OWASP
Open Web Application
Security Project

Top 10 Privacy Risks Project

Results presentation @ German OWASP Day 2014

9 December 2014, Hamburg

Florian Stahl (Project Lead, msg systems, Munich)

Sponsored by .msg

Privacy

- Definitions:
  - A state in which one is not observed or disturbed by other people
  - The right to be let alone (Edward Warren, 1890)
- Different approaches (Europe vs. US)
- IT Security enables Privacy in most cases

Picture source: thedailydose.com

Problem

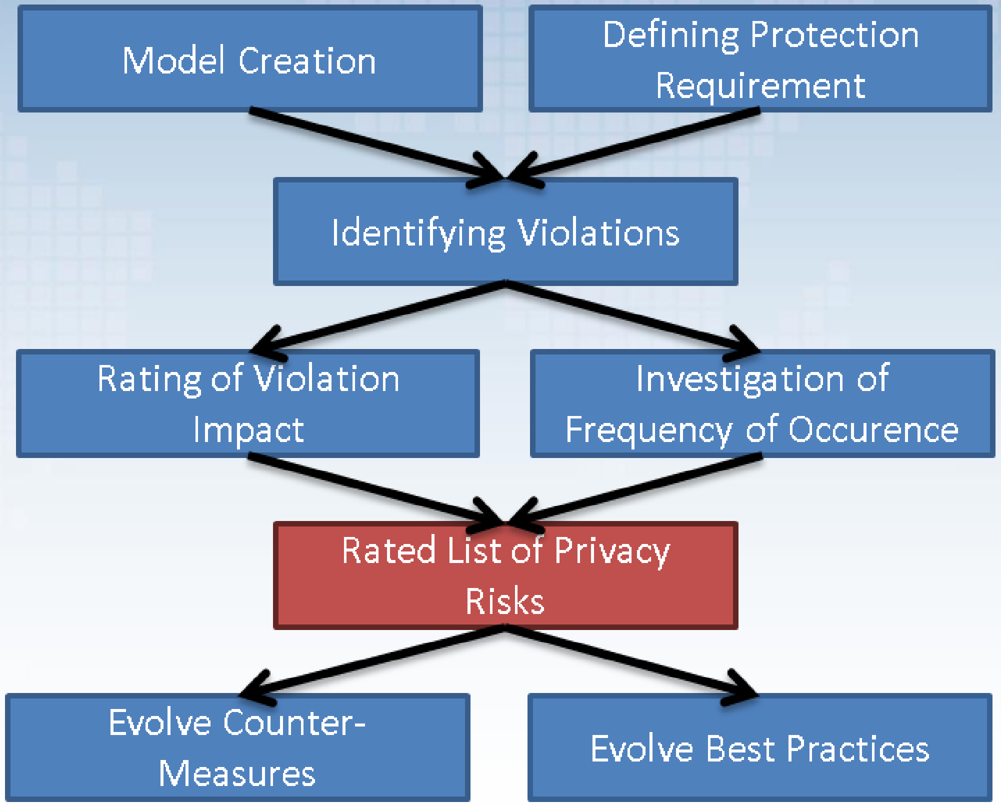
- Many web applications contain privacy risks
- Anyway, they are compliant to privacy and data protection laws because
  - They are hosted in countries with poor privacy laws
  - Lawyers focus on compliance, not on real-life risks for personal data
- No existing guidelines or statistical data about privacy risks
- Foundation of the OWASP Top 10 Privacy Risks Project in early 2014
- Member of Internet Privacy Engineering Network (IPEN)
- Nearly 100 privacy and security experts participated

OWASP
Open Web Application Security Project

Goal

- Identify the most important technical and organizational privacy risks for web applications
- Independent from local laws based on OECD Privacy Principles
- Focus on real-life risks for
  - User (data subject)
  - Provider (data owner)
- Help developers, business architects and others to understand and improve web application privacy
- Provide transparency about privacy risks

Method (1/2)



