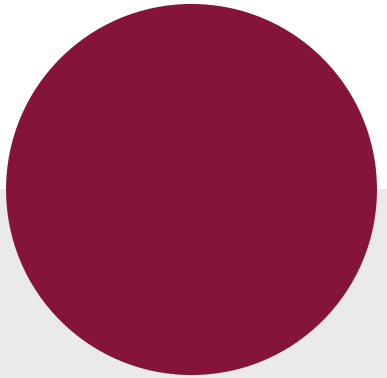
.msg .consulting .solutions .partnership



OWASP Top 10 Privacy Risks Project

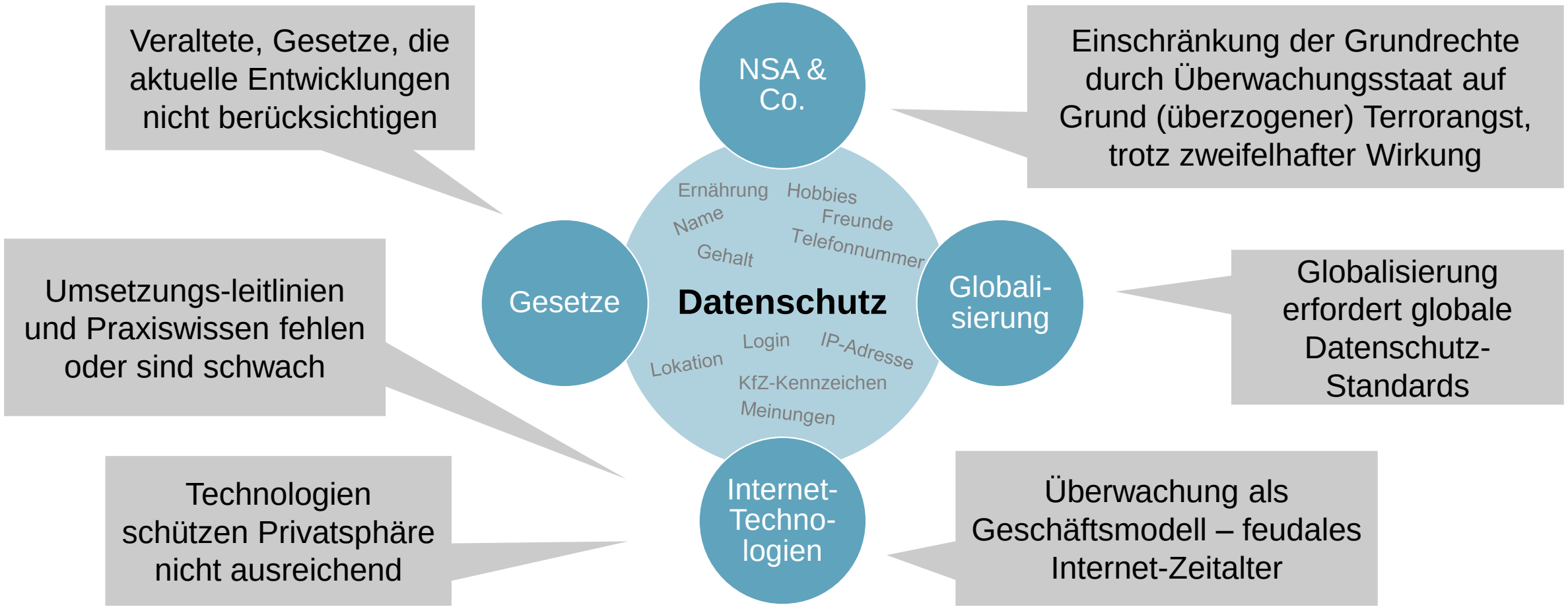
Florian Stahl

Über mich

Florian Stahl

- Lead Consultant im Bereich Information Security der msg
- Dipl.-Winf., MSc, CISSP, CIPT
- Leiter und Gründer des OWASP Top 10 Privacy Risks Project
- Blog: securitybydesign.de
- Hobbies: Frau, Sohn, Mountainbiken, Snowboarden
- florian.stahl@msg-systems.com

