

Vorratsdatenspeicherung

- Bisher: nur Bestandsdaten; Verkehrsdaten nur für Rechnungsstellung
- Jetzt: Verkehrsdaten für 6 Monate
- Begründung dafür: Verfolgen von Strafhandlungen
- Genauer beschrieben ist es im Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen
- Die Urheberrechtsverwerter versuchen auch an die Daten zu kommen

Was gespeichert wird:

- Verkehrsdaten (wer telefoniert oder mailt mit wem)
- Standortdaten (wo ist derjenige der gerade mit dem Handy telefoniert)
- Dasselbe gilt für SMS und Fax!
- Rufnummern, Anrufzeit, IMEI-Nummer, Funkzelle, Aktivierungsdatum bei Prepaid-Karten – jeweils die Daten des Anrufenden und des Angerufenen
- Bei Weiterleitungen jeder beteiligte Anschluß
- Auch Anbieter eines WLAN-Hotspots betroffen
- Nur die Verkehrsdaten, keinen Inhalt

Wie lange wird gespeichert

Medium	Speicherung bisher	Speicherung seit 1.1.2008
Festnetz	80-90 Tage	6 Monate
Mobilfunk	90 Tage	6 Monate
SMS	90 Tage	6 Monate
Internet via ISDN/Analog	80-90 Tage	6 Monate
Internet via DSL/Flat	Durfte nicht	6 Monate
VoIP	Keine Speicherung	6 Monate
Email	Keine Speicherung	6 Monate

Warum wird gespeichert?

- Kriminalitätsbekämpfung – organisierte Kriminalität und Terroristen
- Verfolgung und Aufklärung von bereits begangenen Straftaten
- Ermittlung des Aufenthaltsortes von Terroristen.
- Prävention? Damit nicht möglich
- Laut AK Vorrat wird die Aufklärungsrate um 0.006% gesteigert

Was kann ich tun?

