



|                    |              |                 |        |
|--------------------|--------------|-----------------|--------|
| Medientyp:         | Tageszeitung | Gedr. Auflage:  | 38191  |
| Erscheinungsdatum: | 29.10.2009   | Verk. Auflage:  | N/A    |
| Seite:             | 29           | Verbr. Auflage: | N/A    |
|                    |              | Reichweite:     | 550000 |

# Die unterschätzte Gefahr

40 Prozent der WLAN-Netze in Bremen sind nicht ausreichend gesichert / Verschlüsselung ist ein Muss

**Bremen (emsn).** Knapp jedes zehnte Wireless Local Area Network (WLAN) ist komplett ungesichert, jedes dritte WLAN lediglich mit dem veralteten und unsicheren Verschlüsselungsstandard WEP geschützt. Das ist das zentrale Ergebnis einer aktuellen Untersuchung der PC-Feuerwehr in 22 deutschen Städten. Auch in Bremen ist die Situation alarmierend: Sieben Prozent der WLANs sind vollkommen ungesichert, 33 Prozent mit WEP gesichert. Damit sind 40 Prozent der Funknetze nicht ausreichend gegen Hacker-Angriffe geschützt.

Die Vorteile eines WLANs liegen auf der Hand: Schnelle Verbindungen, keine störenden Kabel und eine weitgehend automatische Konfiguration. Kein Wunder, dass sich viele Internetnutzer mittlerweile für einen solchen Anschluss entscheiden. „Immer noch haben viele Menschen aber nicht erkannt, wie wichtig es ist, seinen Internet-Zugang auch entsprechend zu schützen“, schlussfolgert Marc Trampedach von der PC-Feuerwehr Bremen aus der diesjährigen Untersuchung seines Unternehmens.

Ein unzureichend gesichertes WLAN ist vergleichbar mit einer offenen Haustür: Jeder der das entsprechende Equipment besitzt, kann sich mühelos Zugang zum fremden Internet-Zugang beschaffen. Unerwünschte Fremdbenutzer des eigenen WLANs sind nicht nur lästig, sondern auch gefährlich. Private Daten wie Urlaubsfotos, Passwörter, E-Mails oder Online-Banking-Daten können so in die falschen Hände geraten. Wer sein Internet nicht richtig sichert, kann sich unter Umständen sogar strafbar machen. Denn wenn Fremde über den eigenen Internet-Zugang Straftaten begehen, indem sie beispielsweise illegal Musik herunterladen, kann der Besitzer unter Umständen auch rechtlich belangt werden.

In 22 Städten haben Partner des Franchise-Unternehmens PC-Feuerwehr in diesem Sommer eine etwa 40 Kilometer lange Strecke abgefahren, die sowohl durch Wohn- als auch Gewerbegebiete führte. In diesen Bereichen haben sie Funknetze gezählt und deren Verschlüsselungsstatus ermittelt. Die Bilanz: Im Durchschnitt sind elf Prozent aller WLANs noch unverschlüsselt.

Absolutes Schlusslicht in puncto Sicherheit ist Bad Schwartau: Dort sind knapp 40 Prozent aller WLANs vollkommen ungesichert. Jeder dritte Haushalt mit einem entsprechenden Internetzugang stellt somit ein leichtes Opfer für Hacker und Trittbrettfah-

rer dar. Am besten gesichert sind die drahtlosen Internet-Zugänge hingegen in Offenbach und Darmstadt wo nur gut fünf Prozent unverschlüsselt sind. Auch die Hauptstadt liegt mit sieben Prozent ungeschützten WLANs noch unter dem Durchschnitt.

Dabei ist die Absicherung eines Funknetzwerkes in wenigen Schritten vollzogen. Ist der Router in Betrieb genommen, sollte zunächst das voreingestellte Passwort geändert werden. Per Browser lässt sich über die IP-Adresse (Internet-Protokoll-Adresse, diese steht im Handbuch) auf das Menü des Routers zugreifen. Ist das Passwort geändert, sollte auch die Kennung des Netzwerks (SSID – Service Set Identifier) mit einem eigenen Namen versehen werden. Anschließend muss die Verschlüsselung eingeschaltet werden.

