Besprechungsprotokoll

Thema	
Ort	C2.06
Datum/Zeit	09.09.2021 13:30 -
Teilnehmer	5AHBGM, Pirker, Hoheiser
Verfasser	Elias Brandtner, Vincent Aigner

- **Agenda**
  - **Datenschutz**
  - **Traffic Light Protokoll**
  - **DSGV**
- **Protokoll**

Traffic Light Protocol: Wer darf mit Infos was tun

- Farbe rot: Information darf nur im inneren Kreis weitergegeben werden (Also bei einer Besprechung nur an die Anwesenden)
- Farbe gelb: Information darf innerhalb der Organisation ausgetauscht werden
- Farbe grün: Information innerhalb gleicher Infrastruktur darf weitergegeben werden
- Farbe weiß: bedeutet public (ist auch für Medien und Presse verfügbar)

Unsere Kommunikation ist prinzipiell gelb.

CIA Triade: Confidentiality, Integrity, Availability -> Sind voneinander abhängig

Gesundheitsdaten (personenbezogen)-> sind wegen DSGV. zu schützen

In DSGV wird als 1. die **Vertraulichkeit** angesprochen
-> Verschlüsselung und nur durch Schlüssel lesbar
-> Berechtigungsmodel z.B. in FHIR

Compliance: Nachweis, dass das was ich programmiert habe auch funktioniert

2. **Integrität**: Wenn Befund falsche Informationen -> Problem

Durch Hash-> Signieren – Algorithmus von Daten -> Schauen, ob Daten noch gleich sind

3. **Verfügbarkeit**: Wenn ich Daten nicht habe -> Kann Leistung nicht erbringen -> Daten wären nutzlos

---

Technische und organisatorische Maßnahmen können, müssen aber nicht gleich sein

DSGV enthält auch: TOM-Technische Organisatorische Maßnahmen

Der der den Auftrag gibt, ist für Daten verantwortlich, weil er will das Daten verarbeitet werden

Auftraggeber ist für Daten verantwortlich -> wenn man draufkommt als Auftragnehmer, dass TOM nicht eingehalten wird MUSS man dem Auftraggeber das sagen

Vertrag sollte schriftlich sein -> mündlich würde auch zählen, aber Risiko das jemand sich nicht erinnert

---

Verordnung: Gesetz, das jedes Land einzuhalten hat – Einheitliches Recht für alle Mitgliedsstaaten

Als Programmierer muss man bei Produkt nur auf eine Sache achten

Richtlinie: Nationales Recht muss umgesetzt werden und die Richtlinie befolgen – Kann von Land zu Land unterschiedlich sein

Gesundheitstelematikgesetz: Verlangt von GDAs dass der Transport von Daten verschlüsselt sein muss

Identity Provider: z.B. Bürgerkarte, Githubs OAuth, Google

Dienst, der die Identität eines Benutzers speichert und verifiziert.

Handysignatur – Höhere Qualität der Prüfung durch Ausweis…

Protokoll MIS

Autor 1	Laura Dabrowska
Autor 2	Basmala Elsayad
Datum	12.10.2021
Thema	Verfahrensweise für ein Krisensicherheistmanagement; NIS-Gesetz
Beginn	16:05
Ende	17:05

Inhaltsverzeichnis

Inhalt

Allgemein

Technische Maßnahmen benötigt, um bestimmte Sicherheit zu erreichen.

CIA-Triade: Vertraulichkeit – Integrität – Verfügbarkeit

Gesamte Prozesse betrachten -> in Summe niemals 100%ige Sicherheit erreichbar -> Verfügbarkeit bestimmter Prozesse abstreichen

Herangehensweise: Welche der hier behandelten Assets sind notwenig, um diesen Geschäftsprozess mit bestimmten Sicherheitsniveau aufrechtzuerhalten? -> z.B. Ambulanz: abhängig von Anamnese -> Triage bei Kliniken -> Triage immer verwendet, um verschiedenste Problemfelder medizinisch behandeln zu können (nicht first in-first out wie im extramuralen Bereich). Organisatorische Rahmenbedingungen müssen in IT mitberücksichtigt werden. Welche Ambulanzen sind unbedingt aufrechtzuerhalten / Welche können abgeschalten werden? Wir liefern Infrastruktur -> Normalsituation und Ausnahmesituation (um bestimmtes Niveu halten zu können; nicht einheitlich)

NIS-Gesetz: Welche Bedrohungsbilder wirken auf Netz- und Kommunikationsbildern?

