++
Online-Durchsuchung . . . Bundestronjaner - JA oder NEIN ?
++

Nach wie vor ist der Bundestrojaner in der Politik heftig umstritten, innerhalb des Parlaments, der Koalition und der Parteien selbst.

ein Hintergrundbericht von Bernhard Münkel

Ein Donnerschlag ging am fünften Februar dieses Jahres durch die Republik. Der dritte Senat des Bundesgerichtshofes (BGH) in Karlsruhe hatte in einem Aufsehen erregenden Urteil entschieden, dass die heimliche Online-Durchsuchung von heimischen Computern nicht mit gängigen Gesetzen gedeckt sei. Mit lapidaren Worten teilte das Gericht mit: "Die heimliche Durchsuchung der im Computer eines Beschuldigten gespeicherten Dateien mit Hilfe eines Programms, das ohne Wissen des Betroffenen aufgespielt wurde (verdeckte Online-Durchsuchung), ist nach der Strafprozessordnung unzulässig. Es fehlt an der für einen solchen Eingriff erforderlichen Ermächtigungsgrundlage."

Seit diesem Tag wird aller Orten erbittert gestritten, ob sich das Ausforschen von Computern mit dem Grundgesetz vereinbaren ließe. Denn so wurde das Urteil vielfach verstanden: Der Eingriff verletze den Artikel 13 des Grundgesetzes über die Unverletzlichkeit der Privatsphäre und stelle außerdem einen Eingriff in die informationelle Selbstbestimmung dar.

Dabei hatte der Bundesgerichtshof nur über eine Beschwerde der Generalbundesanwältin Monika Harms entschieden. Diese hatte gegen einen Beschluss protestiert, in dem der Ermittlungsrichter des Bundesgerichtshofs, Ulrich Hebenstreit, im November 2006 einen Antrag auf verdeckte Online-Durchsuchung für rechtswidrig erklärt hatte. Die Entscheidung des Ermittlungsrichterswar dabei nicht die erste ihrer Art. Bereits drei andere Ermittlungsrichter hatten zuvor Online-Durchsuchungen in zwei Fällen stattgegeben.

Fast zeitgleich stellte im November 2006 die Partei "Die Linke" im Bundestag eine kleine Anfrage an die Bundesregierung. Inhalt der Anfrage war jene Beschwerde vor dem Bundesgerichtshof. Die Abgeordneten waren bereitsWochen zuvor über einen Passus gestolpert, der im "Programm zu Stärkung der Inneren Sicherheit" (PSIS) genannt wurde. Dort sollte "die technische Fähigkeit, entfernte PCs auf verfahrensrelevante Inhalte hin durchsuchen zu können, ohne selbst am Standort des Geräts anwesend zu sein" mit insgesamt 200 000 Euro ermöglicht werden.

Das Ergebnis war erschütternd. In ihrer Antwort am 22. Dezember 2006 musste die Bundesregierung einräumen: "Derzeit werden im Rahmen eines Projektes beim Bundeskriminalamt die technischen Voraussetzungen zur Umsetzung einer solchen Maßnahme entwickelt." An anderer Stelle heißt es dann: "Der Bundesregierung liegen keine Erkenntnisse über in Ermittlungsverfahren durchgeführte Online-Durchsuchungen vor. Ihr sind lediglich die folgenden vier gerichtlichen Entscheidungen bekannt, die Online-Durchsuchungen zum Gegenstand haben: [...]" Das aber war nur die halbe Wahrheit, denn genau jene Gerichtsentscheidungen belegten, dass Online-Durchsuchungen in Ermittlungsverfahren bereits eingesetzt wurden.

Die ganze Wahrheit zeigte sich wenige Wochen später: Das Innenministerium räumte im April ein, dass der Verfassungsschutz bereits seit 2005 heimlich Computer durchsucht hatte. Der damalige Innenminister Otto Schily hatte dem verantwortlichen Beamten Lutz Diwell die Zustimmung erteilt.

