Stammtisch Kleinreferat Nr.1 09.12.09

Thema: Selbstdatenschutz im Internet

Unter **Selbstdatenschutz** versteht man die durch den Einzelnen zum Schutz seines Rechts auf informationelle Selbstbestimmung ergriffenen technischen, organisatorischen und rechtlichen Maßnahmen. Dazu werden bisher in erster Linie Verhaltensweisen des Einzelnen gezählt, möglichst wenig Ansatzpunkte für eine Erhebung seiner Daten zu bieten. Selbstdatenschutz bedeutet, die Gefahren hinsichtlich Datenschutz und Datensicherheit kennenzulernen und selbst aktiv Gegenmaßnahmen zu ergreifen. Von: http://de.wikipedia.org/wiki/Selbstdatenschutz

Einleitung:

Daten sind die „Ware“ des Informationszeitalters. Auch wenn das solitäre Sitzen vor dem PC das Gefühl gibt, ist das Internet kein Ort der Anonymität und Privatheit.

Die von so vielen geschätzte „Kostenloskultur“ basiert vor allem auf der „Ware“ Daten, denn diese können zum Zwecke der personalisierten Werbung zu guten Preisen verkauft werden.

Es stellt sich also die Frage jedes Menschen an sich selbst:

Was will ich, dass die Welt über mich weiß?

Probleme:

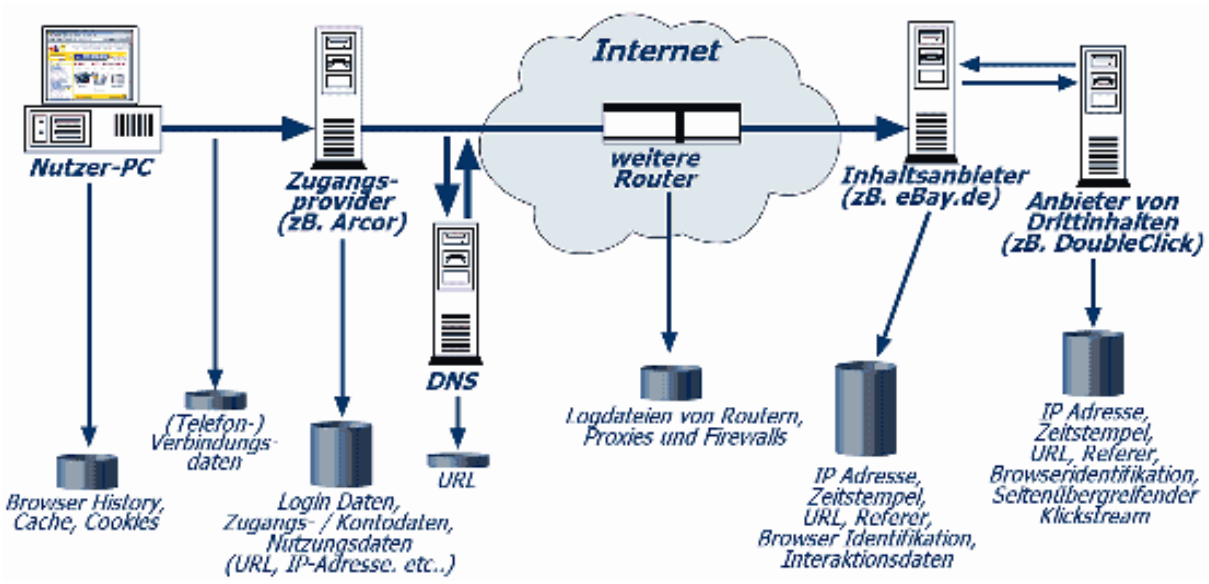
- ➔ Persönlichkeitsschutz: Was denkt man über mich? Wofür hält man mich?
- ➔ Schutz der Privatsphäre: Wer weiß, was ich wann, wo, mit wem, warum tue?
- ➔ Daten können in oder gegen meinem Interesse benutzt werden
  „Könnte es mir schaden, wenn jemand etwas über mich weiß?“

Wirklich geschehen: Arbeitssuchende wurden bei Bewerbungsgesprächen abgewiesen, da im Internet/sozialen Netzwerken Fotos von Akoholexzessen abrufbar waren.

