

Browser Poisoning

oder vertrauen Sie Ihrem Internet Explorer / Firefox / Safari ?



SWITCH

Serving Swiss Universities

Rolf Gartmann

rolf.gartmann@switch.ch

informatica08, „Internet Kriminalität“

6. März 2008

Agenda

- Motivation & Ziele
- Übersicht E-Banking
- Angriffsvarianten
- Mögliches Szenario: Browser Poisoning
- Demonstration
- Schutzmassnahmen
- Diskussion

Motivation

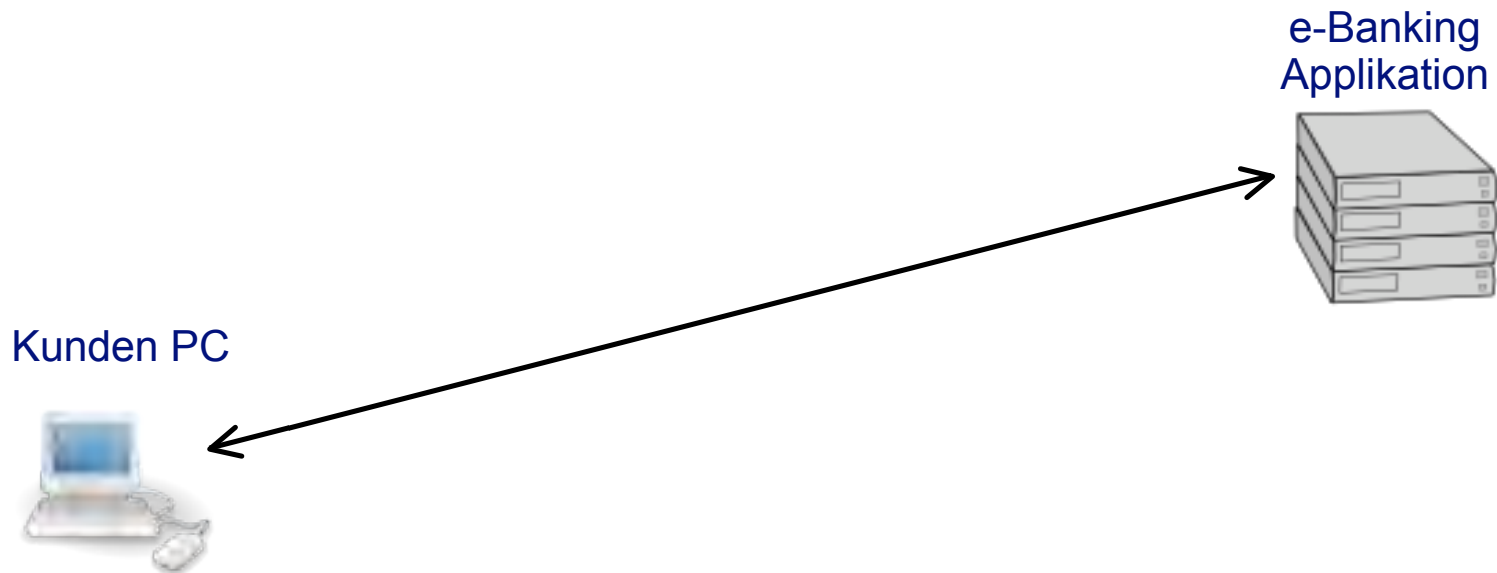
- Als Mitglied eines CERT (Computer Emergency Response Team) generelles Interesse an neuesten Angriffsvarianten im Internet Umfeld
- Eine Antwort auf die Frage finden (2006): „was könnten zukünftige Bedrohungen für e-Banking sein ?“
- Unterstützung Sektor Finanz im Rahmen CIIP Mandats (Critical Information Infrastructure Protection)
- Problematik weitervermitteln anhand einer Demonstration (Bilder sagen mehr als 1000 Worte)

