Schönes neues Internet

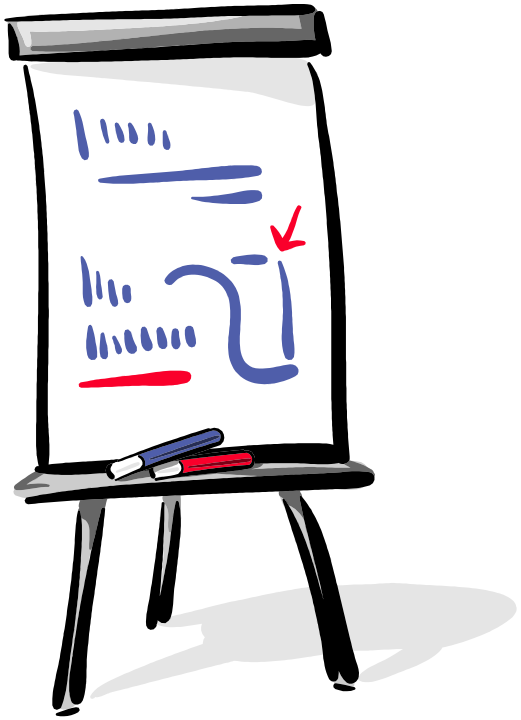
Markus de Brün

Bundesamt für Sicherheit in der Informationstechnik

AK Sicherheit, 7. Oktober 2009

Agenda

- Gefahr aus dem Web
  - aktuelle Lage & Trends
  - Relevanz für Web 2.0
- Web 2.0 Studie
  - Einführung
  - Ajax - Technik
  - Ajax - Folgen
- Schutz
  - ISi-Reihe
  - Weitere Maßnahmen
- (Ausblick)



Gefahr aus dem Web

- Web ist Haupt-Infektionsweg
- Infektionen mit Schadprogrammen
- Früher: E-Mail & Wechseldatenträger
- Heute: Drive-By-Downloads
  - 23.500 infizierte Web-Seiten pro Tag
  - davon 70% kompromittierte legitime Seiten
  - Übertragung von Malware über das Web: +508% (H1, 2009)
  - insgesamt 85% aller Malware über Web verbreitet
  - Schwachstellen in Browsern und Plug-Ins

Browser im Fokus

- IBM XForce Trend Statistics 2008:
  - starker Anstieg an Client-seitigen Schwachstellen mit öffentlichen Exploits von 2004-2008
  - Client-seitige Exploits immer häufiger für Browser statt für Betriebssystem
  - Browser-bezogene Exploits seit 2006 mehr gegen Plug-Ins statt den Browser

Malware im Web 2.0

- Web 2.0 – Seiten primäres Ziel (Breach, 2009)
- Hacking-Vorfälle meist auf Web 2.0 – Seiten (WorkLight, 2009)
- Angreifer widmen ihre Aufmerksamkeit verstärkt Web 2.0 (Sophos, 2009)
- Soziale Netze sind Brutstätte für Malware (Webroot, 2008)

Betroffene Seiten

- 09/09: XSS-Wurm auf Reddit
- 09/09, 08/09, 02/09: Twitter
- 08/08: 1800 Profile auf Facebook mit Trojaner infiziert
- 08/08: Würmer auf MySpace und Facebook versenden Links
- 07/07: Wurm in Videos auf YouTube versteckt
- 12/06: MySpace Wurm sammelt Passwörter
- 06/06: Wurm auf Yahoo-Webmail

Warum Web 2.0

- großes Publikum
- hohe Erfolgsquote durch implizites social engineering
- Möglichkeit eigene Inhalte einzubringen
- Plattformen setzen aktive Inhalte und Plug-Ins voraus
- Schwachstellen in Web 2.0 Tools
- schnelle Verbreitung

