Einführung in die Informationstechnik

FORTSETZUNG SCHADSOFT-WARE UND SCHUTZ

veraltet: Dialer

- Programme, die unbemerkt die Einwahl ins Internet übernehmen
  - meist über so genannte Mehrwertdienst-Nummern
    - 0190 – mittlerweile verboten, 0137, 118x, oder Ausland
- funktionieren nicht bei DSL
- ersetzen die „normale Einwahl“ unbemerkt
- als Schadsoftware aber noch üblich

Andere Formen des Missbrauchs

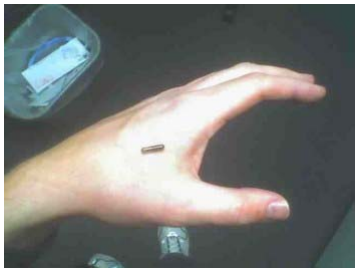
- Podslurping: Nutzung von USB-Sticks, IPods, oä. Massenspeichern zum Datenklau
  - Prinzip: Schlürfen am Rechner
    - Nutzen der Autostart-Funktion zum Starten von Software, die „interessante“ Daten auf den Stick kopiert
- Snarfing: Angriffe auf Drahtlosgeräte (WLAN), Bluesnarfing (Bluetooth)
- Bluejacking

Abzocke

- Nutzung von Kontaktdaten im Netz zur Zustellung von Rechnungen
- Datenermittlung durch dubiose Angebote im Netz
  - Beispiele: Berechnung des zu erwartenden Lebensalters, Senkung des Energieverbrauchs,
- oder: Nutzung erschlichener Kontaktdaten
- oft unter Vortäuschung eines seriösen Absenders wie Single.de, Web.de, etc.

Überwachung allgemein

- Spuren im Internet: Internetprovider speichert Verbindungsdaten
- Handy:
  - wer wen wie lange anruft wird 2 Jahre gespeichert
  - Positionsbestimmung problemlos möglich
- Videoüberwachung: öffentliche Plätze, Bus & Bahn
- Auto: Blackbox, Telemetrie
- Reisen: Flugbuchungen
- Rabattkarten, Kreditkarten
- RFID-Chips: für Waren, Tiere, Menschen



RFID

http://de.wikipedia.org/w/index.php?title=Datei:134_2khz_rfid_animal_tag.jpg&filetimestamp=20100108234403

Wireless LAN

- Gefahren:
  - Fremdnutzung des eigenen WLANs
  - Mithören des WLAN-Verkehrs
- Sicherheitstipps:
  - WLAN nur bei Gebrauch einschalten
  - Verschlüsselte Verbindung aktivieren
  - Nur öffentlicher Hotspots mit sicherer Verschlüsselung verwenden
  - Eigenen WLAN Hotspot nicht über WLAN konfigurieren

Schutzmaßnahmen, BSI empfiehlt:

1. Installation eines Virenschutzprogramms – regelmäßige Aktualisierung
2. (Personal) Firewall installieren und aktualisieren
3. Sicherheitsupdates für Betriebssystem und andere Software durchführen
4. nicht als Administrator arbeiten
5. Zugangsdaten unter Verschluss halten
6. Email-Anhänge nicht bedenkenlos öffnen
7. Downloads überprüfen (Quelle vertrauenswürdig?, gefälscht?)
8. keine persönlichen Daten weitergeben
9. Verschlüsselung der Kommunikation (WLAN, VoIP, Email)
10. Sichungskopien

