Sehr geehrte Damen und Herren,
werte Schülerinnen und Schüler,

Sie wurden als CISO der Klinik von der KOFÜ zur heutigen Leitungssitzung eingeladen. Die KOFÜ der Klinik ist verunsichert, da Ihnen der Bericht über den Ransomware-Angriff auf das Krankenhaus "Clinic de Barcelona" vom österreichische Bundesministerium für Inneres übermittelt wurde.

20230310_Bericht_Ransomware-Angriff

Sie wurden daher beauftragt, Ihren Vorschlag für ein "Security Operations Center" (SOC) in der Klinik bis zur nächsten Leitungssitzung schriftlich zu übermitteln und persönlich durch eine Präsentation zu erläutern. Die Leitung erwartet von Ihnen, dass Sie die technischen und organisatorischen Maßnahmen, die für die Umsetzung dieser wichtigen Verteidigungslinie gegen Cyberangriffe und Datendiebstähle in der Klinik eingeführt werden soll, beschreiben.

Für Ihre Ausführungen steht Ihnen die Beschreibung der Leistungen zur Verfügung.

Leistungsbeschreibung_Klinik

Ihre Ausführungen sollte folgende Vorteile, die für ein SOC sprechen beschreiben:

- Kontinuierlicher Schutz
- Schnelle und wirksame Reaktionen
- Schutz vor Bedrohungen
- Erhöhte Sicherheitsexpertise
- Kommunikation und Zusammenarbeit (intern & extern)
- Einhalten der Compliance-Vorgaben (intern & extern)

Viel Erfolg!
F. Hoheiser-Pförtner

Ps.: Die Klinik hat einen NIS-Bescheid!

Security Information Center

Dokumententyp	Orginasatorische Richtlinie / Technische Richtlinie
Klassifikation	TLB: ~~red /~~ amber ~~/ green / white~~
Autor/in	5BHBGM, Sophie Payer
Letzte Änderung	13.03.2023
Prüfer/in	Sophie Payer
Geprüft am	
Freigeber/in	
Freigegeben am	13.03.2023
Gültigkeitszeitraum	ab Freigabedatum: 12 Monate
Überprüfungsintervall	3 Monate
Version	1.0
Vertraulichkeit	STATUS: freigegeben

Version	Datum	Autor/in	Änderung	Begründung	Betroffene Seiten
V1	13.03.2023	Sophie Payer	Erstellung		

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

es fehlt die Fußzeile

1 Einführung

Dieses Dokument regelt die Vorgehensweise für die Implementierung und regelmäßige Überwachung eines Datenschutz- und Informationssicherheitssystems für die 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. Dabei verweist das Dokument auf die Gesetze NIS; DSGVO und GTelG.

2 Anwendungsbereich

Diese Verfahrensanweisung betrifft alle Mitarbeiter der Klinik, welche mit Patientendaten umgehen müssen. Daraus erschließt sich, dass der Dokumentenstatus gelb ist, und somit die Weitergabe des Empfängers nur an die ausgewählten Mitarbeiter erfolgt.

3 Grundlagen

Da das SOC 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 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).

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.

5 Gefahrenbeschreibung

Nachdem eine Ransomware Attacke auf die Klinik „Clinic de Barcelona“ erfolgt ist, sollen nun Maßnahmen deklariert werden, damit solches nicht in dieser Klinik passiert. Eine Ransomware-Attacke ist ein Cyberangriff, wo schädliche Software auf das System eingeschleust wird. Diese Software verschlüsselt daraufhin die Daten und Systeme auf diesem System und macht diese daher unzugänglich. Ein solcher Angriff ist oft mit einer Forderung für Lösegeld miteingehend. Das Einschleusen der Schadsoftware kann durch mehrere Wege erfolgen, wie E-Mail Anhänge, Websites, Social Engineering oder auch Schwachstellen in dem System. Social Engineering bedeutet, dass z.B. eine Person abgelenkt wird, und somit Angreifer sich Zugriff auf sein System verschafft.