BKA und Verfassungsschutz sollen in dieser Zeit in weniger als zwölf Fällen auf Privatcomputer zugegriffen haben, hieß es anfangs. Mittlerweile gilt es als gesichert, dass das BKA bei zehn Versuchen zweimal Erfolg hatte - waren es vielleicht genau jene zwei Male, auf die sich die vier Gerichtsentscheidungen bezogen? Auch verschiedene Verfassungsschutz-Organe sollen insgesamt zehn Versuche gestartet haben. Mit welchem Erfolg, ist nicht bekannt.

Das alles geschah ohne eine gesetzliche Grundlage. Seit Anfang dieses Jahres ist das anders. In Nordrhein-Westfalen darf der Verfassungsschutz bereits seit Januar Computer online durchsuchen. Dagegen hat Frederik Roggan, Vorsitzender der Bürgerrechtsorganisation Humanistischen Union, Verfassungsbeschwerde eingelegt. Wann das Urteil ergehen und wie es ausfallen wird, weiß niemand mit Bestimmtheit zu sagen.

"Ein Trojaner ist ein Trojaner"

Randy Abrams ist Security Technology Editor bei Eset, ein Anbieter von Antiviren- Software. Er hat vorher 13 Jahre bei Microsoft gearbeitet. Bernhard Münkel sprach mit ihm.

Redaktion: Glauben Sie, dass RFS (Remote Forensic Software) ein guter und sicherer Weg ist, Kriminelle zu überlisten?

R. Abrams: RFS kann eine gute Methode sein, den einen oder andere Kriminellen zu erwischen. Je nachdem, wie es entworfen und benutzt wird, entscheidet sich, wie sicher es ist.

Redaktion: Wie, glauben Sie, kann ein RFS funktionieren?

R. Abrams: Es gibt verschiedene Wege, RFS zu benutzen. Der einfachste Weg wird sein, einen Standard- Trojaner zu nehmen, wie er im Internet zu kaufen ist, und ihn RFS zu nennen.

Die Tastaturanschläge abzufangen ist eine Methode. "Social Engineering"-Methoden, also den Anwender zu überlisten, kann manchmal viel bessere Ergebnisse für dasselbe Problem erzielen.

Redaktion: Wie wird die Antiviren-Industrie reagieren, wenn ihnen so eine Technologie bekannt wird?

R. Abrams: Ein Trojaner ist ein Trojaner! Wenn wir einen Trojaner finden, den wir bis dahin nicht entdeckten, werden wir ihn in Zukunft entdecken und nach Wegen suchen, unsere Heuristik besser zu machen als vorher.

Redaktion: Wie werden Sie reagieren, wenn Sie von einer Regierung angesprochen werden, zu kooperieren?

R. Abrams: Warum sollte eine Regierung einen Hersteller von Antiviren-Software ansprechen? Das würde die ganze Operation in Gefahr bringen. Eine verdeckte Spionageaktion setzt voraus, dass die Informationen sehr wenig gestreut werden. Sollte eine Regierung einen Antiviren-Hersteller ansprechen, müsste sie die Schadensroutinen vorzeigen. Dann würden verschiedene Angestellte des Herstellers diese Schadensroutine und ihre Funktion zu sehen bekommen.

Redaktion: RFS würde wahrscheinlich verschiedene Arten der Malware auf einem PC installieren. Würde das nicht sehr schnell von den heuristischen Techniken eines guten Antiviren-Scanners entdeckt?

R. Abrams: Ein Trojaner, der viele verschiedene Arten von Malware benutzt, ist eine Hollywood-Vorstellung. Komplexität birgt immer Risiken. Für RFS heißt das, möglich wenig Aufsehen zu erregen, während man den Job macht. Antiviren-Produkte mit sehr guter Heuristik erschweren die Aufgabe, unter dem Radar durchzufliegen, machen sie aber nicht unmöglich. Diejenigen, die RFS einsetzen, kennen ihr Opfer bereits gut. Wenn sie wissen, welche Antiviren-Produkte die Person nutzt, wissen sie auch, wen sie überlisten müssen.