Problem:

„Das Internet vergisst nichts“ (schwierig, aber wohl wahr) und Suchmaschinen und spezialisierte Datendienste erleichtern jedem die Suche nach relevanten Informationen

Das Internet nimmt auch im „Normalzustand“ viele Informationen auf



Von https://www.datenschutzzentrum.de/selbstdatenschutz/internet/datenspuren.htm

Schwierig wird es, wenn Daten gezielt gesammelt/gefangen werden, um mit ihnen weitergehende Tagen zu betreiben (Handel, Erpressung, Diebstahl, Betrug, etc.)

Was kann man tun?

- ➔ Datensparsamkeit: Überlegen, welche Informationen man im Internet oder im öffentlichen Leben preisgibt; Vorsicht im Alltag: Informationen werden nicht nur auf elektronischem Weg abgefragt:
  Potentielle Quellen (und Art der Daten) für Datensammler können sein:
  - Preisausschreiben (Namen, Adressen),
  - (Telefon/Internet)Umfragen,
  - Vertragsdaten (falls der Vertragspartner nicht ausdrücklich in den AGBs den Datenverkauf ausschließt; Namen, Adressen, Kaufgewohnheiten),
  - Rabatt und Bonuskarten (Namen, Adressen, Kaufgewohnheiten)
  - **Soziale Netzwerke** (Namen, Adressen, Vorlieben u.a. persönliche Informationen)
  - Einträge in Foren, Blogs, etc. (potenziell missliebige Aussagen etc.)
  - Behörden (dieser Weitergabe kann widersprochen werden (http://www.optoutday.de/)

  Diese Informationen können von vielen gelesen, aber nur mit Aufwand gesammelt und verknüpft werden. Allerdings sind sie sehr wertvoll für die Werbung. Falls Informationen existieren, die man lieber verschweigen möchte, versuchen Betreiber anzuschreiben. Auf Informationsfreiheitsgesetz oder Grundrecht auf informationelle Selbstbestimmung berufen, Robinsonlisten nutzen (https://www.robinsonliste.de/, http://de.wikipedia.org/wiki/Robinsonlisten)

- ➔ Anonymität Pflegen:
  - Anonymisierungsdienste, Proxyserver nutzen,
  - Pseudonyme benutzen,
  - Nie alle relevanten Daten an einer Stelle zusammen aufschreiben (verhindert Querverbindungen),
  - Verschlüsselungssoftware benutzen,
  - Cookies ausschalten (Benutzerprofile können erstellte werden),
  - Wegwerfemailadressen nutzen (z.B. http://sofort-mail.de/ oder andere Dienste),
  - Mehrere Emailadressen nutzen,
  - Regelmäßig selbst googlen, kontrollieren was gefunden werden kann, Daten ggf. zu löschen versuchen.

  Dies dient dem generellen Schutz vor Datensammlungsvorgängen. Die Daten sind allerdings zumeist nur für Statistiken interessant. Bei persönlich auf eine Person gerichteten Angriffen können diese Daten aber über Suchmaschinen zusammengetragen und Profile erstellte werden.

