Technisch Organisatorische Maßnahmen
Anlage 2

EWERK Medical Care GmbH

Brühl 24

04109 Leipzig

1. Revisionshistorie

Revision	Datum	Änderungen	Bearbeiter
V1	12.02.2018	Neuerstellung	EWERK
V 2	03.03.2021	Anpassungen BDSG	EWERK

2. Inhaltsverzeichnis

1

3. Technische und organisatorischen Maßnahmen

Über die Festlegung technischer und organisatorischer Maßnahmen (TOM) wird sichergestellt, dass nur berechtigte Personen Zutritt zu den Gebäuden bzw. Datenverarbeitungsanlagen haben. Diese können auf Wunsch vorgelegt und zu einem festen Vertragsbestandteil erklärt werden.

4. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Der Zutritt zu den Serverräumen in den Rechenzentren der EWERK Gruppe ist durch zwei verschiedene, unabhängige Zugangssysteme nur berechtigten Personen gestattet. Besuchern oder Dienstleistern ist der Aufenthalt in den Räumen nur unter Aufsicht einer zutrittsberechtigten Person gestattet. Zusätzlich sind die Räume im Rechenzentrum alarmgesichert und werden 24h videoüberwacht. Die Rechenzentren befinden sich auf einem rund um die Uhr bewachten Gelände.

Der Zutritt zu den Büroräumen der EWERK Gruppe ist ebenfalls durch ein Zugangssystem mit abgestuften Berechtigungen gesichert. So sind hier insbesondere Technikräume nur bestimmten Mitarbeitern zugänglich. Das Bürogebäude wird außerhalb der Arbeitszeit alarmgesichert und von einem Wachschutz überwacht. Der öffentliche Zugang zum Bürogebäude wird während der Geschäftszeiten durch eine Empfangsperson überwacht. Nebenzugänge, Tiefgaragenzufahrt und der öffentliche Zugang außerhalb der Geschäftszeit sind durch ein Zugangssystem gesichert. Für die Systeme gibt es entsprechende Berechtigungskonzepte mit abgestuften Administrationsrechten für die entsprechenden Aufgabengebiete. Die administrativen Tätigkeiten werden auf den Systemen protokolliert und können somit nachvollzogen werden. Bei der Einrichtung eines Zuganges erhält der Benutzer keine bzw. nur minimale Standardberechtigungen. Diese können nur über festgelegte Beantragungswege erweitert werden, wobei die jeweiligen Vorgesetzten bzw. Verantwortlichen ihre Zustimmung geben müssen. Besonders sensible Daten werden zudem revisionssicher und damit unveränderbar auf entsprechende Datenspeicher geschrieben.

5. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Alle Systeme und Anwendungen erfordern eine Authentifizierung zur Nutzung der Dienste. Je nach Sicherheitseinstufung des Systems gibt es bestimmte Anforderungen an die Passwortgüte, werden Passwortänderungen nach abgestuften Zeiträumen erzwungen und wird nach Mehrfachanmelden mit falschem Passwort das Benutzerkonto gesperrt, um Brute-Force-Attacken zu verhindern.

Zusätzlich sind die Systeme nur aus dem internen Netzwerk bzw. durch ein mehrfach abgesichertes Zugangsverfahren per VPN für berechtigte Mitarbeiter von außen erreichbar und auch von anderen Kunden durch Access Control-Listen an den Routern abgeschottet. Der Zugang zu externen Netzen wird zusätzlich durch Firewalls geschützt.

Weiterhin gibt es zur Erkennung von Angriffen ein Intrusion Detection System.

6. Zugriffskontrolle

Es ist zu gewährleisten, dass die Nutzungsberechtigten ausschließlich auf die ihrer Zugangsberechtigung 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.

Für die Systeme gibt es entsprechende Berechtigungskonzepte mit abgestuften Administrationsrechten für die entsprechenden Aufgabengebiete. Die administrativen Tätigkeiten werden auf den Systemen protokolliert und können somit nachvollzogen werden. Bei der Einrichtung eines Zuganges erhält der Benutzer keine bzw. nur minimale Standardberechtigungen. Diese können nur über festgelegte Beantragungswege erweitert werden, wobei die jeweiligen Vorgesetzten bzw. Verantwortlichen ihre Zustimmung geben müssen. Vergabe, Veränderung oder Entzug von Berechtigungen werden im Ticketsystem dokumentiert. Zu diesem Zweck existiert ein abgestuftes Rechte- und Rollenkonzept, welches den Zugang von Mitarbeitern auf Daten nach dem Need-to-know-Prinzip sicherstellt. Die Vergabe von Rechten bzw. Rollen erfolgt funktionsgetrennt durch 2 Abteilungen: organisatorische Vorgaben und Freigaben der beantragten Rechte sowie zyklische Überprüfungen der vergebenen Rechte durch die Complianceabteilung und die Umsetzung durch die operative Abteilung.