Ziele

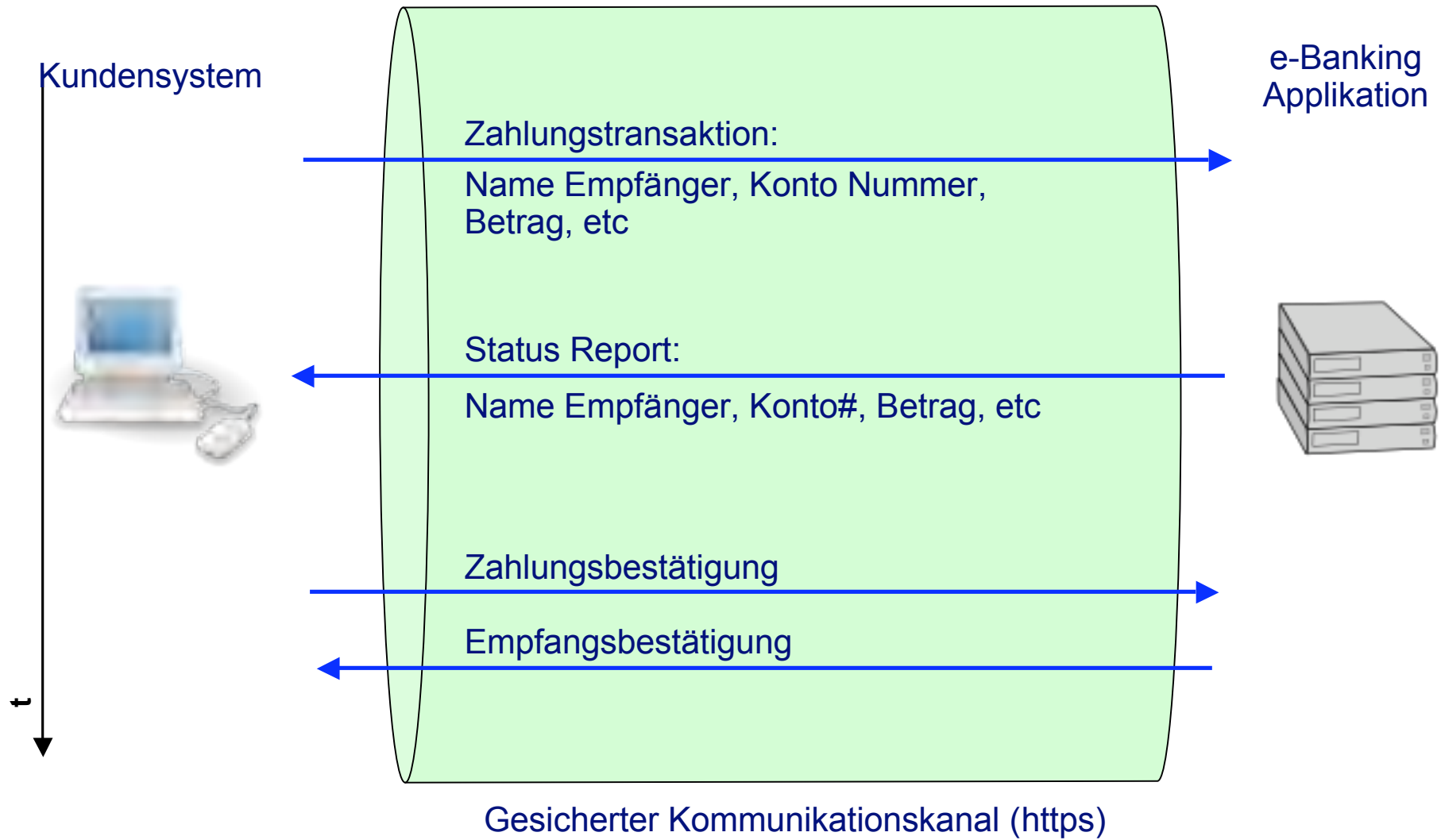
- Einen Blick hinter die Kulissen werfen
- Verständnis vermitteln, wie Angriffe funktionieren
- Bewusstsein von möglichen Gefahren stärken
- Sensibilisierung für den Umgang mit dem Medium Internet
- Umsetzbare Schutzmassnahmen aufzeigen

