

BCC Netzwelt

Das Journal für IP und Netzwerke

Herausgeber: BCC Business Communication Company GmbH

November 2007

Staatliche Online-Durchsuchung

Der Bundestrojaner – Fluch oder Segen?

Ein Aufschrei der Empörung geht durch die deutsche Medienlandschaft, Daten- und Verfassungsschützer schlagen Alarm: Das Bundeskriminalamt (BKA) hat einen Computer-Trojaner entwickelt, der Rechner aus der Ferne durchsuchen und sogar Mobilgeräte wie Handys, Smartphones und Blackberrys ausspionieren kann. Damit sollen Ermittler per E-Mail und unter Angabe eines falschen behördlichen Absenders Spähprogramme auf die PCs von Verdächtigen einschleusen, wo sie dann selbstständig sensible Informationen abgreifen könnten. Bundesinnenminister Wolfgang Schäuble (CDU) sieht darin eine wichtige Maßnahme zum Schutz der inneren Sicherheit und eine wirksame Waffe im Anti-Terrorkampf. Noch entbehrt sie allerdings der rechtlichen Grundlage.



In Deutschland wurden bereits 2005, unter dem damaligen Minister Otto Schily (SPD), Online-Durchsuchungen eingesetzt. Standard war bisher, dass BKA-Beamte in die Wohnung eines Verdächtigen eindringen, dessen IT-Ausstattung analysierten und Spähprogramme installierten, die ihre Erkenntnisse unbemerkt an das BKA übermittelten. Durch den Bundestrojaner hat die Diskussion um Online-Überwachungen eine neue Dimension erhalten. Anfang des Jahres wurden sie vom Bundesgerichtshof untersagt, im April wurde ein Entwicklungsstopp für Remote Forensic Software (RFS), unter die der Trojaner fällt, verhängt. Die politische Debatte zum Thema geht unterdessen mit unverminderter Heftigkeit weiter und erhielt in den letzten Wochen durch die Verhaftung mutmaßlicher Terror-Attentäter zusätzliche Brisanz.

Eingriff in die Privatsphäre

Der Einsatz des Bundestrojaners ist politisch und verfassungsrechtlich stark umstritten. Datenschützer und Juristen sehen den Schutz des Kernbereichs der privaten Lebensgestaltung gefährdet. Vorab definierte Suchkriterien sollen zwar Kernbereichsschutz garantieren, doch halten Kritiker diese für realitätsfern. Sie sehen in Online-Überwachungen einen Meilenstein auf dem Weg zum Überwachungsstaat – auch wenn der Einsatz des Bundestrojaners zunächst nur in Einzelfällen geplant ist. Der Online-„Lauschangriff“ bezieht sich

dabei nicht nur auf private Rechner. Personenbezogene Daten sollen auch aus den Datenbeständen von Unternehmen erhoben und gespeichert werden dürfen, um sie dann erkennungsdienstlichen Untersuchungen zu unterziehen.

Staatlich verordnete Hintertüren?

Auch im technischen Bereich gibt es viele offene Fragen: Die meisten Unternehmen verfügen heutzutage über leistungsfähige Firewalls oder Virenschutz-Systeme. Eine Umfrage unter Herstellern moderner Virens Scanner ergab, dass sie ihren Produkten durchaus zutrauen, Spyware wie den Bundestrojaner aufzuspüren. Die Lösung des Dilemmas wäre eine staatlich verordnete Sicherheitslücke in Anti-Viren-Programmen. Doch Software-Hersteller lehnen eine Zusammenarbeit mit den Behörden bei Online-Durchsuchungen entschieden ab. Praktisch wäre das auch kaum durchführbar. Selbst wenn man in die deutschen Varianten eines Sicherheitspaketes eine Hintertür für den Bundestrojaner durchsetzen würde, gäbe es eine solche Lücke in anderen Ländern nicht. Deutsche Internet-Kriminelle könnten sich die US-Version eines Produktes kaufen und wären wieder geschützt. Zudem ist es international tätigen Anbietern nicht zumutbar, die für die jeweiligen Länder spezifischen Trojaner von der Erkennung auszuschließen. Im Allgemeinen ist zu befürchten, dass bewusste Lücken in Sicherheitssystemen

nicht nur Regierungstrojanern, sondern auch der internationalen Industriespionage und allerlei verbrecherischen Trittbrettfahrern Tür und Tor öffnen würden. Die Computerbranche befürchtet einen generellen Vertrauensverlust in die allgemeine IT-Sicherheit. Zudem untergräbt die Ankündigung des BKA, unter falschem Behördenabsender Spyware zu verbreiten, das öffentliche Vertrauen in die Behörden.