6 Vorgehensweise Informationssicherheitskonzept

6.1 Organisatorische Maßnahmen

Zur Bildung der organisatorischen Maßnahmen verfolgen wir den PDCA-Zyklus.

- Risikoanalyse
    - Es ist essentiell, dass am Anfang die bestehenden Bedrohungen identifiziert werden. daher muss ein Informationsstand der Mitarbeiter eingeholt werden. Dafür würde sich eine Umfrage zum richtigen Verhalten im E-Mail Verkehr oder auch im Internet eignen. Weiters müssen mögliche Schwachstellen im System identifiziert werden. Dabei ist es wichtig, dass überprüft wird, ob die Gesetze NIS; DSGVO und GTelG eingehalten werden. Es ist außerordentlich wichtig, dass, da es sich um Patientendaten handelt, diese auch zu schützen. Die Risiken, welche mithilfe der Risikoanalyse gefunden werden, müssen daraufhin in Kategorien eingeordnet werden. Dabei erfolgt eine Kategorisierung in hoch (kritische Risiken), mittel (wichtige Risiken) und niedrig (nicht schwerwirkende Risiken)
- Maßnahmen zur Risikominimierung:
    - Nach der Analyse der Risiken müssen Maßnahmen zur Reduzierung dieser gebildet werden.
        - Um die Awareness der Mitarbeiter über Ransomware Attacken aufrecht zu halten, sollten wöchentliche Ausschreibungen über dieses Thema gemacht werden. Weiters sollte einmal im Monat ein Meeting zur Informationsvergabe des aktuellen Standes abgehalten werden.
        - Weiters sollen bei allen betroffenen Mitarbeitern, wie auch neuen Mitarbeitern Schulungen gemacht werden. Dabei geht es um die Sensibilisierung der Mitarbeiter zu den Schwachstellen im System (E-Mail Anhänge, usw.). Es wird dabei auch überprüft, ob der Mitarbeiter die Anforderungen überhaupt versteht und umsetzen kann. Dabei sollte diese Sensibilisierung in mehreren Sprachen umsetzt werden. Da in der Klinik immer mehr Personen arbeiten, welche nicht als Muttersprache deutsch haben. Daher sollten diese Schulungen zumindest in Deutsch und Englisch angeboten werden. In den Schulungen müssen unter anderen Themen wie Phishing, Smishing, richtige Passwörter oder auch den Schutz vor Drittpersonen (Social Engineering).
        - Wenn es zu einer Verletzung des DSGVO kommt, muss innerhalb von 72h dies gemeldet werden. Da es sich hierbei um sensible Patientendaten handelt, kann eine Verletzung der DSGVO zu verherrlichen Folgen führen.

        - Damit die Mitarbeiter aller Abteilungen über den Ablauf bei einer Ransomware Attacke informiert sind, sollen in den Pausenräumen aller Abteilungen ein Vorsorge Ablaufplan aufgehängt werden. Dieser informiert die Mitarbeiter zusätzlich und steigert daher die Awareness.
        - Es ist essentiell, dass alle diese Maßnahmen regelmäßig von einer zuständigen Abteilung überprüft und aktualisiert werden. Bei einer Aktualisierung der Maßnahmen müssen alle Mitarbeiter sofort darüber informiert werden und auf ein Dokument, welche die aktuellen Informationen/ Maßnahmen erfasst, referenziert werden.
- Sicherheitsmanagement
    - Wenn es zu einem Verstoß von Maßnahmen kommt, muss dieser sofort gemeldet werden. Bei einem Verstoß der DSGVO muss dieser innerhalb von 72h und bei einem NIS-Verstoß innerhalb von 3h gemeldet werden.
    - Nach der Meldung des Verstoßes wird sofort die vielleicht beschädigte Software zum Sicherheitsteam gebracht eine Analyse der Situation gemacht. Dabei wird aufgearbeitet, wie es zu dieser Attacke gekommen sein konnte und ggf. werden die Maßnahmen aktualisiert. Weiters muss der betroffene Mitarbeiter erneut geschult werden.
    - Alle Sicherheitsvorfälle müssen in einem Dokument gesammelt werden und die Situationslage beschrieben, wie auch die getroffenen Maßnahmen angeführt werden.
- Compliance
    - Es müssen die gesetzlichen Vorschriften und Richtlinien eingehalten werden (NIS, DSGVO, GTelG). Dabei wird besonders Acht auf die DSGVO gelegt, da es sich um Patientendaten handelt.
    - Es muss zu regelmäßigen Überprüfungen, wie auch Aktualisierungen dieser Richtlinie kommen, damit versichert werden kann, dass sie den aktuellen Anforderungen und Standards entspricht. Bei Aktualisierungen müssen diese in der Änderungshistorie genau angegeben werden, wie auch welche Bereiche verändert wurden.
- Verantwortlichkeiten und Zuständigkeiten
    - Es muss ein Notfallteam zusammengestellt werden, welche bei einer Attacke sofort reagieren kann. Dieses setzt sich auch gut ausgebildeten und qualifizierten Personal zusammen, welches von einer Leitungsperson angeführt wird. Dieses Notfallteam ist eine Unterabteilung der Krankenhaussecurity. Bei einem Angriff muss dieses Team so schnell wie möglich verständigt werden und über die Situation aufgeklärt werden.