Datensicherung

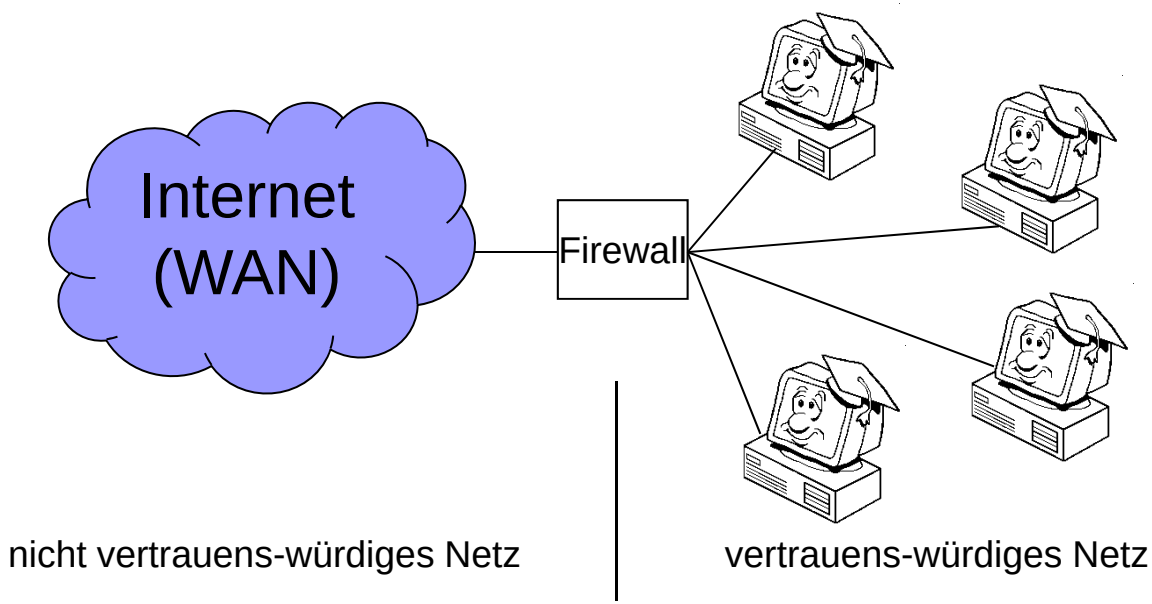
- Auslagerung von Daten auf sichere Datenträger
  - Vorsicht bei mobilen Datenträgern
- Backup
  - vollständig
  - Inkrementell
  - Software:
    - ab Windows Vista Bestandteil von Windows
    - alternativ: Personal Backup
- Prioritäten bei Sicherung:
  1. Sicherung von Anwendungsdaten
  2. Betriebssystem und Anwendungen

Virenschutzprogramme

- durchsuchen Speicher nach Viren
- zwei Betriebsarten:
  - transient: durch den Benutzer gestartet, läuft nur auf Anweisung
  - resident: mit dem Rechner gestartet, läuft permanent im Hintergrund
- wird Virus gefunden $\rightarrow$ Sperrung/Löschung der betreffenden Datei
- Software für Windows: bspw. Microsoft Security Essentials

Firewall

- auch Sicherheitsgateway genannt – eigenständige Netzwerkkomponente
- untersucht die Datenpakete - Filter
- unterbindet unerlaubte Zugriffe auf sicheres Netz und umgekehrt

