

Vorratsdatenspeicherung

- Bisher: nur Bestandsdaten; Verkehrsdaten nur für Rechnungsstellung
- Jetzt: Verkehrsdaten für 6 Monate
- Begründung: 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 bzw. Sender und Empfänger bei Email
- Bei Weiterleitungen jeder beteiligte Anschluß
- Auch Anbieter eines WLAN-Hotspots betroffen (Cafes, Restaurants)
- Nur die Verkehrsdaten, keinen Inhalt

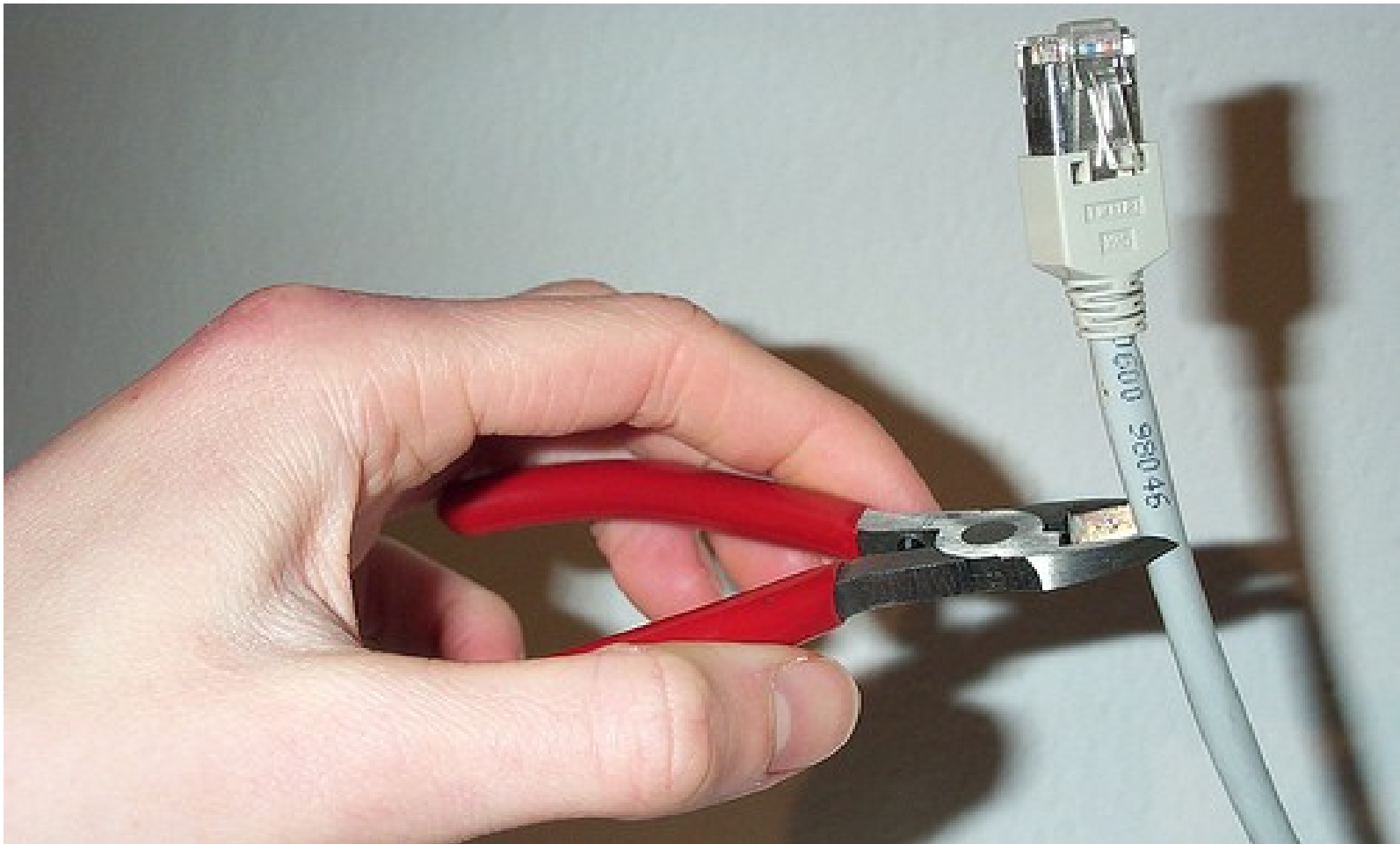
Wie lange wird gespeichert

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?



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?

- 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
- 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)

Vorschläge zu Gegenmaßnahmen

- Münztelefone nutzen
- Briefe schreiben
- Prepaid-Karten nur einmal nutzen, Handys ebenfalls
- Live-CDs
- USB-Sticks mit Daten drauf
- „Zweiter PC im PC“
- Virtualisierung - mit Snapshots

Wahlcomputer

- Wahlcomputer sind rechnergesteuerte Systeme, die bei Wahlen der Abgabe und/oder der Zählung der Wählerstimmen dienen. Im deutschen Wahlrecht werden sie auch als Wahlgeräte bezeichnet.
- Bei Kommunalwahlen kommen auch für die Erfassung und Auszählung von konventionellen Stimmzetteln zunehmend Computersysteme zum Einsatz. Solche Zählsysteme oder Wahlhilfsmittel werden kaum technisch überprüft oder gar auf Manipulationsrisiken untersucht und bedürfen deswegen erhöhter Aufmerksamkeit.

Wahlcomputer (2)

Wie man einen Wahlbetrug erkennt:



Dies ist ein Wahlcomputer



Dies ist ein manipulierter Wahlcomputer

- (Quelle: <https://wahlcomputer.ccc.de>)

Wahlcomputer (3)

- Hauptziel: Einsparung von Geld (weniger Personen müssen die Wahl überwachen)
- Nachteil: Die Erfahrung der letzten Wahlen zeigt dass weder die Wahlverantwortlichen noch die Wähler genau wissen wie die Wahlcomputer zu bedienen sind.
- Alle bisher vorgestellten elektronischen Wahlverfahren geben keine absolute Anonymisierung bei gleichzeitiger korrekten Stimmauszählung her
- Wahlcomputer sind „relativ“ einfach so manipulier- oder abhörbar, dass beides nicht nachzuweisen ist

Wie wird Sicherheit gesehen?

