Hacken für jedermann

Mit einem einfachen Programm können selbst Amateure fremde Festplatten ausspionieren – fast wie die Profis.

Es ist ein kleines Experiment mit einer simplen Fragestellung: Was lässt sich herausfinden über jemanden, von dem man nichts kennt außer dem Inhalt seiner Computerfestplatte? Wie viel Privates vertrauen die Menschen ihrem Rechner an, wie sorgfältig gehen sie mit ihren Daten um? Worauf also würden BKA-Beamte bei einer Online-Hausdurchsuchung stoßen?

Der Versuchsaufbau, vorgeführt von einem PC-Experten: ein handelsüblicher Rechner, ein DSL-Anschluss und ein kleines Programm, kostenlos heruntergeladen von einer niederländischen Webseite, installiert und gestartet.

Jetzt muss man etwa 30 Minuten warten.

Bei dem Programm handelt es sich nicht um ausgefeilte Schnüffelsoftware, echte Hacker würden darüber lachen, aber es lässt sich einfach bedienen, auch von Laien. Das Programm macht nichts anderes, als im Internet nach schlecht gesicherten Rechnern zu suchen. Und das funktioniert erschreckend gut.

Nach einer halben Stunde hat das Programm zwischen 30 und 50 Computer gefunden, die ohne Firewall und andere Vorsichtsmaßnahmen online im Netz stehen. Nun zeigt es in einem Fenster erste Details: Welche Bezeichnung der Besitzer seinem Rechner gegeben hat (Erstaunlich, wie viele PC „Wohnzimmer“ heißen und wie viele Laptops „Läppi“). Es zeigt an, welche Teile der Festplatte und welche Ordner einsehbar sind (oft die Festplatte D, auf der die meisten Windows-Nutzer ihre Daten aufbewahren, häufiger noch den Ordner „Eigene Dateien“).

Die fremden Rechner lassen sich bequem durchforsten, so als säße man vor dem eigenen. Und da die meisten Leute ihre Dateiordner säuberlich benennen, ist das Suchen nach Persönlichem auch gar nicht schwer. Da hat zum Beispiel jemand einen Ordner „Bewerbungen“ angelegt, er sucht eine neue Stelle in der holzverarbeitenden Industrie. Natürlich stehen Name, Adresse und Telefonnummer auf den Dokumenten, da weiß man, wen man vor sich hat. Lebenslauf, Zeugnisse und Bewerbungsfoto liegen auch da.

Im Ordner „Rechnungen“ finden sich Belege für die Karten vom Roger-Whittaker-Konzert, das lässt auf seinen Musikgeschmack schließen. In „Dokumente“ bewahrt er den Schriftkram auf: Streit um die Nebenkostenabrechnung, Kündigung beim Provider, Briefe an den Scheidungsanwalt. Die Ordner „Programme“ und „Filme“ stecken voller geklautem Material, erkennbar an den typischen Dateinamen der Raubkopiererszene. In „XXX“ liegen die gesammelten Pornobilder, in „Fotos“ die Bilder von der Einschulung der Kinder oder der Party zum Vierzigsten und in „Fotos privat“ die ganz privaten Bilder von der Ehefrau.

Mancher, der sich all seine verschiedenen Zugangscodes zu Ebay, zu Diskussionsforen oder E-Mail-Konten nicht merken kann, legt sich dafür einen eigenen Ordner an. Und nennt den brav: „Meine Passworte“.

Rechner für Rechner geht das so, überall private Unterlagen. Mit etwas Geduld lassen sich die Besitzer der Daten quasi komplett durchleuchten.

Die Opfer kriegen davon nichts mit. Dabei ist die Sicherheitslücke, die das alles möglich macht, uralt: Bei Windows kann man Ordner oder ganze Festplatten freigeben, damit andere Rechner darauf zugreifen können. Gedacht ist das, um zum Beispiel die Musik vom Wohnzimmerrechner auf den Laptop zu überspielen oder umgekehrt. Bei unvorsichtigen Benutzern sind diese Freigaben aber nicht nur im eigenen privaten Netzwerk erreichbar, sondern vom gesamten Internet aus.

Die Lücke wäre leicht zu stopfen: Schon das Installieren des „Service Pack 2“, einer kostenlosen Sicherheitssoftware von Microsoft, macht das Türchen für die Möchtegern-Hacker dicht.

