ISMED - Datenschutz- und Informationssicherheitskonzept

Dieses Dokument ist ein Datenschutz- und Informationskonzept der Firma ISMED. Kernelemente beziehen sich dabei auf das Konzept (den Aufbau, die Umsetzung und Aufrechterhaltung) der technischen und organisatorischen Maßnahmen durch ein Datenschutz- und Informationssicherheitssystem. Außerdem wird die Vorgehensweise von Notfallrichtlinien beschrieben.

Prozess der Sicherheitslinien

Es ist wichtig, dass technischen Maßnahmen in einer Organisation überprüft werden:

Organisatorische Maßnahme: Wie soll ein sicherer Datenverkehr gewährleistet sein?
Technische Maßnahme: Nutzung von Sicherheitszertifikaten

Ein PDCA-Zyklus sorgt für das Qualitätsmanagement:

P: Plan = Planung von Maßnahmen, die ein Risiko minimieren sollen (organisatorisch)
D: Do = Durchführung der geplanten Maßnahme (organisatorisch/technisch)
C: Check = Wurde durch die Maßnahme das Risiko minimiert?
A: Act = Reaktion auf das Ergebnis aus der Check-Phase

Um die Sicherheitsrichtlinien zu erstellen, umsetzen, überprüfen und verbessern sollen sie in einem PDCA-Zyklus laufen. Ohne regelmäßige Überprüfung ist die Wirksamkeit der organisatorischen und technischen Schutzmaßnahmen auf Dauer nicht sichergestellt.

Die Dokumentation trägt dazu bei, den Sicherheitsprozess und getroffene Entscheidungen nachvollziehbar zu gestalten und Missverständnisse zu vermeiden. Diese soll in elektronischer Form archiviert werden, um bei Bedarf schnell verfügbar zu sein.

Diese Daten dürfen nicht für jeden verfügbar sein. Es soll das Traffic Light Protocol gelten welches für die Weitergabe der sensiblen Datenentscheidet. Dieses soll nach vier verschiedenen Farben Aussage haben, an wen schutzwürdige Informationen weitergeleitet werden dürfen. Durch einen Klassifizierungsvermerk kann jeder Mitarbeiter unmittelbar erkennen, wie er mit den eingestuften Informationen umzugehen hat.

ROT: Weitergabe an Dritte ist verboten
GELB: Nur notwendige Daten werden weitergegeben
GRÜN: Weitergabe an andere medizinische Organisationen
WEIß: Öffentliche Weitergabe

Die Rollen bestehen aus dem Administrator, medizinischen Personal, technisches Personal und Verwaltungspersonal. Jeder Mitarbeiter hat beschränkte Zugriffsrechte. Der Verlauf wird dokumentiert und aufgezeichnet. Der Zugriff erfolgt anhand biometrischer Identifizierung mit einem Fingerabdruck und zusätzlicher Zwei-Faktorautorisierung.

Der Administrator am Systemprogramm ist der Leiter, welcher Zugriffe erlauben und verweigern kann. Das medizinische Personal darf nur Informationen von den behandelnden Patienten einsehen. Die Weitergabe ist strengstens verboten. Das technische Personal kann keine medizinischen Daten einsehen, sondern nur das Systemprogramm und einige Anwendungsprogramm steuern. Das Verwaltungspersonal hat nur Zugriff auf wenige Anwendungsprogramme, welche für die Verwaltung notwendig sind. Alle Bereiche sind separiert.

Damit Geräte und Daten das Gebäude nicht verlassen wird anhand GPS-Daten geregelt, wo das Gerät sich befindet. Sobald es einen Radius verlässt wird jeglicher Zugriff verweigert. Eine Information wird an den Administrator weitergeleitet. Externe Festplatten werden unverzüglich vom Gerät erkannt und das System wird gesperrt. Diese Daten sind nicht lokal gespeichert, sondern in einer gesicherten Server-Farm im Rechenzentrum. Bei Netzwerk Ausfall soll keiner der Mitarbeiter arbeiten. Diese werden in diesem Fall benachrichtigt, um wichtige Daten nicht zu verlieren.

Die Korrektheit und Stabilität der Maßnahmen und Abweichungen soll in Quartalsabständen überprüft werden.

Prozess der Sicherheitslinien

Bei einem Sicherheitsvorfall ist das Computer-Notfallteam zu verständigen.

Dieses unterscheidet zwischen technischen und Organisatorischen Maßnahmen. Anhand der CIA-Triade erfolgt eine Risikoanalyse.

Verfügbarkeit, Vertraulichkeit und Integrität sind sehr wichtig. Alle Daten müssen vertraulich behandelt werden. Außerdem sollen sie immer verfügbar sein und dürfen nicht manipuliert werden.

Bei einem Sicherheitsvorfall muss eine Risikoanalyse geschehen.
➔ alle Objekte identifizieren, die wir betrachten wollen
➔ Bedrohungen überlegen
➔ Risikoanalyse: wie oft könnte die Bedrohung eintreten & welche Kosten benötigt sie?
➔ Kosten = Kosten der Wiederaufnahme, Kontrolle, Herstellung
➔ so viele Dinge wie möglich im Vorfeld abhalten
➔ Schaden der passieren könnte und Vorbeugungen gegenüberstellen

Diese Risikoanalyse basiert auf den PCDA-Kreislauf. Die Bedrohungen und ihre Wirkung werden analysiert. Auswirkungen sind zu bedenken und möglichst klein zu halten. Der Kreislauf sollte wiederholt werden, bis das Problem gelöst ist. Die Maßnahmen können nicht ganz gesehen, sollen aber protokolliert werden. Auch das geschieht digital, um auf ältere Vorfälle zurückgreifen zu können.

Meldeprozess nach dem NISG und der DSGVO:

Wenn nach der DSGVO personenbezogene Daten verletzt wurden ist eine Meldepflicht binnen 72 Stunden zu tätigen. Bei einem Sicherheitsvorfall ist nach NISG eine Meldepflicht binnen 3h zu tätigen. Laut dem Medizinproduktegesetz ist bei Fehlfunktionen, Änderungen oder Mängel eine sofortige Meldepflicht notwendig. Dieselbe Richtlinie gilt für Beeinflussungen und Qualitätsmangel.

Die Meldezeit gilt dabei innerhalb der Arbeitszeit. Die Arbeitszeiten sind Montag bis Freitag von 7:00 bis 20:00. Wenn die Störung kurz vor 20:00 geschieht, ist ab dem nächsten Tag die übrige Zeit der Meldepflicht gültig. Außerhalb der Arbeitszeiten hat die Zeit der Meldepflicht keine Gültigkeit.