Datenschutz- und Informationsicherheitskonzept

Vorgangsweise

Um sicherzustellen, dass Daten- und Informationssicherheit gewährleistet sind, muss überlegt werden, wer auf welche Daten zugreifen darf und wer nicht. Sobald das geklärt ist, wird überlegt, wie man das technisch umsetzen kann. Nach dem die Technische Umsetzung erledigt ist, wird regelmäßig überprüft, ob auch alles ordnungsgemäß funktioniert. Sollte das nicht der Fall sein, wird überlegt, wie die Fehler behoben werden können, dann werden diese Überlegungen umgesetzt und alles erneut überprüft. Dieser Zyklus wird kontinuierlich wiederholt.

Konzept

Es wird ein Windows Server aufgesetzt und jeweils eine Domäne für die Nephrologie und für die Diabetologie erstellt. Allen Geräten werden Adressen in ihrer entsprechenden Domäne zugewiesen. Zudem wird ein APIS installiert worauf alle Rechner innerhalb der Domäne Zugriff haben.

Alle MitarbeiterInnen erhalten Accounts, die regeln worauf zugegriffen werden kann.

- EmpfangsmitarbeiterInnen können auf die Stammdaten der Patienten (Name, Geburtsdatum, Adresse, Versicherung) einsehen und wenn nötig ändern bzw. neue Datensätze anlegen, wenn ein Patient zum ersten Mal in die Tagesklinik kommt. Zusätzlich können sie neue Termine für die Patienten anlegen bzw. bei einer Absage wieder löschen und alle bereits eingetragenen Termine einsehen. Außerdem können sie den Dienstplan aller Mitarbeiter einsehen, jedoch nicht verändern.

- ÄrztInnen haben auf alles Zugriff, worauf auch das Empfangspersonal Zugriff hat. Zusätzlich können sie gespeicherte Befunde der Patienten einsehen und neue verfassen, jedoch nur von jenen, die sie selbst behandeln, bzw. in der Vergangenheit behandelt haben.

- AdministratorInnen haben auf alles Zugriff, worauf auch ÄrztInnen Zugriff haben. Zusätzlich können sie neue Accounts für Personal anlegen und bereits vorhandene löschen, sowie die Berechtigungen ändern. Außerdem können sie Geräte einer Domäne zuweisen bzw. aus der Domäne löschen.

Um einen Zugriff außer Haus zu ermöglichen wird eine VPN-Verbindung verwendet. MitarbeiterInnen können sich mit ihren Accounts anmelden. Über SMS erhalten sie dann einen sechsstelligen Zahlencode, den sie zur Authentifizierung eingeben müssen.

Ausfallsicherheitskonzept

Vorgangsweise

Um die Sicherheit im Falle eines Notfalls gewährleisten zu können, muss zuerst überlegt werden welche Gründe es für einen möglichen Ausfall gibt (z.B. Stromausfall, Brand, Hackerangriff). Danach muss für jeden dieser Gründe ein Konzept erstellt werden, wie man einerseits den Normalzustand schnellstmöglich wiederherstellen kann und andererseits den Schaden, sowohl an Menschen, Geräten und Daten, so gering wie möglich hält. Danach werden diese Überlegungen technisch umgesetzt und mittels Probealarmen regelmäßig überprüft. Sollte etwas nicht so funktionieren wie gewünscht, oder neue Probleme auftreten, die anfangs nicht bedacht wurden, wird überlegt, wie man diese Mängel beheben kann. Dann werden diese Überlegungen erneut technisch umgesetzt und wieder regelmäßig getestet. Dieser Zyklus wird kontinuierlich wiederholt.

Konzept

- Brandfall:
  Alle Räume werden mit Rauchmeldern und Sprinklern ausgestattet. Alle Brandabschnitte sind mit Brandschutztüren voneinander abgegrenzt und haben ein separates Brandschutzsystem.
  Im Ernstfall werden umgehend Feuerwehr und Rettung verständigt und alle Patienten und MitarbeiterInnen aus dem Haus befördert.

- Stromausfall:

  Für jeden Brandabschnitt wird eine eigener Notstromgenerator installiert, der im Falle eines Stromausfalls, für die Stromversorgung der Therapiegeräte zuständig ist. Außerdem werden alle Therapiegeräte mit einer Batterie ausgestattet, die dafür sorgt, dass sie auch in der Zeit zwischen Beginn des Stromausfalls und laufendem Notstromgenerator mit Strom versorgt werden.

- Hackerangriff:
  Das System wird von der Außenwelt abgetrennt, d.h. kein Internetzugriff mehr und Verbindungen über VPN sind auch nicht mehr möglich. Dann wird nach der Schwachstelle gesucht die sich der Hacker zu nutzen gemacht hat. Sobald diese gefunden und behoben wurde, wird der Normalbetrieb wieder hergestellt. Sollte Verdacht auf Datendiebstahl, bzw. Datenmanipulation bestehen, wird umgehend die verantwortliche Behörde informiert.