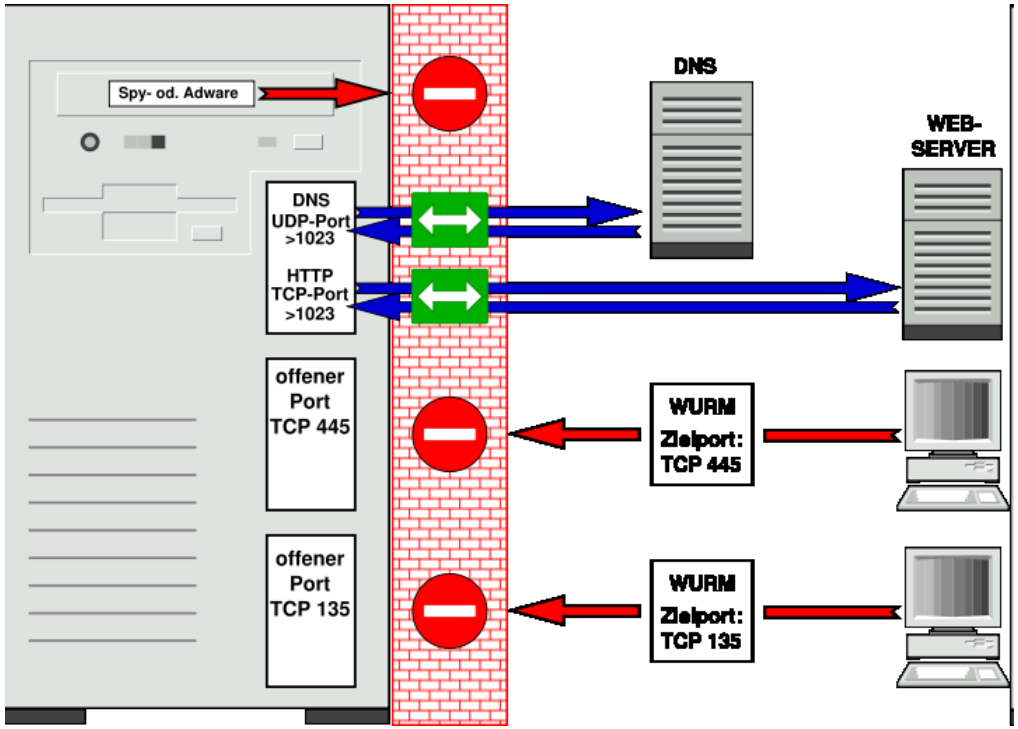


Firewall – Technologien

- **Paketfilter:** verwirft oder lässt Pakete passieren - zum Beispiel Untersuchung Quell- und Zieladresse, Port
  - ganze IP-Bereiche können gesperrt werden
- **Content Filter**:überprüft Inhalt von Paketen
  - Filtert: aktive Inhalte, Spam, Viren,
- **Intrusion Prevention**: sperren von Ports
- **Firewall Policy**: Regeln für das Verhalten einer Firewall

Personal Firewall

- nicht zwischen Netzwerken sondern zwischen Computer und „Außenwelt“
- kontrolliert Zugriffe von außen und von innen
- IDS/IPS
- Paketfilter
- beobachtet Programme
  - Schutz vor Angriffen von innen
- lernfähig



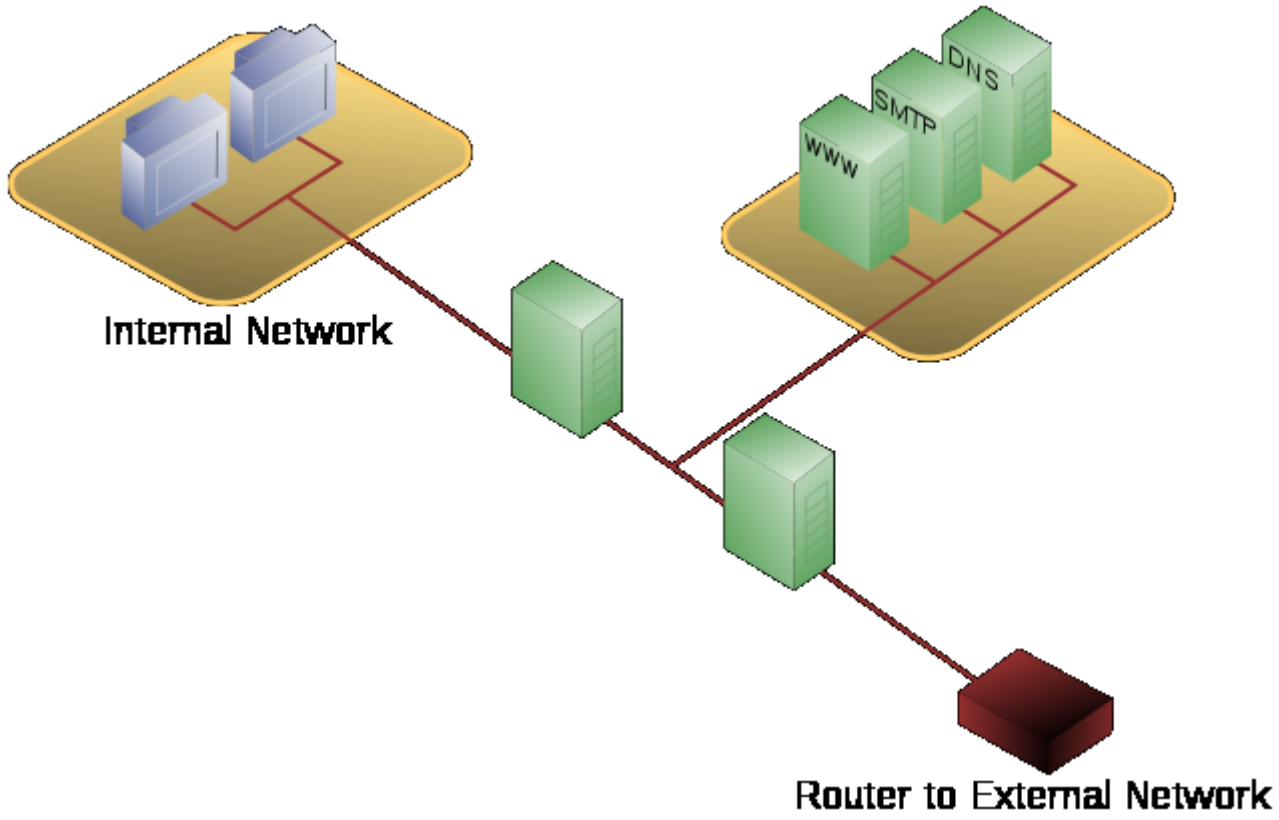
http://de.wikipedia.org/wiki/Personal_Firewall

