

Vorab ...

Ich vertrete hier eine, nämlich meine, Meinung innerhalb des CCCS. Dies ist keine öffentliche Stellungnahme des CCCS oder gar des CCC.

Über mich

Ganz frisch beim CCCS dabei, seit Anfang 2009.
Fachbereichsübergreifend, eigentlich vom Design kommend, Schwerpunkt Interaktionsdesign

Agenda

- > Die Vorratsdatenspeicherung
- > Der Bundestrojaner
- > Verhalten im Netz / Diskussion

Die Vorratsdatenspeicherung

Seit 1. Januar 2008 in Kraft:

Gesetzliche Verpflichtung der Telekommunikationsanbieter zur Speicherung der entstehenden Verkehrsdaten ihrer Kunden.

Anlasslos, **OHNE** jeglichen Anfangsverdacht

Diese Daten werden bei Bedarf den Strafverfolgungsbehörden, den Polizeibehörden sowie den Nachrichtendiensten zur Verfügung gestellt.

Nachzulesen im **Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen**

Warum wird gespeichert?

Hauptziele:

Die Verbesserung der Aufklärung im Bereich Terrorismus und organisierte Kriminalität, Strafverfolgung von TK-Verbrechen

Zwischenstand:

Anforderung von Daten durch die Polizei von 08/2008 bis 02/2009 in lediglich 0,1 % der Ermittlungsverfahren.
(Quelle: AK Vorratsdatenspeicherung)

Übrigens:

Die Aufklärung von TK-Straftaten war schon vorher enorm hoch und die alten Regelungen absolut ausreichend.

Was wird gespeichert?

WER kommuniziert **WANN (WIE LANGE) MIT WEM** und (beim Handy) **WO?**

> Telefon, Fax, Handy (auch SMS, MMS), Internet, E-Mail

Benutzer-/Geräteerkennung der Verbindungspartner
(Rufnummer, IP-Adresse, IMEI)

Datum, Uhrzeit und Dauer der Verbindung

Handy: auch Funkzellen (Standort)

Wichtig:

Es dürfen **KEINE** Inhalte gespeichert werden!

Wie lange wird gespeichert?

Seit 1. Januar 2008:

Speicherung für 6 Monate von Telefon, Handy, Fax

Seit 1. Januar 2009:

Speicherung für 6 Monate auch von Internet und E-Mail

EU-Richtlinie: min. 6 Monate, max. 2 Jahre, nationale Verlängerungen möglich

Polen erwägt eine Speicherung für **15 Jahre!**

Aber:

Eine Speicherung der Verkehrsdaten nur zur Abrechnung oder auf richterliche Anordnung ist für die Strafverfolgung auch absolut ausreichend.

Kritik

Wirksamkeit der Maßnahme ist mehr als zweifelhaft.

Vorhandene Daten können missbraucht werden und wecken Begehrlichkeiten, Bsp. Urheberrechteverwerter.

Auch ohne Speicherung von Inhalten Erstellung eines genauen Profils möglich (Möglichkeiten wachsen in dem Maße, in dem Telekommunikation zunimmt).

Beeinträchtigung der Arbeit von Journalisten und von regierungs- und staatskritischen Personen/Gruppen

Was macht jemanden verdächtig?

Wie werden die Daten interpretiert?

Eindeutige Zuordnung nicht möglich

Kritik

Schwerer Eingriff in das Grundgesetz (Informationelle Selbstbestimmung und Fernmeldegeheimnis) ist nicht zu rechtfertigen:

Jeder Nutzer von Telekommunikation, also fast jede Bürgerin und jeder Bürger ist davon betroffen:

Generalverdacht anstelle konkreter Verdachtsstufen

Wer mit dem Bewusstsein kommuniziert, dass sein gegenwärtiges wie auch künftiges Kommunikationsverhalten einmal gegen ihn verwendet werden könnte, wird dieses wahrscheinlich dementsprechend ändern:

Konformitätsdruck statt Kreativität + kritischem Denken

Wie geht es weiter ...

Klage vor dem BVerfG:

Ende April 2009 einstweilige Anordnung erneut um 6 Monate verlängert

Speicherung bleibt weiter vorgeschrieben,
Zugriff aber nur bei besonders schweren Straftaten
(Katalog in § 100a StPO)

Pflicht der Bundesregierung zur Vorlage eines Berichtes
über die praktischen Auswirkungen der VDS
(1. März 2009 bis 1. September 2009)

Fragenkatalog an Experten, der vorauss. nach der
Sommerpause verhandelt wird

Die Online-Durchsuchung

Heimlicher staatlicher Zugriff auf informationstechnische Systeme über Kommunikationsnetze

Informationstechnische Systeme:
Computer, PDA, Handy, Router, digitale ABs ...

Zugriff:

Einmalig (Online-Durchsicht) oder über einen längeren Zeitraum (Online-Überwachung), maximal 3 Monate mit Verlängerung auf 6 Monate

> Daten ansehen, kopieren, ausschleusen, auswerten

Stellt einen schweren Eingriff in das GG dar,
lt. BVerfG nur unter strengen Auflagen zulässig

Die Online-Durchsuchung

Ziele:

Erhöhung der Sicherheit z.B. vor internationalem Terrorismus

Möglichkeit, die privaten Computer von Tatverdächtigen zu durchsuchen, um Hinweise auf z.B. kriminelle Netzwerke zu erhalten

Lt. Innenministerium und BKA: höchstens 5 bis 10 Einsätze pro Jahr

Der Bundestrojaner

Das Bundesinnenministerium nennt ihn „Remote Forensic Software“

Technische Voraussetzung für die Online-Durchsuchung

Soll vom BKA individualisiert für das zu observierende System erstellt, eingeschleust und ausgewertet werden

Technische Einzelheiten zum Bundestrojaner bisher nicht bekannt

Vermutete Fähigkeiten: Keylogger, Durchsuchung der Dateien/Dokumente nach Stichwörtern, Passwörtern u.ä.

Wie gelangt er ins System?

Soll entweder voll elektronisch oder aber von Observanten persönlich in der Wohnung, bspw. am Rechner des Tatverdächtigen installiert werden:

- Auf Datenträger im Briefkasten, Bsp. CD/USB-Stick
- Aprilscherz: wird mit Elster ausgeliefert
- Über das Internet, Bsp. Sicherheitsupdates, E-Mail
- Via Handy
- altmodisch: Einbruch in die Wohnung

Auch Firewalls oder Virensoftware schützen nicht!

Kritik

Heimlichkeit als Widerspruch zum Wesen einer rechtsstaatlichen Untersuchungshandlung

Einmal drin, besteht Zugriff auf sämtliche Daten, d.h.: E-Mails, Bank-, Steuer-, Gesundheits-, private Daten ...

Software macht keinen Unterschied, ob etwas zum Kernbereich der Privatsphäre gehört (nach Art. 1 GG geschützt) oder sogar dritten Personen

„Zeitnahe Gefahrenabwehrmaßnahmen“ kaum möglich: RFS technisch aufwändig (maßgeschneiderte Software)

Gefahr des Missbrauchs

Misstrauen in behördliche elektronische Kommunikation

Was kann ich tun?

Telefonzellen

Briefe

Live-CDs für die Bearbeitung sensibler Daten verwenden, bspw. Ubuntu Privacy Remix

Zweitsysteme, Virtuelle Systeme
> unter welchen Voraussetzungen?