Faktoren für die sichere Remote-Anbindung

Security-Maßanzug für Zweigstellen

Zweigstelle ist nicht gleich Zweigstelle. Doch unabhängig davon, ob ein Mitarbeiter vom Home Office auf das zentrale Unternehmensnetzwerk zugreift oder ob es den vielfältigen Datenverkehr einer größeren Außenstelle abzusichern gilt, sollten IT-Verantwortliche bei der Umsetzung unternehmensübergreifender Security-Richtlinien keine Kompromisse eingehen.

Bei der sicheren Anbindung von Zweigstellen kommt nicht nur darauf an, den erforderlichen Funktionsumfang der eingesetzten Security-Appliance auf den individuellen Bedarf abzustimmen. Vielmehr müssen auch entsprechende Verantwortlichkeiten zur Gewährleistung der effektiven und gleichzeitig sicheren Nutzung der Geschäftsanwendungen klar zugewiesen sein. Es lassen sich dabei grundsätzlich zwei Einsatzszenarien unterscheiden: Home Office und „klassische" Zweigstelle in Form eines größeren, dezentralen Produktions-, Logistik-, Verkaufs- oder Bürostandorts. Für beide gibt es spezifische Rahmenbedingungen und entsprechende Sicherheitsanforderungen hinsichtlich der Remote-Anbindung zu beachten.

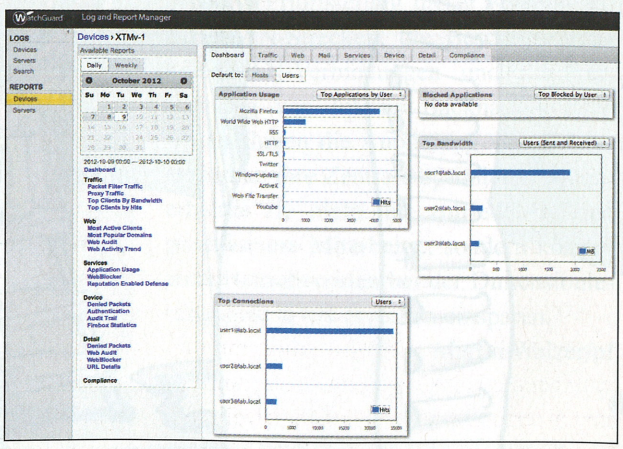
Home Office: Trennung der beruflichen und privaten Sphäre

Die internationale Studie „The Evolving Workforce" des Marktforschungsunternehmens TNS Global befasste sich 2011 mit Veränderungen in der Arbeitswelt. Insgesamt 15 Prozent der 8.360 Teilnehmer gaben an, von zu Hause aus zu arbeiten. In Deutschland allein waren es zehn Prozent. Da davon auszugehen ist, dass die Mehrzahl bei der täglichen Arbeit via Internet auf das Unternehmensnetzwerk zugreift, sollten IT-Verantwortliche die sicherheitsrelevante Bedeutung dieser Form der Zweigstelle keinesfalls unterschätzen. Die besondere Herausforderung liegt darin, dass im Home-Office-Umfeld meistens private und geschäftliche Internet-Nutzung kollidieren. Dadurch wächst die Angriffsfläche der unternehmensrelevanten Anwendungen. Dies gilt besonders, wenn beispielsweise weitere Familienmitglieder ebenfalls über die heimische Internet-Verbindung surfen und Opfer von Viren, Malware und Co. werden.

