Freies Wort

Montag, 7. April 2008
57. Jahrgang, Nummer 81

UNABHÄNGIGE THÜRINGER TAGESZEITUNG

Preis 0,90 €
www.freies-wort.de

AUSGABE SUHL

Wenn die virtuelle Tür sperrangelweit offen steht

Computersicherheit | Viele Nutzer von W-LAN kümmern sich kaum um den Schutz ihres Netzwerks und nehmen so Angriffe in Kauf, stellt ein IT-Experte fest

Von Marco Schreiber

Suhl – „Vater" geht auf Nummer sicher. „C-Team" auch, „Kaacki" ebenso, „Püppchennetz" dito. Die virtuellen Türen ihrer Computer ins weltweite Datennetz sind genauso gut verriegelt wie die Haustüren in der Suhler Friedbergsiedlung. Irgendwo, in einem der knallfarbigen Wohnblocks, haben sie ihre DSL-Router aufgestellt. Computer und Router verständigen sich per Funk, dem so genannten W-LAN. Weil die Reichweite der W-LAN-Sender fast 300 Meter beträgt, kann Alexander Rogon mit seinem Notebook von der Straße aus die Netzwerke von „Vater" aufspüren, von „Kaacki" und von „C-Team". Mit jedem Windows-PC können diese virtuellen Namensschilder gelesen werden. „Kaacki", „C-Team" und „Vater" haben ein recht gutes Schloss an die zugehörige Tür geschraubt, auf ihre Funknetzwerke – und damit auf die Inhalte ihrer Computer – kann niemand ohne Weiteres zugreifen.

N.'* Tür allerdings steht sperrangelweit offen. „Wir haben einen Volltreffer", ruft Rogon. Der Fachmann für Computersicherheit sitzt hinter dem Steuer seines Mercedes und balanciert das Notebook auf den Knien. Das werksseitig eingebaute Windwos-Programm sucht nach allen verfügbaren W-LAN-Netzen und meldet: N. ist ungeschützt. Rogon lässt den Mauszeiger über den Bildschirm tanzen und ist mit wenigen Klicks online. Tippt www.freies-wort.de in die Adressleiste des Browsers und lässt sich die neuesten Artikel anzeigen.

Ein Handy piept leise. Rogon angelt es von der Mittelkonsole seines Wagens. „Das Telefon hat sich jetzt eingebucht", sagt der Mann mit den braunen Augen nach einem Blick auf das Anzeigefeld. Es ist ein W-LAN-Telefon und nicht angewiesen auf das GSM-Netz der Mobilfunkanbieter. Rogon zaubert ein zweites Mobiltelefon hervor und tippt die Nummer des W-LAN-Handys ein. Zwei Augenblicke später tüdelt es leise – dem ungeschützten Netzwerk von N. sei's gedankt. Unter dessen Namen, der IP-Adresse seines Rechners, könnte Rogon jetzt nach Herzenslust telefonieren, E-Mails verschicken oder Kinderpornografie. Er könnte strafbare Dinge tun, Musik und Filme von illegalen Tauschbörsen laden, Terrorbotschaften verbreiten. „Man sieht nur die IP des Netzinhabers", erklärt er. „Die eigene ist nicht sichtbar."

Viele Nutzer sind erschreckend sorglos

Vor zehn Jahren hat sich Rogon nach dem Informatikstudium der IT-Sicherheits-Branche zugewendet. Unter IT, der Abkürzung für Informationstechnologie, versteht er alle Geräte, die in einem Netzwerk auf Daten zugreifen können – den stationären PC im Wohn- oder Chefzimmer, das Zweitgerät des Sohnes oder der Sekretärin, den Laptop, die PDA-Geräte, Telefone, W-LAN-Handys. „Ich versuche, IT-Systeme so abzusichern, dass niemand hineinkann", erklärt Rogon. „Damit niemand die Informationen ausspioniert."

Seit sieben Jahren tut er das mit seiner eigenen Firma in Erfurt. Und stellt immer wieder fest: „Es ist erschreckend, wie sorglos viele Internetnutzer sind." Wie sorglos sie etwa Konto- und Kreditkartendaten preisgeben in Online-Shops. Die Unwissenheit sei groß, meint der Experte, bei Privatnutzern und Unternehmen gleichermaßen. „Es gilt die Devise, ich habe ja nichts zu verbergen", sagt Rogon, klappt das Notebook zu, startet den Wagen und rollt von der Friedbergsiedlung Richtung Innenstadt.

Nächster Halt: die Wohnblocks an der Robert-Koch-Straße. Rogon schaltet den Computer an, startet ein weiteres Programm, ein Werkzeug zur Netzwerkanalyse. In einem schlichten weißen Fenster werden sieben W-LAN-Netze in Reichweite angezeigt. „Sehen Sie? Mein Netz und Bino senden auf dem gleichen Kanal", sagt Rogon und tippt mit dem Zeigefinger auf das Display. „Windows verrät nicht, wenn ein anderes Netzwerk auf der gleichen Frequenz mitspielt", erklärt er. „Das Internet ist langsam, und die Nutzer fragen sich, warum."

Rogon stellt den Computer auf den Beifahrersitz und fährt in die Hainbergstraße. Hält, greift sich das Notebook, tippt ein paar Befehle ein. „Hier ist ein völlig offenes Netz, ohne jede Verschlüsselung", sagt er. „OPN" steht in der betreffenden Zeile, OPN wie open.

