



Sicherheit von Webanwendungen als Maßnahme zum Schutz personen- bezogenener Daten

*Ein Entwurf für
TOP10 des Datenschutzes*

OWASP
20.10.2010

Dr. Ingo Hanke
OWASP-Mitglied
IDEAS

Information & Design Applications
owasp@ideas.de
Tell +49 (0)551 370 00 30

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

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

Einleitung

- Wozu denn TOP 10 des Datenschutzes?
 - ▶ KMU-Umfeld: heterogene Landschaft von Webapplikationen, kein Sicherheits-Konzept
 - ▶ Wenig Bewusstsein bzgl. der Sicherheit von Web-Anwendungen
 - ▶ Erstellung sicherer Webanwendungen wird als selbstverständlich betrachtet, auch dann, wenn keine Risikoanalyse vorliegt!

Einleitung

■ Wozu denn TOP 10 des Datenschutzes?

- ▶ Aber: die Unternehmen sind sich der branchenspezifischen Gefahrenlage sehr wohl bewusst!

ALSO

- ▶ Einsatz von branchen- oder anwendungs-spezifischen "TOP 10 Security Templates".
Beispiel:
 - ▶ Die TOP 10 des Datenschutzes

Einleitung

- Ziel und Besonderheiten für Datenschutz-TOP10
 - ▶ Zielgruppe: Unternehmen, die (online) Personendaten verarbeiten oder speichern
 - ▶ Zu beachten: Datenschutz gehört zur Rubrik "Compliance", nicht "Technik"

Einleitung

■ Sicherheits-Argumente für Projektplanungen

- ▶ Relevante Aspekte des BDSG, z.B. die bußgeldbewehrte Offenlegungspflicht von Datenschutzvorfällen
- ▶ Datenschutz als Teil der Marketing-Strategie
- ▶ Beispiele bekannt gewordener Datenschutz-Vorfälle und deren **öffentliche** Diskussion → TOP 10

Entwurf der Datenschutz TOP10

■ Grundlagen

- ▶ Auswertung von 53 Vorfällen aus den vergangenen ca. 2 Jahren
(Quelle der Vorfälle v.a. projekt-datenschutz.de)
- ▶ Nur Vorfälle in Zusammenhang mit Webanwendungen
- ▶ Unberücksichtigt bleiben:
 - Phishing oder Identitätsdiebstahl
 - Verlust, Diebstahl oder Raub von Datenträgern
 - Datendiebstahl durch Interne oder Dienstleister

Entwurf der Datenschutz TOP10

- TOP 1: Fehler im Zugriffsrechte-Management (18 Fälle)
 - ▶ Vgl. OWASP-TOP10: A6, Security Misconfiguration
 - ▶ Fehlerhafter oder fehlender Zugriffsschutz auf nicht-öffentliche Bereiche oder Dokumente
 - ▶ Ursache sind u.a.
 - versehentliches Löschen von Schutzmechanismen,
 - Unkenntnis der Sicherheitslage ("Security-by-Obscurity„)
 - fehlende oder unklare Regeln, Zuständigkeiten und Rechte für die Publikation von Dokumenten oder Daten

Entwurf der Datenschutz TOP10

- TOP 1: Fehler im Zugriffsrechte-Management (18 Fälle)
 - ▶ Häufiger Schwachpunkt:
Fehlerhaft konfigurierte Content-Management-Systeme (CMS)
 - ▶ Fehlende Kontrollmechanismen bei Publikation
 - ▶ Fehlende/mangelhafte IT-Sicherheitsrichtlinien
 - ▶ Ziel: ein TOP10-Template "CMS".

Entwurf der Datenschutz TOP10

- TOP 2: Unzureichend abgesicherte Datenbanken (14 Fälle)
 - ▶ Vgl. OWASP-TOP10: A1, Injection
 - ▶ Hier speziell SQL-Injection
 - ▶ Weiterverarbeitung von externen Parametern ohne vorherige Validierung.

