheitlichen Verschlüsselungslösung ist erst zu rechnen, wenn öffentliche Netze, wie das Internet, eine sichere Verschlüsselung zwischen den Kommunikationsendpunkten in ihre Standardprotokolle integriert haben. Solange bildet VPN die sicherste und für den Endanwender praktikabelste Möglichkeit der Datenkommunikation.

Lesen Sie zu diesem Thema auch [Wirtschafts- und Wettbewerbspionage](#)