Privacy by Design
am Beispiel Facebook

Florian Stahl
Senior Consultant
Information Security
msg systems ag
florian.stahl@msg-systems.com
+49-89-96101-1134

OWASP
07.11.2012

Über mich

Florian Stahl

Diplom-Wirtschaftsinformatik (Universität Regensburg)

Master of Computer Science (Växjö Universitet, Schweden)

CISSP, CCSK, Mitglied der IAPP

Seit 6 Jahren im Bereich Informationssicherheit tätig, u.A.:

- Security & Privacy Consultant bei Ernst & Young
- Senior Consultant Information Security, msg systems ag
- Externer Datenschutzbeauftragter

Ziel: Interdisziplinäres und ganzheitliches Verständnis für IT-Sicherheit und Datenschutz in Unternehmen

Hobbies:

- Frau und Hund
- Reisen
- Mountainbiken, Tennis und Snowboarden

msg systems

Agenda

1. Vorschlag der EU-Richtlinie zum Datenschutz
2. Begriffsklärung Privacy by Design (PbD)
3. Privacy by Redesign
4. Beispiel Facebook
5. Fazit
6. Chancen & Herausforderungen

Vorschlag EU Datenschutz-Richtlinie

Fakten

- Im Januar 2012 wurde ein Vorschlag zur Überarbeitung der EU-Datenschutzrichtlinie veröffentlicht, Absegnung frühestens 2014
- Einheitliches Regelwerk für die komplette EU
- Gilt auch für nicht-europäische Unternehmen, die Daten von EU-Bürgern verarbeiten (z.B. Facebook, Google, etc.)

Inhalte

- Verantwortlichkeiten und Haftung (neu: Datenschutzbeauftragter in EU)
- Informationspflicht bei Vorfällen (24h)
- Eine zuständige Aufsichtsbehörde innerhalb Europas
- Zustimmung der Einzelpersonen (Opt-in)
- Kontrolle der Umsetzung durch Behörden
- Datenlöschung („Right to be forgotten“)
- Strafen (bis 2% des weltweiten Jahresumsatzes)
- Privacy by Design

Begriffsklärung Privacy by Design

Privacy by Design – 7 Prinzipien von Ann Cavoukian*

1. Proactive, not reactive
2. Privacy as the **Default** Setting
3. Privacy **Embedded into Design**
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

Proposal for the new EU regulation

Section 2 “Data Protection“,

Article 30 “Security of Processing“:

The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for ***privacy by design*** *and* ***data protection by default****, unless paragraph 4 applies.*

