united cloud GmbH

Dokumentation der technischen und organisatorischen Maßnahmen

Inhaltsverzeichnis

1 Rechenzentrum Frankfurt

1.1 Zutrittskontrolle

Definition:
Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

Beschreibung des Zutrittskontrollsystems:

Die Rechenzentrumsbereiche am Standort Frankfurt am Main befinden sich in zwei voneinander abgetrennten Gebäuderiegeln, mit jeweils separaten Brandschutz-, Stromversorgungs- und Löschkonzepten in unmittelbarer Nähe zueinander. Die beiden Bereiche werden daher mitunter als „Redundanzkonzept vor Ort“ genutzt. Beide Rechenzentrumsbereiche sind nicht ohne die Passierung der baulich vorgelagerten Büroräume begehbar. Büroräume und Rechenzentrumsbereiche sie ebenerdig nicht zu erreichen. Das Reguläre Betreten der Immobilie ist entweder (Sondernutzungsbefugnis) durch die Aufzuganlage der Tiefgarage oder im Erdgeschoss über einen vorgeschalteten Empfangsbereich (regulär) möglich. Daneben existiert ein separat gesichertes Treppenhaus als zweiter Fluchtweg. Die Nutzung der Tiefgarage ist nur durch die Geschäftsleitung, leitende Angestellte oder im Ausnahmefall durch vorherige Terminierung über ein Ticket -System möglich. Nach dem Austritt aus der Fahrstuhlanlage (entweder über die Tiefgarage oder über den Empfangsbereich im Erdgeschoss) sind die, den Rechenzentrumsbereichen vorgelagerten Büroräume, nur über zwei zu überbrückende Türsysteme (Vorraum mit Toilettenbereich und danach durch eine weitere Tür zum Eintrittsbereich in die Büroräume) zugänglich. Für Besucher, Interessenten und Neukunden sind diese Zutrittshindernisse bis zu den Büroräumen nur über Gegensprechanlagen, Kamerasysteme, biometrische Datenerfassung und Vorabanmeldung, ggf. mit persönlicher Abholung überwindbar. Für die Geschäftsleitung, leitende Angestellte und Techniker, erfolgt der Zutritt bis in die Büroräume über biometrische Daten oder elektronische Schlüsselsysteme. Büroräume und Rechenzentrumsbereich sind sodann abermals durch Türbereiche mit gleichen Sicherheitsvorkehrungen voneinander getrennt. Elektronische Schlüssel und Fingerabdruck-Abnahmesysteme sämtlicher Türen berücksichtigen abgestufte Befugnis-Kategorien. Alle Rechenzentrums-, Büro- und Vorräume unterliegen bereits jetzt sehr hohen, technischen Sicherheits-Standards, welche im Rahmen unserer laufenden-den, noch nicht abgeschlossenen ISO-Zertifizierung von externen Sachverständigen überprüft werden. Alle Rechenzentrums-, Büro- und Vorräume sind videoüberwacht. Die Schlüsselvergabe an Mitarbeiter und Kunden erfolgt kontrolliert und wird protokolliert. Es existieren Arbeitsanweisung und regelmäßige Wiederholungsbesprechungen, in denen alle Mitarbeiter zu sämtlichen sicherheitsrelevanten Themen informiert werden. Alle Türen und Fenster müssen nach Verlassen der Räumlichkeiten immer geschlossen sein. Jeder Mitarbeiter ist für diese Sicherheitsmaßnahme verantwortlich. Das Gebäude ist nachts verschlossen und wird durch Wachpersonal gesichert.

Es ist ausgeschlossen, dass sich Kunden der First Colo ohne die gleichzeitige Anwesenheit von Mitarbeitern in den Büroräumen oder im Rechenzentrum bewegen können. Selbst außerhalb der Geschäftszeiten, ist nachts der Zugang in die Büroräume und ins Rechenzentrum nur unter gleichzeitiger Anwesenheit von Mitarbeitern der First Colo möglich. Die Anwesenheit eigener Mitarbeiter von First Colo ist zwingende Voraussetzung für den technischen Zutritt Dritter.