Ambulanz – Stationäraufnahme

IT-Unterstützung verschiedenster Prozesse liefern -> welche Konsequenzen hat das für die wesentlichen Personen, wenn

- unsere Komponenten ausfallen oder Inhalt der Informationen, die wir zur Verfügung stellen, nicht verfügbar ist, oder
- der Verdacht ist, dass die Integrität gefärdet wurde oder
- wenn bestimmte Informationen über den gesundheitszustand bestimmter Personen pubik werden (Vertraulichkeit gefärdet)

Schutz der CIA-Triade sehr wichtig wegen NIS, Dsgv, Elga, … -gesetzen

Triage: medizinische Notfälle schneller behandeln
Warteschlangen Liste zwar möglich, aber nicht sinnvoll (zb. Kinder immer zuerst)
Welche Ambulanzen sind wichtiger als andere bzw. welche vernachlässigt werden?
Normalfall oder Ausnahmesituation
Wesentliche Sichtweisen eines Krankenhauses:

- Ambulanz
- Stationär: viele unterstützende Prozesse (Probleme bei der Essensgabe, Stromausfall, Probleme bei der Medikation)

Wer ist betroffen, wenn etwas ausfällt?
Verfälschung von Informationen (Integrität gefährdet)
Publikation von vertraulichen Daten
Priorität ableiten

➔ Faktoren, die eingeplant werden müssen, bei der IT-Infrastruktur Planung

Verschiedenste Modelle, um Vorgangsweise zu unterstützen:
internation: Modelle des Informatiosnsicherheitsmanagementsystems (ISMS) -> Ansammlung verschiedener Normen

Auftraggeber in versus Auftragnehmer -> versuchen, gemeinsames Bild zu erhalten und herauszufinden, wie sie Probleme verhindern

andere Modelle für NIS: Vergleich, wie verschiedene Länder verschiedene Herangehensweisen angehen

Gesetzgeber gibt Liste -> keine Eingrenzung

Managementsystem … Unterstützt Unternehmen im Sinne des Erreichens von Zielen auf hohem Niveau

- Top-Down-Modell: Management gibt vor -> alle machen unten nach
- Button-Up-Modell: handelnde Personen (Operator) arbeiten im Umfeld, erkennen, dass bestimmte Dinge umgesetzt werden sollen, setzen es um, liefern zum Management hinauf

Unsere Überlegungen: Stamdard 7000: Vorgangsweise, die interntaional anerkannt ist und in verschiedenen Dokumenten zu finden ist: zwei davon: BSI, 200er Serie, 4 Dokumente (Deutschland),

Business Continity Planing (BCP): Wer was wann, in welcher Qualität, welcher Zeit, wie lange darf es maximal stehen, …

DRP: etwas ist ausgefallen -> bei Desaster: in welcher Form versuche ich, ein bestimmtes Niveau wieder zu erreichen (Intensivstation -> bei Ausfall werden Informationen zwischengespeichert); Wie kommt man dann wieder zu den Daten? -> Notsystem??

