SCO für KOFÜ der Klinik

Dokumententyp	Organisatorische Richtlinie / Technische Richtlinie
Klassifikation / Vertraulichkeit	TLB: ~~red /~~ amber ~~/ green / white~~
Autor/in	Stefan Mandic
Letzte Änderung	12.03.2023
Prüfer/in	
Geprüft am	
Freigeber/in	
Freigegeben am	
Gültigkeitszeitraum	ab Freigabedatum: 12 Monate
Überprüfungsintervall	2 Monate
Version	1.0
Status	STATUS: in Bearbeitung

Version	Datum	Autor/in	Änderung	Begründung	Betroffene Seiten
1	12.03.2023	Stefan Mandic	Richtlinie erstellt	Sicherheitsmängel	alle

Inhalt

1 Einführung

Dieses Dokument regelt die Vorgehensweise für die Implementierung und regelmäßige Überwachung eines Datenschutz- und Informationssicherheitssystems für die KOFÜ der Klinik. 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

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 Grundlagen

Da die SOC im Sicherheitssektor, sowie im Gesundheitssektor angesiedelt ist und es um den Schutz von sensiblen Daten 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 im IKT-Bereich möglichst hochzuhalten.

4 Qualitätsmanagement

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 Ergebnissen 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).

5 Gefahrenbeschreibung

Innerhalb einer klinischen Organisation spielt die Sicherheit der sensiblen Daten eine sehr wichtige Rolle. Deshalb müssen alle Gefahren, die diese Daten angreifen oder manipulieren würde, identifiziert werden und beschrieben werden. Solche Gefahren greifen die CIA-Triade an und können somit die Vertraulichkeit, Verfügbarkeit und Integrität manipulieren bzw. angreifen.

Zu den möglichen Gefahren zählen:

- DDOs - Angriff
- Ransomware Angriff
- Malware
- Man-in-the-middle Attacke.
- SQL Injection

Und weitere Gefahren.

6 Vorgehensweise Informationssicherheitskonzept

6.1 Organisatorische Maßnahmen

- Risikoanalyse
  - Zunächst soll eine Risikoanalyse durchgeführt werden, in der alle möglichen und bestehenden Risiken und Gefahren beschrieben werden und identifiziert werden. Hierbei betrachtet man, was jener Angriff angreift und was die Folgen eines Angriffs sein können.
  - Die Risiken werden danach bewertet und in den Kategorien: Hoch, Mittel und Niedrig kategorisiert.
- Maßnahmen zur Risikominimierung:
  - Notfallteam
    - Eine wichtige organisatorische Maßnahme ist es, ein Notfallteam aus geeigneten Spezialisten zu bilden, diese kümmern sich dann um die Gefahren, wenn sie Eintreten und versuchen so schnell wie möglich diese zu beseitigen. Das Team wird allen Mitarbeitern als Notfallansprechpartner vorgestellt, damit die Mitarbeiter wissen, dass sie das Notfallteam bei einem Angriff kontaktieren müssen. Das Notfallteam wird von einer Leitperson organisiert und koordiniert.
    - Das Notfallteam beschäftigt sich mit den Angriffen und versucht diese schnell zu identifizieren und eine Lösung dafür zu finden.
  - Schulungen
    - Alle Mitarbeiter, die mit einem Gerät arbeiten, das sensible Daten der Organisation enthält oder mit dem lokalen Netzwerk verbunden sind, müssen eingeschult werden. Den Mitarbeitern wird präsentiert, wie sie sich innerhalb und außerhalb der Klinik verhalten sollen. Solch 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 dem öffentlichen Raum, wie ein Cafe, 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.

  - Plakate
    - Innerhalb der Klinik sollen Plakate aufgehängt werden, die alle Regeln bzw. Themen der Einschulung nochmal zusammenfasst, damit die Mitarbeiter, diese täglich durchlesen können.

- Sicherheitsmanagement
  - Bei einem Sicherheitsvorfall in jeglicher Hinsicht, ist das Notfallteam sofort zu verständigen und kontaktieren. Das Zögern oder Verschweigen eines Fehlers bzw. einer eingegangenen Attacke ist verboten und kann rechtliche Konsequenzen mit sich ziehen.
  - Das Notfallteam analysiert die Attacke und wählt eine technische Maßnahme aus, 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.
  - Zusätzlich sind die Behörden bei einem Angriff sofort zu verständigen.

- Compliance
  - Diese Richtlinie richtet sich in jeder Hinsicht nach der DSGVO, NIS und dem Gesundheitstelematikgesetz. 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.

- Verantwortlichkeiten und Zuständigkeiten

- Die Leitperson des Notfallteams ist das Koordinieren des Notfallteams und für das sofortige Reagieren auf Angriffen verantwortlich.
- Die Mitarbeiter sind nach dem Unterschreiben, der neuen Voraussetzungen nach den Einschulungen für sich selbst verantwortlich in Hinsicht auf die zu beachtenden Regeln.

6.2 Technische Maßnahmen

Die technischen Maßnahmen beschreiben, wie Risiken auf technischer Weise minimiert werden können und wie man bei Angriffen technisch vorgeht, um diese zu beheben.

- 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 einem Ransomware Angriff, bei der das Schadprogramm nicht entfernt werden kann, wird mithilfe eines Entschlüsselungstool versucht alle Dateien zu entschlüsseln und die Schadsoftware zu entfernen. Falls das Notfallteam daran scheitert, wird ein externer Experte dazu geholt, der dabei hilft die Daten wiederherzustellen. Weiters muss das betroffene Gerät des Mitarbeiters unverzüglich vom Netzwerk getrennt werden.
- 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.
- Weiters ist 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.
- Falls ein Mitarbeiter sein bzw. ihr Passwort vergisst, ist das dem Verwaltungsteam mitzuteilen, anbei bekommt der Mitarbeiter eine Möglichkeit per Link, dass per E-Mail gesendet wurde, das Passwor zurückzusetzen, jedoch muss der Mitarbeiter eine Zweifaktor Authentifizierung untergehen um zu verifizieren, dass es sich tatsächlich um den Mitarbeiter handelt.
- Alle mobilen Firmengeräte, welche auch mitnachhause mitgenommen werden können, müssen ein Bitlocker enthalten, um im Falle eines Diebstahles oder Verlustes das Filesystem zu verschlüsseln.

7 Vorgehensweise Ausfallssicherheitskonzept

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

Lösung für das Problem finden. Aus diesem Grund muss ein Notfallkatalog erstellt werden, um alle Mitarbeiter zu informieren, wie sie sich bei einem Ausfall verhalten sollen.

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 bis zu 3 Stunden auf Takt halten kann.
- 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.