Wie sieht ein guter und sicherer Webshop aus?

Intention

In diesem Pattern wird erläutert wie ein Webshop gut und sicher gestaltet werden kann und auf welche Aspekte dabei geachtet werden sollte.

Problemstellung

In den letzten Jahren ist Online-Shopping in aller Munde. Durch die stetig steigende Anzahl an Nutzern und damit verbundenen Nutzerkonten, sind Online-Shops ein beliebtes Ziel von Cyber-Kriminellen.

Szenario

Nur mit der Erstellung des Online-Shops ist es noch lange nicht getan. Die Sicherheit von Kundendaten hat hier oberste Priorität. Es gibt aber auch viele andere Aspekte, die beachtet werden sollten um einen guten und sicheren Webshop zu erstellen.

Lösung

Das Betreiben eines Online-Shops erweist sich nicht immer als einfach. Durch die neue DSGVO (EU-Datenschutz-Grundverordnung) wurden die Rechte der Kunden in vielen Punkten gestärkt. Daher lautet die erste Empfehlung, dass man die Erstellung und das Aufsetzen sowie den Betrieb eines Webshops in die Hände eines Experten legen sollte, wenn dies möglich ist.

Achtung: **Dieses Pattern ist keine Rechtsberatung! Im Rahmen der Recherche zu den Patterns, befassten wir uns zwar mit den geltenden Datenschutzbestimmungen sowie der DSVGO (https://www.dsb.gv.at/gesetze-in-osterreich), doch wir sind weder Juristen noch Datenschutz-Experten. Daher können wir für die Vollständigkeit, Aktualität als auch Richtigkeit der bereitgestellten Inhalte keine Haftung übernehmen.**

Für den Fall, dass man dennoch einen Webshop selbst betreiben will, sollten folgende Punkte beachten werden:

DSGVO

Als Besitzer und Betreiber eines Webshops muss man diesen DSGVO-konform gestalten und viele Regelungen umsetzen, unter anderem auch technische. Mehr Informationen zum Thema DSGVO und welche notwendigen Informationen Websitebesuchern bereitgestellt werden müssen, findet man in dem aufgelisteten Pattern in der Sektion “Beispiele”. Für Webshops ist anzumerken, dass auf die **Widerrufsmöglichkeit** hingewiesen werden muss. Ebenfalls hat ein Kunde das Recht auf **Löschung**, und **Korrektur** sowie ein **Auskunftsrecht** über seine, auf der Seite gespeicherten Daten. Des Weiteren muss auf der Seite angeben sein, ob Daten an **Server außerhalb der EU** weitergegeben werden. Weitere Informationen hierzu: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/AGB_im_Internet_-_allgemeiner_Ueberblick.html

Verschlüsselte Datenverbindung

Es ist zwingend erforderlich die Kommunikation und die Datenübertragung der Websitenutzern mit dem Webshop zu verschlüsseln. Dies wird empfohlen, um Datenintegrität im vornherein zu gewährleisten.

Daten und Systemsicherheit

Im Sinne der DSGVO sollte die Datensicherheit der Systeme gewährleistet sein. Daher sollten alle Systeme und jede Software aktuell gehalten werden. Patterns die sich mit dieser Thematik befassen und einen guten Überblick liefern, sind in der Sektion “Beispiele” zu finden.

Shopzertifikate und Gütesiegel

Shopzertifikate und Gütesiegel schaffen Vertrauen in den Webshop. Dieses Siegel zeigt den Kunden, dass der Webshop kontrolliert worden ist und er deshalb gewisse Anforderungen (Datensicherheit, usw.) erfüllt. Viele Gütesiegel-Anbieter prüfen den Webshop und auch das System. Sie vergeben ihre Siegel erst, wenn die Seite als sicher und gut befunden wurde.

Sichere Passwörter

Wenn man in einem Webshop einkauft, ist es meist notwendig ein Benutzerkonto zu erstellen. Es wird vom Kunden verlangt ein Passwort zu wählen. Es sollte darauf geachtet werden, dass dem Kunden bei der Passworterstellung geholfen wird. Dem Kunden sollte gezeigt werden, wie ein sicheres Passwort erstellt werden kann. Laut Statistik ist ein Passwort mit einer längeren Zeichenfolge viel sicherer als ein Passwort mit einer kurzen Zeichenfolge. Folgende Regeln können beim Erstellen eines Passworts gefordert werden und hilfreich sein, um die Passwortsicherheit zu erhöhen:

- Passwörter sollten Groß- sowie Kleinbuchstaben enthalten
- Sonderzeichen sollten enthalten sein
    - ‘, (,), =, !, usw.
- Vermeiden sollte man einfache Wörter, Geburtsdaten, Namen oder wiederholte Buchstabenfolgen, wie zum Beispiel:
    - asdfasdf, 123456, Heinz1, 12.10.2019, 121212, Supermann
- Mindestlänge sollte 8 Zeichen sein

Beispiele

Sicherheitsaspekte

Wie man eine SSL verschlüsselte Seite einrichtet, wird im Pattern „**Wie verschlüssele ich die Kommunikation mit meiner Website?**“ erläutert. Außerdem sollte man die Sicherheit der Website unter allen Umständen gewährleisten, da mit personenbezogenen Daten (Namen, Adresse, Kontodaten, usw.) gearbeitet wird. Auf diese Punkte wird in den Patterns „**Was trägt alles zur Sicherheit einer Website bei?**“, „**Wann und wie sollte man Backups erstellen?**“, „**Wie speichere ich Daten von Websitebesuchern sicher?**“, „**Welche Daten darf ich auf meiner Website speichern?**“, sowie „**Welche Informationen muss ich den Besuchern auf meiner Website bereitstellen?**“ eingegangen.