Das FBI zu Gast

Auch beim FBI in den USA gibt es einen Trojaner, der erfolgreich eingesetzt wurde.

Der Schreck sitzt tief im Gedächtnis der amerikanischen Öffentlichkeit. Das Massaker an der technischen Universität Virginia, bei dem der ehemalige Student Seung-Hui Cho 32 Schüler erschoss, bevor er sich selbst tötete, war das letzte in einer Reihe von Attentaten an einer Bildungseinrichtung in den USA.

So ein schreckliches Ereignis darf nie wieder passieren, ist die einhellige Meinung in den USA. Deshalb wird umgehend das FBI eingeschaltet, als ein Unbekannter am 30. Mai die Timberlane High Scholl in Lacey, Washington, mit einem Bombenattentat bedroht.

Wenige Tage später wiederholt der potenzielle Attentäter seine Drohung via E-Mail - und fühlt sich scheinbar besonders sicher. Denn er geht dabei versiert zur Sache. "Doug Briggs" alias "Timberlanebombinfo" legt einen Account auf Myspace.com an, besorgt sich fünf E-Mail-Accounts bei Google-Mail und hackt mindestens drei italienische Server, um seine Spuren zu verwischen. Über diese schickt er weitere Drohbriefe an die Schule, in denen er sich sogar damit brüstet, seine Spuren verwischt zu haben. Gleichzeitig macht er kräftig Werbung für das bevorstehende Attentat auf seinem Myspace-Profil "Timberlanebombinfo" und via Instant Messaging.

IPAV - ein FBI-Trojaner

Dieser Account soll ihm aber zum Verhängnis werden. Denn offenbar wurde der FBITrojaner CIPAV (Computer and Internet Protocol Address Verifier) über diesen Weg auf dem Computer des Verdächtigen platziert. In seit Kurzem zur Verfügung stehenden Unterlagen spricht das FBI lediglich davon, dass CIPAV "...through an electronic messaging program from an account controlled by the FBI..." installiert wurde.

CIPAV meldet nach der Installation auf dem Zielrechner alle IP-Adressen, die MAC-Adresse, und " weitere sensitive Information" wie Internetverbindungen und Websiteabrufe an einen Server des FBI.

Anders als hierzulande mit dem "Bundestrojaner" geplant, übermittelte CIPAV aber keine Kommunikations- oder Datei-Inhalte an die Server der Polizei. Im Vergleich zur geplanten Online-Durchsuchung und ähnlichen Maßnahmen dient die behördliche Spyware in diesem Fall lediglich zur Feststellung der Benutzer- und IP-Daten.

Der "FBI-Trojaner" leistete ganze Arbeit. Binnen weniger Tage kann das FBI mit Hilfe von CIPAV über die IP-Nummer seines Rechners die Identität eines ehemaligen Schülers der Timberlane High School ermitteln. Damit dürfte "Timberlanebombinfo" um ein paar Jahre in Freiheit ärmer sein - und das FBI um eine Erfolgsgeschichte reicher.

Kommissar Trojaner

Es vergeht keine Woche, in der nicht neue Positionen und Erkenntnisse über den Einsatz des Bundestrojaners (offiziell Remote Forensic Software, RFS) bekannt werden. Was davon Mythos und was Wirklichkeit ist, ist kaum noch auseinander zu halten. Immerhin hat das Wort Online-Überwachung bei zahlreichen Politikern verschiedenste Assoziationen hervorgerufen. Viele sehen darin lediglich eine Methode von Polizei und Geheimdiensten, verdächtige Personen dabei zu beobachten, welche Webseiten sie besuchen oder welche Dateien sie herunterladen, ähnlich der amerikanischen Variante. Nach Angaben des BKA soll der Kommissar Trojaner jedoch weit mehr können.