Wenn es nun trotz diesen präventiven Maßnahmen zum Eintritt eines Risikos kommt müssen die folgenden Punkte beachtet werden:

- Risikobewertung:
    - Wenn ein Risiko eintritt, muss überprüft werden, ob für dieses schon ein Risikoplan mit Maßnahmen geschrieben wurde. Wenn dies der Fall ist, muss dieser Risikoplan gefolgt werden. Ansonsten wird das Risiko genau analysiert und Maßnahmen dafür festgelegt. Außerdem muss das Risiko bewertet werden, um ein Bild davon zu haben, wie rasch bzw. welche Maßnahmen nötig sind.
- Notfallplan erstellen:
    - Nachdem das Risiko bewertet wurde, muss ein Notfallplan erstellt werden. Dieser Notfallplan kann, wenn das Risiko zuvor schon bekannt war, auch schon vorhanden sein. In dem Notfallplan ist angegeben, welche Meldungsstellen wie schnell

benachrichtigt werden müssen. Außerdem ist ein Notfallteam mit einem Notfallteamleiter aus qualifiziertem Personal angeführt (das CERT Team)

- Auswirkungen auf das System:
    - Je nach Risiko muss die Belastungsfähigkeit des Services eingeschränkt werden, da z.B. eine der Festplatten im RAID System ausgewechselt werden muss.
    - Es wird eine Strategie entwickelt, wie die Qualität des Services auf Erhalten werden kann (Erreichbarkeit).
- Disaster Recovery Plan:
    - Weiters wird auch ein Disaster recovery Plan erstellt, welcher anführt, welche Maßnahmen im Ernstfall durchgesetzt werden müssen, um die kritischen Einrichtungen in der Klinik aufrecht zu erhalten (OP, Intensivstation)