DMZ – Demilitarized Zone

- Ent- oder demilitarisierte Zone
- Problem: Rechner, die aus dem Internet erreichbar sind (sein müssen)
  - Bsp.: Mailserver, Webserver, Tauschbörsensauger
  - Ermöglichen Zugang zum lokalen Netz
- Lösung: Schaffung einer Pufferzone, die aus dem Internet erreicht werden kann, von wo aus aber das Heimnetz sicher ist
- Technisch: Errichtung von zwei Firewalls

http://www.heise.de/netze/artikel/DMZ-selbst-gebaut-221656.html

DMZ - Prinzip



Firewall: Software

- FLI4L: Floppy ISDN for Linux
  - Eigentlich ein Router, trennt aber internes Netz und Internet und bietet Funktionen wie:
    - IP-Masquerading, DMZ, Logging
  - gut kombinierbar mit Eisfair-Server

http://www.fli4l.de/

- IPCop: ähnlich FLI4L,
  - einfachere Konfiguration insbesondere bei mehreren Netzen
    - Drei Netze sind vorkonfiguriert
  - größere Hardwareanforderungen

http://www.ipcop.org/

Schutz der Privatsphäre

- Cookies: speichert persönliche Einstellungen (auf Webseiten)
  - Idee: Einstellungen nur einmal vornehmen
- E.T. Programme: wollen nachhause telefonieren, übermitteln Daten
- Internetspuren: Transparenz beim Surfen
  - Provider vermerkt mindestens IP-Adresse
  - Cache enthält angesehene Webseiten
  - History enthält URLs besuchter Webseiten
- Unverschlüsselte Email: auf jedem Rechner, den die Email durchläuft kann geschnüffelt werden

Schutz der Privatsphäre

- Einkaufen im Internet:
  - Hinterlegen von Adressen
  - Kreditkartendaten
  - Vorlieben, Verhalten, „der gläserne Kunde“
- Instant Messaging: gesamte Kommunikation kann und wird vom Provider gespeichert
- Angaben zur eigenen Person auf Webseiten: wird von Suchmaschinen gespeichert
- Metadaten in Bildern

Schutzmöglichkeiten

- Cookies löschen oder nicht akzeptieren
- Browser-Cache löschen
- History löschen
- Personal Firewall so einstellen, dass ausgehende Verbindungen gemeldet werden
- Emails verschlüsselt versenden: PGP – Pretty Good Privacy
- auf sichere Verbindung achten: „https://“

Kinder- und Jugendschutz

- Ungeeignete Inhalte: Gewalt, Pornographie, Rassismus
- Mißbrauch von Chatrooms:
  - sexueller Kontakt zu Minderjährigen
  - Drogenverkauf
  - Verbreitung von ethisch und moralisch verwerflichen Informationen
  - Vorbereitung von Aktionen
- teure Downloads, Spam, Viren, Dialer

Schutzmaßnahmen

- geeignete Startseiten verwenden
- Technische Möglichkeiten:
  - Filterprogramme gegen jugendgefährdende Inhalte, Spam, Viren
    - Firewall mit Contentfilter (bspw. SquidGuard)
- Aufklärung:
  - allgemein über Gefahren im Internet: Spam, Viren
  - Bewusstsein über Gefahren entwickeln
  - persönliche Daten niemals preisgeben
  - keine Verabredungen außerhalb von Chatrooms

Zusammenfassung

- Bedrohungen „von außen“: Viren & Co., Spam, Spyware
- Bedrohungen „von innen“: eigenes Verhalten, Sorglosigkeit, Unwissenheit
- Schutzmaßnahmen: regelmäßiges Backup, Installation Virenschutz, Personal Firewall, Aufmerksamkeit
- Gefährdung von PDAs, Handys nicht vergessen

GOOGLE = DATENSAMMLER?

