Inhaltsverzeichnis

Geschichte der Mensch-Computer-Interaktion

Vorbilder der Interaktion

- Werkzeug
- Auto
- Klavier
- Fließband
- Interaktion zw. Menschen
- Bürokratie

Rechenmaschine -> Rechenmaschine

Mechanische Einheit für simple Berechnungen. Hat eher den Werkzeugcharakter, keine Interaktivität und schwer zu bedienen. Entwicklung von militärischer Seite für Geschosstabellen, Kryptographie (vgl. Enigma-Maschine)

- Leibniz: 4-Spezies-Rechenmaschine (addieren, subtrahieren, multiplizieren, dividieren)
- Thomas: Arithmometer
- Babbage: Difference Engine (Polynome)
- Babbage: Konzept der Analytical Engine (Mechanischer Computer mit Speicher, ALU und I/O, unmöglich umzusetzen)
- Ada Lovelace: Schreibt Programme für die Analytical Engine, nach ihr ist die Sprache Ada benannt.
- Alan Turing: Turing-Maschine
- Zuse: Z3
- ENIAC

Webstuhl -> Verwaltungsmaschine

Dient zur Automatisierung von Abläufen, der Mensch wird zum Aufseher (vorher: Arbeiter). Hat Fließbandcharakter.

- Jacquard-Webstuhl: Wird durch Lochreihen "programmiert"
- Von dieser Seite entsteht die Entwicklung des Computers als Verwaltungsmaschine.
- Hollerith: Maschine für die Volkszählung 1890. Funktioniert mit Lochkarten. Aus Holleriths Firma wird später IBM.
- Erste Großrechner für Büros, etc. Reine Eingabe-Ausgabe-Einheiten ohne richtige Interaktion.

Mechanische Spielzeuge -> Spielfeld

Dienen rein zur Unterhaltung (bessere Zaubertricks). Ziel: Möglichst viele Menschen verblüffen.

- Mechanische Ente
- "Schreiber" von Jaquet-Droz
- Von hier kommt der spielerische Ansatz als treibende Kraft der Computerentwicklung. Hier spielt Interaktion eine wichtige Rolle!

- Higinbotham, Dvorak: "Tennis for two", Entwicklung rein in Hardware
- Russel: "Spacewar", 2 Raumschiffe, Gravitation, etc.
- Atari: "Pong" (kennt jeder)

Der interaktive Computer

Aus allen drei Richtungen wird der militärisch genutzte Computer SAGE entwickelt. Ein komplettes System mit Bildschirm! SAGE = Semi-automatic Ground Environment. Leider ein Flop, aber eines der ersten interaktiven Systeme.
Rechenmaschinen gibt es immer noch in kleinerer Form (Taschenrechner).

Frühe Entwicklung

- Sutherland: Sketchpad
- Engelbart: Erste Computermaus
- Engelbart: NLS - Ein interaktives System mit Tastatur, Rasterbildschirm, Chord-Keyboard, 3-Tasten-Maus. Full screen editieren, gemeinsames Arbeiten an einem Text, Links (hypertext), Mausgesteuertes Interface, Hochauflösender Screen, Multimedia, Fenster, Messaging
- Alan Key: Dynabook (Konzept für Laptops)
- Bastlerkultur: Die ersten Minicomputer - Altair 8800, Apple I, Apple][
- Heimcomputer, für Spiele u. dgl. optimiert, billig zu haben

IBM PC

- "command line" interpreter (BASIC)
- "screen based"; Formulare, Menüs, etc. werden auf dem Bildschirm angezeigt.
- Einer der größten Erfolge in der Computergeschichte

IBM 360

- 1964 vorgestellt, Großrechner
- Vereint technisches Rechnen und kommerzielle Datenverarbeitung
- Damit erreicht IBM das Monopol im Computermarkt
- Betriebssystem: OS/360, damals größtes ziviles Softwareprojekt.
- Projektleiter Frederick Brooks schreibt später "The Mythical Man-Month"; Zitat: "Adding manpower to a late software project makes it later".

Der interaktive Arbeitsplatz-PC

- Xerox Alto: Forschungsgerät mit Maus und Grafikbildschirm (vorher war das Meiste textbasiert)
- Xerox Star: Erster kommerzieller Rechner mit "Desktop"-Interface wie wir es von Microsoft und Apple kennen. Leider nicht sehr gut bedienbar, langsam und teuer.
- Apple Macintosh: Erster vernünftiger Desktop; 512x384 s/w-Display; Viele grafische Applikationen.
- Jeder versucht, Apple zu kopieren, daraus entsteht auch Windows 1.0

Das Desktop-Paradigma

- Basis ist der (Büro-)Schreibtisch. Analog dazu wird auch die Benutzerschnittstelle

programmiert, damit sich neue Benutzer leichter zurechtfinden.
- Probleme: Ineffizient für erfahrene Benutzer.
- Halasz, Moran: "We wish to argue against the claim that novices are best taught about computer systems by encouraging them to reason analogically. While analogies may ease the way, they are not the most effective way to teach new users. In fact, analogical models can often act as barriers preventing new users from developing an effective understanding of systems."
- Buxton: "It seems to me that the Macintosh was designed for Napoleon: Unless you are typing, you can work all day with one hand tucked into your jacket. This is great if you are one-handed, but a waste if you're not. The image of the user reflected in the technology is lopsided. "Hands-on" computing is largely a myth. It would be better called "hand-on" or even "finger-on.""
- Gentner, Nielsen: "According to the Macintosh guidelines, the design of human interfaces for Macintosh system software and applications is based on a number of fundamental principles of human-computer interaction. These principles have led to excellent graphical interfaces, but we wonder: How do these principles limit the computer-human interface? What types of interfaces would result from violating these principles?"
- Wie jeder weiß, hat sich das Desktop-Paradigma dennoch durchgesetzt.

Der Computer als Medium

- Verteiltes Wissen im www: Google, Wikipedia
- Computer-mediated Communication: Chat über IRC, IM, Video
- Medien im Computer: Media Player, Slideshows
- Kollaboratives Arbeiten: PIM, Mail, Versionsverwaltung
- "Media Center"
- Handys, wie zB das Nokia 5510 mit dem man Musik austauschen kann.
- User Created Content, Web 2.0

Der Weg in die Informationsgesellschaft

- Immer weniger Menschen erzeugen materielle Güter
- Immer mehr Menschen dagegen arbeiten mit Information (Dienstleistung)
- => erfordert längere Ausbildung und v.a. lebenslanges Lernen
- Internet ermöglicht völlig neue Kommunikation über alle Grenzen hinweg

Änderungen im Alltag

- Vorlesungen mit downloadbaren Folien und Blog.. und Arbeitsmappe.. und Wiki.. und Timeline.. und Google Maps.. und .. und .. und dem ganzen Krempel
- Elektronischer Amtsweg
- eBay (z.B. Neuorganisation des Antiquitätenhandels)

Drei Schritte zur Informationsgesellschaft

- Automatisierung: In der Produktion - Taylorismus, Fordismus
- Bürokratisierung: Feste, durch Regeln, Gesetze oder Verwaltungsregelments generell geordnete (behördliche) Kompetenzen schaffen.
- Telematisierung: Abwälzung von Geschäftsvorgängen auf die Kunden. eBanking,

eGovernment. Nur dadurch ist der steigende Verwaltungsaufwand noch bewältigbar. Telematisierung ist leider auch ein sich selbst verstärkender Vorgang, führt also wieder zu neuem Verwaltungsaufwand, der dann wieder duch Telematisierung abgewälzt wird, etc.

