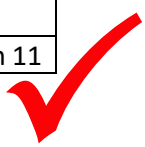
GruppeB

Ausfallssicherheitskonzept für Wien-5-Tagesklinik

Dokumententyp	Orginasatorische Richtlinie / Technische Richtlinie
Klassifikation	TLB: ~~red /~~ amber ~~/ green / white~~
Autor/in	5BHBGM, Imani Dadaeva
Letzte Änderung	14.03.2023
Prüfer/in	Name Prüfer
Geprüft am	Datum geprüft
Freigeber/in	Name Freigeber
Freigegeben am	Datum freigegeben
Gültigkeitszeitraum	ab Freigabedatum: 12 Monate / ~~24 Monate~~ / ~~36 Monate~~
Überprüfungsintervall	3 Monate / ~~6 Monate~~ / ~~12 Monate~~ / ~~18 Monate~~
Version	1.0
Vertraulichkeit	STATUS: ~~in Bearbeitung /~~ freigegeben ~~/ zurückgezogen~~



Version	Datum	Autor/in	Änderung	Begründung	Betroffene Seiten
1.0	23.03.2023	Imani Dadaeva	TOM	Dokumentzusammenstellung	Alle folgenden

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. **wo sind die Gremien für DSIS-Prozess und verantworlichen Rollen (CISO, ..)?**
3. **welches Rollenmodell wird eingesetzt?**
4. **es gibt ein SOC - eine genauer Ausführung wäre von Vorteil und der Meldeprozess für NISG, DSGVO, ... ist nicht vorhanden?**
5. **wo ist die Richlinie für Authenifizierung?**
6. **ein Jump-Host od. Terminal-Server hätte die Richtlinie noch gut erweitert**
7. **usw.**

Inhalt

1 Einführung

Dieses Dokument regelt die Vorgehensweise für die Implementierung und regelmäßige Überwachung eines Datenschutz- und Informationssicherheitssystems für die Wien-5-Tagesklinik. 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 und orientiert sich dabei explizit auf die Gesetze DSGVO, NIS und die GTEL.

2 Anwendungsbereich (Statement of Applicability)

Diese Verfahrensanweisung betrifft alle Mitarbeiter Klinik, sowohl intern arbeitende Mitarbeiter als auch externe Mitarbeiter, des Weiteren sind auch externe Kooperationsmitarbeiter davon betroffen. Daraus erschließt sich, dass das Dokument laut TLP AMBER ist, und somit die Weitergabe des Empfängers nur innerhalb der Organisation erfolgt.

3 Normative Verweise

Da das Projekt im gesundheitlichen Sektor angesiedelt ist und es um den Schutz von Patientendaten geht, ist es wichtig, dass hierbei die DSGVO, GTelG, 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 im IKT-Bereich möglichst hochzuhalten.

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

Diese Verfahrensanweisung betrifft alle Mitarbeiter Klinik, sowohl intern arbeitende Mitarbeiter als auch externe Mitarbeiter, des Weiteren sind auch externe Kooperationsmitarbeiter davon betroffen. Daraus erschließt sich, dass das Dokument laut TLP amber ist, und somit die Weitergabe des Empfängers nur innerhalb der Organisation erfolgt.

6 Führung

Die kollegiale Führung ist die Leitung der Berufsgruppen. Bei einem Ausfall oder Angriff muss dieser sofort an die kollegiale Führung und dem NIS gemeldet werden. Außerdem muss das SOC in Kenntnis gesetzt werden, da dieses dafür verantwortlich ist den Normalzustand wieder herzustellen wie auch das System vor Angriffen zu schützen bzw. die Daten zu sichern.

7 Planung

Auf Basis des PDCA- Zyklus muss zur Vorbeugung eines Ausfalls in der Klinik ein strukturierter Prozess durchlaufen werden. Teilpunkte dieses Prozesses sind die Planung, Umsetzung, Überprüfung und die Verbesserung.

7.1 Organisatorische Maßnahmen

- Identifikation der Gesundheitsservice:
  Um ein Ausfallssicherheitskonzept zu erstellen, müssen zuallererst die Gesundheitsservices der Wien-5-Tagesklinik identifiziert werden, sowie ihre Verknüpfungen zu den IT- Systemen. Folglich wird eine Risikoanalyse gestartet.
- Risikoanalyse
  Um bestehende oder mögliche Angriffe zu verhindern oder zu minimieren, müssen die Risiken im Rahmen einer Risikoanalyse vorerst analysiert werden. Dabei wird folgendermaßen vorgegangen:
  - Identifizierung der möglichen Bedrohungen und Risiken:
    Die Identifizierung der Risiken erfolgt durch das SOC- Team. Dabei werden mögliche Angriffe auf das System im allgemeinen, sowie Angriffe, welche die Geräte der einzelnen MitarbeiterInnen betreffen, analysiert. Die durchgeführte Analyse bezüglich der Risiken muss protokolliert werden und die einzelnen Angriffsszenarien müssen beschrieben werden.
  - Einteilung der Risiken in Kategorien unter Berücksichtigung der DSGVO, NIS, GTel-Gesetze :
    Um einen Überblick über den Schweregrad der Risiken zu verschaffen, müssen diese in den folgenden Kategorien gegliedert werden:
    - Hoch: Eingliederung von Risiken, welche eine besondere Gefahr für die Organisation und den Personen dieser stellen und somit zu einer Prozessbeschädigung der Organisation führt.
    - Mittel: Eingliederung von Risiken, welche eine Gefahr für die Organisation und den Personen dieser stellen, sodass Teile der Organisationsprozesse eingeschränkt sind.
    - Niedrig: Eingliederung von Risiken, welche eine geringe Gefahr für die Organisation und der Personen dieser darstellt.

    Die Einteilung wird in einem Plan festgehalten, sodass beim Auftreten eines Angriffes das Notfallteam einen schnellen Überblick hat.

- Maßnahmen zur Risikominimierung:
  - Verantwortlichkeiten und Zuständigkeiten:
    Die Aufgaben und Verantwortlichkeiten müssen genauestens geregt werden, sodass im Falle eines Ausfalls schnell gegengewirkt werden kann.
    - Leitungsperson für Notfälle: Eine qualifizierte und erfahrene Person in der Organisation wird gewählt, welche mit dem SOC zusammenarbeitet, dieses lenkt und die Vorgesetzte über Änderungen und Fälle informiert.

    - SOC-Team: Das Team ist der erste Ansprechpartner bei aufgetretenen Problemen und muss daher in der Organisation vorgestellt werden. Die MitarbeiterInnen der Organisation sind im Falle eines Angriffes zur sofortigen Kontaktaufnahme mit dem Notfallteam verpflichtet. Für den Fall einer gezielten unterlassenen Kontaktaufnahme, sollen Konsequenzen für die betroffene/n Person/en beschlossen werden. Des Weiteren müssen die MitarbeiterInnen über die Konsequenzen bei der Unterlassung der Kontaktaufnahme informiert werden.
  - Zusammenstellung eines Vorsorgeprotokolls:
    Die Erstellung eines Vorsorgeprotokolls, welches erneut die Verhaltensmaßnahmen zur Vorbeugung von Angriffen oder die Verhaltensweise im Falle eines Angriffes beschreibt, ist verpflichtet und muss für jeden Teilhaber in der Organisation zugänglich sein.

  - Überwachung und Aktualisierung der definierten Maßnahmen: Es finden kontinuierliche Meetings mit der Leitungsperson, der IKT- Abteilung sowie dem Notfallteam statt, um die Einhaltung der Maßnahmen zu besprechen. Des Weiteren ist die Leitungsperson verpflichtet einen monatlichen Bericht zu verfassen und diesen den Vorgesetzten zu präsentieren.

