2007/01 Inland

https://shop.jungle.world/artikel/2007/01/dein-freund-und-hacker

Dein Freund und Hacker

Von **Carsten Schnober**

In Nordrhein-Westfalen darf der Verfassungsschutz private Rechner ohne das Wissen ihrer Besitzer durchforsten. Bald könnte das überall in Deutschland möglich sein. von carsten schnober

Ein Wort schafft es regelmäßig, den Benutzern von Personal Computern (PC) Schweißperlen auf die Stirn zu treiben: Sicherheitslücke. Denn auf vielen Rechnern lagern Informationen, die nicht für die Öffentlichkeit bestimmt, aber durchaus interessant sind – Adressbücher, Kalender, Geschäftspläne, private E-Mails und Bankdaten. Weil zumindest der nordrhein-westfälische Landtag davon überzeugt ist, dass dort auch Terroristen ihre Pläne für Anschläge abspeichern, verfügt der Verfassungsschutz des Bundeslandes seit Dezember als erstes geheimdienstliches Organ über eine rechtliche Grundlage für so genannte Online-Durchsuchungen.

Dieses neue Gesetz ermöglicht den Beamten, auf legalem Weg das zu tun, was sonst eher sportlich motivierte Hobby-Hacker, Kleinkriminelle und Wirtschaftsspione tun. Zum Schutz der Verfassung dürfen sie künftig via Internet sozusagen in Computer einbrechen und Festplatten nach nützlichen Informationen durchsuchen.

Andere Institutionen wie das Bundeskriminalamt (BKA) können sich noch nicht auf eine solche Rechtssicherheit berufen, obwohl das im November vom Haushaltsausschuss des Bundestags abgesegnete »Programm zur Stärkung der inneren Sicherheit« die Online-Durchsuchung ebenfalls vorsieht. Im Rahmen dieses Programms werden dem BKA und dem Verfassungsschutz fast 100 Millionen Euro zur Verfügung gestellt. Dabei steht der Ausbau der »Internet Monitoring- und Analysestelle« im Mittelpunkt. Neue Hardware im Wert von 30 Millionen Euro und etwa 50 weitere Computerspezialisten sollen in Zukunft den Behörden ohne physischen Zugriff und unbemerkt Einblick in PCs ermöglichen.

Für das BKA ist das nichts Neues. So gab die Bundesregierung im Dezember auf Anfrage der grünen Bundestagsfraktion bekannt, dass bereits vier Genehmigungsanträge für Online-Durchsuchungen beim Bundesgerichtshof (BGH) eingegangen waren und es nur wegen technischer Probleme noch nicht zum virtuellen Einbruch gekommen sei. Kurz zuvor hatte ein Richter des Bundesgerichtshofs bemerkt, dass der Einbruch in Computer nicht durch die Strafprozessordnung legitimiert ist. Schließlich handelt es sich beim Zugriff auf die heimische Festplatte eines Verdächtigen weder um eine Wohnungsdurchsuchung noch um eine Telefonüberwachung. In diesem Monat soll ein Urteil Klarheit schaffen.

Bis dahin wird der Bundesinnenminister Wolfgang Schäuble (CDU) keine Online-Durchsuchungen anordnen. Dass er, falls nötig, die gesetzlichen Grundlagen dafür schaffen will, verheimlicht er nicht. Denn in der Sache könne es keinen Zweifel geben, »dass wir diese Möglichkeit brauchen«. Das nordrhein-westfälische Modell dürfte ihm dabei als Vorbild dienen, denn die dortigen Verfassungsschützer benötigen für Online-Durchsuchungen keine richterliche Zustimmung, was Ärger mit peniblen Richtern vermeiden hilft.

Der »Internet Monitoring- und Analysestelle« bleibt so lange Zeit, die neue Ermittlungsmethode technisch voranzutreiben. Das Ganze ist nämlich nicht so leicht, wie es gelegentliche Berichte über spektakuläre Einbrüche in Internetserver erscheinen lassen. Die erste Voraussetzung dafür ist, dass der Rechner mit dem Internet verbunden ist. Weiterhin benötigen die Fahnder dessen Internetadresse, die sich gewöhnlich bei jeder Einwahl ändert, dem jeweiligen Internetanbieter aber bekannt ist. Der Aufwand, dort die Adresse eines Verdächtigen zu erfragen, wächst erheblich, falls dieser jedes Mal einen anderen Provider verwendet.