Web 2.0 - Einführung

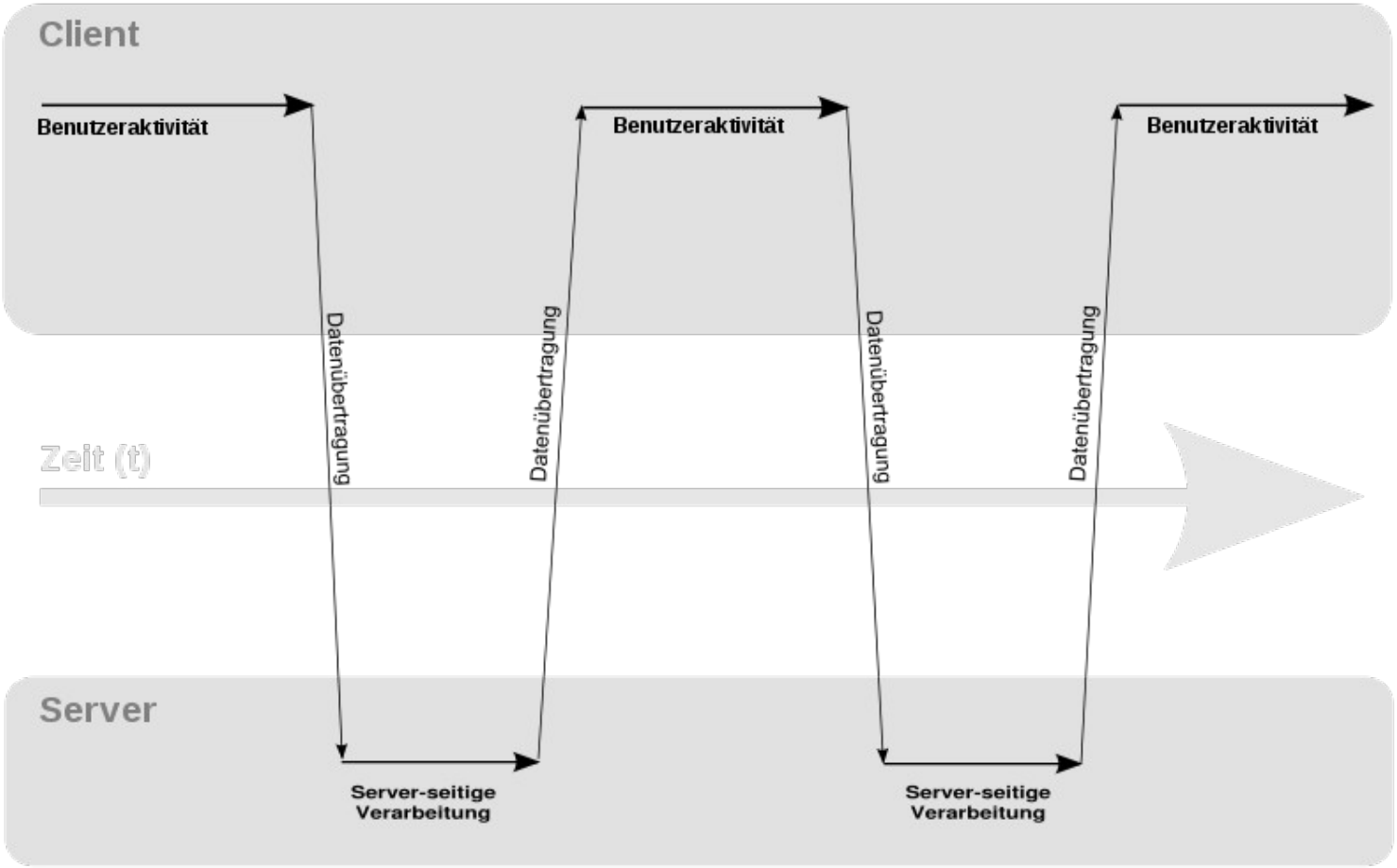
- Beispiele für Web 2.0:
  - Interaktivität
  - Widgets
  - Mashups
  - Soziale Netze
  - Weblogs
  - RSS/Atom
  - Wikis
  - Sharing-Portale
  - …

Ajax

- Asynchronous JavaScript And XML
- Kombination verschiedener Techniken:
  - HTML
  - DOM
  - Javascript
  - XML
  - XMLHttpRequest
- Asynchroner Datenaustausch zw. Client und Server
- Ursprung 1998/99
- Microsoft IE 5.0
- Firefox 1.0

