5.1.1 Cloudsicherheitsrichtlinie

Zielsetzung

Speziell im IT-Umfeld, soll diese Sicherheitsrichtlinie zur Sensibilisierung gegenüber den potenziellen Risiken beitragen und entsprechende Handlungsanleitungen geben.

Wenn Daten mit Hilfe von Cloud-Diensten erhoben, gespeichert bzw. verarbeitet werden, drohen spezielle Gefahren. Insbesondere die dynamische Verteilung der Speicherkapazitäten über verschiedene Standorte, die in der Regel dem Nutzer nicht bekannt sind, verlangen eine spezifische Vorsorge hinsichtlich der Informationssicherheit und des Schutzes der Informationen.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter der IT Manufactory GmbH, wenn sie im Rahmen dienstlicher Tätigkeiten Daten in der Cloud erheben, speichern oder verarbeiten.

Verantwortlichkeiten

Der Die Verantwortung für die Cloudsicherheit liegt bei IT Manufactory GmbH Security, Betrieb und unserem Cloud-Dienstanbietern. Wir sind dafür verantwortlich sicherzustellen, dass die Cloudsicherheitsrichtlinie regelmäßig überprüft und eingehalten werden.

Cloudsicherheit

Die IT Manufactory GmbH arbeitet ausschließlich mit Cloud-Diensten in allen Bereichen des Unternehmens.

Jeder Mitarbeiter, deren dienstliche Tätigkeit direkt oder indirekt davon betroffen sein kann, ist verpflichtet, sich stets an einschlägige Weisungen der IT Manufactory GmbH zu halten.

- Die Speicherung und Verarbeitung von dienstlichen Daten in Cloud- Diensten Dritter, wie beispielsweise pCloud, Strato HiDrive, Dropbox, Luckycloud, Google Drive oder ähnliche Dienste, ist grundsätzlich nicht gestattet.

- Das Abrufen von kostenpflichtigen Informationen für den Privatgebrauch, für den Dienstgebrauch nur nach Zustimmung der Geschäftsleitung.
- Private Up- und Downloads, die nicht dringend für den Dienstgebrauch erforderlich sind.
- Weitergabe von Passwörtern und Zugangsdaten zu Cloud- Diensten.
- Der Zugriff von anderen Personen auf Cloud- Dienste.
- Veränderungen der Konfiguration ohne klare Zustimmung und Anweisung des Vorgesetzten.

Für die Entscheidung in welchen Anwendungen Daten in der Cloud erhoben, gespeichert oder verarbeitet werden, gibt es klare Aufgabentrennungen und Verantwortlichkeiten.

Sollten Unklarheiten bezüglich Daten der Cloud – Dienste bestehen, gibt es eine weiterführende Dokumentation in Organisationsfremde IT-Dienste IT-Dienstleistungen.

Informationssicherheit

Unser IMS und die Informationssicherheitsrichtlinien der IT Manufactory GmbH stellen klar, dass für die Verarbeitung personenbezogener Daten in der Cloud die Bestimmungen des Datenschutzgesetzes (BDSG) und auch der Datenschutz-Grundverordnung (DSGVO) gelten. Es fordert entweder die Einwilligung der Betroffenen (im Fall der Datenverarbeitung außerhalb der EU), oder die Anwendung der Regelungen zur Auftragsdatenverarbeitung (Datenverarbeitung innerhalb der EU).

Darüber hinaus sind auch Geschäftsgeheimnisse i.S.d. Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) schutzbedürftige Daten. Eine Offenlegung von Geschäftsgeheimnissen darf grundsätzlich nur dann erfolgen, wenn der jeweilige Vertrags- oder Geschäftspartner zuvor auf die Vertraulichkeit verpflichtet worden ist und das einzuhaltende Sicherheitsniveau für den Schutz der Daten beim Empfänger der Daten gewährleistet ist.