1.2 Verfügbarkeitskontrolle

Definition:

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

Beschreibung der Verfügbarkeitskontrolle:

Löschsystem: Alle technischen Räume verfügen über ein separates Brandschutzkonzept, dass vom TÜV-Rheinland und der Feuerwehr Frankfurt abgenommen wurden. Jeder Raum verfügt über eine Gaslöschanlage die mit einer Mehrzonen-Detektion ausgestattet ist. Ein einzelner Rauchmelder löst nur einen technischen, internen Vor-Alarm aus. Brandalarm hingegen ist erst gegeben, wenn zwei der im ganzen Raum angebrachten Rauchmelder anschlagen. Im Ernstfall werden die Serverräume mit Löschgas geflutet, um aufkommende (Schwel-)Brände im Vorfeld zu ersticken. Darüber hinaus sind alle Räume mit Brandfrühesterkennungs-Systemen ausgestattet. Mit hoher Alarmqualität meldet sie frühzeitig, bevor ein Brand entsteht, schon die geringsten Partikel einer Rauchentwicklung durch Schwelbrände. Für konventionelle Brandmelder wären solche Gefahren in ihrer Entstehungsphase praktisch nicht zu detektieren.

Redundanzen der Infrastruktur (Klima, Notstrom, Anbindung): Unser Rechenzentrum wurde nach dem Tier2+ Standard errichtet und verfügt über Redundanzen in allen technischen Bereichen. Neben einer redundanten Stromanbindung und Glasfaseranbindung, sind alle technischen Komponenten mindestens in einem n+1 Konzept vorhanden, damit es bei Wartungen oder Ausfällen zu keinen Einschränkungen kommt.

Stromversorgung und Kühlung: Wir schützen unsere Stromkreise durch batteriegestützte USV-Anlagen, die bei Stromunterbrechungen oder Spannungsabfall die Strom-Versorgung des Rechenzentrums übernehmen. Im Ernstfall kann unser Rechenzentrum bis zu 20 Minuten durch unsere USV-Anlagen versorgt werden. Bei Stromunterbrechungen die länger als zwei Minuten dauern, wird die gesamte Last von unserem Dieselgenerator übernommen, damit es zu keinen unnötigen Batterie-Entleerungen der USV kommt. Unser Dieselgenerator lässt sich jederzeit während des Betriebes betanken. Ein Stromausfall könnte somit mehrere Tage und Wochen

überbrückt werden. Rechenzentren produzieren zudem viel Wärme und müssen gekühlt werden. Klima- und Kälteanlagen in unseren Rechenzentren sind nach den Anforderungen für hochverfügbare Systeme ebenfalls redundant ausgelegt. Die moderne Klimatisierungstechnik reguliert Temperatur und Luftfeuchtigkeit der Server-Räume mit Kaltgang-Einhausungen, in denen kalte Luft durch den Boden nach oben gepresst und verdrängte Warmluft abgesaugt wird.

(optional buchbarer) DDoS-Schutz: Zur Abwehr von DDoS-Attacken auf IT-Infrastrukturen setzen wir auf selbst-entwickelte Software in Verbindung mit Hardware-Applikationen weltmarktführender Hersteller. Unsere DDoS-Schutz-Lösung arbeitet mit mehrstufigen Filterprozessen. Sollte ein Anfrage-
Muster demnach als DDoS-Angriff identifiziert werden, sperrt unser DDoS-Schutz den unerwünschten Datenverkehr automatisch durch Umrouten aus dem Netzwerk aus. Unser DDoS-Schutz schützt somit alle Elemente der IT-Infrastrukturen unserer Kunden. Die DDoS-Schutzlösung dokumentiert lückenlos und detailliert alle DDoS-Vorfälle bei allen geschützten IT-Systemen. Die transparente Nachvollziehbarkeit der Schutzlösung dient dem professionellen bzw. geschulten Nutzer der Visualisierung sämtlicher Angriffsvektoren und Angriffs-Szenarien.

Ergänzende Hinweise: Sämtliche, auch die hier nicht ausdrücklich erwähnten, sicherheitsrelevanten (IT-)Technologien (wie Firewalls etc.) entsprechen entweder dem Stand der Technik oder sogar darüberhinausgehenden, überdurchschnittlichen Ansprüchen, wie sie für ein Hochverfügbarkeits-Rechenzentrum Standard sind oder erwartet werden können. Als IT-Infrastrukturanbieter bieten wir lückenlos alle, aber je nach Bedarf abgestufte Verfügbarkeits-, Sicherheits-, Redundanz- und Backup-Konzepte – bis hin zur Spiegelung der gesamten Daten-Infrastruktur in einem georedundanten Rechenzentrum an. Ein etwaiger Datenverlust, der aus unserer Sphäre heraus zu vertreten wäre, ist daher nahezu auszuschließen.

