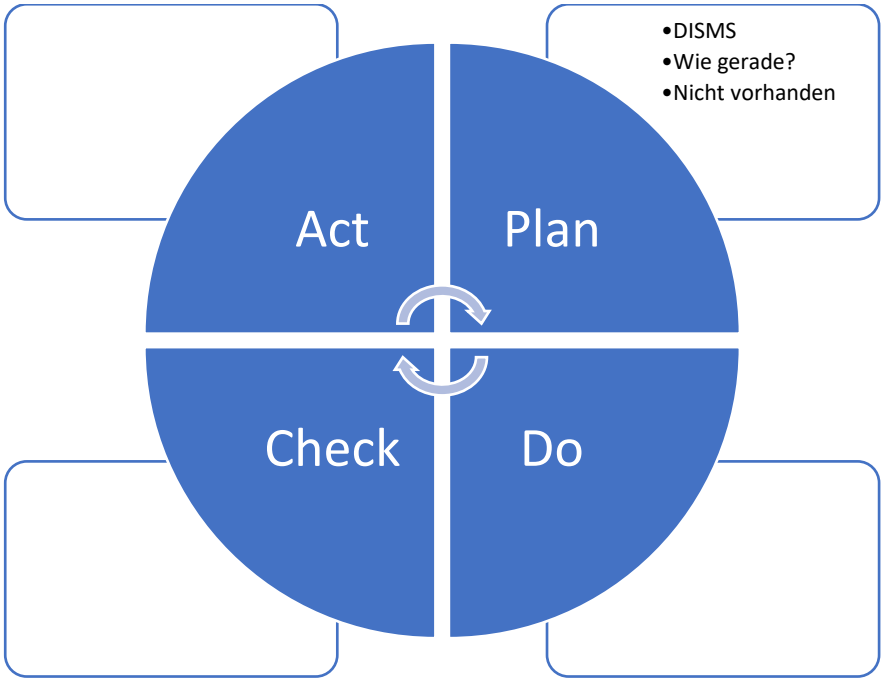
Datenschutz- und Informationssicherheitskonzept



Vorgangsweise

Zuallererst muss sich das derzeitige System der Margaretner-Tagesklinik angesehen werden. Dabei wird mit der Hardware und Infrastruktur begonnen, dann die verwendete Software und Konfiguration näher betrachtet und am Ende die Nutzung durch das Personal analysiert.

Hardware

Angefangen wird in den beiden Rechenräumen. Es wird auf die Brandsicherheit und andere Maßnahmen gegen Umweltrisiken wie Überschwemmungen geachtet. Auch wird die Stromversorgung genauer betrachtet, ob die Zeit zwischen Ausfall und Notstrom überbrückt werden kann.

Im weiteren Verlauf wird die Netzwerkinfrastruktur begutachtet. Welche Kabel wurden/werden verwendet, wie sieht es mit der Abschirmung aus und wer kann sich an das Netzwerk anschließen (z.B. durch Lanports, ab steckbare LAN-Kabel, WLAN, …).

Zuletzt werden sich die Endgeräte angesehen. Wo stehen sie? Wer hat frei Sicht oder Zugriff auf diese? Befinden sich eventuell Authentifizierungsdaten notiert in unmittelbarer Nähe? Sind die Geräte noch auf dem aktuellen Stand der Technik und vollständig in Takt?

Software

Bei der Software sollen sich grundlegend die Versionen angesehen werden, ob sie möglicherweise veraltet und unsicher sind und aktualisiert oder geändert werden sollten. Des Weiteren soll sich die Netzwerkkonfiguration angeschaut werden. Gibt es mehrere Netzwerke? Wer kann auf welchem Netzwerk was machen und wo zugreifen? Zu guter Letzt muss die allgemeine Konfiguration der Programme begutachtet werden. Werden unwissentlich Daten an Dritte geschickt? Wer hat welche Zugriffe und Rechte?

Personal und Umfeld

Wie und wo sind die Endgeräte platziert? Wird der Druckerraum im zugeschlossen oder ist das Schloss kaputt? Kann sich ein Patient hinter den Arzt stellen und die Daten abfotografieren, sich die tippreihenfolge des Passworts merken, …?

Versteckte Stichproben beim Personal sollten durchgeführt werden, die einerseits die oberen Fragen beantworten, andererseits Leute oder Familienmitglieder damit beauftragt werden zu versuchen das Passwort oder andere vertrauliche Infos durch social Engineering herauszufinden.

Sind alle drei Hauptpunkte durchgeführt, müssen nach der Umsetzung alle Maßnahmen erneut überprüft werden und Mängel wieder umgesetzt und überprüft werden. Dieser Kreislauf wird so lange durchgeführt, bis der Datenschutz und die Informationssicherheit gewährleistet ist.

Sicherheitsrichtlinien

Im Folgenden wird ein Rollenmodell definiert. Dabei sind die medizinischen Rollen in intern und extern gegliedert. Dabei steht intern für eine Arbeit im Netzwerk der Klinik vor Ort und extern für eine Arbeit außerhalb der Klinik.

