

Möglichkeiten des Staates zur Online-Überwachung

J. Glorius P. Sutter

Fachhochschule Furtwangen

12.01.2008

Gliederung

- 1 Worum gehts
- 2 Vorratsdatenspeicherung
 - Was muss gespeichert werden
 - Kundendatenbank
 - Tor
 - Datenaufkommen
- 3 Bundestrojaner
 - Implementierung
 - Zweistufiges Design
 - Erster erfolgreicher Einsatz
- 4 Zitate

Gliederung

- 1 Worum gehts
- 2 Vorratsdatenspeicherung
 - Was muss gespeichert werden
 - Kundendatenbank
 - Tor
 - Datenaufkommen
- 3 Bundestrojaner
 - Implementierung
 - Zweistufiges Design
 - Erster erfolgreicher Einsatz
- 4 Zitate

Was ist Online-Überwachung

- Observieren des Online-Verhaltens
- nur beobachten, nicht eingreifen
(↔ Online-Durchsuchung)
- geheim

Wozu Online-Überwachung

- Terror
- organisierte Kriminalität
- Kinderpornographie?

Gliederung

- 1 Worum gehts
- 2 **Vorratsdatenspeicherung**
 - Was muss gespeichert werden
 - Kundendatenbank
 - Tor
 - Datenaufkommen
- 3 Bundestrojaner
 - Implementierung
 - Zweistufiges Design
 - Erster erfolgreicher Einsatz
- 4 Zitate

Was ist das eigentlich?

- Gesetzliche Verpflichtung der Provider
- zur Speicherung der Verbindungsdaten ihrer Kunden
- über sechs Monate hinweg.

Anbieter von Telefondiensten

- Telefon- oder Identifikationsnummern des Anrufers und Angerufenen
- Start- und Endzeitpunkt des Telefonats, incl. Zeitzone
- Mobilfunk:
 - internationale Kennung von Anrufer und Angerufenem Anschluss und Endgerät (doppel doppel)
 - Funkzellen, insbesondere Daten zur geographischen Lokalisierung und Hauptstrahlrichtung der Funkantenne
 - bei im Voraus bezahlten, anonymen Diensten Zeit und Zelle bei erster Aktivierung (?)
- VoIP: IP von Anrufer und Angerufenem

gilt auch für Versand von SMS/MMS

Email-Provider

- Versand: Email-Adressen von Absender und Empfänger, Sender-IP
- Empfang: Email-Adressen von Absender und Empfänger, IP des letzten Relays
- Mailcheck: Email-Adresse und Abrufer-IP

für alle Punkte zusätzlich Zeitpunkte incl. Zeitzone

Internet-Provider

- dem Internetnutzer zugewiesene IP
- Anschlusskennung
- Zeitpunkte und Zeitzone

Dritte

- Wer die erhobenen Daten verfälscht, muss diese selbst wieder erheben
- Privatpersonen, die WLAN- oder Email-Dienst anbieten

Nicht Betroffene

Anbieter von:

- Webseiten
- Webspaces
- Foren und Chat-Dienste

Rahmenbedingungen

- Einhaltungfrist bis Ende 2008
- Verstoß ist Ordnungswidrigkeit

Einträge

- Rufnummer bzw. Email-Adresse
- Name und Anschrift
- Datum des Vertragsbeginns
- Geburtsdatum
- Anschrift des Anschlusses (Festnetz)

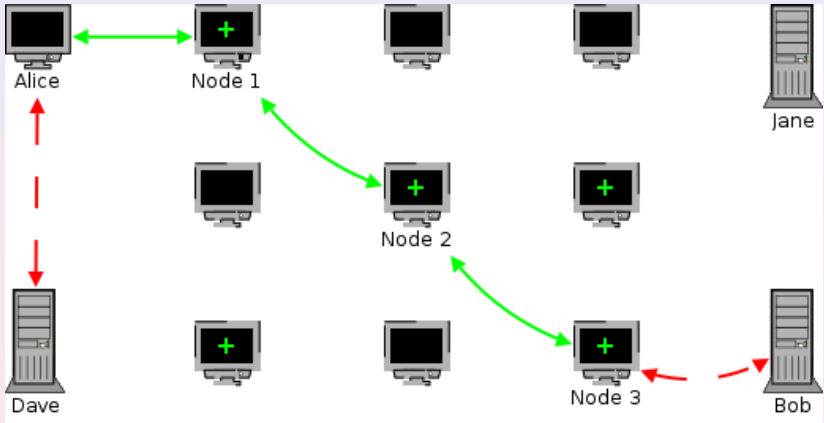
Kurioses

- Email-Anbieter sind von Identifizierungspflicht ausgenommen
- Anbieter ist nicht zur Überprüfung der Daten verpflichtet
- Anbieter sind zu zusätzlichen, individuellen Auskünften verpflichtet:
 - Beispiel: Welcher Kunde hatte dynamische IP XY zum Zeitpunkt Z?
 - Passwörter, PINs, PUKs
 - auch für Verfolgung von Ordnungswidrigkeiten
- Missachtung der Pflicht zur VDS: Strafe bis zu 500'000 Euro und/oder Einstellung des Dienstes (§115 TKG)