Model Creation

Defining Protection Requirement

Identifying Violations

Rating of Violation Impact

Investigation of Frequency of Occurence

Rated List of Privacy Risks

Evolve Counter-Measures

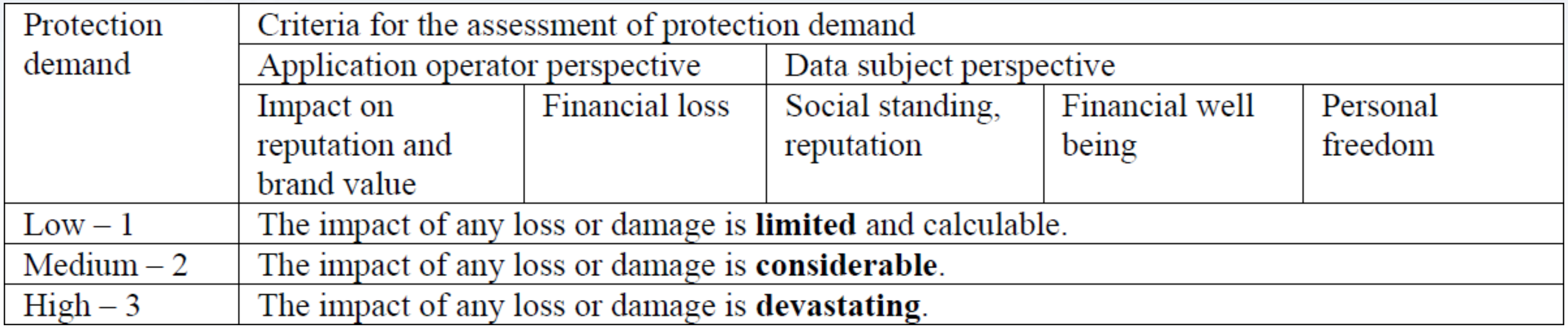
Evolve Best Practices

Method (2/2)

Survey to evaluate frequency of occurence

- 62 privacy and security experts participated
- Rated 20 privacy violations for their frequency in web sites

Impact rating



Protection demand	Criteria for the assessment of protection demand				
	Application operator perspective		Data subject perspective		
	Impact on reputation and brand value	Financial loss	Social standing, reputation	Financial well being	Personal freedom
Low – 1	The impact of any loss or damage is **limited** and calculable.				
Medium – 2	The impact of any loss or damage is **considerable**.				
High – 3	The impact of any loss or damage is **devastating**.				

Result: Top 10 Privacy Risks

P1 Web Application Vulnerabilities

P2 Operator-sided Data Leakage

P3 Insufficient Data Breach Response

P4 Insufficient Deletion of personal data

P5 Non-transparent Policies, Terms and Conditions

P6 Collection of data not required for the primary purpose

P7 Sharing of data with third party

P8 Outdated personal data

P9 Missing or Insufficient Session Expiration

P10 Insecure Data Transfer

P5: Non-transparent Policies, Terms & Conditions

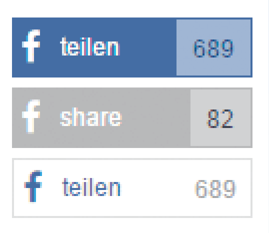
- Privacy Policies, Terms & Conditions are not up-to-date, inaccurate, incomplete or hard to find
- Data processing is not explained sufficiently
- Conditions are too long and users do not read them
- Hard to standardize
- Possible Solutions:
  - Text analyzer: readability-score.com
  - HTTPA: http with accountability

☑ "I have read and agree to the terms and conditions"
Is the **Biggest Lie** on the web.
I confessed
BiggestLie.com

