Ende des Internet?

von: John Walker (2004)

Vortrag und Folien von: Denny Arnold

Gliederung:

- Das Internet im Vergleich mit anderen Medien
- Die Entwicklung des Internet in den 1990er Jahren
- Abschirmung durch Firewalls
- Zertifikate und Trusted Computing
- Quellen

Das Internet und andere Medien

konventionelle Medien:

- „one-to-many“-Medien
  - Fernsehen, Radio oder Printmedien (Zeitungen Magazine oder Bücher)
  - wenige Sender (Fernseh-, Radiostationen und Verleger) und viele Konsumenten(Zuschauer, Zuhörer und Leser)
  - Hohe Kosten für das Erreichen der Konsumenten
    - teure Sendestationen, Satelliten oder neue Publikationen
    - folglich muss ein großes Publikum erreicht werden um diese Kosten zu decken
    - kleine Interessengruppen können nicht erreicht werden
    - Neulinge haben es schwer : es fehlen finanzielle Mittel oder einflussreiche Beziehungen

- „one-to-one“-Medien
  - Post, Telegramme oder Telefon
  - globale Kommunikation von Person zu Person
  - Nachteil: über größere Entfernung höherer Kosten- und Zeitaufwand

das Internet als „many-to-many“-Medium:

- viele Sender und viele Empfänger
- jeder kann Sender und Empfänger sein(Server/Client)
- vereint die Vorteile der „one-to-one“- und der „one-to-many“-Medien
  - Kommunikation zwischen zwei Personen (e-Mail, Messaging), von einer Person zu vielen Personen (Webpages) oder von vielen Personen untereinander (Diskussionsforen)
- Bruchteil der Kosten herkömmlicher Medien
- keine regionale Beschränkung der Erreichbarkeit wie bei Rundfunk oder Printmedien
- jeder mit einem Internetzugang kann seine Ideen und Gedanken der Masse präsentieren nahezu ohne Zensur oder andere Beschränkungen

Folgen des Internetbooms:

- Verlust von Konsumenten für die Medienkonzerne (Fernsehsender, Musiklabels, Verleger etc.) und damit sinkender Umsatz
- schnelle und leichte Verbreitung von OpenSource-Software stellt eine große Konkurrenz dar für Softwarefirmen
- Verlust von Kontrolle durch staatliche Institutionen
  - wenige Massenmedien lassen sich leicht kontrollieren durch Zensur, unzählige Internetseiten, Foren und e-Mails lassen sich nicht kontrollieren
  - verschiedene politische Gruppierungen können nahezu anonym kommunizieren (z.Bsp. Terroristen)
- es liegt nahe, dass Medienkonzerne, Regierungen und Softwarefirmen versuchen die klassische Rollenverteilung (Produzent-Konsument, Regierung-Individuum) wiederherzustellen

„..innerhalb der nächsten 5 bis 10 Jahre werden wir sehen, wie der Flaschengeist Internet wieder in seine Flasche zurückgedrängt werden soll.“

„Das Internet: Ein historischer Fehler“

Der Anfang:

- das Internet entwickelte sich aus dem ARPANET
- ARPANET (Advanced Research Projects Agency Network) wurde in den USA entwickelt und 1969 in Betrieb genommen
- es vernetzte einige amerikanische Universitäten, welche für das Militär forschten

- Jede Maschine im Netz hat eine 32-Bit lange Internet-Protokoll(IP)-Adresse (IPv4)
- dargestellt in der „dotted quad“ Form (Bsp: 192.168.047.110)
- verbunden sind die Maschinen über eine Standleitung in das Netz
- da die IP-Adresse fest an eine Maschine gebunden ist, folgt eine gewisse Verantwortung des Benutzers, da die Adresse zurückverfolgt werden konnte
  - bei Maschinen mit mehreren Benutzern konnte dementsprechend der verantwortliche Benutzer ermittelt werden

- Blöcke von fortlaufenden Nummern wurden an Organisationen übergeben (z.Bsp. 152.0.0.0. bis 152.255.255.255)
- Organisationen können Teilblöcke auch an andere Organisationen weitergeben

Technische Auswirkungen durch den Boom der 1990er:

- das 32 Bit Adressierungssystem umfasst ca. 4.000 Millionen einzigartige Adressen
- im Vergleich: 1999 betrug die Weltbevölkerung 6.000 Millionen Menschen, heute über 6.600 Millionen
  Quelle:*http://www.weltbevoelkerung.de*
- also sollten 4.000 Millionen Adressen völlig ausreichen
  - Aber: Die Adressen wurden durch die Blöcke oft sehr ungünstig verteilt
  - viele Adressen werden nicht benutzt

