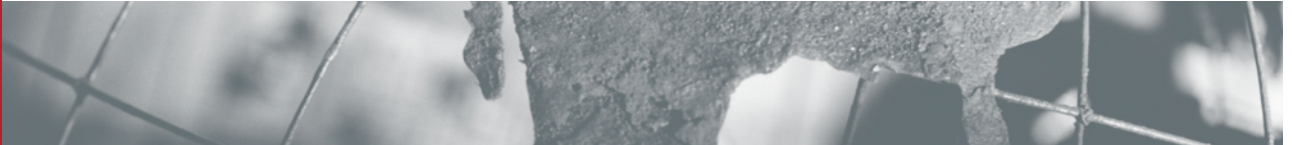


iPass Security. Ihr Best Practices Guide.

10 Tipps, wie Sie Ihre Remote-Zugänge sicherer machen können



Ein praktischer Ansatz

Der Wandel kam scheinbar über Nacht: Heute ist der Fernzugriff auf Unternehmensdaten für alle Geschäftsleute ein Muss. Doch mit jeder neuen Zugangsmethode entstand auch eine neue Technologie, die die Sicherheit in diesem unendlichen Gewirr von drahtgebundenen, drahtlosen und breitbandigen Verbindungen gewährleisten sollte.

Was können Sie tun, damit Ihre mobilen Mitarbeiter produktiv arbeiten können und Ihre wertvollen Unternehmensdaten geschützt sind?

Diese Sammlung von Tipps ist ein Best-Practice-Ansatz, mit dem Sie den Remote-Zugang in einem zunehmend komplexen IT-Umfeld sicherer machen können. Das Technologie-Unternehmen iPass hat sich auf Ihre Sicherheit spezialisiert und bietet Ihnen zahlreiche Dienstleistungen dazu.

Ob Sie sich für den Corporate Access Service von iPass® oder für einen anderen Anbieter entscheiden: Die Hinweise auf den folgenden Seiten helfen Ihnen in jedem Fall, die Sicherheits-Policy für Ihr Firmennetz zu optimieren und zuverlässig geschützte Remote-Zugänge bereitzustellen.

Wenn Sie Ihre Sicherheits-Policy überarbeiten, sollten Sie die Best-Practice-Empfehlung sämtlicher IT-Lieferanten Ihres Unternehmens berücksichtigen. Kritische Komponenten sind: Betriebssysteme, Virenschutz, Firewalls und Personal Firewall Software sowie VPN-Lösungen.

„Meldungen über Sicherheitslücken können den Ruf eines Unternehmens schädigen, den Aktienkurs drücken und zu strafrechtlicher Verfolgung oder Prozessen führen.“

Institute of Internal Auditors (IIA, Insitut für interne Revision), 01/07/03

1. Grundlegende Schritte für Ihre individuelle Risikoanalyse

Die Risikoanalyse ist ein wichtiger Bestandteil jeder Sicherheitsstrategie. Wenn Sie Bedrohungen des Unternehmens, Schwachstellen und Betriebsrisiken unter die Lupe nehmen, bedenken Sie: Beim Remote-Zugang müssen Sie zwischen Ihren Anforderungen und den spezifischen Risiken durch Einzelanwender abwägen. Dazu muss man die Gemeinsamkeiten und Unterschiede zwischen den verschiedenen Benutzerklassen verstehen. Zum Beispiel:

- Auftragnehmer, Aushilfen und Saisonarbeiter stellen unterschiedliche Sicherheitsrisiken dar.
- Die Daten, auf die Ihre Mitarbeiter zugreifen, unterscheiden sich in Vertraulichkeit und Wert – das bedingt unterschiedliche Anforderungen bezüglich der Zugriffsrechte: So unterliegt ein Mitarbeiter, der auf Personaldaten, F&E-Informationen, Verkaufs- und Marketingpläne oder Finanzdaten zugreifen muss, strengeren Sicherheitskontrollen als jemand, der nur gelegentlich E-Mails liest und versendet.