Geschichte

- 1780-1890: Dampfmaschine, Werkzeugmaschine, Eisenbahn, Stahl, Gas, Elektrizität, Farbstoffe. "Volksschule" ist die einzige verpflichtende. 1% Maturanten, 0.5% Studenten.
- 1890-1940: Auto, Flugzeug, Kunststoffe, Telekommunikation. 8 Jahre Schulpflicht. 2% Maturanten, 2% Studenten.
- 1940-1990: EDV, Radar, Mikroelektronik, Raumfahrt. 20%-60% Facharbeiter, 9%-34% Maturanten, 4.2%-23% Studenten.
- 1990-?: Internet, Multimedia, Mobilkommunikation, Bio- und Nanotechnologien. GSI-Vorlesungen. Maturanten- und Studentenzahlen steigen weiter an.

Entwicklung des Berufsbilds im letzten Jahrhundert

- 50er: Techniker und Programmierer auf unterster Maschinenebene
- 60er: Berufsbilder von Hardware- und Softwareentwickler trennen sich
- 70er: Zentrale Rechenzentren (Großrechner), große Entwicklungsteams
- 80er: Einführung des PCs im Massenmarkt, zunehmende Dezentralisierung
- 90er: Vernetzung und Internet, Multimedia, Mobilkommunikation (Handys)
- 00er: "Digital Hub", Wearable Computing, Breitband, Computer in Gebrauchsgegenständen
- Berufsaussichten 2000: 50.000 Computerspezialisten fehlen
- 2003: HTML-Programmierer arbeitslos
- 2005: Pro Jahr fehlen mehrere tausend qualifizierte Hochschulabsolventen

Generelles Wachstum der IT-Branche, aber starke Konturschwankungen. Innovationszyklen und Projektlaufzeiten werden immer kürzer. Der Arbeitsmarkt ist hochgradig spezialisiert, unterschiedliche Bereiche sind von Krisen unterschiedlich betroffen. Allgemeine Qualifikationen werden uninteressant, Spezialgebiete und Doppelqualifikationen interessanter.

(Vergebliche) Visionen der IT-Branchen

- Produktivitätssteigerung durch Computer
  => Abnahme der Produktivität durch Einführung von Computern
- Mass Customization (Unikate für jeden)
  => Sättigung mit Massenartikeln
  *** Build-to-Order
- Veränderung der Firmen-/Arbeitsorganisation
  => Abnahme von Organisationsformen, die auf Kooperation und Mitbestimmung beruhen
  *** Entwicklung ist aber insgesamt uneindeutig
- Neue Arbeitsformen wie "Ich-AG" und virtuelle Unternehmen
  => extreme Selbstausbeutung, kein gewerkschaftliches Bewusstsein
  *** Änderung in Sicht
- Papierloses Büro

=> Noch nie wurde so viel ausgedruckt
- Umweltschonung durch mehr Effizienz, weniger Reisen
  => Just-in-Time Produktion, LKW-Verkehr nimmt drastisch zu
  => Effiziente, stromsparende Technologien (Handys) werden durch Stückzahl aufgewogen
  => Herstellung eines PCs kostet so viel Ressourcen wie Herstellung eines Autos
- Neuer Umgang mit Wissen

Verschmelzung von Wissen und Technik

Informationsexplosion (immer mehr Information wird verfügbar, zur Entwicklung von Produkten verwendet) -> Wissensbasierung der Technik
hält sich die Waage mit **Informationsimplosion** (immer mehr Wissen wird über neue Technologien zugänglich gemacht) -> Technisierung des Wissens

- Für technische Entwicklung und Herstellung von industriellen Gütern sind immer mehr Informationen erforderlich (man denke nur an die Autoindustrie)
- Heutige PKWs besitzen mehr Rechenleistung als die Mondlandungsfähre

Die neue Wissensordnung

- Qualität; Veränderungsfreiheit (Erkenntnisgewinn); Verletzlichkeit von Wissen
- Schutz; Beeinträchtigungsfreiheit (Schutz vor Eingriffen); Privacy
- Verbreitung; Verkehrsfreiheit (freier Informationsfluss); Copyright/Copyleft

Globalisierung

Bereiche

- Handel
- Investitionen
- Dienstleistungen
- Finanzdienstleistungen
- Gegenbewegungen: z.B. attac

Triebkräfte

- Ökonomische Konzentration: z.B. Medienindustrie; immer weniger Unternehmen kontrollieren die Massenmedien, vor kurzem wurden VIACOM und Bertelsmann von Sony/BMG geschluckt.
- Deregulierung: z.B. Red Bull Salzburg, oft kein österreichischer Spieler in der Aufstellung
- Vernetzung; technologische Voraussetzungen (Internet) sind jetzt gegeben

Vernetzung

Geschichte des Internets

- 1969: Arpanet - militärisches Netz zur Verbindung von Militärrechnern und Universitäten (Forschung). Das Ziel: Eine dezentrale Infrastruktur, die mitunter auch Atomschläge überleben kann.
- 1971: Erste E-Mail Software innerhalb des Arpanet. Bald stellt das die überwiegende Nutzung dar (Diskussionen, Mailing Listen, erste Communities). Das ist allerdings unerwünscht (militärische Nutzung steht immer noch im Vordergrund).
- 1973: Verbindung des Arpanet mit London und Norwegen. Das Arpanet wächst in den darauffolgenden Jahren sehr schnell an, immer mehr Rechner kommen dazu.
- 1979: Usenet, auf UUCP (Unix-Unix-Copy) und Modem-Verbindungen basierend. Entwickelt von Tom Truscott, Jim Ellis, Steve Bellovin. Das Zielpublikum ist die Unix-Community (Unix war damals noch Open Source). Im Gegensatz zum Arpanet als offenes, logisches, demokratisches Netz organisiert. Die Organisation geschieht in Form von sogenannten Newsgroups, den Vorläufern heutiger Webforen.
- Im Unterschied zum Arpanet, wo vorwiegend ernsthafte Forschung stattfindet ist das Usenet eine demokratisch organisierte Interessensgemeinschaft.
- 1981: Arpanet und Usenet werden durch ein Gateway verbunden.
- 1983: Entwicklung von TCP/IP. Grundstein für das Internet wie wir es heute kennen.
- DoD (Department of Defense) verlässt das Arpanet und gründet ein neues Netz (Milnet) für rein militärische Nutzung, um die Kontrolle zu bewahren.
- 1984: 1,000 Hosts am Internet, 1989 sind es schon über 100,000.
- Ab dieser Zeit spricht man vom "Internet", weil die ganzen Netze zu einem großen zusammenwachsen (Arpanet, Usenet, Milnet, ...)
- Mögliche Definition von Internet: Alles was durch TCP/IP verbunden wird.

- NSFNet: Backbone des Internet, von der National Science Foundation bereitgestellt. Am Anfang strenge Nutzungsbedingungen (keine kommerzielle Nutzung, keine Werbung. Nur für Forschungszwecke bestimmt.)
- 1990: Arpanet wird komplett eingestellt.

90er Jahre: Das World Wide Web

- Tim Berners-Lee entwickelt den ersten Web-Browser, Erweiterung zu textbasiertem "Gopher"-System.
- Entwicklung von HTML als SGML-Klon, um SGML-Lizenzgebühren zu sparen.
- Als Folge wächst die Nutzung des NFSNet Backbone um 15-25% pro Monat und die aufgestellten Regeln (keine private, kommerzielle Nutzung) werden unterlaufen.
- Privatisierung des Internet: NII (National Information Infrastructure) Initiative stellt 1994 die Weichen für unbeschränkte Kommerzialisierung des Internet.

