idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Technische Universität Darmstadt
Jörg Feuck

12.11.2007
http://idw-online.de/de/news234832

Forschungs- / Wissenstransfer, Forschungsergebnisse
Gesellschaft, Informationstechnik, Politik, Recht
überregional

"Der 'Bundestrojaner' ist teuer und kann ausgetrickst werden"

Online-Durchsuchungen im Visier - Interview mit Prof. Johannes Buchmann Darmstadt, 12.11.07. Die Deutschen diskutieren derzeit heftig über die von Bundesinnenminister Wolfgang Schäuble angeregten Online-Durchsuchungen, mit denen Daten von privaten PCs verdächtiger Zielpersonen dem BKA zugänglich gemacht werden sollen. Die dazu notwendige Software kursiert im Volksmund als "Bundestrojaner". Doch wie so ein Trojaner à la Schäuble funktionieren soll, was finanziell und technisch überhaupt machbar ist, wissen die wenigsten.

Prof. Johannes Buchmann ist Leiter des Fachgebiets Theoretische Informatik der TU Darmstadt. Forschungsschwerpunkte Buchmanns und seiner Mitarbeiter sind ! Kryptographie und Informationssicherheit.

? Herr Prof. Buchmann, was steckt eigentlich hinter dem Begriff Trojaner?

! Ein Trojaner, genauer gesagt ein Trojanisches Pferd, ist ein Computerprogramm, das wie das hölzerne Pferd aus der griechischen Mythologie einen Nutzen vortäuscht, in Wahrheit aber im Hintergrund und ohne Wissen des PC-Besitzers eine ganz andere Funktion erfüllt. Auch der so genannte Bundestrojaner ist ein solches "Schadprogramm", das private PCs manipuliert. Trojaner werden zum Beispiel benutzt, um persönliche Daten oder Passwörter auszuspähen, um den Anwender auf bestimmte Webseiten im Internet umzuleiten oder auch den Rechner zu kriminellen Zwecken fernzusteuern.

? Wie soll so ein Programm überhaupt eingeschleust werden?

! Wie die Software, die übrigens offiziell Remote Forensic Software (RFS) heißt, auf den PC installiert werden soll, hängt laut Innenministerium von dem Nutzungsverhalten der Zielperson ab: in Anhängen von E-Mails, über herumliegende CDs beziehungsweise USB-Sticks oder auch unter Ausnutzung von automatischen Updates oder Sicherheitslücken der aufgespielten Software.

? Was genau soll ein Bundestrojaner herausbekommen?

! Wie mit allen Trojanern will die Bundesregierung mit RFS Daten einsehen oder auch Passwörter ausspionieren. Das geschieht zum einen, indem ausgesuchte Dateien kopiert und an das BKA geschickt werden. Passwörter werden mit einer Technik ausspioniert, die sich Keylogger nennt und bei der die Tasteneingaben "abgehört" werden. Was das Aussuchen der Dateien betrifft, müssen aber zunächst einmal Kriterien herausgearbeitet werden, die die gesuchten Informationen am wahrscheinlichsten umreißen. Schon diese Aufgabe ist nicht einfach zu bewältigen.

? Ist ein Trojaner, wie ihn Schäuble fordert, überhaupt realisierbar?

! Den einen Bundestrojaner wird es ohnehin nicht geben. Um einen Trojaner auf einen spezifischen PC einzuschleusen, muss bekannt sein, welche Hardware existiert, welches Betriebssystem läuft und welche Virenschutzprogramme. Ohne die Software und deren genutzte Versionen zu kennen, können die BKA-Mitarbeiter natürlich nicht wissen, welche Sicherheitslücken vorliegen und wie sie sie umgehen können. Entsprechend müssen sie zuallererst das System ausspionieren, erst darauf hin kann ein Trojaner für diesen einzelnen Computer programmiert werden. Das kostet natürlich Zeit und Geld.