In einen Fragebogen des Bundesjustizministeriums im August wurde bekannt, was das BKA gerne von dem überwachten Rechnersystem erfahren würde:

"Bei der Online-Durchsicht soll der Status Quo ermittelt werden ("Was hat die Zielperson bezogen auf ihr Informationssystem/ihren Rechner in der Vergangenheit gemacht?"). Bei der Online-Überwachung sollen über einen gesetzlich festgelegten Zeitraum die Aktivitäten des Nutzers protokolliert werden ("Was macht die Zielperson bezogen auf ihr Informationssystem/Rechner aktuell?")." Dazu zählt ebenso die gezielte Suche nach bestimmten Dateien oder Dateiinhalten, Informationen über das jeweilige Rechnerssystem, Kennworteingaben sowie Tastaturanschläge über einen längeren Zeitraum, gibt das BKA zu verstehen. Wie aber soll das möglich sein ohne aufzufallen?

Die Erklärungen des BKA bleiben naturgemäß vage: "Abhängig vom Überwachungszweck können alle Ein- und Ausgaben, je nach Bedarf und an die jeweilige Maßnahme angepasst, erfasst werden."

Eine Frage beschäftigt die Öffentlichkeit seitdem besonders: Müssen Benutzer des Internet in Zukunft jederzeit damit rechnen, in die Falle eines RFS zu tappen?

Der Präsident des BKA, Jörg Ziercke, winkt ab. Bislang grenzte er den Bedarf auf wenige Fälle ein. Es gehe "schlicht und einfach um fünf bis maximal zehn solcher Maßnahmen im Jahr", sagte Ziercke dem Magazin Stern. Mehr sei nicht beabsichtigt und auch gar nicht möglich. Sein oberster Dienstherr Wolfgang Schäuble äußert sich ähnlich bescheiden. Die Untersuchungen würden sich auf rund zwölf Fälle pro Jahr beschränken, lässt er einen Sprecher verkünden. Gleichwohl möchte er die rechtlichen Einsatzmöglichkeiten möglichstweit gefasst wissen. Im Entwurf für das neue BKA-Gesetz erlaubt der umstrittene Paragraph 20 sogar einen Einsatz der Online-Durchsuchung ohne richterliche Erlaubnis.

Derartiger Bescheidenheit gegenüber sollte man einigermaßen wachsam sein, setzt Sven Lüders, Sprecher der Humanistischen Union, entgegen. Sowohl der Große Lauschangriff als auch die Telekommunikationsüberwachung (TKÜ) habe gezeigt, dass diese Mittel regen Zuspruch bei den Ermittlungsbehörden fänden, wenn sie erst einmal einsatzbereit und erprobt seien.

Kanzleramtschef Thomas de Maizière (CDU) setzte in einem Interview denn auch eher verfahrenstechnische Grenzen für die OnlineÜberwachung an. So könnten mit 50 bis 100 Mitarbeiter im BKA "vielleicht 500, 600 Menschen in Deutschland überhaupt überwacht" werden. Allein die Komplexität der Maßnahme böte so einen "gewissen Schutz" vor einer millionenfachen Überwachung der Netzbürger.

Ein Blick auf die Zahlen der TKÜ zeigen aber etwas anderes: Eine Vervierfachung auf annähernd 41 000 abgehörte Telefone innerhalb der letzten acht Jahre zeigt, dass Kapazitätsgrenzen kein verlässlicher Schutz gegen Überwachung sind. Daraus folgert der sicherheitspolitische Sprecher der Grünen, Wolfgang Weiler: "Mit verbesserter Technik kann es sein, dass die Online-Durchsuchung in fünf Jahren eine Routinemaßnahme wird." Diese gelte es zu verhindern, fordert er deshalb.

"Wir sind bei Euch..."

