Mitschrift vom 07.10.2020

Zusammenfassung der Hauptaussagen des Dokumentes

Es geht hauptsächlich um Disaster Recovery bei denen auch dann bestimmte Punkt wie RPO und RTO beachtet werden müssen. Das Disaster Recovery bezeichnet bestimmte Maßnahmen, die nach einem Ausfall von Komponenten in der IT eingeleitet werden. Dazu gehört nicht nur die Datenwiederherstellung, sondern auch das Ersetzen von nicht mehr verwendbarer Infrastruktur, Hardware und Organisation.

Eigentlicher Inhalt des Dokumentes

Neuer Standard: BSI 100-04

- RPO: Recovery POINT of Object („Rücksteigepunkt “)
- RTO: Recovery TIME of Object
- RTO1: Notbetrieb vorhanden
- RTO2: Betrieb + Restore der letzten Datensicherung vorhanden
- RTO3: Betrieb + Restore + Daten nach erfasst

RTO=Rekonstruktion

Der letzte Zeitpunkt der Sicherung ist eine Punktbetrachtung und somit auch ein Rücksteigepunkt→Letzte Synchronisation der Datenbank
Die Zeit ist ein Ablauf bzw. eine entsprechende Länge

Wenn zwischen RPO und RT1 Daten verloren gehen dann ist dies eher kritischer.
RT02=Die Daten werden zurückgeführt und die Daten von ZP1 beginnend werden die Daten geholt→Rückführung

<u>Bild 1:</u>
Erster Zeitpunkt ist jener Punkt wo eine Sicherung durchgeführt wurde.
Blitzsymbol(in der Skizze)=Jener Zeitpunkt wo es nicht funktioniert.
Minuszeit: ZP1 bis Blitz → Datenverlust
Die Störung ist ZP0.
Datenverlust→ Jener Punkt zwischen ZP0 und ZP1

x-Achse: Zeitpunkte→ ZP1-ZP4: 4 Zeitpunkte
y-Achse: Leistung→ fiktive Höhe (erbringt Leistung unabhängig ob 1 oder 100 Transaktionen)
Jedes System hat eine bestimmte Leistung, die sie erbringt→y-Achse

ZP1= Letzte Sicherung
ZP2=Notbetrieb
Es braucht eine bestimmte Zeit, um wieder in den Betrieb zu gehen und eine bestimmte Zeit, um in den Notbetrieb zu gehen.
ZP3: in Relation zu ZP1
ZP4: mehr Aufwand der Daten→ >100%
ZP4=Die Daten seit der letzten Sicherung und die Daten die verloren gegangen sind müssen

wiederhergestellt werden→ somit doppelter Aufwand und somit 100%

[PMS=Patient Monitoring System]

Man hat nur die Daten der Patienten, aber nicht die Daten der History.
Es gibt Zeiten, wo man Probleme nicht erkennt und somit auch nicht in den Notbetrieb gehen kann.

(Welche Probleme können entstehen und wie kann man es verhindern damit Probleme nicht entstehen?)

Wenn die Kapazität sinkt, braucht es eine Weile, bis dies bemerkt wird.

Es ist immer wichtig bei einer Applikation, dass wenn es ein Problem gibt, man bei Notfallen eine Wiederherstellung bereit hat. Die verlorenen Daten müssen wiederfasst werden und dies ist hoffentlich schriftlich gespeichert. Deshalb wäre ein Log Buch oder sonstiges, wo man alles bzw. das Verlorene wiederherstellen kann, praktisch.

Dokumentation der letzten 24h müssen von den Datenbanken wiederhergestellt werden.