Fragen, die Sie bei der individuellen Risikoanalyse beantworten sollten:

- Benötigt der Mitarbeiter den Fernzugriff für seine Arbeit oder ist der Fernzugriff bloß eine Annehmlichkeit?
- Wohin reist der Mitarbeiter? Innerhalb der Stadt, national, international oder nur zwischen dem Büro und zu Hause?

- Brauchen Ihre Mitarbeiter High-Speed-Verbindungen?
- Greifen die Mitarbeiter zu Hause auf Netzwerk-Ressourcen des Unternehmen zu? Wenn ja, nutzen sie dazu eigene Rechner oder Rechner des Unternehmens? Verwenden sie einen privaten Breitbandanschluss oder einen privaten Wi-Fi-Zugang?
- Brauchen die Mitarbeiter Zugriff auf vertrauliche Unternehmensdaten und Anwendungen?
- Benutzen die mobilen Mitarbeiter Notebooks, die das Unternehmen zur Verfügung stellt?
- Wie viel technisches Wissen besitzt der Anwender? Können restriktive Maßnahmen ihn vor Schwierigkeiten bewahren? Kann er Sicherheitsmaßnahmen umgehen?

2. Überprüfen Sie alljährlich Ihre Sicherheits-Policy

Unternehmen verändern sich ständig. Neue Geschäftsvorgänge, Personalwechsel, andere Lieferanten und geänderte Prioritäten erfordern die regelmäßige Überprüfung der Sicherheits-Policy. Am besten kontrollieren Sie jedes Jahr, ob Ihre Sicherheitsmaßnahmen noch den Anforderungen des Unternehmens entsprechen.

Kämpfen Sie für eine einzige, gut gepflegte Benutzerdatenbank

Eine einheitliche, bereinigte AAA-Datenbank (Authentifizierung, Autorisierung, Accounting) ist einfach zu verwalten und gewährleistet die Sicherheit Ihres Unternehmensnetzes. IT-Manager nutzen sie nicht nur für den Remote-Zugriff, sondern auch um den Zugriff auf bestimmte Anwendungen und Netzwerk-Ressourcen zu steuern. Gewähren Sie Ihrem Zugangs-Provider Zugriff auf die bestehende AAA-Datenbank und Sie vermeiden das aufwändige Synchronisieren mehrerer Datenbanken!

Zur jährlichen Revision Ihrer AAA-Datenbank gehören auch folgende Schritte:

- Überprüfen Sie die Zugriffsrechte jedes Benutzers. Haben sich seit der letzten Überprüfung Aufgabenfelder der Benutzer geändert oder sind die Benutzer jetzt in einer anderen Abteilung Ihres Unternehmens tätig?
- Enthält die Datenbank ausgeschiedene Mitarbeiter?
- Sind in der Datenbank Lieferanten aufgeführt, mit denen Sie nicht mehr zusammenarbeiten?
- Wie werden in Ihrem Unternehmen die Login-Informationen für Benutzer vergeben? Ist dieser Prozess dokumentiert und wird er streng befolgt? Sieht das Verfahren Prüfungsschritte vor?
- Existieren Prozesse und Prüfverfahren, um Zugriffsrechte zu ändern, wenn ein Mitarbeiter oder Vertragspartner hinzukommt, die Stelle wechselt oder das Unternehmen verlässt?

3. Fordern Sie Authentifizierung und Schutz der Login-Informationen für Benutzer

Einige Anbieter von Remote-Zugangsdiensten können die Authentifizierung an Ihre hauseigene Infrastruktur weiterleiten. Andere nutzen eine eigene Datenbank zur Authentifizierung. Für welchen Ansatz Sie sich entscheiden – die folgenden Tipps verbessern Ihre Sicherheit:

- Stellen Sie sicher, dass alle Verbindungen von Ihren Providern und anderen Geschäftsstellen Ihres Unternehmens, die Ihre Firewall passieren, durch digitale Zertifikate bestätigt werden.
- Schützen Sie die Login-Information der Benutzer auf dem gesamten Weg vom Client bis ins Firmennetzwerk. Sie erreichen dies durch ein privates Netzwerk für den Remote-Zugang oder mit einem Internet-Provider, der für jeden Austausch von Login-Informationen digitale Zertifikate implementiert und die strenge Verschlüsselung von Authentifizierungsanfragen unterstützt.
- Vorsicht bei Provider-Lösungen mit reiner RADIUS-Authentifizierung. Diese übermitteln Login-Informationen entweder im Klartext oder verschlüsseln sie bestenfalls mit einem einfachen MD5-Hash, der mit einem Brute-Force-Angriff problemlos entschlüsselt werden kann.
- Stellen Sie insbesondere sicher, dass die Login-Information beim Aufbau der Verbindung zwischen Client und Zugangspunkt des Providers geschützt ist. Seit es Wi-Fi-Hotspots und private Wi-Fi-Zugänge gibt, ist dieser Aspekt besonders wichtig.

Verwenden Sie moderne Systeme zur Authentifizierung und Passwortverschlüsselung

Moderne Systeme zur Authentifizierung verwenden Sicherheitsmaßnahmen wie Token und digitale Zertifikate, die die Identität eines Benutzers bestätigen und eine einmalige Netzwerksitzung einleiten. Dazu stehen zwei Möglichkeiten zur Verfügung:

- **Token-basierende Authentifizierung**

Der Benutzer besitzt ein Gerät (Token) in der Größe eines Schlüsselanhängers, das einen ID-Code zeigt, der sich alle ein bis fünf Minuten ändert. Um sich am Netzwerk anzumelden, muss er seine ID, das Passwort und den aktuellen Code vom „Token“ eingeben. Obwohl Token die Kosten für Hardware erhöhen und bei Verlust umständlich zu ersetzen sind, sorgen sie derzeit für den besten Schutz beim Remote-Zugang auf der Basis von VPN.

- **Software-basierende, strenge Authentifizierung**

Als kostengünstigere, einfach zu verwaltende Alternative zu Tokens hat iPass die iSEEL-Technologie entwickelt. iSEEL steht für iPass Secure End-to-End Encrypted Login und kombiniert die eindeutige ID des Benutzers, einen Sitzungszähler und einen geheimen Schlüssel zu einem verschlüsselten ASCII-Passwort (131-Bit Elliptik). Diese Technologie schützt vor Diebstahl der Login-Informationen bei allen drahtlosen und drahtgebundenen verteilten Breitbandverbindungen. Darüber hinaus schützt iSEEL vor sog. Replay-Angriffen, da sich der Schlüssel bei jeder Sitzung ändert. Mehr über iSEEL erfahren Sie unter http://www.ipass.com/platform/platform_ps_iseel.html.

4. Verwalten Sie Ihre Passwörter aktiv

Verabschieden Sie Richtlinien für Passwörter:

- Implementieren Sie eindeutige Passwörter. Bestehen Sie darauf, dass die Passwörter so komplex sind, dass sie Wörterbuchangriffen Stand halten. Gleichzeitig müssen sie so einprägsam sein, dass Ihre Mitarbeiter sie nicht vergessen können und nicht aufschreiben müssen. So vermeiden Sie Sicherheits- und Support-Probleme.
- Passwörter müssen mindestens acht Zeichen lang sein. Diese Länge bietet ausreichend Sicherheit, und die Benutzer können sich Passwörter dieser Länge leicht merken.
- Verwenden Sie Passwörter aus Buchstaben **und** Zahlen. Wenn ein achtstelliges Passwort nur aus Kleinbuchstaben besteht, gibt es 268 mögliche Kombinationen – diese können mit Hilfe von vorhandenen Tools entschlüsselt werden.
- Erzwingen Sie durch entsprechende Maßnahmen, dass jeder Benutzer seine Passwörter regelmäßig ändert.