Status quo


Veraltete, Gesetze, die aktuelle Entwicklungen nicht berücksichtigen
NSA & Co.
Einschränkung der Grundrechte durch Überwachungsstaat auf Grund (überzogener) Terrorangst, trotz zweifelhafter Wirkung
Umsetzungs-leitlinien und Praxiswissen fehlen oder sind schwach
Gesetze
Ernährung
Hobbies
Name
Freunde
Telefonnummer
Gehalt
Datenschutz
Globali-sierung
Globalisierung erfordert globale Datenschutz-Standards
Login
IP-Adresse
Lokation
KfZ-Kennzeichen
Meinungen
Technologien schützen Privatsphäre nicht ausreichend
Internet-Techno-logien
Überwachung als Geschäftsmodell – feudales Internet-Zeitalter

Projektziele

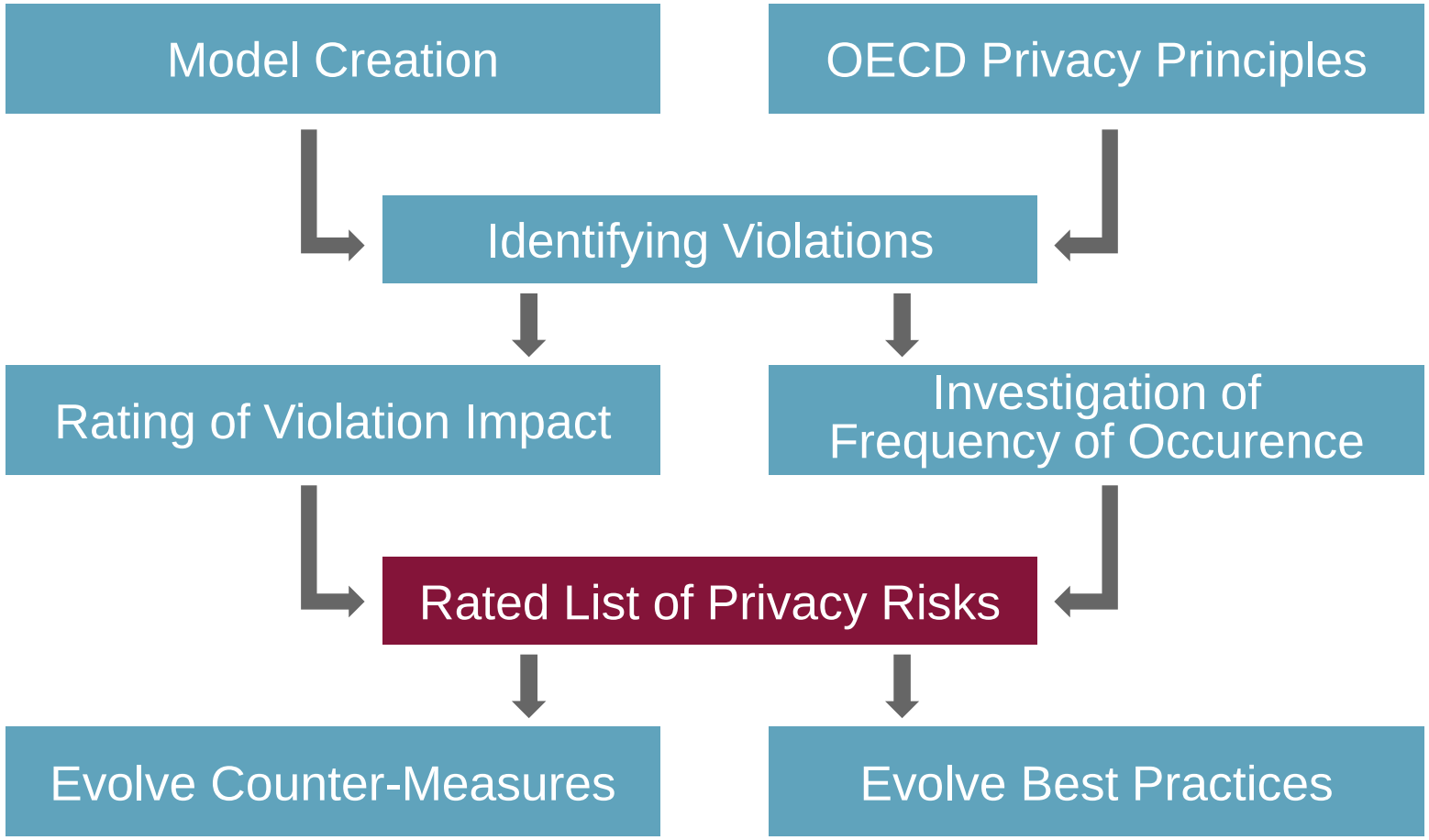
Leitlinien für **echten Datenschutz in Web-Applikationen**

