RFS

Categories : Bankgeheimnis

Welche Geräte durchsucht die RFS?

In beiden Schreiben betont das Innenministerium, dass die Definition "informationstechnisches System" bewusst weit gefasst wurde. Die Anfrage der SPD-Fraktion, ob darunter auch "auch Mobilgeräte wie Handys, Smartphones, Blackberries" fallen, bejaht das Ministerium. Allerdings bedeute das nicht, dass Gespräche mitgeschnitten würden. Telekommunikationsinhalte seien nicht Gegenstand einer Online-Durchsuchung. Im Klartext: Auf Smartphones darf die Software schnüffeln, aber nicht mithören.

Wann ist der Bundestrojaner einsatzfähig?

Jederzeit. Das Innenministerium schreibt extrem zuversichtlich: "Die Entwicklung einer einsetzbaren Version der RFS könnte bei Aufhebung des gegenwärtig verfügten Entwicklungsstopps unverzüglich abgeschlossen sein."

Werden Telefonate über Programme wie Skype mitgeschnitten?

Nicht im Rahmen einer Online-Durchsuchung. Aber es gibt im Innenministerium konkrete Ideen zur Überwachung verschlüsselter Voice-over-IP-Gespräche, die über Programme wie Skype abgewickelt werden. Im Rahmen einer Telekommunikationsüberwachung müsse hier das gesprochene Wort "an der Audioschnittstelle beziehungsweise die Kommunikationsdaten vor der Verarbeitung durch die Verschlüsselungssoftware abgegriffen" werden, heißt es in dem Schreiben des Innenministeriums an das Bundesjustizministerium. "Entsprechende Überlegungen" seien "derzeit Gegenstand von Konzeptionen der Bedarfsträger".

Wie kommt die Software auf die Rechner?

Das ist gar nicht so einfach - so die Kurzfassung der sehr umfangreichen, sehr vagen Ausführungen des Ministeriums dazu. So ist die Rede von einer "Vielzahl von Einbringungsmöglichkeiten", deren Tauglichkeit vor jedem Einsatz geprüft werden müsse. Vorab müsse geklärt werden,

- welches Betriebssystem,
- welchen Internetzugang,
- welchen Browsertyp

der Ausgespähte verwende.

Anfang August hatten bereits Vertreter des Bundeskriminalamts (BKA) dem Computer-Magazin "Chip" erklärt, die Standard-Vorgehensweise sei, dass Beamte unbemerkt in die Wohnung des Verdächtigen eindringen, die IT-Ausstattung analysieren und das weitere Vorgehen darauf

abstimmen. In der Regel werde das Schnüffelprogramm bei einem zweiten Einbruch installiert, seine Erkenntnisse würde es dann unbemerkt ans BKA übertragen.

Diskutiert wird auch, ob man E-Mails unter dem Namen einer anderen Behörde verschickt, um auf diesem Weg Programme auf einen Computer zu bekommen. Generell wird davon abgeraten - doch könne "in begründeten Ausnahmefällen" dieses Mittel zum Einsatz kommen.

Anmerkung: Das wird wohl der Regelfall werden.

Entdecken Virenscanner die RFS?

Wohl kaum - glaubt das Bundesinnenministerium. Interessant ist die Argumentation: Die Software werde für jeden Einsatz überarbeitet und "vor dem Einsatz mit aktueller Anti-Viren-Software geprüft". Außerdem sei auch durch die "insgesamt geringe" Einsatzhäufigkeit der RFS das Entdeckungsrisiko durch Anti-Virenprogramme "sehr gering".

Allerdings:

Zum einen schreibt das Innenministerium, die "insgesamt geringe" Einsatzhäufigkeit der RFS mache eine Entdeckung wenig wahrscheinlich. Dazu Hartmut Pohl von der Gesellschaft für Informatik: "Wenn ein Sicherheitsprogramm verdächtiges Verhalten bemerkt, gelingt das auch beim ersten Mal." Moderne Virenscanner achteten nicht mehr allein auf bekannte Dateimuster von Schadprogrammen, sondern suchten immer häufiger nach verdächtigen Verhaltensweisen, sagt Informatiker Pfitzmann.

Er hält auch die zweite Begründung des Innenministeriums für wenig stichhaltig, wonach die RFS Fundstücke auf der Festplatte des Ausgespähten verschlüsselt. Das verhindert laut Pfitzmann kaum, dass das Programm entdeckt wird: "Es gibt praktikable Methoden, gerade nach verdächtigen, verschlüsselten Informationen auf einer Festplatte zu suchen."

Das Entdeckungsrisiko sei bei solchen Schnüffelprogrammen immer gegeben, sagt auch Frank Rosengart vom Chaos Computer Club. Und: "Wenn der Trojaner erstmal entdeckt wird, können den Ermittlern sogar gefälschte Beweismittel untergejubelt werden."