Wiederherstellung bei Absturz (Automatisiert oder Checkliste)
Nachdem das Problem erkannt wurde, müssen Maßnahmen gesetzt werden→Wiederherstellung(Skizze)→ entweder automatisiert oder anhand einer Checkliste

<u>Szenarios:</u>
Szenario Graz: Viele mussten Strafe nicht zahlen, weil Systeme ausgefallen sind
Mögliches Szenario im Spital: hat er die Spritze schon bekommen? → JA/NEIN→ doppelte Dosis → Mord → Wer ist schuld?
→Programmfehler → Programmierer
→ Keine Dokumentation → Krankenschwester

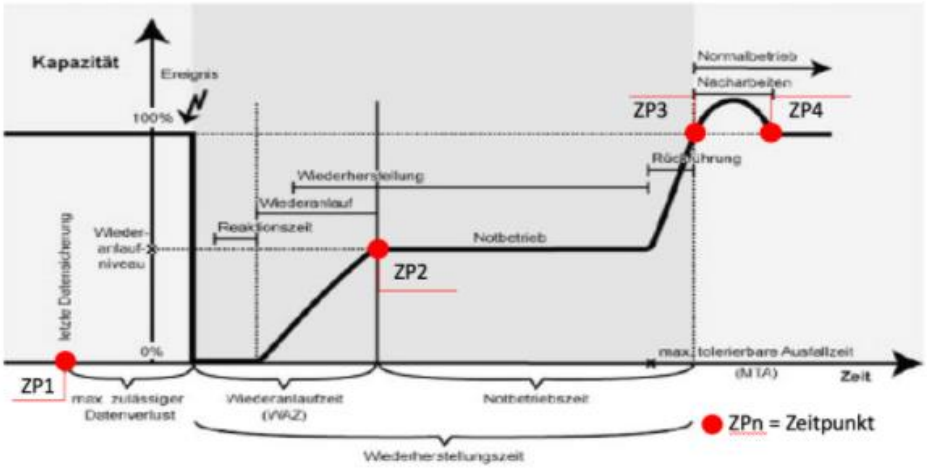
<u>Risikoanalyse:</u>
→ Welche Bedrohungen gibt es: Ausfall, Integrität

Risikoanalyse=Was könnte passieren und was hat es für Auslösungen
Wichtige Aspekte=Wie, Wo, Wann, Was, Wie oft etc. aber auch Verfügbarkeit, Integrität

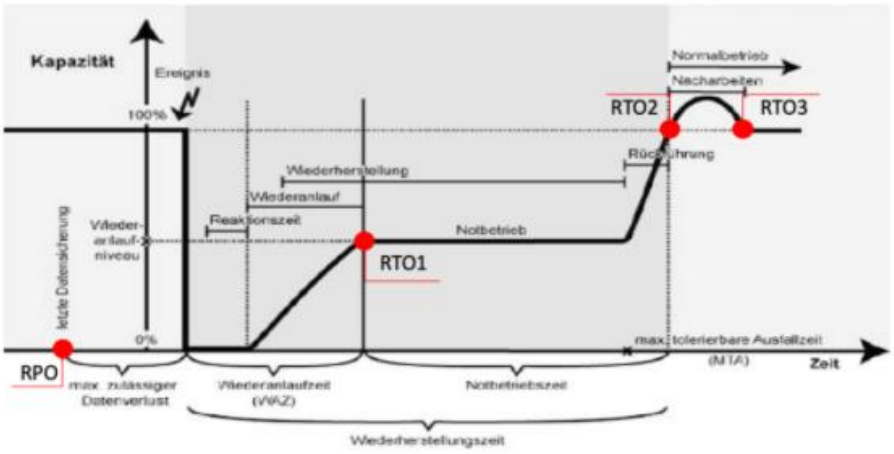
Was nicht auffallen könnte=Manipulation(mit Signatur, Validierung, Vertraulichkeit etc.)
Was auffallen kann=Ausfall, Verschlüsselung

RPO / RTO

Recovery POINT Objective &
Recovery TIME Objective lt. BSI 100-4



Recovery POINT Objective &
Recovery TIME Objective lt. BSI 100-4



Quellen:

https://de.wikipedia.org/wiki/Disaster_Recovery#:~:text=Bei%20der%20Recovery%20Point%20Objective,betr%C3%A4gt%20die%20RPO%200%20Sekunden.