„Unsere Mitarbeiter müssen sich nur einen einzigen Benutzernamen und ein einziges Passwort für iPass, das VPN und die Windows NT-Domäne merken. Wir haben die AutoSave-Funktion für Passwörter deaktiviert, so dass sich auch unsere Nutzer ihre Passwörter merken müssen. Das reduziert die Anzahl der Anrufe an unserem Help Desk von Nutzern, die nach ihrem Passwort fragen.“

— **Andrew J. Daniels, Leiter der Abteilung Network Operations bei PECO II, Inc.**

Schützen Sie Ihre Passwörter:

- Weisen Sie jedem Mitarbeiter seinen eigenen Benutzernamen und sein Passwort zu und verbieten Sie, dass mehrere Benutzer dieselben Anmeldeinformationen verwenden. Hier überwiegt das Sicherheitsrisiko gegenüber der Benutzerfreundlichkeit, vor allem dann, wenn ein Mitarbeiter das Unternehmen verlässt.
- Deaktivieren Sie alle AutoSave-Funktionen für Passwörter, denn AutoSave macht jedes Notebook Ihres Unternehmens in den falschen Händen zur offenen Tür zu Ihrem Netzwerk.

5. Machen Sie Ihre Firewalls wasserdicht

Beschränken Sie die Quellen Ihres Internetverkehrs – so schränken Sie die Zugriffe auf Ihr Unternehmensnetzwerk ein.

Rang	Land
1	Peru
2	Iran
3	Kuwait
4	Vereinigte Arabische Emirate
5	Nigeria
6	Saudi-Arabien
7	Kroatien
8	Vietnam
9	Ägypten
10	Rumänien

Die Firewall Ihres Unternehmens

Ein einziger zuverlässiger Provider für eingehenden Verkehr

Sie vermindern Ihre Sicherheitsrisiken ganz einfach, indem Sie ausschließlich Daten von der IP-Adresse eines einzigen Service-Providers durch Ihre Firewall passieren lassen.

Sperren Sie einzelne Länder, um Hackerangriffe oder Cyber-Terrorismus zu vermeiden

Natürlich können Hackerangriffe auf Ihr Netzwerk von überall her kommen. Doch wenn Sie die Länder sperren, die Ihre Mitarbeiter nicht besuchen, vermindern Sie das Risiko für solche Angriffe. Ganz ehrlich: muss jeder Mitarbeiter auch von Nigeria aus auf Ihr Unternehmensnetz zugreifen können? Die Tabelle listet – gemäß einer Untersuchung von Symantec – die zehn Länder auf, von denen die meisten Hackerangriffe pro

Internetanschluss ausgehen. Untersucht wurden Länder, in denen von Januar bis Juni 2003 zwischen 100.000 und einer Million Internetnutzer aktiv waren¹).

Schließen Sie ungenutzte Ports

Wahrscheinlich werden einige Ports gar nicht für Fernzugriffe benutzt. Schließen Sie sie aus Sicherheitsgründen! Die folgende Liste zeigt verschiedene Netzwerk-Scans, die Spähaktivitäten an den Ports aufzeigen – geordnet nach den Diensten, die am häufigsten angegriffen werden. Beachten Sie bitte, dass Angriffe auch Diensten (wie Microsoft SQL-Server und File-Sharing) gelten, die auf jedem Notebook verfügbar sind.

Top Ten Netzwerk Scans² (Januar 2003 – Juni 2003)

Rang	Scantyp	Port	Alle Angriffe in Prozent
1	Common Internet File System (CIFS)	445/tcp	24%
2	NetBIOS Name Service	137/udp	16%
3	Microsoft SQL-Monitor	1434/udp	11%
4	HTTP	80/tcp	10%
5	FTP	21/tcp	6%
6	Microsoft SQL-Server	1433/tcp	6%
7	17300/tcp	17300/tcp	4%
8	HTTPS	443/tcp	4%
9	NetBIOS Session Service	139/tcp	4%
10	NetBIOS RPC	135/tcp	2%

Persönliche Firewall:

- Stellen Sie sicher, dass alle Geräte mit einer Personal Firewall geschützt werden.
- Wählen Sie einen Service-Provider, der Ihnen während jeder Internetverbindung den ununterbrochenen Schutz durch die Personal Firewall gewährleistet.
- Stellen Sie sicher, dass die Personal Firewall auf sämtlichen Geräten der Endbenutzer korrekt konfiguriert ist. Öffnen Sie nur solche Ports, die auf Anwendungen zugreifen, die der Endbenutzer tatsächlich braucht. Vermeiden und schließen Sie alle Ports, die für ihre Verwundbarkeit durch Angriffe bekannt sind.