1.3 Backups

Sämtliche erstellten Backups, sowohl System-Backups durch united cloud erstellt, als auch durch Kunden gebuchte Backup Dienste werden an einem zweiten, 10km entfernten Standort in Frankfurt gesichert.

2 united cloud Allgemein

2.1 Zugangskontrolle

Definition:

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Beschreibung der Zugangskontrolle:

Die Speicherung von personenbezogenen Daten ist ausschließlich auf den dafür vorgesehenen Servern zulässig. Eine arbeitsplatzbezogene Speicherung erfolgt nicht. Beim Log-in erfolgt eine Passwortabfrage. Zunächst wird dem Mitarbeiter vom Systemadministrator ein „Erstpasswort“ zur Verfügung gestellt, welches dann vom entsprechenden Mitarbeiter geändert werden muss.

Nur auf den Servern im Rechenzentrum sind die Kunden- und Verwaltungsdaten zentral gespeichert. Die Server im Rechenzentrum verfügen zur Administration über entsprechende Benutzerkonten.

Zusätzlich gibt es noch ein Administrator-Konto für den Zugriff von Mitarbeitern des Rechenzentrums, welches jedoch nur im Bedarfsfall (und je nach vertraglicher Vereinbarung nur durch den Kunden selbst) aktiviert wird.

Um unautorisierten Zugang zu verhindern, sind die Server zudem in getrennten Netzwerkbereichen sowie über Firewalls geschützt.

Der Zugang zu den Rechnern in den Büroräumen wird über Benutzerkonten kontrolliert. Hierzu hat jeder Mitarbeiter ein eigenes Benutzerkonto sowohl für den lokalen Rechner, als auch für die Verwaltungssoftware, mit deren Hilfe auf die Kunden- und Verwaltungsdaten im Rahmen des Supports kontrolliert zugegriffen werden kann.

2.2 Zugriffskontrolle

Definition:

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Beschreibung der Zugriffskontrolle:

Als „Beherbergungsbetrieb“ für datenverarbeitende Unternehmen sind uns in der Regel nach Installations- und Anmeldeprozessen mit erstmaliger Passwortvergabe, weitestgehend sämtliche nachfolgenden administrativen Befugnisse ab der Passwortänderung durch den Kunden entzogen.
Die Installations- und Anmeldeprozesse erfolgen nach individuellen vertraglichen Regelungen, die in diesem Dokument aus Sicherheitsgründen und aufgrund der individuellen Praktikabilität nicht darstellbar sind.

Überwiegend sollen intern jedoch insbesondere folgende Ziele erreicht werden:

- Schutz vor Datenmanipulation (beabsichtigt / unbeabsichtigt)
- Sicherheit vor unbefugtem Zugriff
- Sicherstellung von rechtlichen Bindungen gegenüber Dritten (z.B. Lizenzrecht)

und damit die obersten Schutzziele der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität der Daten.

Für alle Nutzer von Datenverarbeitungseinrichtungen wird ein Benutzeraccount eingerichtet, der zum Zugang zu den entsprechenden Geräten mittels Benutzerkennung und Passwort auf der Grundlage der unternehmensweiten Passwort-Policy berechtigt. Auf Basis der Zugangsberechtigung wird für bestimmte Nutzer bzw. Nutzergruppen die Vergabe von konkreten Benutzerrechten (Zugriffsrechten) geregelt. Zugriffsrechte können vergeben werden

- für das Recht, bestimmte Programme zu nutzen,
- für das Recht, bestimmte Geräte (wie Drucker, Scanner usw.) zu nutzen,
- für das Recht, bestimmte Schnittstellen (z. B. Internet) zu nutzen und
- für das Recht, auf bestimmte Datenbestände in unterschiedlicher Art und Weise (Lesen, Schreiben, Verändern, Löschen, Dateistruktur bzw. Dateiattribute ändern, usw.) zuzugreifen.

