news 03.08.2007 13:52

"Bundestrojaner" heißt jetzt angeblich "Remote Forensic Software"

Das Bundeskriminalamt (BKA) wirbt weiter für **heimliche Online-Durchsuchungen[1]** und gibt dabei an, die Schnüffelsoftware hauptsächlich physisch nach dem Eindringen in die Wohnung Verdächtiger installieren zu wollen. Im Endeffekt soll es sich bei dem Programm laut jüngsten Verlautbarungen der Wiesbadener Polizeibehörde um einen aufgebohrten, mit einer Spyware-Komponente ausgerüsteten Keylogger handeln. Mit einer solchen Überwachungswanze, die von Ermittlern heimlich direkt auf Zielcomputern installiert wird, lassen sich unter anderem die Tastatureingaben für Passwörter, Login-Daten und PINs vor einer möglichen Verschlüsselung von Informationen aufzeichnen. Davon erhofft sich das BKA, alle Zugangsdaten für genutzte Dienste per Fernübertragung frei Haus geliefert zu bekommen.

Im Gegensatz zum FBI, das in der Entwicklung eines "Bundestrojaners" laut US-Medienberichten anscheinend schon weiter ist als das BKA und echte Online-Durchsuchungen mit dem **Werkzeug "CIPAV" (Computer Internet Protokoll Address Verifier)[2]** durchführt, bevorzugen die Wiesbadener Ermittler laut einem **Bericht[3]** des Computermagazins Chip das traditionelle, "robuste Agenten-Handwerk". Demnach soll die "Remote Forensic Software" (RFS) getaufte Schnüffelapplikation in der Regel **nicht online[4]** auf den Zielrechner etwa mit einer E-Mail, einer manipulierten Website oder Huckepack über normale Downloads im Internet aufgespielt werden. Die Erfolgsaussichten dieser Methode schätzt das BKA als noch zu schlecht ein, sodass es den weniger unauffälligen direkten Zugang zu den Wohnräumen Verdächtiger in den Vordergrund rückt. In diesem Sinne hatte sich BKA-Chef Ziercke **bereits auf einem Symposium Mitte Juli geäußert[5]** und betont, das BKA entwickele keine Schadsoftware oder Software mit eigenen Verbreitungsroutinen.

Konkret soll sich nach "Umfeld-Analysen" mit Hilfe verdeckter Ermittler ein BKA-Team heimlich in die vier Wände einer zu überwachenden Person vorarbeiten, dort zunächst Kopien von allen zu findenden Festplatten ziehen und die Daten analysieren. Wie BKA-Präsident Jörg Ziercke **bereits wiederholt[6] ankündigte[7]**, werde daraufhin gleichsam in Einzelanfertigung die RFS gebastelt und direkt auf das Zielsystem zugeschnitten. Im Rahmen einer erneuten "Wohnungsöffnung" soll das modulare Überwachungsprogramm dann auf dem bereits in Grundzügen ausgeforschten PC installiert werden. Dies habe den Vorteil, auch gleich dort bereits installierte Sicherheitssoftware wie Firewalls neu einzustellen. Damit soll verhindert werden, dass diese beim "Nach-Hause-Telefonieren" der Schnüffelsoftware Alarm schlägt. Warum das BKA aber plötzlich heimlich in Wohnungen eindringen darf und wie bei der beschriebenen Vorgehen der spätestens nach dem **Bundesverfassungsgerichtsurteil zum Großen Lauschangriff[8]** der absolut geschützte Kernbereich privater Lebensgestaltung ausgespart werden soll, bleibt auch nach den jüngsten Äußerungen aus dem BKA unklar.

Mit dem hohen Aufwand will das BKA jedenfalls sicherstellen, dass es im günstigsten Fall nicht auf staatlich verordnete Sicherheitslücken oder die Zusammenarbeit mit Herstellern von Sicherheitssoftware oder Betriebssystemen angewiesen ist – ohne aber die Installation des Trojaners bei Verdächtigen über das Netz ausschließen zu wollen. Die Anbieter von Sicherheitssoftware hatten allerdings wiederholt darauf hingewiesen, heimliche Zugriffe der Polizeibehörde zur Durchsuchung von Computern über das Internet mit ihren Schutzprogrammen zu blockieren. "Im Interesse unserer Kunden weltweit gewähren wir keinen Institutionen Zugang zu Kundencomputern", betonte Andreas Zeitler, Geschäftsführer des Unternehmens Symantec Deutschland, gerade noch einmal in der ***Süddeutschen Zeitung*[9]**. "Unsere Software wird also auch im Fall eines so genannten Bundestrojaners den Trojaner stoppen und entfernen." Auch der

Geschäftsführer der Firma Kaspersky Lab, Andreas Lamm, erklärte, dass ein Spionageprogramm des BKA "vermutlich erkannt werden würde".