Google = Datensammler?

- Was weiss Google?
  - kommt darauf an ☺
- Suchmaschine nur einer von vielen Diensten
  - Google = etwa 50 Dienste
- Oft behauptet: Google bietet massenhaft kostenlose Dienste – Nutzer revanchiert sich mit einem Einblick in seine Privatsphäre

Suchmaschine

- sehr gute Suchergebnisse durch PageRank Verfahren
- Problem: Speicherung
  - IP-Adresse - neun Monate lang, freiwillige Anonymisierung
  - welcher Browser benutzt wird
  - die Suchanfrage selbst
  - Datum
  - Hinterlassen von Cookies zur Identifizierung
  - außerdem Spartensuche: Produkte, wiss. Artikel, Landkarten, Bücher, Videos

interessenbasierte Werbung

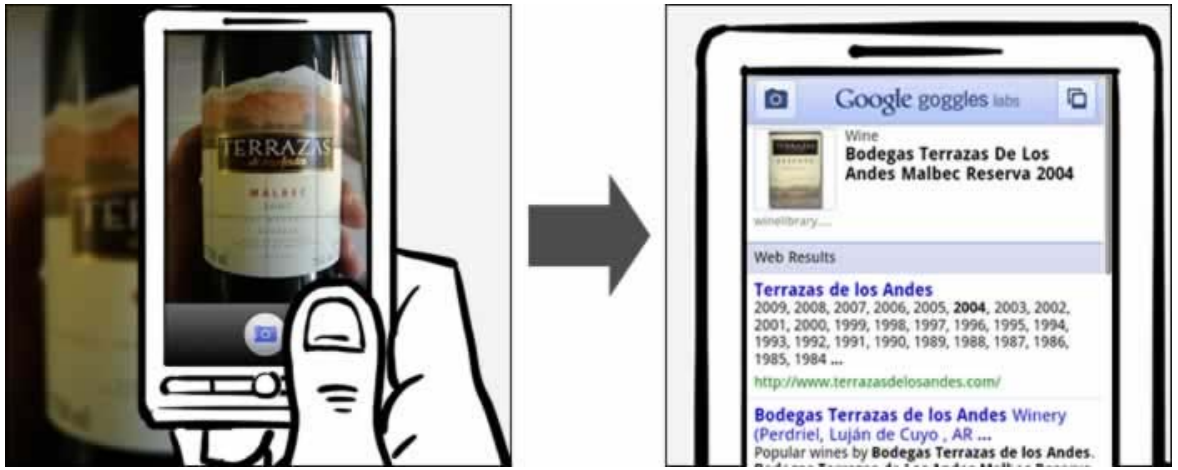
- Partnerseiten liefern Daten darüber, was sich ein Surfer anschaut + IP des Surfers
- Google erstellt Profil und liefert passende Werbung
- meist verdeckte Nutzung
- Transparenz unter: http://www.google.com/ads/preferences

GMail – Account

- Name des Nutzers/der Nutzerin
  - wenn Kontoname = Nutzername
- Durchsuchen der Emails nach Stichwörtern zur gezielten Einblendung von Werbung
- viele Dienste mit Account verknüpft
  - Terminkalender, Docs, Health, Fotos, Blogger, Talk
- von Email abhängiger Dienst (ohne Anmeldung nutzbar): Alerts
  - Angabe einer Emailadresse notwendig

Google Goggles

- Suche über Bilder
- Prinzip: mit Handykamera Photo zu Google senden → Antwort: Informationen zum photographierten Objekt



- Problem: Personensuche
- Vorlieben, Interessen, Standorte

Google Chrome

- Googles Browser
- Probleme:
  - Omnibox – Adresszeile als Eingabefeld für URLs und Suchbegriffe
    - Autovervollständigung → sendet ständig Daten an Google
  - Jede Installation enthält eine eindeutige Identifikationsnummer
    - wird an Google gesendet, bspw. bei Aktualisierungsprüfung
  - Senden von Programmfehlern an Google:
    - ID, momentan offene Dateien und Programme sowie Dienste und Dateiinhalte werden an Google gesendet
- viele „problematische“ Dienste sind abschaltbar

