Sicherheits- & Datenschutzkonzept

1. Allgemeine Informationen

1.1. Firmendaten

Wiesmüller & Gschwantner OG
Zeltgasse 12/9
1080 Wien

1.2. Stand

21.06.2018

2. Sicherheitskonzept

2.1. Infrastruktur

Aufgrund der kleinen Größe beschränkt sich die Netzwerkinfrastruktur auf einen Router und die jeweiligen Arbeitsgeräte der Geschäftsführer und Mitarbeiter, plus ein Raspberry Pi Server. Innerhalb des Netzwerkes existieren keine ungeschützten Freigaben oder Zugänge, der Zugriff von außen ist prinzipiell nicht möglich.

2.1.1. Interne Infrastruktur

Die Server Infrastruktur besteht aus einem Root Server im Hetzner Rechenzentrum und einem Raspberry Pi Server im internen Firmennetzwerk. Letzterer wird vor allem als Datenbank Server für die lokale Entwicklung benutzt. Auf diese Datenbanken kann nicht ohne Benutzername und Passwort zugegriffen werden.

Der Root Server wird für verschiedene Services von inspiredminds benutzt:

- Web Server für eigene Websites und temporäre Entwicklungs- bzw. Staging Umgebungen für Kundenaufträge
- ownCloud Server für Cloud Speicherplatz, Sharing, Kontaktdaten
- InvoicePlane für das Erstellen und Verschicken von Rechnungen an Kunden
- Passbolt Open Source Password Manager
- Matomo Website Besucher Statistik Analyse

2.1.2. Externe Infrastruktur

Folgende externe Services werden eingesetzt, mit denen personenbezogene Daten verarbeitet werden:

- Google G Suite: Kalenderdaten, Emails an und von Kunden
- MailChimp: Für den Versand von Newsletter
- GitLab: Sourcecode Versionierung
- WebGo: externes Webhosting

2.2. Verwaltung von Anmeldedaten

Im Zuge der Entwicklung für Aufträge von Kunden speichert inspiredminds Zugangsdaten von Server, Email Postfächern, Datenbanken und dergleichen.

- Alle Anmeldedaten werden in einer verschlüsselten Datenbank (KeePass 2.x) gespeichert.

- Es wird ein sicheres Passwort für diese Datenbank verwendet, welches einmal jährlich gewechselt wird.
- Das Passwort dieser Datenbank ist nur den Geschäftsführern bekannt.
- Besteht kein aktiver Vertrag oder Kontakt mit einem Kunden, werden die damit verbundenen Zugangsdaten aus der Datenbank gelöscht.
- Die Software wird so eingestellt, dass das Passwort nach einer gewissen Zeit oder wenn der Computer gesperrt wird, wieder neu eingegeben werden muss.

Bei der Weitergabe von Passwörtern an Mitarbeiter wird ein Open Source Password Manager namens “Passbolt” eingesetzt (Siehe Punkt 2.1.). Diese Software stellt ein hohes Maß an Sicherheit in Bezug auf Verschlüsselung und Sicherheit der Passwörter her.

- Mitarbeiter bekommen nur die für das jeweilige Projekt relevanten Zugangsdaten.
- Der Zugriff auf die Passwörter wird jeweils nach Ende des Projektes entzogen.

2.3. Verwendung von Anmeldedaten

Geschäftsführer und Mitarbeiter von inspiredminds sind angehalten folgende Richtlinien einzuhalten:

- Falls Passwörter in einem externen Programm (wie z.B. FileZilla oder Firefox) zwischengespeichert werden, um schnell darauf zugreifen zu können, muss dies jeweils mit einem eigenen, sicheren Master Password abgesichert sein.
- Nicht mehr benötigte Passwort Daten müssen aus den externen Programmen entfernt werden.
- SSH Keys sollten zusätzlich mit einem eigenen Passwort gesichert sein.
- Eigens festgelegte Passwörter müssen einen von der Geschäftsführung festgelegten Sicherheitsstandard erfüllen.

2.4. Office Space & Geräte

Es gibt kein gesondertes Konzept für die physische Absicherung von außen. Geschäftsführer und Mitarbeiter haben Schlüssel für die Büroräumlichkeiten. Es wird eine Schlüsselliste geführt. Alle Geräte sind Passwort geschützt und werden bei Inaktivität gesperrt.

2.5. Projekt- & Kundendaten

Alle sonstigen Projekt bzw. Kundendaten werden in der ownCloud gespeichert. Beispiele sind Designs, Verträge, Bildmaterial, Angebote, Rechnungen, etc.

Nur die Geschäftsführer haben Zugriff auf alle Daten. An Mitarbeiter werden nur die für sie und das jeweilige Projekt relevanten Daten freigegeben. Nach Abschluss des Projektes wird die Freigabe wieder entzogen.

Es gibt keine personenbezogenen Daten, die als Hardcopy aufbewahrt werden.

3. Datenschutzkonzept

Als Entwickler von Web Applikationen ist es das Ziel die Verarbeitung bzw. Speicherung von personenbezogenen Daten, auf die während der Entwicklung Zugriff besteht, zu minimieren, die Daten zu löschen wenn sie nicht mehr gebraucht werden und den unbefugten Zugriff auf die Ressourcen von inspiredminds zu verhindern. Das beinhaltet auch, dass keine personenbezogenen Daten als Hardcopy aufbewahrt werden - mit Ausnahme von Mitarbeiter Daten (siehe Punkt 3.2.).

Im Wesentlichen müssen bei inspiredminds drei Punkte bzgl. dem Schutz von personenbezogenen Daten beachtet werden.

3.1. Kunden Stammdaten & Email Verkehr

Die Kontaktdaten zu einzelnen Kunden werden an zwei verschiedenen Stellen gespeichert. Einerseits im CardDAV Service des ownCloud Cloud Speicher Services, andererseits im InvoicePlane Verrechnungs-Service.

Beide Services werden von inspiredminds auf einem eigens verwalteten Root Server, der im Rechenzentrum von Hetzner steht, betrieben. Alle Benutzerzugänge zu diesen Services verwenden sichere Passwörter, die in der im Punkt 2.2. erwähnten Datenbank gespeichert werden.

Darüber hinaus verwendet inspiredminds Google G Suite für die Kommunikation mit Kunden über Emails.

3.2. Sekundäre Personendaten

Damit sind Daten gemeint, auf die inspiredminds aufgrund der Entwicklung von Aufträgen für den Kunden Zugriff hat. Bspw. personenbezogene Daten von Benutzern von Web Services.

Während eines Auftrags zur Entwicklung und Wartung von Web Applikationen können Backups von Datenbanken anfallen, in denen sich personenbezogene Daten befinden. Diese werden jedoch immer nur temporär gespeichert, sofern vom Kunden nicht ein entsprechender Auftrag zur Durchführung und Verwaltung von Backups besteht.

- Server & Datenbankzugänge etc. werden wie in Punkt 2.2. erwähnt bei nicht Bestehen eines Auftrages gelöscht.
- Etwaige Datenbank Backups oder sonstige temporäre Inhalte mit personenbezogenen Daten werden unmittelbar nach dem notwendigen Einsatz gelöscht.

3.3. Mitarbeiter Stammdaten

Die digitalen Daten zu den Mitarbeitern werden auch in der ownCloud gespeichert. Diese Daten umfassen Kontaktdaten und Dokumente.

Dokumente zu den Mitarbeitern können auch als Hardcopy existieren.