Web 1.0 - Technik

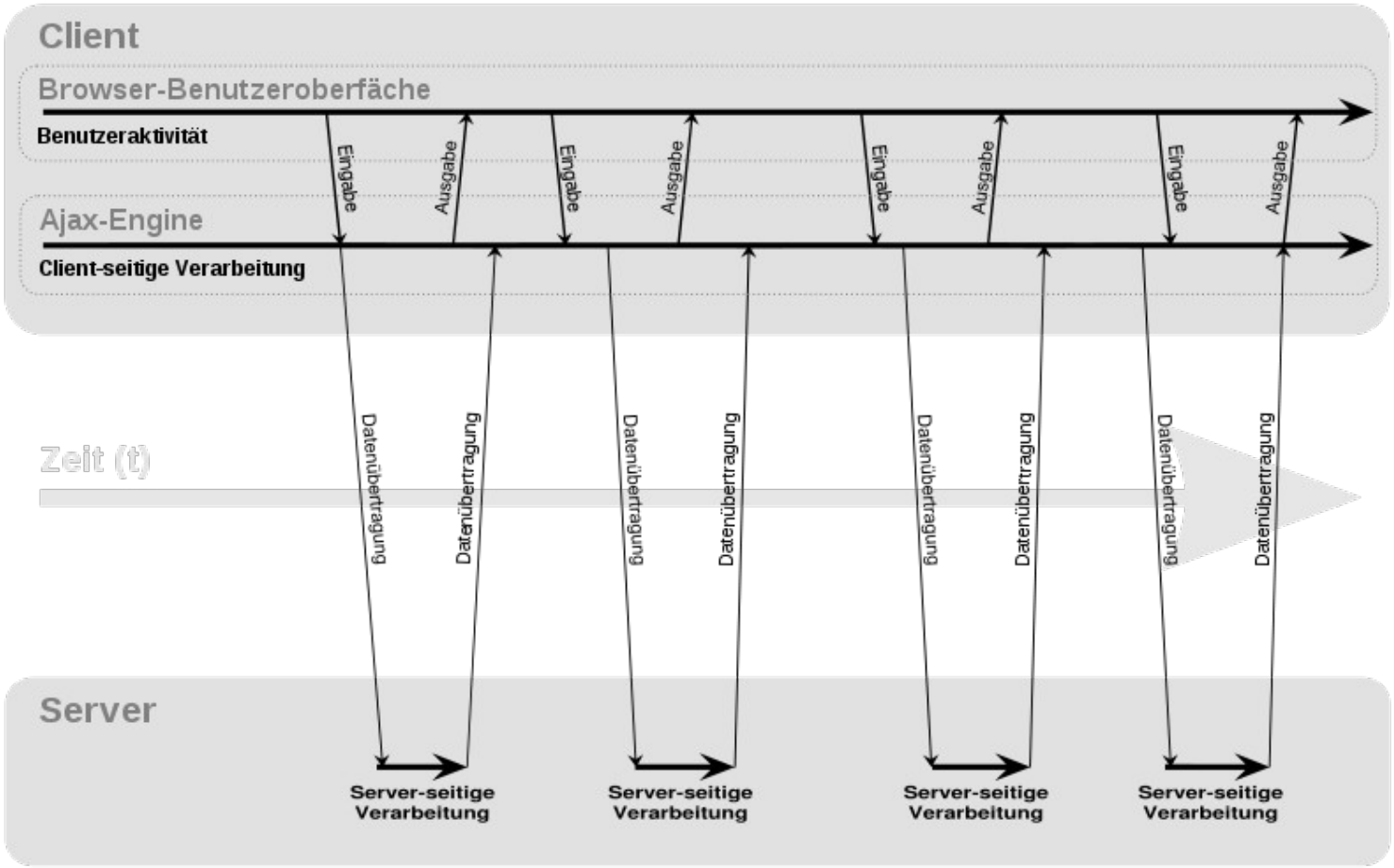
Klassisches Modell einer Web-Anwendung (synchrone Datenübertragung)



Quelle: wikipedia.org

Web 2.0 - Technik

Ajax Modell einer Web-Anwendung (asynchrone Datenübertragung)