MIS-Mitschrift

Zusammenfassung der Hauptaussagen des Dokumentes

Die Risikoanalyse ist zur Erkennung von potenziellen unerwünschten Ereignisse. Hierfür wird nach dem PDCA-Kreislauf gehandelt und dabei die CIA-Triade berücksichtigt. Die Risikoanalyse wird in regelmäßigen Zyklen durchführt. Die Dauer dieser Zyklen wird durch die Wichtigkeit der betroffenen Objekte bestimmt. Bei den Maßnahmen unterscheiden man zwischen denjenigen, die im Vorfeld getroffen werden (proaktiv), und denjenigen, die im Nachhinein getroffen werden (reaktiv).

Eigentlicher Inhalt des Dokumentes

Risiko = Gefährdung für Patienten & Personal

2 wichtige Aspekte bei der Aufnahme:

1. eindeutige Zuordnung zu der Person erstellen (Person als Patient aufnehmen, Daten speichern, haben wir bereits Daten?, …)

2. Anamnese: welche Beschwerden? Vorerkrankungen? Unklarheiten? → klären mit Unterstützungselemente z.B. Labor & bildgebende Diagnostik

ambulante Behandlung: benötigt keine Aufnahme, ähnlich wie bei einer niedergelassenen Gesundheitseinrichtung

stationäre Behandlung: benötigt Aufnahme und Vorbereitung & Durchführung auf Behandlung/Operation

Entlassung: Informationen für den/die NachbehandlerIn (niedergelassener Bereich bzw. mobile Pflegedienste)

ELGA: gewisse Informationen von einem/r PatientIn erfassen und den behandelnden Ärzte bereitstellen, sofern der Patient dies erlaubt

Netzwerk: 7 Schichten, Switches, Router, WLAN, Client & Server

Risikoanalyse: potenzielle unerwünschte Ereignisse analysieren (Was wäre wenn?/Welche Möglichkeiten gibt es?/wo könnte dies auftreten?/Welche Schwachstellen haben diese einzelnen Systeme?) & dann bewerten (Eintrittswahrscheinlichkeit & Schadensausmaß)

- ➔ alle Objekte identifizieren, die wir betrachten wollen
- ➔ Bedrohungen überlegen
- ➔ Risikoanalyse: wie oft könnte die Bedrohung eintreten & welche Kosten benötigt sie?
- ➔ Kosten = Kosten der Wiederaufnahme, Kontrolle, Herstellung
- ➔ so viele Dinge wie möglich im Vorfeld abhalten
- ➔ Schaden der passieren könnte & Vorbeuge gegenüber stellen

Risikoanalyse: PDCA-Kreislauf (Plan-Do-Check-Act) → Business Continuity/Disaster Recovery (BC/DR)

1. Plan: wo? wie? wann? was?
Gefahren überprüfen
Bedrohung verhindern (Bedrohungskatalog – irgendwo aus der Erfahrung)
Maßnahmen/vorbeugende Maßnahme ableiten

2. Do: Plan durchführen
3. Check: regelmäßige Kontrolle
4. Act: Maßnahmen einsetzen

gewisse Dinge müssen einmal vorbereitet werden und hin und wieder kontrollieren, ob diese Dinge noch vorhanden sind
gewisse Dinge müssen regelmäßig durchgeführt & kontrolliert werden

Risikoanalyse: welche Bedrohungen haben wir? Worauf könnten sie wie wirken? Welche Möglichkeiten haben wir dies zu verhindern? Welchen Schaden löst dies aus? Welche Maßnahmen gibt es?