P7: Sharing of Data with 3rd Party

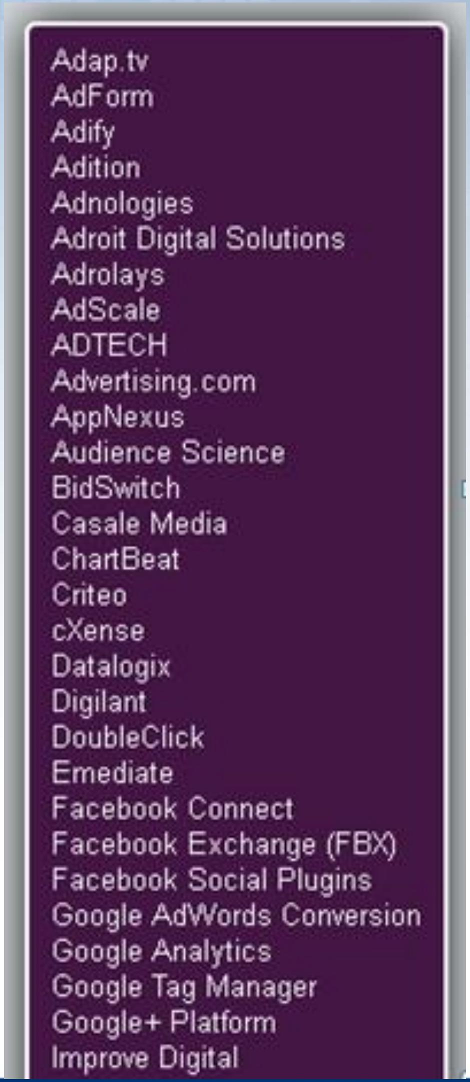
Third Parties:

- Advertisers
- Subcontractors
- Video integration
- Maps
- Social networks



Problems:

- Data is transferred or sold to third parties without user's knowledge and consent
- Complete loss of control



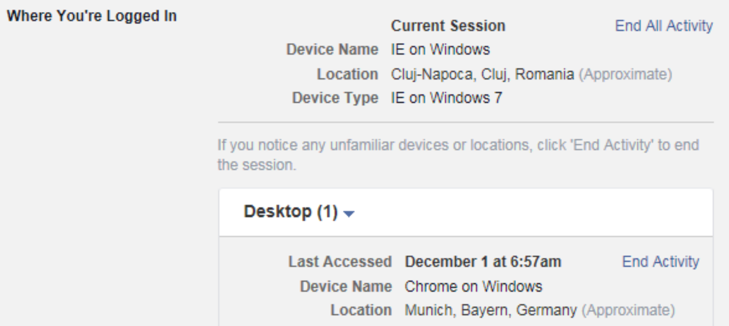
Adap.tv
AdForm
Adify
Adition
Adnologies
Adroit Digital Solutions
Adrolays
AdScale
ADTECH
Advertising.com
AppNexus
Audience Science
BidSwitch
Casale Media
ChartBeat
Criteo
cXense
Datalogix
Digilant
DoubleClick
Emediate
Facebook Connect
Facebook Exchange (FBX)
Facebook Social Plugins
Google AdWords Conversion
Google Analytics
Google Tag Manager
Google+ Platform
Improve Digital

Picture sources: Ghostery, heise.de

P9: Missing or Insufficient Session Expiration

Automatic session timeout and a highly visible logout button is security state-of-the-art, not for:

- Google
- Facebook
- Amazon



Where You're Logged In

Current Session — End All Activity

Device Name: IE on Windows

Location: Cluj-Napoca, Cluj, Romania (Approximate)

Device Type: IE on Windows 7

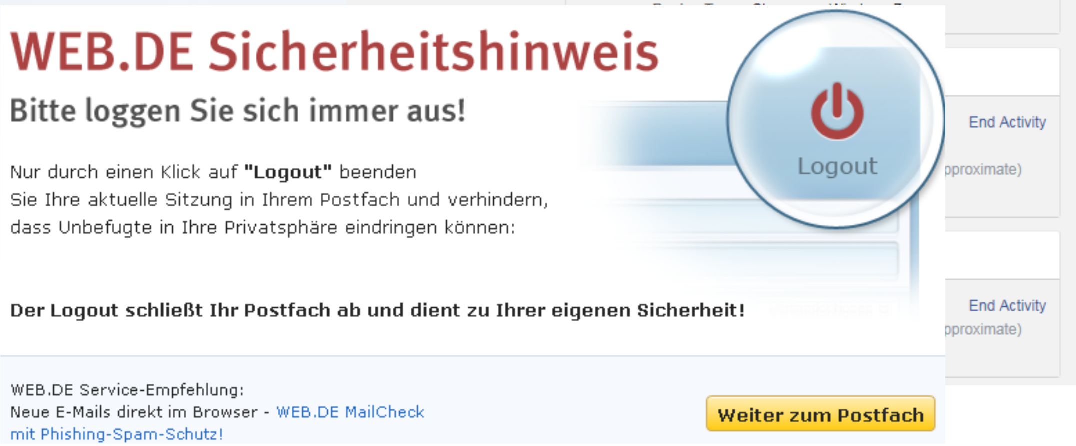
If you notice any unfamiliar devices or locations, click 'End Activity' to end the session.