➔ Wehren gegen Illegale Formen der Datenbeschaffung:

- Aktueller Virenscanner und Firewall am eigenen PC + Überprüfung auf unerlaubt nach draußen telefonierende Programme schützen
- Sichere Passwörter benutzen (Nicht zu kurz, keine echten Wörter, möglichst viele Zeichen groß/klein/Sonder/Zahlen durcheinander)
- Cookies ausschalten (soweit möglich)
- An fremden Rechnern Daten von persönlichen Konten (Email, Onlinebanking, etc.) nur eingeben, wenn der Rechner vertrauenswürdig ist. (Keylogger u.a.) Offene oder öffentlich mit nutzbare WLAN Netze sind zumeist nicht oder nicht genug gesichert.
- Daten auf Servern von Sozialen Netzwerken liegen zentral, diese Server sind lohnende Ziele für Hacker -> keine Daten dort eintragen.
- Keine Links in Mails nutzen -> Phishing-Gefahr (http://de.wikipedia.org/wiki/Phishing),
- Keine Passwörter auf nicht vertrauenswürdigen Seiten oder in Programmen eingeben, die diese an die eigentlichen Server weiterleiten (wollen) – manche ziehen auch eine Kopie,
- Bei Benutzung von Sicherheitsrelevanten Daten auf Adresszeile Achten. Statt http:// sollte dort http**s**:// stehen. Diese Kommunikation ist verschlüsselt.

Tipps:

Soziale Netzwerke: Niemals Klarnamen verwenden. Auch wenn der Betreiber dies so verlangt, nach Paragraph §13, Abs.6 des Telemediengesetzes (TMG) sind Anbieter verpflichtet eine Nutzung ihrer Dienste unter Pseudonym zu ermöglichen!! http://bundesrecht.juris.de/tmg/__13.html

Schlussbemerkung:

Eine Verantwortungsbewusste Nutzung des Internets bleibt natürlich jedem selbst überlassen. Wer seine Daten preisgeben möchte kann dies tun. Auch muss dies ihm nicht automatisch zum Nachteil gereichen. Allerdings sollte diese Entscheidung bewusst und mit dem Wissen um die Gefahren getroffen werden. Problematisch ist es, wenn Daten aber ohne Wissen der Person gesammelt und genutzt werden. Im harmlosen aber nervigen, wohl aber am häufigsten anzutreffenden Fall, werden diese Daten nur für Werbung genutzt. Allerdings kann es beispielsweise auch geschehen, dass Personen mit Informationen aus ihrer Vergangenheit konfrontiert werden, was ihnen zum Nachteil gereicht, wenn diese im Internet weiterhin verfügbar sind. Über die juristisch klar strafbaren Handlungen (gestohlene/ausgespähte/geratene Passwörter oder Anderes) können auch spürbare wirtschaftliche Schäden entstehen. Um diesen negativen Auswirkungen zu entgehen, ist eine Beschäftigung mit der Frage des Datenschutzes und der Internetsicherheit für jeden, nicht nur Internetnutzer, wichtig. Aktualisierte Virensoftware und Firewalls sowie sichere Browser (v.a. aktuell) sollten selbstverständlich sein.

Links:

1.) Der Sächsische Datenschutzbeauftragte, Broschüre zum Datenschutz in Sozialen Netzwerken:

„Ich suche Dich. Wer bist Du?“

http://www.saechsdsb.de/datenschutz-fuer-buerger/369-selbstdatenschutz-in-sozialen-netzwerken

2.) HANSEN, Marit; KRAUSE, Christian:

„Selbstdatenschutz – Sicherheit im Eigenbau“

http://www.bpb.de/files/FRSFFH.pdf

3.) Stern, Zehn Tipps zum Selbst-Datenschutz:

http://www.stern.de/digital/online/soziale-netzwerke-zehn-tipps-zum-selbst-datenschutz-651840.html

4.) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein:
Selbst Sichern – Sicher Surfen im Internet

https://www.datenschutzzentrum.de/selbstdatenschutz/index.htm

5.) Virtuelles Datenschutzbüro

http://www.datenschutz.de/

Sonstige Links:

http://www.optoutday.de/

https://www.robinsonliste.de/

http://de.wikipedia.org/wiki/Robinsonlisten

http://www.ichhabediewahl.de/?cid=39 (Robinsonliste)

http://infodatenschutzblog.com/

http://www.datenschutz.de/info-material/selbsthilfe/