¹ Symantec Corporation, "Symantec Internet Security Threat Report: Attack Trends"

² Symantec Corporation, "Symantec Internet Security Threat Report: Attack Trends"

6. Verwenden Sie sichere VPN-Tunnel

Mit High-Speed-Breitbandverbindungen können Ihre mobilen Mitarbeiter schneller und effektiver arbeiten – zu Hause, im Hotelzimmer oder an öffentlichen Plätzen. Allerdings sind diese ständig verfügbaren Verbindungen auch ein attraktives Angriffsziel – Hacker benutzen sie gerne als Hintertür in Ihr Unternehmensnetzwerk. Deshalb ist das Virtual Private Network (VPN) heute ein Muss im mobilen und stationären Fernzugriff.

Ein Balanceakt: Benutzerfreundlichkeit und Sicherheitsrisiken

Stellen Sie sicher, dass die Lösung Ihres Service-Providers mit Ihrer VPN-Lösung kompatibel ist und einfach integriert werden kann. Um die passende Integration auszuwählen, müssen Sie Risiken und Benutzerfreundlichkeit gegeneinander abwägen. Die folgende Tabelle zeigt verschiedene Integrations-Optionen und erklärt, welche Option sich für welche Endbenutzer eignet.

Funktion	Beschreibung	Empfehlung
1-Klick-VPN-Integration	Die Benutzeroberfläche des iPass Clients gibt die Login-Informationen (Benutzername und Passwort) an den VPN-Client weiter. Dadurch wird automatisch eine Verbindung für den Benutzer hergestellt.	<i>Verwenden Sie eine 1-Klick-Lösung, um die Anzahl der Anmeldeinformationen einzuschränken, die sich Ihre Endbenutzer einprägen müssen.</i>
1,5-Klick-AutoStart	Der VPN-Client wird automatisch über die Benutzeroberfläche des iPass Clients gestartet, der Benutzer wird zur Eingabe der Login-Informationen aufgefordert.	<i>Erforderlich für Lösungen, die eine zusätzliche, Token-basierende Authentifizierung verwenden.</i>
2-Klick-Integration	Nach der erfolgreichen Internet-authentifizierung startet der Benutzer selbst den VPN-Client.	<i>Diese Option empfiehlt sich nur, wenn Sie einen VPN-Client einsetzen, der keine 1- oder 1,5-Klick-Lösung bietet.</i>
GINA Voranmeldung	Einige Lösungen bieten eine Integration in Microsoft GINA an. Hier erstellt der Benutzer direkt eine Internetverbindung, ohne vorher den Anmeldeprozess für Windows NT/2000/XP durchlaufen zu müssen.	<i>Eine Voranmeldung in Verbindung mit einer 1- oder 1,5-Klick-VPN-Lösung ermöglicht es dem Benutzer, sich „live“ an der NT-Domäne anzumelden. Diese Lösung wird zur Unterstützung der Windows NT-Domäne empfohlen, bei Meldungen über Passwortablauf, NT-Scripting und bei benutzerdefinierter Laufwerkkonvertierung.</i>

Bei der Mellon Financial Corporation hat der Übergang zum neuen VPN-Provider reibungslos geklappt – vor allem wegen der Integration von iPass und dem Cisco VPN-Client. Die Benutzer schwärmen geradezu von der 1,5-Klick-Lösung mit iPassConnect™, das den Cisco VPN-Client automatisch lädt, sobald die Verbindung hergestellt ist.

