DEUTSCHER PRÄVENTIONSTAG

„Media Security – Who is Responsible?“

von

Frank Ackermann

Dokument aus der Internetdokumentation
des Deutschen Präventionstages www.praeventionstag.de
Herausgegeben von Hans-Jürgen Kerner und Erich Marks im Auftrag der
Deutschen Stiftung für Verbrechensverhütung und Straffälligenhilfe (DVS)

Zur Zitation:
Frank Ackermann: Media Security – Who is Responsible?, in: Kerner, Hans-Jürgen u. Marks, Erich (Hrsg.), Internetdokumentation des Deutschen Präventionstages. Hannover 2011, www.praeventionstag.de/Dokumentation.cms/1608

Verband der deutschen Internetwirtschaft e. V.

GERMAN CONGRESS ON CRIME PREVENTION
ANNUAL INTERNATIONAL FORUM

Oldenburg, May 30 - 31, 2011

Media Security - Who is Responsible ?

Frank Ackermann
Director Self-Regulation, eco

Verband der deutschen Internetwirtschaft e. V.

Media Security ?

Zur Anzeige wird der QuickTime™
Dekompressor „“
benötigt.

Examples of Threat Sources

- **Bot-network operators**
- **Criminal groups**
- **Foreign intelligence services**
- **Hackers**
- **Insiders**
- **Phishers**
- **Spammers**
- **Spyware/malware authors**
- **Terrorists**

Examples of Threat Portals

- **Social Media**
- **Game Consoles**
- **Geodata Services**
- **Online Banking**

e. g. Facebook

- **Facebook e-Commerce**
  - IT-security typically not involved in social meia
  - Huge gapping hole
  - e. g. taking over „buy now“ button

- **„Like“-Button**
  - Download from 3rd party site (FB)
  - IP-addresses can be tracked and stored by FB. What happens to them ?
  - Legal ?

- **Cross-site scripting (XSS)**
  - Used to spread viral links

Geotracking

- **Google Location Services (Cell Tower, WiFi); Skyhook (WiFi); SimpleGeo (Geofences); SocialGeo**
- **e. g. Facebook, Smartphones, even Browsers (FF > 3.5 using Google, IE 9 HTML5-based, Opera & Safari using Skyhook)**
- **Joe Stump (founder SocialGeo): „So you basically just say „Track User“ and we handle in our API along with record history. I can then come back and say „Show me the last 10 places the user was“.**
- **Who is responsible ? Or rather, what can be done ?**
- **Market worth § 5 billion in 2013 only on mobile phones**

Game Consoles

Sony case

- **Did not have firewalls fully enabled**
- **Cybercriminals used Amazon Cloud services**
  - No verification other then a live credit card and email address
- **Sony did not have a CSO or CISO (!)**
- **May 18 a PlayStation exploit was reported**
  - Sony responded it was not hacked and that there was a URL exploit that enabled access to a user's password with the use of a birth date and email address.
  - http://blog.us.playstation.com/2011/05/18/update-on-psn-password-reset-process/

Geodata

- **e. g. Google Street View, SightWalk, telefonbuch.de, etc.**

- **Protection of personal data through Data Protection Codex**
  - Proposed by industry as self-regulatory instrument
  - Regulates online image services
  - Protected are individuals, their children, cars, place of residence
  - Possibility for individual to object - online or offline, w/o reasoning
  - Objection via button next to picture
  - One-stop-shop for information and objection-handling
  - Website with search function and information on scheduled recordings
  - External complaints handle for procedural complaints

- **Not considered sufficient to protect personal data by Ministerial Conference of Justice**

Online Banking

- **Manifold threat scenarios**
- **European banks not as careless as e. g. US banks**
  - chipTAN, iTAN, etc.
  - EV SSL
- **Most banks don‘t make a fuzz if user not grossly negligent**
- **User awareness raising alone doesn‘t help, but securing local system is key**

Law Enforcement and Internet Industry Collaboration

- **Hotlines**
  - INHOPE

- **Anti-Botnet-Activities**
  - Anti Botnet Advisory Centre
  - Whitehat Projects (e.g. VeriSign‘s Cyber Abuse Initiative Whitehat Program to provide a standard, auditible process and partnerships to expedite the handling of abuses of domain names or DNS infrastructure)

- **Anti-Spam activities**
  - Whitelisting services (e. g. Certified Senders Alliance)

Verband der deutschen Internetwirtschaft e. V.

Law Enforcement and Internet Industry Collaboration

- **24/7 SPOCs for police**
- **Client-level filtering**
  - Global Alliance Matrix
  - Interstate Contract for Youth Protection in the Media
- **Identifying and supporting Critical Infrastructures**
- **Technical training for law enforcement**

Platforms

Interest groups for industry and law enforcement

- **MAAWG**
- **LAP**
- **APWG**

Annual Conferences

- **Octopus Conference**
- **LE/Industry Collaboration Conference**
- **International Cybercrime Conference KCSC (biannual)**
- **Cybercrime Conferences of the EU Presidency**

Verband der deutschen Internetwirtschaft e. V.

Awareness Raising

- **EU-SIP Safer Internet Centres**
  - National Awareness Centres (e. g. Klicksafe - hall 3, stand 3108)
  - Organised inside INSAFE-Network
  - Annual Safer Internet Day (2nd Tuesday in February)
- **Online Trust Alliance (OTA)**
- **Awareness Raising Initiatives**
  - www.media-awareness.ca Media Literacy Week Nov. 2011
  - ACMA www.cybersmart.gov.au
  - Deutschland sicher im Netz (hall 3, stand 3008)
  - White IT (hall 3, stand 3041)
- **Awareness raising for teachers as multipliers**
  - Schulen surfen - aber sicher !

So who is responsible ?

So who is responsible ?

We all are !

Verband der deutschen Internetwirtschaft e. V.

Frank Ackermann
Director Self-Regulation

eco – Association of the German Internet Industry
Lichtstr. 43h
50825 Cologne
Germany
+49 (0)221 7000 48 - 0
frank.ackermann@eco.de
www.eco.de