IT-Sicherheit

- Sicherheit vernetzter Systeme -

Kapitel 17: Datenschutz

Inhalt

1. Persönlichkeitsrechte und Datenschutz
2. Wie kommen Daten ins Netz ?
3. Wer besitzt Daten von mir ?
4. Wo entstehen Datenspuren ?
   - 4.1.Cookies
   - 4.2.Techniken zur Erstellung von Profilen
   - 4.3. Serverseitige Spuren
   - 4.4.HTTP-Header
5. Schutzmaßnahmen beim Surfen
6. Beispiele aus der Praxis: Probleme beim Datenschutz

Persönlichkeitsrechte und Datenschutz

- Allgemeine Persönlichkeitsrechte
  - Art. 1 Grundgesetz: „Würde des Menschen ist unantastbar“
  - Art. 2 Grundgesetz: „freie Entfaltung der Persönlichkeit“ ... „Recht auf Leben und körperliche Unversehrtheit“
- Daraus wird Recht auf informationelle Selbstbestimmung abgeleitet
  - Selbstbestimmung über
    - Preisgabe und
    - Verwendung personenbezogener Daten
- Personenbezogene Daten (Bundesdatenschutzgesetz BDSG)
  - „Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person“ (§ 3 Abs. 1 BDSG)
  - Besonders schutzbedürftige Daten: „rassische und ethische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“ (§3 Abs. 9)

Historischer Rückblick: Volkszählung 1983 / 1987

- Geplante Volkszählung April bis Mai 1983
  - Totalerhebung
  - Registerabgleich erschien zu fehleranfällig, deshalb „Kopfzählung“
  - Zusätzliche Informationen zu Lebens- und Arbeitsverhältnissen
  - Fragebogen über Google Books („Volkszählungsfragebogen 1983“)
- Erhebliche Bürgerproteste (Gefahr des „gläsernen Bürgers“)
- Verfassungsbeschwerde
- Volkszählungsurteil
  - Grundrecht der informationellen Selbstbestimmung
  - „Meilenstein des Datenschutzes“
- Volkszählung wurde in veränderter Form 1987 durchgeführt

➡ Daten, die 1983 absolut strittig waren, werden heute von vielen freiwillig ins Internet gestellt (Stichwort: soziale Netze, Networking, Geschäftskontaktmanagement)

Wie kommen persönliche Daten ins Netz?

- Durch mich selbst:
  - Bewusst
    - Private Webseite
    - Soziale Netzwerke, Kommentare, Guestbooks, ...
    - ....
  - Unbewusst
    - Mail an Verteiler mit Webarchiv
    - Datenspuren bei der Dienstnutzung
    - Personalisierung von Diensten (z.B. google)
    - ....
- Freunde, Bekannte
- Schule, Universität, Verein, Arbeitgeber, usw.
- (Personen-) Suchmaschinen
- .....

Wer besitzt persönliche Daten von mir?

- Öffentliche Einrichtungen:
  - Gemeindeverwaltung (Meldeamt, Passamt)
  - Finanzamt (Steuererklärung)
  - Polizei, Staatsanwalt, Verfassungsschutz (Ermittlungsverfahren)
- Private Einrichtungen und Unternehmen:
  - Krankenkassen und sonstige Versicherungen, Banken
  - Schufa (Schutzgemeinschaft für allgemeine Kreditsicherung)
  - Handels- und Wirtschaftsauskunfteien
  - Telekommunikationsunternehmen (Telefon, Handy, DSL,....)
  - Online-Shops; Betreiber von Web-Seiten; Google, ...
  - Adresshändler
  - ..... ?
- Mögliche Gefahren
  - ➡ Verknüpfung von Daten aus unterschiedlich(st)en Quellen
  - ➡ Möglichkeiten der Profilbildung (Räumlich, zeitlich, Verhalten, Vorlieben, Kaufverhalten, Interessen, ...) u. deren (kommerzielle) Nutzung

Wo entstehen Datenspuren?

