Nachbesprechung 2. PLF Hoheiser

TIR 3 Logik

mit Prozentsatz nach TIR 3

Man muss alles beachten:

- Autor hinzufügen
- Rollenverteilung
- Punktuelle Anführung
- Mandantenfähigkeit, hier muss man organisatorische Dinge finden damit die getrennt sind nicht auch gleichzeitig auch admin sein

---

Dokumentenlenkung

Wichtig ob es einen der Klassen entspricht geheim/ intern/ öffentlich

internes Dokument → Dokument ist nur für die Mitarbeiter gedacht ist

öffentlich → ohne vereinbarung jeder kann darauf zugreifen

Entwurfsstadium, welches zuerst durch ein Grämium durchlaufen werden muss, damit es freigestellt wird

Wie wird das Dokument angewendet, wer darf es einsehen?

Wenn es noch im Entwurfsstadium ist kann es nicht öffentlich sein

Zeitraum festlegen von wann bis wann es gültig ist

Vorgangsweise - welche dinge müssen wo umgesetzt werden

Basissicherheit, welche bei allen Anzuwenden ist bzw. welche Besonderheiten es gibt

Mandantenfähigkeit, alle organisatorischen und rechtlichen Rahmenbedingungen so aufzusetzen das nur die Person zugreifen darf die die berechtigung dazu hat - unterschiedliche Berechtigungen sind durch berechtigungssysteme getrennt

Admin hat zwei Berechtigungen - 1 für die Klinik und 1 für das Radiologische Institut

Optionale wäre es: Gesamte Technik aus dem Verbund des Spitals rausnehmen und die Technik in eine eigene GesMBH geben, aber das geht nicht immer und war auch bei der plf keine möglichkeit

Trennung ist wichtig - Rollen und Berechtigungssystem

Rollenkonzept es sollte auch Notfallbeauftragte geben

Begriffsdefinition - Aufgabe der Person und Tätigkeit dokumentieren

z.B.: oben hinschreiben und unten dann den Ablauf und dann darauf referenzieren

Dokumentenlenkung und Begrifflichkeiten sind eben organisatorische Aufgaben, dient dazu das er nachschauen kann. Kann auch für Begriffe wie CIA Triade gemacht werden

Meldeprozess muss beschrieben werden, wer hat das Recht diese Meldung abzusetzen. Z.b.: nur der Notfallbeauftragte

3 Meldewege:

- Data Bridge Notification (prinzipell innerhalb von 72h verpflichtet; aber wenn die Rahmenbedinungen unangenehm sind und es bald droht rauszukommen dann früher)
    - Datenschutzmeldung
    - Datenschutzbeauftragte oder Notfallbeauftragte

    - z.b. hat den Datenschutzbeauftragten schon informiert oder ist mit ihm abgestimmt
    - Analyse der Situation, z.b einspielung der Software und jetzt passt das System nicht mehr

Wenn es mit der Software zusammenhängen kann

- Bundesamt für Sicherheit an das Gesundheitswesen - das Gefahr in Verzug ist
    - Bundesamt für Sicherheit an das Gesundheitswesen informieren (sofort melden!)
    - Nichts auf dem Gerät machen bis wir wissen was is - bzw. auf ein anderes Gerät umgeleitet
    - Frage wie bringen wir die Patienten dort rüber - das aufgabe der medizinischen abteilung
    - Weitere Vorgangsweise
- vlt spezialisten zu holen
- Systeme zu separieren bzw. vom restlichen Netz - zur Vorbeugung, und zur Fehlersuche zur Beweissicherung (wer ist in das System eingedrungen → forensik? -Beweissicherung)
- wer/ was/wie/wann macht
- was wäre wenn vorzusehen
- Dokument soll als checkliste dienen - wir gehen immer vom Worst-Case-Scenario aus

Wenn man einem Cyberangriff unterliegt

- CRP Melden

Prozesse:

PLAN

DO

ACT

CHECK

Bei einem Notfall gibt es eine Besonderheit - dieser Prozess den wir beschreiben

Notfall muss ausgerufen werden - es muss Mitgeteilt werden das es einen Notfall gibt

Nächste Woche Montag - schriftliche Leistungsüberprüfung mitmachen wer mag

bis spätestens Freitag → Mitarbeitsaufgabe ist auch machbar, da kann man eine verbesserte Variante abgeben und am Montag dann den Test aber nur eines der beiden verbessern

Kontinuierlicher Verbesserungsprozess basiert auch auf PDAC

Und schauen ob sich was geändert hat? bzw. ob sich ein Gesetz verändert hat.

Dokument regelmäßig überprüfen und dem Lenkungsausschuss vorgelegt, nachschauen gibt es eine änderung kommt etwas dazu, fällt etwas weg

Beschreibung des Prozesses muss es geben, wie kommt es zum Dokument

Dokument beschreibt wie sie bestimmte Sachen tun müssen

1. Betrifft das Dokuemnt
2. die Handlungsweise für die Person die es ausführt

Fehler:

- Dokumentenlenkung
- Nicht vorhandener Prozess fürs Ausrufen (Meldeprozess)
- Beschreibung des Systems (wie erreiche ich die Ausfallsicherheit - zwei Rechenzentren, Überbrückung durch ein zweites System, zweites externes Rechenzentrum, usw.)

2. Dokument

Zutritt und Zugriff

- Dokumentenlenkung gilt hier auch

- Klassifizierung der Räume, darf der Pat mitrein? TechnikRaum hat der Arzt auch nicht unbedingt was zu suchen
- Zutritt zu einem Technik Raum muss man auch externen Personen geben - mit regeln (darf nicht alleine rein, nur mit einem anderen Mitarbeiter, oder per Vertrag und mittels Vertrauen - sollte aber nachweisbar sein bsp. Mitarbeiterkarten)
- Schlüsselbuch wäre auch eine option - Portier
- Überwachung - wer war wann in welchem Raum - muss nachweisbar sein
- Berechtigungsystem mit Usern und ein log system → Rollen und Berechtigungskonzept
- Wer vergibt die Rollen? Das muss auch vergeben werden - zur Berechtigungsvergabe
- Wie dokumentiert man die Rollen → log system
- Kontrolle ist wichtig - Beschreibung das in Regelmäßigen oder unregelmäßigen Zyklen die Zutritt oder Zugriffs oder authentifizierung kontrollieren - kann zb. der Datenschutzbeauftragte machen, weil der ein jourist ist
- Wer hat zu welchen dings zugriff um das system aufrecht zu halten