Empfohlene Anbieter von Zertifikaten und Gütesiegeln

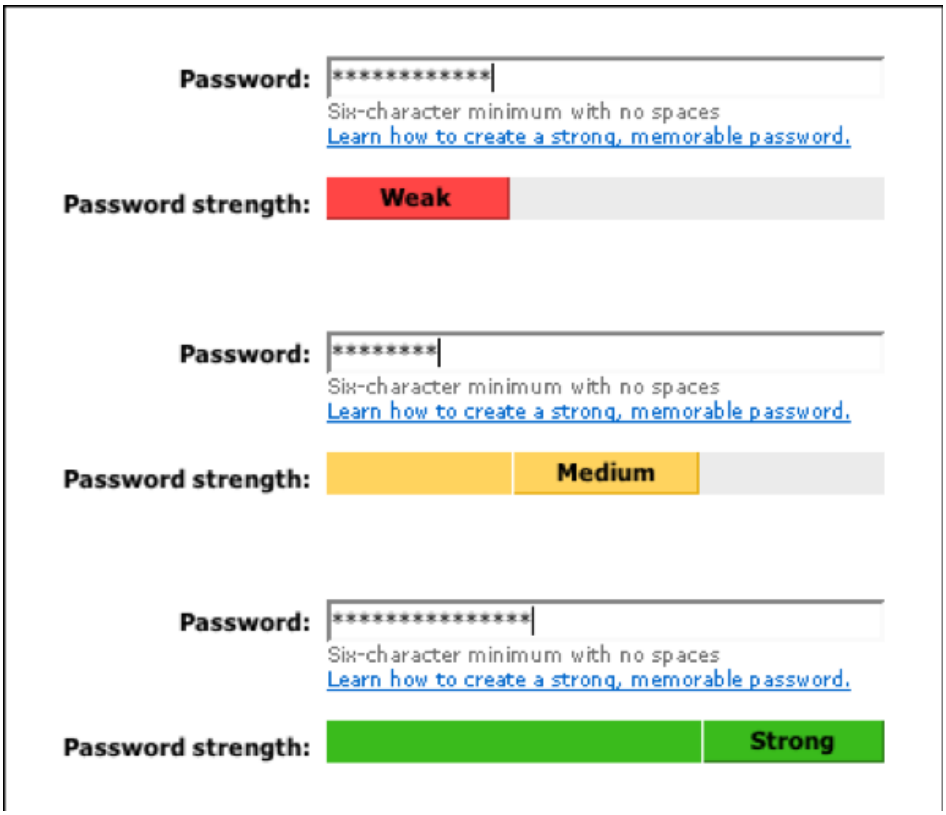
- https://www.trustedshops.at
- https://www.tuev-sued.de/fokus-themen/it-security/safer-shopping/onlinehaendler
- https://www.datenschutz-cert.de/ips-internet-privacy-standards.html
- https://ehi-siegel.de

Datenauskunft

Jeder Nutzer einer Website hat ein Recht auf Datenauskunft. Wenn eine Datenauskunft von einem Nutzer verlangt wird, muss man diese Auskunft binnen eines Monats leisten. Mehr Informationen hierfür findet man unter: https://www.dsb.gv.at/fragen-und-antworten#Wie_beantworte_ich_ein_Auskunftsersuchen

Password-Meter für sichere Passwörter

Folgende Grafik zeigt ein Password-Meter, das die Sicherheit eines Passwortes anzeigt.



_____ unsicher _____

- Im ersten Fall ist das Passwort länger als die geforderten 6 Zeichen, jedoch wurde eine wiederholte Zeichenfolge gewählt (z.B. „asdfasdf“), dies macht das Passwort unsicher.

_____ akzeptabel _____

- Im zweiten Fall ist das Passwort kürzer, aber es entspricht den Mindestvoraussetzungen. Da es den Voraussetzungen entspricht ist es akzeptabel aber nicht übermäßig sicher.

_____ sicher _____

- Fall Nummer drei zeigt ein viel längeres und damit auch sichereres Passwort.

Referenzen

https://www.troyhunt.com/86-of-passwords-are-terrible-and-other-statistics/
Wirtschaftsrecht / Gewerberecht – Muster für den Bestellablauf – Info der WKO
Datenschutzbehörde Österreich _

Keywords

DSGVO, Datenschutz, Personenbezogene Daten