End-to-End vs. Intelligente Netze

- **End-to-End**: Vollständige Symmetrie aller Verbindungen. Was am einen Ende reinkommt, kommt am andern Ende unverändert wieder raus.
  Voraussetzung für öffene Kommunikation, p2p, offenen und gleichen Zugang für alle, aber auch für DDoS, Spam, Würmer, Viren.
  Niemand (nicht einmal der Netzbetreiber selbst) kann das Internet in dem Sinne kontrollieren, dass er gezielt bestimmte Aktionen/Nutzung verhindert.
- **Intelligente Netze**: Gegenkonzept zu End-to-End. Infrastruktur besitzt eine gewisse Intelligenz, kann Traffic gezielt filtern. Damit wird es für Infrastrukturbetreiber möglich, die Nutzungsbedingungen rein technisch festzulegen. Wären unsere Netze intelligent, wäre es für den Provider möglich, Filesharing, Spam, einzelne Webseiten, etc. einfach zu sperren bzw. dafür zusätzlich Geld zu verlangen. Die Folge: Mehr Kontrolle für den Betreiber, weniger Freiheit für den Konsumenten.
- Das derzeitige Internet ist (noch) größtenteils End-to-End.

Wer kontrolliert das Internet?

- Technische Grundlage sind 13 "Root-Server". 10 davon stehen in den USA. 2 davon werden von VeriSign betrieben (Aufgabe: SyncMaster für die übrigen Server).
- ICANN (Internet Corporation for Assigned Names and Numbers) vergibt TLDs (Top Level Domains) und IP-Adressen, koordiniert Internetprotokolle.
- Top-Level-Domains: länderübergreifend (.com, .net, .org) und länderspezifisch (.at, .de, .dd, .cc)
- Missbrauch: VeriSign richtet 2003 eine Standardseite für nichtexistierende Domains ein und verdient kräftig an der geschalteten Werbung.
- Missbrauch: USA hat viel mehr Einfluss über das Internet (Domainvergabe) als internationale Regierungen.
- 2005: World Summit on the Information Society. EU fordert mehr internationale Kontrolle. Entwicklungsländer fordern internationales Gremium. USA erklärt, dass sie die Kontrolle nicht aufgeben werden. UN will die Aufgaben der ICANN nicht übernehmen.
- Ergebnisse des World Summit: 2006 richtet die UN das "Internet Governance Forum" ein, das die ICANN kontrolliert.

Wie international ist das Internet?

- Der Zugang zum Internet ist im Verhältnis zur Bevölkerungsdichte sehr ungleichmäßig verteilt (dritte Welt hat fast gar keinen Zugang).
- Der "Digital Divide" schafft eine neue Kluft, und zwar zwischen Menschen mit Zugang zu den neuen Technologien und Menschen ohne.
- Lösungsansätze zum Digital Divide: Simputer (Indien), OLPC (dritte Welt)

OLPC

"One Laptop Per Child" - grünes laptopähnliches Gerät für Entwicklungsländer.

Features

- Linux-basiert, alle Spezifikationen offen
- WLAN und Mesh-Networking (OLPCs erzeugen selbstständig ein eigenes Netzwerk)
- Haltbares, robustes Design
- Niedrige Kosten, niedriger Stromverbrauch

Verteilung

- Werden von staatlichen Organisationen der dritten Welt gekauft
- Zielpreis: $100, die Dinger kosten zur Zeit allerdings noch $200
- Give 1, Get 1 Programm

Kritische Stimmen

- "Shared Internet Access" (z.B. Internet-Cafes) wäre eine billigere Lösung. Gegenargument: Für Kinder ist es wichtig, ein eigenes Gerät (eben so ein Laptop Dings) zu haben.
- Microsoft: Das Ding ist nur Spielzeug und kein Vergleich zu einem echten (Windows-) PC. Mittlerweile wird allerdings seitens Microsoft an einem abgespeckten Windows XP für XO gearbeitet.
- Entwicklungsländer brauchen andere Dinge viel dringender als Laptops. Gegenargument: OLPC ist nachhaltige Entwicklungshilfe und gibt den Entwicklungsländern wichtiges Know-How das sie später noch bitter nötig haben werden.

Monopolisierung + Gegenbewegungen

John Sherman (republikanischer Kongressabgeordner), 1890: Internationale Geschäftsbeziehungen, (wirtschaftliche) Verschwörungen, Kartelle und Monopolisierung ist illegal. Ein Gesetz gegen den Missbrauch des freien Marktes (Preisabsprachen, Marktaufteilung, etc.).

Schäden durch Monopole

- Vernichtung von Konkurrenten
- Preisdiktat
- Verhinderung von Innovation, der Mächtige gewinnt, und nicht der mit dem besseren Produkt

Monopolstrategien

- Erpressung (z.B. Vorschlag der Marktaufteilung mit Schadensdrohung)
- Embrace and Change (Untermauern von Standards; siehe Java, Kerberos, HTML)
- Leverage (z.B. Internet Explorer, Windows Media Player)
- Verdrängung (z.B. Winmodem, Winprinter, Windows XP ohne Java, etc.)
- Behinderung
- FUD (Fear, Uncertainity and Doubt): Verleumdung von (besseren) Konkurrenzprodukten

Anti-Trust-Verfahren im IT-Bereich

- 1969: Lyndon B. Johnson (US-Präsident) gegen IBM. Vorwurf: Kontrolle von 3/4 des Computermarkts. Verfahren 1982 eingestellt.
- 1974: Gerald Ford (US-Präsident) gegen AT&T. Vorwurf: Alleinherrschaft über das US-Telefonnetz. 1984 musste AT&T 23 Tochtergesellschaften abgeben, die seither unabhängig arbeiten.
- 1998: Bill Clinton (US-Präsident) gegen Microsoft. Vorwurf: Verdrängung von Netscape, Unterlaufung des Java-Standards (HotJava), Verdrängung von Quicktime und Realplayer, Verhinderung der Auslieferung von Cross-Platform-Libraries wie der Intel Signal Processing Library, etc.
  Folgen: Microsoft soll zuerst unter Richter Thomas Penfield zerschlagen werden. Allerdings wird 2001 George W. Bush gewählt, dieser setzt einen anderen Richter ein und die Strafe fällt schwach aus.
  Urteil: Kein Einfluss auf Hardwarehersteller, Einheitliche Lizenzbedingungen, Installation von fremder Software muss erlaubt sein, APIs, Kommunikationsprotokolle müssen offengelegt werden, Fremdprogramme dürfen nicht beeinflusst werden.
  Im Endeffekt machen die Aktien von Microsoft einen gewaltigen Sprung nach oben. Es folgen noch einige Zivilklagen (z.B. von Sun Inc. (Java) und der EU). Microsoft macht offene Formate und startet das Shared Source Programm.

Gegenkulturen zum Monopol

- Community Networks, freies WLAN
- Open-Source und Free Software Communities
- Open Content (Wikipedia), Information Sharing, User Created Content
- P2P-Netze
- Social Software, Web 2.0 (del.icio.us, Blogger, Wikipedia, Youtube)

Open Source

- Entwickelt mit dem Ziel, möglichst viele Anwender zu erreichen
- Kann von jedem weiterentwickelt werden
- Microsoft: Halloween-Dokumente (Open Source muss zerschlagen werden)
- Martin Taylor (Microsoft): Open Source funktioniert super, aber ist nicht erweiterbar, die Plattform ist nicht stabil
- Brad Smith, Horacio Gutierrez (Microsoft): Open Source verletzt 235 Microsoft Patente

Gegenvereinigungen

Gegen Kommerzialisierung, Monopolisierung im IT-Bereich

- EFF (Electronic Frontier Foundation), ACLU, EPIC
- CPSR (Computer Professionals for Social Responsibility), FlFF
- CCC (Chaos Computer Club)

Gefährdungen und Schäden

Die Verletzlichkeit der Informationsgesellschaft.

