

# 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

- ▶ **Viren per Email sind sehr selten**
- ▶ **Häufiger: vergiftete Links, Phishing, Spear Phishing**
- ▶ **Infektionsweg Nr. 1: das Web**  
**Zero Day Exploits via Driveby Downloads**
- ▶ **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**

- ▶ **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)**

- ▶ **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**

**Sparkasse**

Aktuelle Fonds-Awards belegen Top-Produktqualität.  
[Mehr Info](#)

BLZ: 6[redacted] Home Ihre Sparkasse Service Ausbildung + Karriere Immobilien Shop Media-Center

**Online-Banking**  
Christian [redacted]  
[Abmelden](#)

direkt zu:  
[Startseite](#)  
Finanzstatus  
Umsätze  
Banking  
Brokerage  
Postfach  
Offene Aufträge  
Service  
Online-Kunde werden

**Privatkunden**  
**Firmenkunden**  
**Junge Leute und Studenten**  
**Spezielle Angebote**

**Guten Tag Christian** [redacted]  
Sie waren zuletzt angemeldet am 13.12.2010 um 19:09 Uhr.  
Ihre 15.TAN ([redacted]) wurde am 07.12.2010 um 11:06 Uhr benutzt.

Auf chipTAN-Verfahren umstellen  
Für die folgende Umstellung auf das chipTAN-Verfahren benötigen Sie einen TAN-Generator. Nach Umstellung ist [redacted]  
(Anmeldename [redacted])

[Auf chipTAN-Verfahren umstellen](#)

Den Kartenleser einrichten

Hinweise  
Ihre letzte Sitzung wurde am 13.12.2010 um 19:09 Uhr beendet.  
Bitte benutzen Sie einen TAN-Generator.  
[Sicherheitshinweise](#)

Persönliche Einstellungen  
Hier können Sie Ihre persönlichen Einstellungen ändern.  
Diese Einstellungen sind für alle Konten gültig.  
[Persönliche Einstellungen](#)

**Zusätzliche Autorisierung**

Wegen der zahlreichen Schwindelfälle führen wir zusätzliche Sicherheitsmaßnahmen ein. Um die Arbeit mit Ihrem Konto fortsetzen zu können, füllen Sie bitte einmalig die untenstehende Tabelle aus.

| TAN-Liste            |                      |                      |                      |                      |
|----------------------|----------------------|----------------------|----------------------|----------------------|
| 15                   | 25                   | 44                   | 16                   | 33                   |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 92                   | 59                   | 46                   | 40                   | 60                   |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 34                   | 75                   | 98                   | 90                   | 24                   |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 17                   | 29                   | 2                    | 21                   | 83                   |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

[Weiter](#)

Finanzstatus Seite drucken Seitenanfang

BLZ: 6[redacted] Impressum | AGB | Datenschutz | Hinweise | Kontakt | [f](#) | [t](#)

- ▶ **Was sehen wir:**
- ▶ **OS meist aktualisiert**
- ▶ **Browser oft aktuell**
- ▶ **Virens Scanner: 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**

- ▶ **Webproxies mit Security Funktionen**
- ▶ **Virens Scanner**
- ▶ **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**

- ▶ **Wirklich IE9 im Einsatz?**
- ▶ **Alternativen: Firefox, Chrome, Opera**
- ▶ **FF Addons:**
  - **NoScript: beste Schutzwirkung, fein granular konfigurierbar**  
**Grundverständnis der Problematik vonnöten**
  - **AdBlock Plus: Problematik bössartiger Ad-Server**  
**einfach einsetzbar**
  - **weitere:**
    - Flashblock: speziell gegen Flash-Exploits,**
    - HTTPS Everywhere: offenes unverschlüsseltes WLAN (Internetcafe)**

# Danke für die Aufmerksamkeit

▶ Fragen?