Entwurf der Datenschutz TOP10

- TOP 3: Unverschlüsselte oder unzureichend verschlüsselte Datenbankendaten (10 Fälle)
 - ▶ Vgl. OWASP-TOP10: A7, Insecure Cryptographic Storage
 - ▶ Im Unterschied zu TOP 2 geht es hierbei um Daten, die ohne Einschränkungen oder nur geringen Einschränkungen für die Funktionalität der Anwendungen verschlüsselt werden könnten, aber nicht oder unzureichend verschlüsselt wurden.
 - ▶ Usability vs. Sicherheit

Entwurf der Datenschutz TOP10

- TOP 4: Unautorisierter direkter Zugriff auf Daten mittels Parameter-Manipulation (9 Fälle)
 - ▶ Vgl. OWASP-TOP10: A4, Insecure Direct Object Reference
 - ▶ Änderung von request-Parametern (GET/POST/etc.), dadurch Zugriff auf personenbezogene Daten Dritter (in Folge: Möglichkeit zum Identitäts-Diebstahl)

Entwurf der Datenschutz TOP10

- TOP 5: Fehlerhafte Authentifizierungs-Mechanismen (9 Fälle)
 - ▶ Vgl. OWASP-TOP10: A3, Authentication and Session Management
 - ▶ Komplexität von Authentifizierungs-Maßnahmen wird häufig unterschätzt
 - ▶ NB: Auch die Sicherheit verschlüsselter Passwörter (md5) wird vielfach falsch eingeschätzt

Entwurf der Datenschutz TOP10

■ TOP 6: Email – Missmanagement (5 Fälle)

- ▶ Vgl. OWASP-TOP10: -
- ▶ Fehler bei der Zustellung von Emails
 - über Website-Formulare
 - Backend-Webapplikationen (automatisiert)
 - Newsletter-Systeme

Entwurf der Datenschutz TOP10

- TOP 7: (Sonstige) logische Softwarefehler (5 Fälle)
 - ▶ Vgl. OWASP-TOP10: -
 - ▶ Gemeint sind Fehler in der Business-Logik und unzureichende Testmechanismen
 - ▶ Führen zu Exposition persönlicher Daten Dritter auch bei regulärer Nutzung der Software

Entwurf der Datenschutz TOP10

- TOP 8: Fehlendes Unrechtsbewusstsein, Unkenntnis, Fahrlässigkeit (4 Fälle)
 - ▶ Vgl. OWASP-TOP10: -
 - ▶ Fehlende Sachkenntnis der Redakteure (Bedienung des CMS, Upload von Dokumenten via FTP/SSH)
 - ▶ Unzureichende Kenntnis der gültigen Rechtslage und möglicher Konsequenzen auf Seiten der Geschäfts- und Projektleitung

Entwurf der Datenschutz TOP10

■ TOP 9: (Interne) Sabotage (1 Fall)

- ▶ Vgl. OWASP-TOP10: m.E. A6, Security Misconfiguration
- ▶ Durch technische Maßnahmen nur eingeschränkt absicherbar
- ▶ Beispiele:
 - „Steuersünder-CDs“
 - Interne Kundendatenbank Fa. Schlecker

Entwurf der Datenschutz TOP10

- TOP 10: Unzureichender Schutz gegen "Data-Mining" (1 Fall)
 - ▶ Vgl. OWASP-TOP10: -
 - ▶ Data-Mining: Erkennung von Mustern in komplexen Datenstrukturen
 - ▶ Identifikation und Persönlichkeitsprofile einzelner Personen möglich
(auch bei anonymen/pseudonymen Anwendungen)
 - ▶ Problem von „false-positives“

Zusammenfassung

- Konzept branchen- oder anwendungsspezifischer "Security-Templates" auf Basis der OWASP TOP10
- Entwurf von TOP10 des Datenschutzes
 - ▶ Sicherheitsniveau von Web-Anwendungen mit personenbezogenen Daten verbessern
 - ▶ Bewusstsein der Verantwortlichen erhöhen („offene Ohren“-Konzept)

Ausblick

- Das Konzept der "Security-Templates" kann auf weitere Themengebiete angewandt werden:
 - ▶ Mobile Apps
 - ▶ Web-Services
 - ▶ Web2.0 / Social Networks
 - ▶ Content-Management-Systeme



Sicherheit von Webanwendungen als Maßnahme zum Schutz personen- bezogenener Daten

*Ein Entwurf für
TOP10 des Datenschutzes*

OWASP
20.10.2010

Dr. Ingo Hanke
OWASP-Mitglied
IDEAS
Information & Design Applications
owasp@ideas.de
Tell +49 (0)551 370 00 30

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

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