Risikoanalyse iterativ (in wieder kehrenden Zyklen) durchführen & niederschreiben
→ Wichtigkeit der Objekte bestimmt die Länge der Zyklen (täglich/wöchentlich/monatlich/jährlich)

Maßnahmen: Bedrohungen so gut wie möglich verhindern (100% ist nie möglich)

bestimmte Dingen im Vorfeld erkennen und versuchen zu verhindern

CIA-Triade: Confidentiality (Vertraulichkeit) – Integrity (Integrität) – Availability (Verfügbarkeit)
→ ist immer Teil der Risikoanalyse

Confidentiality: Authentifizierung durch Zwei-Faktor (Biometrie oder Besitz) und Rollenverteilung

damit das System nicht ausfällt: Redundanz
→ mehrere Netzwerk-Verbindung/gleiche Rechner/Switches/Router/…

Maßnahmen einsetzen → muss immer protokolliert und kontrolliert werden

2 Arten von Maßnahmen:
1. Proaktiv: Maßnahmen, welche im Vorfeld getroffen werden
2. Reaktiv: Maßnahmen, die nachher getroffen werden

MIS-Mitschrift

Zusammenfassung der Hauptaussagen des Dokumentes

NISG= Netz- und Informationssicherheitsgesetz -> betrifft alle kritischen Bereiche. GDA wird vom Innenministerium dazu verpflichtet sich an NISG zu halten und hat 3 Jahre Zeit, um einen Nachweis zu erbringen. Dieser Nachweis kann durch ein Audit einer qualifizierten Stelle erfolgen. Für die Einhaltung des Gesetzes müssen 2 Arten von Maßnahmen getroffen werden, welche im PDCA-Zyklus ständig verbessert werden müssen -> Risikominimierung

Organisatorische Maßnahme: Wie soll ein sicherer Datenverkehr gewährleistet sein?

Technische Maßnahme: Einspielung von Sicherheitszertifikaten

Zugriffschutz: Stellt sicher, dass ausschließlich berechtigte User/Personen durch ihr Passwort Zugriff auf bestimmte Dienste/Räume haben.

Zutrittsschutz:
Zutrittskontrolle meint im Datenschutz, Maßnahmen zu ergreifen, die verhindern, dass unbefugte Personen den physikalischen Zutritt zu Datenverarbeitungsanlagen erhalten.

Eigentlicher Inhalt des Dokumentes

NISG = Netz- und Informationssicherheitsgesetz -> betrifft alle Sektoren, die zur kritischen Infrastruktur gehören wie z.B. Gesundheitssystem

Ein Gesundheitsdienstanbieter wird als Betreiber des wesentlichen Dienstes angesehen und wird über die Kritikalität des Dienstes über einen Bescheid aufgeklärt. In Deutschland sind Organisationen selbst dafür verantwortlich zu ermitteln, ob sie vom NISG betroffen sind oder nicht. Dahingegen stellt in Österreich das Bundesministerium für Inneres diesen Bescheid aus. Der Innenminister darf dabei qualifizierte Stellen (Überprüfungsstellen) wie z.B. TÜV benennen, die die Einhaltung der Gesetzte sowie Verordnungen von den Betreibern überprüft (auditiert).

Audit= durchgeführte Überprüfung einer qualifizierten Stelle, die in der Lage ist (fachlich), ein Unternehmen auf die Erfüllung von Standards, Gesetzen und Richtlinien zu prüfen

Bei Erhalt des Bescheids hat das Unternehmen eine bestimmte Einspruchsfrist, in der begründet werden kann, dass man z.B. nicht unter das NISG fällt. Anschließend wird dieser Einspruch von unabhängigen Richtern überprüft und entschieden, ob das Gesetz für die Organisation in Kraft tritt oder nicht. Nachdem das NISG in Kraft getreten ist, hat der Betreiber 3 Jahre Zeit, um einen Nachweis an das Innenministerium zu übermitteln, welcher bestätigt, dass das Gesetz zur Gänze eingehalten und erfüllt wird.

