Die Sinnlosigkeit der Vorratsdatenspeicherung

Nicolas Roeser <nicolas.roeser@ulm.ccc.de>
Michael Feiri <michael.feiri@ulm.ccc.de>
Marcel Linden <marcel.linden@ulm.ccc.de>
Stefan Schlott <stefan.schlott@ulm.ccc.de>

"Sie werden hinnehmen müssen, daß der Gesetzgeber in Sachen Vorratsdatenspeicherung anderer Meinung ist als Sie. (...) Ich wäre für die Vorratsdatenspeicherung auch dann, wenn es überhaupt keinen Terrorismus gäbe."

http://www.abgeordnetenwatch.de/dr_dieter_wiefelspuetz-650-5785--f78879.html#frage78879

Was wird gespeichert?

Verkehrsdaten öffentlich zugänglicher TK-Dienste für Endbenutzer.
Explizit genannt (§ 113 TKG):

- Telefonverbindungen (auch vergebliche Versuche!)
  - Kunde, gerufene Nummer, Uhrzeit, Dauer
  - ...bei Handys zusätzlich der Standort (Funkzellen)
- Verbindungsaufbau mit dem Internet
  - Kunde, zugewiesene IP-Adresse, Uhrzeit, Dauer
- E-Mail-Versand
  - Zeit, Absenderkennung, Absender-IP, Empfängerkennung
- E-Mail-Eingang am Mailserver
  - Zeit, Absender- und Empfängerkennung, IP-Adresse der sendenden TK-Anlage
- E-Mail-Abruf (POP/IMAP/...)
  - Kunde, Zeit
- Analoges gilt für SMS und Fax

...und was ist mit Foren, Jabber, etc.?

- Ich bin kein Anwalt :-)
- In §111 TKG steht:

„Wer **geschäftsmäßig** Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern“

Wie reagieren Kriminelle darauf?

- Gezieltes Umschiffen von Vorschriften

- Kleinkriminelle sind (angeblich) nicht das Ziel der VDS
- Größere kriminelle Organisationen besitzen
  - Ressourcen (Geld, Personen)
  - Know How (oder kaufen selbiges)
  - Kontakte in verschiedene Länder

VDS beim Telefon aushebeln

- Benutze einen Kommunikationsdienst außerhalb der EU
  - Beispielsweise Skype
    - Gibt es sogar für SymbianOS
- Benutze Relays außerhalb der EU
  - VoIP-Relay, per Interface konfigurierbar
  - Asterisk-Server, Ringback, Weiterwahl zum nächsten Telefon
- ...noch komplizierter zu verfolgen:
  - VoIP via Tor (geht das?)
  - Vermischung von POTS- und VoIP-Strecken
  - Statische Relays zu unsicher? Rent-a-Botnet!

VDS bei E-Mail aushebeln

- Was schon vor der VDS gemacht wurde:
  - Mailaccount bei Freemail-Anbieter
  - Login war allen Mittätern bekannt
  - Mails wurden nicht versandt, sondern im Entwurfsordner gespeichert
- Was würde die VDS loggen?
  - Zugriff auf Mailbox von verschiedenen IPs
  - Erst Auflösung der IPs auf Benutzer würde Datenaustausch offenbaren

- Benutze nichtprotokollierte Dienste
  - Eigener Mailserver außerhalb der EU
  - Bulletin-Board-Systems, Web-Foren
  - Store-and-forward von Chat-Diensten

VDS bei E-Mail aushebeln

Prinzip „toter Briefkasten“

- Analog zum Entwurfsordner: Informationen an bekanntem Ort deponieren
  - Mail-Entwurfsordner
  - Webforum
  - Kostenloser Webspace-Anbieter (geocities & Co.)
  - Kostenloser Filesharing-Anbieter
- Schutz gegen Mithörer: Verschlüsselung

- Problem: Protokollierung des Internet-Zugangs
  - Verteilen über Usenet News Network: alt.anonymous.messages
  - Steganographisch einbetten in ein Youtube-Jux-Video

Anonymous Remailers

- Grundlage: „Untraceable electronic mail“ (Chaum, 1981)
- „Onion Routing“, „Mix Routing“:
  - Versand über mehrere Zwischenschritte (Mixe)
  - Mehrfache Verschlüsselung
  - Jeder Mix „entfernt Zwiebelschale“ (Entschlüsseln)
  - Sieht damit nächsten Empfänger

- Padding der Nachricht auf einheitliche Größen
- Zeitliche Korellation verhindern: Sammeln von Nachrichten (Store-and-forward), Verzögern, Burst-Versand
- Versand von Dummy-Nachrichten zwischen Mixen

Populäre Systeme: Mixmaster, Mixminion

Anonymous Remailers

Problem: Antwortadresse

- Absenderadresse muß von den Mixen entfernt (bzw. ersetzt) werden
- Für private Kommunikation: Einfach einbetten
- Für öffentliche Kommunikation:
  - Antwortkette für bestimmte Zeit in Mixen cachen
  - Fertig vorbereitete Mix-Kaskade
  - Bei Mixminion: SURBs (Single Use Reply Blocks)

Praktischer Einsatz: Leider wenig GUI-Unterstützung

- Mixminion: „Actions“ für Sylpheed Claws, Win32-GUI
- Mixmaster: Unterstützung in mutt (und einigen weiteren)