7.2 Technische Maßnahmen

- Verschlüsselung der Daten -> kryptografische Verschlüsselungsmechanismen
  Da in der Klinik mit sensiblen und personenbezogenen Patientendaten gearbeitet wird ist eine Verschlüsselung laut dem GTel notwendig und verpflichtend. Die Daten müssen bei Ablage in eine Datenbank verschlüsselt werden und auch beim Versenden innerhalb der Organisation. Mitarbeiter, welche ständig mit Patientendaten arbeiten, sind verpflichtet ihr Filesystem mittels Bitlocker zu verschlüsseln. Zusätzlich müssen diese Personen eine Sichtschutzfolie auf ihren Geräten verwenden, um die Sicherheit vor Dritten zu steigern. Betreffend der Passwörter, ist neben dem Hashen auch ein Pepper und Salt Verfahren einzusetzen.
- Implementierung von Firewalls
- Zugriffskontrolle:

RBAC: Rollenbasierte Zugriffskontrolle
Die Klinik ist verpflichtet, die Zugriffe auf die Systeme nach dem RBAC zu verwalten. Die User müssen in Rollen eingeteilt werden, welche unterschiedliche Berechtigungen besitzen.
So kann bsw. ein Ramsomware- Angriff auf dem Rechner einer Pflegekraft weniger Schäden anrichten als ein Angriff auf dem Gerät eines Administrators.
2 Faktor Authentifizierung:
Software, welche Patientendaten beinhaltet und mit diesen arbeitet muss eine Zwei-Faktor-Authentifizierung besitzen, um so die Identität eines Nutzers zu überprüfen.
Zusätzlich muss ein Logging und Time Keeping erfolgen, sodass die Aktivitäten der Mitarbeiter mitprotokolliert werden.

- Einsatz von Thin- Clients:
  Der Einsatz von Thin-Clients für das medizinische Person, ist eine mögliche Maßnahme, um Cyberangriffe zu reduzieren. Eine äußerst empfehlenswerte Maßnahe ist die Authentifizierung am Thin- Client mittels Kartenleser, denn so kann die Wahrscheinlichkeit von Identitätsdiebstahl, sowie der unbefugte Zugriff auf Patientendaten durch Dritte verringert werden.
- Regelmäßige Datensicherung: Es müssen regelmäßige Backups durchgeführt werden, sodass im Falle eines Angriffs die Möglichkeit besteht, die Originaldaten sowie den vorherigen Stand des Systems wiederherzustellen. Es muss eine Protokollierung der erstellten Backups erfolgen.
- Überwachung des Netzwerks, um verdächtigte Aktivitäten schnell zu erkennen.
- Monatliche Erinnerungs- E-Mails zu IT- Sicherheit, vor allem bezogen auf Phishing- und Smishing Nachrichten: Um die MitarbeiterInnen auf die Cybergefahren immer wieder aufmerksam zu machen, könnten monatlich eine automatische E-Mail versendet werden, dessen Inhalt Merkmale von Phishing- und Smishing- Nachrichten erläutert und erneut die Gefahren aufmerksam macht.
- Installation von Antivirusprogramme
- Verwendung von HTTPS: Da in der Klinik das Versenden von Patientendaten üblich ist, muss die Kommunikation in der gesamten Klinik das http- Protokoll laufen, um so die Vertraulichkeit und Integrität sicherzustellen und Cyberangriffe zu minimieren.
- Raid Systeme (Redundanzen): Am besten eignet sich RAID 5 oder RAID 10
- Outsourcing: Durch das Outsourcing kann die Wahrscheinlichkeit eines Ausfalls vermindert werden und ist aus diesem Grund zu empfehlen.

Sollte genauer erklärt werden, weil es sich um einen GDA handelt!
Welche Sicherheitsüberlegungen müssen dabei beachtet werden!

8 Unterstützung

- Schulungen:

Neue Mitarbeiter der Organisation sind verpflichtet eine Schulung zu den Themen Cyber-Security und Vorbeugung vor Angriffen zu besuchen. Im Falle eines bestehenden Angriffes müssen die MitarbeiterInnen über die Themen Datenschutz, Sicherheit, Netzwerkangriffe und Vorbeugung von Angriffen sensibilisiert werden. In den Schulungen müssen die Mitarbeiter über Phishing- Smishing- Angriffe informiert werden. Des Weiteren sollen die Mitarbeiter über eine sichere Passwortwahl aufgeklärt werden und die Konsequenzen, welche auftreten könnten, bei zu schwachen Passwörtern. Ein besonders wichtiges Thema hierbei sind die Dienstgeräte.