- in der Praxis wurde klar die Adressen sind bald erschöpft
- 1997 gibt es in Europa 19,45 Mio. Internetnutzer
- 2001 bereits schon 119 Mio. Internetnutzer in Europa
  - Quelle:*http://www.eds-destatis.de*
- Lösung: Erweiterung des Adressraums

Die Ausdehnung des Adressraums:

- 1991 begann die Internet Engineering Task Force (IETF) mit der Entwicklung eines 128 Bit Adressprotokolls
- 1995 wurde dieses Protokoll mit dem Namen IPv6 fertiggestellt
- selbst wenn jeder einen eigenen 48 Bit Adressraum bekäme, gäbe es Adressen für 1.2×10^{24} Internetnutzer
- Eine Umstellung auf IPv6 hätte jedoch bedeutet, dass Betriebssysteme, Anwendungen, Router und Netzwerkknoten hätten umgerüstet werden müssen
- der Adressraum war bereits sehr knapp und die Umstellung hätte zu lange gedauert
- theoretisch hätte das 32 Bit Adressprotokoll über IPv6 „getunneln" können, jedoch haben alle Firmen, alles in den Ausbau des IPv4 investiert
- man musste Maßnahmen entwickeln um mit IPv4 klar zu kommen

„Jede dieser Maßnahmen aber hatte die unbeabsichtigte Folge, das Internet von dem ursprünglich geplanten reinen Peer-Netzwerk zu einem Netzwerk mit „Publizisten" und „Konsumenten" umzuwandeln und dabei die Anonymität des Internetzugangs zu erhöhen"

Die dynamischen IP Adressen:

- viele Internetbenutzer haben sich nur für kurze Zeit eingewählt
- warum sollten diese Nutzer eine feste Adresse haben, wenn sie eh nie erreichbar sind?
- Die Lösung ist eine dynamische IP Adressierung

- beim Einwählen bekommt man eine IP-Adresse zugewiesen, die bis zur Trennung aufrecht erhalten wird
- ein Benutzer mit dyn. Adressierung konnte nun aber nicht mehr erreicht werden unter einer festen Nummer
- die Lösung brachten Dienste wie ICQ, DynDNS oder No-IP-Server
- die IP-Adressen wurde ausgetauscht und so konnte wieder der normale Peer-to-Peer Kontakt aufgenommen werden
- Nachteil: eine zentrale Schwachstelle z.Bsp. bei Ausfällen, aber auch eine kontrollierbare Stelle (wie zum Beispiel Napstar)

Abschirmung durch Firewalls

<u>Netzwerkadressübersetzung NAT und Router:</u>

- wird von Routern verwendet, damit mehrere Rechner einen gemeinsamen Internetanschluss benutzen können
- NAT teilt dem aufgerufenen Internetdienst eine Quellportnummer mit, über diese dann der Dienst mit dem richtigen Rechner kommunizieren kann
- NAT lässt nur eingehende Verbindungen einer bestimmten Quelle zu, wenn der Nutzer zuerst eine Verbindung zu dieser Quelle aufgebaut hat
- der Nutzer ist somit vom eigentlichem Internet abgeschirmt und kann keine eigenen Dienste anbieten, da NAT alle eingehenden Verbindungen verwirft
- er wird in die Rolle des Konsumenten gezwungen, weil er auf Dienste anderer angewiesen ist
- solche Dienste können eine Kommunikation zwischen 2 NAT Nutzern ermöglichen, jedoch müssen sie alle Daten „durch leiten“
    - Möglichkeit der Kontrolle, Überwachung oder sogar Manipulation
- die meisten Router können definierte Ports öffnen um direkt erreichbar zu sein aber:
    - vielen Nutzern fehlt die Kompetenz diese Einstellung zu tätigen
    - der Internetanbieter kann bestimmen, welche Router er dem Kunden zur Verfügung stellt
- NAT ist sozusagen eine einfache Firewall, lässt aber trotzdem Würmer und Viren von Browsern oder E-Mail Clients durch

- asynchrone Breitbandzugänge
  - hohe Downloadbandbreite aber sehr geringe Uploadbandbreite
  - der Nutzer ist sehr beschränkt, wenn er selbst Dienste anbieten möchte mangels Upload

- öffentliches WLAN
  - auch ein NAT-Netzwerk
  - Routereinstellungen kann nur Administrator durchführen
  - in öffentlichen WLAN daher starke Beschränkung

