Andrea Strässle Journalistin
www.journalistin.ch

Facts | Informatik | 27. November 2003

Die Freiluftspione

Mit Laptops und selbst gebastelten Antennen ausgerüstet horchen IT-Fans drahtlose Computernetze von Firmen aus. Die Hobby-Datenjäger machen leichte Beute.

Gestalt tappt zickzack über den spärlich beleuchteten Parkplatz im Basler Rheinhafen. In der einen Hand hält sie eine Zigarette, mit der anderen schwenkt sie eine Pringles-Chips-Dose in der Luft, langsam, als brenne sie bengalische Zündhölzchen ab. Aus einem zehn Schritte entfernt parkierten Campingbus brüllt einer im Zweisekundentakt: «Schlecht. – Schlecht. – Besser. – Schlecht.» Es ist Dienstagnacht, halb zehn. Die Wardriver sind auf der Jagd nach drahtlosen Computernetzen.

Das bizarr anmutende Hobby findet zunehmend Anhänger in der Schweiz. Um die hundert solcher Freiluftthacker, schätzt einer von ihnen, kurven mit Laptops, aus Verpackungen gebastelten Antennen und GPS-Geräten durch die Gegend. Ob in Zürich, Bern, Basel, Luzern, Zug oder Genf – die IT-Fans machen sich einen Sport daraus, Funknetzwerke, so genannte WLANs (Wireless Local Area Networks) zu orten, zu kartieren und auszuhorchen.

Markus, 29-jährig, mit einem Ring im Ohrläppchen, lässt den Arm mit der Pringles-Dose sinken. «Scheissbetonmauern», knurrt er. Seine Richtfunkantenne Marke Eigenbau hat eine Reichweite bis zu 300 Metern, gebastelt ist sie nach einer Anleitung aus dem Internet. «Was wären wir ohne unseren Kollegen, den Lötpapst?», sagt Markus und zieht an der Zigarette. Ein Kabel führt hinüber zum Bus. Hinter den Scheiben hockt der 21-jährige Alex, Brille auf der Nase, Laptop auf den Knien. Sein Blick klebt am Bildschirm.

WLANs sind bei Computerspezialisten wie -amateuren äusserst beliebt. Dank WLAN können Laptops, Computer und Server drahtlos kommunizieren. Die Daten fliessen per Funk über eine Basisstation, den so genannten Access Point. Das erspart Firmen aufwändige Kabelinstallationen, und Heimbenutzer können auch vom Balkon aus im Internet surfen. Doch die frei durch die Luft schwirrenden Daten sind leichte Beute für die Lauscher mit ihren Laptops und Antennen.

Wardriving, die Alternative zum einsamen Hackerdasein im stickigen Kämmerlein, begeistert den 14-jährigen Schüler genauso wie den gesetzten Hacker. Ihr Begehren gilt unverschlüsselten Access-Punkten von Arztpraxen in den besten Zürcher Quartieren, frei zugänglichen Netzwerken von Schweizer Grossverteilern oder einem Basler Architekturbüro, in dem Geschäftsund Mitarbeiterdaten, E-Mails und Bewerbungsdossiers zum Stöbern einladen.

Während einige der Schnüffler als verschworene Zweierteams durch die Strassen kurven, organisieren sich andere in Regionalgruppen, die regelmässige Treffen und gar Workshops anbieten. Die Tessiner kennen die Zürcher, die Berner kennen die Basler. Die meisten Trupps sind über EMail locker verbunden, laden gegenseitig zu Touren ein, tauschen Tipps aus und pflegen Kontakte auch nach Deutschland, Österreich und in die USA.

Alex und Markus kennen sich seit der Informatikerlehre. Inspiriert von einer Wardriver-Homepage im Internet packte Markus letzten Herbst auf dem Weg zur Arbeit kurzerhand im Tram seinen Laptop aus und ortete mit einer normalen WLANKarte erste Signale. Diese Vorstudie kam den zwei Frischlingen auf ihrer ersten Tour im November vor einem Jahr zugute: Kaum waren sie losgefahren, merkten sie, dass ihnen eine Software fehlte. Im Nu hatten die beiden mit Markus' Laptop ein unverschlüsseltes Netz angezapft, den Zugang zum Internet aufgespürt und die Software gratis heruntergeladen. Wer ein Wardriver ist, weiss sich zu helfen.