Teilweise schon im aktuellen Bundesdatenschutzgesetz verankert

* Quelle: www.privacybydesign.ca

Privacy by Redesign

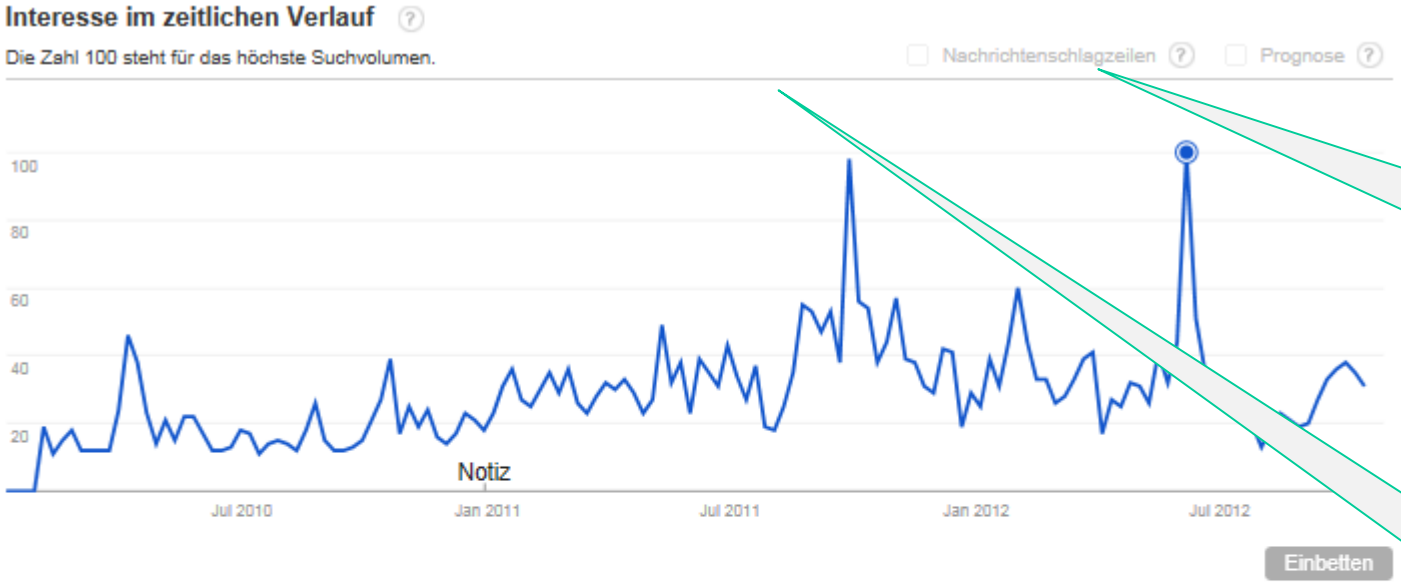
Existierende Systeme müssen umstrukturiert werden

- Viele Systeme / Produkte wurden ohne Rücksicht auf Datenschutz entwickelt
- Nachträgliche Implementierung durch Privacy by Redesign zunächst wohl wichtiger als PbD, aber wie setzt man das um?

Prozess nach Ann Cavoukian und Ernst & Young

- **Rethink** existing mitigation strategies, systems and processes with a view to finding new privacy-focused approaches.
- **Redesign** system functionality to achieve better standards of privacy protection, without losing sight of business objectives.
- **Revive** systems through an IT transformation that incorporates privacy protection as a fundamental tenet

Google Trends „Datenschutz Facebook“



Abstimmung neue Facebook Datenschutz-regeln

Herausgabe persönliche Nutzerdaten Max Schrems (Student, Wien)

Regionales Interesse

Schleswig-Holstein	100
Hamburg	91
Baden-Württemberg	89
Nordrhein-Westfalen	80
Bayern	79

Verwandte Begriffe — Beliebteste | Zunehmende

facebook button datenschutz	100
datenschutz und facebook	95
facebook daten	90
facebook button	90
datenschutz bei facebook	80

Quelle: Google Trends (20.10.2012)

Privacy by Design für Facebook (1/4)

Transparenz Datenverarbeitung

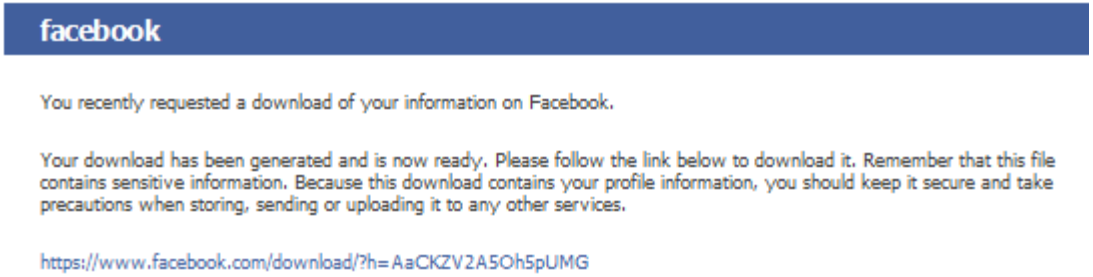
- Zitat John Perry Barlow auf der IAPP Privacy Academy San Jose: *„If I make my data visible it should be visible to me what is done with that data.“*
- Benutzer kann von Facebook ein Download seiner gespeicherten Daten anfordern (Profil, Wall, Fotos, Videos, Freunde, Nachrichten)

Privacy by Redesign

Im Download fehlen z.B.:

- Location Data
- „Likes“ & Like-Button (Surfverhalten)
- Durchgeführte Analysen
- Login-Daten (wann, wo, etc.)
- Daten von Nichtmitgliedern?

