SPENGERGASSE

Datenschutz- und Informationssicherheitskonzept

Änderungshistorie

Version	Autor	Notiz
1.0	Stefan Mandic	Erstversion

Wien-5-Tagesklinik	Datenschutz- und Informationssicherheitskonzept	Version 1.0
Verfasser: Stefan Mandic	Aufbau, die Umsetzung und die Aufrechterhaltung der TOM durch ein Datenschutz- und Informationssicherheitsmanagementsystem (DISMS)	

Version	Datum	Autor/in	Änderung	Begründung	Betroffene Seiten
1	14.03.2023	Stefan Mandic	Alles		alle

1. **der HLS-Aufbau ist vorhanden** (**Einleitung / Anwendungsbereich (Statement of Applicability) / Normative Verweise / Abkürzungs- und Begriffsverzeichnis / Kontext der Organisation /Führung / Planung / Unterstützung / Betrieb / Bewertung der Leistungen / Verbesserungen (KVP –Kontinuierlicher Verbesserungsprozess)**
2. **der Prozess für die Risikoanalyse sollte noch genauer sein!**
3. **wo sind die Gremien für DSIS-Prozess und verantworlichen Rollen (CISO, ..)?**
4. **das Rollenmodell sollte noch genauer sein!**
5. **es wird ein SOC angeführt - eine genauer Ausführung wäre von Vorteil und der Meldeprozess für NISG, DSGVO, ... ist NICHT vorhanden**
6. **die Richlinie für Authenifizierung sollte noch genauer sein!**
7. **ein Jump-Host od. Terminal-Server hätte die Richtlinie noch gut erweitert**
8. **der Aufbau ist nicht immer logisch - viele Wiederholungen**
9. **keine Möglichkeit verwenden - MUSS ERFOLGEN, MUSS UMGESETZ WERDEN**

Warum TLP: RED = STRENG VERTRAULICH?

Erstellt: 14.03.2023	Geprüft: /	Freigegeben: /	Gültig bis:
NAME Stefan Mandic	NAME	NAME	
ROLLE: Berater	ROLLE	ROLLE	ROLLE
Vertraulichkeit:	red ~~/ amber / green / white~~		
Überprüfungsintervall:	**3 Monate**		
Gültigkeitszeitraum:	12 Monate		
Status:	in Bearbeitung		Seite 2 von 12

Inhalt

1 Zweck und Anwendungsbereich

Dieses Dokument beschreibt die Vorgehensweise für die Einführung eines Datenschutz- und Informationssicherheitssystems für die Wien-5-Tagesklinik. Weiters wird beschrieben, welche technische und organisatorische Maßnahmen, welche sich nach der DSGVO halten, wichtig sind, um den Datenschutz und die Datensicherheit für alle Patienten und Patientinnen, sowie allen Mitarbeitern und Mitarbeiterinnen zu gewährleisten. Damit in der gesamten Klinik diese Sicherungen wirken, ist es notwendig, dass alle Individuen, diese Informationen zur Kenntnis nehmen und sich daran halten, ohne Ausnahmen.

Das Dokument basiert auf die rechtlichen Gegebenheiten des österreichischen Gesetzesrahmen.

2 Datenschutz und Informationssicherheitskonzept

2.1 Organisatorische Maßnahmen

Für jedes mögliche Risiko muss eine Risikoanalyse durchgeführt werden, für bestehende aber auch für alle möglichen Risiken oder Gefahren. Hierbei betrachtet man, was jener Angriff angreift und was die Folgen eines Angriffs sein können. Anschließend werden die Risiken in den Kategorien: Hoch, Mittel oder Gering bewertet, je nach den Gefahren, die solche Attacken oder Angriffe mit sich ziehen, sowie den Ausmaß dieser Attacken.

- Maßnahmen zur Risikominimierung:
  - SOC
    - Das Security Operation Center, fungiert als Notfallteam, diese sind daher bei Notfällen, wie Angriffe oder Attacken bzw. Manipulationsversuche der sensiblen Daten sofort zu verständigen. Diese versuchen dann, das Problem, schnellst möglichst zu beseitigen. Das Notfallteam wird von einer Leitperson organisiert und koordiniert. Das Team muss sich jede Woche treffen um den aktuellen Stand zu besprechen, jede Besprechung wird von einer Person dokumentiert. Dieses Dokument ist für alle Mitarbeiter ein sichtlich, dies dient dazu, dass alle Mitarbeiter am aktuellen Stand sind.
  - Schulungen
    - Allen Mitarbeitern, die mit einem Gerät arbeiten, dass mit dem Netzwerk verbunden ist, oder mit sensiblen Daten von Patienten arbeiten oder Ähnliches, sind dazu verpflichtet sich einer internen Schulung zu untergehen. Solche eine Einschulung kann folgende Punkte enthalten:
      - Mitarbeiter dürfen keine Links oder Dateien anklicken, öffnen oder runterladen, welche von externen nicht identifizierbaren Quellen

stammen, wie Z.B fremde Emails. Solche Vorfälle müssen sofort der IT-Abteilung übermittelt werden, diese überprüfen dann die Quelle der Daten und um welche Gefahr es sich hierbei handelt.

- Alle Mitarbeiter müssen ein starkes Passwort verwenden, das aus mindestens 10 Zeichen besteht, weiters muss das Passwort Sonderzeichen, klein- und groß geschriebene Buchstaben enthalten und Zahlen. Mithilfe eines starken Passworts können Mitarbeiter die Gefahr umgehen, dass Drittpersonen in ihre Accounts hineindringen.
- Allen Mitarbeitern ist es verboten sensible oder private Daten auf die Arbeitsgeräte zu speichern.
- Allen Mitarbeitern ist es verboten externe Applikationen auf die Arbeitsgeräte zu installieren.
- Falls ein Arbeitsgerät mit Nachhause mitgenommen wird, muss dieses eine Blickwinkel Folie haben, damit Drittpersonen nicht auf den Bildschirm von der Seite schauen können. Weiters müssen alle Mitarbeiter, alle Daten und Aktivitäten an den Arbeitsgeräten vor Dritten zu schützen, daher ist das Verwenden eines Arbeitsgerätes in öffentlichen Räumen, sowohl intern als auch extern strengstens verboten.
- Updates der Geräte oder Systeme dürfen nicht von unbefugten Mitarbeitern durchgeführt werden, sondern nur ausschließlich von der IT-Sicherheitsabteilung.
- Allen Mitarbeitern ist es untersagt im Internet zu surfen oder in sozialen Medien hineinzugehen.
- Die Mitarbeiter müssen diese Regeln unterschreiben, und machen sich daher für sich selbst verantwortlich. Bei nicht beachten der Vorschriften und Regeln, ist eine sofortige Wiederholungseinschulung vorzunehmen.

  - Diese Schulungen, haben den Vorteil, dass die Mitarbeiter sich bewusst sind, dass es sich in dieser Klinik um sensible Daten handelt und daher eine hohe Sicherheit, sehr wichtig ist.
- Sicherheitsmanagement
  - Im Falle eines Sicherheitsvorfalles, ist die SOC, sofort zu kontaktieren und zu verständigen. Das Verschweigen eines Vorfalles, kann rechtliche Konsequenzen mit sich ziehen.
  - Nachdem die SOC die Eilmeldung bekommt wird die Attacke analysiert und dann wird eine technische Maßnahme ausgewählt, um die Attacke zu umgehen.