Tor

- Anonymisierungsdienst
- lokaler Socks5-Proxy
- verschlüsselte Verbindungen
- nutzt Netz von Freiwilligen

Funktionsweise



Etwas Mathematik

- Email-Provider mit 1000 Kunden
- rufen Emails alle 2 Minuten ab (12h am Tag)
- gespeichert werden: Email-Adresse (30 Zeichen), IP (4 Byte), Zeitpunkt (4 Byte) und Zeitzone (1 Byte)

$$1000 * 30 * 12 * 30 * 6 * (30 + 4 + 4 + 1) = 2,35GiB$$

Etwas mehr Mathematik

- Tor-Server mit 8000 Verbindungen (jederzeit), je 2min Dauer
- Zeit zwischen zwei neuen Verbindungen (im Mittel):
 $120/8000 = 0,015$
- Anzahl Verbindungen an einem Tag:
 $86400/0,015 = 5,76M$
- Datenmenge pro Verbindung:
 $2xIP + 2xTimestamp (2 * 4 + 2 * 4 + 1 = 17)$
 $5760000 * (30 * 6) * 17 \approx 16,8GiB$

Widersprüche

- Verpflichtung zur Einrichtung einer Schnittstelle für Behörden, **die nicht abgehört werden kann**
- Verhältnismäßigkeit der insgesamt hohen Datenaufkommen bei 10-15 Fällen pro Jahr

Gliederung

- 1 Worum gehts
- 2 Vorratsdatenspeicherung
 - Was muss gespeichert werden
 - Kundendatenbank
 - Tor
 - Datenaufkommen
- 3 **Bundestrojaner**
 - Implementierung
 - Zweistufiges Design
 - Erster erfolgreicher Einsatz
- 4 Zitate

Was ist gemeint

- „Remote Forensic Software“
- Mittel zur Verhinderung von Straftaten

Voraussetzungen zur Implementierung

- gesammelte Daten verschlüsseln
- Daten nur so lange wie nötig speichern
- **erst** Ermittlung relevanter Daten, **dann** Übertragung derer
- Einschleusen ohne Hilfe von Providern oder Produzenten

Konzepte

- Herkömmlicher Trojaner
- Präparierte DSL-Router
- USB-Stick

Durchsuchung in zwei Stufen

- Stufe 1:
 - reine Durchsicht der Daten
 - Ermittlung des Status-Quo
 - vergangene Aktivitäten bestimmen
- Stufe 2:
 - Online-Überwachung
 - Protokollierung der Nutzeraktivitäten
 - Erfassung flüchtiger oder verschlüsselter Daten

Der Fall Reda „Gotteskrieger“ Seyam

- Frühjahr 2006: Terrorverdacht
- Geheimdienst BfV schickt ihm Email mit Trojaner im Anhang
- Seyam klickt den Anhang an
- Spähangriff dauert bis 2007
- Funde bei der Online-Durchsuchung:
 - Anleitung zum Bombenbau
 - Bilder von verstümmelten US-Soldaten
- Seyam: „Ich habe einen russischen Virusscanner, der hat damals angeschlagen“

Seyam nutzt seither Internet-Cafés fürs Chatten

Gliederung

- 1 Worum gehts
- 2 Vorratsdatenspeicherung
 - Was muss gespeichert werden
 - Kundendatenbank
 - Tor
 - Datenaufkommen
- 3 Bundestrojaner
 - Implementierung
 - Zweistufiges Design
 - Erster erfolgreicher Einsatz
- 4 Zitate

BKA-Aussagen

- Zur Veränderung des Zielsystems:
jedes Computersystem verändert sich dynamisch, und statische „Urzustände“ sind ohnehin nicht mehr wiederherstellbar
- Online-Durchsuchung dient nicht der Ausspähung von Personen, sondern es werden nur „relevante Erkenntnisse auf informationstechnischen Systemen erhoben“

Es gibt keine wirklich sichere Methode bei der Online-Durchsuchung, auch die Keylogger nicht. Die Dummen wird man mit der Durchsuchung finden, die anderen nicht. Das haben wir heute schon bei der Vorratsdatenspeicherung, mit der Urheberrechtsverletzungen gefunden werden und nicht der einen Anschlag planende Terrorist.

Peter Schaar

Quellen

- Antispy-Spyware:
<http://www.honeynet.org/tools/sebek/>
- Details zur Online-Durchsuchung:
<http://www.heise.de/ct/hintergrund/meldung/94880>
<http://www.heise.de/newsticker/meldung/95010>
- Heise-Artikel zum Fall Reda Seyam:
<http://www.heise.de/newsticker/meldung/101322>
- The Onion Router:
<http://www.torproject.org/>
- Zur Umsetzung der VDS:
<http://de.wikipedia.org/wiki/Vorratsdatenspeicherung>