Kann man im Web 2.0 sicher surfen?

CEO-Version des Vortrags: NEIN!

Jens Hektor

Admin Treffen/ 18.7.2011 / HS IEHK

Stand: 15.7.2011

Version 1.0

Malware Situation heute

- Viren per Email sind sehr selten
- Häufiger: vergiftete Links, Phishing, Spear Phishing
- Infektionsweg Nr. 1: das Web
  Zero Day Exploits via Driveby Donwloads
- Infektionsweg Nr. 2: USB-Sticks
  der Copyshop ist aktuell ein Thema!
- Infektionsweg Nr. 3: Freunde
  „keygen.exe“ ist böse

- Gecrackte Server an der RWTH mittlerweile sehr selten

RWTH-IN 20110721 / DFNCERT 70129

- Einige hundert Papras-Bot Infektionen zwischen Juli 2010 und Februar 2011
- POST-Request mit Authentifizierungscredentials anderer Webseiten Daten leckten nach Moldavien/Ukraine/Litauen/Panama/...
- LMU hat ähnliches beobachtet (nach Hinweis von RWTH)
- Mehr Fälle als vom Blast-o-mat gefunden

- User meldet „komisches“ Verhalten beim Online Banking
- Admin (Herr Stab, DWI) bemerkt Kommunikation nach Moldawien und kontaktet RZ
- IP-Adresse einschlägig bekannt (Google)
- Überwachung der Kommunikation Richtung des Servers zeigt weitere betroffene Systeme
- Analyse der Kommunikation zeigt weitere Datensenken (passive DNS Replikation, URLs)

