Datenschutz- und Informationssicherheitskonzeptes

für „Margaretner-Tagesklinik“

Dieses Dokument ist zuständig für die Beschreibung des Aufbaues, die Umsetzung und die Aufrechterhaltung der technischen und organisatorischen Maßnahmen durch ein Datenschutz- und Informationssicherheitsmanagementsystems für die „Margaretner-Tagesklinik“.

Erstellen eines Datenschutz- und Informationssicherheitskonzeptes

Es muss zur Erfüllung des NISG (= Netz- und Informationssicherheitsgesetz) und der DSVGO (=Datenschutz-Grundverordnung) organisatorische und technische Maßnahmen erfüllt und definiert werden.

organisatorische Maßnahmen:

Die Tagesklinik hat von Mo - Fr von 7:00 – 20:00 offen. Das heißt, dass aufgrund des SLA (= Service Level Agreement) die Reparatur innerhalb von 6h geschehen sein muss. Wenn nun zum Beispiel ein Fehler am Montag um 19:00 passiert, muss dieser bis Dienstag 13:00 behoben sein. Es gibt verschiedene Levels der SLA. So spaltet sich dieses in Gold, Silber und Bronze. Gold wird eingerufen, wenn ein schwerer Fehler die Arbeit stört. Hier muss nach 3h die Meldung an die NIS-Behörde abgegeben werden. Bei Silber ist es nach 4h und Bronze nach 6h.
Die Räumlichkeiten sind pro Ebene in fünf Brandabschnitte geteilt. Hier muss ein Feuernotfallplan erstellt werden, der immer aktualisiert werden muss, wenn es Änderungen im Fluchtweg gibt. Da die zwei Rechnerräume je einen eigenen Brandabschnitt haben muss hier ein separater Feuernotfallplan erstellt werden, jedoch gilt bei diesem auch, dass dieser kontinuierlich überprüft werden muss und ein Alerting abgegeben werden muss, wenn dieser geändert werden muss.
Zudem kommt eine interne Richtlinie dazu, die besagt, dass verschiedene Türen der Margaretner Tagesklinik, wie zum Beispiel für die zwei Rechnerräume zwischen 20:00 und 7:00 des nächsten Tages nicht betreten werden darf.
Um Daten sicher zu halten, sollte man diese verschlüsseln.

technische Maßnahmen:

Um das Netz und die Daten sicher zuhalten sollen auf den verwendeten Computern Antiviren-Programme raufgespielt werden. Bei diesem Antiviren-Programm sollte jedoch geachtet werden, dass es den Anforderungen der Sicherheit der Programme instand hält. Weiters ist es den normalen Anwendern (Mitarbeiter) nicht befugt, dieses zu deinstallieren. Um die Sicherheit noch mehr zu erhöhen, haben die eingegebenen Passwörter eine ein Jahr Gültigkeit. Die Passwörter müssen aus minimal 12 Buchstaben bestehen, eine Kombination aus Groß- und Kleinschreibung und Zeichen sein.
Da Chipkarten für die zwei Rechnerräume benutzt werden, werden die Chipkarten so umprogrammiert, dass diese in der entsprechenden Zeit den Zugang zu den Türen verhindern.
Falls es zu Homeoffice kommt, wird ein VPN verwendet. Um die Daten zuhause zu schützen, müssen die Mitarbeiter und Mitarbeiterinnen die Zwei-Faktor-Authentifizierung per Handy erfüllen. Sie melden sich im internen Netz an und es wird ein Token an Ihr Handy geschickt, den sie für den VPN eingeben müssen.
Um den Austausch von schutzwürdigen Informationen gewährleisten zu können, hält man sich an das TLP (= Traffic Light Protocol). Es wird in TLP: RED, TLP: AMBER, TLP: GREEN und TLP: WHITE geteilt. Bei Rot dürfen die Daten an Dritte nicht weitergegeben werden. Bei Stufe Amber dürfen die Daten in der eigenen Organisation weitergegeben werden. Bei Klasse Grün darf die Information an andere Organisationen innerhalb des Unternehmens weitergegeben werden. Letztlich bei White gibt es keine Einschränkungen und die Daten dürfen an jede Person ausgeschickt werden.