- Aktuell haben viele Web-Applikationen Datenschutz-Risiken weil
  - Sie in Ländern mit schwachem Datenschutz gehostet sind
  - Sie den Fokus auf Compliance (auf dem Papier) legen
  - Die Betreiber mit Daten Geld verdienen wollen
  - Entwicklern, Architekten und Produkt-Designern Datenschutz-Wissen fehlt
- Fehlen existierender Leitlinien hat zur Projekt-Gründung geführt
  - Gründung im Februar 2014 in Zusammenarbeit mit der Hochschule München
  - Open Web Application Security Project (OWASP) als renommierte Non-profit Open Source Plattform
  - Mitglied im Internet Privacy Engineering Network (IPEN) der EU-Datenschutz-Aufsicht

Zehn wichtigste **technische und organisatorische** Datenschutz-Risiken identifizieren

- Datenschutz-Risiken in Web-Applikationen transparent machen und Gegenmaßnahmen aufzeigen
- Unabhängig von Gesetzen, basierend auf den OECD Privacy Principles
- Nicht im Scope: Selbst-Schutz für Benutzer

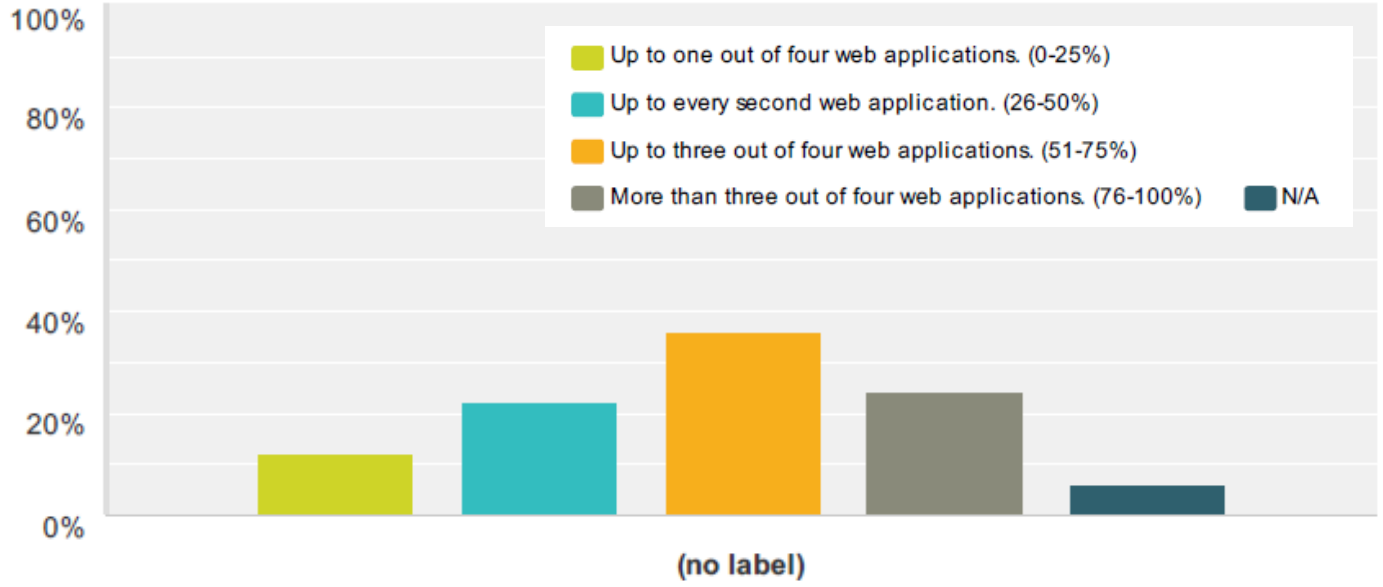
Methodik (1/2): Wissenschaftlicher Ansatz



1. Begrenzte Datenerhebung
2. Datenqualität
3. Zweckbestimmung
4. Nutzungsbegrenzung
5. Sicherheit
6. Transparenz
7. Mitspracherecht
8. Rechenschaftspflicht