Zur Erfüllung des NISG müssen vom Unternehmen organisatorische Maßnahmen definiert werden, welche anschließend auch technisch umgesetzt werden müssen (TOMs). Beispiel:

- Maßnahme organisatorisch: Erstellung einer internen Richtlinie: Tür 22 darf zwischen 12 und 13 Uhr nicht betreten werden
- Maßnahme technisch: Die Chipkarte der befugten Personen wird so umprogrammiert, dass sie in dieser Zeit ungültig ist

Factsheets unter https://www.nis.gv.at beschreiben Bereiche, die in verschiedenen Normen versucht haben, die vorhandenen Risiken auf bestimmte Bereiche einzugrenzen

Beispiel:

Es liegen Daten vor. Diese müssen zunächst klassifiziert werden (Feststellung der Kritikalität) -> Einteilung in nicht kritisch, mäßig kritisch, kritisch. Kritische Daten unterteilen sich dabei in:

- Personenbezogene Daten
- Unternehmensinterne relevante Daten die nicht personenbezogen und dennoch kritisch sind

Zunächst betrachtet man potentielle Risiken die auf das Unternehmen wirken. Wenn das Risiko von Datenmissbrauch besteht muss sich das Unternehmen Gedanken machen, wie man dieses minimiert. Eine Möglichkeit wäre die Verschlüsselung der Daten -> hier ist wichtig, dass man definiert wie diese Verschlüsselung intern aussehen soll = organisatorische Maßnahme. Nachdem organisatorische Maßnahmen definiert wurden, sollen diese nun technisch umgesetzt werden. Eine technische Maßnahme wäre in diesem Fall, dass der Datenverkehr nur noch über https laufen würde. Für eine optimale Sicherheit ist es essentiell, dass technische und organisatorische Maßnahmen miteinander kombiniert werden.

PDCA-Zyklus ->Qualitätsmanagement

P: Plan = Planung von Maßnahmen, die ein Risiko minimieren sollen (organisatorisch)

D: Do = Durchführung der geplanten Maßnahme (organisatorisch/technisch)

C: Check = Wurde durch die Maßnahme das Risiko minimiert?

Act: Reaktion auf das Ergebnis aus der Check-Phase

Zugriffschutz: Stellt sicher, dass ausschließlich berechtigte User/Personen durch ihr Passwort Zugriff auf bestimmte Dienste/Räume haben.

Zutrittsschutz:
Zutrittskontrolle meint im Datenschutz, Maßnahmen zu ergreifen, die verhindern, dass unbefugte Personen den physikalischen Zutritt zu Datenverarbeitungsanlagen erhalten.

Nis.gv.at → Factsheets

NIST CYBER SECURITY FRAMEWORK: Wichtig für amerikanische Organisationen, eher unwichtig, wenn das Unternehmen nur in Österreich ist. Kann man nutzen, muss man aber nicht.

https://www.nist.gov/cyberframework

CIS CSC: Center for Internet Security, hilft bei der Planung die Sicherheit in der Organisation zu verbessern. Ist nicht verpflichtend. Vermehrt in Nordamerika

https://learn.cisecurity.org/control-download

BSI: Bundesamt für Sicherheit und Informationssicherheit, hat mehr Relevanz als die anderen 2, da Deutschland ein Nachbarsland ist.

https://www.bsi.bund.de/DE/Home/home_node.html

Österreichische Informationssicherheitshandbuch: Ist das wichtigste von allen, da es auf den Rechtsrahmen von Österreich zugeschnitten.

https://www.sicherheitshandbuch.gv.at/

NIS Gesetz ist das Gesetz, was man umsetzen muss. Muss umgesetzt werden bis zur Deadline → Muss alle 3 Jahre überprüft werden. Ein Audit prüft, ob die Umsetzung dem Gesetzt entspricht. Das Audit muss eine staatlich qualifizierte Stelle sein und kann nicht ein Selbstaudit sein.

https://www.nis.gv.at/NIS_Fact_Sheet_2018_08_3_0.pdf

https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00078/fname_710319.pdf

2 Möglichkeiten für die Umsetzung:

- Organisatorische Maßnahmen
- Technische Maßnahmen

SOP: Standard Operation Procederes

MIS-Mitschrift

Zusammenfassung der Hauptaussagen des Dokumentes

Das NIS-Gesetz findet man unter:
www.nis.gv.at

Den IT-Grundschutz findet man unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=5

Das österreichische Informationssicherheitshandbuch findet man unter:
https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf

Den NIST findet man unter:
https://www.nist.gov/

Hier findet man alle Informationen, um Gesetze Genüge zu tun.

