Wie speichere ich Daten von Websitebesuchern sicher?

Intention

Dieses Pattern befasst sich mit dem sicheren Speichern von Content und Nutzerdaten der Websitebesucher.

Problemstellung

Das sichere Speichern von Daten, sei es auf dem Server oder in einer Datenbank ist gerade bei personenbezogenen Daten, bedingt durch die *EU-Datenschutz-Grundverordnung (DSGVO)*, ein Muss. Es ist daher erforderlich Maßnahmen zu ergreifen, die eine sichere Datenspeicherung ermöglichen.

Szenario

Webspace und Domain sind eingerichtet. Eine Website ist aufgesetzt, diese erlaubt Benutzern Kommentare zu schreiben und auch Daten (Bilder oder Ähnliches) hochzuladen. Die Daten und Kommentare der User sollten nun sicher auf die Website übertragen und abgesichert werden.

Lösung

- Verwenden eines sicheren und aktuellen Systems
  - Ein aktuelles System mit einem Antivirenprogramm bietet weniger Angriffsvektoren für Hacker.
- Verschlüsselte Kommunikation (HTTPS) verwenden
  - Dies ermöglicht es den Datenaustausch im Vorhinein abzusichern, bevor dieser überhaupt gespeichert wird.
- Daten anonymisiert und/oder verschlüsselt speichern
  - Daten sollten nicht direkt als Klartext in der Datenbank gespeichert werden. Es bietet sich an, die Daten in verschlüsselter Form in der Datenbank abzusichern.
  - Einige Daten dürfen **nur verschlüsselt bzw. anonymisiert gespeichert werden** (beispielsweise **personenbezogene Daten**).
    - Mehr hierzu findet man im Pattern: „**Welche Daten darf ich auf meiner Website speichern?**“
- Zugriffsrechte setzen
  - Je weniger Personen einen Zugriff auf die Daten haben, desto sicherer sind diese.
  - Zugriffsrechte für die einzelnen Admins und Nutzer anpassen.
    - Jeder soll nur den eingeschränkten Zugriff auf Dateien oder Datenbanken bekommen, den er für seine Arbeit benötigt.

- Backup der Datenbank
    - Es geht nicht nur darum die Daten sicher zu speichern. Auch das Absichern der gespeicherten Daten ist wichtig.
- Verschlüsselung der Backups
    - Wenn Backups erstellt werden, bietet es sich an diese zu verschlüsseln. Dieser Schritt ist *optional*, kann aber den Zugriff unbefugter Personen auf die Dateien immens erschweren.

Beispiele

Sicherheit des eigenen Systems sicherstellen
Ein System, das auf dem aktuellsten Stand ist, bietet weniger Angriffsvektoren für potentielle Hacker. Daher sollte man immer die aktuellsten Updates installieren. Mehr dazu findet man im Pattern „**Wann und wie oft sollte man Updates installieren?**“. Es ist es auch notwendig die Website selbst abzusichern. Wie dies geschehen kann, beschreibt das Pattern „**Wie überprüfe ich die Sicherheit meiner Website?***“.*

Datenintegrität gewährleisten
Im Pattern „**Wie verschlüssele ich die Kommunikation mit meiner Website?**“ wird erklärt wie man eine SSL-Verschlüsselung auf der eigenen Seite integriert. Mit der sicheren HTTPS-Verbindung geschieht die Kommunikation zwischen dem Webbrowser des Nutzers und der verschlüsselten Website. Somit kann sicher gegangen werden, dass alle Daten die vom Nutzer stammen auch wirklich von ihm sind.

Verschlüsseln von gepackten Daten-Backups (Beispiel verwendet 7Zip)
- https://www.heise.de/tipps-tricks/ZIP-Archiv-mit-einem-Passwort-schuetzen-So-geht-s-3907870.html

Wie man mit php Passwörter verschlüsseln kann (englisch)
- https://paragonie.com/blog/2017/12/2018-guide-building-secure-php-software#secure-php-passwords

Referenzen

https://www.onlinesicherheit.gv.at/praevention/datensicherung_und_loeschung/datensicherung_und_wiederherstellung/249920.html
https://codex.wordpress.org/Function_Reference/wp_hash_password
http://www.kvcodes.com/2016/09/wordpress-password-hash-generator/

Keywords

Datensicherheit, Verschlüsselung, Datenspeicherung, personenbezogene Daten