Beispiele für Angriffe

- 12.12.1986: Ausfall des ARPANet; ein Bagger hatte die Leitungen durchtrennt (physisch)
- 2001: Code Red Worm infiziert fast alle IIS-Server und startet DDOS-Attacken (syntaktisch)
- 25.8.2000: Falsche Internet-News lässt Emulex-Aktien um 61% sinken. Der Täter wird gefasst.
  (semantisch)

Arten von Attacken

- physisch: gegen Computer, Leitungen
- syntaktisch: gegen Software, Algorithmen, Protokollen. Ausnutzung von Sicherheitslücken, DDOS-Attacken
- semantisch: Ausnutzung auf die Art und Weise wie Information verarbeitet wird. "Amateurs attack machines, professionals target people" - Bruce Schneier.

Begriffe

- Verletzlichkeit = Wahrscheinlichkeit für Schaden multipliziert mit der Schadenshöhe
- vulnerability, kompromittiert, malware (Schadsoftware), buffer overflow, code injection, cross site scripting
- Risikofaktoren: Schwachstellen, Dimensionierung, Geschwindigkeit, Irrtumsanfälligkeit, Vertrauensseligkeit, Komplexität
- Ursachen der Gefährdung: **Böse Absicht**, **Fahrlässigkeit (Bugs)**, **Denkfehler (Fehler im Design)**, **Systemische Bedingungen (Komplexität)**, **wenig Sicherheitsbewusstsein**, **schlampiges Sicherheitsmanagement**

Böse Absicht

- Malware (Viren, Würmer, Trojaner); Letzer Trend: JavaScript-Viren wie Jikto.
- Bedrohung durch Malware nimmt seit Jahren ständig zu
- Windows XP ohne Updates, Virenscanner oder Firewall überlebt gerade mal ein paar Stunden im Internet
- Bill Gates (Microsoft): "Wir sind ständig um Sicherheit bemüht"
- Fallbeispiel "Sober": Installiert sich in der Windows-Registry, verschickt sich selbst mit gefälschtem Absender an Mailadressen aus dem Adressbuch. Kann Code aus dem Internet ausführen. Damit hat der Erfinder von Sober kurzzeitig Zugriff auf mehrere hunderttausend Rechner. => Mit Malware kann man ja Geld verdienen!

- otnet: Netzwerk aus infizierten Rechnern.
- Trojanische Pferde: Falsches Loginfenster verleitet den User dazu, seine Daten nicht an die offizielle Stelle sondern eine böswillige Person zu geben. Gutes Beispiel sind Kontodaten oder Kreditkartennummern. Das nennt man auch Phishing (Password Fishing).
- DDOS-Attacken: Lahmlegen eines Servers durch Überbeanspruchung, z.B. von einem Botnet aus.
- Das "Storm Worm" Botnet ist mächtiger als die meisten Supercomputer.
- Wirtschaftlicher Schaden von Attacken auf Computernetze sind schwer abschätzbar. Wie viel kostet es wirklich, wenn ein Computer eine Zeit lang nicht funktioniert? Wie fasst man die Veröffentlichung von geheimen Daten in konkrete Zahlen (Geld)?
- Empfehlungen der Industrie: Keine unbekannten Programme ausführen, Immer einen aktuellen Virenscanner haben.
- Trend: Malware wird professioneller und auf Gewinn ausgerichtet (Vermieten von Botnets, Verkauf von organisierten Angriffen)
- In der Folge von 9/11 ist Hacken in den USA gleichbedeutend mit einem terroristischen Anschlag

Bugs

- 14.9.2004: Flugverkehr in Kalifornien bricht wegen Windows-Fehler für einige Stunden zusammen. Ursache: Windows wurde nicht regelmäßig neu gestartet.
- 15.1.1990: AT&T-Fernverbindungen brechen zusammen. Telefonnetz ist für 9 Stunden stark beeinträchtigt. Ursache: Bug im Kommunikationsprotokoll zwischen einzelnen Stationen

Denkfehler

- 1985-87: Bestrahlungsgerät "therac-25" gibt aufgrund falscher Bedienung (richtige Bedienung ist aufgrund Designfehler unlogisch) viel zu hohe Dosen ab -> tötet in Folge Patienten
- 28.1.1986: Raumfähre "Challenger" explodiert 72 Sekunden nach dem Start. Ursache: Ein Dichtungsring hält die niedrigen Außentemperaturen nicht aus. Die Techniker wussten das im Vorfelt, waren aber nicht in der Lage diese Informationen (Beanspruchung von Dichtungsringen bei verschiedenen Temperaturen) verständlich aufzubereiten.
- WLAN: Verschiedene Verschlüsselungsstandards, von denen nur ein oder zwei wirklich sicher sind, führen zu komplett offenen Netzen.

Designfehler

- 7.11.2000: George Bush gewinnt Präsidentschaftswahl. Mögliche Ursache: Designfehler des Stimmzettels (es ist unklar, welches Kreuz zu welchem Kandidaten gehört)
- Fiktionales Szenario: Ein Fertigungsroboter tötet Bart Mattews, weil es keinen einfach erreichbaren Notaus-Schalter gibt
- Jahr-2000-Problem: Auf Lochkarten und in großen Datenbanken wird die Jahreszahl nur 2-stellig (ohne 19 bzw. 20) gespeichert. Mit dem Jahrhundertwechsel (1999 auf 2000) stellt das ein großes Problem dar.
- Key Bumping: Sicherheitsschlösser sind mit Spezialwerkzeug sehr einfach zu

knacken.

Systemische Bedingungen

- Oktober 1987: Internationaler Börsencrash, verursacht durch automatisierte Börsenkäufe (Software kauft/verkauft automatisch Aktien)
- eVoting: Maschinen wurden schnell eingeführt, weisen aber noch erhebliche Probleme in Punkto Sicherheit und Vertrauenswürdigkeit auf. Sehr schlecht: Diebold Wahlmaschinen, wie sie in Amerika eingesetzt wurden. Studie zeigt, dass es sehr einfach ist, unerkannt Stimmen zu fälschen.

Mangelndes Sicherheitsbewusstsein

- "Security by Obscurity" (Verstecken von Sicherheitsmaßnahmen) ist kein gutes Konzept
- Viele Webseitenbetreiber kümmern sich nicht um die Sicherheit ("Wird schon nichts passieren"). Das ist kurzsichtig.
- Schlampiges Sicherheitsmanagement - viele Fälle zeigen folgendes: Wenn es eine Lücke gibt, ist es nur eine Frage der Zeit bis sie gefunden wird.

Sicherheit vs. Freiheit

Offenheit und Sicherung sind grundsätzlich zwei verschiedene Richtungen. Macht man ein System offener, ist es nicht mehr so sicher. Schottet man ein System gegen Angriffe ab, ist es nicht mehr so offen wie vorher.

- Free flow of information, offene Netze vs. Abschottung, Kontrolle, Überwachung
- Verletzlichkeit der Informationsgesellschaft => Grundlage für weiteren Ausbau der Sicherheitsapparate?
- Sicherheitszwang der IuK-Technologien trägt dazu bei, dass gesellschaftliche Verhältnisse erstarren und zu verhärten drohen
- Aber: Ist eine gesicherte Gesellschaft auch eine sichere Gesellschaft
- Beispiel: Seit Einführung von ABS fahren viele Leute schneller und unvorsichtiger. Auf gut beleuchteten Straßen sind Autofahrer nicht mehr so vorsichtig.
- Problem: Wird die Sicherheit irgendwo ausgebaut, konzentrieren sich die Angriffe auf Ziele, wo das nicht passiert ist. Die Folge davon ist, dass sich durch die meisten Sicherheitsmaßnahmen die allgemeine Sicherheit nicht erhöht, die Freiheit aber sehr wohl eingeschränkt wird.

Gestaltungsvorschläge

- Die Freiheit des Individuums ist höher zu bewerten als die Sicherheit der Gesellschaft. - (sinngemäß) Roßnagl et al, "Die Verletzlichkeit der Informationsgesellschaft", 1989

Vorschläge nach Roßnagl

- Statt Verhinderung von Missbrauch: Folgen reduzieren, Schäden minimieren.
- Statt Automatisierung: Unterstützende Technik, Menschiches Zusammenwirken als Grundlage.
- Statt Monopolen: Alternativen erhalten, Vielfalt sichern.

- Statt Verlass auf eine Lösung: Redundanzen schaffen.
- Statt vollkommene Abhängigkeit vom Hersteller: zeitliche, räumliche, technische und organisatorische Vielfalt.
- Statt Zentralisierung: entkoppelte, transparente und dezentrale Lösungen.
- Statt Totalausfall: stabiler Zustand bei teilweisem oder ganzen Versagen.
- Statt Überraschungen: Systematische Notfallplanung.
- Statt Fremdbestimmung: Gestaltung der Technik und der Sicherheitssysteme mit Zustimmung der Betroffenen und der Öffentlichkeit.
- Verzicht auf ökonomischen Vorteil, Komfortgewinn, wenn das Schadenspotenzial zu hoch ist.

Praxistipps

- Mehrere Betriebssysteme installieren! Redundanzen schaffen - Windows kann mit Hilfe von Linux wiederhergestellt werden und umgekehrt.
- Backups machen! Datenverlust ist immer eine furchtbare Sache.
- Zweifelhafte Features sofort abdrehen! Zum Beispiel nicht benötigte Toolbars im Internet Explorer.
- Infizierter Rechner? Nicht lange fackeln und sofort neu aufsetzen! Sonst hat man möglicherweise einen Trojaner o.ä. im Hintergrund, was ein großes Risiko darstellt.
- Webseiten für mehrere Betriebssysteme/Browser gestalten!
- Webseiten für unterschiedliche Bedürfnisse gestalten! Screenreader, textbasierte Systeme, Mobiltelefone, etc.
- Sichere Verbindungen verwenden! SSL wenn möglich.
- Kein HTML in E-Mails verwenden!
- Immer eine Firewall+Monitoring verwenden! Damit hat man einen Überblick, welche Programme auf das Internet zugreifen.

Was ist "Privatsphäre"?

Das Konzept der Privatsphäre ist kein selbstverständliches. Beispiel: "Sonnenkönig" Ludwig XIV. hielt Audienzen u.a. in seinem Schlafzimmer, auch während des Ankleidens ab. So etwas wie Privatsphäre war damals nicht wirklich vorhanden.

- 1890: "The right to privacy": Warren und Brandeis begründen die Idee der Privatsphäre als eigenständiges Persönlichkeitsrecht. Ihrer Meinung nach ist es für den Menschen wichtig, sich ab und zu von der Welt zurückzuziehen, um Stress zu vermeiden. Auslöser für diese neuen Konzepte war höchstwahrscheinlich die Erfindung des Fotoapparats und damit die Entstehung der ersten "Paparazzi".
- Warren/Brandeis: Privacy = "the right to be let alone"
- Alan Westin: Privacy = Recht eines Individuums, selbst zu bestimmen, welche persönlichen Informationen an andere weitergegeben werden.
- Froomkin: Privacy = a right to be left alone, to autonomous choice regarding intimate matters, to autonomous choice regarding other personal matters
- Österreichisches Gesetz: Jeder hat Recht auf Geheimhaltung des Privat- und Familienlebens und seiner personenbezogenen Daten.

Angriffe auf die Privatsphäre

Immer schon gab es Versuche der Staatsmacht, die Kommunikation der Bürger zu überwachen und einzuschränken. In Diktaturen selbstverständlich, in Demokratien braucht es dazu spezielle Gesetze.
Durch die Verfügbarkeit neuer Technologien entstehen immer wieder "Begehrlichkeiten" in Richtung Überwachung.

Verschiedene Angriffe aus der Geschichte

- Frankreich, ab 1971: "Tachygraf", optischer Telegraf zur Übermittlung von Nachrichten über große Strecken. Aufgrund eines Missbrauchfalls wird private Kryptographie in Frankreich verboten (erst in den 90er Jahren wieder aufgehoben).
- USA: Nach dem 2. Weltkrieg Exportverbot für kryptographische Methoden, werden als "Munition" definiert.
- USA, 1993-96: Versuch, alle Verschlüsselungsmethoden in Telefonnetzen bis auf den standardisierten "Clipper Chip" (mit Hintertür für Überwachung) zu verbieten.
- USA, 2001: Als Reaktion auf den Anschlag am 11. September werden "Anti-Terror"-Gesetze verabschiedet, die staatliche Überwachung verstärken um gegen Terroristen vorzugehen. Diese Gesetze werden leider missbraucht, um z.B. gegen illegales Glücksspiel vorzugehen.
- Projekt Echolon: Abhörung sämtlicher Kommunikation durch die NSA und beteiligter Länder. Die Daten werden automatisch nach Reizworten durchsucht. Es existiert allerdings kein Beweis für Echolon.

Überwachungskameras

- In Österreich sind laut Schätzungen über 100.000 illegale Überwachungskameras mit Aufzeichnungsfunktion in Betrieb.
- London, 2002: Laut Schätzungen mehr als 500.000 Kameras.

- United Kingdom, 2005: ca. 4,7 Mio. Kameras im Einsatz. Auch die private Nutzung (Geschäfte, Privatpersonen) nimmt stark zu.

Argumente

- Befürworter: sinkende Kriminalität, Angst der Unschuldigen nimmt ab
- Gegner: haben keine Auswirkungen auf Verbrechensrate (statistisch)
- Tatsächlicher Effekt: Kameras haben kaum Auswirkungen auf Verbrechen, können aber durchaus für andere Zwecke genutzt werden (unerwünschte Personen vom Stadtzentrum fernhalten, Kontrolle, Überwachung)
- Problem: Niemand überwacht die Überwacher. Wer sagt, dass Kameras nicht missbraucht werden?
- Gewöhnungseffekt: Nach 12-18 Monaten kümmert sich kaum einer um die Kameras bzw. findet einen Weg, die Überwachung zu umgehen.

Umkehr der Unschuldsvermutung

- In Einzelfällen (Verdacht auf Terrorismus) wird schon eingeschritten, wenn sich eine überwachte Person verdächtig verhält.
- Das entspricht einer Umkehr der Unschuldsvermutung (Schuldig, sobald Beweis für begangene Tat vorliegt, also nicht schon bevor die Tat überhaupt begangen wurde).
- Beispiel: In Brasilien wird ein Mann erschossen, weil er plötzlich losrennt. Die Polizei dachte, er wäre ein Selbstmordattentäter (war er aber nicht).

Biometrische Identifikation

Identifikation aufgrund von Körpermerkmalen. Zwei Anwendungen.

- Für mich, z.B. Fingerabdruckscanner am Notebook
- Über mich, z.B. biometrische Daten im Reisepass

Probleme

- Nicht alle Menschen sind gleich, bei manchen sind biometrische Merkmale wie Fingerabdruck oder Iris zu schwach ausgeprägt.
- Alles lässt sich irgendwie fälschen, bei Fingerabdrücken ist das sogar ziemlich einfach.
- Missbrauch: Genetische Tests an Mitarbeitern
- Biometrische Identifikation hat den Anspruch auf Richtigkeit, aber es gibt trotzdem immer wieder Fälle von Verwechslungen.
- Identitätsdiebstahl ist trotz allem immer noch möglich. Durch die vorgegaukelte Sicherheit biometrischer Maßnahmen ist es sehr leicht, mit einer erfolgreich gefälschten Identität durchzukommen (keine Fragen, etc. solange der Ausweis "stimmt").