Eigentlicher Inhalt des Dokumentes

NIS: Mapping-Sheets: fact sheets

Das NIS ist in 11 Kategorien geteilt, damit Informationssysteme umgesetzt werden können. Man muss diese 11 Kategorien erfüllen, Hilfestellung von gängigen Standards.

Normen: ISO27001 Sicherheitsmanagement, BSI IT-Grundschutz (D) und das Ö. Informationssicherheitshandbuch. → kostenpflichtig

Beim Grundschutz muss man beachte, dass dieser auf Deutschland ausgelegt ist, d.h., dass diese Rechtsnormen nicht für Österreich anwendbar sind. (nur österreichische und EU Normen). Jedoch kann man das österreichische Recht mit dem Grundschutz ergänzen.

Weiters sind IHE oder FHIR amerikanische Standards. Diese referenzieren Gesetzgebungen der USA → HIPPA (Health Insurance Portability and Accountability Act of 1996) → NIST

Gesetze haben im europäischen Raum Verordnungen, die unter Richtlinien auf uns wirken. Gesetze, die vom EU-Parlament (Verordnung) beschlossen werden, müssen nicht ins lokale Recht überführt werden. Der gesetzliche Rahmen sagt, dass man sich an diese Gesetze halten muss. Wiederum ist es bei Richtlinien so, dass diese ins lokale Recht überführt werden müssen. Die EU gibt vor und die Länder führen ein. So war die DSVGO einmal eine Richtlinie, wurde dann aber auf Verordnung geändert. In Zukunft wird mit hoher Wahrscheinlichkeit auch das NIS-G zur Verordnung (jetzt Richtlinie).

Rahmenbedingungen sind zu beachten, der Rechtsrahmen liegt hier in der DACH-Region (=Deutschland, Österreich und Schweiz).

FHIR ist stark HIPPA lastig, hier muss geschaut werden, ob er für den europäischen Kontext ausreicht, sonst muss dieser angepasst werden.

Aufgabenstellung:
Separation eines Netzwerks
Das Spital muss geschützt werden, das Spital hat ein Problem mit dem Netzwerk, da es flach ist (Problem würde alle PCs im selben Netz angreifen). Deshalb: Separation in verschiedene Netze

Vorgangsweise:
Separation /überlegen um Risiken zu minimieren
2 Aspekte:
→Plan erstellen (organisatorische und technische Maßnahmen)

→organisatorische: Mapping-tabelle (Bedrohungen, Separation)

→Prozess erstellen (Team sollten sich 1 mal im Monat treffen) → dies ist jedoch ergänzbar: Gefahr im Verzug (Problem = sofort treffen) → jemand muss das Risiko erkennen → Entscheidung ob es ein Notfall ist oder keiner? → international ein Problem oder ein Fehler der immer schon da war oder neue Situation, weil sie nicht im Grundschutzhandbuch steht → Risko muss bewertet werden → Entscheidung ob genügend Zeit vorhanden ist → Frage muss sich gestellt weden, ob die organisatorischen und technischen Maßnahmen ausreichen → wenn nein, dann diese verändern

→Wenn es ein Gefahr in Verzug ist dann, business continuity oder disaster recovery (Kategorie 10 und 11)

→Prozessbeschreibung: kritikal oder nicht kritikal → Ableitung ob Maßnahmen reichen

Aufgabenstellung 2:
Entwickeln Sie ein Vorgangsmodell zu Homeoffice Sicherheit

Vorgehensweise 2:
organisatorische und technische Maßnahmen → VPN (hier kann jemand auf den Laptop zugreifen, unerlaubte Benutzung, sofort im gesamten Netz) → Lösung: biometrische (körperlich), Zwei-Faktor-Authentifizierung (Handy), Personenerkennung
Internetanschluss → Mobile Access, Endpoint-Protection (Antivirus etc…), Rechte einschränken