        - Dabei wird jeder Schritt dieses Zyklus dokumentiert, sowohl vom Notfallteam als auch vom betroffenen Mitarbeiter, um das Risiko zukünftiger Attacken solcher Art zu minimieren. Dabei wird der Datenschutz der personenbezogenen Daten (DSVGO) und das NISG vollständig beachtet und durchgeführt.
        - Zusätzlich sind die Behörden bei einem Angriff sofort zu verständigen
    - Compliance
        - Diese Richtlinie richtet sich in jeder Hinsicht nach der DSGVO, NISG und dem Gesundheitstelematikgesetz. Dies beschreibt die Regeltreue der Klinik, daher muss sich diese an alle Gesetze halten sowie allen Richtlinien
        - Weiters muss eine regelmäßige Überprüfung durchgeführt werden, um sicherzustellen, dass sie den aktuellen Anforderungen und Standards der Gesetze entspricht.
    - Verantwortlichkeiten und Zuständigkeiten
        - Die Leitperson des Notfallteams ist für das Koordinieren des Notfallteams, sowie für das sofortige Reagieren auf Angriffen verantwortlich.

2.2 Technische Maßnahmen

- Wichtige technische Maßnahmen die kontinuierlich durchzuführen sind, sind:
    - Regelmäßige Backups, damit man bei Angriffen wie Ransomwares, ein sofortiges Backup durchführen kann, falls die Ransomware nicht zu umgehen ist.
    - Update der Technologie, um immer auf den aktuellen Stand der Technologie zu sein.
    - Logging aller Aktivitäten, mit Time Keeping, um die Manipulation der Zeit zu umgehen
- Bei einer Attacke, bei der ein Schadprogramm in das System der Klinik hineindringt, wird zunächst mit einigen Tools versucht, diese zu entfernen. Falls das Notfallteam daran scheitert, wird ein externer Experte dazu geholt, der dabei hilft die Daten wiederherzustellen bzw. die Schadsoftware zu entfernen.
    - Expertenhilfe: Hierbei wird ein externer Experte dazu geholt, der versucht das Problem zu lösen und die Attacke zu umgehen. Der Experte verbindet sich mit einer virtuellen Maschine in das interne System mittels Jump Host. Mithilfe dessen können alle Tätigkeiten des Experten überwacht und protokolliert werden. Wenn der Experte jedoch daran scheitert, das Problem zu beheben, muss ein vollständiges Backup eingespielt werden.
    - Es ist wichtig, dass ein externer Experte keinen Zutritt auf sensible Daten der Klinik oder der Patienten hat, deshalb ist es von großer Bedeutung, dies zu kontrollieren.

- Weiters ist es wichtig, dass alle Firmengeräte passwortgeschützt sind, die Mitarbeiter können sich auf jedem Gerät anmelden, jedoch bekommen sie nur ihre Daten zu sehen, da ein Active Directory verwendet wird. Nach einer Inaktivität von 10 Minuten, werden die Geräte wieder gesperrt und setzen ein erneutes Passwort und Benutzername Eingabe voraus
- Verschlüsselung
    - Jegliche Dateien, die in den Datenbanken der „Wien-5-Tagesklinik“ gespeichert werden sind kryptografisch zu verschlüsseln.
    - Alle mobilen Firmengeräte, welche auch mitnachhause mitgenommen werden können, um das Home-Office zu ermöglichen, müssen ein Bitlocker enthalten, um im Falle eines Diebstahles oder Verlustes das Filesystem zu verschlüsseln.
- Technische Implementierung von Firewalls
- Zugriffskontrolle:
    - RBAC: Rollenbasierte Zugriffskontrolle
        - In der Klinik, ist es wichtig die Zugriffe nach dem RBAC Schema zu verwalten. Dabei werden Rollen für jede unterschiedliche Funktion in der Klinik erstellt, anschließend werden alle Benutzer in ihren jeweiligen Rolle eingeteilt und bekommen nur beschränkte Berechtigungen. Dies setzt voraus, dass bei jeder Anmeldung sich der Benutzer mit einer 2 Faktor Authentifizierung authentifiziert. Administratoren haben in dieser Hinsicht nicht alle Berechtigungen, da ein Administrator in der Technik-Abteilung sein kann, aus diesem Grund soll dem Administrator kein Zugriff auf die Patientendaten gewährt sein.
        - Es ist auch eine Telearbeit möglich, wo man sich mit der Klinik verbinden kann, ortsunabhängig. Dies setzt jedoch voraus, dass sich der Benutzer an einer virtuellen Maschine verbindet, jedoch muss eine zwei Faktor Authentifizierung durchgeführt werden.

