Datenschutz- und Informationssicherheitskonzept für die Tagesklinik Margareten

Erstellt von: Paul Urtz

Erstellungsdatum: 17.03.2021

Erstellungsort: HTL Spengergasse

Erstellungsumstand: MIS PLF

Inhaltsverzeichnis

Einleitung

Im folgenden Dokument werden technische, sowie organisatorische Maßnahmen beschrieben, welche zur Sicherstellung des Informationssystems und der dazugehörigen patientenbezogenen Daten dienen. Anhand eines Datenschutz- und Informationssicherheitsmanagementsystems (DISMS) werden die gesetzten Maßnahmen mit einem Deming-Kreis (PDCA-Zyklus) festgehalten.

Datensicherung

Die Datensicherung (Redundanz) wird durch ein RAID 5 gewährleistet. Jeweils zwei der vier Festplatten sind in einem Rechnerraum untergebracht, sodass bei einer Beeinträchtigung jeder Art eines Raumes, die Daten physisch getrennt liegen und somit sicher sind. Zur weiteren Datensicherung wird dieses RAID 5 System gespiegelt und jeweils getaucht in den Rechnerräumen aufgebaut. Somit könne Updates auch installiert werden, ohne, dass Wartungszeiten entstehen, da immer ein System online bleiben kann.

Authentifizierung

Um verschiedene Funktionen nutzen zu können und Daten einsehen zu können muss ein Authentifizierungssystem mit jeweiligen Rollen gewährleiste sein. Dies dient zur Sicherung von Daten und Systemfunktionen.

Zur Authentifizierung wird eine 3 Faktorauthentifizierung eingesetzt. Diese besteht aus einem Benutzer + Passwort, einem Biometrischem Merkmal (Fingerprint) und einem Gegenstand, welchen man bei sich führt. In diesem Fall ist dies ein Smartphone. Möchte sich sein User authentifizieren so wird ihm nach der Eingabe des Benutzers + Passworts und des des Biometrischen Merkmals ein Einmalcode zugesandt, welchen er auf dem Gerät, auf dem er sich anmelden will, angeben muss.

Rollenvergabe

Je nach rollenvergabe hat die authentifizierte Person mehr oder weniger Rechte. Dies bezieht sich auf die Rechte Änderungen am System durchzuführen, Daten einzusehen oder zu verändern.

System-Admin: Änderungen am System

Behandelnder Arzt: Einsicht, Erstellung und Änderung patientenbezogener Daten

Behandelnde Schwester: Einsicht und Erstellung von patientenbezogenen Daten

Datenaustausch

Um den Datenaustausch über das Internet zu vermeiden, wird ein VPN eingerichtet, wodurch sich authentifizierte Personen direkt zum Netzwerk verbinden können und somit das Risiko einer Man in the Middel Attacke verringert wird.

Ausfallsregelung

Die Ausfallregelung betrifft das IT System der ganzen Datenschutz und Informationssystem der Tagesklinik Margareten. Dabei spielt die Art des Ausfalles eine wichtige Rollen.

Zuallererst muss abgeklärt werden welche Teile betroffen sind. Ist die Integrität, Verfügbarkeit oder Vertraulichkeit betroffen.

Sobald ein Fehler im System entdeckt wurde und Daten bzw. die Benutzbarkeit beeinträchtigt ist müssen Maßnahmen gesetzt werden.

SLA (Service Level Agreement)

- Gold: maximal 1h / Meldung an NIS-Behörde, wenn der Fehler oder Angriff nicht innerhalb von 3h behoben wurde
- Silber: 3h
- Bronze: 6h

Informieren der Behörde bei einem Data-Breach nach 72h.
Unverzügliches informieren der Behörde bei einem Unfall oder beinahe Unfall mit einem Medizinprodukt.

Ablauf eines Recoveryprogramms

Hierbei werden die einzelnen Systeme in verschiedene Securityklassen eingeteilt.

Klasse 1: Wesentliche Funktion des Systems mit Gefährdung patientenbezogener Daten. Integrität, Verfügbarkeit und Vertraulichkeit betroffen.

Klasse 2: Wesentliche Funktion des Systems mit Gefährdung nicht patientenbezogener Daten.

Klasse 3: Unwesentliche Funktion des Systems mit Gefährdung nicht patientenbezogener Daten

Meldungszeiten

Klasse 1: unverzüglich

Klasse 2: schnellstmöglich, max 20 Minuten nach Erkennung wenn wesentlichen Tätigkeiten zu erledigen sind.

Klasse 3: Innerhalb des jeweiligen Arbeitstages.

RPO (Recovery Point Objective)

Zeitraum zwischen 2 Datensicherungen

Klasse 1: eine Stunde

Klasse 2: 1 Tag

Klasse 3: 7 Tage

RTO (Recovery Time Obejctive)

Zeitpunkt des Schadens bis zur Wiederherstellung der vollkommenen Funktionalität des Systems

Klasse 1: eine Stunde

Klasse 2: drei Stunden

Klasse 3: ein Tag

Notfalleinrichtungen

Zu den Notfalleinrichtungen in der Tagesklinik Margareten zählen zwei Notstromaggregate. Der erste ist für die Versorgung der Intensivstation und der Operationssäle zuständig und hat eine unverzügliche Übernahme der Energieversorgung. In der Zeit zwischen Stromausfall und Übernahme des Notstromaggregats übernimmt ein Akku die Energieversorgung, welcher für mindestens 30 Minuten die vollständige Energieversorgung dieser Stationen übernehmen kann.

Das zweite Notstromaggregat für die restlichen Stationen hat eine Übernahmezeit der Energieversorgung von max. 10 Sekunden.