Methodik (2/2): Umfrage zur Bestimmung der Häufigkeit

- Fehlen statistischer Daten machte Umfrage notwendig
- Teilnahme von 63 Datenschutz- und Sicherheits-Experten
- Bewertung wie häufig identifizierte 20 Datenschutz-Verstöße in Webseiten vorkommen
- Beispiel: Weitergabe von Daten an Dritte (Durchschnitt: 1,8)



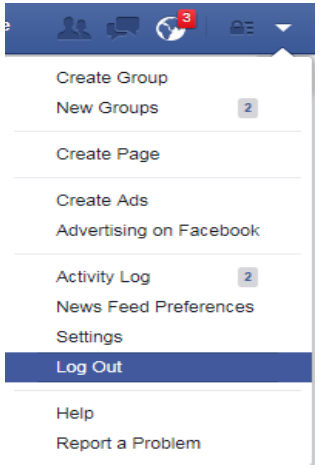
Ergebnis: Top 10 Datenschutz-Risiken

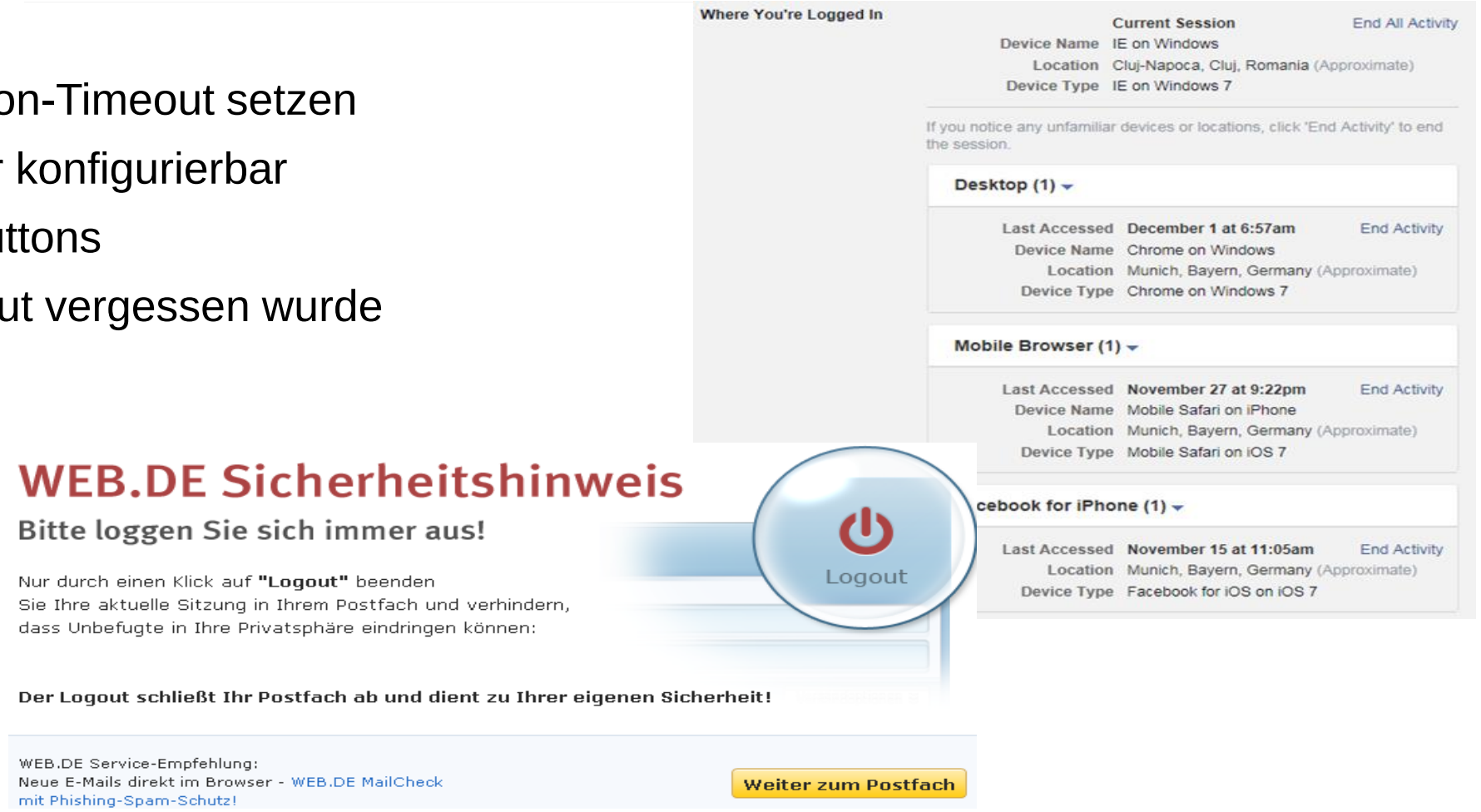
- **P1** Schwachstellen in Web-Applikationen
- **P2** Datenabfluss beim Betreiber
- **P3** Unzureichende Reaktion bei einer Datenpanne
- **P4** Unzureichende Löschung personenbezogener Daten
- **P5** Intransparente Nutzungsbedingungen
- **P6** Sammeln von Daten, die über den eigentlichen Zweck hinaus gehen
- **P7** Weitergabe von Daten an Dritte
- **P8** Veraltete personenbezogene Daten
- **P9** Fehlendes oder unzureichendes Session-Ende
- **P10** Unsichere Datenübertragung

