dsb
datenschutzbeauftragter
kanton zürich

Merkblatt

Sichere Website

1 Einleitung

Dieses Merkblatt richtet sich an Entscheidungsträgerinnen und Entscheidungsträger sowie Website-Verantwortliche. Das Merkblatt 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:

- Datendiebstahl 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) i.V.m. § 25 IDV (Verordnung über die Information und den Datenschutz, LS 170.41) entspricht. Siehe Leitfaden Bearbeiten im Auftrag.

- Integration einer Datenschutz- und Sicherheitserklärung, die festhält, welche persönlichen Daten beim Zugriff auf die Website durch das öffentliche Organ erfasst und gespeichert werden. Beim Abschnitt Sicherheit muss beispielsweise darüber informiert werden, ob die Datenübermittlung per Kontaktformular verschlüsselt erfolgt oder nicht.

- 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, sollten mindestens folgende Massnahmen umgesetzt sein:

- Einsatz von Sicherheitskomponenten wie Firewall, Web Application Firewall und Virenschutz
- Definition von klaren Vorgaben und Anforderungen, dass stets aktuelle Software und Komponenten verwendet werden, sowie regelmässige Aktualisierung und Installation von Sicherheitsupdates
- Regelmässige Sicherung der Daten (Back-up) sowie Überprüfung, dass die Daten wiederhergestellt werden können
- Konsequenter Einsatz von starker Authentifizierung und Verwendung von modernen und sicheren Verschlüsselungsprotokollen:
  - Einhaltung der Passwort-Qualität und -Richtlinie
  - Verwendung eines zusätzlichen Faktors für die Authentifizierung (mTAN / SMS, mobile ID, Zertifikat oder eines ähnlichen Verfahrens)
- Regelmässige Überprüfung der Applikation auf Schwachstellen (Penetration Test) sowie Kontrolle der Protokolleinträge auf ungewöhnliche Vorkommnisse

5 Weiterführende Informationen

Datenschutzbeauftragter 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
- Bereitstellung von Webangeboten
- Leitfäden zur Entwicklung sicherer Webanwendungen
- Massnahme, ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen
- Massnahme, OPS.1.1.4.A5 Betrieb von Viren-Schutzprogrammen
- 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
- TLS/SSL Best Practice

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 1.2 / Juli 2018

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh