

Stiftung Menschenrecht *in Gründung Freiheit ist selbst bestimmtes Leben ohne Angst*

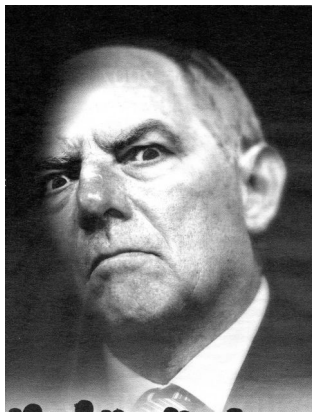
der Menschenrechtsinitiative **Allen Kindern beide Eltern**

Alle Kinder haben ein Geburtsrecht auf die gelebte Beziehung zu Vater, Mutter, Großeltern und allen Verwandten

Vorsitzender Dipl.-Ing. BMT Peter Christof
Lerchenstraße 7
D - 90537 Feucht

Telefon: 09128 – 7240967
Telefax: 09128 – 7240966
Email: menschenrecht@web.de

int. Stiftung Menschenrecht *in Gründung*
der Menschenrechtsinitiative Allen Kindern beide Eltern
Peter Christof – Lerchenstraße 7 – 90537 Feucht



Dr. Wolfgang Schäuble
Bundesinnenminister

Skizziertes Szenario von **Christian Stephan** Stellv. Chefredakteur PC Magazin

Besser auswandern

Montag: Kurz mit dem Finanzbeamten telefoniert.
Dienstag schickt er auch schon die Mail mit dem Steuerformular.
Donnerstag wegen Netzstörungen bei der DSL-Störungsstelle angerufen.
Freitags gelingt die Anmeldung am PC nicht mehr.

Zwei Wochen später: Die Kreditkarten-Abrechnung belastet mit 2000 Euro - die Sie nicht ausgegeben haben.

Gratuliere!

Sie sind mit dem Bundestrojaner infiziert worden.

Den Hook im Betriebssystem machte sich dann ein Hacker zunutze. Sie sind jetzt 2000 Euro ärmer und Ihr Rechner ist verseucht.

Werden die Entwürfe des BKA-Gesetzes umgesetzt, sollten Sie in Zukunft auf keinen Fall mehr Mails von offizieller Stelle laden oder Verbindung mit einer öffentlichen Dienststelle mittels Computer aufnehmen. Denn dann könnten Sie sich einen heftigen Computerschädling einfangen. Der späht eben nicht nur die Verbindungsdaten aus, sondern speichert Passwörter und Tastatureingaben, öffnet und durchsucht Dateien auf dem PC und schickt jedes kleine Detail an die ermittelnde Behörde.

Selbst wenn ich jetzt allen Ermittlungsbeamten beste Absichten unterstelle -und dies anzunehmen ist kindlich naiv - so bleibt der Bundestrojaner zumindest eines: eine massive Gefährdung für jeden häuslichen PC. Trotz aller Be-
teuerungen, die Spionage-Software mit Timebombs wieder zu deaktivieren, können sich an den staatlich subventionierten Virus natürlich Hacker und Webgesindel hängen. Die bekommen das Betriebssystem dank Kernel-Hook dann ruck, zuck geöffnet. Die Injektion des Bundestrojaners erfolgt ja durch vertrauenswürdige Stellen und damit ist auch jeder gefährdet, der vorher durch vernünftiges Handeln im Internet sicher war.

Und ein Stück bin ich gespannt, wann der erste Hacker den Bundestrojaner zweckentfremdet. Weil er ein lustiger Spaßvogel ist, hinterlässt er dem BKA eindeutige Terrorhinweise im infizierten PC. Dann ist nicht nur das Konto leer, sondern man darf in einer Zelle lange über den Sinn eines sicheren Systems nachdenken und sich überlegen, warum man 2007 nicht ausgewandert ist, als niemand etwas gegen den Bundestrojaner unternommen hat. Bleiben Sie besser bei uns und lesen Sie, wie Sie Ihren PC schützen.

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."

Thilo Weichert, Datenschutzbeauftragter Schleswig-Holstein

HORCH WAS KOMMT VON DRAUSSEN...

Immer klarer zeichnet sich ab, wie der Bundestrojaner funktionieren, welche Daten er kopieren und wie er PCs infizieren soll. VON WOLFGANG NEFZGER

Das BKA arbeitet nach Auskunft des Bundesministerium des Inneren seit geraumer Zeit an einer Software für Online-Durchsuchungen und Online-Überwachungen. Derzeit liegen die Arbeiten aber auf Eis, bis die gesetzlichen Grundlagen geklärt sind. Trotzdem sind bereits viele Details zu diesem Remote Forensic Software, kurz RFS genannten Tool-Paket bekannt. So hat der Präsident des BKA auf einer Sicherheitstagung in Hamburg im Juni die Grundrisse vorgestellt.



Am 22. August hat das Bundesministerium des Inneren (BMI) ausführlich auf zwei Anfragen der SPD-Bundestagsfraktion und des Justizministeriums geantwortet, die auf der Web-Seite Netzpolitik bereitgestellt wurden. <http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf> <http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf>

Neben rechtlichen Themen enthielt der Fragenkatalog auch Auskunftswünsche zu vielen technischen Details. Auch wenn die Antworten des BMI oft nebulös wirken, sind sie in einzelnen Punkten doch sehr auskunftsfreudig.

Remote Forensic Software

Die RFS ist das Programm, das auf dem PC installiert wird, der online durchsucht oder überwacht werden soll. Mit anderen Worten: RFS ist der amtliche Name für den Bundestrojaner.

Das BMI geht davon aus, dass für jeden Einsatz des RFS eine individuelle Version des Programms entwickelt wird. Dazu ermitteln die Fahnder zunächst möglichst genau, wie der Ziel-PC ausgestattet und konfiguriert ist. Portscans schließt das BKA dabei ausdrücklich aus und nennt stattdessen klassische Wege wie Telefonüberwachung oder Vertrauenspersonen im Umfeld der zu überwachenden Person als Quelle. Dabei geht es neben der Betriebssystemversion sicher vor allem um die Security-Software wie Antivirenprogramm und Virens Scanner. An Hand dieser Eckdaten programmieren BKA-Spezialisten dann einen Trojaner, der genau darauf zugeschnitten ist. Natürlich wird überprüft, ob verbreitete Antivirenprogramme und Firewalls bei der Installation oder im Betrieb Alarm schlagen. Dieser Trojaner soll nach Angaben des BMI jeweils nur für eine einzige Überwachungsmaßnahme zum Einsatz kommen. Das Risiko einer Entdeckung sei dadurch sehr gering. Wie der fertige Bundestrojaner auf den Ziel-PC gelangen soll, lässt das BMI weitgehend offen: „Es gibt eine Vielzahl von Einbringungsmöglichkeiten, die auf Tauglichkeit für den jeweiligen Einsatz überprüft, ausgewählt und eventuell angepasst werden müssen.“

Daten finden und übertragen

Ist der PC erst einmal infiziert, geht es an die Durchsuchung. Nach Auskunft des BMI sind dabei folgende Aktivitäten vorgesehen:

- Informationen zum PC an sich
- Gespeicherte Dateien
- Suche nach Dateien mit bestimmten Namen

- Suche nach Dateien mit bestimmten Dateieendungen
- Suche nach Eigenschaften/Attributen (Zugriffdaten etc.) ,^
- Schlüsselwortsuche ^
- Suche in bestimmten Verzeichnissen
- Suche nach Dateien eines bestimmten Dateityps
- Erfassung von Passworteingaben, in Bearbeitung befindlicher verschlüsselter Dateien etc.

Entschlüsselung

Eine Abfrage von eventuell an den PC angeschlossenen Webcams oder Mikrofonen ist laut BMI nicht vorgesehen, obwohl technisch kein Problem. Eine solche „Wohnraumüberwachung“, besser als großer Lausangriff bekannt, ist gesetzlich anderweitig geregelt. Auch eine Überwachung von VoIP-Gesprächen ist nach BMI-Angaben deshalb in RFS nicht vorgesehen.

Die zu übertragenden Daten sollen bereits auf dem Ziel-PC möglichst genau selektiert werden. Zum einen dürfen die Fahnder keine Daten aus dem „Kernbereich persönlicher Lebensgestaltung“ erfassen, zum anderen ist natürlich die meist geringe Übertragungsrate der Internetverbindung zu berücksichtigen. Die Daten sammelt der Bundestrojaner zunächst in einer verschlüsselten Logdatei. Bei der nächsten Internetverbindung schickt er sie an den BKA-Server. Das BMI geht dabei davon aus, dass der Versand durchaus mehrere Tage in Anspruch nehmen kann - schließlich soll er auch nicht auffallen.