P9: Fehlendes oder unzureichendes Session-Ende

Gegenmaßnahmen:

- Angemessenes Session-Timeout setzen
- Flexibel vom Benutzer konfigurierbar
- Prominente Logout Buttons
- Erinnerung, falls Logout vergessen wurde

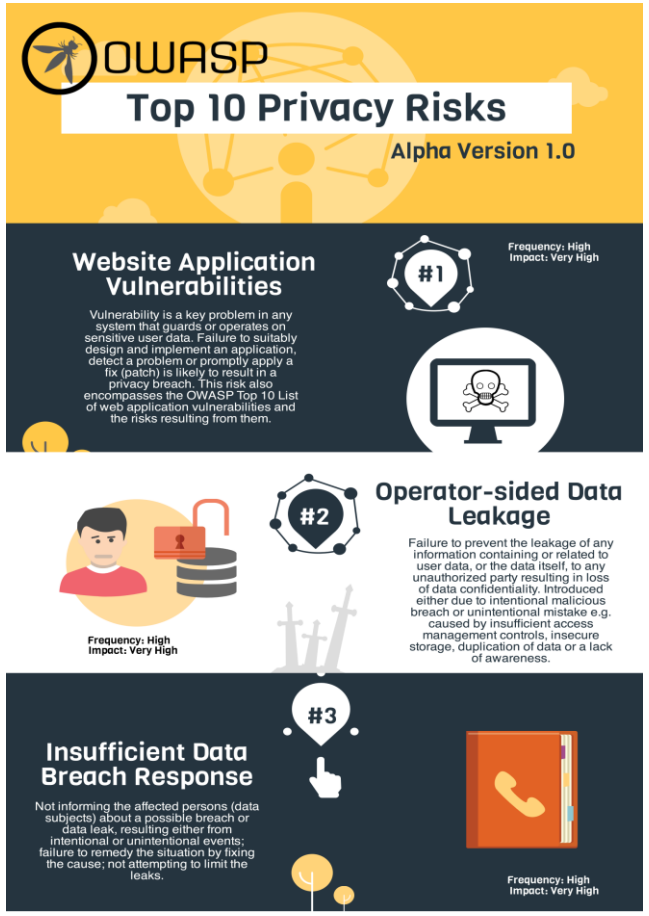




* Bildquellen: facebook.com, web.de

Zusammenfassung & weiterführende Informationen

- Datenschutz ist in vielen Web-Applikationen verbesserungswürdig
- Das OWASP Top 10 Privacy Risks Projekt wurde gegründet, um diese Defizite anzugehen und Entwickler, Architekten, aber auch Juristen weiterzubilden
- Das Projekt identifiziert technische und organisatorische Risiken unabhängig von der lokalen Gesetzgebung
- Projekt-Webseite: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
- Artikel in iX 04/2015: Bollwerk
- Aktuell werden Gegenmaßnahmen detailliert – jeder kann mitmachen (auch Master Thesis möglich)
- Projektflyer und weitere Infos am Stand der msg 12.0-323



P5: Intransparente Nutzungsbedingungen (Backup)