→nichts lokal speichern → Daten können wegsein (Laptop gestohlen=
→Storage → hier muss erst jemand reingelangen → fällt dieser jedoch aus, entsteht ein problem, deswegen: Redundanzen

→Terminal-server: lokale PC, dient nur als Eingabeeinheit über Tastatur, Maus und Bildschirm, alles andere über Server-Farm im Rechenzentrum

→kein Netzwerk = nichts arbeiten

→immer die Fragen stellen: Was könnte sein?, Was wäre wenn?, Wie wollen wir es verhindern

→merken: WENN ICH DER PATIENTIN BIN, DANN WILL ICH NICHT, DASS XYZ PASSIERT

→Separation ist immer ein guter Ansatz zB. in medizinische (Labor, Röntgen…), Hausverwaltung, Administration

→auch in Prioritäten: PRIO1, PRIO2, PRIO3 → kann ausfallen, Patientenadministration darf hier aber nicht laufen, sowie Küche, Reinigung, Apothekenbestellungen

Oder man seperated nochmals in Prioritäten und gibt ihnen verschiedene Prioritäten

Überlegen:

Was ist die Aufgabenstellung?

Was muss ich lösen?

Was ist das Ziel?

Matura:
→Beschreibe mit Unterlagen, welche orginasatorische und technische Maßnahmen ich nehmen sollte

→auch erklären: Warum sind Endpoints wichtig?, Warum Netzwerke unterteilen?, Wie komme ich auf dies? → Risikoanalyse → medizinische, technische, verwaltungs-, Prozesse, → unterscheiden ob wichtig oder weniger wichtige → zusätzliche Separation

MIS – Mitschrift

Um das Risiko zu minimieren ➔ flaches Netz entfernen und in Bereiche aufteilen z.B. Geräte, Verwaltung, Öffentlichkeit

Kritikalität pro Segment: niedrig, mittel, hoch

Reifegradmodell (diverse Modelle im Internet):

- 0: keine Maßnahmen, nichts geplant, …
- 1: Situativ / Ad-hoc
- 2: Wiederholbar
- 3: Definiert
- 4: Überprüft
- 5: Optimiert / wird kontinuierlich verbessert

Endgeräte zusammenzählen: Werden Sie benötigt, um den Betrieb zu gewährleisten?

Klinik: Unfall, Notfall, Röntgen, Labor

- Stationen, auch Intensivstation
- Entbindungsstation mit dazugehöriger Neologie
- Blutreinigung
- Welche Stationen, sind wann im Betrieb?

Bei einer Aufgabenstellung hat man nur eine Momentaufnahme. Wie würde ich es organisieren, wenn ich es jetzt umsetzen müsste? Habe ich Informationen, die mir helfen können (NIS, Handbücher etc.). Kein Copy & Paste, da man das auf die Situation anpassen muss!

Arten von Endgeräten:

- IT-Endgeräte
- Medizinprodukteendgeräte
- Steuerungselemente für Klima, Heizung und Lüftung und Warmwasser,
- Ver- und Entsorgung

Gesamttechnik im KH:

- Medizintechnik
- Betriebstechnik
- IKT (Informations- und Kommunikationstechnik)

Brauche ich alle für den Betrieb eines Spitals?

Aus der Angabe erkennt man eine gewisse Kritikalität, ansonsten trifft man Annahmen. Welche der Station haben wir 24h/365 Tage aktiv. Welche Stationen und Ambulanten werden nur tagsüber betrieben? → Wichtig für die Risikoanalyse!