Eine Alternative wäre, den Bundestrojaner nach der Installation vielleicht über Wochen Ergebnisse aufzeichnen zu lassen. Im Rahmen einer normalen Hausdurchsuchung kann ein Fahnder die Logs dann zusammen mit dem PC beschlagnahmen. Diese Option ist in den Antworten des BMI allerdings nirgends erwähnt.

Entdeckung verhindern

Um eine größere Verbreitung auszuschließen, hat das RFS eine Art Verfallsdatum eingebaut. Nach Ablauf einer bestimmten Frist deinstalliert sich das Programm rückstandsfrei inklusive aller eventuell angelegten Logdateien. Diese Deinstallation kann auch der Controller im BKA per Online-Befehl auslösen. Auch wenn RFS längere Zeit keinen Online-Kontakt mehr zum BKA-Server herstellen kann (etwa, weil eine neue Firewall die Verbindung blockiert), ist eine automatische Deinstallation vorgesehen. Ein Problem sind Updates für die Antiviren-Software, die nachträglich doch zu einer Entdeckung führen könnten. Sobald RFS installiert ist, weiß der Ermittler allerdings exakt darüber Bescheid, welches Antivirenprogramm in welcher Version auf dem PC vorhanden ist. So könnte er parallel an einem Test-PC jeweils die Erkennung testen und gegebenenfalls die Deinstallationsroutine des RFS aufrufen. So merkt die überwachte Person nicht, dass der PC manipuliert wurde. Ausdrücklich weist das BMI darauf hin, dass vorhandene Security-Software nicht einfach abgeschaltet würde, um eine Entdeckung zu verhindern. Auch eine Änderung an der Konfiguration solcher Programme schließt das BMI an anderer Stelle des Antwortenkatalogs zum Thema Deinstallation aus - in der Praxis ist das wohl eher illusorisch. Insgesamt setzt das BKA vor allem darauf, dass durch die ge-

Inge Verbreitung einer individuellen Version des Bundestrojaners eine Entdeckung kaum möglich ist. Droht eine Entdeckung, so soll sich die Software selbst rückstandsfrei deinstallieren. Der Programmcode selbst ist laut Antwortenkatalog durch „kryptografische Mittel“ vor einer Analyse gut geschützt und lässt keine Rückschlüsse auf die Polizei als Urheber zu. Die betroffenen Zielpersonen sollen den Bundestrojaner für eine der lästigen Web-Plagen halten, die sowieso millionenfach im Umlauf sind.

Verbreitungswege

In einem Punkt halten sich die Antworten des BMI deutlich zurück: Wie soll der Ziel-PC infiziert werden? Schwammig ist von vielen „Eindringungsmöglichkeiten“ die Rede, unter denen die Ermittler im konkreten Fall die erfolgversprechendste auswählen. Sehr verwegen wirkt der Vorschlag, den Bundestrojaner getarnt als „offizielle“ E-Mail von Bundesbehörden wie etwa Finanzämtern zu versenden. Der Tro-

janer wäre dabei etwa als 5DF-Version eines Steuerelements getarnt, beim Öffnen des Anhangs per Doppelklick installiert sich der Spion und öffnet dann das

Satz ein, er würde keinesfalls ohne Rücksprache mit der entsprechenden Behörde erfolgen. Das dürfte wohl auch selbstverständlich sein, denn die E-Mail muss im PDF sinnvolle Daten enthalten, sonst wird der Empfänger sofort misstrauisch.

Jeder halbwegs erfahrene PC-Nutzer dürfte in den letzten Jahren gelernt haben, nicht einfach auf irgendwelche Dateianhänge von E-Mails zu klicken. Spätestens mit den gefälschten E-Mails von BKA, Ikea oder I&L, die Spam-Versender zur Infektion neuer Zombie-PCs für ihre Botnetze im letzten Jahr einsetzen, dürften sich nur noch wenige Anwender von „offiziellen“ Absenderadressen einlullen lassen. Und die Äußerungen des BMI gießen noch Öl aufs Feuer.

Manipulierte Downloads

Präziser wären manipulierte Downloads von Programmdateien, die sich die Zielperson herunterlädt. Dazu könnte das BKA über den Internet-Provider den Datenstrom des Ziel-PCs überwachen. Lädt der Anwender eine Programmdatei herunter, fügt ein Programm in den Download automatisch den Bundestrojaner ein. Die Techniken sind von echten Viren bekannt und einfach umzusetzen. Beim Start des Downloads wird zunächst der Trojaner aktiv und klinkt sich im System ein. Darauf startet der Viruscode das ursprüngliche Programm.