Die Vergabe neuer, das Ändern und Aufheben / Löschen von bestehenden Zugriffsrechten erfolgt über einen Benutzerantrag. Die Neuanlage / Änderungen / Aufhebung wird (durch die Geschäftsführung, die Personalabteilung oder einem Abteilungsleiter) dem Informationssicherheitsbeauftragtem (ISB) mitgeteilt. Dieser füllt den Benutzerantrag aus und stößt den Freigabeprozess an. Daraufhin werden die benötigten Informationen freigegeben.

Einrichtung: Die Einrichtung und Pflege der Nutzer erfolgt durch die verantwortlichen System-Administratoren.

Zugriff: Der Zugriff auf computergestützte Systeme und Daten bzw. das Wahrnehmen von Systemprivilegien, ist nur nach bewusstem Anmelden mit dem individuellen Benutzer- / Administrator-Namen möglich. Damit ist sichergestellt, dass Einträge einem Benutzer / Administrator persönlich zugeordnet werden.

Dokumentation

Die Dokumentation des Zugriffsschutzes muss eine Beschreibung der Anforderung an Passwörter (Länge, Zeichenfolge, erlaubte Zeichen, Groß- / Kleinschreibung des Passwortes, Sperre) enthalten (sogenannte Passwortkonvention, s. u.).

Passwortänderung: Die regelmäßige Passwortänderung ist technisch erzwungen (Passwortkonvention, s. u.).

Irrtum / Fehler: Für den Fall eines notwendigen Passwortrücksetzens (z. B. vergessenes Passwort) kann mit Hilfe des Systemadministrators das Passwort ersetzt werden.

Regelung für Benutzernamen: Der Benutzername zur Anmeldung an das Netzwerk setzt sich immer aus dem ersten Buchstaben des VORNAMENS, einem Punkt und dem NACHNAMEN zusammen (Beispiel: M.SCHMIDT). Groß- und Kleinschreibung wird nicht unterschieden. Sollte der Fall von gleichnamigen Mitarbeitern eintreten, wird hierfür zusammen mit der Geschäftsführung oder dem ISB eine Sonderregelung getroffen, so dass Benutzernamen eindeutig bleiben und eine Zuordnung stets möglich ist.

Regelung für Passwörter (Passwortkonvention)

Allgemein: Passwörter für Systeme und Anwendungen bei der united cloud GmbH dürfen nicht leicht zu erraten sein. Beispiele wie eigener Name, Kfz-Kennzeichen oder Geburtsdatum dürfen deshalb nicht als Passwörter gewählt werden.

- Es werden 24 Passwörter vorgemerkt.

- Ein Passwortwechsel ist zwingend durchzuführen, wenn das Passwort einer anderen Person bekannt geworden ist.
- Die Passwörter der Benutzer müssen eine Mindestlänge von 8 Zeichen aufweisen.
- Die Einstellung „komplexe Passwörter“ ist gesetzt und muss dementsprechend erfüllt sein.
- Die Eingabe des Passwortes muss unbeobachtet stattfinden. Mitarbeiter werden aufgefordert, andere Mitarbeiter aktiv dazu hinzuweisen, bevor eine Passworteingabe erfolgt. Diese sind angewiesen, sich für den Zeitraum der Passworteingabe kurz wegzudrehen bzw. den Blick woanders hinzurichten.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Benutzerkennungen und -accounts werden nur für den Zeitraum eingerichtet, in dem sie tatsächlich benötigt werden.
- Die Anmelde-Fehlversuche sind auf maximal 5 begrenzt. Danach ist das System für 30min gesperrt. Die Fehlversuche werden protokolliert und das Protokoll wird stichprobenhaft ausgewertet.
- Aufgrund der möglichen 7x24h-Arbeitszeit ist eine zeitliche Begrenzung der Zugangsberechtigung als kontraproduktiv zu bewerten, weshalb darauf verzichtet wird.
- Eine Automatische Anmeldung (Auto-Login) ist nicht möglich. Die Arbeitsstationen und Terminals werden nach 5 min gesperrt. Ein Session-Timeout ist auf 30 Minuten gesetzt.

Erfolgskontrolle

Die Schulungs- und Erfolgskontrolle erfolgt in einer „Frontal“-Schulung nach aktuellem Schulungsplan.