Um die Sicherheit geschäftlicher Anwendungen zu gewährleisten, sollte der unternehmensbezogene Datenverkehr daher konsequent vom privaten abgegrenzt und separat gesichert sein. Eine zwischengeschaltete Security-Appliance ist in der Lage, diese physische Trennung durch verschiedene Ports herzustellen, deren Freigabe sich individuell kontrollieren lässt. So lässt sich beispielsweise festlegen, dass nur über einen Port, der mit dem Arbeitsrechner des Mitarbeiters verbunden ist, via IPSec oder VPN mit dem Unternehmensnetzwerk kommuniziert wird. Zusätzlich garantieren (mehrstufige) Authentifizierungsmechanismen bei der Anmeldung an der Firewall, dass nur tatsächlich gewollte Verbindungen zugelassen sind. Entsprechendes gilt für WLAN-Zonen, wenn mobile Geräte wie Smartphones oder Tablets vor Ort zum Einsatz kommen. So lässt sich gewährleisten, dass zum Beispiel der Datenverkehr via Ipad, das sich in der „Firmenzone" bewegt, automatisch den relevanten Sicherheitsvorgaben des Unternehmens entspricht. Von Bedeutung ist dabei auch das Thema Quality of Service. Ein Praxisbeispiel dazu: Der Musik-Download eines Familienmitglieds sollte nicht die VoIP-Qualität geschäftlicher Gespräche beeinflussen. Dabei gilt es, den Datenverkehr entsprechend zu priorisieren und Bandbreiten für spezifische Anwendungen zu garantieren, damit der relevante Traffic aus der Zweigstelle verlässlich ankommt.

Unterstützung geschäftskritischer Anwendungen

Quality of Service stellt bei der Anbindung „klassischer" Zweigstellen ebenfalls einen wichtigen Punkt dar. Die Praxis zeigt, dass viele Unternehmen bei der Kommunikation von Filialen aus Performance-Gründen bewusst auf Aufteilung setzen. Nicht selten laufen geschäftskritische Anwendungen wie CRM-, E-Mail- oder Warenwirtschaftssysteme via VPN über eine leistungsstarke Business-Leitung, während für die weitere Datenkommunikation eine zweite Leitung vorgesehen ist. So ist garantiert, dass die Bandbreite des VPN-Tunnels zum zentralen Netzwerk nicht beeinträchtigt wird. Gleichzeitig lassen sich



Das Reporting gibt Aufschluss darüber, welcher Benutzer welche Applikation nutzt.

allgemeine, Internet-bezogene Aktivitäten über die zusätzliche Leitung der Zweigstelle direkt ausführen. In diesem Fall ist neben der Multi-Provider-Fähigkeit eine klare Steuerung des Datenverkehrs erforderlich – das so genannte Traffic Shaping, das jedoch nicht alle im Markt verfügbaren Lösungen unterstützen.

Die Sicherheits-Appliance sollte darüber hinaus über eine Applikationskontrolle verfügen, bei der sich die Kommunikation bestimmter Anwendungen gezielt per Mausklick zu- und abschalten lässt – bestenfalls sogar nutzerspezifisch. Dienste, die wie Facebook oder Instant Messaging im Verdacht stehen, die eigentliche Produktivität der Mitarbeiter herabzusetzen oder sich besonders anfällig gegenüber Viren oder Malware zeigen, sind somit bei Bedarf jederzeit blockierbar. Falls für eine Zweigstelle neben der Performance-Steuerung zudem Hochverfügbarkeit dringend erforderlich ist, sollten IT-Verantwortliche bei der Auswahl der Sicherheits-Appliance auf Cluster-Fähigkeit achten. Die Anbieter sehen dieses Feature nicht bei allen ihren Modellen vor.

Konsequente Absicherung von Anfang bis Ende

Um Policies unternehmensübergreifend umzusetzen, müssen sowohl der Zentrale als auch den Niederlassungen die gleichen Sicherheits-Features zur Verfügung stehen. Im Zweigstellenumfeld sollte erkennbar sein, welche Anwendungen tatsächlich im Einsatz sind, um entsprechende Einstellungen vornehmen zu können. Bei der Anbindung einzelner Standorte ist es ratsam, in regelmäßigen Audits zu prüfen, wie sich der Datenverkehr von Filialen im Detail darstellt. Über Applikationskontrolle wird beispielsweise deutlich, welche Dienste die Anwender konkret nutzen. Der Abgleich eines solchen Reportings mit der Unternehmens-Policy zeigt, ob Anpassungen erforderlich sind. Die jeweiligen Änderungen müssen anschließend einfach umsetzbar sein.

