Jan Krissler und Constanze Kurz

Die heimliche Online-Durchsuchung

Was ist die in den Medien „Bundestrojaner" genannte Online-Durchsuchung eigentlich? Anzunehmen ist, dass weder der Bundesinnenminister Wolfgang Schäuble als vehementer Forderer noch der BKA-Präsident Jörg Ziercke als zukünftiger Anwender dies technisch erläutern können. Mal spricht der eine von zu durchsuchenden Internet-Servern, mal der andere von auszuspionierenden Privat-PCs.

Während der Innenminister betont, persönliche Daten wie Liebesbriefe, Onlinebanking- und Arztdaten sollten nicht angetastet werden, will der BKA-Chef alle Daten genauestens durchsuchen, denn vermeintliche Terroristen würden ihre geheimen Anschlagspläne auch in privaten Tagebuchaufzeichnungen verstecken. „Zum Schutz des Kernbereichs des Persönlichkeitsrechts der Betroffenen können z. B. je nach dem Einzelfall bestimmte Schlüsselbegriffe als Suchbegriffe verwendet werden", sagte Ziercke beim Fachgespräch der Grünen zum Bürgerrechtsschutz im digitalen Zeitalter im Bundestag. An welche Suchbegriffe mag er gedacht haben – „Bombenbastelanleitung" oder doch eher „Tagebuch"?

Seit dem 8. Juni 2005 war der Einsatz der heimlichen Online-Durchsuchung durch eine einfache Dienstvorschrift des damaligen Innenministers Otto Schily erlaubt. Nach Bekanntwerden setzte Schäuble die Vorschrift außer Kraft, da der Bundesgerichtshof zwischenzeitlich die Unzulässigkeit der heimlichen Durchsuchung festgestellt hatte. Nun aber treibt der Bundesinnenminister aktuell die Schaffung einer Gesetzesgrundlage für die Online-Schnüffelei als präventive, verdeckte Überwachungsmaßnahme voran – falls nötig sogar inklusive einer Änderung des Grundgesetzes.

Was droht dem verdächtigten Bürger nun? Ein Trojaner könnte jeden Tastendruck des durchsuchten Computers mitprotokollieren, um etwa Passwörter mitzulauschen. Auch die Auskundschaftung der gesamten Kommunikation des Nutzers per E-Mail, Chat oder Internettelefonie wäre technisch machbar. Der Bundestrojaner könnte aber auch den Inhalt der Festplatte durchsuchen, dabei Daten auslesen, sogar löschen oder verändern. Man muss kein juristisches Staatsexamen haben, um sich auszumalen, welche rechtlichen Probleme daraus folgen. Die grundgesetzlich geschützte Unverletzlichkeit der Wohnung ist genauso betroffen wie die informationelle Selbstbestimmung. Anders als bei der nur dem Namen nach vergleichbaren Hausdurchsuchung, die zu einer Beschlagnahme eines Computers führen kann, ist die Online-Durchsuchung gerade keine Momentaufnahme des Inhalts der Festplatte. Denn die Spionagesoftware wird nicht nur heimlich, sondern auch dauerhaft auf dem Rechner platziert. Der BKA-Chef Ziercke erläuterte dazu, der Bundestrojaner werde aber „ein Datum zur Selbstauflösung haben", da eine zeitliche Begrenzung auf maximal sechs Monate vorgesehen ist.

Für Menschen, die regelmäßig privat oder beruflich mit einem Computer arbeiten, dürfte die Vorstellung, jemand blicke dauerhaft beim Surfen über die Schulter und ermittle ein komplettes Abbild ihrer Kommunikation mehr als unbehaglich sein. Denn der Inhalt der Festplatte und die Surfgewohnheiten sind Teile des Privat- und Berufslebens, die niemand gerne preisgibt. Im Gegensatz zu gut informierten Technikern kann sich der normale Benutzer nicht vor der Ausspionierung schützen. Hier wird der Einsatz des Bundestrojaners als tatsächliche Chimäre deutlich, denn informierte Kriminelle werden sich technisch zu helfen wissen und sich wirkungsvoll gegen die Spionagesoftware abschotten können.

Eine noch offene Frage ist dabei die technische Versiertheit der Entwickler des Bundestrojaners, denn Auskünfte zu technischen Details verweigert das BKA bisher. Setzen die Ermittler bei der Programmierung auf Standardkomponenten und bereits bekannte Sicherheitslücken, kann die Spionagesoftware sehr schnell durch Virenscanner oder Firewalls erkannt werden und bleibt damit wirkungslos. Das Entdeckungsrisiko wäre außerdem für die Ermittler hoch.

Werden hingegen neu entwickelte Trojaner eingesetzt, ist das Risiko der Entdeckung zwar gering, der Aufwand jedoch größer. Eine zeitintensive Ausforschung des Rechners im Vorfeld hinsichtlich des Betriebssystems und der benutzten Software muss aber gezielt erfolgen. Dazu sind Experten nötig, die Sicherheitslücken auch auf eventuell gut gewarteten Systemen finden. Das Entdeckungsrisiko kann auch bei aufwändiger Vorbereitung jedoch nie ausgeschlossen werden. Fehler bei der Programmierung passieren selbst geübten Anwendern, werden also auch den auf diesem Feld noch wenig versierten BKA-Entwicklern unterlaufen. Spätestens nach der gesetzlich geplanten Benachrichtigung des Spionageopfers nach Abschluss der Maßnahme ist der Belauschte im Besitz der Schadsoftware. Einer Analyse der ausgenutzten Sicherheitslücke steht dann nichts im Wege. Der Chaos Computer Club hilft Betroffenen gerne dabei.

Über die Autoren
Jan Krissler arbeitet am Fraunhofer-Institut und ist seit 10 Jahren im Chaos Computer Club aktiv, wo er sich vor allem mit Biometrie- und RFID-Technik beschäftigt. Constanze Kurz ist Informatikerin, arbeitet an der Humboldt-Universität zu Berlin und engagiert sich in ihrer Freizeit im Chaos Computer Club.