Technisch Organisatorische Maßnahmen

DataReporter GmbH

Zeileisstraße 6
4600 Wels
Österreich

1. Zutrittskontrolle

1.1. Absicherung von Eingängen, Fenstern, Serverraum, etc.

Beschreibung:

Sämtliche Eingänge sind verschlossen, Türen und Fenster über Nacht geschlossen, Tür verriegelt wenn niemand im Büro ist

Risiken:

Zutritt von Unbefugten, Diebstahl

Verhaltensregeln:

Türschloss verriegeln bei verlassen

1.2. Biometrische Zugangssperren

Beschreibung:

Haupttür mit Fingerprint - Reader abgesichert. Administration nur von Büro aus möglich.

Risiken:

Zutritt von Unbefugten

2. Zugangskontrolle

2.1. Authentifikation mit Benutzername / Passwort

Beschreibung:

Sämtliche Systeme sind nur mit Benutzername / Passwort zugänglich.

Risiken:

Nutzung von Unbefugten

2.2. Einsatz einer Hardware-Firewall

Beschreibung:

Eine zweistufige Hardwarefirewall wird verwendet, um das Büronetzwerk abzusichern

Risiken:

Hacking

2.3. Einsatz von Anti-Viren-Software

Beschreibung:

Auf sämtlichen Workstations und Servern wird aktuelle Antivirussoftware verwendet

Risiken:

Hacking, Trojaner, Viren, Ransomware

2.4. Einsatz von VPN-Technologie

Beschreibung:

Um bei Kunden Fernwartungen durchzuführen wird entweder auf VPN - Technologie, oder Teamviewer zurückgegriffen.

Risiken:

Nutzung von Unbefugten, Hacking

2.5. Sicherung der Administrationszugänge

Beschreibung:

Die Administrationszugänge der Server werden über zertifikatsgesicherte SSH - Zugänge realisiert, die nur über einen verschlüsselten VPN - Zugang zugegriffen werden können

Risiken:

Hacking, unbefugter Zugriff

2.6. Verschlüsselung von Datenträgern in Laptops / Notebooks

Beschreibung:

Sämtliche Notebooks und mobile Geräte (Handy, Tablet) sind vollständig hardwareverschlüsselt

Risiken:

Nutzung von Unbefugten bei Verlust

2.7. Verschlüsselung von mobilen Datenträgern

Beschreibung:

Mobile Datenträger, die Geschäftsgeheimnisse oder Personendaten enthalten werden verschlüsselt

Risiken:

Nutzung von Unbefugten bei Verlust

3. Zugriffskontrolle

3.1. Einsatz einer Software - Firewall

Beschreibung:

Durch Konfiguration einer Software - Firewall mit den minimalst nötigen Zugriffsberechtigungen wird ein Angriff auf offene Datenbank- oder Dateizugänge ausgeschlossen.

3.2. Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

Beschreibung:

Ein Aktenvernichter mit Datenschutz - Gütesiegel ist vorhanden und wird bei sämtlichen Dokumenten vor der Entsorgung verwendet

Risiken:

Datenzugriff von Unbefugten

3.3. ordnungsgemäße Vernichtung von Datenträgern

Beschreibung:

Datenträger werden vor der Entsorgung (sofern möglich) sicher gelöscht und danach hardwaremässig unlesbar gemacht. Datenträger (auch bereits gelöschte) werden unter keinen Umständen an Dritte abgegeben oder verkauft.

Risiken:

Datenzugriff von Unbefugten

3.4. physische Löschung von Datenträgern vor Wiederverwendung

Beschreibung:

Vor der Wiederverwendung im Unternehmen werden Datenträger sicher gelöscht

Risiken:

Datenzugriff von Unbefugten

3.5. Sichere Aufbewahrung von Datenträgern

Beschreibung:

Datenträger werden in einem versperrbaren Kasten mit 4-stelligem numerischem Code gelagert

Risiken:

Datenzugriff von Unbefugten

4. Weitergabekontrolle

4.1. Verschlüsselte Datenübertragung und -verarbeitung von Kundendaten

Beschreibung:

Daten aus Kundensystemen werden mit Secure Socket Layer/Transport Layer Security (SSL/TLS) verschlüsselt auf den Server übertragen. Alle Dokumente aus Kundensystemen werden verschlüsselt auf einem Amazon S3 Server gespeichert. Es gibt zu keinem Zeitpunkt Zugriff auf Passwörter oder Schlüssel. Passwörter werden sicher gehashed (und dadurch unidentifizierbar). Die Datenbanken für Kundendaten werden täglich gesichert und verschlüsselt auf einem redundanten Amazon S3 - Bucket in der Region Frankfurt aufbewahrt.

5. Auftragskontrolle

5.1. Auswahl der Provider

Beschreibung:

Der Provider wird nach bestem Wissen ausgesucht, Mindestvoraussetzung ist eine ISO 27001 - Zertifizierung und ein verbindliches Verfügbarkeits- und Servicelevel.