— *iPass Case Study, Dezember 2003*

7. Koordinieren Sie Ihre Sicherheits-Policy zentral

Sicherheitsmanagement ist von Haus aus ein mehrschichtiger Prozess. Leisten Sie sich dafür die jeweils besten Werkzeuge von verschiedenen Lieferanten mit zahlreichen Verwaltungskonsolen! Ihr Remote-Zugang benötigt einen Service, mit dem Sie Ihre Sicherheits-Policy zentral koordinieren können. Sowohl für den Zugangsdienst als auch für die eingesetzten Sicherheitsprodukte von Drittanbietern. Das erleichtert die Verwaltung und stellt sicher, dass Ihre Policy stets angewendet wird.

Eine zentrale Managementlösung sollte

- ermöglichen, dass Maßnahmen für individuelle Benutzerklassen konfiguriert und durchgeführt werden.
- einfach überprüfen, wo und wie lange sich jeder Benutzer einloggen kann.
- gewährleisten, dass Sicherheitsprodukte von Drittanbietern aktiviert sind und korrekt genutzt werden. Dies gilt insbesondere für VPN-Lösungen und ihre Konfiguration, Personal Firewalls, Regeln für Maßnahmen, Virusschutz und Definitionsdateien.
- sofortige Updates für Software erzwingen, die nicht (mehr) Ihrer Policy entspricht. Dies gilt auch für Betriebssysteme und Patches.
- unbefugte Änderungen dadurch verhindern, dass die Sicherheits-Policy während jeder Internetsitzung kontinuierlich mit dem Server abgeglichen wird.

Allegheny Energy hat seine Clients aktualisiert, indem man die VPN-Lösungen verknüpfte und das Update mit Hilfe des iPass Policy Enforcement Tools automatisch während des Logins durchführte. Die Benutzer haben nicht einmal gemerkt, dass ein anderer VPN-Provider für sie zuständig ist.

— *iPass Case Study, Dezember 2003*

Funktion	Beschreibung	Empfehlung
Vorher	Der Service-Provider lässt keine Verbindung zu, wenn die Personal Firewall entweder nicht läuft oder deaktiviert ist.	<i>Legen Sie fest, dass die Benutzer sowohl die Personal Firewall als auch die Anti-Virus-Software starten müssen, bevor sie sich ins Internet einwählen.</i>
Während	Wenn Sie offene Verbindungen zum Unternehmensnetz ermöglichen, entstehen Sicherheitsrisiken und die Kosten für den Fernzugriff steigen. Einige Service-Provider erlauben dem IT-Personal, die Dauer der Sitzung durch eine Gesamtzeit oder den Abbruch bei längerer Inaktivität zu begrenzen.	<i>Legen Sie die Dauer der Nutzung und der erlaubten Inaktivität pro Benutzergruppe fest. Manche Unternehmen gestatten leitenden Angestellten längere Verbindungszeiten.</i>
Danach	Der Service beendet die Internetverbindung, sobald der Benutzer den VPN-Client deaktiviert oder die Authentifizierung am VPN-Gateway fehlschlägt.	<i>Mit dieser Funktion stellen Sie sicher, dass alle Verbindungen zum Unternehmensnetzwerk durch das VPN laufen. Verbunden mit der Sperrung des Split Tunneling stellen Sie sicher, dass alle Internetzugriffe über Ihre Firewall erfolgen. Das ermöglicht z.B. unternehmensspezifische Datenfilter.</i>

„Der iPass Service optimierte unsere bestehenden Systeme. Gleichzeitig konnten wir weiterhin unsere eigene Sicherheits-Policy durchsetzen. Der Service hat uns gezeigt, dass drahtloser Netzwerkzugang sicher und erschwinglich sein kann.“

Dustin Harris, Leiter der Abteilung IT Network und Security bei NetIQ Corporation

Policy Enforcement am Endgerät bringt umfassende Kontrolle

Die vielen Methoden des Fernzugriffs stellen höchste Anforderungen an Ihre Sicherheits-Policy. Idealerweise setzen Sie die Sicherheits-Policy im Endgerät des Benutzers vor, während und nach der Internetsitzung durch. Die Art der Kontrolle muss sich nach dem Zustand der Verbindung und nach der Benutzergruppe richten.

