Technische und Organisatorische Maßnahmen (TOMs)

TOMs der ITEG IT-Engineers GmbH

Version 1.0 vom 7.5.2018

Hinweis: PDF-Downloads aller veröffentlichten Versionen finden sich am Beginn von Vereinbarungen über ITEG-Hosting als Auftragsverarbeitung nach Art. 28 DSGVO.

Einleitung und Ausblick

Bei ITEG IT-Engineers GmbH wurde intuitiv immer schon sicher und am Stand der Technik gearbeitet. Dies werden wir durch eine Zertifizierung nach ISO 27001 im Lauf des Jahres 2018 auch offiziell bestätigt bekommen. Sobald dies erfolgt ist werden wir hier die ISO-Zertifizierten TOMs einarbeiten bzw. auf ISMS-Maßnahmen verweisen.

Um auch in der Zwischenzeit DSGVO-konforme Auftragsverarbeitungs-Vereinbarungen abschliessen zu können finden sich folgend unsere wichtigsten Technischen und Organisatorischen Maßnahmen:

Zugangskontrolle

Alle Hosting-Server befinden sich in versperrten Racks in Datencentern mit elektronischer Zutrittskontrolle sowie Videoüberwachung.

Die verschlüsselten Offline-Backups werden in einem versperrten Stahlschrank im ITEG-Büro aufbewahrt.

Datenträgerkontrolle

Unverschlüsselt werden die Hosting-Daten werden nur auf den internen Festplatten der jeweiligen Server sowie am primaren Backup-Space (ebenfalls im Datacenter) gespeichert.

Der Backup-Spiegel auf einem NAS im ITEG-Büro ist verschlüsselt.

Die einzigen mobilen Datenträger, die externen Backup-Medien, sind verschlüsselt und werden in einem versperrten Stahlschrank gelagert.

Benutzerkontrolle und Zugriffskontrolle

Die Daten-Verzeichnisse und Datenbanken verschiedener Shared-Hosting-Kunden sind vor gegenseitigem Zugriff durch entsprechende Vergabe der Verzeichnis-Berechtigungen geschützt. Dies wird gelegentlich überprüft.

Bei virtuellen Root-Hosts werden verschiedene Bereiche die von verschiedenen Webagenturen bzw. Entwicklern betreut werden nach Möglichkeit nach dem gleichen Schema vor gegenseitigem Zugriff geschützt.

Über Administratorenrechte auf physischen Hosts und virtuellen Server verfügen ITEG-seitig nur die beiden Geschäftsführer, die sich ausschliesslich mit PIN-geschützten Hardware-Token (yubikey) einloggen können. Der Zugriff auf physische Hosts ist außerdem auf bestimmte Client-IP-Adressen (ITEG-Büro, Wohnung des CTO, ...) eingeschränkt.

Auf virtuellen Root-Hosts haben teilweise auch die jeweiligen Kunden (die Verwantwortlichen) bzw. von den Verantwortlichen beauftragte volle Administratorenrechte und sind für die Benutzerkontrolle mitverantwortlich.

Zugriff auf virtuelle Roothosts ist generell nur mit SSH möglich, FTP wird nur auf ausdrücklichen Wunsch ermöglicht.

Übertragungskontrolle, Eingabekontrolle

Die einzige von ITEG durchgeführten Übertragungen erfolgen im Rahmen des Backups. Das nächtiche Backup auf ITEG-eigene Backup-Server wird geloggt, die Aktualisierung der externen Generationen-Backups wird intern und auf den Medien dokumentiert.

Transportkontrolle

Der Transport von Daten zwischen ITEG-Systemen, z.B. imzuge der nächtlichen Backups, erfolgt ausschließlich SSH-verschlüsselt.

Die einzigen mobilen Datenträger, die externen Backup-Medien, sind LUKS-verschlüsselt und werden - außer zur Aktualisierung des Backup-Standes - in einem versperrten Stahlschrank gelagert.

Wiederherstellung

Alle Daten (Dateien, Datenbanken als Dumps) werden nächtlich auf einen Backup-Space gesichert der wiederum auf einen 2. Backup-Standort gespiegelt (verschlüsselt) wird von dem aus 6 verschlüsselte externe Backup-Medien (je 2 Wochen-, Monats- und Jahres-Stände) befüllt werden.

Die Wiederherstellbarkeit von Daten aus den Backups wird durch entsprechende Kundenanfragen regelmäßig geprüft.

Datenintegrität

Auf allen Servern werden mindestens einmal im Monat die vom Hersteller verfügbaren Sicherheitsupdates eingespielt.

Bei Bekanntwerden von kritischen Lücken (die eine unberechtigte Übernahme von Systemen aus der Ferne ermöglichen) erfolgt die Absicherung binnen 24 h, durch Einspielen der entsprechenden Updates oder ggfs. durch Konfigurationsanpassungen.

Disclaimer Alt-Software Betriebssysteme

Beim für Hosting eingesetzten Betriebssystem, Debian Linux, wird jede Generation nur für ca. 2-5 Jahre mit Updates versorgt. Gehostete Kundendienste (Webanwendungen, ...) müssen daher regelmäßig auf neuere virtuelle Server migriert werden um weiterhin sicher genug zu sein.

Für die Verarbeitung von Personenbezogenen Daten auf nicht mehr mit Sicherheits-Updates versorgten Betriebssystemen übernimmt ITEG keinerlei Verwantwortung.

Die Migration von bei ITEG gehosteten Projekten auf neuere Betriebssystem-Generationen wird von ITEG kostenlos durchgeführt und begleitet.

Disclaimer Web-Anwendungen

Bei allen häufig eingesetzten Frameworks (WordPress, Typo3, u.v.a.) werden regelmäßig Sicherheitslücken bekannt die nur durch Zeitnahe bzw. regelmäßige Updates der Frameworks geschlossen werden können bzw. müssen.
Auch individuell programmierte Web-Anwendungen enthalten oft typische Sicherheitslücken.
Die Zuständigkeit für diese Bereiche liegt beim Auftraggeber bzw. Verantwortlichen.

Eine Liste typischer Fehler bzw. Problembereiche samt Lösungsstrategien findet sich in den OWASP Top Ten auf https://www.owasp.org/.