3 Normative Verweise

Die Klinik ist ein gesundheitlicher Sektor und arbeitet mit sensiblen Patientendaten, daher ist es eine Voraussetzung, dass man sich hierbei an die DSGVO, GTelG und das NISG hält. Das gesamte Sicherheitskonzept muss nach aktuellen Standards und unter Einhaltung der entsprechenden Normen zu implementieren.

4 Abkürzungs- und Begriffsverzeichnis

CIA	Confidentiality, Integrity, Availability (=Vertraulichkeit, Integrität, Verfügbarkeit)
CISO	Chief Information Security Officer
DSGVO	Datenschutzgrundverordnung
GDA	Gesundheitsdiensteanbieter
GTelG	Gesundheitstelematikgesetz
KOFÜ	Kollegiale Führung
KVP	Kontinuierlicher Verbesserungsprozess
NISG	Netz- und Informationssicherheitsgesetz
PDCA	Plan, Do, Check, Act (=Planen, Durchführen, Kontrollieren, Agieren)
SOC	Security Operations Center

5 Kontext der Organisation

Die „Wien-5-Tagesklinik“ besteht auf 2 Ebenen aus je acht Untersuchung. Und Behandlungszimmer, Umkleideräumen, Warte- und Aufnahmebereichen, vier Ärzt:innenzimmern, Sozial- und Sanitärräumen für Mitarbeiterinnen und Patientinnen sowie im Keller aus Technikräumen für Heizung, Lüftung und Klima und zwei Rechenräumen. Die Räumlichkeiten sind pro Ebene in fünf Brandabschnitte unterteilt, wobei die zwei Rechenräume je ein eigener Brandabschnitt ist.

6 Führung

Die Führung ist die Leitung der jeweiligen Berufsgruppen. Im Falle eines Ausfalls oder Angriffs muss dieser sofort an die kollegiale Führung und dem NISG gemeldet werden.

7 Planung

Im Falle eines Ausfalles bzw. eines Angriffes sind folgende Punkte vorzunehmen:

7.1 Organisatorische Maßnahmen

- Im Falle eines Ausfalles muss das gesamte Notfallteam dafür sorgen, dass das System wieder hochzufahren, um den Normalbetrieb wiederherzustellen. Dies muss innerhalb 2 Stunden erfolgen, währenddessen muss das Notfallteam, den Angriff identifizieren und eine sofortige
- Bewertung der Risiken und Schwachstellen unter Berücksichtigung der DSGVO, NIS, GTel-Gesetze

7.2 Technische Maßnahmen

- Bei einem Ausfall der Systeme oder des Rechenzentrums müssen die Daten auch parallel in einer Cloud-Lösung, die die DSGVO beachtet gespeichert werden, sodass die Verfügbarkeit der Daten jederzeit gegeben ist.
- Backups müssen ebenfalls kontinuierlich erstellt werden, diese können bei gewissen Angriffen wie Ransomware Attacken eingespielt werden.
- Weiters muss ein Notstrom Diesel-Aggregat vorhanden sein, der das Rechenzentrum für 2 Stunden in Takt hält.
- Ersatzgeräte für alle Mitarbeiter müssen ebenfalls vorhanden sein, falls ein Gerät ausfällt, wechselt der Mitarbeiter das Gerät, der Mitarbeiter muss davor die IT-Abteilung verständigen und bekommt daraufhin ein Ersatzgerät. Mithilfe des Active Directorys, kann der Mitarbeiter seine Daten unabhängig von den Geräten wieder einsehen.
- Der Serverraum muss auch Raid-5 Systeme enthalten, da solches vor Datenverlust schützt sowie höhere Kapazitäten als ein Raid-1 System bietet. Im Falle eines Ausfalles eines Speichermediums, kann das 2. Bzw. das gespiegelte noch arbeiten und ist daher funktionsfähig.
- Im Falle eines Brandes im Rechenzentrum, ist Argon gas einzusetzen, jedoch muss sichergestellt werden, dass sich hierbei aber niemand im Rechenzentrum befindet.

