

Sicherheit für das mobile Netzwerk

Ist Ihre Sicherheitslösung auf die Anforderungen von heute vorbereitet?

SONICWALL[®]

PROTECTION AT THE SPEED OF BUSINESS[®]

Überblick	1
Eine neue Welt: Grundlegende Veränderungen beim Remote Access	2
Mobile Netzwerke: Vor- und Nachteile für das Unternehmen	3
Die Auswirkungen: Benutzer und Geräte lassen sich nicht mehr so einfach schützen	4
Hohe Benutzermobilität führt zu unsicheren Netzwerken	5
Sicherheit von kritischen Ressourcen in mobilen Netzwerken	6
Fazit	7

Überblick

Sind Sie der Meinung, dass Sie Ihre Unternehmensressourcen mit einem herkömmlich abgesicherten LAN vollkommen schützen können?

Dann liegen Sie falsch.

Große Fortschritte in den Remote Access-Technologien haben eine mobile Revolution in Gang gebracht. Dies hat dazu geführt, dass Unternehmensnetzwerke heute von jedem beliebigen Ort aus zugänglich sind. Noch nie gab es so viele mobile Arbeitsplätze und so viele mobile Geräte wie heute. Jeder Benutzer ist ein potentieller Remote-Benutzer. Somit ist auch jedes Gerät heute potentiell unsicher. Herkömmliche Methoden zur Sicherung der Unternehmensressourcen sind zu komplex, teuer und ineffizient geworden. Deswegen sind neue Lösungen außerhalb des Netzwerkrandes anzusetzen.

Eine neue Welt: Grundlegende Veränderungen beim Remote Access

Jeden Tag kommen neue Web 2.0-Mobilgeräte, -Services und -Unternehmenslösungen auf den Markt. Mit VoIP sind selbst Telefongespräche zu einer neuen Form des Remote-Datenzugriffs geworden. Und Mitarbeiter erhalten so gut wie überall mit ihrem Laptop, PDA oder Smartphone eine drahtlose 3G Breitband-Internetverbindung.

Dieser Wandel hat unsere Geschäftsprozesse grundlegend verändert. Wir arbeiten, wo wir uns gerade aufhalten – in Außenbüros, Home Offices, vor Ort bei Geschäftspartnern, an Produktionsstätten, in Hotels oder in Flughäfen. „Das Büro“ befindet sich nicht mehr an einen bestimmten Ort hinter einem abgesicherten Netzwerkrand. Unternehmensnetzwerke sind heute von jedem beliebigen Ort aus zugänglich.



*Die traditionellen
Netzwerk Grenzen verschwinden*

Mobile Netzwerke: Vor- und Nachteile für das Unternehmen



Mobile Netzwerke ermöglichen Einsparungen bei Gebäude- und Energieausgaben, sowie bei Pendelzeiten und -kosten, sie fördern globale Geschäftspartnerschaften und helfen Unternehmen dabei, kompetente Mitarbeiter zu gewinnen und an sich zu binden. Weitere positive Auswirkungen sind umfangreichere Bewerberpools, erweiterte Märkte und kürzere Antwortzeiten von Kunden. Da Remote Access eine entscheidende Rolle für die Wettbewerbsfähigkeit von Unternehmen spielt, ist es wichtiger denn je, dass die kritischen Systeme überall verfügbar sind und zuverlässig funktionieren.

Doch diese Vorteile sind eine Belastung für die Sicherheit. Führungskräfte und Manager erwarten einen umfassenden Zugriff auf Dateien und Anwendungen über Standard-Webbrowser. Mitarbeiter in Finanzabteilungen müssen sensible Finanzdaten auf Großrechnern in Remote-Rechenzentren abrufen können. Vertriebsmitarbeiter verlangen einen sicheren Datenzugriff von PDAs und öffentlichen Terminals in Hotels, Flughäfen und Kongresszentren. Und „externe“ Partner, Lieferanten und Berater müssen von außerhalb auf „interne“ Anwendungsressourcen zugreifen und dabei interne und externe Firewalls passieren.