Übersicht e-Banking

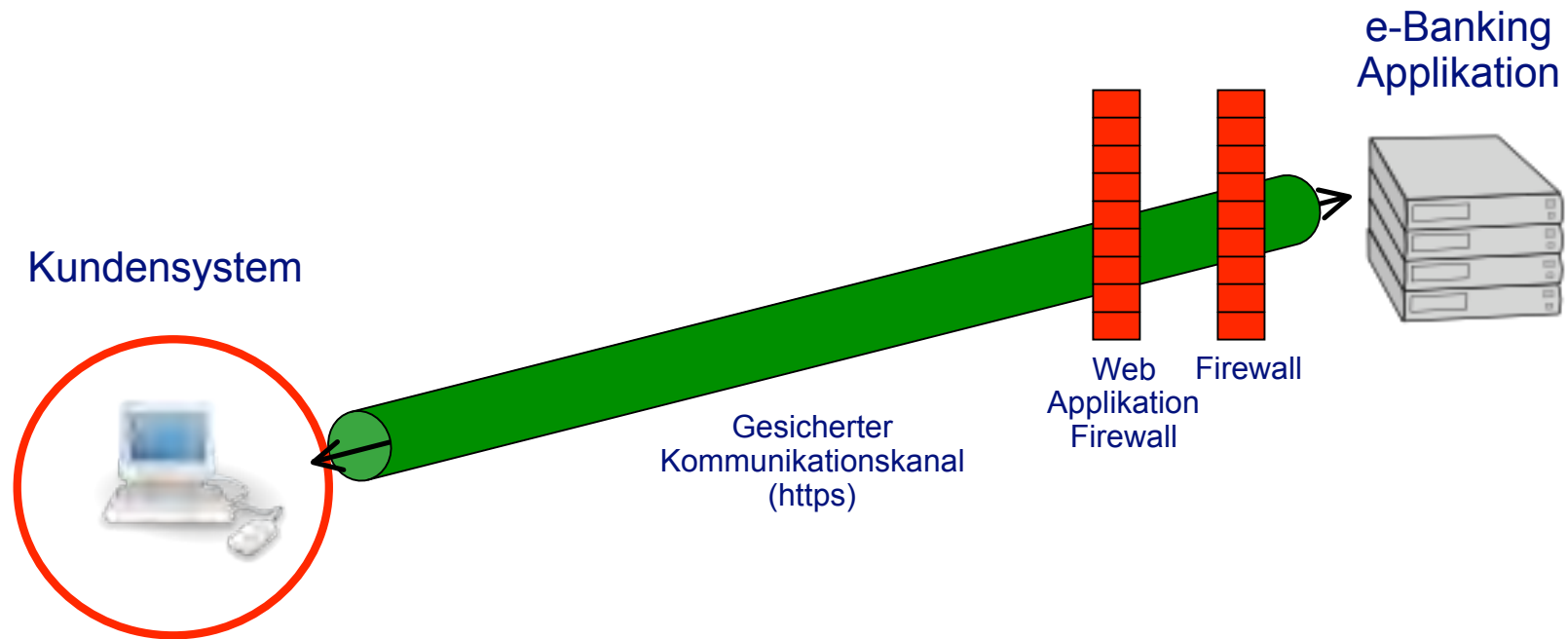
- Grundlage der Überlegungen bilden die heute üblicherweise verwendeten e-Banking Architekturen:
 - Client: Web Browser (Internet Explorer, Firefox)
 - Server: Web Applikation