Zertifikate und Trusted Computing

<u>Was ist ein Zertifikat?:</u>

- eine Art elektronischer Pass
  - identifiziert einen Benutzer eindeutig
  - mit einer eindeutigen Bitfolge, wie die Passnummer
- wird ausgestellt von einer Zertifizierungsstelle, welche für die Authentizität haftet
- Glaubwürdigkeit des Zertifikats hängt vom Ruf der Zertifizierungsstelle ab
- eingesetzt werden Zertifikate zum Beispiel in e-Commerce-Seiten oder e-Mail-Programmen
- der Nutzer ist verpflichtet sein Zertifikat zu schützen wie seinen Pass, Kreditkarte oder ähnliches

- Zertifikat besteht aus 2 Teilen: privater und öffentlicher Teil:
  - privater Teil:
    - ist unbedingt geheim zu halten
    - unterzeichnet Dokumente, legitimiert Zahlungen, entschlüsselt e-Mails
  - öffentlicher Teil:
    - identifiziert den Nutzer anderen Nutzern gegenüber
    - wie eine Telefonnummer

Was kann zertifiziert werden?:

- natürliche Personen:
  - jeder kann ein Zertifikat einer Zertifizierungsstelle bekommen, wenn er seine Identität nachweisen kann

- Minderjährige:
  - können auch Zertifikate erhalten mit Einverständnis der Erziehungsberechtigten
  - Zertifikate können ungeeignete Informationen aus dem Netz blockieren oder filtern

- Unternehmen/Organisationen:
  - Zertifikat gilt hier als „Qualitätssiegel“ speziell für Online-Shops
  - alle Unternehmensformen, non-Profit Organisationen, Bildungseinrichtungen oder staatliche Institutionen können Zertifikate bekommen, wenn sie sich ausreichend ausweisen
  - Unternehmen können auch „Sub-Zertifikate“ erstellen, welche Abteilungen, Büros oder sogar einzelnen Mitarbeitern zugeordnet sind
  - Mitarbeiter können so zur Verantwortung gezogen werden, wenn sie falsch handeln

- Computer:
  - zur Zeit meist nur Seriennummer auf Chips
  - in Zukunft wird eine Maschine zertifiziert werden können
  - somit ist die Maschine eindeutig identifiziert
  - Software könnte freigeschaltet werden, welche nur für diesen Computer lizenziert wurde
  - Netzwerktransfer kann eindeutig einer Maschine zugeordnet werden
    - schwindende Anonymität

- Programme:
  - Zertifikat versichert, dass ein Programm nicht von Viren, Würmern und anderer Gefährlicher Software korrumpiert wurde
  - Betriebssysteme können nicht zertifizierte Software verweigern oder Zertifikate im Internet aktualisieren und vergleichen

- Inhalte:
  - Inhalte sind Dokumente, Bilder, Audio, Video, Datenbanken etc.
  - hier wird das Eigentumsrecht und die Authentizität versichert
  - Dateien können vom Ersteller identifiziert und verschlüsselt werden, um sie so zu schützen
  - Dokumente können an Organisationen gebunden sein, ohne Zertifikat kann man die Datei nicht öffnen
    - Bsp: Eine Office-Anwendung zertifiziert und verschlüsselt die Dokumente beim speichern
    - andere Programme wie OpenSource Software können dieses Dokument nicht öffnen, obwohl sie das Dateiformat kennen und lesen könnten

<u>Trusted Computing:</u>

- ist das Zusammenwirken von zertifizierter Hard- und Software
- Jeder Rechner ist eindeutig identifizierbar
- alle Dateien können zertifiziert und verschlüsselt werden
- es kann Korrumpierung von Software beseitigt werden
- Datenaustausch zwischen 2 Systemen wird stark beschränkt sein
- Das Betriebssystem kann Sicherheitslücken schnell erkennen und sich sofort im Internet aktualisieren
- Software wird nur für genau eine Maschine lizenziert werden können
  - Eindämmung von illegaler Programmvervielfältigung
- selbst die unterste Softwareebene das ROM-BIOS kann nur zertifizierte Betriebssysteme zulassen
- im Trusted Computing wird vieles automatisch ohne das Wissen des Nutzers passieren
  - fehlende Transparenz kann zu Datenmissbrauch führen (Datenschutz)
- der Nutzer ist vollkommen Abhängig vom Hersteller und somit ein klassischer Konsument

Quellen:

Telepolisartikel:

http://www.heise.de/tp/r4/artikel/16/16631/1.html
http://www.heise.de/tp/r4/artikel/16/16647/1.html
http://www.heise.de/tp/r4/artikel/16/16648/1.html
http://www.heise.de/tp/r4/artikel/16/16650/1.html
(letzter Zugriff: 09.01.2008)

Demographische Informationen:

http://www.weltbevoelkerung.de
(letzter Zugriff: 09.01.2008)

Internetstatistiken:

Statistisches Bundesamt Deutschland -> Europäischer Datenservice
http://www.eds-destatis.de
(letzter Zugriff: 09.01.2008)