Die Mitarbeiter sind dazu verpflichtet, das Speichern von privaten Dateien auf Dienstgeräten, wie Tablets oder Smartphones, zu unterlassen.

Das wesentliche Ziel der Schulungen ist die Stärkung des Bewusstseins bezüglich der Wichtigkeit von IT-Sicherheit und Datenschutz im Gesundheitswesen und die Sicherstellung, dass die Mitarbeiter die getroffenen Anforderungen verstehen.

Nachdem Vollenden der Schulungen müssen die Mitarbeiter eine Erklärung unterschreiben, dass sie die Schulungen besucht und verstanden haben und, dass sie mit der Hausordnung einverstanden sind.

- Compliance

Diese Richtlinie richtet sich in jeder Hinsicht nach der DSGVO, NIS und dem Gel. Daher muss jeder Schritt und jede Aktivität sich diesen Gesetzen anpassen.
Es muss eine regelmäßige Überprüfung und Aktualisierung der Richtlinie durchgeführt werden, um sicherzustellen, dass sie den aktuellen Anforderungen und Standards der Gesetze entspricht.

9 Betrieb

Mitarbeiterinnen und Mitarbeiter des SOC haben jeweils oder in festgelegten Teams ein Gebiet dieser Verteidigungslinie. Auf diesem Gebiet sind sie spezialisiert.
Je nach Aufgabenbereich sind manche für die Verschlüsselung der Daten verantwortlich, das Speichern dieser Daten auf einen Backup-Server, um die Verfügbarkeit zu garantieren oder Daten allgemein zu schützen.
Mittels gezielten Tests und Angriffen seitens der IT-Abteilung werden Sicherheitslücken aufgedeckt, die wiederum von anderen Beschäftigen des SOCs gelöst werden. Regelmäßig, nach jedem Update oder Wartungen eines Systems muss das System wieder getestet werden.
Weiters soll das SOC das System vor Angriffen schützen und diese abwehren.
Die Richtlinien und Dokumente, die vom SOC ausgehen müssen laufend aktualisiert werden, sofern sich Dinge, wie Geräte oder ähnliches ändern.

10 Bewertung der Leistungen

- Riskobewertung:
    - Der erste Schritt ist die Bewertung des Risikos anhand des erstellten Risikoplans. Nachdem ermittelt wurde unter welche Kategorie der Angriff fällt, können dementsprechende Maßnahmen eingeleitet werden.

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)

PDCA-Zyklus: Für die Überprüfung der Maßnahmen, ob sie tatsächlich wirken, muss es einen regelmäßigen Kontrollprozess geben (Qualitätsmanagement). In der Planungsphase werden die TOMs definiert und geplant. Im Do werden diese umgesetzt und implementiert. Im Check werden diese überwacht und die Planung mit den Ergebnisse verglichen. Im Act werden Fehler behoben und versucht den Prozess zu verbessern. Es ist wichtig für jedes Risiko die Maßnahmen regelmäßig zu überprüfen und auch immer wieder neue Bedrohungen in den Prozess miteinzubeziehen (z.B. Lessons Learned nach einem Notfall).

4. Aufgabenstellung

4.1 Erstellen eines „Datenschutz- und Informationssicherheitskonzeptes“ (100 Punkte):

Kernelemente des Datenschutz- und Informationssicherheitskonzeptes sind der Aufbau, die Umsetzung und die Aufrechterhaltung der TOM durch ein Datenschutz- und Informationssicherheitsmanagementsystem (DISMS) für die “Wien-5-Tagesklinik”.

Dieses Managementsystem basiert auf den Grundsätzen **„Privacy & Security by Design“** und **„Privacy & Security by Default“**, die die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung, Verbesserung und den Schutz der **„Services der Wien-5-Tagesklinik“** sowie der personenbezogenen Gesundheitsdaten abdecken soll.

Vorgangsweise für das DISMS “Wien-5-Tagesklinik”:

Beschreiben Sie für die “Wien-5-Tagesklinik” folgende technisch-organisatorische Maßnahmen anhand des Deming-Kreises (PDCA-Zyklus).

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

***ACHTUNG:* PUNKT A + B WERDEN IN EINEM DOKUMENT ABGEGEBE!**