Statt beim Internet-Provider anzusetzen, könnte die Polizei auch die Downloads auf Websites manipulieren, die der Anwender nur nach einem Login erreicht. Die kriminellen Kollegen der BKA-Beamten wissen, wie Sie Nutzer dazu verleiten, sich selbst einen Trojaner auf die Festplatte zu laden.

Scheidung darüber liegt beim Anwender. Besonders effizient sind diese Varianten also nicht. Zudem gibt das BMI in seinem Antwortkatalog an, dass die Installation von RFS ohne die Mithilfe Dritter (wie etwa Provider) erfolgen soll.

Exploits im Hintergrund

Neutral betrachtet stehen die kriminellen Betreiber von Botnetzen vor demselben Problem wie die Polizei: Sie wollen mit möglichst großer Effizienz PCs infizieren, ohne dass die Besitzer etwas davon merken. Die bevorzugte Lösung der Botnetzer sind derzeit Drive-by-Downloads.

Surft man eine normale Webseite an, so klopft im Hintergrund ein JavaScript-Programm, das in den HTML-Code der Webseite eingebettet ist, den Browser auf Sicherheitslücken ab. Diese Sicherheitslücke nutzt dann der entsprechende Exploit aus, um den Trojaner zu installieren.

Die Polizei will nur einen ganz bestimmten PC infizieren. Sie könnte wieder über den Internet-Provider während der Übertragung einzelne HTML-Dateien abfangen und manipulieren. Oder Sie versendet E-Mails, die gezielt Exploits im E-Mail-Programm oder anderen Komponenten auf dem PC ausnutzen. Wenn etwa bekannt ist, dass die Zielperson einen Webmail-Anbieter benutzt, könnte nach dem Login auf den Webseiten entsprechender Code untergebracht sein. Oder an diese E-Mail-Adresse wird eine Nachricht gesendet, die wiederum Exploits im Browser ausnutzt. Höchstwahrscheinlich hat auch das FBI beim dokumentierten Einsatz der CIPAV-Software diese Technik gewählt, um den PC einer unbekanntem Zielperson auszuspähen. Wie das BKA an Kenntnisse über Exploits kommen will, bleibt offen. Zwar lehnt das BMI in seinem Antworten katalog den Kauf von so genannten Zero-Day-Exploits über die Hackerszene ausdrücklich ab. Vielsagend heißt es aber schon im nächsten Satz: „Informationen, die die Sicherheit von Betriebssystemen und Programmen betreffen, sind im Internet in der Regel frei zugänglich.“ Mit anderen Worten: Bestehende Sicherheitslücken mit bekannten Exploits wird das BKA sehr wohl zur Infektion eines Ziel-PC einsetzen. wn

Weitere Informationen zum Thema finden Sie unter www.pc-magazin.de.

PC Magazin 11/2007 www.pc-magazin.de

Welche genauen technischen Möglichkeiten gibt es und welche davon sollen genutzt werden, um die Maßnahmen umzusetzen, differenziert nach a) dem Aufbringen der Überwachungssoftware auf das informationstechnische System

Es gibt eine Vielzahl von Einbringungsmöglichkeiten, die nunmehr auf Tauglichkeit für den jeweiligen Einsatz überprüft und eventuell angepasst werden müssen. Grundsätzlich ist dabei die unwissentliche Mitwirkung der Zielperson notwendig, um eine Entdeckung der Maßnahme zu verhindern. Eine generelle Aussage zur genauen Einbringungsmethode ist nicht möglich, da sie jeweils vom Einzelfall und vom Nutzungsverhalten der Zielperson sowie der vorliegenden technischen Bedingungen abhängig ist.

Das Bundesministerium des Inneren antwortet dem Justizministerium nicht sehr konkret. Vom Bundestrojaner ganz allgemein von „informationstechnischen Systemen“. Eine höchst schwammige Formulierung, die viel Freiraum für Interpretationen lässt. Der Fragenkatalog der SPD-Bundestagsfraktion an das Bundesministerium des Inneren geht unter Punkt 27 darauf ein und zählt in der Frage explizit Handys, Smartphones, Blackberries, Infrastrukturkomponenten wie Router, Switches und DE-CIX-Komponenten (DE-CIX ist ein zentraler Austauschknoten für Datenpakete im deutschen Internet). Die lapidare Antwort des BMI: „Somit sind die aufgezählten Beispiele ebenfalls umfasst.“ Natürlich wären dafür entsprechend angepasste Versionen von RFS oder sogar ganz andere Programme erforderlich.

