Organisatorische und Technische Maßnahmen bezüglich Cyberangriffe und Datendiebstahl

Dokumententyp	Organisatorische Richtlinie / Technische Richtlinie
Klassifikation	AMBER
Autor/in	Imani Dadaeva*
Letzte Änderung	13.03.2023
Prüfer/in	
Geprüft am	
Freigeber/in	Imani Dadaeva
Freigegeben am	13.03.2023
Gültigkeitszeitraum	12 Monate
Überprüfungsintervall	3 Monate
Version	1
Status	Fertiggestellt

*Das Dokument wurde von der 5BHBGM als Vorlage erstellt.

Version	Datum	Autor/in	Änderung	Begründung	Betroffene Seiten
1	13.03.2023	Imani Dadaeva			

Inhalt

Ihre Ausarbeitung sollte folgende Struktur haben:

Einleitung
1. Anwendungsbereich (Statement of Applicability)
2. Normative Verweise
3. Abkürzungs- und Begriffsverzeichnis
4. Kontext der Organisation
5. Führung
6. Planung
7. Unterstützung
8. Betrieb
9. Bewertung der Leistungen
10. Verbesserungen (KVP – Kontinuierlicher Verbesserungsprozess)

der Aufbau wurde mit der Klasse besprochen

1 Einführung

Dieses Dokument regelt die Vorbeugungsmaßnahmen gegen Cyberangriffe und Datendiebstaht, sowie organisatorische und technische Maßnahmen im Falle eines Cyberangriffs für die KLINIK. Dabei werden die Gesetzte

- DSGVO
- NISG
- Gesundheitstelematikgesetz

Berücksichtigt.

Diese Maßnahmen betreffen alle MitarbeiterInnen der KLINIK.

2 Grundlagen

Einleitung

Dieses Dokument dient als Vorschlag für ein Security Operations Center der Spengerklinik. Es werden unter anderem die technischen und organisatorischen Maßnahmen, die für die Umsetzung dieser Verteidigungslinie gegen Cyberangriffe und Datendiebstähle eingeführt werden soll, beschrieben. Dabei geht man insbesondere auf den Kontinuierlichen Schutz, die schnelle und wirksame Reaktion, der Schutz vor Bedrohungen, erhöhte Sicherheitsexpertise, interne und externe Kommunikation/Zusammenarbeit sowie das interne und externe Einhalten der Compliance-Vorgaben ein.

usw.

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

Das SOC nimmt durch das Security Advisory eine allgemeine Kategorisierung der Gefahrenlage (Kritikalität) von niedrig bis kritisch bei der Schwachstellenbewertung vor.

siehe Anmerkungen zu Punkt 3 (nächste Seite)

Das SOC Überwacht den IKT-Betrieb der Spenger-Klinik 24 Std / 7 Tage, um mögliche Angriffe zu erkennen.

3 Maßnahmen zur Vorbeugung von Cyberangriffen

3.1 Organisatorische Maßnahmen

In diesem Kapitel werden die organisatorischen und technischen Maßnahmen zur Vorbeugung von Angriffen beschrieben.

- Risikoanalyse/ Disater-Recovery-Plan
  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 ein professionelles und erfahrenes 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:
    Leitungsperson für Notfälle: Eine qualifizierte und erfahrene Person in der Organisation wird gewählt, welche mit dem Notfallteam zusammenarbeitet, dieses lenkt und die Vorgesetzte über Änderungen und Fälle informiert.
    Zusammenstellung eines Notfallteams:
    Die erste Maßnahme, die getroffen werden sollte, ist das Zusammenstellen eines Spezialisten- Team, welches für Notfälle, wie bsw. bei einem Ramsomeware- Angriff, zuständig ist. 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.
    ➔ Dokumentierung der gemeldeten Fälle

- 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.

- 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. – Wollte noch was schreiben—Des Weiteren ist die Leitungsperson verpflichtet einen monatlichen Bericht zu verfassen und diesen den Vorgesetzten zu präsentieren.

- Compliance
  Die gesetzten Maßnahmen müssen die Teilbereiche der DSGVO, NISG und GTel-Gesetz decken. Jeder Teilhaber der Organisation ist. Es soll ein Team zusammengestellt werden, welche anhand dieser Richtlinien die Vorschriften für die Organisation zusammenstellt.
  Das Team ist für die Aktualisierung der Organisationsvorschriften zuständig, im Falle neuer Veränderungen bei den Richtlinien DSGVO, NISG und GTel

  Das SOC führt regelmäßig Überprüfungen durch, um die getroffenen Maßnahmen zu überprüfen.

3.2 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.
- Backups: 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?

4 Vorgehensweise beim bestehenden Angriff

In diesem Kapitel werden die organisatorischen und technischen Maßnahmen bei einem bestehenden Angriff auf das System und die Organisation beschrieben.

4.1 Organisatorische Maßnahmen

- Bekanntgabe beim Notfallteam: Je früher der Angriff bekanntgegeben wird, desto schneller können die Maßnahmen eingeleitet werden.
- Bekanntgabe bei Partnerkliniken, sodass aufwändige Fälle weiterverwiesen werden können
- Risikobewertung durch Notfallteam:
    - 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.
    - Das Notfallteam ist verpflichtet die Notfallleitung zu informieren
- Einleitung des Disaster Recovery Plan

4.2 Technische Maßnahmen

- Identifizierung und Isolierung des betroffenen Systems/Rechner:
    - Durch die Netzwerküberwachung könnten Angriffsmuster erkannt und die Quelle des Angriffs ausfindig gemacht werden. Nach der Identifizierung ist es wichtig das betroffene System schnellstmöglich zu isolieren. Handelt es sich um ein Gerät des Mitarbeiters, so müssen folgende Schritte eingeleitet werden:
        - Kontosperrung des Mitarbeiters
        - Die Geräte aus dem Netzwerk
- Bei der Auffindung der Quelle:
    - Sperren des Mitarbeiter Kontos
    - Mitarbeiter- Geräte oder System aus dem Netzwerk entfernen
    - Herunterfahren des Gerätes/Systems
- Backup: Es wird versucht durch das Backup, die daten wiederherzustellen
- Externen Mitarbeiter:
  Wenn das interne Team nicht zur Lösungsfindung kommen kann, muss ein externes Spezialisten-Team engagiert werden. Hierfür sind einige Maßnahmen zu beachten:
    - Jump Host: Das externe Team greift über ein Netzwerk auf den Jump Host zu, um von dort aus mit der Identifizierung und Lösung des Cyberangriffes zu starten. So wird alles mitprotokolliert.