Risiko für die Systemsicherheit

Ein spezielles juristisches Problem liegt darin, dass die Echtheit elektronischer Daten gerichtlich angezweifelt werden kann. Ist der Späh-Trojaner erst einmal entdeckt, besteht die Möglichkeit, ihm gefälschte Beweismittel unterzujubeln. Er kann sogar genutzt werden, um den Rechner der Ermittler zu infiltrieren. Experten fürchten, dass die Applikation selbst zum Risiko für die Systemsicherheit wird, wenn Sicherheitslücken zum Einfallstor für Verbrecher werden, die den Bundestrojaner ihrerseits zum Datendiebstahl und -missbrauch nutzen könnten. Angesichts der vielfältigen Probleme und Fragen, die der Einsatz des Bundestrojaners aufwirft, werden auch dem prinzipiellen Befürworter von Online-Überwachungen Zweifel kommen, ob der Bundestrojaner in Bezug auf seine Einsatzbereitschaft, Verfassungskonformität und Tarnung im Einsatz wirklich schon ausgereift ist oder vielmehr noch großen Nachbesserungsbedarf aufzuweisen hat. ■ nr

Editorial

Liebe Leserin, lieber Leser,

wie weit darf der Schutz von Menschen und Leben gehen? Wie viel Sicherheit muss der Staat dabei bieten? Wovon will und muss er seine Bürger schützen?

Die EU will Behörden ermöglichen, im umfangreichen Maß Daten von Fluggästen zu sammeln. Außerdem will sie ein zentrales Register, in dem die Reisebewegungen von Nicht-EU-Bürgern gespeichert werden. Andererseits hat sie jüngst das Strafrecht für das Eindringen in fremde Computer und Netzwerke verschärft. Meint Schutz die totale Überwachung – Big Brother lässt grüßen – oder auch den sorgsamsten Umgang mit dem Bürgerrecht Datenschutz? Der „Bundestrojaner“ wird in Politik und Medien heiß diskutiert. Bis jetzt bleibt jedoch vor allem eine Frage offen: Wie sicher ist in puncto Online-Durchsuchung ein Missbrauch auszuschließen? Unser Leitartikel benennt, welche Probleme IT-Experten mit den staatlichen Spähprogrammen haben, denn vor allem technische Argumente sprechen gegen den Einsatz des Bundestrojaners.

Doch wie sieht es mit der Rechtsstaatlichkeit aus? Beim „großen Lauschangriff“ sprach das Bundesverfassungsgericht von einem „absolut geschützten Kernbereich des Privaten“. Wir dürfen gespannt darauf sein, wie dieses Gericht den PC und die darauf gespeicherten Daten einordnet.

Mit kriminellen Energien der ganz anderen Art befasst sich unser Artikel zum Thema Grauimporte auf Seite drei. Gefälschte und minderwertige Netzwerk-Hardware verursacht immer wieder Probleme in Unternehmensnetzen. Was auf den ersten Blick wie ein unschlagbares Schnäppchen aussieht, entpuppt sich im Nachgang oft als Bumerang. Wir geben Tipps, wie Sie auf Nummer sicher gehen und „faule Eier“ rechtzeitig erkennen.

Zum Abschluss ein Hinweis in eigener Sache: Ab sofort beinhaltet die BCC Netzwelt regelmäßig eine Beilage mit Netzwerkkomponenten für konvergente Kommunikationsplattformen: zu fairen Konditionen und selbstverständlich mit Herstellerservice bzw. Garantie. Zu beziehen sind diese Produkte über den neuen BCC Online-Shop. Bei Fragen zögern Sie nicht – rufen Sie uns an. Unsere Mitarbeiter in unserem Kontakt-Center helfen Ihnen gern.

Herzlichst,

Ihre Angelika Levak

Inhalt

Seite 1.....

- Staatliche Online-Durchsuchung
Der Bundestrojaner – Fluch oder Segen?

■ Editorial

Seite 2.....

- Mammographie-Screening
Zuverlässiges Netz gewährleistet
Vorsorge-Qualität
- Customer Service
Rundum gut betreut

Seite 3.....

- Dubiose Grauimporte
Preisvorteil in der Praxis schnell
hinfällig
- Cisco TelePresence
Virtuelle Konferenzen in neuer
Dimension

Seite 4.....

- Note
GEZ-Pflicht für Computer
BCC ist Cisco-Gold-Partner
IT-Bedarf im öffentlichen Sektor
wächst
DSL-Boom ungebrochen
- Kanalbündelung
Die richtige Balance finden
- Garantierte Bandbreiten,
höhere Qualität
IP-Telefonie mit hoch verfügbarem
DSL
- Kurz != Giga günstig
Ausblick
Impressum

Beachten Sie unsere Shop-Beilage

Jeden Monat neu: Netzwerknähe
Hardware-Angebote aus unserem
Internetshop zu Top-Konditionen.