Rollenname	Zugriffsrechte	Anwendungen	Ort
Administrator	Alle Rechte	Alle Anwendungen	Nur intern auf stationären Endgeräten ohne Einsicht von Dritten
Arzt	Lesen Erstellen Bearbeiten	Dokumentationsprogramme Medizinische Geräte KIS ausgenommen Finanz Fehlermeldesystem	Behandlungszimmer Anmeldeschalter Arztzimmer
Krankenpfleger	Lesen Erstellen* *neue Werte, keine Bearbeitung, keine Arztbriefe, keine Diagnosen	Medizinische Geräte KIS ausgenommen Finanz Fehlermeldesystem	Behandlungszimmer Anmeldeschalter
Haustechnik	Lesen Erstellen Bearbeiten	Fehlermeldesystem	Intern und extern
Verwaltung	Lesen Erstellen Bearbeiten	KIS ausgenommen Ärztliche Befunde, Akten, … Fehlermeldesystem	Intern und extern
Arzt extern	Lesen Bearbeiten	Dokumentationsprogramme KIS ausgenommen Finanz	extern
Krankenpfleger extern	Lesen Bearbeiten	KIS ausgenommen Finanz	extern

Im weiteren Verlaufen wird die Authentifizierung der einzelnen Rollen thematisiert

Rolle	Authentifizierungsmethoden
Administrator	Username Passwort (min. 10 Zeichen, Symbole, Zahlen, groß/klein Buchstaben, regelmäßiger Wechsel) 3x Sicherheitsfragen Biometrisch (3x Fingerabdrücke)
Arzt	Username

	Passwort (min. 10 Zeichen, Symbole, Zahlen, groß/klein Buchstaben, regelmäßiger Wechsel)
Krankenpfleger	Username Passwort (min. 10 Zeichen, Symbole, Zahlen, groß/klein Buchstaben, regelmäßiger Wechsel)
Haustechnik	Username Passwort (min. 10 Zeichen, Symbole, Zahlen, groß/klein Buchstaben)
Verwaltung	Username Passwort (min. 10 Zeichen, Symbole, Zahlen, groß/klein Buchstaben)
Arzt extern	Username Passwort (min. 10 Zeichen, Symbole, Zahlen, groß/klein Buchstaben, regelmäßiger Wechsel) Authenticationkey*
Krankenpfleger extern	Username Passwort (min. 10 Zeichen, Symbole, Zahlen, groß/klein Buchstaben, regelmäßiger Wechsel) Authenticationkey*

*Authenticationkey: Hierbei handelt es sich um einen Schlüssel, welcher für den externen Zugriff benötigt wird. Dieser Schlüssel muss unter der Woche täglich, für das Wochenende am Freitag durch anstecken an einen internen PC neu generiert werden.

Ausfallssicherheitskonzept

Vorgangsweise

Zuallererst werden anhand von Plänen und Rundgängen alle potentiellen Gefahren, ohne Berücksichtigung der derzeitigen Sicherheitsmaßnahmen, beachtet. Im Folgenden werden die Schutzmaßnahmen für die jeweiligen Gefahren berücksichtigt und begutachtet, ob diese ausreichend sind oder nicht.

Im weiteren Verlauf wird ein besonderes Augenmerk auf Notfälle gesetzt. Hierbei wird der bereits oben beschriebene Prozess durchlaufen. Darüber hinaus werden aktiv Tests und Übungen durchgeführt, um Fehlerquellen zu analysieren und die Reaktion der Mitarbeiter bei Notfällen zu erkennen. Anlagen wie Feueralarm, Schleusen und Türen werden wiederholt auf ihre Funktionalität überprüft.

Alle erkannten potenziellen Fehler, Gefahren, Notfälle und Mängel werden daraufhin in folgende 3 Klassen geteilt:

- **Bronze**: Unwichtige Mängel, Gefährdeten keinerlei Daten oder Leben
- **Silber**: Stellen eine potenzielle Gefährdung von vertraulichen Daten oder Leben dar
- **Gold**: Stellen eine Gefährdung von vertraulichen Daten oder Leben dar oder entsprechen nicht den Vorgaben der DSGVO oder NISG. Müssen in jedem Fall beim Entdecken dem Computer-Notfallteam gemeldet werden.

Mängel, Gefahren, Probleme oder Fehler welche während der Begutachtung aufgetreten sind, müssen gänzlich abhängig der Klassifizierung gemeldet und behoben werden. Zukünftig auftretende Mängel müssen ebenfalls beim Auffinden/Melden klassifiziert und behoben werden. Notfälle müssen nach dem folgenden Schema behandelt werden:

Notfall

Unter Notfall zählt eine akute, plötzlich aufgetretene Verletzung von Gesetzen bzw. eine nicht gewährleistete Vertraulichkeit, Verfügbarkeit oder Integrität sensibler Daten oder eine Gefährdung von Leib und Leben durch Defekte, Brände oder ähnliches.

Tritt so ein Notfall auf muss sofort ein Notfallmeldung über das Fehlermeldesystem erfolgen, sollte dies durch Einrichtungen wie Brandmelder ohnehin nicht schon geschehen sein. Danach werden Notfallpläne durch das verantwortliche Personal ausgeführt und überwacht.

Ist eine direkte Meldung nach Gesetz möglich, hat diese sofort zu erfolgen!

Notfallversorgung

Die Tagesklinik hat zwei Haupteinrichtungen für Notfälle. Einerseits das Brandmeldesystem und Andererseits System bei Stromausfällen.

Bei einem Brand werden alle Brandabschnitte durch Türen und Schleusen automatisch geschlossen. Im gleichen Moment kommt es zum Brandalarm und einer automatischen Meldung an die Feuerwehr.

Bei einem Stromausfall läuft die IT, vor allem die Rechner und alle notwendigen Medizingeräte ununterbrochen aufgrund von Akkus weiter, bis der Dieselgenerator die Arbeit für 24h übernehmen kann.