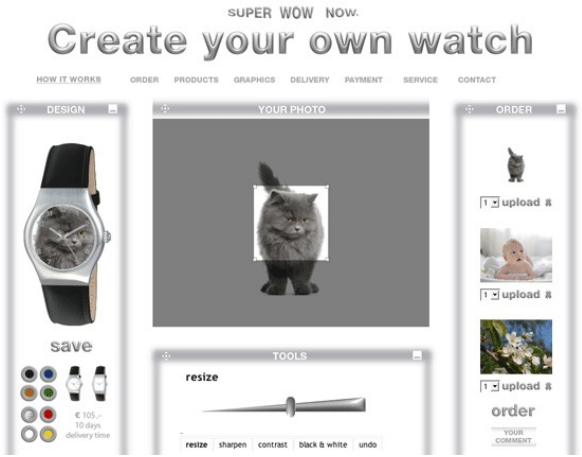


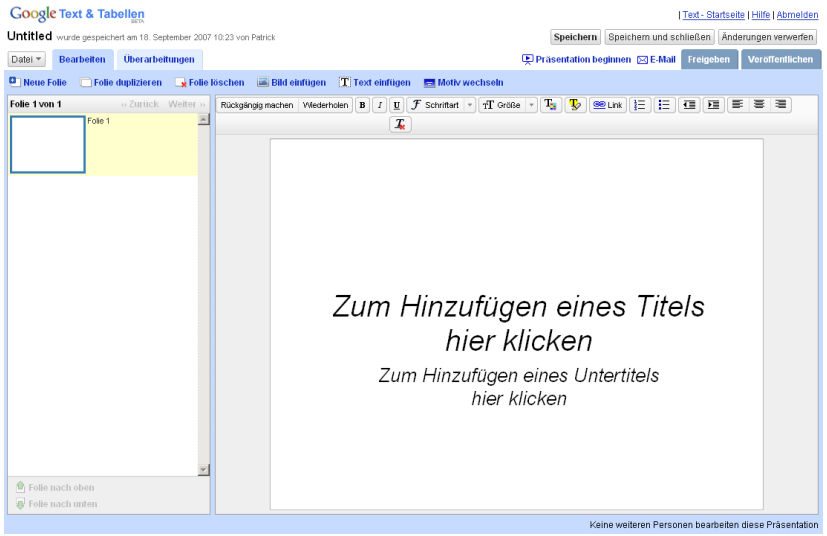
Quelle: wikipedia.org

Ajax - Nutzen

- Interaktive Eingaben →
- Benutzerfreundlichkeit

- Desktop-ähnliche Anwendungen →





Ajax – Probleme

- Nebeneffekte
  - HTTP Verkehr wird für den Benutzer unkontrollierbar
  - keine visuellen Rückmeldungen wie z.B. Ladebalken
  - Nutzer gezwungen AI zu aktivieren

    → Höheres Risiko für die Nutzer
  - Keine Barrierefreiheit

Überblick verloren

- AJAX
  - HTTP Verkehr wird für den Benutzer unkontrollierbar
- RSS & Co
  - Inhalte aus verschiedenen Quellen zusammentragen
- User generated content
  - schwierig legitime und bösartige Inhalte zu unterscheiden
  - anonyme Kollaborationen
  - Unterschiedliche Inhalte machen Plug-Ins notwendig

Was macht mein Browser?

Aufruf von *www.sport1.de*

Was passiert:

- 235 GET Requests
- 63 Javascripts
- 11 Flash-Apps
- 10 verschiedene IPs

Zwischenfazit

- Gefahr aus dem Web so groß wie nie zuvor
  - Verbreitung von Malware
- Unübersichtlicher Verkehr
  - oft unklar, woher Daten stammen
- Häufig vorausgesetzt werden
  - Aktive Inhalte
  - diverse Plug-Ins

Angriffe über AI

- Session-Hijacking
  - Cookies mittels Script klauen
- Cross-Site-Scripting (XSS)
  - 65% der Web-Seiten anfällig
  - Script wird beim Client ausgeführt
- Cross-Site-Request-Forgery (CSRF, Session-Riding)
  - bestehende Session ausnutzen
- Session-Fixation
  - unsicheres Session-Management
  - erleichtert durch Javascript

Beispiel-Angriffe

- Session-Riding in der Online-Shop-Plattform
  - JS im Angebotstext
  - Betrachter bestellt automatisch
- Session-Fixation beim Online-Banking
  - Angreifer holt sich gültige Session-ID
  - Angreifer schiebt Opfer die ID unter
  - Opfer meldet sich an
  - Angreifer hat Zugriff

Angriffe über Plug-Ins

- angebliche Videos oder Applikationen
  - Benutzer soll Plug-In oder Codec installieren
- Drive-By
  - Schwachstelle im Browser oder Plug-In
  - ohne Nutzer-Interaktion
- mit präparierten
  - PDF-Dokumenten
  - Flash-Applikationen
  - Videos

ISi-Reihe

- BSI Standard zur Internetsicherheit
- ISi-Reihe → www.isi-reihe.de
- Module zu verschiedenen Themen:
  - Sicheres Bereitstellen von Web-Angeboten
  - Sichere Nutzung von Web-Angeboten
- Studie, Leitlinie, Checklisten

Maßnahmen

- Server-seitig
  - www.ohne-aktive-inhalte.de
  - Sicherheit wichtiger Aspekt der Entwicklung

    → Ein- und Ausgaben-Filter

    → sicheres Session-Management
- Client-seitig
  - kein AI am Arbeitsplatz

    → ReCoBS, Internet-PCs, Virtuelle Surf-Umgebung...
  - Absicherung

    → Patches, AV, Personal Firewall, …

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Markus de Brün
Godesberger Allee 185-187
53175 Bonn

Tel: +49 (0)22899-9582-5336
Fax: +49 (0)22899-10-9582-5336
markus.debruen@bsi.bund.de

www.bsi.bund.de
www.bsi-fuer-buerger.de
www.isi-reihe.de

Bruteforce 2.0

- Passwort-Datei → Google Docs
- Falsches Datenformat → Dapper
- Angriff zusammenklicken → Yahoo Pipes

- Automatisch
- Anonym
- Alles super

Wurm 2.0

- Wurm 2.0
  - Schwachstelle gefunden
  - schnell ausnutzen
  - möglichst viele infizieren
- Wurm 2.5
  - xssed.org
  - Schwachstellen Beschreibung

    → mit Beispielcode
  - anfällige Seiten
  - automatische Updates