5.2. Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

Beschreibung:

Unternehmen mit denen wir zusammenarbeiten werden sorgfältigst auf Seriösität und Einhaltung aller datenschutzrechtlichen Erfordernisse geprüft

Risiken:

Mißbräuchliche Verwendung der Personendaten

5.3. laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Beschreibung:

Ein jährliches Audit aller Auftragnehmer soll sicherstellen, dass sich an der Qualität der Tätigkeiten nichts verschlechtert hat und der Auftragnehmer am aktuellen Stand der Technologie ist.

Risiken:

Mißbräuchliche Verwendung der Personendaten

5.4. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Beschreibung:

Sofern nicht anders vereinbart, werden Daten nach der Auftragsbeendigung und einer angemessenen Löschfrist vollständig vernichtet.

Risiken:

Mißbräuchliche Verwendung der Personendaten

5.5. vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

Beschreibung:

Sofern möglich, werden die Sicherheitsmassnahmen des Auftragnehmers persönlich und vor Ort geprüft. Ansonsten werden nur Auftragnehmer verpflichtet, die über eine ISO - Zertifizierung verfügen.

Risiken:

Mißbräuchliche Verwendung der Personendaten

6. Verfügbarkeitskontrolle

6.1. Aktualisierungsmanagement

Beschreibung:

Sämtliche Server werden über ein automatisiertes Updatemanagement aktualisiert (inklusive Testumgebung) um Sicherheitslücken durch veraltete Systemsoftware auszuschliessen.

Risiken:

Unbefugter Zugriff

6.2. Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Beschreibung:

Die Backups werden vollverschlüsselt und an einem zweiten Standort zusätzlich gelagert (> 30 km entfernt)

Risiken:

Datenverlust

6.3. Erstellen eines Backup- & Recoverykonzepts

Beschreibung:

Die Datenbanken für Kundendaten werden täglich gesichert und verschlüsselt auf einem redundanten Amazon S3 - Bucket in der Region Frankfurt aufbewahrt. Die Rotation für Backups sind täglich über die letzten 7 Tage, monatlich und jährlich. Nach 3 Jahren werden die ältesten Backups gelöscht. Die Verschlüsselung ist am neuesten Stand der Technik und mittels asynchroner Verschlüsselung realisiert. Der private Schlüssel wird nirgends in der Cloud gelagert.

Entwicklungsdaten werden täglich gesichert und aufbewahrt.

Alle Daten werden monatlich in einen internen Datenspeicher im Rechenzentrum von Datareporter übertragen.

Risiken:

Datenverlust

Verhaltensregeln:

Neben dem täglichen automatisierten Monitoring werden monatlich auch händisch die Backupvorgänge überprüft. Zusätzlich wird ein zufälliges Backupfile entschlüsselt und auf inhaltliche Konsistenz geprüft.

6.4. Feuer- und Rauchmeldeanlagen

Beschreibung:

Das gesamte Gebäude verfügt über eine vernetzte Rauch-, CO2 und Brandmeldeanlage, die den verantwortlichen über SMS alarmieren kann. Alle 3 Monate wird eine Funktionsprüfung der Anlage vorgenommen.

Risiken:

Datenverlust

6.5. Klimaanlage in Serverräumen

Beschreibung:

Im Büro und Serverraum wird eine Klimaanlage eingesetzt um Ausfälle durch Überhitzung zu vermeiden.

Risiken:

Datenverlust

6.6. Schutzsteckdosenleisten in Serverräumen

Beschreibung:

Die Server und Büros sind vollständig mit Überspannungsschutz ausgestattet

Risiken:

Datenverlust

6.7. Serverräume nicht unter sanitären Anlagen

Beschreibung:

Server stehen im Obergeschoss, es sind keine Wasserleitungen darüber verbaut.

Risiken:

Datenverlust

6.8. Testen von Datenwiederherstellung

Beschreibung:

Alle 6 Monate wird eine Prüfung sämtlicher Datensicherungen vorgenommen.

Risiken:

Datenverlust

6.9. Unterbrechungsfreie Stromversorgung (USV)

Beschreibung:

Sämtliche Server, Netzwerkgeräte und Workstations verfügen über eine USV - Sicherung mit automatischem Shutdown. Die Kapazitäten genügen für einen Betrieb für mindestens 15 Minuten bevor der Shutdown eingeleitet wird. Eine Prüfung erfolgt alle 6 Monate.

Risiken:

Datenverlust

7. Trennungsgebot

7.1. Trennung von Produktiv- und Testsystem

Beschreibung:

Produktiv- und Testsysteme sind strikt voneinander getrennt (hardwaremässig). Testdaten und Datenbanken die von Kunden zu testzwecken erhalten wurden werden in einem speziellen Speicherbereich gelagert, der nach der definierten Löschrfrist von 6 Monaten automatisch gelöscht wird.

Risiken:

Datenverlust, Datenpanne