Inhalt

1 Zweck und Anwendungsbereich

Dieses Dokument beschreibt die technischen, sowie organisatorischen Maßnahmen, welche zur Sicherstellung der Informationssicherheit und Datenschutz dienen. Anhand eines Datenschutz- und Informationssicherheitsmanagementsystems (DISMS) werden die gesetzten Maßnahmen mit einem Deming-Kreis (PDCA-Zyklus) festgehalten. Um das Sicherheitsniveau möglichst hochzuhalten, ist es nötig, dass das Dokument in der gesamten Unternehmensstruktur gilt und ohne Ausnahme befolgt werden muss. Das Dokument basiert auf die rechtlichen Gegebenheiten des österreichischen Gesetzesrahmen.

2 Grundlagen

Da das Projekt im gesundheitlichen Sektor angesiedelt ist und es um den Schutz von Patientendaten geht, ist es wichtig, dass hierbei die DSGVO sowie das NISG in Kraft tritt. Es wird verlangt das Sicherheitskonzept für die Praxis nach aktuellen Standards und unter Einhaltung von entsprechenden Normen zu implementieren, um das Sicherheitsniveau möglichst hochzuhalten.

3 Vorgehensweise Informationssicherheitskonzept

3.1 Organisatorische Maßnahmen

Um den Prozess durchzuführen und zu überwachen wird ein Team von 4 Personen erstellt. 2 von der Firma HEALTHSYS und 2 Fachkräft der Tagesklinik. Bei Normalbetrieb trifft sich das Team 2-mal im Monat, also alle 2 Wochen. Das Team arbeitet nach dem PDCA-Zyklus:

- Plan: TOMs planen
- Do: Geplantes Vorgehen durchführen
- Check: Fortschritt überprüfen
- Act: Fehlerbehebung, Verbesserung

Das heißt, sie prüfen auf mögliche Bedrohungen und Gefährdungen und planen folglich passende Maßnahmen zur Risikominimierung. Auch werden jeweils Risikoanalysen nach dem Österreichischen Informationssicherheitshandbuch gemacht. Anschließend werden die neu geplanten Maßnahmen zur Reduktion der Risiken in der Organisation dokumentiert, umgesetzt und die Mitarbeiter werden darüber informiert.

Zur Sicherung der IT-Infrastruktur muss auch ein IT-Team nach PDCA arbeiten, um sie möglichst gut zu verbessern. Dabei wird besonders der Datenschutz nach DSGV und das NISG vollständig beachtet. Ziel ist dabei immer die Optimierung des Niveaus der CIA-Triade. Der IT-Leiter ist dabei verantwortlich, dass die beschlossenen Maßnahmen eingehalten werden und Prozess und die Planung ordnungsgemäß abläuft.

3.2 Technische Maßnahmen

Die Anwendungsprogramme werden nach Auswirkung bei Datenleak eingeteilt.

- **Kritisch (Rot)**: Das Programm enthält Informationen, die streng geheim sind. Beispiel sind Patientenbezogene Daten und Mitarbeiterinformationen. Diese Anwendungen sind streng zu schützen und dürfen nur von autorisierten Personen benutzt werden
- **Hoch (Gelb)**: Das Programm arbeitet mit Informationen, die innerhalb der Organisation an Personen, die es wissen dürfen, weitergegeben werden. Es wird das „Need-to-know“ Prinzip angewandt
- **Niedrig (Grün)**: Die Anwendung arbeitet mit Informationen, welche an jeden innerhalb der Organisation weitergegeben werden dürfen
- **Kein Risiko:** Das Programm arbeitet mit Informationen, welche frei zugänglich sind und nicht geschützt werden müssen.

Um den Datenschutz zu gewährleisten, muss auf Basis dieser Klassen eine Zugriffpolitik eingeführt werden. Die Mitarbeiter werden dafür in verschiedene Klassen eingeteilt, welche jeweils andere Zugriffsrechte besitzen:

- Medizinischen Personal: Hat Zugriff auf medizinische Daten über Informationssystem und Zugriff zu medizinischen Räumen wie OP-Sälen, Krankenzimmern…
- Verwaltungspersonal: Hat Zugriff zu öffentlichen Räumlichkeiten sowie Büros und weitere benötigte Zimmer
- Technisches Personal: Hat je nach Rang und Notwendigkeit Zugriff zu technischen Räumlichkeiten