Da die Tagesklinik mit vielen verschiedenen Daten arbeitet, muss als aller erstes diese klassifiziert werden und die Kritikalität festgestellt werden. Kritische Daten sind personenbezogenen Daten und unternehmensinterne relevante Daten, die nicht personenbezogen sind, dennoch aber kritisch eingestuft werden.
Als erstes werden mögliche Risiken betrachtet. Wenn das Risiko von Datenmissbrauch hoch ist, muss wie oben genannt, Schutzmaßnahmen (= Antiviren-Programm) eingerichtet werden, die das Risiko minimieren oder gar auf null senken. Eine Maßnahme wäre, dass auf den Zugriffschutz geachtet werden soll. Hier stellt man sicher, dass nur berechtigte User durch Passwort oder Chip-Karte Zugriff auf bestimmte Dienste oder Services hat.
Das Team des Tagesklinikum Margareten sollte sich mindestens einmal im Monat treffen. Wenn jedoch Gefahr in Verzug ist, heißt, wenn ein Problem auftritt, dann muss das Risiko erkannt werden und Entscheidungen gefällt werden, ob dies ein Notfall ist oder keiner. Risiko muss per Grundschutzhandbuch bewertet werden und über die noch vorhandene Zeit muss entschieden werden. Wenn man noch genügend Zeit hat, greift man auf die organisatorischen und technischen Maßnahmen zurück. Diese können je Problem verändert und angepasst werden.

Dies führt uns somit zu verschiedenen Rollen. Es gibt 3 Rollen, die Administratoren, Anwender und Entwickler. Anwender dürfen die internen Anwendungsprogramme verwenden. Durch Zugriffschutz und Zutrittskontrollen wird sichergestellt, dass nur im System vermerkte User auf diese Programme zugreifen dürfen, oder, dass es Maßnahmen (Chip-Karte) gibt, die verhindern, unbefugte Personen den physikalischen Zutritt zu Datenverarbeitungsanlagen zu geben. Administratoren dürfen ihre Chipkarte ändern. Das heißt, dass diese auch in den oben genannten Zeiten in die Rechnerräume Eintritt haben. Entwickler sind äußert wichtig für die Software, die das Tagesklinikum Margareten verwendet.

Ausfallssicherheitskonzept für die „Margaretner-Tagesklinik“

Falls es zu einem Ausfall kommt, sollte man das Tagesklinikum separieren und diese in Prioritäten 1, 2 und 3 teilen. Das Tagesklinikum Margareten teilt man in medizinische Bereiche, Hausverwaltung und Administration.
Die Administration ist in diesem Fall Priorität 1. Bereiche, die auf Priorität 3 sind, können ausfallen, jedoch sollte die Patientenadministration hier nicht laufen. Dies gilt auch für die medizinischen Bereiche.

<u>organisatorische Maßnahmen:</u>
Um Datenverlust zu vermeiden sollte am besten nichts lokal gespeichert werden. Da die Daten bei einem Ausfall oder ähnlichem weg sein könnten. Wenn man einen Ausfall nicht beheben kann, haltet man sich wieder an das SLA.

<u>technische Maßnahmen:</u>
Um die Daten bestmöglich zu schützen, werden Storages verwendet. Hier kann man auch verhindern (Chipkarte), dass unbefugte Personen zu diesem Storage Befugnis erlangen. Die Ausfallsicherheiten sind wichtig, da oftmals die Zeiten, die in der SLA definiert worden sind, zu lange sind. Ein 3h Ausfall in einem Krankenhaus könnte schon eine Katastrophe werden.

Wenn ein wirklicher Notfall eintritt, muss die Kritikalität pro Segment in niedrig, mittel und hoch bestimmt werden. Wenn der Ausfall in maximal 3h nicht behoben wird, muss aufgrund NIS die NIS-Behörde nach 3h verständigt werden.

///Notfallmanager → überprüft
////melden wenn man Daten verliert

Wenn ein Ausfall des Stroms passiert, sollte es einen Notstromaggregrator geben, der das Tagesklinikum mit Strom versorgt. Es sollten Backups von Daten auf den Storages gemacht werden, falls es zu einer Hackerattacke kommt oder Datenverlust.

Wie oben genannt, muss man nach einem 3h Ausfall das NISG kontaktieren und diesen Vorfall melden. Falls Daten in falsche Hände geraten worden sind, muss dies der DSVGO bekannt gegeben werden.