

# Does my (social) network need a firewall? (öffentliche Version)

Hacking Night 2010.5

25. November 2010, Hagenberg  
Florian Brunner & Emanuel Mathis

# Does my (social) network need a firewall? Yes!

Hacking Night 2010.5

25. November 2010, Hagenberg  
Florian Brunner & Emanuel Mathis

**Hacking Group:**  
Yes, you need one!

# Wer wir sind?

## Florian Brunner

- Student Sib08
- Software Engineer
- CTF-Team h4ck!nb3rg
- monkey-cert.at
- (No) Ethical Hacker

## Emanuel Mathis

- Student Sim08
- Security Researcher
- Ethical Hacker

# Agenda

- Motivation
- Überblick über die Sozialen Plattformen
- Aktuelle und zukünftige Geschäftsmodelle
- Why privacy matters?
- Angriffsszenarien auf Soziale Plattformen
- Verteidigungsstrategien
- Fazit

„Ich denke, also bin ich.“,

René Descartes

„Ich denke, also bin ich.“,

René Descartes

„Ich nutze (Facebook), also bin ich.“,

flo

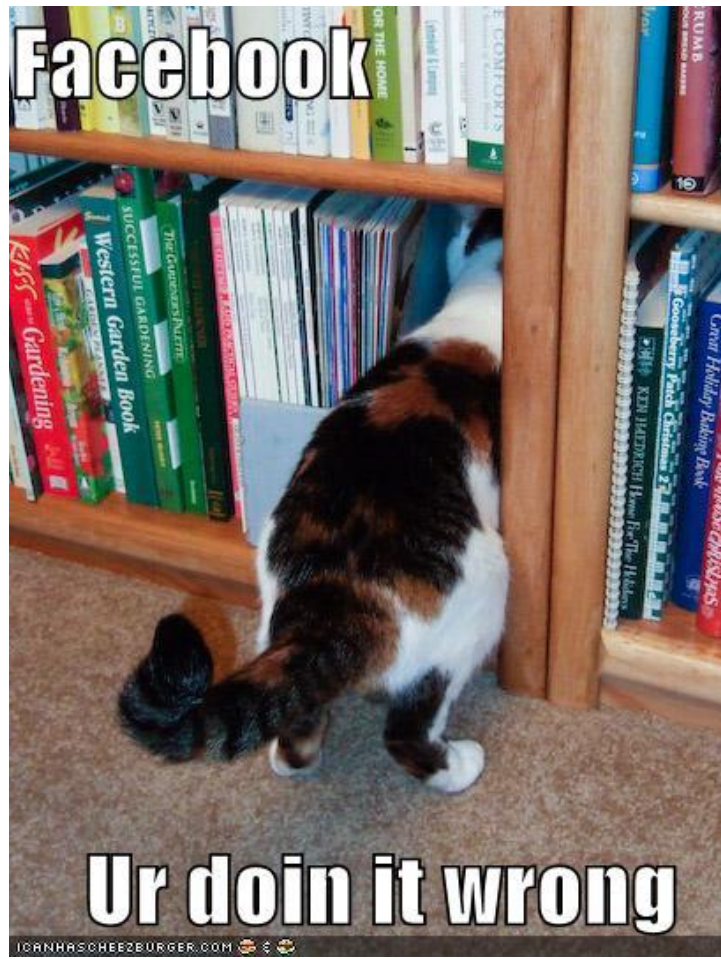


# Überblick über soziale Plattformen

Soziale Plattformen werden über das Internet angewendet und führen zur plötzlichen Äußerung von Gedanken, Wortmeldungen oder dem Erscheinen von privaten Fotos oder Videos. Als Nebenwirkungen treten öfters Freundschaftsanforderungen, dubiose Bekanntschaften oder sinnlose Nachrichtenüberflutungen auf. Zu Risiken und Nebenwirkungen lesen Sie die Packungsbeilage und fragen Sie Ihren Arzt oder Apotheker.