Ist der gesuchte Rechner geortet, fängt die eigentliche Arbeit an. So genannte Remote Exploits – Sicherheitslücken, durch die die Angreifer über das Netz eindringen können – treten zwar immer wieder auf, werden aber mit den Updates der Betriebssysteme meist schnell wieder geschlossen. Zu den Rechnern mit dem am weitesten verbreiteten Betriebssystem, Windows, könnte der Hersteller Microsoft theoretisch Zutritt verschaffen. Das bliebe aber in diesem mit viel Misstrauen beobachteten System nicht lange verborgen und würde den ohnehin angeschlagenen Ruf der Firma in puncto Sicherheit ruinieren. Es ist unwahrscheinlich, dass die Forderung einer einzelnen Regierung das Unternehmen dazu bewegen könnte.

Der Einbrecher braucht also Unterstützung von dem Rechner, auf den er es abgesehen hat. Dazu dienen so genannte Trojaner, die sich auf einem PC einnisten und den Zugriff via Internet möglich machen. Die Referenz an das legendäre Holzpferd verdanken die kleinen Programme dem Umstand, dass der Benutzer sie meist selbst installiert. Das geschieht beispielsweise durch einen unbedarften Klick auf den Anhang einer E-Mail, das Aufsuchen einer entsprechend präparierten Homepage mit einem anfälligen Webbrowser oder den Download eines verlockenden Programms.

Mit Hilfe solcher Trojaner unterstehen weltweit vermutlich zigtausende private PCs der Kontrolle durch Fremde und die Zugriffsmöglichkeiten auf die Computer werden sogar weitervermietet, beispielsweise an Versender von Spam-Mails. Allerdings haben geschäftsorientierte Computerpiraten einen großen Vorteil gegenüber staatlichen Ermittlern: Für sie spielt es keine Rolle, welche Rechner sie kapern, weshalb sie wahllos nach anfälligen PCs stöbern. Dass die Erfolgsquote dabei gering bleibt, stört nicht, denn in absoluten Zahlen erreichen sie dennoch viele Rechner.

Letztlich bleibt den staatlich legalisierten Hackern wohl nur die Entwicklung einer unter dem Namen »Bundestrojaner« durch die Medien geisternden Spionage-Software. Schweizer Behörden erproben bereits ein ähnliches Programm, das, einmal installiert, die Inhalte von Verzeichnissen und über das Internet geführte Telefongespräche protokolliert. Darüber hinaus kann es angeschlossene Webcams und Mikrofone steuern und auf diese Weise einen Raum überwachen. Da die Software nur an Ermittlungsbehörden geliefert wird, erkennen Programme gegen Viren sie nicht. Eine zeitlich festgelegte selbständige Deinstallation macht es zudem schwierig, dem Überwachungsprogramm auf die Spur zu kommen.

Wie aber sollen Ermittler einen solchen Schädling auf einen PC bekommen, dessen System auf dem neuesten Stand ist und dessen Besitzer sich beharrlich weigert, den zugemailten Trojaner anzuklicken oder eine entsprechende Webseite aufzusuchen? Denkbar wäre, ähnlich wie beim Verwanzen eines Raums, den Schädling bei einem heimlichen Einbruch in der Wohnung eines Verdächtigen auf dem PC zu installieren.

Die Mitarbeiter der Firma Kaspersky, einem Hersteller von Software gegen Computerviren, geben sich gelassen: »Es ist nicht das erste und sicher nicht das letzte Mal, dass Behörden mit solchen Infiltrationsmethoden hausieren gehen. Es ist nur eine Frage der Zeit, bis man eines von den Dingern in die Hände bekommt. Danach ist es einfach, diese Malware zu identifizieren.« Im Gegensatz zu ihren illegalen Konkurrenten bleiben den staatlichen Hackern im Falle eines gescheiterten Angriffs aber immer noch die konventionellen Überwachungsmethoden.

Eine absurde Legitimation für den Einbruch in private PCs ohne richterliche Kontrolle lieferte Nordrhein-Westfalens Innenminister Ingo Wolf (FDP): »Wer die Überprüfung von Daten auf Rechnern potenzieller Terroristen für einen Einbruch in den grundgesetzlich geschützten Wohnraum hält, hat das Wesen des Internets nicht verstanden«, hieß es im Oktober in einer Pressemitteilung. Denn »der Nutzer befinde sich weltweit online und verlasse damit bewusst und zielgerichtet die geschützte häusliche Sphäre«.