8. Machen Sie bei drahtloser Sicherheit keine Kompromisse

Der drahtlose Zugang ist eine weitere Herausforderung für die Sicherheit Ihres Unternehmens. Die folgenden Vorschläge verbessern die Sicherheit am Sitz Ihres Unternehmens und am Wohnort Ihrer Mitarbeiter, die über drahtlose Netze, Wi-Fi-Hotspots und Breitbandverbindungen auf das Unternehmensnetzwerk zugreifen.

Ändern Sie das Standardpasswort des Administrators Ihrer WLAN-Router

Wenn ein möglicher Angreifer ein drahtloses Netz entdeckt, ist das Standardpasswort einer der einfachsten Wege das Netz zu schädigen.

Verwenden Sie Media Access Control-Filterung (MAC) und Wired Equivalent Privacy (WEP)

Verwenden Sie möglichst viele Kontrollwerkzeuge, um den Zugriff über private drahtlose Netzwerke auf autorisierte Benutzer zu beschränken – einschließlich der MAC-Adressfilterung. Wenn an Ihrem WLAN-Router nur WEP zur Verfügung steht, benutzen Sie einen Schlüssel, der schwer zu erraten ist und ändern Sie ihn regelmäßig.

Halten Sie alle Firmware, wie WLAN-Router, stets auf dem neuesten Stand

Mit aktueller Firmware lösen Sie Kompatibilitätsprobleme; Sie schließen Sicherheitslücken und korrigieren eventuelle andere Fehler. Durchsuchen Sie deshalb regelmäßig die Webseiten Ihrer Lieferanten nach neuen Updates.

Nicht mehr Leistung als nötig

Mehr Leistung ist nicht zwingend besser. Die drahtlosen Router, Zugangspunkte und Bridges einiger Anbieter lassen sich so einstellen, dass das drahtlose Netz seine Signale nur so weit überträgt, wie es nötig ist.

Ermöglichen Sie den Zugriff auf Ihr Unternehmensnetzwerk nur per VPN

Jeder drahtlose Zugriff auf Ihr LAN sollte heute per VPN erfolgen. Technologien, die auf 802.1X und WPA basieren, werden immer besser – ziehen Sie jetzt einen Umstieg in Erwägung.

Beachten Sie besonders den Zugriff über Hotspots

Der Zugang über öffentliche Hotspots ist anfällig für Angriffe. Deshalb muss Ihre drahtlose Lösung alle Zugangsinformationen und Passwörter an den Endgeräten verschlüsseln und die Benutzung digitaler Zertifikate für die gegenseitige Authentifizierung von Benutzern und Hotspots vorschreiben. Achten Sie darauf, ob Ihr Wi-Fi-Hotspot-Provider plant, 802.1X und WPA-basierende Lösungen einzusetzen.

Schreiben Sie VPN auch für den drahtlosen Zugriff von privaten Rechnern vor

iPass empfiehlt Ihnen dringend, VPN für sämtliche Zugriffe auf Ihre Unternehmensdaten zu nutzen. Das gilt insbesondere für Benutzer, die von zu Hause aus drahtlos auf Ihr Netzwerk zugreifen.

„Im Jahr 2003 waren rund 42% aller Notebooks Wi-Fi-fähig. Bis zum Jahr 2007 werden es 98% sein!“

IDC, 2003

9. Sensibilisieren Sie Ihre Benutzer für Sicherheitsfragen

Verstehen Ihre Benutzer, warum Netzwerksicherheit so notwendig ist? Sind sie sich der möglichen Schwachstellen bewusst? Sobald sie begreifen, wie sehr eine Sicherheitslücke dem Unternehmen und damit auch ihrer persönlichen Lebensgrundlage schaden kann, werden sie ein erstaunliches Sicherheitsbewusstsein an den Tag legen.