8 Unterstützung

- Schulungen:
- Compliance

9 Betrieb

Das Notfallteam sind jeweils spezialisiert auf einen bestimmten Bereich der Verteidigungslinie. Sie sind verantwortlich für die Verschlüsselung, das Speichern und den Schutz von Daten. Regelmäßige Tests und Angriffe werden durch die IT-Abteilung durchgeführt, um Sicherheitslücken aufzudecken, die vom Notfallteam gelöst werden. Das Notfallteam muss das System vor Angriffen schützen und diese abwehren, sowie die Richtlinien und Dokumente laufend aktualisieren, um Änderungen im System zu berücksichtigen. Jedoch sind auch alle Mitarbeiter dazu verpflichtet ihren Teil zur Cyber Security beizutragen.

10 Bewertung der Leistungen

- Riskobewertung:
  - Risikoplan einholen
  - Betroffene Risiken priorisieren (Hoch Mittel Niedrig)

INCIDENT Prioritäten Matrix					
		Auswirkung			
		gering	moderat	erheblich	großflächig
Dringlichkeit	kritisch	hoch	hoch	kritisch	kritisch
	hoch	mittel	hoch	hoch	kritisch
	mittel	mittel	mittel	mittel	hoch
	niedrig	niedrig	niedrig	niedrig	mittel

11 Verbesserungen (KVP – Kontinuierlicher Verbesserungsprozess)

Der PDCA-Zyklus ist ein Konzept im Qualitätsmanagement, das sicherstellt, dass Maßnahmen effektiv sind und kontinuierlich verbessert werden. Der Zyklus besteht aus vier Schritten: Planung, Umsetzung, Überwachung und Verbesserung. Es ist wichtig, Maßnahmen regelmäßig zu überprüfen und neue Bedrohungen miteinzubeziehen.

A. **55 Punkte für:** Beschreiben Sie die Vorgangsweise für die PDCA-Zyklus für die Datenschutz- & Informationsrichtlinie (DSIS-Policy) der Tagesklinik. Welche Personen, welche Expertengruppe zur Erfüllung bestimmter Aufgaben setzen Sie ein, welche Aktivitäten, welche Schritte führen Sie für die Erstellung, Umsetzung, Überprüfung und Verbesserung durch. Beschreiben Sie Ihre Vorgangsweise für den Prozess, der die DSIS-Policy) erstellt, umsetzt, überprüft und verbessert.

   Nach der Beschreibung der Vorgangsweise und den notwendigen Aktivitäten (z.B.: Bedrohungsanalyse, ...) erstellen Sie einen Vorschlag für eine spezifische Richtlinie mit folgenden Inhalten:

B. **45 Punkte für:** Organisatorische und technische Vorgaben für Authentifizierung anhand verschiedenen Rollen für Anwendungsprogramme und Systemprogramme (Anwender:innen, System-Administator:innen).

   Beachten Sie dabei, dass System-Administrator:innen und Service-Techniker:innen für medizintechnische bzw. technische System nicht nur den Zugriff in den Räumlichkeiten der „Wien-5-Tagesklinik“ durchführen können, sondern auch über FERNZUGRIFF oder TELEARBEIT. Dabei ist auf die Nachweisbarkeit der Aktivitäten der Technicker:innen auf den Ziel-Systemen zu achten.

C. **10 Punkte für:** Form und Qualität der Ausarbeitung