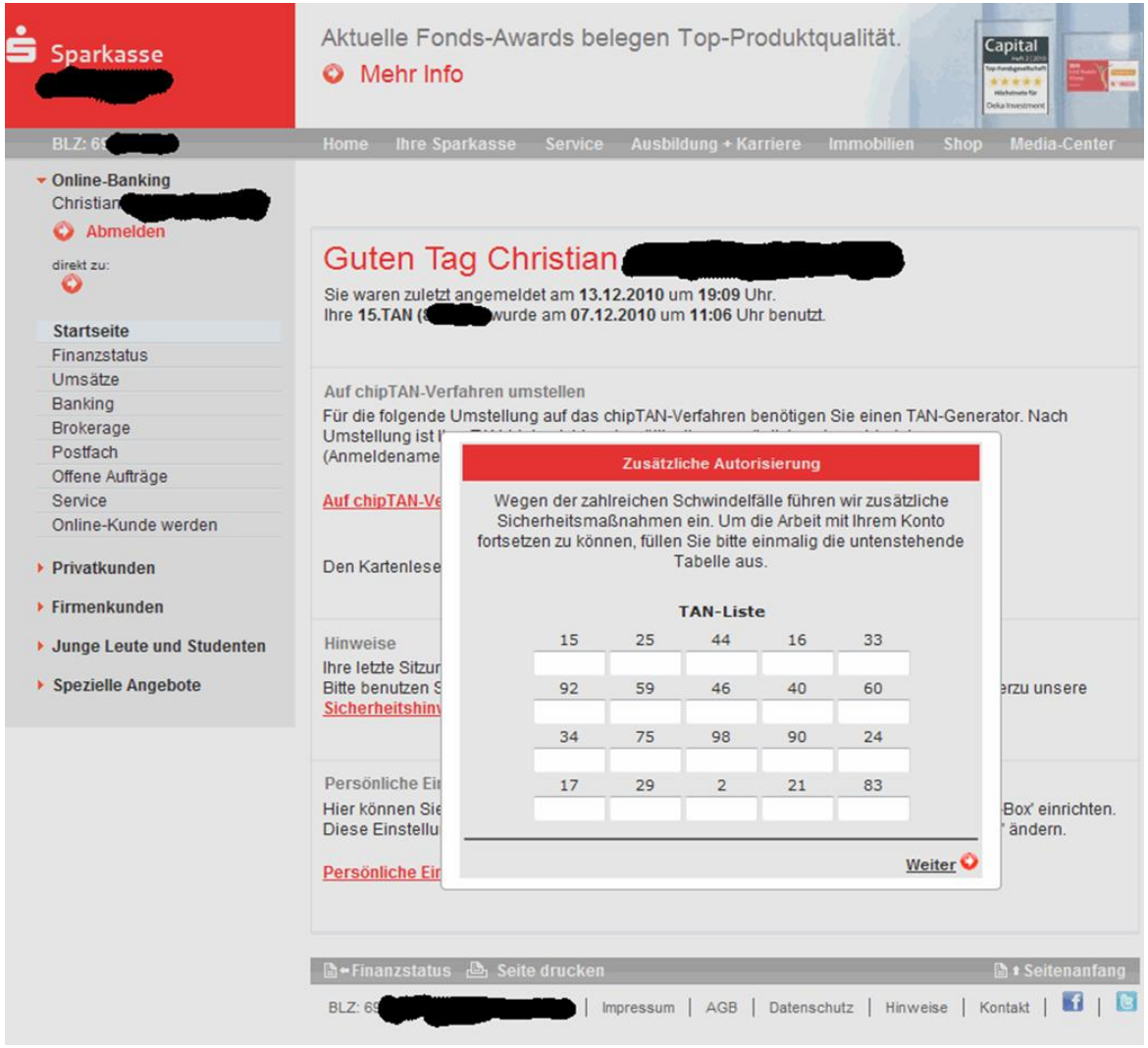
Anatomie einer Infektion

- Google-Suche („elektromobilität“)
- Blog-Seite zum Thema mit „Werbebanner“ durch den Serviceprovider (Bloghoster)
- Werbebanner macht 3 redirects bis zum Java-Exploit
- Trojaner wird installiert als DLL für typische Webbrowser (IE und Firefox verifiziert):
  Registry Eintrag für das Menü „recently opened webpages“

- Fazit:
  ein „tödlicher“ Klick auf eine eigentlich vertrauenswürdige Seite

  andere Seiten, bei denen so etwas passierte:
  stern.de
  rtl.de

Merkt man das?



Problematik: Ökosystem Webbrowser

- **Was sehen wir:**

- **OS meist aktualisiert**
- **Browser oft aktuell**
- **Virenscanner: von nicht vorhanden bis aktuell**
- **und der Rest?**

Was ist mit:

- PDF Viewer
- Flash Player
- Shockwave Player
- Java
- ...

3 Ansatzpunkte zur Absicherung

- **A&O:**
  Aktualität der Software:
  (s. die anderen Vorträge)

- **Security Proxy nutzen**

- **Browser härten**

Cisco Ironport WSA (Web Security Appliance)

- Webproxies mit Security Funktionen
- Virenscanner
- Reputationsbasiertes Sperren von Seiten
  (z.B. bekannte Malwarehoster, akut bekannte Systeme)
- Seit Juni 2010 für EduRoam/VPN und Wohnheime aktiv
- Viel Wirbel („Zensur“), sensitive Logs (Datenschutz)
- Blast-o-mat Ereignisse auf ca. 25% zurückgegangen
- 2 Verpflichtungsszenarien:
  - transparenter Proxy per WCCP
  - browserbasiert per PAC
- 2 Nutzungsmöglichkeiten:
  - anonymisierend (2 Geräte)
  - nicht anonymisierend: X-ForwardedFor im Request (3 Geräte)
- ca. 10 Institute (in Teilen oder flächendeckend) per WCCP dabei
- Ausbau mit Landeslizenz ab 1.1.2012

Härten des Browsers

- Wirklich IE9 im Einsatz?
- Alternativen: Firefox, Chrome, Opera
- FF Addons:

  - NoScript: beste Schutzwirkung, fein granular konfigurierbar
  Grundverständnis der Problematik vonnöten

  - AdBlock Plus: Problematik bösartiger Ad-Server
  einfach einsetzbar

  - weitere:
  Flashblock: speziell gegen Flash-Exploits,
  HTTPS Everywhere: offenes unverschlüsseltes WLAN (Internetcafe)

Danke für die Aufmerksamkeit

- **Fragen?**