Als Unterstützung für die zentrale IT-Abteilung ist es in vielen Fällen sinnvoll, in der Zweigstelle einen Netzwerkverantwortlichen zu definieren. Da nicht immer ausgebildete IT-Security-Profis vor Ort verfügbar sind, sollte die Bedienung der Sicherheitslösung intuitiv und ohne umfassenden Schulungsaufwand möglich sein. Es empfiehlt sich in diesem Zusammenhang, die Berechtigungen für den zentralen Management-Server qualifikationsabhängig zu vergeben. So verspricht es bereits Entlastung für die Unternehmens-IT-Abteilung, wenn der Verantwortliche der Filiale das Anlegen und Verwalten einzelner Benutzer oder beispielsweise die Freigabe neuer Drucker für das Netzwerk übernehmen kann. Denkbar ist auch, separate Administrationsrechte für den VPN-Tunnel zum Netzwerk zu vergeben.

Das zugrunde liegende Rechtekonzept sollte in diesem Umfeld genau durchdacht sein: Wer dabei von Anfang an aufmerksam vorgeht, kann auf lange Sicht den Administrationsaufwand senken und Sicherheitsregeln dennoch schnell, verlässlich und unternehmensübergreifend durchsetzen. Die eingesetzte Firewall muss diese Flexibilität jedoch nahtlos unterstützen. Daher ist es klar von Vorteil, wenn alle eingesetzten Plattformen unabhängig von der Größe auf einem einheitlichen Management basieren. Gleichzeitig liegt ein Fokus auf der Skalierbarkeit der Lösung, um ohne viel Aufwand auf neue Anforderungen reagieren zu können.

Um stets auf dem aktuellen Stand der Sicherheitstechnik und damit neuartigen Bedrohungen gewachsen zu sein, sollten IT-Verantwortliche darauf achten, wie der Hersteller der Security-Appliance seine Softwareaktualisierungen handhabt. Neben den Update-Zyklen gilt es zu hinterfragen, welche Kosten mit den Erweiterungen einhergehen. Im besten Fall stehen Updates kostenlos zur Verfügung und kommen spätestens nach den regelmäßigen Service-Wartungen zum Tragen.

Kriterien für die Auswahl einer Security-Appliance

- Benutzergruppenspezifische Applikationskontrolle,
- Aktualisierungszyklen der Software,
- Cluster-Fähigkeit,
- effektive Authentifizierungsmöglichkeiten,
- Skalierbarkeit,
- Quality of Service,
- einfache Administration,
- zentrales Management,
- Reporting-Möglichkeiten,
- Umsetzung benutzerbezogener Policies und
- Traffic Shaping.

Details als Zünglein an der Waage

Grundvoraussetzung ist, dass die Security-Lösung alle geschäftsrelevanten Anforderungen abdeckt, einfach zu implementieren ist und die Anbindung aller Rechner mit sicherer Technik unterstützt – sei es IPSec/L2TP, PPTP oder SSL. Dabei müssen selbst kleinere Zweigstellen nicht auf Hochverfügbarkeit, passgenaue Performance und die modernen Eigenschaften einer „Next Generation Firewall" verzichten. Denn ein umfassender Funktionsumfang der Zweigstellen-Appliances geht nicht zwangsläufig mit den Kosten einer Konzernlösung einher – in beiden Fällen gilt jedoch, dass das Preis-Leistungs-Verhältnis stimmen muss und alle spezifischen Bedürfnisse kompromisslos abgedeckt sind.

Besonderes Augenmerk sollte auf der einfachen Administrierbarkeit liegen, die im Zweigstellenumfeld von entscheidender Bedeutung ist. Die Reduzierung der Komplexität betrifft in vielen Fällen auch die reibungslose Verwaltung mobiler Endgeräte. Neben den eigentlichen Leistungsmerkmalen der Lösung können auch weitere mittelbare Faktoren – wie ein schneller Austausch-Service – bei der Produktauswahl eine Rolle spielen. Dazu noch ein Aspekt aus der Praxis: Einstiegs-Appliances verschiedener Hersteller unterscheiden sich nicht zuletzt hinsichtlich der Belüftung. Gerade in kleineren Büros kann eine Box ohne Lüfter, die im gleichen Raum steht, hinsichtlich der Geräuschkulisse von Vorteil sein. Dominic Haußmann/pf

Dominic Haußmann ist Senior Sales Engineer Central Europe bei Watchguard Technologies.