

Freier Eintritt in die Netzwerke

Zahl der offenen Funknetzwerke in Bremen steigt / Mangelndes Sicherheitsbewusstsein der Hansestädter

Von unserem Mitarbeiter
Peter Tänzler

BREMEN. Das Thema Sicherheit in der Computerwelt beherrscht seit Monaten die Fachpresse. So ziemlich jedes PC-Magazin wie auch unzählige Internetseiten weisen in regelmäßigen Abständen ausführlich auf die vielen Gefahren hin, die ungesicherten Rechnern und Netzwerken sowie den dort befindlichen Daten drohen. Vor allem drahtlose Verbindungen (WLAN) erweisen sich aufgrund ihres großen Empfangsbereiches als anfällig. Doch an den hanseatischen PC-Besitzern scheinen die zahlreichen Warnungen ungehört abzuprallen. Laut einer Untersuchung der PC-Feuerwehr stieg die Zahl der ungesicherten WLANs im Vergleich zum Vorjahr sogar an.

25 Prozent (2006: 22,5 Prozent) der Funknetzwerke auf einer 40 Kilometer langen Teststrecke erwiesen sich als ungesichert. Spitzenreiter ist die bayerische Landeshauptstadt. In 35,8 Prozent der drahtlosen Netzwerke in München konnte ungehindert eingedrungen werden. Zum Vergleich: In Dresden und Hamburg sind 90 beziehungsweise 88 Prozent der drahtlosen Netzwerke ausreichend gesichert.

Wer sein Netzwerk ohne Absicherung lässt, handelt grob fahrlässig. Denn für ein unbefugtes Eindringen in diese sind keine Fachkenntnisse notwendig. Ein einfaches Notebook mit WLAN-Karte reicht aus. Datenspione können so nicht nur auf den Festplatten aller angeschlossenen Rechner schnüffeln, sondern auch einen möglicherweise vorhandenen Internetzugang verwenden. Nach einem Urteil des Landgerichts Hamburg (AZ 308O407/06) hat ein unverschlüsseltes drahtloses Netzwerk auch rechtliche Folgen: Demnach müssen Betreiber eines Funknetzwerks Vorsorge vor gesetzwidrigem Missbrauch treffen.

Warum die Zahl der ungesicherten Netze in Bremen dennoch gestiegen ist, lässt sich angesichts der umfangreichen Medienberichterstattung und der expliziten Warnungen der Hersteller eigentlich kaum erklären. „Es ist eigentlich unglaublich“, sagt auch Volker Bannert von der PC-Feuerwehr in Bremen, „aber aus meiner Erfahrung weiß ich, dass sich immer noch viele keine Gedanken machen und sich der Gefahren nicht bewusst sind“. Zudem würden viele Nutzer versuchen, ihren Router über das

Funknetzwerk zu aktivieren. Wenn jedoch eine Verschlüsselung auf diesem Wege eingetragen und aktiviert wird, bricht die Verbindung zunächst ab. Erst wenn auch am Rechner (in den Einstellungen der WLAN-Karte) der entsprechende Schlüssel bekannt ist, funktioniert die Verbindung wieder. „Viele wissen nicht, wo sie das einstellen müssen und sind froh, wenn sie über-

haupt eine Online-Verbindung hinbekommen“, weiß Bannert.

Dabei ist die Absicherung eines Funknetzwerkes ist 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 Netzwerkes (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-PSK). 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 auf-

grund von Sicherheitsmängeln nicht mehr zum Einsatz kommen.

Zwei weitere Methoden sorgen zusätzlich dafür, unerwünschte Eindringlinge vom Netzwerkverkehr fernzuhalten. So wird über die MAC-Adresse nur ausgewählten Netzwerkkarten die Verbindung erlaubt. Hintergrund: Jeder Netzwerkchip 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 Funkadapters 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 stets wiederholt werden.

Die Zeit für diese vier Schritte beträgt 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. Zudem sollte das Urteil des Landgerichts Hamburg zusätzlich sensibilisieren. „WLANs sind eine sinnvolle Technik und bieten viel Flexibilität im Alltag, aber ungesichert eingesetzt stellen sie eine große Gefahr dar“, bilanziert PC-Experte Bannert.



Surfen im Garten ist eine schöne Sache, kann jedoch zum Ärgernis werden, wenn das WLAN nicht gesichert ist.