Desktop (1)

Last Accessed: December 1 at 6:57am — End Activity

Device Name: Chrome on Windows

Location: Munich, Bayern, Germany (Approximate)



WEB.DE Sicherheitshinweis

Bitte loggen Sie sich immer aus!

Nur durch einen Klick auf **"Logout"** beenden Sie Ihre aktuelle Sitzung in Ihrem Postfach und verhindern, dass Unbefugte in Ihre Privatsphäre eindringen können:

Der Logout schließt Ihr Postfach ab und dient zu Ihrer eigenen Sicherheit!

WEB.DE Service-Empfehlung:
Neue E-Mails direkt im Browser - WEB.DE MailCheck mit Phishing-Spam-Schutz!

Solution:

- Configure to automatically logout after X hours / days
- Obvious logout button
- Educate users

Picture sources: facebook.com, web.de

Outlook

- Aiming to receive Lab Project Status
- Currently collection of countermeasures
- Master student wanted (preferred location Munich)
- Spread the Word
  - 22 January 2015: CPDP, Brussels (IPEN panel discussion)
  - 4-6 March 2015: IAPP Global Privacy Summit, Washington
- Regular review of Top 10 Privacy list

OWASP
Open Web Application
Security Project

OWASP
Open Web Application Security Project

Top 10 Privacy Risks Project

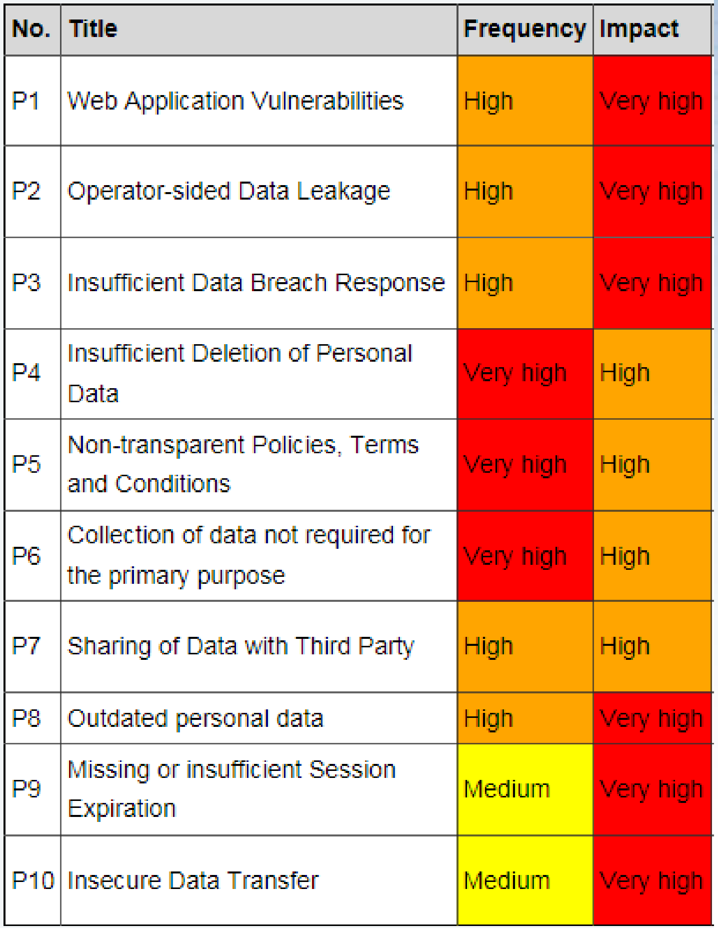
Results presentation @ German OWASP Day 2014