Anders denken die Mitglieder der CDU. Unisono äußern sie in allen Medien, nur der intensive Einsatz der technischen Mittel könne verhindern, dass Deutschland von fanatischen Terroristen unterwandert werde. Diese gelte es zu entlarven, lässt sich auf dem Online-Portal Abgeordnetenwatch.de, von Insidern liebevoll "Abgewatscht" genannt, im Forum des innenpolitischen Sprecher der CDU, Ronald Pofalla, nachlesen: "Niemand denkt bei Online-Durchsuchungen an eine Schleppnetzfahndung im Internet. Die Privatsphäre des Einzelnen bleibt selbstverständlich gewahrt."

Der Koalitionspartner SPD gibt sich noch zurückhaltend. "Wir stehen noch ganz am Anfang der Überlegungen", vermeldet der SPDInnenexperte Dieter Wiefelspütz aus einer gemeinsamen Arbeitgruppe der Regierungsparteien.

Zudem wollen einige Abgeordnete erst die Entscheidung des Bundesverfassungsgerichts zum nordrhein-westfälischen Verfassungsschutzgesetz abwarten, bevor sie sich endgültig festlegen. Ähnlich äußerten sich auch Peter Struck und Brigitte Zypries.

Die Abgeordneten der drei Oppositionsparteien stellen sich geschlossen gegen die Pläne aus dem Innenministerium. Ulla Jelpke, innenpolitische Sprecherin der Partei "Die Linke", fürchtet jedoch, dass das Gesetz nicht zu stoppen sei. "Schließlich ist der Bundestrojaner faktisch schon zwei Jahre im Einsatz," so Jelpke. Wolfgang Wieland von den Grünen hofft hingegen auf den Einspruch des Bundesverfassungsgerichts, denn schließlich dringe der Bundestrojaner in den Kernbereich der privaten Lebensgestaltung ein.

Geheimpolizeistrukturen

Der Bundesgerichtshof in Karlsruhe hat den Einsatz der heimlichen Online-Hausdurchsuchung vorläufig gestoppt.

Dieser Argumentation schließt sich auch Sven Lüders von der Humanistischen Union an: "Die Wohnung kann heutzutage nicht mehr auf die eigenen vier Wände beschränkt werden, sondern muss im Zeitalter der virtuellen Kommunikation auf die Festplatte ausgedehnt werden." Dies schließe dann aber den verfassungsrechtlich garantierten Schutz des Kernbereichs der privaten Lebensgestaltung ein. Bisherige Überwachungsmaßnahmen wie die Feststellung der IP-Adressen bei der Kommunikation oder das Mitlesen von E-Mails würden vollkommen ausreichen.

Noch einen Schritt weiter geht Padeluun von der Bürgerrechtsorganisation Foebud. Der Bundestrojaner sei ein "Schwindel und kein taugliches Mittel" gegen Kriminelle. Er diene der "Großmannssucht der Paternalisten". Sein Zweck liege allein darin, in der Bevölkerung das Gefühl der ständigen Beobachtung zu erzeugen.

Eine Lehre aus den totalitären Staaten des vergangenen Jahrhunderts sei doch, "alles, was ein Staat heimlich tut, mit größten Argwohn zu betrachten". Das seien Geheimpolizeistrukturen. Padeluun verweist auch darauf, dass der Sinn demokratischer Politik sei, "Beamten im Zaum zu halten, damit sie nicht freien Zugriff auf die Menschen haben." Darin würde der Bundesinnenminister kläglich versagen.

Werner Hülsmann, Vorstandsmitglied der Deutschen Vereinigung für Datenschutz, hat eher Bedenken an dem Wahrheitsgehalt der gewonnenen Erkenntnisse: "Wenn eine staatliche Überwachungs-Software auf einem Rechner installiertwerden kann, bedeutet das zuerst einmal, dass dieser Rechner durch Dritte manipuliertwerden kann. Ein Gericht kann also in letzter Konsequenz nicht sicher sein, dass die ausgespähten Daten auch wirklich von der observierten Person stammen und nicht von einer anderen Stelle eingeschleust wurden. Mithin können diese Daten auch nicht von einem Gericht als Beweismittel zugelassen werden."