Es lebe der deutsche Rechtsstaat.

Was späht die RFS aus?

Vorab definierte Suchkriterien sollen eine "begrenzte Suche" sicherstellen. Hintergrund: Das Bundesinnenministerium fürchtet zum einen, dass die Schnüffel-Software eher entdeckt wird, wenn sie große Datenmengen überträgt. Zum anderen will man damit den sogenannten Kernbereichsschutz garantieren. Das Bundesverfassungsgericht verlangt nämlich in Urteilen zum Lauschangriff, dass ein "Kernbereich privater Lebensgestaltung" unangetastet bleibt. Diese Forderung sieht das Innenministerium dadurch erfüllt, dass die "Verwendung bestimmter

Suchkriterien" generell verboten wird. Als Beispiele für mögliche Suchkriterien führen die Schreiben des Innenministeriums auf:

- Dateinamen,
- bestimmte Dateiendungen,
- Eigenschaften/Attribute (Zugriffdaten etc.),
- Schlüsselwörter,
- bestimmte Verzeichnisse,
- Dateien eines bestimmten Dateityps.

Wie kommen die Daten zu den Behörden?

Übers Netz: Die RFS speichert die Suchergebnisse verschlüsselt auf dem ausgespähten Computersystem. Sobald eine Internetverbindung hergestellt ist, soll die Software die Daten verschlüsselt an einen "von den Sicherheitsbehörden genutzten Server übertragen" und anschließend löschen.

Wie teuer ist die Überwachung?

Dazu schreibt das Ministerium nichts Konkretes. Aber die Schreiben deuten an, dass der Aufwand immens ist und ein Masseneinsatz sehr kostspielig werden dürfte, da die Software für jede Überwachung neu geprüft und angepasst werden soll. Konkret steht in den Schreiben, dass zum Beispiel für die Wahl der Einbringungsmethode "mehrere Personentage /-wochen notwendig werden" könnten und der "Aufwand verdeckter Maßnahmen" generell vor der Durchführung "kaum abschätzbar" sei.

Der Präsident des Bundeskriminalamts (BKA) Jörg Ziercke nennt in einem Interview mit dem Magazin "Stern" die Debatte um Online-Durchsuchungen eine "Angstmacher-Diskussion". Es gehe "um maximal zehn solcher Maßnahmen im Jahr". Mehr seien nicht möglich, "weil wir jeweils eine eigene Software entwickeln müssen".

Diese Argumentation überzeugt den Informatiker Andreas Pfitzmann von der TU Dresden nicht. Das Zuschneiden der Software auf verschiedene Systeme sei nicht so aufwendig. Pfitzmann zu SPIEGEL ONLINE: "Das kann man automatisieren, so dass die Mitarbeiter letztlich in einem Toolkit nur alle Details zum zu überwachenden System eingeben müssen und dann eine passende Software erhalten."

Außerdem ist zu bedenken, dass viele Computer mit der Standardinstallation ab Werk arbeiten. Hat man eine RFS für einen dieser Rechner fertiggestellt, sind alle anderen ebenso konfigurierten mit demselben Programm angreifbar. Eine vergleichbare Standard-Konfiguration gibt es auch in vielen Unternehmen. In so einer Umgebung kann dasselbe Programm ohne Aufwand alle Rechner ausspähen, sagt Hartmut Pohl, Sprecher des Arbeitskreises Datenschutz und IT-Sicherheit der deutschen Gesellschaft für Informatik.

Der Einsatz muß sich auf jeden Fall lohnen. Was folgt daraus?

Wie immer: Man propagiert, daß mit diesem System Terroristen und Drogenhändler enttarnt werden sollen, organisierte Kinderschänder und Schwerstkriminelle - und Presse und breites Publikum sind beeindruckt und stimmen zu.

Tatsächlich wird man damit

„Otto Normalverbraucher“ in seiner Eigenschaft als Steuerzahler

ausspionieren, wenn man mittels

Kontenabruf

glaubt Grund zu der Annahme zu haben, daß sich dieser Einsatz lohnen könnte.

§370a AO i.V.m. § 261 StGB in ihren Neufassungen haben im Ergebnis hinsichtlich mehr oder minder alltäglicher Steuerhinterziehungen, aus einem Vergehen (in der Schweiz eine Ordnungswidrigkeit) nicht mehr und nicht weniger als ein Verbrechen gemacht. Und da kann man denn ja den Bundes-Trojaner trefflich anwenden - und wird das auch tun.

Bringt der routinemäßige Kontenabruf bei der Bank nichts, wird kaum etwas passieren.

Und dieser Abruf bringt dann nichts, wenn die wesentlichen Vermögenswerte sicher und diskret in einem geeigneten Land außerhalb der EU angelegt sind - in einem Land, in dem das Bankgeheimnis noch etwas Wert ist.

Dabei helfen wir gern.