Informationssicherheits, -ausbildung und -schulung

Jeder Mitarbeiter der IT Manufactory GmbH hat regelmäßig an Schulungen, die über das Vorgehen bei Sicherheitsvorfällen, Datenpannen und über die Bedeutung und mögliche Konsequenzen von Verstößen, teilzunehmen oder muss sich darüber beim ISMS-Beauftragten der IT Manufactory GmbH informieren.

Zugangssteuerung

Die IT Manufactory GmbH steuert die Registrierung und Deregistrierung von Benutzern, dass ausschließlich eine Zuteilung von Benutzerzugängen, sowie Informationszugangsbeschränkung einem berechtigten Personenkreis im Rahmen der dienstlichen Tätigkeit erlaubt wird.

Kryptographischen Maßnahmen

Der Mitarbeiter hat vorrangig den verschlüsselten Internetzugang der IT Manufactory GmbH zu nutzen. Für das Telearbeit (Home-Office / Mobiles arbeiten) gelten die Telearbeitsrichtlinien. Das eingesetzten von Verschlüsselungsverfahren und möglichen Optionen ist Pflicht.

Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Jeder Mitarbeiter hat die datenschutzrechtlichen Maßnahmen einschließlich Risikobetrachtung auch für Situationen, in denen Testdaten verwendet werden zu berücksichtigen.

Sicherung von Information

Bei der Nutzung von Cloud – Diensten sind die in Frage kommenden Datenmengen auf das

notwendige Mindestmaß zu begrenzen. Der primäre Speicherplatz für Daten bleibt weiterhin das Dokumentenmanagementsystem Microsoft SharePoint der IT Manufactory GmbH. Cloud Anbieter Back-Ups sind soweit möglich und relevant konfiguriert.
Eine weiterführende Dokumentation zur Sicherung von Informationen, befindet sich in der Datensicherheitsrichtlinie.

Löschung von Daten

Anbieter von Cloud-Speicher setzen normalerweise Speichertechniken zur effizienten Ausnutzung der physikalischen Speicherkapazitäten ein. Aufgrund dieser Speichertechnik können Daten oft erst nach einer gewissen Zeitspanne gelöscht werden. Grundsätzlich kann nicht ausgeschlossen werden, dass beim Absetzen des Löschbefehls die Daten lediglich für den Anwender ausgeblendet, aber nicht gelöscht werden. Daher sind Daten, die einer beispielsweise gesetzlichen Löschverpflichtung unterliegen, für die Ablage in der Cloud ungeeignet.

Ereignisprotokollierung

Protokollierung von Zugriffen und alle Arten von Änderungen werden soweit möglich und relevant zu jeder Zeit einsehbar. Protokoll-Informationen werden nur zu beauftragten Zwecken und dazu befugten Mitarbeitern genutzt. Die Daten werden regelmäßig nach Ablauf von angemessenen und dokumentierten Fristen gelöscht.

Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Jeder Mitarbeiter der IT Manufactory GmbH hat im Rahmen seines Arbeitsvertrags die Verpflichtung zur Geheimhaltung.

Meldung von Verstößen

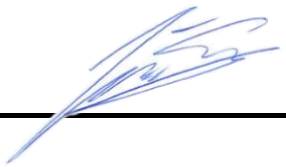
Vorgehensweise bei Verstößen gegen die Cloudsicherheitsrichtlinie.
Wenn personenbezogene Daten, Geschäftsgeheimnisse verletzt werden oder eine solche Verletzung droht (z.B. Verlust von Arbeitsgeräten oder Dokumenten, Hacker-Angriffen, Angriffen durch Schadsoftware etc.), hat der Mitarbeiter umgehend die Geschäftsführung, Vorgesetzten oder den Datenschutzbeauftragten zu informieren. Bei IT-Verstößen ist ferner unverzüglich die IT-Abteilung zu informieren.

Wichtige Kontaktdaten

IT-Notfälle: ISMS-Beauftragte siehe Notfall Kontakte

Ort, den

Passau, 14.03.2023



Geschäftsführung