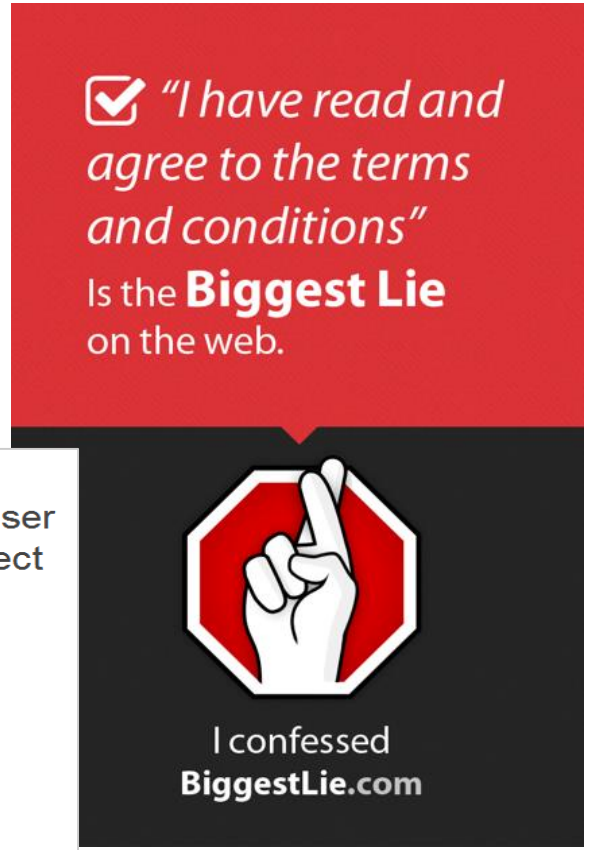
- Nutzungs- oder Datenschutzbestimmungen sind nicht aktuell, für Laien unangemessen komplex, unvollständig oder schwer zu finden
- Verarbeitung personenbezogener Daten ist nicht ausreichend beschrieben
- Nutzungsbedingungen sind zu lang und Benutzer lesen sie nicht, besser ist eine Kurzversion:

Information You Provide to Us:

We receive and store any information you enter on our website or provide to us in any other way. You can choose not to provide us with certain information, but then you may not be able to take advantage of many of our special features.
Registration: In order for you to use 500px services you must complete a registration form. As part of this registration form, we require select personal information.
User Profile: To allow you to express yourself beyond just the information collected during registration, we enable you to provide additional information, such as a bio, favorite URLs, and instant messaging IDs. In addition, you may choose to include photos of yourself in your profile. As indicated below, in the section titled "Sharing Your Information", you can control how your information is displayed and used.
Automatic Information:
We receive and store certain types of information whenever you interact with us. 500px and its authorized agents automatically receive and record certain "traffic data" on their server logs from your browser including your IP address, 500px cookie information, and the page you requested. 500px uses this traffic data to help diagnose problems with its servers, analyze trends and administer the website.
500px may collect and, on any page, display the total counts that page has been viewed. This includes User Profile pages.
Many companies offer programs that help you to visit websites anonymously. While 500px will not be able to provide you with a personalized experience if we cannot recognize you, we want you to be aware that these programs are available.

Basically,

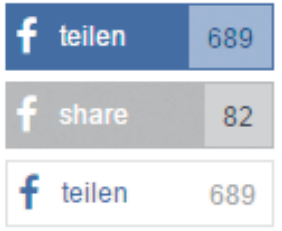
We collect your registration and user profile data. Our servers also collect log information used to make the website faster and better.



P7: Weitergabe von Daten an Dritte (Backup)

Gegenmaßnahmen

- Services Dritter sollten nur benutzt werden, wenn sie wirklich nötig sind
- Entwickeln einer Monitoring-Strategie für Services Dritter
  - Gateway mit Whitelist oder Blacklist (vertrauenswürdige Dritte)
  - Vertragsvereinbarungen mit Richtlinien zur Datennutzung, etc. (ADV in DE)
  - Transparenz gegenüber den Nutzern
- Anonymisieren / Masking von Daten vor der Übertragung
  - `anonymizeIp()` für Google Analytics
- Datenübermittlung nur bei Nutzeranfrage (Klick)
  - `Enhanced Privacy Mode` für Einbettung von Youtube-Videos
  - `Heise Shariff` für Social Media Buttons



Florian Stahl
msg Information Security

+49 171 8625807
florian.stahl@msg-systems.com

msg systems ag (Firmenzentrale)
Robert-Bürkle-Str. 1, 85737
Ismaning/München

www.msg-systems.com

.consulting .solutions .partnership