Transparenz sollte um diese Daten und vor allem um die Verarbeitung der Daten ergänzt werden (z.B. Chatüberwachung)



Quelle Screenshot: Facebook

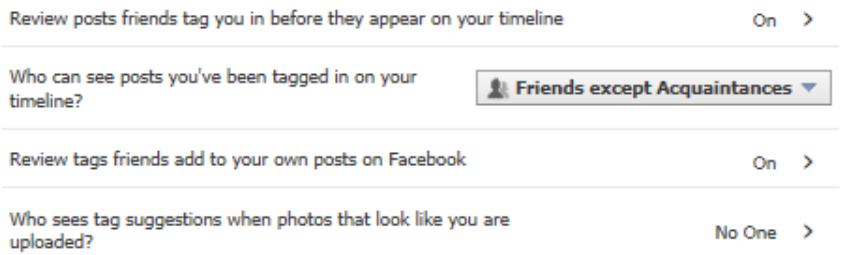
Privacy by Design für Facebook (2/4)

Sharing von Fotos

- Face Recognition und Tagging ist standardmäßig aktiviert
- Leute laden Bilder von einem hoch, die nicht alle sehen sollten
- Aber: Nicht nur Tagging ist datenschutzrechtlich problematisch, sondern auch das simple Hochladen von Bildern kann die Privatsphäre verletzen
- Privacy als Default-Einstellung, Transparenz und Benutzerzentrierung werden nicht umgesetzt

Privacy by Redesign

Review von „Tags“ standardmäßig aktivieren, Vorschläge deaktivieren:



Gesichter bis zur Freigabe verschleiern:

Quelle Screenshot: Facebook

Privacy by Design für Facebook (3/4)

Technischer Datenschutz

Einige gute Sicherheitsmaßnahmen vorhanden:

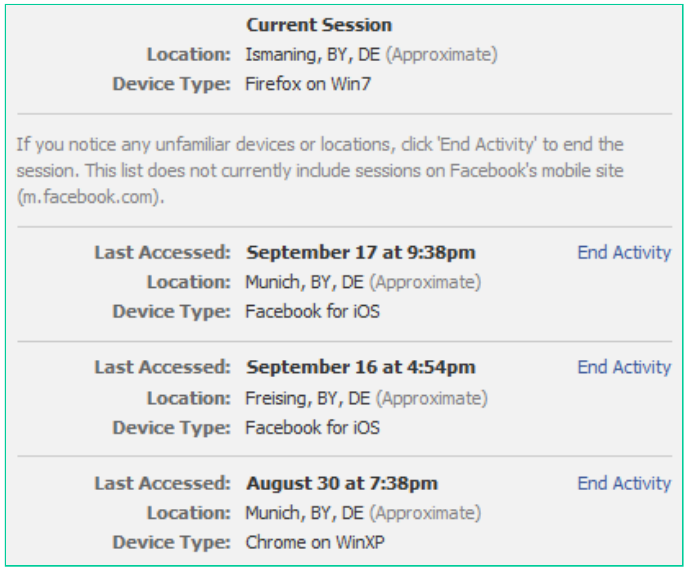
- https-Verbindung möglich, wenn auch nicht als Standard
- Rückfrage bei Login aus einem fremden Land (Freunde erkennen)

```
Dear Florian,

Your Facebook account was recently logged into from a compute

Did you log into Facebook from a new device or an unusual loc

 - If this was not you, please log into Facebook from your co

 - If this was you, there's no need to worry. Simply log into
```

- Aber: Benutzerfreundlichkeit und Möglichkeit zur Datenanalyse meist wichtiger als Sicherheit