Elf andere Netzwerke in Reichweite arbeiten verschlüsselt. „Mit den Windows-Bordmitteln ist ein Zugriff auf diese Netze nicht möglich", erklärt Rogon. Seine Suhler Stichprobe zeigt: Fast fünf von 100 W-LAN-Nutzern verzichten auf jeglichen Schutz. Viele haben noch nicht einmal den Namen ihres Netzwerks geändert, es heißt noch immer Fritz-Box-WLAN, default oder Speedport 501 V.

Etwa ein Drittel der Stichprobe habe den Verschlüsselungsstandard WEP benutzt, stellt Rogon fest, Klaus zum Beispiel, Familie und Haus. Allerdings: „Der WEP-Standard ist nicht mehr sicher." Innerhalb von Minuten könne der Schlüssel geknackt werden – ein Konstruktionsfehler des Programms, meint der Sicherheitsexperte. Der Hacker – oder ein neugieriger Nachbar mit Langeweile – könnte sich auf dem Rechner so frei bewegen, als wäre es der eigene. Er könnte sich durch die E-Mails klicken und den Schriftverkehr lesen. Die Fotos vom letzten Strandurlaub wären genauso wenig sicher wie die Zeugnisse.

Von der Neugier des Nachbarn ist es für Rogon nicht weit zu einem anderen Szenario. „Ein Hacker könnte die Informationen auf dem PC verschlüsseln", sagt Rogon. „Fotos, Lebensläufe, Zeugnisse, brisante Informationen." Er könnte drohen, die Informationen zu veröffentlichen. Oder zu vernichten, um den Besitzer zu erpressen. In den USA, erzählt Rogon, habe es solche Hackerangriffe schon gegeben. Gegen Zahlung von 1000 Dollar, so der Deal, bekomme man den Schlüssel zum eigenen PC.

Ein weiteres Szenario setzt kaum mehr kriminelle Energie voraus. „Der Angreifer kann im Namen des Nutzers Waren im Internet bestellen und mit den ausgespähten Bankdaten auch bezahlen." Mit etwas mehr Hackerwissen könnte der Angreifer einen Trojaner auf den geknackten Rechner schmuggeln, ein Spionageprogramm. Wenn das Spähprogramm ein selbst verfasstes ist, würde es von keinem Virenscanner gefunden, so Rogon.

Der Trojaner könnte melden, wann der Nutzer seine Online-Bank besucht und welche PIN ihm Einlass gewährt. Beim nächsten Aufruf der Bankseite könnte der Angreifer dem Nutzer eine gefälschte Homepage vorsetzen – und so die TAN-Nummer abgreifen. „Wenn dann das Konto leergeräumt ist, wird die Bank nicht dafür haften", erklärt Rogon. „PIN und TAN wurden ja korrekt eingetippt." Er selbst nutzt einen persönlichen Schlüssel, wenn er Bankgeschäfte abwickelt, berichtet er und zieht eine briefmarkengroße Speicherkarte aus dem Notebook.

Wenig kriminelle Energie genügt

Etwa zwei Drittel der W-LAN-Netze, die Rogon bei der Nachmittagsfahrt durch Suhl aufspürt, sind mit WPA und WPA 2 abgesichert. „Beide gelten als sehr sicher", sagt der Experte. „Nur bei WPA gibt es erste Knack-Ansätze." Welcher Standard im heimischen oder im Firmennetzwerk verwendet wird, hängt von der Einstellung der DSL-Routers ab. „95 Prozent der Surfer kaufen DSL-Router mit W-LAN", schätzt der Experte. In der EU werden schon jetzt mehr Notebooks mit eingebautem W-LAN-Chip verkauft als stationäre PC. „Über W-LAN kann man viel einfacher in einen Computer einbrechen als über das Internet", stellt Rogon fest.

Viele Nutzer seien sich der Gefahren nicht bewusst – oder wehren sie lapidar ab. „Wer will schon auf meinen PC drauf, wird gefragt, oder: So wichtig sind meine Daten nicht", zählt Rogon auf. Verstehen kann er es nicht. Kaum jemand möchte einen Einbrecher im Haus haben, der in der Post herumschnüffelt, Fotoalben durchblättert, Zeugnisse liest, intimste Gewohnheiten beobachtet, die EC-Karte samt PIN-Nummer klaut – Dinge, die sich ein Angreifer auch von vielen heimischen Computern holen kann. Ein Drittel der Suhler, so Rogons Stichprobe, sind potenziell gefährdet.

Über N.' Netz wird während der Stichprobe ein Film aus dem Internet gesaugt, der Titel erscheint auf Rogons Display. „Daddy ohne Plan" kam im Herbst 2007 in die US-Kinos und läuft seit wenigen Tagen in Deutschland. Legal ist diese Aktion mit Sicherheit nicht – egal, ob der Besitzer des Netzes oder ein Nachbar dahinter steckt.

**Name geändert*

Info

W-LAN ist die Abkürzung für Wireless Local Area Network und bezeichnet kabellose lokale Netzwerke. Der W-LAN-Standard **WEP** gilt als unsicher, weil das Passwort mit frei erhältliche Programmen entschlüsselt werden kann. Außerdem kann jeder Nutzer den Datenverkehr mitlesen. Deshalb sollte **WPA** aktiviert werden. Als noch sicherer gilt **WPA 2,** solange keine simplen Passwörter verwendet werden, die über eine Wörterbuch-Attacke geknackt werden können. **Passwörter** sollten Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen enthalten und nicht kürzer als 32 Zeichen sein. Außerdem sollten die werkseitigen Passwörter sowie der SSID-Name geändert und die Fernkonfiguration des Routers deaktiviert werden.