6.2 Technische Maßnahmen

- Um dem Diebsstahl von Patientendaten entgegenzuwirken, können die Daten verschlüsselt werden. Dafür muss die Kommunikation der Daten, wie auch die Datenspeicherung festgelegt werden.
    - Bei der Kommunikation von Daten kann das Public Key Verfahren angewendet werden. dabei haben beide Kommunikationspartnern jeweils einen Öffentlichen und einen privaten Schlüssel. Der eine Kommunikationspartner verschlüsselt die Nachricht mit dem öffentlichen Schlüssel des anderen. Dieser kann daraufhin als einziger die Nachricht wieder entschlüsselt, da er den privaten Schlüssel hat.
    - Bei der Speicherung der Daten kann es bei Cyberattacken dazu kommen, dass die Angreifer sich Zugriff auf die Daten auf der Festplatte schaffen. Um dem Diebstahl der Daten entgegenzuwirken, kann BitLocker eingesetzt werden. Durch BitLocker wird das ganze Dateisystem verschlüsselt und wenn nun die Festplatte selbst gestohlen wird oder sich eine unbefugte Person Zugriff auf die Festplatte verschafft, kann dieser mit den Daten nichts anfangen.
- Weiters kann durch RBAC begrenzt werden, welche Daten anfällig sind. Bei der rollenbasierten Zugriffskontrolle werden die Benutzer in Rollen aufgeteilt. Jede Rolle hat bestimmte Berechtigungen, womit ein Arzt z.B. nicht auf dieselben Daten Zugriff at wie ein Admin. Wenn nun bei einem Arzt eine Ransomware Attacke erfolgt, werden nicht so viele Daten verschlüsselt, als bei einem Admin.
- Weiters können Zugriffskontrollen der Benutzer mithilfe von Chipkarten eingeführt werden. Dabei bekommt jeder Benutzer, welche auf das System zugreifen muss, eine Chipkarte. Diese Chipkarten haben verschiedene Berechtigungen (RBAC). Wenn nun ein Benutzer von Gerät zu Gerät geht (Abteilung zu Abteilung oder Visite zu Visite), muss sich dieser nicht jedes Mal an- und abmelden, dies erfolgt durch die Chipkarte. Dadurch kann vermieden werden, dass sich ein Benutzer vergisst abzumelden und dadurch eine Schwachstelle aufkommt.
    - Wenn nun ein User für 10 Minuten angemeldet ist, ohne Aktivität wird dieser automatisch aus dem System ausgeloggt. Damit wird vermieden, dass, wenn ein Benutzer seine Chipkarte vergisst mitzunehmen, eine Drittperson Zugriff auf das Netzwerk bekommt.
- Bei bestimmten Geräten, welche länger benützt werden, als die Visite- Geräte (z.B. zur Bildaufbereitung beim Röntgen) kommt es zu einer Zwei- Faktor- Authentifizierung. Dabei ist der Computer passwortgeschützt, jedoch der User bekommt bei der Anmeldung noch einen TAN auf sein Arbeitshandy geschickt.

- Außerdem muss ein Logging eingeführt werden. bei dem Logging werden alle Aktivitäten des Netzwerkes in eine Datei protokolliert. Damit kann, bei dem Eintreten eines Risikos, festgesellt werden, woher dieses kam (z.B. über welchen User eine Schadsoftware eingeschleust wurde)
- Eine weitere Risikoquelle sind SQL- Injections. SQL- Injections sind Texteingaben, welche ein SQL- Statement beinhalten. Wenn solch eine Texteingabe z.B. bei der Namenseingabe eines Benutzers eingegeben wird und der Input einfach ungefiltert in die Datenbank gespeichert wird, kann passieren, dass die Datenbank dadurch gelöscht, verschlüsselt oder kopiert wird. Daher muss als Maßnahme eingeführt werden, dass bei allen Inputs eine Textkontrolle durchgeführt wird (Es dürfen keine Anführungszeichen vorkommen). Weiters muss die Datenbankabfragen durch Parameter erfolgen oder bei großen Abfragen aus Stored Procedures bestehen.
- Es müssen regelmäßige Backups durchgeführt werden. Wenn es nun zu einer Ransomware Attacke gekommen ist, sollte man auf ein Backup zurückgreifen können, um die Daten wiederherzustellen.
- Weiters soll bei der Datenspeicherung am Server ein RAID 5 System eingesetzt werden. ein RAID 5 System besteht aus mehreren Festplatten, bei denen die Informationen immer teilweise gespeichert werden. Dadurch kann beim Ausfall einer Platte, die Informationen aus den anderen Festplatten wiederhergestellt werden. Dieses RAID System bietet eine hohe Leistung, welche in einem Krankenhaus gebraucht wird, wie auch eine hohe Redundanz.

Das SOC ist 24 Std. / 7 Tage mit Personen besetzt, die

- Schwachstellen Monitoring durchführen
  - erkennen und Lösungen umsetzten
- Security Advisory
  - Das SOC nimmt durch das Security Advisory eine allgemeine Kategorisierung der Gefahrenlage (Kritikalität) von niedrig bis kritisch bei der Schwachstellenbewertung vor.
- Security incident Rsponse
  - erkennen von Angriffen und Gegenmaßnahmen einleiten

z.B.:

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