

netopia®

**Vereinfachte Wireless-
Sicherheit für Netzwerke bei
Privatanwendern und kleinen
Unternehmen**

**60% bis 70%
der Netzwerke,
die privat oder
von kleinen
Firmen betrie-
ben werden,
sind ungesichert**

WiFi Protected Setup (WPS) ist auf Netopias Gateways für Privatanwender und Geschäftskunden aktiviert. Mit WPS wird das Einrichten eines sicheren WiFi-Netzwerks im Heimbereich oder im Büro so einfach wie das Eingeben einer PIN oder Drücken einer Taste. Das Netopia-Gateway erkennt, wenn sich neue WiFi-Geräte innerhalb der Reichweite befinden, und fragt den Benutzer, ob das Gerät mit dem Netzwerk verbunden werden soll. Netopia wird WPS ab Anfang 2007 in Gateways für Privatanwender und Geschäftskunden einsetzen.

HINTERGRUNDINFORMATIONEN ZUR SICHERHEIT VON WIRELESS- NETZWERKEN

Wireless-Sicherheit ist für Konsumenten und kleine Unternehmen aus den gleichen Gründen wichtig wie für Großunternehmen. Wenn Sie ein ungesichertes Funknetzwerk in Ihrem Haus oder Büro betreiben, kann jeder in der näheren Umgebung Ihre Online-Aktivitäten ausspionieren. Abhängig von der Konfiguration Ihres Netzwerks ist es sogar möglich, dass Fremde Zugriff auf die Festplatte Ihres Computers erhalten könnten.

Auch wenn es niemanden in Ihrer Nähe gibt, der Sie ausspionieren oder schädigen will, könnten Nachbarn Ihre Internetverbindung nutzen. Dies würde Ihnen nicht nur Bandbreite entziehen, für die Sie bezahlt haben. Falls Ihr Nachbar online etwas Illegales tun würde, könnte Ihr Netzwerk als Ausgangsort identifiziert werden. Schätzungen zufolge sind 60% bis 70% der Netzwerke, die privat oder von kleinen Firmen betrieben werden, ungesichert. Umfragen lassen darauf schließen, dass die Chancen hoch sind, dass ein ungesichertes Netzwerk auch ausgenutzt wird.

WARUM SIND SO VIELE WIRELESS-NETZWERKE VON KONSUMENTEN UND KLEINEN UNTERNEHMEN UNGESICHERT?

Die Technologien zum Absichern von Funknetzwerken in diesen Umgebungen stehen seit einiger Zeit zur Verfügung. Frühere Versuche, Netzwerke sicherer zu machen, konnten aufgrund der dürftigen Verschlüsselungstechnologie einfach unterlaufen werden, wie dies bei WEP

(Wired Equivalent Privacy) der Fall war. WEP war dazu gedacht, eine vergleichbare Vertraulichkeit wie herkömmliche kabelgebundene Netzwerke zu bieten. Jedoch litt WEP unter einigen Problemen. Die Installation, Einrichtung und Konfigurierung war für die meisten Anwender sehr kompliziert. Daher wurde es oft nicht oder fehlerhaft installiert. Zudem wurde bei solchen Netzwerken, bei denen WEP korrekt installiert war, eine gravierende Schwachstelle gefunden: jeder WEP-Schlüssel kann mit frei erhältlicher Software in zwei Minuten oder noch schneller geknackt werden. Dies ist alles andere als sicher!

WIFI PROTECTED ACCESS (WPA UND WPA2)

WEP wurde zuerst im Jahr 2003 von WPA (WiFi Protected Access) und später, im Jahr 2004, vom vollständigen IEE 802.11i-Standard (auch als WPA2 bezeichnet) abgelöst. Sowohl WPA als auch WPA2 sind eine Klasse von Systemen zur Absicherung von drahtlosen Computernetzwerken. Sie wurden als Reaktion auf die Schwachstellen entwickelt, die beim Vorgängersystem WEP gefunden wurden.

Bei WiFi Protected Access handelt es sich um auf Standards basierende, interoperable Sicherheitserweiterungen, die die Datensicherheit (Verschlüsselung) und Zugangskontrolle (Authentifizierung) für bestehende und zukünftige WiFi-Wireless-LAN-Systeme erheblich verbessert. Ein weiterer Grund für die Entwicklung des neuen Standards war die Notwendigkeit, durch Software-Upgrades die WiFi-Sicherheit bestehender WiFi CERTIFIED™-Produkte erhöhen zu können.