DAS SIGNAL IM RHEINHAFEN ist zu wackelig, als dass sich Alex in das Netz einklinken könnte. Markus zuckt mit den Schultern. «Was solls, suchen wir was anderes.» Die Fahrt geht Richtung Innenstadt. Alex' Laptop, das alle eingehenden Signale akustisch vermeldet, tutet fast pausenlos: Basel ist von Drahtlosnetzwerken überzogen. Alle paar hundert Meter blinkt auf den Bildschirmen ein neues Netz auf. Eine im Internet frei erhältliche Software listet alle georteten Access Points automatisch mit Namen, allfälliger Verschlüsselung, Kanal und Signalstärke auf und speichert die Informationen inklusive erschnüffelten Datenpaketen und GPSKoordinaten.

Mehr als die Hälfte der Access Points auf Alex' und Markus' Bildschirmen funken den gesamten Datenverkehr unverschlüsselt ins Offene hinaus. Die Standard-Verschlüsselung WEP (Wired Equivalent Privacy) sei zwar mit etwas Sachverstand zu knacken, sagt Alex. Dazu müsse einer aber Stunden oder gar Tage dem verschlüsselten Datenverkehr lauschen. Ein Aufwand, der Alex und Markus den Appetit auf ein Netz verdirbt. Sie bevorzugen die Klartextfunker und prüfen die Namen der aufgelisteten Access Points. «Netzbezeichnungen geben Hinweise, wo es sich lohnt, genauer hinzuhören», erklärt Markus.

Mitten in einem Wohnquartier taucht ein Access Point namens «any» auf der Liste auf. Ein Heimbenutzer, der bei seinem Gerät nicht einmal die Grundeinstellung des Herstellers geändert hat, vermutet Alex und winkt ab. Er lauert auf Netzbezeichnungen, die einen klingenden Firmennamen in den Äther hinausposaunen und brisante Daten erahnen lassen. Heute bleibt der Durchbruch jedoch aus. Schliesslich beherzigen sie die Botschaft eines Netznamens in Bahnofsnähe: «Zupfdi».

Mit schwererem Abhör-Geschütz als einer Chipsdose fahren die beiden Informatiker Christoph und Dani auf, zwei Urgesteine des Wardrivings aus der Zürcher Szene: Auf dem Dach ihres Opel Omega thront eine 80 Zentimeter lange Rundstrahlantenne, auf einem selbst gebauten Holzträger fixiert und mit Plastikriemchen festgezurrt. Christoph, in dessen braunen Bart sich bereits ein paar graue Haare mischen, steuert durch Zürich Nord. «HAL Hacking at Large 2001» prangt auf seinem blauen T-Shirt, Souvenir eines internationalen Treffens der Hackergilde, zu dem Tausende mit Zelt und Laptop in die Niederlande gereist waren. Dani, in verblichenen Jeans und Schlabberpulli, hat sich mit dem Laptop auf dem Beifahrersitz eingerichtet. An den Seitenfenstern kleben zwei Linux-Pinguine.

«Wir haben aus Jux damit angefangen», sagt Christoph. Vor zwei Jahren erzählten Freunde aus den USA von dem neuartigen Zeitvertreib. Christoph und Dani waren begeistert, starteten mit Kollegen auf erste Touren und reservierten im Mai 2002 die Internet-Domaine wardriving.ch.

WÄHREND DIE SOFTWARE fleissig Zugangspunkte aufzeichnet, plaudern Christoph und Dani über den vergangenen Mittwochabend, an dem sie sich mit einer anderen Spielart des Wardrivings offensichtlich bestens amüsiert haben: Zehn Leute der Zürcher Szene trafen sich zu einem Wardrive Contest. Vier Teams in je einem Auto zogen aus, um in der Stadt möglichst viele Zugangspunkte aufzuspüren. «Mit drei bis vier Leuten im Auto steigt automatisch der Fun-Faktor», sagt Dani und kann ein Glucksen nicht unterdrücken. Innerhalb von zwei Stunden hatten die Wardriver 1813 Access Points kartiert, 1346 davon waren unverschlüsselt. «Über 1000 Firmen- und Privatnetze, die alles ausplaudern, was über sie gesendet wird.»

Der nicht ganz unauffällige Kombi hat das Hallenstadion passiert. «Einmal, in der Industrie Winterthur, da haben mich die Bullen herausgewinkt», erinnert sich Christoph. Denen sei sein Schneckentempo und die Antenne auf dem Dach wohl nicht geheuer gewesen. Er habe ihnen dann verklickert, dass er Messungen für ein Forschungsprojekt mache und allein deshalb zu nächtlicher Stunde unterwegs sei, weil tagsüber die Natelstrahlung stören würde. Christoph lacht in seinen Bart hinein: «Das haben sie mir glatt abgekauft.» Wardriver befinden sich in einer rechtlichen Grauzone. «Bis jetzt ist keiner drangekommen», sagt Christoph. «Wir schauen ja nur, knacken keine Passwörter und richten keinen Schaden an.»

