OWASP Top 10 Datenschutzrisiken

Alpha Version 1.0

#1 Schwachstellen in Webanwendungen

Häufigkeit: Hoch
Schaden: Sehr hoch

Schwachstellen sind ein zentrales Problem in jedem System, mit dem sensible Nutzerdaten erhoben, verarbeitet und genutzt werden. Bestehen Fehler im Design oder in der Implementierung der Applikation, werden Probleme nicht entdeckt oder Sicherheitspatches nicht unverzüglich eingespielt, führt dies mit hoher Wahrscheinlichkeit zu einer Verletzung des Persönlichkeitsrechts. Dieses Risiko wird bereits in anderen Projekten behandelt, wie der OWASP Top 10 Liste der häufigsten Sicherheitsrisiken für Webanwendungen.

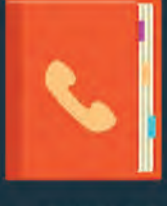
Häufigkeit: Hoch
Schaden: Sehr hoch

#2 Datenabfluss beim Betreiber

Wird die unerwünschte Preisgabe personenbezogener oder personenbeziehbarer Daten an nicht autorisierte Personen nicht wirksam verhindert, ist dies ein Verlust der Vertraulichkeit. Ursachen sind entweder ein vorsätzlich durchgeführter Datenabzug oder unbeabsichtigte Fehler wie beispielsweise unzureichendes Zugriffsmanagement, unsichere Datenablage, Datendopplung oder fehlendes Problembewusstsein (Awareness).

#3 Unzureichende Reaktion bei einer Datenpanne

Betroffene werden nicht über mögliche Pannen oder Datenlecks benachrichtigt, die durch Angriffe oder unbeabsichtigte Ereignisse entstehen. Angemessene Abhilfemaßnahmen zum Schließen der Lücken und Beseitigung der Ursache fehlen.



Häufigkeit: Hoch
Schaden: Sehr hoch

#4 Unzureichende Löschung personenbezogener Daten

Personenbezogene Daten werden nicht termingerecht oder nicht effektiv nach Zweckablauf bzw. aufgrund einer Löschanfrage gelöscht.

Häufigkeit: Sehr hoch
Schaden:hoch

Dieses Projekt wird unterstützt von msg:
www.msg-systems.com

Intransparente Nutzungsbedingungen

#5

Informationen zur Datenverarbeitung wie Erhebung, Speicherung und Nutzung personenbezogener Daten sind unzureichend. Diese Informationen sind nicht leicht zugänglich oder für juristische Laien nicht verständlich aufbereitet.

Häufigkeit: Sehr hoch
Schaden:hoch

#6

Sammlung von Daten, die über den eigentlichen Zweck hinaus gehen

Es werden Beschreibungsdaten, demographische Daten oder sonstige personenbezogene Daten gesammelt, die nicht für den vereinbarten Zweck der Anwendung benötigt werden. Ebenso werden Daten gesammelt, für deren Erhebung der Nutzer keine Einverständniserklärung abgegeben hat.

Häufigkeit: Sehr hoch
Schaden:hoch

Weitergabe von Daten an Dritte

#7

Personenbezogene Daten werden ohne Einverständnis des Nutzers an Dritte weiter gegeben bzw. diesen zur Verfügung gestellt. Die Weitergabe von Daten und Erkenntnissen erfolgt entweder direkt oder auf Anfrage, gegen Zahlung oder auch durch unsachgemäßen Einsatz von Diensten Dritter wie beispielsweise Widgets für Webseiten (z.B. Landkarten, Buttons von sozialen Netzwerken), Analysetools oder Web Bugs (z.B. Beacons).

Häufigkeit: Hoch
Schaden: Hoch

#8

Veraltete personenbezogene Daten

Es werden veraltete, inkorrekte oder gefälschte personenbezogene Daten genutzt. Datenaktualisierungen oder -korrekturen finden nicht in ausreichendem Maße statt.

Häufigkeit: Hoch
Schaden: Hoch

Fehlendes oder unzureichendes Session-Ende

#9

Unzureichendes Beenden von Sessions. Dies kann dazu führen, dass zusätzliche Nutzerdaten ohne Einverständnis oder Wissen des Nutzers gesammelt werden.

Häufigkeit: Mittel
Schaden: Sehr Hoch

#10

Unsicherer Datenaustausch

Die Datenübermittlung erfolgt nicht auf verschlüsselten und sicheren Kanälen, so dass ein unautorisierter Zugriff nicht verhindert wird. Mechanismen zum Verringern der Angriffsfläche, werden nicht umgesetzt. Hierzu gehört es zu verhindern, dass durch das Verhalten der Webanwendung Rückschlüsse auf Nutzerdaten möglich sind.

Häufigkeit: Mittel
Schaden: Sehr Hoch

Source: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project