Möglicherweise wissen Ihre Wi-Fi-Benutzer nicht, was es bedeutet, auf ihrem Notebook „file sharing“ zu aktivieren: Nun können andere Benutzer sehen, was sich auf ihrer Harddisk befindet! Und wenn sie wüssten, welche Konsequenzen es hat, die Firewall zu deaktivieren, würden sie wohl zweimal nachdenken, bevor sie die entsprechende Aufforderung eines Download-Programms befolgen.

Lancieren Sie eine Kampagne zum Thema „Sicherheitsbewusstsein“

Die Kommunikations- oder Schulungsabteilung Ihres Unternehmens kann Ihnen helfen, bei den Benutzern das Bewusstsein für Sicherheitsthemen zu schärfen. Damit gewinnen Sie nicht nur die Unterstützung der Angestellten für Sicherheitsmaßnahmen und ihre Umsetzung – Sie können gleichzeitig die Funktion Ihrer Abteilung vermitteln und sich Respekt für Ihre Dienstleistungen verschaffen. Hier sind einige grundlegende Sicherheitsvorkehrungen, die jeder Mitarbeiter befolgen sollte:

- Schalten Sie den Computer aus, wenn Sie Ihren Arbeitsplatz verlassen.
- Nehmen Sie Ihr Notebook mit nach Hause oder schließen Sie es an einem sicheren Ort ein.
- Verwenden Sie einen Passwort geschützten Bildschirmschoner, wenn Sie Ihren Rechner unbeaufsichtigt lassen.
- Notieren Sie niemals Ihre Zugangsdaten oder persönliche Passwörter. Speichern Sie sie auch nicht auf Ihrem Computer.
- Lassen Sie Passwörter niemals automatisch speichern – egal, für welche Anwendung.
- Loggen Sie sich nicht ins Internet ein, wenn die File-Sharing-Funktion aktiviert ist.
- Bevor Sie Webseiten durchsuchen oder Dateien herunterladen, überzeugen Sie sich von der Integrität der jeweiligen Seite.

10. Verwenden Sie Tools zur Überwachung und Verwaltung, um Ihre Sicherheits-Policy zu optimieren

Jede Lösung für den Fernzugriff muss Werkzeuge enthalten, mit denen der Kunde seine Verbindungen überwachen und verwalten kann. Damit erhält das IT-Personal nicht nur wertvolle Informationen über die Verbindungen, sondern auch die Möglichkeit:

- Muster für mögliche Missbräuche zu entdecken
- Die Nutzungsgewohnheiten aller Endbenutzer festzustellen, um Sicherheitsmaßnahmen zu verfeinern
- Nutzer zu erkennen, die eine Schulung benötigen
- Spezielle Überwachungsmethoden zu entwickeln für Benutzer mit besonders hohem Risiko oder Zugang zu besonders wertvollen Unternehmensdaten

Sie möchten mehr wissen?

iPass ist einer der führenden Anbieter für Zugangsdienste und ist mit „allgegenwärtigen“, einfachen und sicheren Lösungen für externe und mobile Mitarbeiter bei vielen großen Unternehmen in aller Welt vertreten.

Der iPass Corporate Access Service gibt IT-Mitarbeitern die Möglichkeit zu strengen Kontrollen und zur Umsetzung von Sicherheitsvorschriften – im weltweiten virtuellen iPass Netzwerk in 150 Ländern. Das gilt auch für Wi-Fi-Netzwerke und private Breitbandverbindungen der Unternehmen. Die einzigartige Kombination von Sicherheit, Flexibilität und Kontrolle ist für viele Unternehmen das wichtigste Argument, wenn sie iPass zum exklusiven Dienstleister für den Remote-Zugang und für mobile Datenzugriffe machen.

Um mehr über iPass Corporate Access zu erfahren, besuchen Sie noch heute www.ipass.com. Dieses Handbuch im PDF-Format können Sie bei www.iPassIsThere.com herunterladen.