Vorratsdatenspeicherung

Der Gesetzliche Auftrag an Datenverarbeiter, diese eine bestimmte Zeit lang zu speichern und auf Abruf von autorisierter Stelle bereitzuhalten.

- Telefon- und Handyverbindungen, Internet, E-Mail-Verkehr, Fax, SMS, etc.
- Müssen bis zu 6 Monate bzw. 1 Jahr vom jeweiligen Verarbeiter (Provider) gespeichert werden.

- Seit 9.11. in Deutschland, demnächst auch in Österreich (Druck von Seiten der EU).
- Probleme: Hohes Missbrauchsrisiko (Daten könnten an Dritte weitergegeben werden), Kosten für die Provider, Verstoß gegen Grundrechte (informationelle Selbstbestimmung), ...
- In ganz Europa gibt es massiven Widerstand seitens der Datenschützer.

Andere staatliche Angriffe

- USA: öffentliche Liste von Sexualstraftätern
- Elektronischer Reisepass (RFID-Chip). Problem: nicht abhörsicher, biometrische Merkmale schlagen zu 10% fehl. (In Österreich werden derzeit noch keine biometrischen Merkmale auf dem Pass gespeichert, in Deutschland sind Fingerabdrücke erforderlich).
- Verdeckte Online-Durchsuchung aka. "Bundestrojaner". Ab 2008 dürfen in Österreich Ermittler Festplatten Verdächtiger über das Internet absuchen.

Zitate

- Prof. Viktor Mayer-Schönberger meint, dass eine Gesellschaft, die nicht in der Lage ist, Informationen zu vergessen, mit der Zeit verrückt wird.
- "Ich habe manchmal den Eindruck, wir werden ähnlich stark überwacht wie seinerzeit die DDR-Bürger von der Stasi" - Karl Korinek, Präsident des österr. Verfassungsgerichtshofes. Seiner Meinung nach verdrängt der Wunsch nach Sicherheit nach und nach wichtige Grundrechte.

Private Angriffe

Im Gegensatz zu staatlichen Angriffen gibt es auch genügend private Angriffe auf die Privatsphäre des Individuums. Im Gegensatz zu staatlichen Angriffen sind diese meist illegal.

- Profiling, Spyware, Spam
- Monitoring Systeme, Tempest Attacke
- Social Engineering

Profiling

- Amazon.com: "Sie haben X gekauft, wollen Sie nicht auch Y kaufen?"
- TiVo in den USA: Stellt ein individuelles Profil aus den aufgenommenen Programmen jedes Nutzers zusammen.
- Cookies, vor allem die Sorte die nie abläuft. Google kann damit die Suchprofile den verschiedenen Nutzern zuordnen.
- HTTP Referer wird oft benutzt, um einen Statistik zu erstellen, wer von welcher Seite kommt.
- Internet Mining: Gezielt nach Personen mit gewissen Internetdaten suchen. Beispiel: Suche nach allen Menschen, die "gefährliche" Bücher in der Amazon.com-Wunschliste haben.
- Web 2.0: Viele Nutzer veröffentlichen freiwillig Daten. Diese können aber auch von potentiellen Arbeitgebern gefunden und außerhalb des Kontexts verwendet werden. Der Standard berichtet, dass bei 40% aller Bewerbungen der Arbeitgeber potentielle Kandidaten mittels Google überprüft und auch aussortiert.
  Soziale Netzwerke wie Facebook und StudiVZ sind hier besonders "gefährlich".

- Auswege: Anonymes Auftreten (z.B. unter einem Pseudonym), über einen Proxy surfen, Remailer wie Trashmail oder Mailinator, Bugmenot (Logindaten teilen).

Spyware

Software, die unerkannt im Hintergrund läuft und Nutzerinformationen über Surfverhalten, laufende/installierte Programme, etc. an einen Dritten weitergibt. Das ist Informationsdiebstahl.

Spam

Massenmails, die an tausende willkürlich gewählte Mailadressen verschickt werden. Meistens mit Werbung oder dubiosen Angeboten. Laut Studien haben 11% aller Internetuser schon etwas aufgrund von E-Mail-Spam gekauft. 9% sind schon einmal auf einen Internetbetrug hereingefallen.

Tempest-Attacke

Auffangen elektromagnetischer Wellen. Damit ist es z.B. möglich, das Bildsignal eines Röhrenmonitors durch eine Wand hindurch zu rekonstruieren. Oder die Datenkommunikation zwischen RFID-Chip und -Leser abzuhören.

Social Engineering

Ausnutzen menschlicher Schwächen.

- Benutzer dazu bringen, ihr Password zu verraten.
- "Hier ist die EDV-Abteilung. Wir bräuchten Ihren Zugangscode, weil uns ..."
- "Shoulder Surfing"
- Unsichere Passwörter erraten.
- Müll durchsuchen.
- "Spear Phishing" - im Internet gezielt Personen suchen, deren Schwächen man ausnutzen kann (Beispiel: Uhrensammler)

Online Tracking

Am Beispiel von Facebook. Wenn ein Facebook-Nutzer in einem Internet-Shop etwas kauft, wird das auf seiner Seite vermerkt und kann von seinen Facebook-Freunden gesehen werden. Inzwischen ist dieses "Feature" allerdings nicht mehr zwingend.

Schutz der Privatsphäre

Gesetzlicher Schutz: Österreichisches Telekommunikationsgesetz, Datenschutzgesetz.

Telekommunikationsgesetz

Regelt Datenschutz bei Telediensten. Ein Zusatz verbietet Spam-Mails. Das ist allerdings wirkungslos, weil es nur für Absender innerhalb Österreichs gilt und die meisten Spam-Mails aus dem Ausland kommen.

Datenschutzgesetz - Auskunftsrecht

"Nach der Verfassungsbestimmung des §1 DSG 2000 hat jedermann das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden."
Allerdings hat sich dieses Gesetz noch nicht richtig etabliert.

Novelle zum Sicherheitspolizeigesetz

Mit dem Abänderungsantrag 2007 werden Sicherheitsbehörden berechtigt, von Betreibern Auskunft über gespeicherte Daten zu erhalten, auch ohne richterlichen Beschluss und nur auf Verdacht. Das betrifft auch Internetprofile und Auskunft über IP-Adressen (welcher Nutzer, Name + Adresse hatte zu diesem Zeitpunkt diese IP-Adresse). Vorraussetzung für derartige Auskünfte: "Gefahr im Verzug", ein dehnbarer Begriff.

Privacy Policies

Viele Webseiten geben als freiwillige Verpflichtung sogenannte "Privacy Policies" - Richtlinien zur Privatsphäre der Benutzer - an. Probleme sind oft die Komplexität solcher Policies (Rechtssprache), oft sind sie auch schwer zu finden.

Kryptographie

Als technische Schutzmaßnahme der Privatsphäre steht Kryptographie zur Verfügung. Ein gemeinsames Problem aller Verfahren ist der Schlüsselaustausch, der über einen gesicherten Kanal erfolgen muss. Ein gewisses Risiko stellt dabei die "Man-in-the-Middle-Attack" dar. Lösungsansätze sind Public-Key-Parties oder alternative Kanäle (Telefon, Postweg) bei denen die Identität des Absenders besser überprüft werden kann.