9 December 2014, Hamburg

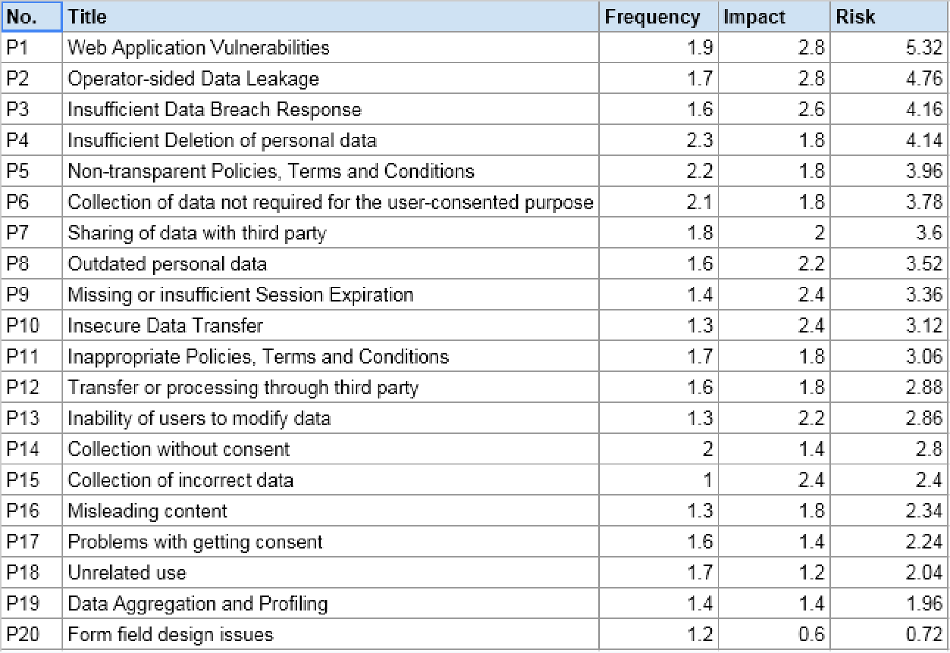
Florian Stahl (Project Lead, msg systems, Munich)

Sponsored by msg

Backup



No.	Title	Frequency	Impact
P1	Web Application Vulnerabilities	High	Very high
P2	Operator-sided Data Leakage	High	Very high
P3	Insufficient Data Breach Response	High	Very high
P4	Insufficient Deletion of Personal Data	Very high	High
P5	Non-transparent Policies, Terms and Conditions	Very high	High
P6	Collection of data not required for the primary purpose	Very high	High
P7	Sharing of Data with Third Party	High	High
P8	Outdated personal data	High	Very high
P9	Missing or insufficient Session Expiration	Medium	Very high
P10	Insecure Data Transfer	Medium	Very high



No.	Title	Frequency	Impact	Risk
P1	Web Application Vulnerabilities	1.9	2.8	5.32
P2	Operator-sided Data Leakage	1.7	2.8	4.76
P3	Insufficient Data Breach Response	1.6	2.6	4.16
P4	Insufficient Deletion of personal data	2.3	1.8	4.14
P5	Non-transparent Policies, Terms and Conditions	2.2	1.8	3.96
P6	Collection of data not required for the user-consented purpose	2.1	1.8	3.78
P7	Sharing of data with third party	1.8	2	3.6
P8	Outdated personal data	1.6	2.2	3.52
P9	Missing or insufficient Session Expiration	1.4	2.4	3.36
P10	Insecure Data Transfer	1.3	2.4	3.12
P11	Inappropriate Policies, Terms and Conditions	1.7	1.8	3.06
P12	Transfer or processing through third party	1.6	1.8	2.88
P13	Inability of users to modify data	1.3	2.2	2.86
P14	Collection without consent	2	1.4	2.8
P15	Collection of incorrect data	1	2.4	2.4
P16	Misleading content	1.3	1.8	2.34
P17	Problems with getting consent	1.6	1.4	2.24
P18	Unrelated use	1.7	1.2	2.04
P19	Data Aggregation and Profiling	1.4	1.4	1.96
P20	Form field design issues	1.2	0.6	0.72

OWASP
Open Web Application Security Project