Derzeit gängig ist die WPA2-Verschlüsselung (Wi-Fi Protected Access 2), in kleineren Netzwerken mit einem Preshared Key (WPA2-PKS). Diese Zahlenfolge muss allen Teilnehmern des WLANs bekannt sein, da mit ihrer Hilfe der Netzwerkschlüssel generiert wird. Auch der Vorgänger WPA bietet ausreichend Schutz. Lediglich das veraltete WEP (Wired Equivalent Privacy) sollte aufgrund von Sicherheitsmängeln nicht mehr zum Einsatz kommen.

Zwei weitere Methoden sorgen zusätzlich dafür, Eindringlinge vom Netzwerkverkehr fernzuhalten. So wird über die MAC-Adresse nur ausgewählten Netzwerkkarten die Verbindung erlaubt. Hintergrund: Jeder Netzwerk-Chip wird vom Hersteller mit einer eigenen Kennung (MAC – Media Access Control) versehen. Unter der Option „MAC-Filter“ lassen sich im Menü eines Routers diejenigen Karten eintragen, die auch wirklich untereinander kommunizieren dürfen. Über den Befehl „ipconfig /all“ kann die Adresse des Funk-Adapters auf dem jeweiligen Computer in Erfahrung gebracht werden. Völlige Sicherheit bietet jedoch auch diese Methode nicht, da sich entsprechende Adressen auch fälschen lassen.

Standardmäßig ist bei den meisten Routern DHCP (Dynamic Host Configuration Protocol) aktiviert. Jedem Neuankömmling im Netz wird dadurch automatisch eine Adresse zugewiesen. Das ist zwar praktisch, wenn weitere Rechner eingebunden werden sollen, doch bedeutet es auch, dass eventuelle Angreifer stets eine gültige Adresse erhalten. Sicherer ist es, die DHCP-

Server-Funktionalität zu deaktivieren und den Teilnehmern, die sich in das Netzwerk einwählen dürfen, eine feste IP-Adresse zu geben. Diese wird dann ebenfalls im Menü des Routers eingetragen. Allerdings muss die Prozedur für jeden neu hinzukommenden Rechner wiederholt werden. Die Zeit für diese vier Schritte beträgt aber nur wenige Minuten und sollte unbedingt investiert werden. Auch wenn es eine hundertprozentige Sicherheit nicht gibt, erschweren diese Methoden das unerwünschte Eindringen in Funknetzwerke doch erheblich.

Insgesamt ist trotz allem ein positiver Trend in Sachen Sicherheit zu verzeichnen. So führt die PC-Feuerwehr bereits seit fünf Jahren jedes Jahr eine Überprüfung der Sicherheitsstandards durch. Im Vergleich

zum Vorjahr ist mit elf Prozent ungesicherten WLANs bereits ein deutlicher Sicherheitsanstieg zu beobachten: So waren beispielsweise vor vier Jahren noch 36 Prozent aller WLANs ungeschützt, in Bremen waren 2007 noch 25 Prozent der Netzwerke offen. Diese positive Tendenz lässt sich sicherlich auch darauf zurückführen, dass Internet-Anbieter inzwischen immer öfter automatische Verschlüsselungen bei der Einrichtung von Funknetzen vornehmen. „Trotzdem spüren wir bei der täglichen Arbeit immer noch Unsicherheiten bei unseren Kunden, wie sie sich und ihren Computer gegen ungewollten Missbrauch schützen können“, weiß Trampedach aus der Praxis des PC-Notdienstes zu berichten.



WLAN sorgt für komfortables, kabelloses Surfen. Wer sein Netzwerk jedoch nicht richtig absichert, wird unter Umständen nicht lange Freude daran haben.

FOTO: AVM