Dies ist ein Vorschlag und muss für alle anderen benötigten Rollen nachfolgenden Grundlagen erarbeitet werden:

- welche Subjekte (z. B. Personen, Programme, Prozesse, …) und welche Objekte (z. B. IT-Anwendungen, Daten, …) unterliegen der Rechteverwaltung,
- welche Arten von Rechten (z. B. Lesen, Schreiben, Ausführen, …) können zwischen Subjekten und Objekten existieren,
- wer darf Rechte einsehen, vergeben bzw. ändern,
- welche Regeln müssen bei Vergabe bzw. Änderung eingehalten werden (Authentisierung, evtl. 4-Augen-Prinzip),
- welche Rollen müssen durch die Rechteverwaltung definiert werden (z. B. AdministratorInnen, Revision, BenutzerInnen, …),
- welche Rollen sind miteinander unvereinbar (z. B. BenutzerIn und Revision, AdministratorIn und AuditorIn, …),

Um eine Zwei-Faktor-Authentifizierung zu gewährleisten, werden Chipkarten in Kombination mit einem Passwort benutzt. Denkbar ist auch eine Multifaktorauthentisierung, wo eine PIN zusammen mit biometrischen Merkmalen herangezogen wird. Dadurch kann die PIN zur leichteren Handhabe verkürzt werden. Neben einer physischen Zugriffkontrolle werden die Chipkarten auch bei Anwendungsprogrammen herangezogen. Die Programme dafür müssen folgende Anforderungen erfüllen:

- **Passwortschutz bei Programmaufruf**: Das Programm kann nur gestartet werden, wenn vorher ein Passwort korrekt eingegeben wurde. Dies verhindert die unberechtigte Nutzung des Programms.
- **Zugriffsschutz zu einzelnen Dateien**: Das Programm kann nur dann auf eine geschützte Datei zugreifen, wenn das mit dieser Datei verknüpfte Passwort korrekt eingegeben wird. Dies verhindert den unerlaubten Zugriff mittels des Programms auf bestimmte Dateien.
- **Automatische Speicherung von Zwischenergebnissen**: Das Programm nimmt eine automatische Speicherung von Zwischenergebnissen vor, so dass ein Stromausfall nur noch

die Datenänderungen betrifft, die nach der letzten automatischen Speicherung eingetreten sind.

- **Verschlüsselung von Dateien**: Das Programm ist in der Lage, eine Datei verschlüsselt abzuspeichern, so dass eine unbefugte Kenntnisnahme verhindert werden kann. Die Inhalte der Datei sind damit nur denjenigen zugänglich, die über den verwendeten geheimen Chiffrierschlüssel verfügen.

Das Arbeiten muss dabei nicht zwingend innerhalb der Räumlichkeiten passieren. Fernzugriffsmöglichkeiten können mit unterschiedlichen Endgeräten (Desktop, Notebook) realisiert werden. Die Verbindung zwischen dem Endgerät und der Zentrale führt in der Regel über das Internet. Um dabei die Sicherheit zu gewährleisten, müssen folgende Maßnahmen erfüllt sein:

- eine erfolgreiche Authentifizierung der BenutzerInnen gegenüber ihren Endgeräten und dem Netz der Institution,
- Verschlüsselung der Daten auf dem Endgerät und eine regelmäßige Sicherung der Daten im Netz der Institution, um die auf dem Endgerät gespeicherten Daten vor Verlust und gegen Vertraulichkeitsverletzungen zu schützen
- Einsatz eines kryptografisch gesicherten VPN, um die Kommunikationsverbindung zwischen dem Endgerät und dem Netz der Institution vor unbefugtem Mitlesen zu schützen. Die Absicherung wird durch das Verschlüsseln und gegebenenfalls Signieren der ausgetauschten Datenpakete erreicht, nachdem die Kommunikationspartner authentisiert wurden.
- Die Verbindung muss nach 10-minütiger Inaktivität deaktiviert werden.

Wurden Endgeräte entwendet oder gestohlen, sollten sich die Fernzugriffe der betroffenen BenutzerInnen durch die Institution kurzfristig sperren lassen. Zusätzlich sollte eine Anwenderrichtlinie die BenutzerInnen auf ihre Sorgfaltspflichten hinweisen, um so die Risiken durch Nachlässigkeit zu reduzieren.