

Datenschutz heute – wichtiger denn je - vergessener denn je

Ihre Referentin:

Andrea 'Princess' Wardzichowski

Chaos Computer Club Stuttgart /
Haecksen

<princess@bofh.de>, <http://www.querulantin.de/>

Agenda

- 1) Datenschutz heute
- 2) Datenschutz in Webanwendungen /
Betreiberseite

Informationsfreiheitsgesetz

- Historischer Abriß: Volkszählungsurteil
- Informationsfreiheitsgesetz
- 80er Jahre

Datenschutz heute

- Möglichkeiten der EDV (heute: IT) viel größer als in den 80er Jahren
- Chips werden immer kleiner, RFID, Ubiquitous Computing
- Datenschutzbewußtsein hingegen: kaum vorhanden

Datensammlungen im Real Life

- Einwohnermeldeamt (Biometrie!)
- Telekommunikationsanbieter
- GEZ
- Bank
- Versandhändler
- Rabattsysteme (Payback, Happy Digits)

Datensammlungen im Internet

- Webseite
- Blog
- Forenbeiträge / News(Usenet)
- Fotosammlungen
- Online-Communities (Orkut, Qype, StudiVZ, Xing, Lokalisten...)
- Erreichbarkeit per Mobilfunk

Wo ist das Datenschutzbewusstsein hin? (1)

- Jugendliche: Erreichbarkeit, Coolness
- „In der Zukunft wird jeder für 15 Minuten berühmt sein“ (Andy Warhol, 1975)
- Bevölkerungspyramide: ältere Menschen, weniger Beweglichkeit, schlechte Sicht, subjektives Unsicherheitsempfinden, Wunsch nach mehr Überwachung (objektiv aber: Kriminalität rückläufig!)

Wo ist das Datenschutzbewusstsein hin? (2)

- „Bildungsferne Schichten“: egal.
- „...aber ich habe doch nix zu verbergen!“
- „Die DDR ist schon zu lange weg“

Gefahren der Freigiebigkeit bei personenbezogenen Daten

- Werbung (Papier, Spam, Anrufe)
- Stalking
- Arbeitsverhältnisse (Meinungsäußerungen)
- Fotos

=> staatliche und privatwirtschaftliche
Begehrlichkeiten (Musikindustrie!)

Wohin führen staatliche Datensammlungen? (1)

- großer Lauschangriff (Erfolgskontrolle?)
- Mautdaten: nun doch Verwendung für Fahndungszwecke
- Biometrie im Pass
(Foto, ab November 2007 auch Fingerabdrücke).
Wozu? Nicht wegen des 11.9.

Wohin führen staatliche Datensammlungen? (2)

- Videoüberwachung (staatlich und privat) verhindert nichts, verändert aber das Verhalten!
- „Bundestrojaner“
- Vorratsdatenspeicherung

Strafverfolgung vs. Datenschutz (1)

- Strafverfolgung ist wichtig
- Datenschutz ebenso
- Augenmaß auch!
- Erfolgskontrolle findet kaum statt
- Bürgerrechte, Grundgesetz, Demokratie darf nicht ausgehöhlt werden

Strafverfolgung vs. Datenschutz (2)

- Langsame Umkehrung der Rechtslage
- drohender Wegfall der Unschuldsvermutung
- Datenspur hinterlassen um Umschuld zu beweisen?

Wo führt das hin?

„Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird am Ende beides verlieren“

Benjamin Franklin, 1706-1790

..und wenn ich auf der anderen Seite sitze?

Datenschutz in Webanwendungen / Betreiberseite

Datenschutz beim Webanbieter

ACHTUNG: ich bin kein Jurist. Dies sind unverbindliche Hinweise!

Anbieter müssen

- Datensparsamkeit einhalten
- für Datensicherheit sorgen
- für Löschung sorgen
- SSL/https zwingend für personenbezogene Daten
- Bestandsdaten vs. Nutzungsdaten
(Telekom, Amazon, Videothek um die Ecke)

Transparenz (1)

Eine Datenschutzerklärung muß vorliegen, wenn

- permanente Cookies verwendet werden
- IP-Adressen gespeichert werden
(Hochschulbereich: oft feste Adressen!)

Logauszug:

```
p57AAF687.dip.t-dialin.net - - [24/Oct/2007:22:48:12 +0200] "GET /index.html HTTP/1.1" 304 -  
"http://www.querulantin.de./Querulierungen/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; (R1 1.5); .NET CLR  
1.1.4322)"  
p57AAF687.dip.t-dialin.net - - [24/Oct/2007:22:48:14 +0200] "GET /Vortraege HTTP/1.1" 301 368  
"http://www.querulantin.de./index.html" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; (R1 1.5); .NET CLR  
1.1.4322)"
```

Transparenz (2)

- Externe Links müssen gekennzeichnet werden
- Impressum: ladungsfähige Adresse (kein Postfach)
- Verfahrensverzeichnis (Vorabkontrolle, Sicherheitskonzept, in einigen Bundesländern vorgeschrieben)

Sichere Programmierung

- JEDEN Input verifizieren
(Inhalt, Länge, Sonderzeichen)
- Postparameter, nicht per GET auf der URL-Zeile übergeben
- auf Cookies achten
- Referrer
- versteckte Variablen

Eigener Webserver

- sichere Config. Google hilft. Die LUG um die Ecke auch. Das Systemhaus von nebenan auch.
- Ports / Dienste schließen
- eigener User für Server und Datenbank, Rechte setzen
- php.ini ansehen
- updaten und patchen nicht vergessen!
- Private Blogs / Foren:
- Gefahr, als „Mitstörer“ belangt zu werden. Bei längerem Urlaub evtl. schließen.

Was ist zu tun, um die Welt zu retten?

Gehet hinaus und seid in Eurem Dunstkreis wachsam, infiltriert Euer Umfeld!

Bißchen Paranoia schadet nix.

Und auch wenn man nicht paranoid ist, heißt das nicht, daß sie NICHT hinter Euch hersind...