SLA = Service-Level-Agreement

Bsp.:

- SLA: Reparatur innerhalb 6h
- Betriebszeit: Mo-Fr, 8-16 Uhr
- Fehler: Mi, 15 Uhr
- Behebung bis Do, 13 Uhr

Ausfallsicherheit wichtig, da oftmals die Zeiten, die in der SLA definiert sind, zu lang sind.
Z.B. IT-Ausfall im KH, 3h → Katastrophe

Verschiedene Levels der SLA:

- Gold: max. 3h Ausfallszeit, aufgrund NIS: Wenn ein wesentlicher Dienst durch einen Fehler oder Angriff in Mitleidenschaft gezogen wurde und die Leistung nicht erbracht werden kann, muss man der NIS-Behörde nach 3h eine Meldung erstatten.
- Silber: 4h
- Bronze: 6h

Zeitfaktoren:

- Nicht gesetzliche
    - Mean Time Between Failures: Noch nicht gesetzlich verankert
- Gesetzliche:
    - Data Breach Notification: nach 72h muss die Behörde informiert werden
    - Medizinproduktegesetz/-verordnung: Nach einem Unfall oder beinahe Unfall, ist die Behörde unverzüglich zu informieren.

MIS-Mitschrift

Das Ziel ist es immer die NISG zu benutzen; und man soll nicht wortwörtlich kopieren, sondern sinngemäß anpassen;

Prioritäten setzen; mit der Summe der Bedrohungen, die es gibt, geht es sich zeitlich nicht aus; man sucht sich Dinge aus, welche für die Aufgabenstellung am wichtigsten sind; CIA-Triade muss immer abgedeckt werden; man muss niederschreiben, wie man sich vorstellt, wie es umgesetzt wird; Organisatorisch und technischer Teil; muss klar ersichtlich sein;

Begriff Dokumentenlenkung: das Dokument bekommt:

- Wer hat es Dokument geschrieben/Autor
- Freigegeben von
- An wen geht es
- Traffic Light Protocol (Farben haben eine unterschiedliche Aussagekraft; man verwendet meistens vier Farben;
  Rot: man darf es auf keinen Fall weitergegeben werden
  Gelb: man darf innerhalb der Organisation weitergeben;
  Grün: man darf es an eine gewisse Gruppe weitergeben
  Weiß: es ist für die Öffentlichkeit verfügbar

Sagt aus, was der Empfänger des Dokuments machen darf z.B. Vertragspartner weiß, wie man damit umgehen kann; Muss beim Dokument, das man schreibt drauf stehen

NSIG: Verfügbarkeit ist am wichtigsten; 100% Schutz ist nicht möglich;

Es gibt zwei Gruppen auf die die Regeln zutreffen: Administratoren, Anwender

Bei Software: auch Entwickler

Verfügbarkeit: messbar; Vertrag mit Kunden (intern OLA, extern SLA) -> Vertrag/Dokument mit Kriterien die Kontrollieren ob die Leistungen die man bekommt den Zielvorgaben (Messung) entspricht; zum Beispiel 3h nach Ausfall in der Betriebszeit: wenn 16 Uhr Ausfall; bis 17 Uhr Dienst → man kann noch bis nächsten Tag inlusive 2 Stunden am Problemarbeiten;

es ist wichtig, dass technischen Maßnahmen in einer Organisation überprüft werden;

Beispiel: Feuernotfallplan an der Tür: Bacherplatz ist eine Baustelle: Plan stimmt nicht -> PDCA -> Entweder kontinuierliche Überprüfung oder Alerting, dass Plan nicht funktioniert;

Antiviren-Programm: man sollte auch prüfen, ob die dieses den Anforderungen entspricht; wie oft gibt es doch Viren; wenn es zu viele Meldungen gibt → falsche Konfig, schlechtes Programm;

Org: auf allen PC ist ein Antivirenprogramm installiert; man kann es nicht deaktivieren; Personen im Home-Office müssen sich min. 1 mal in der Woche mit dem Netz der Org verbinden um die neuste Organisation

Technisch: immer, wenn man es verhindern kann, wenn man technische Einstellungen umschiffen kann (Passwörter ein Jahr Gültigkeit; 12-15 Buchstaben und Zahlen; Großklein; keine Wörter; Zeichen etc.)

Möglichkeit zum Unterbrechen von Applikation: Webapplikation

Immer wenn man das Unternehmen verlassen, wird immer 2. Faktorauthentifizierung eingeschaltet; man kann auch nur Smartkarten verwenden; eventuell mit Fingerprint;

Oder mit Tokenverfahren