Besonders sensible Daten werden zudem revisionssicher und damit unveränderbar auf entsprechende Datenspeicher geschrieben.

7. Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht 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.

Datenübertragungen nach extern erfolgen nur über vertrauenswürdige Leitungen und Netze, welche ein Mitprotokollieren nicht ohne weiteres ermöglichen. Auch hier sind wieder Netzsegmente zusätzlich durch Access Control-Listen voneinander abgeschottet und das gesamte Netzwerk durch mehrstufige Firewall-Systeme abgesichert. Muss bei der Übertragung eine nicht vertrauenswürdige Datenleitung verwendet werden, so erfolgt die Übertragung verschlüsselt (z.B. über VPN). Zur Vernichtung von Datenträgern und Dokumenten mit sensiblen Daten wird eine entsprechende Fachfirma durch EWERK beauftragt.

Für Datenverbindungen zwischen den Rechenzentrumsstandorten der EWERK Gruppe werden Verschlüsselungstechnologien eingesetzt, darüber hinaus kommen dedizierte Leitungen zum Einsatz. Die Bereitstellung ist in der Leistungsvereinbarung mit dem Kunden vertraglich zu regeln.

8. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert und entfernt worden sind.

Eingabe, Änderungen und Löschung von Daten werden auf Systemen mit hoher Sicherheitseinstufung protokolliert, die entsprechen Logdateien revisionssicher auf einem zentralen Logserver persistiert. Dabei werden der Benutzername und der Änderungszeitpunkt erfasst.

9. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die Verarbeitung personenbezogener Daten im Auftrag der EWERK Gruppe oder durch Subdienstleister im Auftrag von EWERK erfolgt auf Grundlage schriftlicher Verträge mit besonderen Regelungen zur Einhaltung der Datenschutzvorschriften sowie stets entsprechend den Anweisungen des Auftraggebers. Die Einhaltung der Regelungen für die Auftragsdatenverarbeitung wird durch ein betriebliches Merkblatt und eine Mustervereinbarung zu §11 BDSG unterstützt. Zugleich werden regelmäßig alle Mitarbeiter auf das Datengeheimnis nach §5 BDSG verpflichtet. Stichprobenartige Kontrollen bei dem Auftragnehmer durch die datenverarbeitenden Bereiche sind möglich.

10. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die EWERK Gruppe unterhält ein Monitoringsystem, das unter anderem die Verfügbarkeit der Servicekomponenten überwacht.

Die Systeme verfügen über verschiedene Mechanismen, um Datenverlust zu vermeiden. Standardmäßig stehen die Festplatten in RAID-Gruppen redundant zur Verfügung. Somit führt ein Festplattenausfall nicht zu einem Datenverlust. Es stehen mehrstufige Backupmechanismen zur Verfügung.

Die konkrete Ausgestaltung des Backups ist im Leistungsvertrag zu vereinbaren. Dies betrifft insbesondere die Sicherungsart (Fullbackup, Inkrementelles Backup), Sicherungshäufigkeit (z.B. Uhrzeiten und Tage) sowie die Aufbewahrungsdauer der Datensicherung.

Weitere Maßnahmen zur Sicherung der Verfügbarkeit sind:

- redundante Hardware (von Infrastrukturelementen bis zu ganzen Servern)
- geclusterte Systeme
- redundante Netzanbindungen und Netzwerkinfrastruktur
- USV und Notstromversorgung
- Zwei Rechenzentren mit unterschiedlichen Brandabschnitten und entsprechender Aufteilung der Systeme
- Datensicherung an zweiten Standort
- Notfallkonzepte und Havarieplan

Auslagerung der mit dem Backup beschriebenen Medien im wöchentlichen Rhythmus in ein Bankschließfach.

11. Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Für unterschiedliche Zwecke erhobene Daten können in verschiedenen Systemen verarbeitet werden. Sensible Daten sind somit je nach dem entsprechenden Verarbeitungszweck auf unterschiedliche Systeme verteilt. Dabei gibt es Abstufungen von logischer Trennung auf unterschiedlichen Volumengruppen bis zu physikalischer Trennung über unterschiedliche Plattensysteme bzw. SAN-Storages. Darüber hinaus findet, wenn vom Kunden spezifiziert, eine Aufteilung der Systeme auf verschiedene VLANs statt.