Netzwerke, VPN und WLAN richtig absichern

Bild: Nmedia - Fotolia.com

Lauschangriffe auf Netzwerke lassen sich nur verhindern, wenn sämtliche Verbindungen angemessen verschlüsselt sind. Nicht nur bei der SSL-Verschlüsselung im Internet gibt es Nachholbedarf, auch andere Kommunikationswege sind oft nicht umfassend abgesichert. Dieser Beitrag beleuchtet die wichtigsten Traffic-Baustellen. Von Oliver Schonschek

Als Sicherheitsverantwortlicher kann man schon froh sein, wenn IT-Nutzer vertrauliche Daten nur dann an Webapplikationen übermitteln, wenn die Verbindung per SSL/TLS gesichert ist. Leider kann man aber selbst in diesem Fall nicht davon ausgehen, dass Lauschangriffe ausgeschlossen sind. Zum einen wurden bereits SSL-Zertifikate gestohlen bzw. gefälscht, nachdem einzelne Zertifizierungsstellen erfolgreich angegriffen wurden. Zum anderen wird die SSL-Verschlüsselung im Internet häufig unzureichend implementiert.

So meldete TeleTrust, dass bei der Hälfte der schutzwürdigen Internetkommunikation möglicherweise unsichere Algorithmen verwendet werden (PDF, 140 KB). Serverseitig werde automatisiert ein Profil ausgewählt, das Verschlüsselungsalgorithmen wie RC4 oder DES-Varianten nutzt, die eine Entschlüsselung durch unbefugte Dritte nicht ausreichend verhindern. Auch der Online-Dienst SSL Pulse (Trustworthy Internet Movement) liefert Statistiken zu überprüften SSL-Verbindungen, die die Verbindungssicherheit in Frage stellen: Nicht einmal ein Viertel der mehr als 160.000 geprüften Webseiten wurde als sicher eingestuft.

Netzwerkverschlüsselung bleibt kritisch

Auch andere Verschlüsselungsmethoden für Netzwerke werden in der Praxis nicht immer so eingesetzt, wie es erforderlich wäre: Ob Virtual Private Networks (VPNs), Wireless LAN (WLAN) oder Layer-2-Verschlüsselung, Unter-

Bild: Secunet

Mobile Nutzer benötigen eine verschlüsselte Verbindung, wenn sie auf das Firmennetzwerk zugreifen wollen. Möglich wird dies zum Beispiel mit SINA Business. Das Bild zeigt einen VPN-Stick am Laptop.

nehmen sollten prüfen, wie die Verschlüsselung umgesetzt ist, und bei Bedarf nach passenden Lösungen suchen.

VPN: An jeden Nutzertyp denken

Wenn mobile oder externe Mitarbeiter auf das Firmennetzwerk zugreifen, sollte dies nicht über das offene Internet geschehen. VPNs bieten sich für sichere Verbindungen an und bilden einen Tunnel zwischen Mitarbeiter und internem Netzwerk. Jedoch sollte dabei die Komplexität der VPN-Verbindung nicht unterschätzt werden: Die anzubindenden Mitarbeiter nutzen zum Teil private Smartphones oder Tablets für den Netzwerkzugriff (Bring Your Own Device), wollen neben dem Firmennetzwerk auch betriebliche Cloud-Dienste verwenden und haben Endgeräte im Einsatz, die sich auch im Betriebssystem unterscheiden.

Insellösungen für verschiedene VPN-Nutzer sollten vermieden werden, erhöhen sie doch den Administrationsaufwand und das Risiko für Konfigurationsfehler. Deshalb sind VPN-Lösungen gefragt, die sich als App oder über mobile Browser nutzen lassen, die flexibel mehrere Netzwerke parallel unterstützen und die für verschiedene Betriebssysteme angeboten werden.

Gerade bei mobilen Geräten und dem damit verbundenen Verlustrisiko sollte an Sicherheitsfunktionen wie Zwei-Faktor-Authentifizierung gedacht werden, damit die VPN-Verbindung nicht zur Hintertür ins Firmennetzwerk wird. Beispiele für VPN-Lösungen, die Clients für mehrere Betriebssysteme bieten, sind ViPNet OFFICE 4.0 oder die NCP Secure Entry Client Suite. Möglichkeiten zur VPN-Anbindung von Smartphones und Tablets sehen zum Beispiel HOBLink Mobile und NCP Mobile VPN vor.