- Auf eigenem Rechner:
  - Adressen besuchter Seiten (History des Browsers)
  - Inhalte (Cache)
  - Inhalte von Web-Formularen (Passwörter, Nutzernamen, Adresse,....)
  - Cookies
- Beim Provider
  - Zuordnung Anschluss zu IP-Adresse
  - Zeitpunkt und -dauer der Nutzung
  - Adressen und Inhalte der gesamten Kommunikation
- Beim Inhalteanbieter
  - Zeitpunkt und -dauer
  - Abgerufene Seiten
  - IP-Adresse, Browser, Betriebssystem, ... und vieles andere mehr

➡ Gefahr der Profilbildung

Grundsatz der Datensparsamkeit

- Bei jeder Dienstnutzung fallen Profildaten an
  - Internet-Radio
  - Video on Demand
  - Zeitungen online
  - Online-Shops
  - Suchmaschinen, personalisierte Suchmaschinen
  - New-Portale
  - Location-based Services
- Primary-Key: IP-Adresse, Account, Geräte-ID, Cookie,.....
- Internet kennt keine „Gnade des Vergessens“
- Keine Sicherheit über Datenverwendung
- Tendenz zur „Vorratsspeicherung“
- Verwendung der Daten für einen „anderen Zweck“
- Verknüpfung mit anderen Datenbeständen

Bsp.: Cookies

- Datenbank speichert Datum beschränkte Zeit
  - Austausch von Informationen zwischen Computerprogrammen
- Bsp. HTTP-Cookie
  - Wird vom Server erzeugt
  - Zum Client übertragen und dort gespeichert
  - Werden transparent dem Server zur Verfügung gestellt
- Nutzungsbeispiele:
  - Session Management
  - Identifizierung des Surfers
  - Persönliche Einstellungen (z.B. iGoogle)
  - Erstellung von Bewegungs- und Nutzungsprofilen
  - Benutzerangepasste „Empfehlungen“ und Werbung (z.B. Amazon)

Cookies: Datenstruktur

- Cookie besteht aus
  - Name und Wert
  - Version
  - optionalen Attributen:
    - Expires
    - Max-Age
    - Domain
    - Path
    - Comment
    - Secure
    - ...
    - Daten

Erstellung von Profilen

- Third-Party- oder Tracking-Cookies
  - Inhalt einer Web-Seite kann auf andere Server verweisen
    - z.B. Werbebanner
    - 1x1 Pixel große Bilder (Web Bugs) o.ä.
  - Falls Cookie gesetzt ist, wird dies zum Server übertragen, dort geändert und zurückgeschickt
- HTTP-Referrer-Feld enthält Adresse der aufrufenden Seite
- Individualisierte URLs (www.myshop.de/?id=a348ksldksfj)
- Spuren in den Webserver-Logs

➡ Mit diesen einfachen Techniken ist ein Tracking des Benutzers möglich

Informationen aus Serverlogs

- Aufrufende IP-Adresse
- Verlangte URL
- Informationen über den Browser
  - Hersteller
  - Betriebssystem
  - Versionen
  - MIME-Types
  - ....
- Datum, Uhrzeit, Zeitzone
- .....

- Welche Informationen liefert ein Broswer; Test-Seite: http://browserspy.dk

Bsp. Google Analytics (GA)

- Kostenloser Dienst zur Analyse von Nutzerverhalten
- Detaillierte Statistiken
  - Herkunft der Besucher
  - Tracking durch Referrer (Suchmaschinen, Ads, pay-per-click networks, ...)
  - Verweildauer
  - Suchbegriffe
  - Verknüpfung mit Google AdWords
- Funktionsweise:
  - GATC (Google Analytics Tracking Code) auf jeder Seite, lädt
  - Javascript vom Google-Webserver (ga.js)
  - Sammelt Daten über den Besucher und sendet diese an Google-Server
  - Insbesonder IP-Adresse
- Bayerischer Datenschutzbeauftragter; 24. Tätigkeitsbericht
  - GA verstößt ohne ausdrückliche Einwilligung gegen Telemediengesetz
  - GA darf von Bayerischen Behörden nicht mehr verwendet werden