Google Toolbar

Erweiterung von Firefox, IE und Chrome

- erlaubt direktes Suchen bei Google auch andere Suchdienste wie Bildersuche, Scholar, usw.
- Popup-Blocker
- Durchsuchen der aktuellen Webseite
- Infos zur aktuellen Seite: u.a. ähnliche Seiten, Seiten die auf diese verweisen
- Synchronisierung mit Google-Konto
- Rechtschreibkorrektur in Formularfeldern
- SideWiki
- Hervorhebung von Suchwörtern
- Webprotokoll: Protokoll der eigenen Webaktivitäten
- Mein Standort: Ortsbezogene Informationen bekommen

http://toolbar.google.de/
http://de.wikipedia.org/wiki/Google_Toolbar

Probleme: Google Toolbar

Google toolbar

- Rechtschreibkorrektur erfordert das Senden der Daten zu Google
- SideWiki: Kommentare werden bei Google gespeichert
- Synchronisierungsfunktion: speichert Browsereinstellungen. incl. Autofill-Infos im Googlekonto
- Autofill sendet: Daten über Struktur der Seiten die das Webformular enthalten und deren Gliederung
- Webprotokoll speichert Verlaufsdaten im Googlekonto
- Mein Standort sendet Infos über: MAC-Adresse, SSIDs des WLANs, ID des Routers (MAC-Adresse), Signalstärke des Routers

http://www.google.com/support/toolbar/bin/static.py?page=privacy.html&hl=de&v=

Google Desktop

- Indizierung von Dokumenten auf dem lokalen PC
  - Office-Dokumente, Textdateien, PDF, Musik, Bilder, Videos, Emails, Webseiten, History
- Vorteil: lokale Dokumenten können durchsucht werden
- Problem: Suchfunktion über mehrere Rechner
  - erfordert Zwischenspeicherung von Daten bei Google → Suchindex der Dokumente
  - erlaubt Zugriff auf private Dokumente

Google Talk

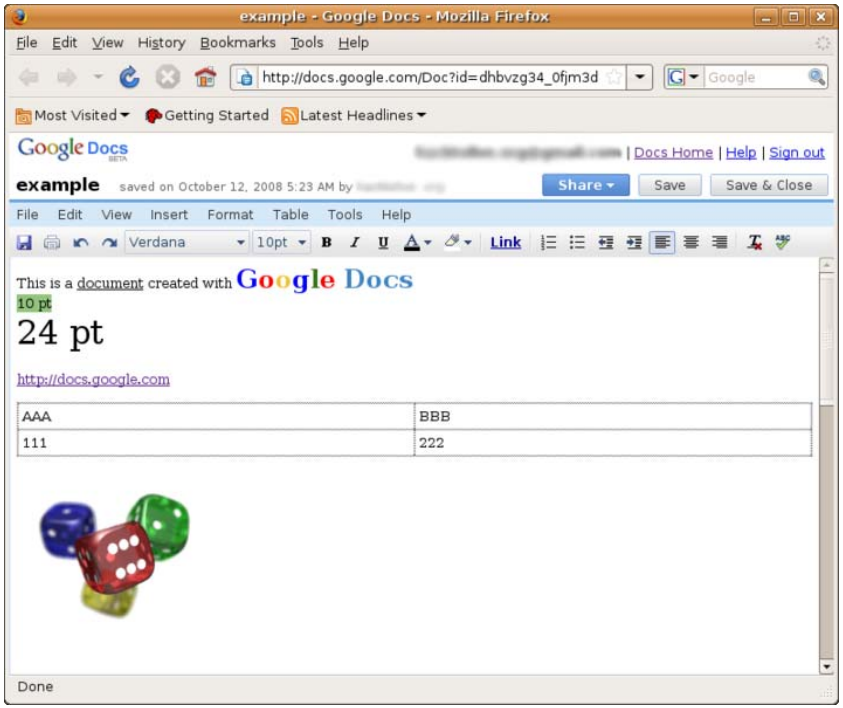
- Instant Messaging
  - auch für Handy wie iPhone, Android, Blackberry
- VoIP - Funktionalität
- Problem: alle Nachrichten werden über Google-Server geleitet