Andreas Pfitzmann, Informatikprofessor an der Technischen Universität Dresden, riet Richtern, die Echtheit der von staatlichen Schnüffelprogrammen übertragenen Daten anzuzweifeln. "Wenn ein Bundestrojaner auf dem Rechner läuft, verändert er automatisch das System, welches er untersucht", sagte der Experte. "Das widerspricht allen Gepflogenheit der Forensik und schwächt die Glaubwürdigkeit der gesammelten Daten." Zudem würden Kriminelle häufig fremde Rechner kapern und als Zwischenspeicher für illegale Dateien wie Kinderpornografie verwenden. Cracker oder Cyberkriminelle würden verbotene Daten nicht auf ihrem eigenen Rechner speichern, betonte Pfitzmann. Tatsächlich würde die Installation der "RFS" rasch an ihre Grenzen stoßen, wenn terroristische "Gefährder" von ihnen als schutzwürdig erachtete Dateien etwa auf verschlüsselten USB-Sticks lagern und für die Kommunikation Rechner in Internet-Cafés verwenden. Darüber hinaus lasse das geplante Vorgehen weiter offen, wie der Kernbereich der privaten Lebensgestaltung beim Kopieren der Festplatten und der Anwendung des Spionagewerkzeugs außen vor gehalten werden sollte.

In der großen Koalition geht der Streit um Online-Razzien derweil weiter. Die SPD im baden-württembergischen Landtag gab bekannt, die umstrittenen Netzbespitzelungen strikt abzulehnen. Zum Vorschlag der CDU, dieses Fahndungsmittel in das **Landespolizeigesetz aufzunehmen[10]**, sagte der SPD-Abgeordnete Rainer Stickelberger am Freitag in Stuttgart laut dpa, Freiheitsrechte dürften nicht im Namen der Sicherheit zu Tode geschützt werden. Der parlamentarische Geschäftsführer der SPD-Fraktion, Reinhold Gall, warf der CDU im Land vor, "Erfüllungsgehilfe" von Bundesinnenminister Wolfgang Schäuble (CDU) zu sein. Dieser fordert schon seit Monaten, der Polizei verdeckte Ermittlungen auf fremden Computern über das Internet zu ermöglichen.

Auf Bundesebene brach die CDU-Innenpolitikerin Beatrix Philipp eine Lanze für heimliche Online-Durchsuchungen. "Ich verstehe nicht, dass die Bürger dem Staat weniger trauen als Aldi, Plus und Metro, denen sie bedenkenlos sämtliche Daten geben", sagte sie der ***Rheinischen Post*****[11]**. Der SPD-Rechtspolitiker Lothar Binding äußerte sich dagegen auf der Plattform **Abgeordnetenwatch[12]** skeptisch: "Oft zeigen mir bestimmte Ideen hinsichtlich der Überwachung von (privaten) Rechnern, welcher Ideengeber von Rechnern, Netzen, Verschlüsselung, Datenschutz und Datensicherheit nicht genug versteht", kritisierte er Schäuble und seine Unterstützer. Auch die jüngsten Ideen über den Einsatz von Keystroke-Loggern "würden wenigstens einmal mehr als eine Online-Verbindung zu meinem PC erfordern. Herr Schäuble müsste schon vorbei kommen". Die rechtskonforme beziehungsweise verfassungsfeste Begründung zur Ausspionierung auch persönlicher Identifikations-Nummern und Passwörter möchte Binding zudem "gern mal sehen".

Die heimliche Online-Durchsuchung von Computern stößt bei vielen Datenschützern und Juristen auf Skepsis. Sie melden grundsätzliche Bedenken an und warnen vor eventuell angestrebten Grundgesetzänderungen. Siehe dazu:

- **Ist die Online-Durchsuchung wirklich notwendig?[13]**
- **Ist die Festplatte eine Wohnung?[14]**
- **Skeptische Stimmen zur Online-Durchsuchung[15]**

Zu den Auseinandersetzungen um die erweiterte Anti-Terror-Gesetzgebung, die Anti-Terror-Datei sowie die Online-Durchsuchung siehe auch:

- **Von der Anti-Terror-Gesetzgebung über die Anti-Terror-Datei zum "Schäuble-Katalog"[16]**

(*Stefan Krempl*) **/**

(**jk[17]**/c't) (jk/c't)

URL dieses Artikels:
http://www.heise.de/newsticker/meldung/93807

Links in diesem Artikel:
[1] http://www.heise.de/newsticker/meldung/93746
[2] http://www.heise.de/newsticker/meldung/92914
[3] http://www.focus.de/digital/computer/chip-exklusiv/chip-exklusiv_aid_68603.html
[4] http://www.heise.de/security/artikel/86415/
[5] http://www.heise.de/newsticker/meldung/92578
[6] http://www.heise.de/newsticker/meldung/87421
[7] http://www.heise.de/newsticker/meldung/87132
[8] http://www.heise.de/ct/hintergrund/meldung/45223
[9] http://www.sueddeutsche.de
[10] http://www.heise.de/newsticker/meldung/93708
[11] http://www.rp-online.de/public/article/regional/duesseldorf/duesseldorf-stadt/nachrichten/465106
[12] http://www.abgeordnetenwatch.de/lothar_binding-650-5620--p475.html
[13] http://www.heise.de/newsticker/meldung/93395
[14] http://www.heise.de/newsticker/meldung/93307
[15] http://www.heise.de/newsticker/meldung/93226
[16] http://www.heise.de/ct/hintergrund/meldung/85995
[17] mailto:jk@ct.heise.de