TomTom

- HD-Traffic
  - Top-aktuelle Verkehrsinformationen über Staus, Behinderungen, Verzögerungszeiten, Vorschläge für Alternativrouten
  - HD-Traffic Gerät liefert Informationen an TomTom-Server
    - Geschwindigkeit, Postion, Streckeninformationen, usw.
    - Je mehr HD-Nutzer desto besser die Vorhersagen
  - Informationen werden zum Teil auch Offline an TomTom übermittelt (TomTom Home)
  - Daten werden lt. TomTom anonym in Datenbank gespeichert
- Mit den Daten lassen sich Verkehrsprofile erstellen
- TomTom verkaufte Daten an Niederländische Behörden
  - Ziel: Finden von Verkehrsengpässen
  - Einleitung neuer Bauvorhaben
  - Mit den Daten sind aber auch „Raser-Schwerpunkte“ erkennbar
  - An diesen Hot-Spots wurden dann verstärkt Radarkontrollen durchgeführt

Mobilfunk: Verkehrsdaten

- Diskussion über Vorratsdatenspeicherung
- Malte Spitz (Grüne) verklagt 2009 Telekom auf Herausgabe von über ihn gespeicherte Vorratsdaten
- Er erhält Daten vom August 2009 bis Februar 2010
  - Nummern der Angerufenen bzw. Anrufer wurden von der Telekom aus dem Datensatz entfernt
  - Spitz übermittelt diese Daten an die Zeitung „Die Zeit“
  - Veröffentlicht (zum Teil geschwärzt) auf Google Docs https://docs.google.com/spreadsheet/ccc?authkey=COCjw-kG&key=0An0YnoiCbFHGdGp3WnJkbE4xWTdDTVV0ZDlQeWZmSXc&hl=en_GB&authkey=COCjw-kG#gid=0

Verkehrsdaten Spitz; Auszug

Beginn	Ende	Dienst	ein/ ausgehend	Laenge	Breite	Richtung	Cell-Id_A	Cell-Id_B
8/31/09 7:57	8/31/09 8:09	GPRS	ausgehend	13.39611111	52.52944444	30	45830	XXXXXXXXX
8/31/09 8:09	8/31/09 8:09	GPRS	ausgehend	13.38361111	52.53	240	59015	XXXXXXXXX
8/31/09 8:09	8/31/09 8:15	GPRS	ausgehend	13.37472222	52.53027778	120	1845	XXXXXXXXX
8/31/09 8:15	8/31/09 8:39	GPRS	ausgehend	13.37472222	52.53027778	120	1845	XXXXXXXXX
8/31/09 8:20			ausgehend					XXXXXXXXX
8/31/09 8:20		SMS	ausgehend	13.38361111	52.53	240	9215	XXXXXXXXX
8/31/09 8:39	8/31/09 9:09	GPRS	ausgehend	13.37472222	52.53027778	120	1845	XXXXXXXXX
8/31/09 9:09	8/31/09 9:39	GPRS	ausgehend	13.37472222	52.53027778	120	1845	XXXXXXXXX
8/31/09 9:12	8/31/09 9:12	Telefonie	ausgehend	13.37472222	52.53027778	120	1845	XXXXXXXXX

- Insgesamt 35.831 Datensätze (Zeilen)

Verkehrsdaten Spitz

Beginn	Ende	Dienst	ein/ ausgehend	Laenge	Breite	Richtung	Cell-Id_A	Cell-Id_B
8/31/09 7:57	8/31/09 8:09	GPRS	ausgehend	13.39611111	52.52944444	30	45830	XXXXXXXXX

- Koordinaten der Basisstation
- Richtung
  - Sendemasten hat i.d.R. 3 Segement-Antennen die je 120 Grad abdecken
  - Richtung in den Daten: Grad-Angabe des Handy relativ zur Basisstation
  - Entfernung zur Basisstation wird nicht ermittelt / gespeichert
  - Größe der Funkzelle als obere Schranke für max. Entfernung
  - Mobilfunkantennen-Atlas: http://emf2.bundesnetzagentur.de/karte.html
- Cell-ID: Eindeutige ID der Basisstation
  - Cell-ID_A: ID der Basisstation von Spitz
  - Cell-ID_B: ID der Basisstation des Kommunikationspartners (geschwärzt)

Datenauswertung

- „Die Zeit“ nutzt diese Daten und weitere öffentlich zugängliche Info (Twitter, Blogs, Webseiten) zur Erstellung einer interaktiven Karte:
  http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten
- Bis auf wenige Lücken nahezu vollständiges Bewegungsprofil
- Genaue Analyse des Kommunikationsverhalten möglich
- Ableitung von Gewohnheiten und Vorlieben
- Erstellung einer Heatmap (wo hält er sich am häufigsten auf)
- Wie und wann reist er
  - 300 km/h -> ICE
  - 700 km/h -> Flugzeug
- Durchschnittliche Gesprächsdauer
- .....
- Handy war und wird kaum noch ausgeschaltet!