WPA ist eine modifizierte Version von WEP, bei der der Schlüssel sehr häufig geändert wird. Es ist erheblich sicherer als WEP. Ab September 2003 müssen alle Geräte der Standards 802.11b und 802.11g, die im Rahmen der WiFi-Zertifizierung getestet werden, WPA implementieren. Daher ist WPA sehr weit verbreitet. WPA implementiert den größten Teil des IEE 802.11i-Standards und war als Zwischenlösung vorgesehen, die WEP ersetzt. WPA wurde mit dem Ziel entwickelt, mit allen Wireless-Karten zu funktionieren, aber nicht unbedingt mit Wireless-Zugangspunkten der ersten Generation.

43% der WiFi-Anwender halten die Installation von Sicherheitsfunktionen in einem privaten WiFi-Netzwerk für mittelschwer bis sehr kompliziert

WiFi Protected Access ist eine sehr große Verbesserung der Wireless-Sicherheit. Zwar kann keine Sicherheitslösung für sich beanspruchen, absolut sicher zu sein, jedoch ist die von WPA gebotene Sicherheit bedeutend. Viele Kryptographen sind sich sicher, dass WiFi Protected Access alle bekannten Angriffe gegen WEP abdeckt. Es bietet zusätzlich eine starke Benutzerauthentifizierung, die es in WEP nicht gibt.

WPA2 ist die Implementierung der zweiten Generation, basierend auf neuer Verschlüsselungstechnologie. Das originale WPA nutzt die WEP-Verschlüsselung, die mit häufigem Schlüsselwechsell verbessert wurde. WPA2 hingegen nutzt die neue Verschlüsselungstechnologie AES (Advanced Encryption Standard). Die Zertifizierung für WPA2 begann im September 2004. Seit dem 13. März 2006 müssen alle Geräte, die das WiFi-Zeichen tragen, für WPA2 zertifiziert sein. WPA2 implementiert den vollständigen IEEE 802.11i-Standard.

WPA und WPA2 verfügen über einen speziellen Modus für Privatanwender und kleine Unternehmen, die keinen Zugriff auf Netzwerkserver haben. In diesem Modus gibt der Benutzer manuell das Anfangskennwort ein, um WiFi Protected Access zu aktivieren.

Im Enterprise-Modus erfolgt die Authentifizierung über 802.1X und EAP. Im Personal-Modus (für Privatanwender und kleine Unternehmen) wird nur ein Zugangspunkt und ein Client-Gerät benötigt, im Enterprise-Modus wird üblicherweise ein RADIUS-Server oder ein anderer Authentifizierungsserver eingesetzt.

DIE EINRICHTUNG IST SOWOHL BEI WPA ALS AUCH BEI WPA2 IMMER NOCH SEHR KOMPLIZIERT

Für viele Anwender im Privatbereich und bei Kleinunternehmen ist die Installation, Einrichtung und Konfigurierung sehr kompliziert. Neueste Umfragen ergaben, dass 43 % der WiFi-Anwender die Installation von Sicherheitsfunktionen in einem privaten WiFi-Netzwerk für mittelschwer bis sehr kompliziert halten (WiFi Alliance/Kelton Research, 2006).

Auch moderne WiFi-Produkte verbessern die Situation nicht wirklich, da die Konfiguration der Sicherheitsfunktionen immer noch langsam und wenig intuitiv ist. Ein Beispiel: Um WiFi WPA in Windows XP verwenden zu können, muss der Benutzer die Wireless-Clients unter Windows XP manuell patchen und außerdem sicherstellen, dass die Wireless-Zugangspunkte und -Netzwerkadapter korrekt konfiguriert sind.

Hier sind die nötigen Anweisungen, um WPA in WiFi-Netzwerken mit Windows XP-Clients einzurichten:

1. Lesen Sie den „Überblick über das WPA-Sicherheitsupdate für drahtlose Verbindungen in Windows XP“ (Microsoft Knowledge Base, Artikel Q815485).
2. Verifizieren Sie, dass auf jedem Windows XP-Client Windows XP Service Pack 1 (SP1) oder höher läuft.
3. Verifizieren Sie auf jedem Windows XP-Client, dass der Adapter mit dem Dienst „Konfigurationsfreie drahtlose Verbindung“ (Wireless Zero Configuration, WZC) kompatibel ist. Details erhalten Sie in der Dokumentation des Adapters, auf der Website des Herstellers oder beim telefonischen Support. Aktualisieren Sie, wenn nötig, den Treiber für den Netzwerkadapter und die Konfigurations-Software, damit WZC auf dem Clients unterstützt wird.
4. Laden Sie bei jedem Windows XP-Client das „Windows XP-Supportpatch für Wireless Protected Access“ herunter und installieren Sie es anhand der beiliegenden Anweisungen.
5. Führen Sie die Schritte durch, die in dem in Schritt 1 angegebenen Artikel unter „Änderungen an drahtlosen Zugriffspunkten“ beschrieben sind.
6. Führen Sie die Schritte durch, die in dem in Schritt 1 angegebenen Artikel unter „Änderungen an drahtlosen Netzwerkadaptern“ beschrieben sind.

