2 Informationssicherheitsmanagementsystem (ISMS)

2.1 Der Informationssicherheitsmanagementprozess

Um die zentralen Aufgaben des ISMS zu behandeln:

- die Entwicklung einer organisationsweiten Informationssicherheitspolitik
- die Durchführung einer Risikoanalyse
- die Erstellung eines Sicherheitskonzeptes
- die Umsetzung der Sicherheitsmaßnahmen
- die Gewährleistung der Informationssicherheit im laufenden Betrieb
- die kontinuierliche Überwachung und Verbesserung des ISMS

muss das Spenger Spital in verschiedene Bereiche unterteilt werden. Wir ziehen jede Abteilung separat heran und betrachten diese Aspekte auch dementsprechend. Jedoch wird Abteilungsübergreifend Rücksprachen mit den Leitern und den Primaren gehalten.

2.1.1 Entwicklung einer organisationsweiten Informationssicherheitspolitik

Hier werden definiert:

- Was ist zu schützen?
- Strategien, um Daten zu schützen
- Fehlermeldewege

Was ist zu schützen?

Zu schützen sind all jene Daten welche Rückschlüsse auf Patienten, Personal oder Besucher schließen lassen. Sie sind mit höchster Sorgfalt zu behandeln und es gilt diese unter allen Umständen zu wahren.

Strategien, um Daten zu schützen:

Die einzelnen Strategien werden nach Abteilung und Gefährdung der Daten definiert. Jedoch herrscht überall ein Grundschutz welcher gegeben falls angepasst wird.

Fehlermeldewege

Fehlermeldewege sind ein essentieller Bestandteil der Datensicherheit. Bemerkt ein Mitarbeiter oder eine Mitarbeiterin einen Fehler in einem System oder einen Virus auf ihrem Endgerät wird dies in folgender Reihenfolge gemeldet:

IT-Abteilung → nächster Vorsitzender → Leiter/in der Abteilung → KH Leitung

2.1.2 Risikoanalyse

Grundschutz:

Wir definieren einen Grundschutz, welcher bei JEDEM IT-System umgesetzt werden muss. Unser Grundschutz beinhaltet:

- Für alle Endgeräte einen Antivirus Schutz
- Jedes Netzwerk muss min. eine Firewall beinhalten.
- Jedes System arbeitet mit Rollen, welche von der IT vergeben werden.

2.2 Erstellung eines Sicherheitskonzeptes

Maßnahmen werden vom IT-Personal in Zusammenarbeit mit der KH Leitung erstellt. Außerdem muss eine Liste bereitstehen welche mögliche Risiken angibt, die trotz Maßnahmen anfallen können.

Die vergabe verschiedener Rollen werden durch die IT geregelt. Diese werden auf eine Chipkarte gespeichert, welche dann bei verschiedenen Kartenleser angehalten werden kann.

Firewall vergabe geschieht außerdem durch die IT und wird bei Verwaltungsprogrammen und Laborendgeräten erhöht.

Wir kombinieren den Grundschutz mit einem erweiterten Schutz. Für CT, MRT und derartige Endgeräte MUSS der Antivirenschutz des Herstellers angewendet werden.

2.3 Umsetzung des Informationssicherheitsplans

Schritt 1: Implementierung der Sicherheitsmaßnahmen

Für die Installation der Firewalls und Antivirus Programme erfolgt durch das IT-Personal.

Die Rollenverteilung geschieht in Zusammenarbeit von IT mit Verwaltungspersonal.

Schritt 2: Testplan und Tests

Für die Programme müssen wöchentliche Modultests durchgeführt werden. Diese erfolgen Automatisiert. Die Endgeräte werden auf ihre Funktionsfähigkeit von einem internen Techniker kontrolliert 1-mal im Monat.

Hierzu wird es ein Testprotokoll geben, welches von jedem Techniker auszufüllen ist.

Schritt 3: Prüfung der Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking)

Um die gesetzten Maßnahmen zu kontrollieren, werden unangekündigte Tests durchgeführt. Diese werden durch die Krankenhaus Leitung angeordnet. Die Ergebnisse des Tests müssen herangezogen werden, um möglicherweise neue Maßnahmen zu setzen (Schulungen, andere Programme, Firewalls)

Alle Mitarbeiter müssen zu jedem Zeitpunkt wissen welche Maßnahmen gesetzt sind und sind verpflichtend zu laufenden Schulungen zu gehen. Diese werden von externen Firmen oder dem internen IT-Personal geleitet.

2.3.4 Akkreditierung

Hierzu wird eine externe Firma herangezogen, um die Sicherheit der Daten in dem laufenden Betrieb zu überprüfen. Hierzu werden Dokumente und Protokolle geschrieben welche den Zustand der Sicherheit zu beschreiben. Im Anschluss wird eine Zertifizierung angestrebt.

2.4 Informationssicherheit im laufenden Betrieb

2.4.1 Aufrechterhaltung des erreichten Sicherheitsniveaus

Monitoring muss durchgehend durchgeführt werden. Durch Tests wird die Sicherheit andauernd sichergestellt. Die Verantwortlichen Personen wurden im obigen Punkt schon definiert.

2.4.2 Wartung und administrativer Support von Sicherheitseinrichtungen

Zu Wartung zählen Backups, welche im Sohn-Vater-Großvater Prinzip erstellt werden. Das Einspielen von Backups in einer virtuellen Maschine ist empfehlenswert, um diese auf Viren zu überprüfen.

Zu den Backups gehören auch technische Protokolle und die Protokolle der durchgeführten Tests.

Die Wartung erfolgt durch Firmeneigene Techniker.

2.4.3 Überprüfung von Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking)

Dies ist im obigen Punkt Schritt 3 beschrieben.

2.4.4 Fortlaufende Überwachung der IT-Systeme (Monitoring)

Um den Betrieb so sicher wie möglich zu halten, wird ein Monitoring empfohlen welchen wie oben beschrieben durchgeführt werden soll.

Welche Punkte noch?

7.1.7 Clear-Desk-Policy

So wird gewährleistet das in Abwesenheit einzelner Personen niemand zu Informationen gelangt, an die er nicht kommen darf. So ist nicht nur die IT-Sicherheit, sondern auch die analoge Sicherheit gewährleistet.

14.2 Evaluierung und Zertifizierung

Mit einer Zertifizierung kann sichergegangen werden, dass die Maßnahmen funktionieren.

17 Disaster Recovery und Business Continuity

So besteht im Unternehmen ein Plan wie der Betrieb schnellstmöglich wieder aufgenommen werden kann und wie man in diesen Situationen reagiert. (Gesetzlich Vorgeschrieben)