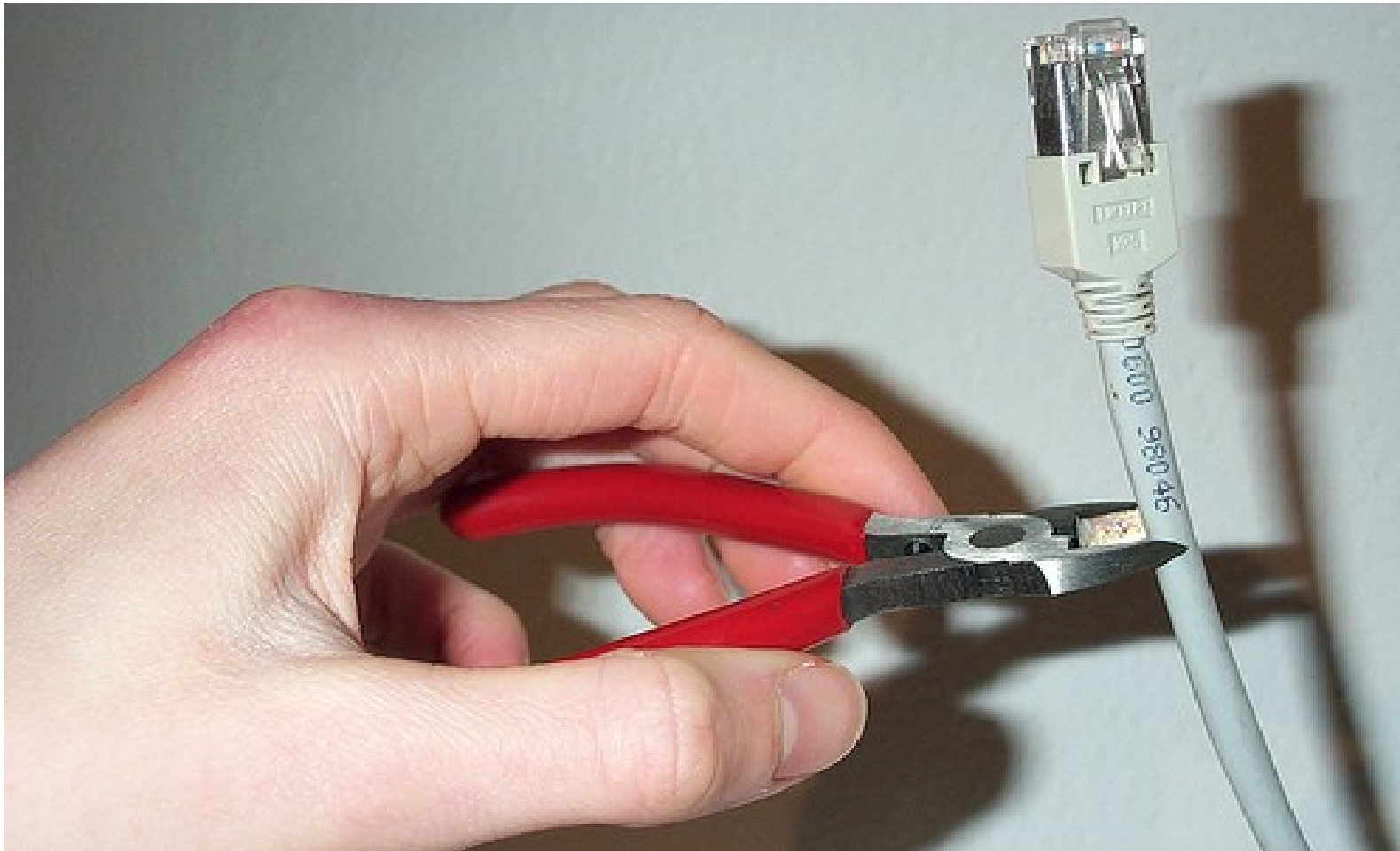


Foto von Germanium: <http://www.flickr.com/photos/germanium/1580297705/>

CCCS: Princess & Rince @ ATTAC Ludwigsburg, 21.2.2008

Bundestrojaner

- Viele Gerüchte, wenig wirklich bekannt
- Ein Stück Software welches auf dem Zielrechner installiert wird
- Soll „Die Festplatte“ des Rechners nach Stichworten durchsuchen und die Ergebnisse speichern
- Soll Online-Kommunikation abhören, bevor sie ins Netz geschickt wird (Skype) oder bevor Daten auf die Festplatte gespeichert werden

Das Ziel des Bundestrojaners

- Gedacht für jedes elektronische Systeme – das heisst Computer, Router, Access Points, Telefon, Anrufbeantworter, Wecker..
- Die „Remote Forensic Software“ wird vom BKA erstellt und ist einsatzbereit – und bereits zweimal benutzt worden
- Wird gebraucht weil doch alle Leute ihre Festplatten verschlüsseln
- Und weil VoIP direkt mit Verschlüsselung arbeitet

Was kann der Bundestrojaner?

- Er muss einsetzen bevor Verschlüsselung einsetzt, muss also tief im System sich einnisten
- Es soll ein Keylogger sein
- Unterschied Online-Überwachung vs. Online-Durchsuchung
- Maximal 10 Einsätze pro Jahr; hohe behördliche Hürden

Wie soll er das Opfer erreichen(1)?

- Man braucht einen Richterbeschuß zumindest momentan von zwei Richtern
- Vertrieb:
 - Via Email (von staatlichen Behörde)
 - CD/USB-Stick im Briefkasten
 - Programme wie Elster
 - Generelle Sicherheitsupdates (Gerade DSL-Router!)
 - In die Wohnung eindringen und „einspielen“
 - Via Handy

•Wie soll er das Opfer erreichen(2)?

- Nach Richtererlaubnis kann die RFS eingesetzt werden – zeitlich begrenzt, maximal drei Monate - diese Zeit wird in der Software selbst eingetragen, so dass sich der Trojaner selbst deinstalliert (laut Fachleuten)
- RFS muss vorbereitet werden für das Zielsystem – dieses Vorbereiten kann einige Wochen dauern.

Vorschläge zu Gegenmaßnahmen

- Münztelefone nutzen
- Briefe schreiben
- Von externen Massenspeichern booten – von LiveCDs wie Knoppix (<http://www.knopper.net>) oder Ubuntu (<http://www.ubuntu.com>)
- „Zweiter PC im PC“ - VmWare
- USB-Sticks mit Daten drauf und diesen immer mitnehmen

Wie wird Sicherheit gesehen?



<http://tim.geekheim.de/2008/02/02/security-vs-privacy/>



<http://www.pulitzer.org/year/2002/editorialcartooning/works/101101.html>

Vielen Dank für die Aufmerksamkeit

- Dieser Vortrag wird unter der Creative Commons License veröffentlicht:

