CSBW CYBER SICHERHEITS AGENTUR BADEN-WÜRTTEMBERG

Sensibilisierung für die Absicherung Ihres Webshops

Webshops sind für viele Institutionen ein bedeutsamer Vertriebskanal, um Kundinnen und Kunden eine komfortable Einkaufsmöglichkeit anzubieten. Gleichzeitig verarbeiten Webshops zahlreiche sensible und personenbezogene Daten wie Namen, Adressen oder Zahlungsinformationen von Kundinnen und Kunden.

Daher sind Webshops ein attraktives Ziel für Angreifende, etwa um personenbezogene Daten zu stehlen, Bestellungen zu manipulieren, Rechnungen zu fälschen oder die Erreichbarkeit der Dienste lahmzulegen. Mögliche Folgen sind Umsatzeinbußen, Verluste von Kundinnen und Kunden sowie Datenschutzverstöße.

Mit den folgenden Maßnahmen lässt sich das Risiko, dass sensible Daten über den eigenen Online-Dienst an Unbefugte gelangen, deutlich reduzieren:

Sichere Passwörter:

Passwörter sind der Schlüssel für den Zugriff auf personenbezogene Daten. Nutzen Sie daher ausschließlich lange Passwörter für administrative Zugänge (mindestens 14 Zeichen). Verwenden Sie bitte zudem eine musterlose Kombination von Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.

Sie können für Ihren Webshop festlegen, wie sicher ein Passwort mindestens sein muss. Personen mit administrativen Zugängen können dann nur Passwörter verwenden, die diese Vorgaben erfüllen. Die Passwort-Anforderungen sollten idealerweise auch für Zugänge Ihrer Kundinnen und Kunden gelten.[1]

Sensibilisieren Sie dafür, dass **keine** personenbezogenen Daten, Begriffe aus dem Wörterbuch oder Institutionsnamen für Passwörter verwendet werden sollten. Das für Ihren Webshop verwendete Passwort sollte zudem einmalig sein und nicht für andere Dienste oder Profile verwendet werden. Das Passwort für den Webshop lässt sich über einen individuellen Merksatz oder durch einen Eintrag in einem Offline-Passwortmanager festhalten.

[1] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Zwei- oder Multi-Faktor-Authentifizierung

Durch die **Z**wei-**F**aktor-**A**uthentifizierung (2FA) wird neben dem Passwort (Wissen) ein zweiter Faktor (Besitz) erforderlich, um auf das System zuzugreifen. Zur Authentifizierung wird zusätzlich ein temporärer Bestätigungscode auf dem Smartphone, ein biometrisches Merkmal (z.B. ein Fingerabdruck) oder eine lokale Schlüsseldatei benötigt.

Wird ein Passwort gestohlen, können Angreifende nicht ohne das Vorliegen des zweiten Faktors auf die Accounts Ihrer Administration oder von Kundinnen und Kunden zugreifen. Die Zwei-Faktor-Authentifizierung sollte für Administrationszugänge des Webshops, für Hosting- und Serverzugänge, für E-Mail-Konten sowie für Profile Ihrer Kundinnen und Kunden eingerichtet werden.

Bei der **M**ulti-**F**aktor-**A**uthentifizierung (MFA) werden mehr als zwei Faktoren erforderlich, was die Sicherheit sensibler oder personenbezogener Daten zusätzlich erhöht.

Die 2FA bzw. MFA erhöht maßgeblich die Datensicherheit und den Schutz vor Webshop-Manipulationen sowie vor Zugriffen durch unbefugte Dritte.[2]

Patchmanagement

Anwendungen und Betriebssysteme weisen regelmäßig Sicherheitslücken auf, die von Angreifenden genutzt werden können, um unbefugt Zugriff auf Daten zu erhalten. Regelmäßige und unverzügliche Updates sorgen dafür, dass diese Sicherheitslücken geschlossen werden. Aktualisieren Sie regelmäßig Ihre Software für Webshop, Server und Betriebssysteme sowie Plugins/Erweiterungen. Aktivieren Sie automatische Updates für Ihre Anwendungen, sofern möglich. Bitte beachten Sie, dass während des Installationsvorgangs die Verfügbarkeit Ihres Dienstes vorübergehend eingeschränkt sein kann.[3]

[2] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_web_server_leitlinie.pdf?__blob=publicationFile&v=1

HTTPS-Verschlüsselung

Die HTTPS-Verschlüsselung (**H**yper**t**ext **T**ransfer **P**rotocol **S**ecure) maskiert die Kommunikation zwischen einem Webclient und einem Webserver bzw. zwischen dem Webshop und den Kundinnen und Kunden. Sie sorgt dafür, dass Browser und Server eine Sprache sprechen. Mit der Verschlüsselung soll verhindert werden, dass unbefugte Dritte Zugriff auf die Datenkommunikation erhalten. Geschützt werden dabei Login-Daten, persönliche Informationen sowie Zahlungsdaten.

Die HTTPS-Verschlüsselung wird durch sogenannte SSL- (**S**ecure **S**ockets **L**ayer) bzw. TLS-Zertifikate (**T**ransport **L**ayer **S**ecurity) ermöglicht. Diese Zertifikate bestätigen die Echtheit Ihres Webshops. Da diese zeitlich begrenzt sind, müssen sie rechtzeitig erneuert werden. Laufen die Zertifikate ab, erhalten Nutzende Warnmeldungen durch ihren Browser oder ihr Virenschutzprogramm, dass Ihr Webshop nicht sicher sei.[4]

Stellen Sie daher stets sicher, dass Ihre Zertifikate aktuell und gültig sind. Gegebenenfalls bietet Ihr Hosting-Anbieter eine automatische Zertifikatserneuerung an. Klären und verschriftlichen Sie hierzu die Zuständigkeiten mit Ihrem Hosting-Anbieter.[5]

Mehr Sicherheit, mehr Vertrauen:

Mit diesen gut umsetzbaren Maßnahmen lässt sich die Sicherheit für Ihren Webshop deutlich erhöhen. Die sorgfältige Einrichtung und regelmäßige Pflege der Sicherheitseinstellungen sind eine wichtige Investition, um Ihren Webshop zu schützen und gleichzeitig das Vertrauen Ihrer Kundinnen und Kunden durch sorgsamen Schutz ihrer Daten zu stärken.

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_web_server_leitlinie.pdf?__blob=publicationFile&v=1

[5] https://blog.rwth-aachen.de/itc/2022/12/28/ssl-zertifikate/