DATENSCHUTZ & SICHERHEIT

Armin Jakupovic, Roman Etter

AB04 – Modul 150

Inhalt

Datenschutz

Datenschutz ist ein wichtiges Thema, ob im geschäftlichen Kontext oder als Privatperson. Sowohl die juristische als auch gewöhnliche Person werden vom Datenschutzgesetz behandelt, vorausgesetzt deren Daten werden verarbeitet. Hierbei kann man zwei unterschiedliche Arten unterschieden, wobei beide personenbezogen sind und mit entsprechender Sorgfalt behandelt werden sollen.

Datenerhebung und Rechte

Das Erheben und Verarbeiten von Daten erfordern die explizite Zustimmung der Person. Stimmt diese nicht zu, so ist die Verarbeitung ihrer Daten der nicht gestattet. Der Person muss die Begründung bzw. der Zweck der Datensammlung und -verarbeitung offengelegt werden. Sie ist jederzeit in der Lage, die Datenverarbeitung abzulehnen. Die Person kann zu jeder Zeit Einsicht auf die gesammelten bzw. verarbeiteten Daten verlangen und deren Herkunft erfahren. Dieses Recht muss unter allen Umständen gewährt werden.

Persönliche Daten

Der Schutz der persönlichen Daten, sowohl von Kunde als auch Mitarbeiter, spielt gerade bei einer Firma wie Interdiscount eine grosse Rolle. Mit dem Webshop werden tagtäglich hunderte Bestellungen und damit auch persönliche Daten verarbeitet. Per Richtlinie werden ausschliesslich Daten verarbeitet, die auf vertraglicher Basis eine Notwendigkeit aufweisen. Dies kann, zum Beispiel, bei einer Bestellung im Webshop auftreten – damit der Kaufvertrag erfolgreich abgewickelt werden kann, wird auf persönliche Informationen wie der vollständige Name und Adresse zurückgegriffen.

Zu den persönlichen Daten gehören unter anderem folgende Bestandteile:

- Name
- Adresse
- Pseudonymisierte Daten
- Jegliche Daten die zur direkten Identifizierung einer individuellen Person verwendet werden können

Sensible Daten

Parallel zu den persönlichen Daten, existieren Daten, die aufgrund ihrer sensiblen Natur weitere Massnahmen zum Schutz dieser benötigen. Damit dieser erweiterte Schutz gewährleistet ist, werden Massnahmen auf der technischen und firmenspezifischen Seite eingeführt. Aus technischer Sicht werden hier strengere Zugriffsbeschränkungen, DSGVO basierte Massnahmen wie Pseudonymisierung, Anonymisierung oder erweiterte Verschlüsselungen eingesetzt. Firmenspezifisch können Geheimhaltungsvereinbarungen durchgesetzt werden, die das Verbreiten von sensiblen Daten auch auf juristischer Ebene einschränkt.

Zu den sensiblen Daten gehören unter anderem folgende Bestandteile:

- Ethnizität und Herkunft
- Politische Meinung, Weltanschauung
- Religion
- Genetische und Biometrische Daten
- Gesundheit, Sexualität und Sexualleben

Authentifizieren

Grundlagen

Eine E-Business-Anwendung wird üblicherweise von mehreren Personen verwendet. Diese müssen voneinander getrennt behandelt werden und somit klar identifiziert werden. Eine sichere Authentifikation ist gerade aus dem Grund wichtig, da unterschiedliche Benutzer auf eine Reihe von persönlichen und, unter Umständen, auch sensible Daten Zugriff haben. Die Authentifizierung wird heutzutage oftmals mit der eigenen E-Mail-Adresse und einem Passwort durchgeführt. Die Anforderungen an das Passwort kann zwar von Applikation zu Applikation unterschiedlich gehandhabt werden, jedoch hat sich im Verlauf der Zeit ein Referenzpunkt durchgesetzt. Meist wird ein mindestens 8 Zeichen langes Passwort erwartet, welches Grossbuchstaben, Kleinbuchstaben und Ziffern beinhaltet. Eine weitere Anforderung, die sich immer mehr -verbreitet, ist das hinzufügen eines Sonderzeichens. Gerade Applikationen mit sensiblen Daten und Zugriffen gehen diesen weiteren Schritt und fordern Sonderzeichen und tendenziell noch längere Passwörter.

Bei der Interdiscount wird, beispielsweise, beim Webshop ein 8 Zeichen langes Passwort erwartet, welches sowohl Gross- und Kleinbuchstaben als auch eine Ziffer oder Sonderzeichen enthält. Bei internen Anwendungen werden höhere Ansprüche gefordert, über die wir keine Auskunft geben dürfen.

Zwei-Faktor Authentifizierung

Eine etwas neuartige Methode, die in vielen E-Business-Applikationen Platz gefunden hat, ist die Zwei-Faktor Authentifizierung. Dabei handelt es sich um eine erweiternde Art von Authentifizierung, die auf den oben erklärten Massnahmen aufbaut. Um eine erfolgreiche Authentifizierung durchzuführen, werden zwei bestätigende Faktoren erwartet. Zum einen wird eine normale Authentifizierung mit der passenden E-Mail und Passwort Kombination durchgeführt. Erfolgt diese, so wird der zweite Faktor ausgelöst, die dem Benutzer einen Code zur endgültigen Authentifizierung bereitstellen soll. Dieser wird an ein persönliches geschütztes Gerät, normalerweise dem Smartphone, zugestellt. Das kann auf zwei unterschiedliche Wege geschehen – SMS und App - die nochmals näher angeschaut werden. Der erhaltene Code wird dann in der Applikation eingegeben. So wird sichergestellt, dass keine Fremdperson per Zufall an das Passwort des Benutzers gelangt ist und nun Zugriff über die Applikation erhält.

SMS-Zustellung

Ein Zwei-Faktor Code kann an die persönliche Telefonnummer zugestellt werden. Diese Methode wird auch heute noch eingesetzt und ist weit verbreitet. Experten in der Security Branche sind gegenüber dieser Methode jedoch etwas skeptisch. Sie stufen den Versand über SMS als kritisch ein, da Nachrichten unsicher verschickt werden und von Angreifern ohne allzu grossen Aufwand abgefangen oder verfälscht werden können. Die Zwei-Faktor Authentifizierung würde sich auf ein unsicheres Kommunikationsmedium verlassen und so die Wirksamkeit beeinträchtigen.

Authentifizierungs-App

Eine bevorzugte Methode für den Erhalt eines Codes ist das Verwenden einer App – beispielsweise Google Authenticator. Die App generiert auf konstanter Basis neue Codes, die für einen bestimmten Zeitraum gültig sind – grundsätzlich nicht länger als 30 Sekunden. Das Generieren von Codes funktioniert auch ohne Zugriff auf das Internet. Die Möglichkeit, Codes abzufangen oder eine Aufforderung zu verfälschen, wird damit aus dem Weg gegangen. Einige E-Business-Applikationen fordern den Benutzer auch auf eine App, statt der eigenen Telefonnummer, zu verwenden.

Speicherung von Passwörtern

Eine Regel, die heutzutage trotzdem immer wieder gebrochen wird und Schlagzeilen macht, ist das Speichern von Passwörtern als lesbarer Text in der Datenbank. Dies sollte unter allen Umständen ausnahmslos vermieden werden und **niemals** so gehandhabt werden. Das Schadensrisiko, im Falle das ein

Angreifer Zugriff auf die Datenbank erhält, ist enorm. Er hätte vollen Zugriff auf jegliche Logins. Der Standard heute basiert auf Hashing, sowohl beim Benutzer, der die Login Request stellt, als auch bei den in der Datenbank gespeicherten Daten.

Hashing

Wie bereits erwähnt, werden Passwörter mit dem Hashing Verfahren behandelt. Passwörter in der Datenbank, in einer Request und beim Vergleich befinden sich immer im verschlüsselten bzw. gehashten Zustand. Bei einer Authentifizierung wird aus der Benutzereingabe ein Hash generiert, welches anschliessend mit dem gespeicherten Hash in der Datenbank verglichen wird. Sind die zwei Hashes identisch, so wird die Authentifizierung als erfolgreich angesehen.

Interne Applikationen

Die Authentifizierung wird bei unseren internen Applikationen etwas anders gehandhabt. Das Login passiert mit einem Benutzernamen und Passwort, eine E-Mail ist zwar dem Konto zugewiesen, wird aber nicht für das Login verwendet. Darauf bauend ist die oben erklärte Zwei-Faktor Authentifizierung, diese ist nämlich verpflichtend. Bis vor kurzem war der SMS-Versand davon noch möglich, inzwischen wird in den meisten e-Business-Applikationen eine App erwartet. So ziemlich Applikationen, die mit sensiblen Daten interagieren, setzen dieses Verfahren durch.

Verschlüsselungen

Der Sinn und Zweck einer Verschlüsselung ist es, Dritten und Unbefugten die Einsicht in Daten zu erschweren und gar unmöglich zu machen. Es gibt viele Wege, wie ein solches Prinzip realisiert werden kann. Im Laufe der Zeit wurden unzählige Verschlüsselungsalgorithmen und Verfahren entwickelt und verwendet. Einige davon wurden in der Zwischenzeit geknackt und gelten als unsicher, andere hingegen haben den Test der Zeit so weit überlebt, dass sie als sicher angesehen werden.

Einsatz von Verschlüsselung

Wie oben erwähnt, gilt es bei der Verschlüsselung, Dateneinsicht für Unbefugte zu verhindern. Es gibt verschiedene Einsatzgebiete, in denen der gezielte Einsatz eines Verschlüsselungsverfahrens zu mehr Sicherheit und Vertrauen in das System führen kann. Ein wichtiges Einsatzgebiet ist sicherlich die Übertragung von Daten, insbesondere sensibler oder persönlicher Daten. Optimalerweise wird bei Kommunikation über das http Protokoll ein SSL Zertifikat eingesetzt, welches die Verbindung verschlüsselt. Somit werden übertragene Daten für Dritte, die sich einklinken möchten, unleserlich.

Ein weiteres Einsatzgebiet, in welchem Verschlüsselung definitiv seinen Platz hat, ist bei der Speicherung von Daten. Es bringt nichts, wenn zwar die Übertragung der Daten zur Datenbank sicher ist, aber die Speicherung ungeschützt verläuft. Je nach dem, was die Daten beinhalten und in welchem Kontext sie stehen, ist es lohnend, diese verschlüsselt und gesichert zu speichern. Eine geklaute Datenbank, die zwar unleserliche Passwörter hat, aber dennoch persönliche Daten wie Adressen, Namen, AHV-Nummern oder ähnliches beinhaltet, ist ein hohes Risiko. Kriminelle können diese Daten für Identitätsdiebstahl verwenden, dies kann für die betroffene Person schwere Folgen haben. Verschlüsselung kann hierbei helfen und persönliche Daten schützen.

Verschlüsselung bei Interdiscount

Bei Interdiscount setzen wir selbstverständlich alle Standarte ein. Sprich, die Kommunikation mit Endgeräten der Benutzer, erfolgt mit dem SSL Zertifikat. Zudem werden die vertraulichen Daten der Benutzer verschlüsselt gespeichert. Falls ein Angreifer also trotz allen Sicherheitsvorkehrungen, bis zur Datenbank gelangen sollte, kann dieser nichts Grosses damit anfangen. Ausserdem besteht mit Hilfe von Verschlüsselung Schutz gegen Session-Hijacking, genauere Angaben dazu sind jedoch leider vertraulich.