Naturgemäß stehen auch die Datenschützer dem Ansinnen der Bundesregierung ablehnend gegenüber. Thilo Weichert, Leiter des unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) sieht ebenfalls Gefahr im Einsatz der Spionage-Software: "Eine beweissichere Dokumentation des Angriffs ist nicht ansatzweise möglich," so Thilo Weichert. "Die Ermittler greifen auf die untersuchten Systeme nicht exklusiv zu. Das Unterschieben krimineller Inhalte lässt sich nicht verhindern."

"Mit dem Bundestrojaner würde der Staat das Instrument krimineller Hacker einsetzen: Das Vertrauen in die Sicherheit des Internet würde sabotiert. Niemand könnte sicher sein, dass nicht in der E-Mail einer Behörde oder in dem Update eines Virenschutzprogramms der Trojaner versteckt ist."

Online-Durchsuchungen stoßen auch bei der Sicherheits-Software-Branche auf Ablehnung. Sie wollten in ihren Programmen keine "Hintertür" für Ermittlungsbehörden offenlassen, betonen führende Antiviren-Spezialisten. Zugleich aber räumen sie ein: Ein gut geplanter und gezielter Angriff kann die besten Schutzmauern durchbrechen. Wie das vonstatten gehen könnte, beschreibt Constanze Kurz vom CCC in einem Interview in der Süddeutschen Zeitung: "Das heißt jetzt sicher nicht, dass das BKA gleich beim Verdächtigen einbricht. Das BKA wird die Verfahren danach abstimmen, wie arglos der Verdächtigte ist. Ist er das, kann der Trojaner sicher auch über einen E-Mail-Anhang in den Rechner eingeschleust werden."

Auch Hersteller von Antiviren-Software tippen auf diese Mittel. Sie stehen als erste vor der Frage, wie sie auf das Eindringen von Schad-Software reagieren wollen. Die Ablehnung ist einhellig: "Ein Trojaner ist und bleibt eine Spionage-Software. Sollte jemand die Struktur des Trojaners an die Firma melden, würde er ohnehin in unser Verzeichnis bekannter Viren aufgenommen", beschreibt Tjark Auerbach, Geschäftsführer Avira, die Vorgehensweise seines Unternehmens.

Dirk Hochstrate, Vorstand GData, bringt einen weiteren Aspekt in die Diskussion: "Da nur ein Bundestrojaner zweifelsohne entdeckt und geblockt würde, werden wir es vermutlich eher mit einem ganzen Heer von Bundestrojanern zu tun bekommen. Dass das der Sicherheit des Internets erheblich schadet, liegt auf der Hand. Denn es besteht die Gefahr, dass Internet-Kriminelle und Cyberterroristen die Funktionen und Wirkungsweisen der Bundestrojaner nachahmen und sogar dieselben Sicherheitslükken für ihre kriminellen Aktivitäten nutzen."

Andreas Lamm, Geschäftsführer der Kaspersky Labs, sieht das genauso: "Ein Trojaner zeigt ein bestimmtes Verhalten - ob er jetzt staatlich oder nicht-staatlich ist. Unsere Produkte analysieren dieses Verhalten und unterbinden es, wenn es ihnen gefährlich vorkommt. Ein "gutes" Spionageprogramm gibt es nicht. Dass widerspricht der Natur der Sache."

"Ein, gutes Spionageprogramm gibt es nicht. Dass widerspricht der Natur der Sache."

Kann man also unbesorgt sein, wenn man nur aktuelle Sicherheits-Software auf seinem Computer installiert hat? So einfach ist die Sache wahrscheinlich nicht zu betrachten. Denn der beste Schutz wird weiterhin größtmögliche Wachsamkeit sein - gegenüber dem eigenen Computer, aber auch gegenüber dem Staat und seinen Dienern.

"Unsere Lösungen nehmen keine Rücksicht auf den Ursprung eines Angriffes oder den Urheber."