Anders als richtige Hacker oder die Profis vom BKA können die Nutzer des niederländischen Programms nicht gezielt auf einen bestimmten Rechner zugreifen, das Laienprogramm sucht einfach wahllos im Internet nach anfälligen Rechnern.

Auch die Spezialisten vom BKA würden über Sicherheitslücken in fremde PC eindringen, allerdings über andere, weniger bekannte Wege. Auf diversen Sicherheitsseiten im Internet werden allwöchentlich neue Lücken bekannt: Manchmal lässt sich über präparierte Musikstücke ein Code auf fremde Rechner schmuggeln, mal gelten Bildbetrachtungsprogramme als gefährdet, dann wieder sind Datenbankprogramme unsicher. Selbst in scheinbar harmlosen Word-Dokumenten können sich Schädlinge verbergen, manchmal ist sogar Anti-Viren-Software lückenhaft. Kaum jemand kann alle Sicherheitslöcher im Blick halten – und seinen Rechner sauber.

Unter Umständen reicht sogar der Besuch einer Webseite, um sich einen Trojaner einzufangen. Diese Miniprogramme laden dann weitere Programme nach, beispielsweise eine Software zum Fernsteuern des PC. Oder einen Keylogger, der alle Tastatureingaben unauffällig mit-

ULLSTEIN BILDERDIENST

Jugendlicher beim Surfen, Bundeskriminalamt in Wiesbaden: *Mit Geduld lassen sich die*

protokolliert und bei Gelegenheit zurücksendet.

Lücken dafür gibt es also genug, man muss das Opfer des Angriffs nur dazu bringen, in die Falle auch hineinzutappen. Irgendwie muss das Ziel ja überzeugt werden, das präparierte Musikstück zu laden, die vergiftete Webseite zu besuchen. Dieses Verfahren nennen die Experten „Social Hacking“. Da geht es nicht um technische Finessen, das ist die Kunst der Manipulation von Menschen. Hackerprofis wenden sie schon länger an.

In den letzten Wochen zum Beispiel machten E-Mails die Runde, die angeblich von der GEZ stammten oder vom Internetprovider 1&1. In beiden Fällen enthielt die Mail eine unerwartete Rechnung, Details könne man sehen, wenn

STEFAN HUSCH / TERZ

Besitzer der Daten komplett durchleuchten

man den Anhang der Mail öffne. Wer darauf klickte, installierte in Wahrheit ein bösartiges Programm.

Eine besonders raffinierte Mail kam – angeblich – vom BKA selbst. Man sei beim Raubkopieren erwischt worden, hieß es darin. Eine Anzeige sei erlassen, das Dokument im Anhang möge man bitte ausdrucken und mit einer Stellungnahme versehen zurück ans BKA faxen.

Eine Falle, klar. Im Grunde wissen die meisten Internet-Nutzer mittlerweile, dass man den Anhängen in E-Mails nicht vertrauen darf, niemals – aber wenn die Post doch vom BKA stammt? Und so echt aussieht? Und weil gerade ohnehin überall die Rede von den BKA-Fahndern war, fühlte sich so mancher offenbar ziemlich ertappt. Die Finte war so erfolgreich, dass sogar das Bundeskriminalamt vor der falschen BKA-Post warnte.

Ansbert Kneip

wachungsstaat umgebaut, Schäuble setzt das jetzt konsequent fort.“

Tatsächlich ist für immer mehr Bürger der eigene Rechner in den letzten Jahren zu einer zentralen Schnittstelle ihres Alltags geworden. Sie erledigen darüber private und geschäftliche Korrespondenz, ihre Steuererklärung, Bankgeschäfte, Reiseplanungen und viele Einkäufe, sie speichern auch privateste Fotos und Videos.

Schon ambitionierte Amateure können weite Teile fremder Festplatten ausspähen (siehe Kasten). Zudem lassen sich an den heimischen Rechner angeschlossene Webcams und Mikrofone (wie sie etwa zum Video-Telefonieren verwendet werden) mit entsprechendem Know-how von außen auch als Guck- und Horch-Apparaturen zweckentfremden.