Im Industriegebiet zwischen Oerlikon und Glattbrugg biegt Christoph in einen Innenhof ein, steigt aus und öffnet den Kofferraum: Der Blick fällt auf ein Sammelsurium an Antennen. Der aus Basel bekannte Klassiker «Pringles Original», daneben das etwas grösseres Modell «Sirop de Menthe» – «etwas vom Besten, kriegst du aber nur in Frankreich und stinkt am Anfang saumässig» –, weiter ein mit Kupferdraht umwickeltes Plastikrohr, eine Variation mit Holzgriff und schliesslich zwei professionelle Antennen inklusive Magnetknopf fürs Autodach.

Christoph hockt vor den Kofferraum und mustert die Liste an verfügbaren Zugangspunkten auf dem Laptop. Ein paar Minuten später hat er sein Opfer ausgewählt: Ein bekannter Name aus der Modebranche. Dani prüft über Twixtel, ob die Postadresse der Firma übereinstimmt. Treffer. Christoph klopft beim Access Point an. Sofort erhält er Zugang zum Firmennetz. Christoph schüttelt den Kopf: «Die Firma hat bestimmt Tausende von Franken investiert, um das Firmennetz mit tollen Firewalls gegen das Internet abzugrenzen. Aber den Access Point lassen sie sperrangelweit offen, so dass du unbehelligt mitten ins Netzwerk eintauchen kannst.»

Dani und Christoph beugen sich tiefer über den Laptop, zwischendurch huschen Christophs Finger über die Tasten. «Ist ja abartig», entfährt es ihm. Der Server listet ihm ohne irgendein Passwort bereitwillig 3800 User auf, mit Vor- und Nachnamen. Christoph und Dani wissen aus beruflicher Erfahrung, dass immer ein paar darunter sind, die ihren Namen auch als Passwort verwenden. Grosser Beliebtheit erfreuen sich zudem Passwörter wie «Blume» oder «Sonne». Es wäre keine Kunst, sich einzuloggen und Daten zu klauen oder zu manipulieren.

Von solchen krummen Dingern würden sie jedoch die Finger lassen, versichern die beiden Wardriver, «aber das Gefühl zu wissen, dass man könnte, wenn man wollte …», fügt Christoph mit einem Zwinkern hinzu. Dass man könnte – zum Beispiel über den Mailserver dieses Modeunternehmens eine E-Mail an die Konkurrenz schicken: «Hallo, Lacoste! Scheissware, die ihr da produziert.» Grosses Gelächter. Oder dem Druckerserver eine Netzadresse zuteilen, die bereits von einem Server belegt ist, und damit das Firmennetz lahm legen? Dani verzieht das Gesicht: «Wenn das bloss bei mir nie jemand macht. Als Administrator legst du Nachtschicht ein, bis du den Fehler findest.»

OFT INFORMIEREN DIE WARDRIVER die Netzbetreiber per E-Mail über die Sicherheitslecks. In den meisten Fällen bleibt eine Antwort aus; die Verschlüsselung wird stillschweigend aktiviert oder der Zugangspunkt abgeschaltet. Keine Firma will Versäumnisse an die grosse Glocke hängen.

Es wird kalt auf dem Industrieparkplatz in Zürich Nord. Dani und Christoph können sich kaum vom Firmennetz des Modeunternehmens losreissen. Sie fachsimpeln, finden eine Abzweigung zu einem weiteren Netz. «In einem Netzwerk dieser Grösse könnte man sich tagelang herumtreiben, und es würde nicht langweilig», findet Christoph. «Das ist wie im Hölloch,» sagt Dani. «Und wir sind die Höhlenforscher.» Doch schliesslich fährt auch dem zähesten Höhlenforscher die Kälte in die Knochen, und er packt zusammen. Ab in die Beiz.

Service-Box:

W-LAN dicht machen

Ändern Sie die Liefereinstellung der SSID (Service Set Identifier). Die SSID ist der Name Ihres Access Points. Er darf keine Rückschlüsse auf Sie oder Ihre Firma erlauben.

Schalten Sie die WEP-Verschlüsselung ein, und ändern Sie den Schlüssel regelmässig.

Verstecken Sie Ihr Netz, indem Sie den SSID-Broadcast deaktivieren. So ist das WLAN nur zu orten, wenn Datenpakete gesendet werden.

Verwenden Sie eine Zeitschaltuhr, und schalten Sie Ihr WLAN bei längerem Nichtgebrauch ganz aus.

Schützen Sie Computer und Server mit Passwörtern.

Beschränken Sie den Zugang zum WLAN auf Benutzer mit berechtigter MAC-Adresse. Die MAC (Medium Access Control) ist die Hardware-Kennung eines Gerätes.