**Über 90 % der Angestellten
arbeiten seit 2006* mobil oder remote.**

Hohe Benutzermobilität führt zu unsicheren Netzwerken

Mitarbeiter, Partner und Kunden können heute von jedem beliebigen Ort über Internet und Intranet bzw. über private, öffentliche, kabelgebundene oder drahtlose Netzwerke auf die gewünschten Unternehmensressourcen zugreifen. Beim mobilen Netzwerk verläuft der Netzwerkrand um die Anwendungsressourcen im Datacenter herum. Zwar leisten Firewalls immer noch wichtige Dienste am Gateway, aber sie können nicht überall Schutz gewährleisten.



Der webbasierte Zugriff auf Unternehmensressourcen von jedem beliebigen Ort aus lässt sich in vielerlei Hinsicht mit E-Commerce vergleichen. Was die Sicherheit angeht, können wir viel von innovativen E-Business-Unternehmen lernen. Um Online-Transaktionen zu sichern, werden hier Technologien wie Secure Sockets Layer Virtual Private Networking (SSL VPN) eingesetzt.

Wie können wir für Sicherheit sorgen?

Sicherheit von kritischen Ressourcen in mobilen Netzwerken

Statt nur das Kernnetzwerk abzusichern, in dem sich die Unternehmensressourcen befinden, ist es wichtig, die Verbindungen zu diesen Ressourcen zu schützen. Um eine sichere Datenübertragung zu gewährleisten, müssen alle Benutzer und ihre Endpunkte bekannt und vertrauenswürdig sein. Außerdem müssen Regeln definiert sein, die nur geeignete Ressourcen freigeben.

Im Idealfall sollten Sie die Identität aller Benutzer bestätigen, egal, ob sie sich „innerhalb“ oder „außerhalb“ des traditionellen LANs befinden und alle angeschlossenen Geräte scannen, um die Integrität zu überprüfen (z. B. ob ein gültiges Gerätezertifikat oder die neueste Viren-Signatur vorhanden ist). Nur dann sollten Benutzer regelbasierten Zugriff auf Ressourcen hinter ihrer Firewall erhalten. Um die beschriebenen Prozesse zu realisieren, benötigen Sie eine umfassende SSL VPN Remote Access-Sicherheitslösung.



***60 % der Unternehmen wünschen sich Sicherheitskontrollen,
bevor Verbindungen zugelassen werden*.***

Fazit



Unternehmensnetzwerke sind heute von jedem beliebigen Ort aus zugänglich. Traditionelle Lösungen, die den Netzwerkrand schützen, bieten heute keine umfassende Sicherheit mehr. Mit den Secure Remote Access-Technologien von SonicWALL lassen sich Geschäftsdaten in mobilen Netzwerken sicher übertragen. Dafür sorgen folgende Features:

- Bestätigung der Identität und des Sicherheitszustands aller Endpunktgeräte
- Zugangskontrolle aufgrund der Vertrauenswürdigkeit der Remote-Benutzer und ihrer Geräte
- Zugriffserlaubnis auf Ressourcen, die für autorisierte Mitarbeiter freigegeben sind

Wie erhalte ich weitere Informationen?

- Laden Sie das Whitepaper „The Center is Everywhere“ des US-Marktforschungsunternehmens Nemertes herunter: www.sonicwall.com/whitepaper
- Hören Sie sich folgenden Webcast an: www.sonicwall.com/us/9778.html
- Lassen Sie sich unseren SonicWALL-Newsletter zuschicken:
http://forms.sonicwall.com/forms/Subscription_NA

Wenn Sie uns Feedback zu diesem E-Book, anderen E-Books oder Whitepapers von SonicWALL geben möchten, senden Sie eine E-Mail an folgende Adresse: feedback@sonicwall.com.

Über SonicWALL

Als führender IT-Sicherheitsanbieter sorgt SonicWALL mit seinen intelligenten und dynamischen Service-, Software- und Hardware-Lösungen für den reibungslosen Betrieb von High-Performance-Unternehmensnetzen und senkt nicht nur die Risiken und Kosten, sondern auch die Komplexität. Weitere Informationen erhalten Sie auf unserer Website unter www.sonicwall.com.

*Statistische Angaben: Nemertes Research