dsb
datenschutzbeauftragte
des kantons zürich

Merkblatt

Sichere Website

1 Einleitung

Das Merkblatt richtet sich an Entscheidungsträgerinnen und Entscheidungsträger sowie Website-Verantwortliche. Es hilft, den Aufbau und Betrieb einer datenschutzkonformen und sicheren Website zu gewährleisten.

2 Risiken und Gefahren im Internet

Internetkriminalität betrifft alle, die Dienste im Internet anbieten oder beziehen. Die Behebung eines Schadens kann sehr hohe Kosten verursachen (Imageverlust, Datenverlust usw.). Zu den gängigsten Risiken zählen:

- Diebstahl einzelner Datensätze (Brute-Force-Angriff) oder ganzer Datenbestände (SQL Injection)
- Ausnutzen von Schwachstellen (Hacking) oder Kompromittieren von Systemen (Malware-Angriff), um zum Beispiel falschen Inhalt zu publizieren oder andere kriminelle Handlungen zu begehen
- Beeinträchtigung des Dienstes durch gezielte Überlastung (Denial-of-Service-Angriff)

Beim Betrieb einer Website sind auch rechtliche Voraussetzungen zu beachten. Ein unsachgemässer Aufbau oder Betrieb einer Website kann zu Verletzungen von Datenschutz- oder Geheimhaltungsvorschriften führen.

3 Datenschutzrechtliche Voraussetzungen

Der Betrieb einer datenschutzkonformen Website setzt die folgenden Vorkehrungen voraus:

- Abschluss einer vertraglichen Vereinbarung mit den Auftragnehmenden für die Entwicklung und den Betrieb der Website, die den Anforderungen von § 6 IDG (Gesetz über die Information und den Datenschutz, LS 170.4) und § 25 IDV (Verordnung über die Information und den Datenschutz, LS 170.41) entspricht. Siehe Leitfaden Bearbeiten im Auftrag.
- Werden Dienste Dritter verwendet beispielsweise Analysetools, so müssen diese auf die Datenschutzkonformität überprüft werden. Siehe Merkblatt Dienste Dritter auf Websites.

4 Organisatorisch-technische Massnahmen

Um den störungsfreien und sicheren Betrieb einer Website zu gewährleisten, sind mindestens folgende Massnahmen umzusetzen:

- Erhebung der Gefährdung und der notwendigen Massnahmen mit einer Risikoanalyse auf Basis der Top-10-Risiken des Open Web Application Projects (OWASP) und Open Web Application Project API
- Umsetzung der Massnahmen aus der Risikoanalyse
- Einsatz von Sicherheitskomponenten (Firewall, Web Application Firewall und Virenschutz)
- Konsequenter Einsatz von starker Authentifizierung und Verwendung von sicheren Verschlüsselungsprotokollen:
  - Verwendung eines zusätzlichen Faktors für die Authentifizierung (Authenticator App, MobileID, Zertifikat oder eines ähnlichen Verfahrens)
  - Verschlüsselte Übermittlung der Daten (data in transport) und verschlüsselte Speicherung (data at rest)
- Einhaltung der Passwortqualität und -richtlinie sowie Unterstützung der Benutzerinnen und Benutzer bei der Wahl eines starken Passworts (z.B. Anzeigen der Passwortstärke)
- Speicherung der Passwörter nach dem Stand der Technik mittels kryptographischer Einwegverfahren (salted hash)
- Definition von klaren Vorgaben und Anforderungen, damit stets aktuelle Software und Komponenten verwendet werden
- Regelmässige Sicherung der Daten (Back-up) sowie Sicherstellung, dass die Daten wiederhergestellt werden können
- Regelmässige Überprüfung der Applikation auf Schwachstellen (Penetration Test)
- Kontrolle und Auswertung der Protokolleinträge auf ungewöhnliche Vorkommnisse

5 Datenschutzfreundliche Einstellung von Cookies

Cookies sind meist Voraussetzung für die Funktion von Websites und Webanwendungen:

5.1 Checkliste Cookies-Konfiguration

Cookie-Attribut / Feld[1]	Checklisten Punkt	Erledigt
Name / Value	Sensitive Daten sind verschlüsselt im Cookie abgelegt.	☐
	Cookies für kritische Funktionen sind serverseitig signiert.	☐
Expires	Das Cookie besitzt eine funktionsabhängige und verhältnismässige Laufzeit.	☐
Max-Age		
Domain	Die Internetadresse(n), an die das Cookie zurückgeschickt werden darf, sind definiert.	☐
Secure	Die Option Secure ist gesetzt (in Verwendung mit TLS-Verbindungen (HTTPS)).	☐
HttpOnly	Die Option HttpOnly ist konfiguriert.	☐

Die einzelnen Attribute / Felder sind in Kapitel 5.2 erklärt.

[1] Internet Engineering Task, Request for Comments: RFC 6265, HTTP State Management Mechanism, https://tools.ietf.org/html/rfc6265#section-8 (zuletzt besucht am 16. September 2022).

5.2 Erklärung der Cookie-Attribute / Felder

Cookie-Attribut / Feld	Beschreibung	Datenschutzfreundliche Konfiguration (Privacy by default)
Name / Value	Die Attribute Name und Value werden zusammen verwendet. Dabei sind: – Name = Name des Cookies – Value = Inhalt des Cookies Beispiele: – Name = Value – Sprache=Deutsch – Warenkorb=«Produkt1:Produkt2» Name und Value werden an die Website zurückgeschickt (siehe auch Domain).	Je nach Verwendungszweck des Cookies ist der Name möglichst zufällig zu wählen und der gespeicherte Inhalt (Value) angemessen zu schützen. Bei kritischen Funktionen und besonders sensitivem Inhalt sind die im Cookie gespeicherten Informationen serverseitig mit modernen kryptischen Verfahren zu verschlüsseln und zu signieren.
Expires	Mit dem Attribut Expires wird die maximale Laufzeit eines Cookies im Format Datum und Uhrzeit spezifiziert.	Wenn die Attribute Expires oder Max-Age nicht gesetzt werden, bleibt das Cookie gültig, bis der Browser geschlossen wird. Diese Option ist zu bevorzugen. Für gewisse Fälle kann eine kürzere oder längere Laufzeit nötig sein, wie für die Gültigkeitsdauer der Anmeldeinformationen bei Inaktivität, die Spracheinstellung oder die (Nicht-)Einwilligung zur Aufzeichnung der Websiteaktivitäten (Consent). Längere Laufzeiten sind verhältnismässig zu wählen, idealerweise nicht länger als 3 Monate.
Max-Age	Mit dem Attribut Max-Age wird die maximale Laufzeit eines Cookies in Sekunden spezifiziert.	
Domain	Über das Attribut Domain wird die Internetadresse konfiguriert, an die das Cookie zurückgeschickt werden darf, zum Beispiel zh.ch. Es können mehrere Internetadressen eingetragen werden. Wenn das Attribut nicht konfiguriert wird, wird die Internetadresse verwendet, von der das Cookie gesetzt wurde.	Im Attribut Domain sollte nur die Internetadresse hinterlegt werden, die von der Benutzerin oder dem Benutzer aufgerufen wurde.
Path	Das Attribut Path bestimmt, auf welchen Verzeichnissen der Website das Cookie verwendet werden kann, beispielsweise auf der Haupt- und allen Unterverzeichnissen oder nur auf einem bestimmten Unterverzeichnis	Die Verwendung des Attribut Path kann für bestimmte Websites sinnvoll sein, etwa wenn eine Website neben dem öffentlichen Bereich in einem Unterverzeichnis einen geschützten Mitgliederbereich enthält und die Cookies ausschliesslich im Mitgliederbereich verwendet werden sollen.
Secure	Ist das Attribut Secure gesetzt, schickt der Browser das Cookie nur über einen verschlüsselten Kanal zurück, typischerweise über eine mit dem Transport Layer	Die verschlüsselte Verbindung (HTTPS) gehört heute zum Standard. Die Option Secure ist zwingend zu verwenden, um Risiken zu vermeiden.

Cookie-Attribut / Feld	Beschreibung	Datenschutzfreundliche Konfiguration (Privacy by default)
	Security (TLS) gesicherte HTTPS-Verbindung.	
HttpOnly	Cookies können bei einigen Browsern nicht nur per HTTP / HTTPS zurückgeschickt werden, sondern auch über Schnittstellen zur Verfügung gestellt werden. Mit dem Attribut HttpOnly kann dies verhindert werden.	Die Option HttpOnly ist zwingend zu verwenden. Der Browser sollte das Cookie nur an die Internetadresse zurückschicken, von der es gesetzt wurde.

6 Weiterführende Informationen

Datenschutzbeauftragte des Kantons Zürich
- Fragenkatalog Sicherheitsmassnahmen Webdienste
- Leitfaden Bearbeiten im Auftrag
- Merkblatt Cloud Computing
- Merkblatt Dienste Dritter auf Websites

Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
- Baustein, CON.3 Datensicherungskonzept
- Baustein, NET.3.2 Firewall
- Baustein, OPS.1.1.3 Patch- und Änderungsmanagement
- Leitfäden zur Entwicklung sicherer Webanwendungen
- CON.10 Entwicklung von Webanwendungen
- Massnahme, ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen
- Massnahme, OPS.1.1.4.A5 Betrieb von Virenschutzprogrammen
- Prävention von DDoS-Angriffen
- Sicherer Einsatz von JavaScript
- Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)
- Sicheres Webhosting
- TLS nach TR-03116-4 Checkliste für Diensteanbieter

Open Web Application Security Project (OWASP)
- OWASP Top Ten Project – die 10 häufigsten Sicherheitsrisiken für Webanwendungen
- Forgot Password Cheat Sheet

Wikipedia
- Brute-Force-Methode
- SQL Injection
- Web Application Firewall

V 1.8 / September 2022