Der Bedarf an erhöhtem Zugangsschutz über Zwei-Faktor-Authentifizierung lässt sich ebenfalls abdecken, unter anderem mit dem ECOS VPN-Client und den VPN-Lösungen von NCP. Eine schnelle VPN-Einführung unterstützen VPN-Appliances wie genua genucrypt, SecureGUARD UAG Appliances, secunet SINA Business, Sirrix TrustedVPN, Securepoint Black Dwarf VPN-Gateway und Gateprotect Extended VPN.

Bild: Securepoint

Wer sein Netzwerk auf Außenstellen ausweiten möchte, sollte zu einer VPN-Lösung greifen. VPN-Gateways wie das Securepoint VPN-Gateway Black Dwarf ermöglichen einen schnellen Einstieg.

Layer 2: Glasklare Sicherheit für alle Standorte

Unternehmen mit mehreren Standorten wollen mit ihren Niederlassungen am liebsten so schnell und sicher kommunizieren, als ob alle Einheiten in der Zentrale angesiedelt wären. Um dies zu ermöglichen, kommen Ethernet-Services zum Einsatz, die meist auf Glasfaserverbindungen basieren, entweder als „Hub and Spoke"- oder Any-to-Any-Vernetzung.

Ohne entsprechende Verschlüsselung sind die Verbindungen zwischen den Niederlassungen ⇨

Die VPN-Lösung der Wahl sollte alle Nutzertypen unterstützen, die im Unternehmen vorkommen, zum Beispiel auch Mac-Nutzer, für die ggf. ein eigener VPN-Client benötigt wird. Das Bild zeigt den NCP Enterprise Secure Client für Mac-Nutzer.

Bild: NCP

↪ und der Zentrale (Hub and Spoke) bzw. zwischen allen angeschlossenen Standorten (Any-to-Any) allerdings ungeschützt. Hier setzen Lösungen im Bereich Layer-2-Verschlüsselung an, die schnelle Datentransporte auf der Data-Link-Schicht absichern, darunter InfoGuard Layer 2 Encryption, secunet SINA L2 Box, der CE-Infosys PowerCryptor und der atmedia 100M Ethernet-Verschlüsseler.

WLAN: Fehler aus dem Home-Office nicht wiederholen

Bei WLAN-Verbindungen besteht die Gefahr, dass der drahtlose Teil des Firmennetzwerkes genauso unsicher konfiguriert wird, wie dies in vielen Privathaushalten und Home-Offices der Fall ist.

Umfragen zeigen, dass deutschen Nutzern die Sicherheit von WLAN-Hot-Spots sehr wichtig ist. Gleichzeitig besteht aber Nachholbedarf bei der WLAN-Verschlüsselung am eigenen Hot Spot. Für Unternehmen konzipierte Produkte helfen dabei, die Verschlüsselung für WLAN- und VPN-Verbindungen einzurichten, und vermeiden so die häuslichen Fehler. Beispiellösungen sind Teldat bintec W2003n-ext, LANCOM L-452agn dual Wireless und die FRITZ!Box 7490 für das Home-Office. Allerdings sollte nicht vergessen werden, dass auch WLAN-Router Sicherheitslücken haben können, die die Verschlüsselung gefährden, wie zum Beispiel die Eingabe des Suchbegriffs „WLAN" bei CERT-Bund zeigt.

Bild: Secunet

Die Standortvernetzung über Glasfaserleitungen bedarf einer sicheren Verschlüsselung, um Lauschangriffe abwehren zu können. Eine Layer-2-Verschlüsselung bietet zum Beispiel die secunet SINA L2 Box.

Fazit: Keine Vernetzung ohne Verschlüsselung

Ganz gleich, ob nun mobile und externe Mitarbeiter, verteilte Standorte oder der WLAN-Drucker in der Firma vernetzt werden sollen: Ohne die passende Verschlüsselungslösung geht es nicht. Dabei sollte die jeweilige Verschlüsselung natürlich auch dem Stand der Technik entsprechen, wie das Beispiel der unsicheren SSL-Verbindungen zeigt. Bei der Prüfung der Verschlüsselung hilft auch die BSI-Richtlinie „TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen". □


Bild: Teldat

Werden WLAN-Verbindungen im Unternehmen oder Home-Office genutzt, sollte auf Sicherheitsfunktionen geachtet werden, die die notwendige Verschlüsselung einrichten und VPN-Verbindungen unterstützen. Auf dem Markt gibt es spezielle Business-Geräte wie Teldat bintec W2003n-ext.