# Facebook?!



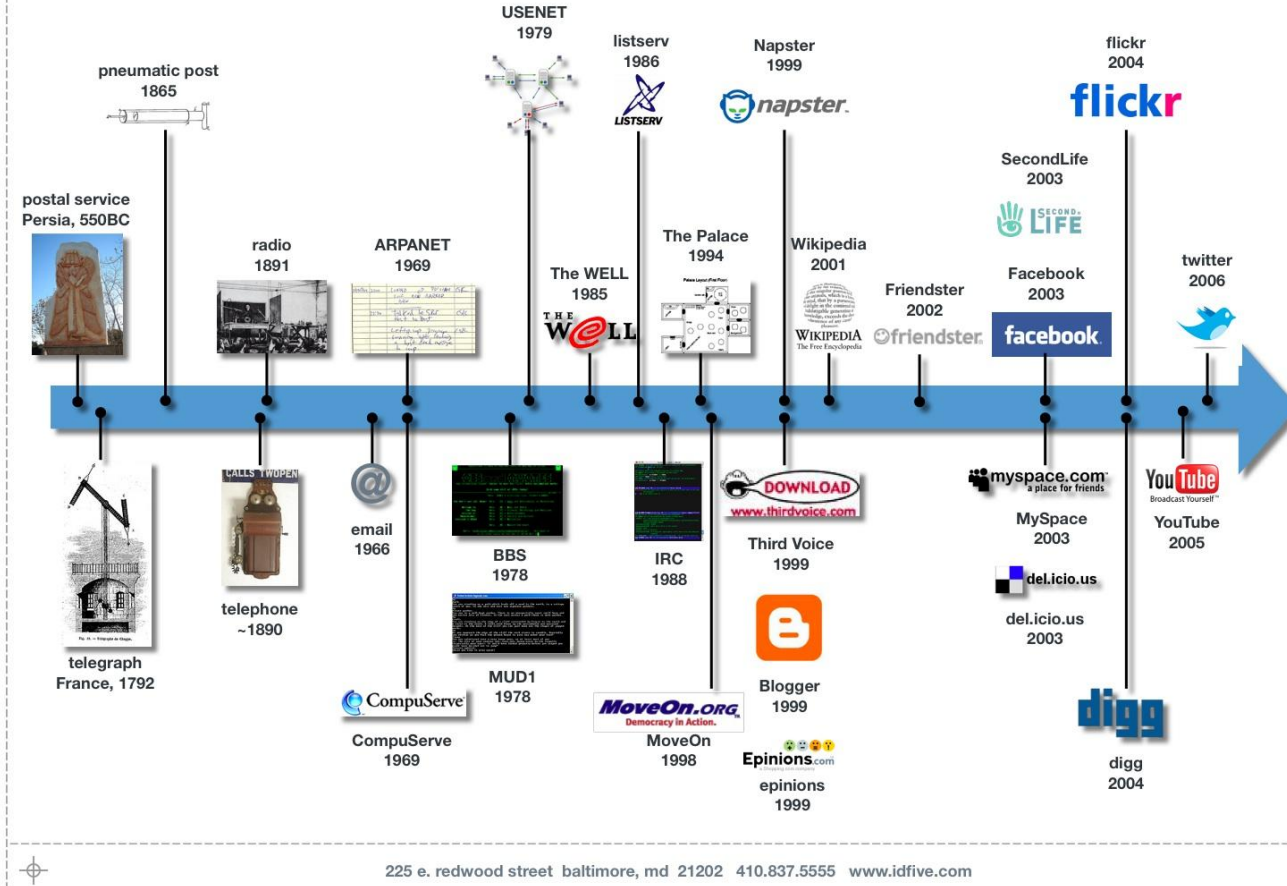
# Timeline

15

## A (somewhat incomplete) Timeline of Social Media

not to scale

idfive



225 e. redwood street baltimore, md 21202 410.837.5555 www.idfive.com

# Geschäftsmodelle



# Why privacy matters?

# Google is evil?!



## Article 12.

“**No one** shall be subjected to **arbitrary interference** with his **privacy**, family, home or **correspondence**, nor to attacks upon his honour and reputation. **Everyone** has the **right** to the **protection** of the **law** against such **interference** or **attacks**. „

## Bedeutet

- seclusion: the desire to be left alone
- property: the desire to be paid for one's data
- autonomy: the ability to act freely

## Internet: Kontrolle

**PRIVACY** encompasses the  
rights  
and obligations of individuals  
and  
organizations with respect to  
the...

- **Collection**
- **Use**
- **Disclosure, and**
- **Retention**

...of personal  
information.

# Welche Information gibst du preis?

- Wenn Dich jemand auf der Straße fragt?

# Welche Information gibst du preis?

- Wenn Dich jemand auf der Straße fragt?
- Wenn Du einkaufen gehst und jemand Deine PlZ wissen will?

# Welche Information gibst du preis?

- Wenn Dich jemand auf der Straße fragt?
- Wenn Du einkaufen gehst und jemand Deine PLZ wissen will?
- Wenn Du ein Foto auf Facebook reinstellst?

# Welche Information gibst du preis?

- Wenn Dich jemand auf der Straße fragt?
- Wenn Du einkaufen gehst und jemand Deine PLZ wissen will?
- Wenn Du ein Foto auf Facebook reinstellst?
- Wenn Du neue Freunde kennen lernen willst?