Mobilfunk Verkehrsdaten

- Spitz veröffentlicht nicht alle Felder der Daten
- Sehr viel weitere Info beim Provider vorhanden und an Spitz übermittelt:
  - IMSI beider Seiten (eindeutige Kennung der SIM)
  - IMEI beider Seiten (eindeutige Gerätekennung)
  - IP-Adresse (privat; netzintern)
  - IP-Adresse (öffentlich)
  - Ports (derzeit nicht gespeichert)
  - Access Point Name (APN)
  - HotSpot-Kennung

Gutachten zur Vorratsdatenspeicherung und Aufklärungsrate

- Justizministerium gibt Gutachten in Auftrag: Vorratsdatenspeicherung (VDS) von essenzieller Bedeutung für Strafverfolgung?
- 27.01.12 Veröffentlichung; Quelle: http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/20120127_MPI_Gutachten_VDS_Langfassung.pdf?__blob=publicationFile
- „Fehlen (der VDS) ist nicht mit sichtbaren Unterschieden der Sicherheitslage verbunden“
- Verkehrsdaten spielen nur in Verbindung mit anderen Ermittlungsmethoden eine Rolle
- Max Stadler, Staatssekretär: Notwendigkeit VDS empirisch nicht belegt

iPhone Tracker

- IOS 4 speichert regelmäßig Zeitstempel und Geodaten in eine Datenbank
- Dämon locationd schreibt in consolidated.db (unverschlüsselt)
- Datenbank wird bei der Sicherung unverschlüsselt auf Rechner abgelegt
- Geo-Info über WLAN- und Mobilfunkzellen nicht über GPS
- 20.04.11: Pete Warden und Alasdair Allen veröffentlichen iPhone Tracker
  - Software liest consolidated.db aus Backup aus
  - Stellt Geodaten auf Karte mit Zeitleiste dar
- Apple nimmt Stellung
  - gesteht Fehler ein
  - berichtet über Aufbau einer Verkehrsdatenbank für Staumeldungen

iPhone Tracker

- 5.5.11: IOS 4.3.3 „behebt den Software-Fehler“
  - Cache Größe wir reduziert
  - Geodaten nicht mehr im Backup
  - „in nächstem Release wird DB verschlüsselt auf iPhone gespeichert“
- Viele Apps nutzen Ortungsdienst
- Apps können Daten an Server übertragen
- Oft unklar welche Daten übertragen und wie genutzt werden
  - eindeutige Device-ID (UUID)
  - Koordinaten
  - Funkzelle
- Daten werden auch an Advertising-Netzwerke geschickt
- Analyse der „beliebtesten iPhone-Apps“ auf Übertragung der UUID:
  - http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf

Soziale Netzwerke / Suchmaschinen

- Facebook Gesichtserkennung
- Timeline: „Erzähle deine Lebensgeschichte“
- Alle Daten gespeichert und in Timeline zur Verfügung gestellt
- Änderung der Nutzungsbedingungen:
  - Timeline kann nicht deaktiviert werden
  - Zugriff auf Timeline kann eingeschränkt werden
- Google ändert Nutzungsbedingungen für personalisierte Dienste zum 1.3.12
  - „Google kennt Kalender, Standort, Verkehrslage und weist auf alternativen Weg hin“
  - Daten werden zwischen alle Anwendungen verknüpft
  - Betrifft auch Mobile Geräte unter Android
  - Nutzung auch für „Nutzer-relevante Werbung“
  - Daten werden Dritten nicht zur Verfügung gestellt
- Wie halten die Unternehmen es mit dem Datenschutz?

Schlussfolgerungen

- Nutzung vieler kostenloser Dienste „bezahlt“ man mit seinen Daten
- Tendenz zur zunehmenden Verknüpfung von Daten, um „Dienst zu verbessern“
- Vielfach nicht klar welche Daten gespeichert werden
- Vielfach kein „Recht auf Löschung“
- Datenschutzgesetze (Rahmengesetzgebung) gelten nur in Deutschland

- Nutzer sollte Grundsatz der Datensparsamkeit berücksichtigen