Steganographie

Eine Methode, um geheime Informationen auszutauschen ohne dass ein Dritter mithören kann. Dazu wird die Nachricht/Information in einem Trägermedium versteckt, wodurch die Bedeutung der Übertragung verschleiert wird.
Beispiel: Text (binär, verschlüsselt) in einem Bild verstecken; bei richtiger Anwendung ist zwischen Bild mit verstecktem Text und Originalbild mit bloßem Auge/statistischen Verfahren kein Unterschied festzustellen.

Pseudonyme

Verwendung eines Decknamen, um die eigene Identität nicht preisgeben zu müssen. Damit wird bei Internetangelegenheiten der Bezug zur realen Person vermieden. Mit Hilfe eines Proxys/Anonymisierungsnetzwerks kann auch die eigene IP versteckt werden.
Aber: Wollen wir wirklich in einem pseudonymisierten öffentlichen Raum leben?

Praxistipps

- mailinator.com - Mailgateway
- bugmenot.com - Gemeinsam verwendete Logindaten; Online-Registrierung umgehen
- automatisches Laden von Bildern in E-Mails ausschalten (Webbugs!)
- Mailadressen auf Webseiten nie im Klartext angeben

- Kein HTML in E-Mails verwenden
- Zertifikat besorgen und E-Mails siginiert, verschlüsselt versenden (z.B. thawte.com)

Copyright/Urheber/Patentrecht

Die Idee des geistigen Eigentums stammt aus der Renaissancezeit, vorher gab es nur materiellen Besitz.

Intellectual Property

Idee: Zeitlich befristeter Schutz, damit der Autor eine Zeit lang alleine von seiner Idee profitieren kann.
Zwei Traditionen:

- Angloamerikanisch: "Copyright", reines Verwertungsrecht, übertragbar
- Europäisch: Urheberrecht, nicht übertragbar

Zwei Standpunkte im Patentrecht:

- Individuum: Will von seiner Idee profitieren und vor Konkurrenz geschützt sein
- Gesellschaft: Sieht sich als "Framework" für Kreativität. Will Idee des Individuums verwenden und verwerten.

=> Urheber- und Patentrecht ist ein Kompromiss zwischen diesen Standpunkten.
Typischerweise gibt es auch Schrankenbestimmungen, die das Copyright beschränken: Privatkopie, Bibliotheken, Videotheken, Privatverkauf, Zitieren, Universitäten, etc.
Neue Technologien (Peer-to-Peer) drohen das Gleichgewicht ins Wanken zu bringen. Der freie Informationsaustausch wird immer einfacher und unkontrollierbar, d.h. die Gesellschaft profitiert mitunter auf Kosten des Individuums.

Geschichte

- Pianola: automatisches Klavier. Hersteller kaufen Noten und machen daraus Pianola-Rollen. Die Folge: Notenverlage protestieren heftig und fordern den Verbot des Pianolas. Lösung: Für jede hergestellte Pianola-Rolle müssen 2c an den Notenherausgeber bezahlt werden.
- Plattenspieler: John Philip Sousa geht zum US-Kongress und gibt dort massive Bedenken an. Plattenspieler würden die Kultur des Landes gefährden, weil die Menschen nicht mehr selbst Musik machen würden.
- Erster Videorekorder von Sony, 1975: 1976 wird Sony von Disney und Universal (Filmproduzenten) verklagt. Die Klage wird abgewiesen.

Copyright

Das Recht, über einen bestimmten Zeitraum der alleinige "Publisher" von bestimmten Ideen zu sein. Das ist kein Schutz von Ideen, sondern ein Schutz des Publikationsrechts und soll Anreiz sein, Neues zu schaffen.

Patentrecht

Das Recht, über einen bestimmten Zeitraum der Einzige zu sein, der eine erfundene Methode anwendet, im Austausch für deren Veröffentlichung über das Patentamt.

- Anreiz zu Innovation, Austausch und Konkurrenz.
- Kein Schutz von Ideen, sondern von Verfahren.
- Durch Offenlegung entsteht auch ein gesellschaftlicher Nutzen (sobald das Patent

ausläuft).

Wie lange währt das Schutzrecht?

- US-Copyright - Ursprünglich: 14+14 Jahre (1 Verlängerung möglich)
  Heute: Lebenszeit des Autors + 50 bzw. 70 Jahre, 1 Verlängerung +70 möglich
  Seit 1998: 20-Jähriges "Moratorium" auf das Auslaufen durch "Sonny Bono Copyright Extension Act" (um Mickey Mouse zu schützen).

Fair Use

- Ursprünglich sieht jede Art von Copyright "Fair Use" vor
- USA - Copyright Act of 1976: "... the fair use of copyrighted work, [...] for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright."
- Üblicherweise anerkannt: Exzerpte, Parodien, Zitate, Auszugsweise Kopien (z.B. zum Lernen), Time-shifting, Space-shifting, Format-shifting, Backups

Technologisch verursachte Problemfelder

Patentierbarkeit von Software

- Im Laufe der 80er-Jahre beginnt man in den USA, alle Patentanträge entgegenzunehmen, auch auf Software und Geschäftsabläufe. Ein Verfahren, das patentiert werden kann, muss innovativ, nicht offensichtlich und nützlich sein.
- EU: Das europäische Patentamt folgt dieser Praxis, allerdings ohne gesetzliche Grundlage. In Österreich nach wie vor keine Patentierbarkeit von Software.
- 1999: eolas verklagt Microsoft wegen Patentverletzung (Plugins). Außergerichtliche Einigung.
- IPIX vs. kleine Software-Entwickler und Free Software. Teilweise mit Erfolg. (IPIX ist ein Unternehmen, dessen Hauptgeschäft das Aufkaufen und Verwerten von Patenten ist).
- 2006: Mehr als 40.000 Software-Patente erlassen. Insgesamt gibt es aber nur 400.000 Patente. Viele dieser Sofwarepatente sind Trivialpatente. Z.B. US-Patent 7,212,296: Priority-Queue. Ein durchschnittlicher Webshop verletzt 20 Trivialpatente.
- Oft findet man auch Patente, die bewusst allgemein formuliert sind, damit sie eine große Bandbreite abdecken.
- Diese aggressive Patentpolitik zeigt jetzt schon negative Auswirkungen. Die Patentierwut der "großen" wird zu einer Gefahr für kleine und mittlere Softwareentwickler, sowie Free Software. Diese können es sich nicht leisten, gegen große Unternehmen in den Patentkrieg zu ziehen und müssen ihre Software beschneiden, um Patentstreitigkeiten aus dem Weg zu gehen.
- Inzwischen gibt es in Europa ernsthaften Widerstand gegen die Patentierbarkeit von Software. Eine rechtliche Grundlage konnte bis heute aufgrund von Widerstand der Mitgliedsstaaten nicht geschaffen werden.

Verlustfreie Kopierbarkeit digitaler Information

Alles, was in digitaler Form vorliegt, kann verlustfrei kopiert werden, ohne das Original

dabei zu beeinträchtigen. Diese Kopien können mittlerweile in hoher Geschwindigkeit erzeug und verbreitet (z.B. über das Internet, P2P-Netze) werden.
Diese technologische Entwicklung ist eine harte Herausforderung für die Content-Industrie (vor allem Musik-, Film- und Softwareindustrie).
Ergebnis - ein Spannungsfeld:

- Einerseits werden bestehende Strukturen (Musikvertrieb, Hollywood, etc.) stark gefährdet
- Andererseits werden Vertriebs- und Gestaltungsformen möglich, die es vorher noch nie gegeben hat: Mashups, Remixes, Open-Source, Freeware, etc. Es ist für jeden Einzelnen möglich, seine kreativen Ideen ohne großen Aufwand an tausende von Nutzern kostenlos zu verteilen. Und die Industrie sieht das gar nicht gerne.