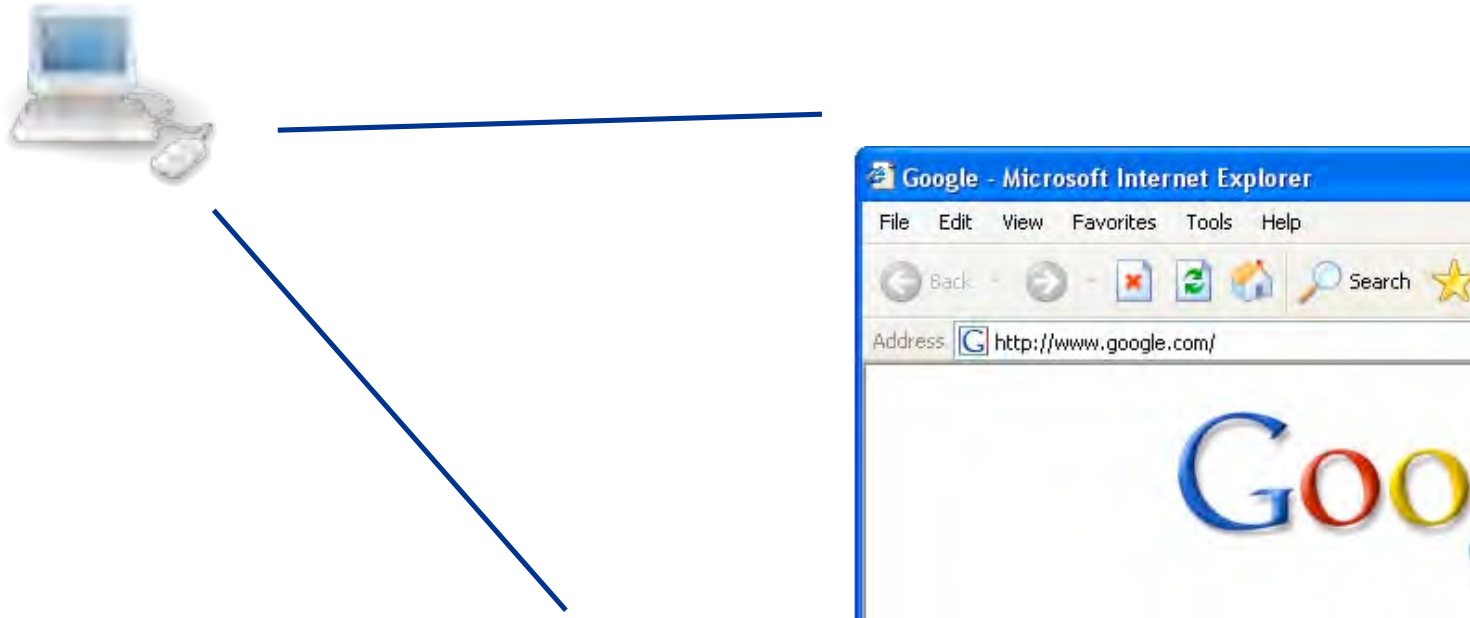
Ablauf e-Banking



Angriffsvarianten



Angriffsvarianten



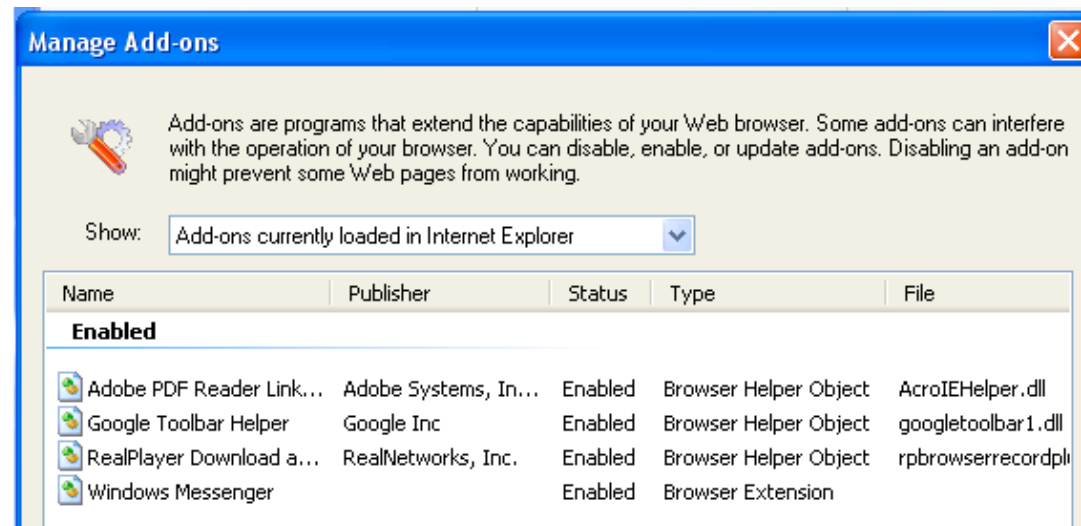
- Kundensystem ist schwächstes Glied in dieser Kette
- Einfachster Angriffspunkt