Ein dokumentierter Fall betrifft die US-amerikanische Bundespolizei FBI. Für besondere Fälle nutzt die Behörde das Tool CIPAV (Computer and Internet Anzeige Protocol Address Verifier). Dabei geht es darum, nachzuweisen, dass ein PC zu einem definierten Zeitpunkt mit einer bekannten IP-Adresse im Internet unterwegs war. Die eidesstattliche Erklärung eines FBI-Agenten mit Details zu CIPAV gibt es hier im Original zu lesen: www.pouitechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf Im konkreten Fall hat ein ehemaliger Schüler der Timberline High School im Bundesstaat Washington der Schule mehrmals mit Bombendrohungen per E-Mail zukommen lassen. Dazu benutzte er fünf unterschiedliche Google-Mail-Adressen und richtete das Myspace-Konto timberlinebombinfo ein. Dort sollten „Sympathisanten“ ihre Kommentare hinterlassen und die Bombenaktion so unterstützen. Zudem startete er einen Denial-of-Service-Angriff auf den Mail-Server der Schule.

Das Problem für das FBI: Der Schüler nutzte drei mit Malware manipulierte PCs in Italien als Zwischenstation, um sich bei Google und Myspace einzuloggen. So hatten die Ermittler zwar die entsprechenden IP-Adressen von Google und Myspace, konnten daraus aber keine Rückschlüsse auf den Absender ziehen. Und hier kam CIPAV ins Spiel. Die Software installiert sich auf dem Windows-PC des Verdächtigen und protokolliert verschiedenste Daten.

Diese sendet es in regelmäßigen Abständen an das FBI.

Konkret sind das laut Erklärung folgende Details:

- IP-Adressen, mit denen der PC Kontakt hatte
- Die zuletzt besuchte Webadresse
- Liste aller IP-Adressen, mit denen Kontakt bestand
- MAC-Adresse der Netzwerkkarte
- Liste aller laufenden Programme
- Browser-Informationen wie Typ und Version
- Betriebssystemversion samt Seriennummer
- Benutzerinformationen aus der Registry
- Liste offener TCP- und UDP-Ports
- Name des eingeloggt Benutzers

Im Gegensatz zum geplanten Bundestrojaner schneidet CIPAV nicht Inhalte der Kommunikation oder der Festplatte mit. Dies betont der FBI-Agent in seiner Erklärung mehrmals ausdrücklich. Ob das eine technische Einschränkung der Software ist oder im konkreten Fall durch den richterlichen Beschluss nicht abgedeckt war, ist unklar. Auch gehen die veröffentlichten Dokumente nicht darauf ein, wie CIPAV auf den PC des Schülers gelangte. Nur so viel ist klar: Beim Abholen von E-Mails bei Google Mail oder nach dem Einloggen in Myspace wurde der PC des Täters infiziert. Einen direkten Zugriff auf den

PC hatte das FBI nicht - sonst hätte man sich den Software-Einsatz gleich sparen können. Der Schüler wurde im Juni 2007 verhaftet und vom Gericht zu 90 Tagen Jugendhaft verurteilt.
Nichts gewusst: Auf der offiziellen FBI-Homepage will man von CIPAV nichts wissen.

PC Magazin 11/2007 www.pc-magazin.de

Ein Trojaner ist ein Trojaner Randy Abrams, Security Technology Editor bei Eset

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

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

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.

Wie, glauben Sie, kann ein RFS funktionieren?

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.

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

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.

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

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.

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?

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 durchzufliessen, 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.