? Wie es aussieht, werden die Betreiber von Antivirenprogrammen die Zusammenarbeit mit der Bundesregierung verweigern und keine eigenen Sicherheitslücken schaffen. Neue Viren bzw. Trojaner werden also sehr schnell erfasst werden.

! Das ist richtig. Deshalb ist ein Trojaner, wie Schäuble ihn möchte, auch nur für den einmaligen Gebrauch bestimmt, ein Wegwerfprodukt sozusagen. Dafür sorgen schon Programme wie Windows von Microsoft, das sich ja auch ständig automatisch updatet. Damit wiederum werden alte Sicherheitslücken womöglich gekittet und neue Lücken müssen gefunden werden.

? Ist es überhaupt möglich, einen PC zu durchsuchen, ohne dass sein Nutzer etwas davon bemerkt?

! Das hängt davon ab, wie viele Daten kopiert und verschickt werden sollen und über welchen Stand der Technik der observierte Nutzer verfügt. Wenn er noch mit einem Modem arbeitet, ist es praktisch nicht möglich, denn die Übertragungsgeschwindigkeit ist viel zu niedrig.

? Wenn nach Durchsuchung der Festplatte zum Beispiel sieben verdächtige Dateien ausgewählt wurden, von denen vielleicht eine noch ein Bild enthält, ist man schon bei 20 Megabyte Datenumfang. Selbst bei einer Hochgeschwindigkeitsverbindung, sagen wir einmal DSL 1000, würde man 20 Minuten benötigen, um diese Daten zum Steuerrechner des BKA zu transferieren. Damit der Nutzer nichts von alledem bemerkt, muss das Internet in dieser Zeit bei gleicher Geschwindigkeit störungsfrei weiterlaufen. Somit kann die Übertragung durchaus auch zwei Stunden dauern. Die Datenmenge ist auch beim Mitschneiden der Tastaturbetätigungen der limitierende Faktor.

? Können potenzielle Zielpersonen den Bundestrojaner umgehen?

! Das ist an sich kein Problem. Denn ein Trojaner kann nur dort angreifen, wo eine Verbindung zum Internet besteht. Wenn man seine Daten auf einem mit dem Internet verbundenen PC verschlüsselt empfängt, kann man sie auf einen USB-Stick übertragen und erst auf einem zweiten PC, einem Offline-PC ohne Internet-Verbindung, entschlüsseln. Auf dem ans Netzwerk angeschlossenen PC kann man dann die Daten löschen. Allerdings muss man sie komplett löschen, also auch die Version, die zunächst einmal im Papierkorb landet.

? Welche Möglichkeiten gibt es, Telefongespäche über das Internet abzuhören?

! Das ist derzeit offensichtlich noch nicht möglich. Skype etwa - der bekannteste Anbieter von VoIP-Telefonie - verschlüsselt die Audio-Daten, die also abgegriffen werden müssten, bevor sie von der Verschlüsselungssoftware bearbeitet werden. Das heißt, es muss einer der beiden beteiligten Rechner angezapft werden. Dafür wiederum ist eine weitere Anwendung notwendig, die es anscheinend noch nicht gibt.

? Gibt es in anderen Ländern vergleichbare Regierungs-Initiativen?

! In den USA ist im vergangenen Juli erstmals von einer heimlichen Online-Durchsuchung berichtet worden. Das FBI hat eine Spyware namens CIPAV eingesetzt. Damit ist es ihm gelungen, die Identität eines ehemaligen Schülers einer Timberland High School zu ermitteln, der seiner früheren Schule mehrfach Bombendrohungen geschickt hatte. Im

Gegensatz zu den geplanten Online-Durchsuchungen in Deutschland wurden allerdings nicht die Inhalte der Kommunikation übermittelt. Das hat das FBI mehrfach und eidesstattlich versichert. Heimlich an Computern installierte Keylogger werden in den USA aber schon länger eingesetzt.

gek/he

URL zur Pressemitteilung: http://www.cast-forum.de/home - Workshops zur Informationssicherheit