Angriffsvarianten



Browser Manipulation

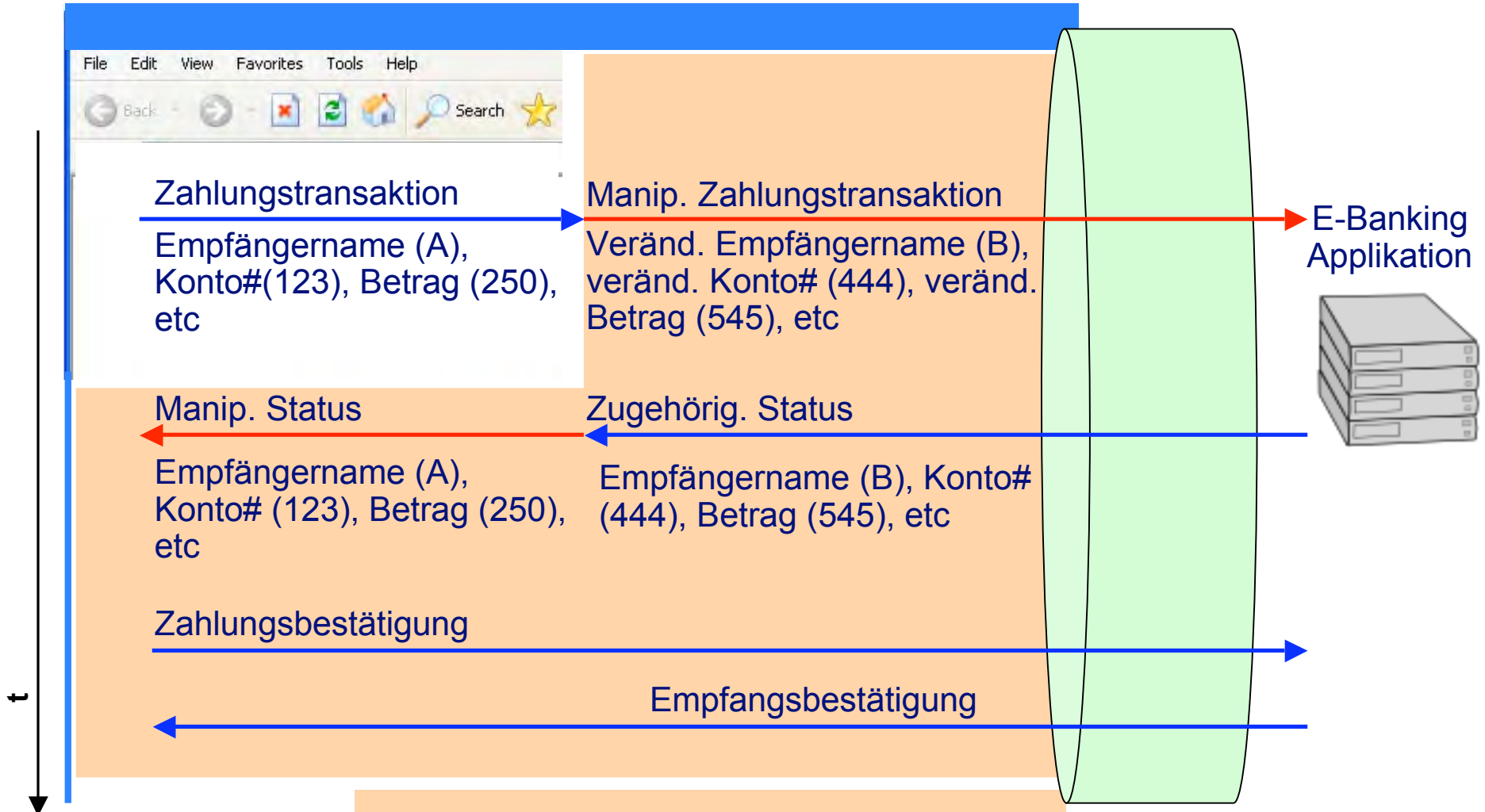
- Heutige Web Browser (Internet Explorer, Firefox, etc) sind sehr modular



Trauen Sie Ihrem Browser ?

Einfluss der Browser Poisoning Attacke

Browser beim Kunden



Demonstration

- Vereinfachte Darstellung einer e-Banking Applikation
- Infektion des Systems
 - „Drive-by Infection“
 - Quicktime Software Schwachstelle
(QuickTime RTSP "Content-Type"-Header Pufferüberlauf)
 - Installation der Malware als Browser Helper Object (IE)
- Was sieht der Kunde, was sieht die Bank

Demonstration

Schutzmassnahmen

- Patchen
- Patchen
- Patchen (v.a auch Applikationen wie Acrobat Reader, Quicktime, etc)
- Aktuelle Antivirenlösung (mit aktuellen Erkennungssignaturen)
- Firewall aktivieren (Sicherheitseinstellungen)
- Sorgfältiger Umgang mit dem Medium Internet
- Patchen

Schutzmassnahmen II

- Landwirtschaft: Monokultur risikoreich
- Keine Administratoren Rechte
- Live CDs

Fragen / Diskussion

Danke für Ihre Aufmerksamkeit
und
„safe Netsurfing“