**ONLINE-DURCHSUCHUNG
JA ODER NEIN?**

internationale Stiftung Menschenrecht - Peter Christof - Lerchenstraße 7 - 90537 Feucht - T: 09128 7240967 - menschenrecht@web.de ../6
Comdirect Bank BLZ: 20041133 Konto: 3739182 BIC / SWIFT-Code: COBADEHD001 IBAN: DE30 2004 11330373918200
<http://www.menschenrechtsinitiative.de> <http://www.stiftungmenschenrecht.de> <http://www.stiftung-menschenrecht.de>

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 einen Antrag auf verdeckte Online-Durchsuchung für rechtswidrig erklärt hatte. Die Entscheidung des Ermittlungsrichters war 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 SPD im Bundestag eine kleine Anfrage an die Bundesregierung. Inhalt der Anfrage war jene Beschwerde vor dem Bundesgerichtshof. Die Abgeordneten waren bereits Wochen zuvor über einen Passus gestolpert, der im „Programm zur 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-Organen sollen insgesamt zehn Versuche gestartet haben. Mit welchem Erfolg, ist nicht bekannt. (Verfassungsschutz bereits seit Januar Computer online durchsuchen. Dagegen hat Frederik Roggan, Vorsitzender der Bürgerrechtsorganisation Humanistischen Union, Verfassungsbeschwerden eingeleitet.)

Kommissar Trojaner

Es vergeht keine Woche, in der nicht neue Positionen und Erkenntnisse über den Einsatz des Bundestrojaners (offiziell Remote Forensic Software, RFS) bekanntwerden. Was bei manchen 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 einem 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 Rechnersystem, 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 möglichst weit gefasst wissen. Im Entwurf für das neue BKA-Gesetz erlaubt der umstrittene Paragraph 20 sogar einen Einsatz der Online-Durchsuchung ohne richterliche Erlaubnis.

PC Magazin 11/2007 www.pc-magazin.de

O 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 School 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.

Dieser Account soll ihm aber zum Verhängnis werden. Denn offenbar wurde der FBI-Trojaner 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 Web-siteabrufe 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 Spy-ware 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.

Derartiger Bescheidenheit gegenüber sollte man einigermaßen wachsam sein, setzt Sven Lüders, Sprecher der Humanistischen Union, entgegen. Sowohl der Große Lauschangriff als auch die Telekommuni-

kationsüberwachung (TKÜ) habe gezeigt, dass diese Mittel regen Zuspruch bei den Ermittlungsbehörden fänden, wenn sie erst einmal einsatzbereit und erprobt seien.

Kanzleramtschef Thomas de Maiziere (CDU) setzte in einem Interview denn auch eher verfahrenstechnische Grenzen für die Online-Überwachung 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 Schleppnetzfehndung 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 SPD-Innenexperte Dieter Wiefelspütz aus einer gemeinsamen Arbeitsgruppe 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. UUa Jelpke,

Der Bundestrojaner ist taktisch 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

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

Werner Hülsmann, „Ein gutes' Spionageprogramm gibt es nicht. Das widerspricht der Natur der Sache.“

Andreas Lamm, Geschäftsführer der Kaspersky Labs

Deutschen Vereinigung für Datenschutz, hat eher Bedenken an dem Wahrheitsgehalt der gewonnenen Erkenntnisse: „Wenn eine staatliche Überwachungs-Software auf einem Rechner installiert werden kann, bedeutet das zuerst einmal, dass dieser Rechner durch Dritte manipuliert werden 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 Landesentrums 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."

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

abstimmen, wie arglos der Verdächtige 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 Heervon 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 Sicherheitslücken 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." 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. whs

Weitere Informationen zum Thema finden Sie unter www.pc-magazin.de/sicherheit.

PC Magazin 11/2007 www.pc-magazin.de

Jede Freude, jedes Glück, was wir anderen bereiten, kommt zu uns ebenso sicher zurück, wie jedes Leid, das wir verursachen.

Ändern wir die Zielrichtung von Machtgier, Habsucht, Neid, Missgunst, ... zu einem Miteinander - denn mit dem Ende der Gier, lässt sich auch das Leid, der Hungertod und jeder Krieg beenden.

Es liegt nur an uns selbst - niemand wird es für uns tun - wir müssen es selbst tun !

Helfen Sie unserer *Stiftung Menschenrecht*, lassen Sie es uns gemeinsam angehen - HEUTE noch!

Ohne Hoffnung gibt es keine Zukunft !

Ihr Peter Christof Vorsitzender
Stiftung Menschenrecht *in Gründung*
der Menschenrechtsinitiative
Allen Kindern beide Eltern
mit ihrem Projekt

Selbst bestimmtes Leben ohne Angst in Freiheit, geachtet und gesund an Geist, Körper und Seele ist das Geburts - Recht eines jeden Menschen. Dies schließt alle Kinder - auch die von Trennung und Scheidung betroffenen ein!

Kinder haben ein Geburtsrecht auf die gelebte Beziehung zu Vater, Mutter, Großeltern und allen Verwandten