Peer-to-Peer

Eine Technologie, um Informationen auf demokratischem Weg zu verteilen. Jeder Rechner, der an solch ein Netz angeschlossen ist, hilft mit, das System aufrechtzuerhalten. Damit ist völlig unkontrollierbarer Datenaustausch möglich.

Digital File Check

Auf der anderen Seite gibt es den "Digital File Check", eine von der Content-Industrie bereitgestellte Technologie. Damit ist es möglich, zu überprüfen, ob Musik oder Filme auf dem Rechner "legal" sind. Problem: Es wird alles als illegal markiert und mitunter auch automatisch gelöscht, was nicht von der Content-Industrie kommt.

(Re-)Aktionen

Reaktion der Content-Industrie

Nach Aussagen der Content-Industrie (RIAA, MPAA) stellt das freie Kopieren im Internet einen großen finanziellen Verlust dar. Das Problem ist nur, wie viel kostet es wirklich, wenn jemand einen Film aus dem Internet lädt? Hätte derjenige den Film wirklich gekauft wenn es P2P nicht gäbe? Der tatsächliche Verlust ist schwer abschätzbar.
Eine Studie in Kanada jedenfalls stellte fest, dass Nutzer von Online-Tauschbörsen mehr CDs kaufen. In Kanada gab es auch den Gesetzesvorschlag, eine zusätzliche Gebühr für Internetuser einzuführen und dafür P2P komplett zu legalisieren.

Begriffe

- Raubkopie? Raub = Gewaltsames Aneignen einer fremden beweglichen Sache. Damit ist dieser Begriff überzogen und irreführend.
- Softwarepirat? Pirat = Räuber, der von einem Schiff aus angreift. Wieder nur ein Schlagwort ohne wirklichen Sinn.
- Musikdiebstahl? Diebstahl = Aneignen einer fremden beweglichen Sache. Problem: Bei digitalen Kopien wird die Sache dem Besitzer nicht weggenommen.
- Diese Begriffe stellen eine missbräuchliche Verwendung von Begriffen zugunsten der Content-Industrie dar.

Lobbying

- DMCA mit "Anti-Circumvention Provision" - es ist verboten, Kopierschutz zu umgehen. Entsprechende Regelungen gibt es auch in der "EU Copyright Direktive".
- Click-Thru/Shrink-Wrap Lizenzen:
  Frontpage 2002 EULA: Man darf keine Webseiten erstellen, die Microsoft negativ darstellen, WinXP Professional: Microsoft darf unangekündigt und automatisiert Systemupdates einspielen, Windows 98/.NET/SQL Server: Benchmarks sind verboten.
- Hollings Act: Alle Geräte, die Medienwerke wiedergeben können, müssen mit Sicherheitstechnologien ausgestattet sein, die Missbrauch verhindern.
- Bermann Bill schlug vor, Crack- und DDoS-Attacken gegen P2P-Betreiber legalisieren zu lassen.
- INDUCE: Soll Herstellung von Software und Geräten illegal machen, die zu Copyright-Verletzungen verleiten.
- Massive Klagen gegen Nutzer und Entwickler von P2P
- Einführung "kopiergeschützer" CDs, viele lassen sich nicht mehr ordentlich in Standard-CD-Playern abspielen.
- Entsprechende Kampagnen ("Raubkopierer sind Verbrecher").

Gegenaktionismus

- monochrom.at fordert dazu auf, Fotos von den Copyrightwarnungen in Kinos zu machen.
- Rainer Kuhlen (sinngemäß): Fair Use ist schon allein technisch bedingt, Kopierschutzmaßnahmen können vollständig unterlaufen werden. Außerdem sind bei digitalen Medien Sachen verboten, die früher ganz normal erlaubt waren (Verleihen/ Weitergeben von Büchern ist bei den meisten kommerziellen eBooks nicht möglich).
- DRM-geschützte Musik wurde nie richtig von den Kunden angenommen, weil die Einschränkungen mehr als lästig waren. Die Folge: Heute wird so etwas kaum noch verkauft. Außerdem ist DRM viel restriktiver als es normale (weitgehend ungeschützte) CDs sind. Allerdings steht in den Nutzungsbedingungen der meisten Online-Musikanbietern immer noch, dass die Musik nicht weiterverkauft, verliehen, geteilt oder vermietet werden darf, was bei CDs problemlos möglich und legal ist.
- Lawrence Lessig: Kampf gegen Piraterie ist eine Perversion der Copyrightgesetze.

Participative Culture

Dieser Begriff bezeichnet eine neue Kultur, die durch den technologischen Wandel begünstigt/ermöglicht wird. Wie der Name schon sagt, geht es darum, dass jeder Benutzer gleichzeitig auch Anbieter von Information sein kann. Duch P2P-Netze wird der unbürokratische und größtenteils kostenlose Austausch von Information und Unterhaltungsmedien aller Art ermöglicht. Leider ab und zu auf Kosten der Unterhaltungsindustrie, die nach wie vor Geld auf die Hand haben will.

Medienindustrie vs. aktueller Trend

- Wunsch der Medienindustrie: Aus Usern sollen Konsumenten werden, der Computer ist ein Organ, das die Medienkonsumation überwacht. Das Internet ist ein reiner Zustelldienst von Information und Unterhaltung.
- Aktueller Trend: Aus Usern werden Teilnehmer einer neuen Kultur, von der der

Gesetzgeber keine Ahnung hat. Der Computer ist ein Medium, das neue Ausdrucksmöglichkeiten anbietet. Das Internet ist ein zweiseitiges Kommunikationsmedium.
- Beispiele für die "neue Kultur": Computerspiel-Levels, Mashups, Remixes, Open Source, Web 2.0, Machinimas, Mods, Youtube, Demoszene, ...

Copyright vs. Copyleft

- 1982: MIT steigt von selbstentwickeltem System auf closed-source UNIX um.
- Richard Stallman kann das nicht einsehen und gründet die Free Software Bewegung.
- Als Folge entsteht die GPL, GNU, und später GNU/Linux.
- GPL ist eine virale Lizenz (alles, was GPL-Code verwendet wird automatisch auch GPL) -- Richard Stallman nennt dieses Konzept in einem Anfall zweifelhafter Kreativität Copyleft.
- Der Vorteil von GPL ist, dass der Sourcecode mitveröffentlicht wird, der Nachteil dass man diesen Code nur nutzen kann, wenn man selbst ein haariger Softwareaktivist ist.
- Microsoft versucht seither mit allen Mitteln, Open Source und Free Software aufzuhalten, vor allem weil viele Firmen und Serverbetreiber von Microsoft-Produkten auf kostenlose Open-Source-Software umsteigen.

- CC-Bewegung: Statt Copyright werden nur noch bestimmte Grundrechte (kann sich jeder selbst aussuchen) vorbehalten. Das bezeichnet man dann als (cc) anstatt von (c).
- Hier gibt es auf Wunsch ebenfalls virale Elemente (Nutzung nur erlaubt, wenn Ergebnis ebenfalls (cc) mit denselben Bedingungen ist).
- Übliche Möglichkeiten sind, kommerzielle Nutzung und Veränderung (optional mit viraler Komponente) zu erlauben. Private, kostenfreie Nutzung ist bei (cc) standardmäßig integriert.
- Die CC-Lizenz wird in der Praxis vor allem auf digitale Medien (Video, Bilder, Text) und weniger auf Software (hier gibt es schon Lizenzen wie GPL, die sich mit der Sourcecodeproblematik auseinandersetzen) angewandt.
- Flickr-Kultur (hier findet man viele CC-Lizenzierte Fotos).
- Reaktionen der Medienindustrie: Creative Commons ist ein kommunistisches Konzept, das ausgeräuchert werden muss.