Mitarbeiter von united cloud haben (wenn überhaupt) immer nur Zugriff auf die Kundendaten, die sie im Rahmen ihrer Tätigkeit gerade benötigen.

united cloud hat mit jedem Mitarbeiter eine schriftliche Vereinbarung über die sichergestellt wird, dass Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

2.3 Weitergabe Kontrolle

Definition:

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht von unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Beschreibung der Weitergabe Kontrolle:

Die Kundendaten werden nur innerhalb von united cloud verwendet und verarbeitet. Die Zugriffskontrolle ist wie zuvor beschrieben. Damit ist ein unbefugtes lesen, kopieren, verändern oder löschen der Daten ausgeschlossen. Die Weitergabe Kontrolle wird bei united cloud durch den einzigen Speicherort der Kunden- und Verwaltungsdaten im Rechenzentrum und die restriktive Zutritts- und Zugangskontrolle zu diesem Speicherort sichergestellt. Die Kundendaten werden (wenn überhaupt) nur in verschlüsselter Form nach außerhalb des Rechenzentrums übertragen oder in verschlüsselter Form außerhalb des Rechenzentrums gespeichert. Das Kennwort zur Entschlüsselung der Kundendaten ist nur den Mitgliedern der Geschäftsführung und leitenden Angestellten bekannt, so dass eine unberechtigte Weitergabe ausgeschlossen werden kann.

2.4 Eingabekontrolle

Definition:

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

Beschreibung der Eingabekontrolle:

Systemrelevante Vorgänge werden entsprechend der gängigen DV-Richtlinien protokolliert. Eine Überprüfung und Speicherung von Eingaben, Veränderungen bzw. Löschungen von Standard-Office-Anwendungen (Word-, Excel- oder PowerPoint-Dateien) erfolgt nicht. Der Zugriff auf sämtliche relevanten Daten und Verzeichnisse ist beim Absatz „Zugriffskontrolle“ beschrieben. Die Eingabekontrolle wird bei relevanten Daten über Protokolldateien gewährleistet. Die

Protokolldateien sind Textdateien und Teil der Kunden- bzw. Verwaltungsdaten. Sie sind nur nach Anmeldung auf dem Server im Rechenzentrum einsehbar. Ein Löschen der Daten durch Unbefugte ist aufgrund der existierenden Rechtevergabe ausgeschlossen.

2.5 Auftragskontrolle

Definition:

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle).

Beschreibung der Auftragskontrolle:

united cloud verwendet die zur Verfügung gestellten Daten ausschließlich im Rahmen der vertraglichen Vereinbarung. Eine weitere Nutzung insbesondere eine etwaige Nutzung im eigenen Interesse erfolgt nicht. Es existiert eine Arbeitsanweisung, dass nach Projektende solche Daten gelöscht werden müssen. Damit dieser Arbeitsschritt zuverlässig erfolgt, werden die Daten automatisiert in regelmäßigen Abständen gelöscht. Mit einem externen Dienstleister wurde ein Servicevertrag geschlossen, in dem diese Datenschutzmaßnahmen dokumentiert sind. Eine laufende Überprüfung durch einen Datenschutzbeauftragten findet statt.

2.6 Trennungskontrolle

Definition:

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Beschreibung der Trennungskontrolle:

Personenbezogenen Daten werden nur während der Projektabwicklung bei united cloud gespeichert. Die Löschung der personenbezogenen Daten erfolgt durch die Auftraggeber selbst oder nach deren Weisung. Bei einigen Server-Systemen werden die Daten mehrerer Kunden gleichzeitig auf einem Server verarbeitet. Zur Gewährleistung der getrennten Verarbeitung sind die Daten unterschiedlicher Kunden auf dem Server nach Verzeichnissen getrennt gespeichert, d.h. für jeden Kunden

existiert ein eigenes Verzeichnis, in dem nur die Daten dieses einen Kunden gespeichert sind. Für jeden Kunden existiert eine eigene Datenbank und ein eigener Betriebssystem-Prozess, in dem nur die Daten dieses einen Kunden verarbeitet werden. Daten unterschiedlicher Kunden werden nie gemeinsam in einem Betriebssystem-Prozess verarbeitet oder in einer gemeinsamen Datenbank verwaltet, sondern sind stets strikt getrennt.