Privacy by Redesign

- https als Standard einrichten
- 2-Faktoren-Authentifizierung per OTP ermöglichen (wie z.B. Google)
- Automatisches Session-Timeout erzwingen (inkl. mobile Site)



Quelle Screenshot: Facebook

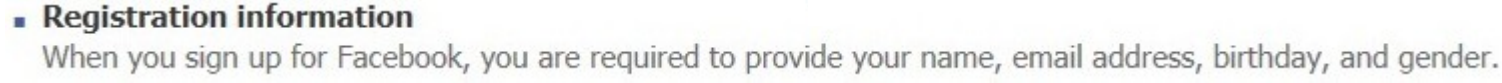
Privacy by Design für Facebook (4/4)

Respect for User Privacy?

- Benutzer müssen die Vorgaben von Facebook akzeptieren und können selbst kaum mitbestimmen
- Facebook verweigert Pseudonyme
- Löschung von Daten nicht wirklich möglich
- Opt-out meistens als Standard
- Datenschutz wird in der Entwicklung zunächst nicht berücksichtigt (z.B. Facebook App API bei Applikationen Dritter, Beacon Advertisement System,

Privacy by Redesign

- Benutzer von Beginn an fragen, welche Einstellungen zum Schutz ihrer Privatsphäre sie haben sollen (z.B. durch Umfrage ohne Mindestwahlbeteiligung von 30%)
- Opt-in an Stelle von Opt-out
- Ermöglichung pseudonymer Nutzung
- Echte Datenlöschung ermöglichen (Speicherdauer festlegen)
- Unabhängige Experten sollten schon bei der Entwicklung eingebunden werden (Privacy Impact Assessment für bzw. durch die Aufsichtsbehörde)



Quelle Screenshot: Facebook

Fazit für Facebook

Todesurteil für Facebook?

- Der User ist für Facebook das Produkt, das Geschäftsmodell basiert auf der Nutzung der personenbezogenen Daten seiner Benutzer
- Eine strenge Auslegung von Privacy by Design würde viele Funktionen von Facebook zur Frage stellen bzw. „non-compliant“ machen
- Die Plattform könnte so für Benutzer uninteressant werden

Oder eine neue Chance?

- **Transparenz** zu schaffen
- In wichtigen Bereichen Privacy als Default-Einstellung zu implementieren
- Auf die (Datenschutz-) Bedürfnisse der Benutzer eingehen

Ändern des Geschäftsmodells?

- **Will der Benutzer** zumindest teilweise die **Offenlegung seiner Daten**, wenn er Mitglied bei Facebook wird?
- Oder ist vielleicht eine **werbefreie Bezahl-Version** von Facebook eine (europäische) Alternative zur werbefinanzierten, kostenlosen Version?

Chancen & Herausforderungen PbD

Chancen

- **Datenschutz** wird **von Beginn an** im Produkt- und Systemdesign verankert
- Vorbeugende Maßnahmen senken das Risiko und **verringern die Anzahl an Datenschutzvorfällen**
- Verbesserung des Datenschutzniveaus durch Verpflichtung zu PbD und höhere Strafen durch die geplante Neuerung der EU-Datenschutzverordnung

Herausforderungen

- Konsequente Umsetzung von Privacy by Design (wer trägt die Kosten?)
- Unterschiedliche **Interpretationsmöglichkeiten**
- Datenschutz-Grundlagen in vielen Bereichen erforderlich (Produkt- und Softwareentwicklung, Projektmanager, etc.)
- **Fehlende Wissensträger** verursachen Engpässe
- **Kontrolle der Umsetzung durch Behörden**
- Reorganisation des Datenschutzes in der EU

Privacy by Design
am Beispiel Facebook

Florian Stahl
Senior Consultant
Information Security
msg systems ag
florian.stahl@msg-systems.com
+49-89-96101-1134

OWASP
07.11.2012

The OWASP Foundation
http://www.owasp.org