# Do you get it? – They didn't!



die dummen die gehn zur **arbeit** , die schlaunen  
pennen aus

4 hours ago



hockt da in der **Arbeit** top-unmotiviert, sigiert ihre  
Arbeitskollegin und futtert Eiskonfekt xDD

6 hours ago

# You get it? – They didn't!



♀ [\[blurred\]](#) fuck bin ich **besoffen** ^^ achja ich hab ne neue handynummer und ne neue hausnummer alle die die haben wollen einfach melden ^^

13 days ago

# Angriffsszenarien

- Datenschutzbezogene Bedrohungen
- Traditionelle Bedrohungen der IKT-Sicherheit
- Identitätsbezogene Bedrohungen
- Soziale Bedrohungen

# Datenschutzbezogene Bedrohungen

- Aggregation persönlicher Daten

# Datenschutzbezogene Bedrohungen

- Aggregation persönlicher Daten
- Sekundäre Datenerfassung

# Datenschutzbezogene Bedrohungen

- Aggregation persönlicher Daten
- Sekundäre Datenerfassung
- Angriffe durch Gesichtserkennung

# Datenschutzbezogene Bedrohungen

- Aggregation persönlicher Daten
- Sekundäre Datenerfassung
- Angriffe durch Gesichtserkennung
- CBIR – Content Based Image Retrieval

# Datenschutzbezogene Bedrohungen

- Aggregation persönlicher Daten
- Sekundäre Datenerfassung
- Angriffe durch Gesichtserkennung
- CBIR – Content Based Image Retrieval
- Verknüpfung von Meta-Daten

# Datenschutzbezogene Bedrohungen

- Aggregation persönlicher Daten
- Sekundäre Datenerfassung
- Angriffe durch Gesichtserkennung
- CBIR – Content Based Image Retrieval
- Verknüpfung von Meta-Daten
- Schwierigkeiten bei Kontolöschung

- Social Networking Spam

# Old School Attacks

- Social Networking Spam
- Cross Site Scripting, Vieren & Würmer

# Was ist XSS?

The screenshot shows a web browser displaying the DNSstuff.com website. At the top, there is a login form with fields for 'Username' and a password field (represented by dots), and buttons for 'Login' and 'Forgot login?'. Below the login form is a navigation menu with links for 'Home', 'Tools', 'Products', 'Forum', 'Company', 'Account', and 'Support'. The 'Tools' link is highlighted. On the left side of the page, there is a cartoon monkey pointing to the right. In the center, an alert box is displayed with the title 'The page at http://www.dnsstuff.com says' and the content '1'. Below the alert box, there is a line of code: `...n_aa6a08f34cd80cc9320f633c54515182.gif onload=alert(1); /<a=">Email Results Email Results`. Below the code, there is a link 'Return to tools'. At the bottom left, there is a 'DNSreport Demo' section with a text input field containing 'google.com' and a 'Go' button. At the bottom right, there is a 'New! Mail Server Test Center' advertisement. At the bottom left of the page, there is a 'WHOIS - 75.125.82.251' link.

# Old School Attacks

- Social Networking Spam
- Cross Site Scripting, Vieren & Würmer
- SNS Aggregatoren

Sämtliche Grafiken wurden entfernt.

# Identitätsbezogene Bedrohungen

- Spear Phishing

# Identitätsbezogene Bedrohungen

- Spear Phishing
- Infiltration des (sozialen) Netzwerkes

# Identitätsbezogene Bedrohungen

- Spear Phishing
- Infiltration des (sozialen) Netzwerkes
- Profile-squatting und Rufschädigung

# Soziale Bedrohungen

- Stalking

# Soziale Bedrohungen

- Stalking
- Cybermobbing & -grooming

# Soziale Bedrohungen

- Stalking
- Cybermobbing & -grooming
- Industrie- und Wirtschaftsspionage

# Social Engineering?!

Grafik wurde entfernt.

# Verteidigungsstrategien

- Search yourself!

# Verteidigungsstrategien

- Search yourself!
- Google Alerts

# Verteidigungsstrategien

- Search yourself!
- Google Alerts
- Z'erst denken, dann twittern!

# Verteidigungsstrategien

- Search yourself!
- Google Alerts
- Z'erst denken, dann twittern!
- Behandelt Privatsphäre wie ein Geschenk!

# Verteidigungsstrategien

- Search yourself!
- Google Alerts
- Z'erst denken, dann twittern!
- Behandelt Privatsphäre wie ein Geschenk!
- Sechster Sinn für Privacy!

# Fazit

- Jeder ist involviert.

- Jeder ist involviert.
- Du bist involviert....

- Jeder ist involviert.
- Du bist involviert, auch wenn Du nicht willst!

- Jeder ist involviert.
- Du bist involviert, auch wenn Du nicht willst!
- Daten werden verknüpft werden!



# Fazit – cause we can...



- Jeder ist involviert.
- Du bist involviert, auch wenn Du nicht willst!
- Daten werden verknüpft werden!