Google Health

- zentrales Abspeichern von Gesundheitsdaten
  - Befunde, Allergien, Laborergebnisse, Medikamente
- Überprüfung von Wechselwirkungen mit anderen Medikamenten
- Backup für Befunde
- Suche nach Ärzten und Krankenhäusern
- Problem: alle Daten landen bei Google auf dem Server

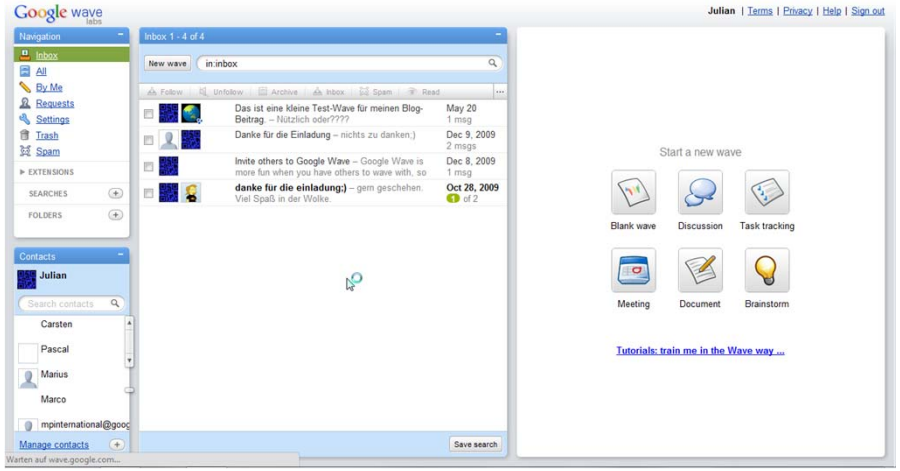
Google Docs

- gemeinsames Bearbeiten von Dokumenten
  - Textverarbeitung, Tabellenkalkulation, Präsentationen
- Problem: Dokumente liegen bei Google auf dem Server



Google Wave

- das gruppenenarbeits-, projektbarbeitungs-, photosharing-, brainstorming-, interactive games tool ☺
- Gruppenarbeit unter Benutzung von Photos, Karten, Videos, Textverarbeitung
- Problem: alle arbeiten online → alle Daten bei Google



Anonym bleiben?

- ist möglich
  - fiktiven Benutzernamen wählen
  - nicht über Google surfen: nicht anmelden
  - Nutzung von Anonymisierungsdiensten
  - Nutzung alternativer Suchmaschinen wie: http://www.ixquick.com → speichert keine Daten
  - Googles Suchmaschine nicht benutzen
  - Transparenz: Google Dashboard
  - http://www.google.com/ads/preferences
- aber schwierig:
  - siehe interessensbasierte Werbung
    - selbst wer nicht über Google surft wird an Google gemeldet
  - Google Analytics: Webseitenbetreiber können analysieren lassen, wer sich wofür interessiert → Weiterleitung an Google → Profilerstellung

Aktuell: Google-Analytics

- Browser-Erweiterung – erlaubt es, Google Analytics das Datensammeln zu verbieten
- Für Chrome, Firefox, IE
- Alternative: Webseitenbetreiber können IP-Adressen verkürzen

http://www.spiegel.de/netzwelt/web/0,1518,696816,00.html

Zusammenfassung

- Google erschafft ein virtuelles Gedächtnis
- Ziel: auf alle Fragen die eine richtige Antwort zu geben
- Problem: richtige Antwort auf alle Fragen verlangt viel Wissen über den der fragt
- bisher versichert Google, dass die angebotenen Dienste nichts voneinander wissen
- theoretisch möglich: Zusammensetzen aller Informationen aus verschiedenen Quellen
  - anhand von IP-Adressen, gesetzten Cookies, angegebenen Nutzernamen (auch von Werbepartnern)
  - Worst case: Abgleich mit anderen Quellen wie Amazon, Paypal
- Vision: online über Google, Browser als Plattform für alle Anwendungen, Speicher → Google, Stichwort cloud computing