Selbst die schärfsten Kritiker bestreiten nicht, dass das Internet immer stärker dazu genutzt wird, Straftaten vorzubereiten – und dass die Sicherheitsbehörden darauf reagieren müssen. Nur gibt es die notwendigen Grundlagen längst: Seit 2001 wurden mehr als zehn Gesetze erlassen, erweitert oder modifiziert. Die neuen Vorhaben wie die Online-Durchsuchungen sind da nur die Spitze. Sie allerdings stellen den vom Bundesverfassungsgericht zuletzt in seinem Urteil zum Großen Lauschangriff 2004 verbürgten „Kernbereich privater Lebensgestaltung“ besonders krass in Frage.

Parallel rüsten die Dienste ihre IT-Bereiche auf. Erst Anfang des Jahres nahm in Berlin ein „Gemeinsames Internet Zentrum“ die Arbeit auf, das unter der Führung des Bundesamts für Verfassungsschutz (BfV) steht, in das aber auch BKA-Beamte entsandt werden. Sie sollen das Netz präventiv nach möglichen „Gefährdern“ (Fahnder-Jargon) durchsuchen.

Der Bedarf an Fachkräften ist offenbar groß. Von acht aktuellen Stellenausschreibungen auf der BfV-Web-Seite haben sieben einen IT-Bezug. Auch in dem im vorigen Herbst aufgelegten rund 130 Millionen Euro schweren „Programm zur Stärkung der Inneren Sicherheit“ (PSIS) spielt das Internet eine zentrale Rolle.

In der PSIS-Wunschliste des Innenministeriums an den Haushaltsausschuss war von der „Online-Durchsuchung“ die Rede. Es gehe um „die technische Fähigkeit, entfernte PC auf verfahrensrelevante Inhalte hin durchsuchen zu können“.

Tatsächlich ist man in Wiesbaden schon deutlich weiter. Immerhin hatte der Generalbundesanwalt das BKA schon im März 2006 gebeten, die technischen Voraussetzungen zu schaffen und dabei erwähnt, dass „dem Vernehmen nach verschiedene deutsche Sicherheitsbehörden bereits seit geraumer Zeit erfolgreich mit dem Instrument des heimlichen Abziehens von Daten auf fremden Computern“ arbeiten.

In Nordrhein-Westfalen wurden Online-Durchsuchungen in der letzten Novelle des dortigen Verfassungsschutzgesetzes ausdrücklich erlaubt – allerdings nur für Verfassungsschützer, nicht für Polizisten. Gerhart Baum (FDP), ehemaliger Bundesinnenminister, hält aber schon das NRW-Gesetz für „unglaublich“ und bereitet eine Verfassungsbeschwerde dagegen vor. „Das Gesetz ist so offenkundig gegen die Grundsätze der Verfassung gerichtet, dass man nur staunen kann.“

Auf den Rechtsweg und Gerichte hoffen auch die zahlreichen Gegner der Vorratsdatenspeicherung. Medienverbände fürchten weitere erhebliche Einschränkungen des Informantenschutzes, betroffene Telekom-Unternehmen vor allem Mehrkosten für Technik und Personal in angeblich dreistelliger Millionenhöhe.

Burkhard Hirsch sagt: „Sobald das Gesetz wird, klage ich.“ Auch die Kritiker-Initiative „Arbeitskreis Vorratsdatenspeicherung“ kündigt bereits Verfassungsbeschwerde an.

Die Hoffnung auf die Justiz ist begründet – nicht nur wegen der aktuellen BGH-Entscheidung: Sowohl bei der Volkszählung als auch beim Großen Lauschangriff hat das Verfassungsgericht die Pläne der Politik zumindest deutlich gestutzt.

Beim BKA will man langwierigen Gesetzes- oder gar juristischen Verfahren nicht untätig zusehen. Das Amt habe immerhin die Aufgabe, neue Ermittlungstechniken zu entwickeln, heißt es dazu im Innenministerium – man könnte dort also argumentieren, dass sich etwa die BKA-Forschungsabteilung auch weiterhin mit Trojanern und Co. befassen muss. Die Frage wird nur sein, mit welchem Etat. Innenausschuss-Chef Edathy bezeichnet es jedenfalls als „ungewöhnliche Situation, dass im Haushalt Gelder für die Entwicklung einer Technik bereitstehen, deren Anwendung rechtswidrig wäre“.

Petra Bornhöft,
Matthias Gebauer, Marcel Rosenbach