DIE LÖSUNG ZUR EINFACHEN EINRICHTUNG DER WIRELESS-SICHERHEIT: WIFI PROTECTED SETUP (WPS)

WPS verfügt über die leistungsfähigen Sicherheitsfunktionen von WPA und WPA2, sorgt aber dafür, dass deren Installation und Aktivierung in einem WiFi-Netzwerk schnell und einfach vonstatten geht

WiFi Protected Setup hat das Ziel, die Installation und Aktivierung der Sicherheitsfunktionen eines Netzwerks für private WiFi-Anwender zu erleichtern. Dazu verfügt WiFi Protected Setup über die leistungsfähigen Sicherheitsfunktionen von WPA und WPA2, sorgt aber dafür, dass deren Installation und Aktivierung in einem WiFi-Netzwerk schnell und einfach vonstatten geht.

„Die WiFi-Technologie wird im Bereich der Unterhaltungselektronik immer weiter verbreitet, sodass eine einfache Benutzung wichtiger denn je ist,“ so Frank Hanzlik, WiFi Alliance Managing Director. „Die WiFi Alliance wird weiterhin eine zentrale Rolle bei der Verbesserung der Bedienbarkeit spielen.“

Die Zertifizierung für WiFi Protected Setup erweitert das Portfolio an Zertifizierungen, die Mitgliedern der WiFi Alliance zur Verfügung stehen. Diese Mitglieder stellen eine Vielzahl von Geräten her, angefangen bei PCs und Druckern über Fernsehgeräte und Kameras bis hin zu Spielekonsolen.

Das WPS-System ermöglicht es Konsumenten, mit nur wenigen Klicks eine starke WPA-Verschlüsselung in ihren Heimnetzwerken zu aktivieren. Keine komplizierten Kennsätze mehr, die gemerkt werden müssen. Keine langen Sequenzen mit Hexadezimalzahlen mehr, die eingegeben werden müssen. Kein „Das ist mir zu mühsam“ mehr.

WiFi Protected Setup erleichtert die Einrichtung sicherer WiFi-Netzwerke im Heimbereich und bei kleinen Unternehmen. Es verwendet Methoden zur Konfigurierung des Netzwerks und zur Aktivierung der Sicherheitsfunktionen, die die meisten Endanwender kennen, wie beispielsweise die Eingabe einer PIN oder das Drücken einer Taste. Das neue System, das auch in Windows Vista integriert ist, funktioniert mit Computern, Gateways, Peripheriegeräten und Unterhaltungselektronik. Der Grundgedanke ist, dass Sie einen WPS-Modus am Gateway initiieren, dann eine einfache Zahlenfolge (ähnlich einer PIN) eingeben und eine Taste drücken (oder auf ähnliche Weise einen sicheren Schlüsselaustausch zum Abrufen eines WPA-Schlüssels starten). Für alle Fälle sind auch die Geräte in der Lage, den zugrundeliegenden WPA-Schlüssel zu generieren. Es wurde bereits die Möglichkeit erwogen, diesen Schlüssel beispielsweise auf ein USB-Gerät zu übertragen, um einen Schlüsselaustausch über Hardware statt über Funk zu ermöglichen.

WPS ist eine nicht-proprietäre Spezifikation, die sich optimal in die heterogene WiFi-Welt eingliedert und als zertifizierte Technologie von der WiFi Alliance kontrolliert wird. Jedes Gerät, das das WPS-Zeichen trägt, muss die Laborprüfung durchlaufen und bestanden haben. ■

netopia®

Netopia Europe
Tel +33 (0) 1 45 29 91 00
info@netopia-europe.com

Weitere Informationen erhalten Sie telefonisch unter +33 1 45 29 91 00 oder auf unserer Web Site: www.netopia.com

Copyright© 2006, Netopia Inc. Alle Rechte vorbehalten. Netopia, das Netopia-Design und 3-D Reach sind eingetragene Marken der Netopia Inc., eingetragen beim U.S. Patent and Trademark Office. "Broadband Without Boundaries" sind Marken der Netopia Inc. Alle anderen Marken sind Eigentum der jeweiligen Inhaber.

DE_wifi_security_simple_181206