SKKM (Staatliches Krisen- und Katastrophenschutzmanagement) -> bestimmte Dinge, die eintreten können, sind nicht von alleine bewältbar -> brauchen staatliche Hilfe (Blaulichtorganisationen) Ausnahmesituation in einer Ausnahme: Wenn Katastrophe eintritt, muss jemand sie ausrufen (KatastrophenverantwortlicheR) -> muss Organisation in Katatstophenmodus schalten (200‘4 BSI) -> bestimmte Systeme über alle gleichgefahren; Einsatzleiter + 7 Personen (Stabsoffiziere, S1-S7) darunter, die bestimmte Aufgaben haben, Dinge zu erledigen + Vorbereitungen

S1: Zuständigkeit: Personal -> Leute dazuholen + Disposition

Ergänzung

Triage … Einteilung der Verletzten (bei einer Katastrophe) nach der Schwere der Verletzungen

NIS-Gesetz … Netz- und Informationssystemsicherheitsgesetz

Informationssicherheitsmanagement
Informationssicherheitsmanagement ist ein komplexer Prozess der Steuerung von materiellen, konzeptionellen und menschlichen Ressourcen mit dem Ziel, den Anforderungen an die Aspekte Auftragserfüllung, Vertraulichkeit, Integrität und Verfügbarkeit einer Organisation angemessen zu entsprechen.

Andere Länder gehen es anders an, andere Normen -> Unsicherheit bei der Gesetzlage

➔ **Aufgabe ist es herauszufinden welcher der aufgelisteten Normanwendungen sinnvoll ist**

Managementsystem

Ein Managementsystem hilft einer Organisation dabei, Ziele umzusetzen. Und das auf eine systematische Art und Weise. Das Ergebnis ist ein System, in dem alle Beteiligten eingebunden sind und an dessen Erstellung auch alle mitgearbeitet haben. Je nachdem, welchen Schwerpunkt die Ziele haben (Umwelt, Qualität, Sicherheit…) handelt es sich um ein Umweltmanagementsystem, Qualitätsmanagementsystem, Sicherheitsmanagementsystem.

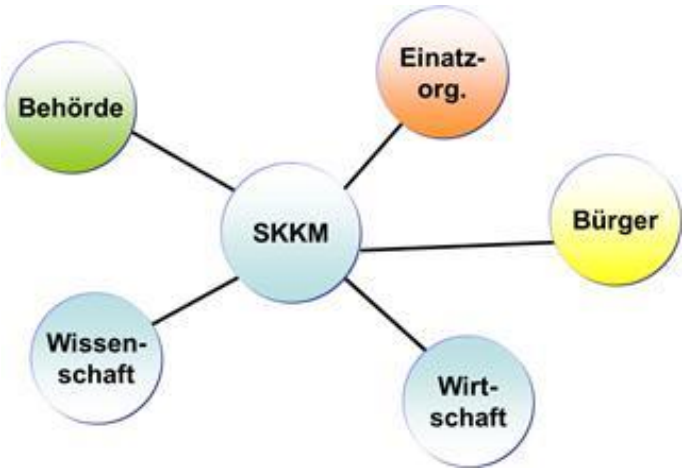
Top-down und Bottom-up

Bei der Top-Down-Planung legt der Auftraggeber Inhalte, Budgets oder Termine als Rahmen des Projekts fest, ohne dass einzelne Details bereits ausgearbeitet sind. Die Projektplanung strukturiert dann diese groben Vorgaben bis hinab zu einzelnen Werken (Lieferobjekten, Produkten), Kostenpositionen und Vorgängen. Der Vorteil dieser Herangehensweise ist, dass die Planung exakt auf bestimmte Zielgrößen hin erfolgen kann. Der Nachteil besteht darin, dass die Ergebnisse der detaillierten Planungen in Widerspruch zu den Vorgaben stehen können und es keine einfache Lösungsmöglichkeit für diese Widersprüche gibt.

Die Bottom-up Planung stellt das Gegenteil der Top-down-Planung dar. Die Planung beginnt auf der untersten Hierarchieebene und bewegt sich dann schrittweise aufwärts, also *von unten nach oben*. Jede Ebene plant ihre Ziele und Maßnahmen und leitet ihren Teilplan an die übergeordnete Ebene weiter. Dort werden die Teilpläne koordiniert, kontrolliert, integriert, ergänzt und wiederum an die nächst höhere Ebene weitergeleitet. Der Aggregationsgrad nimmt dabei stetig zu. Am Ende des Prozesses steht die strategische Planung für das gesamte Unternehmen.

Die internationale Norm **ISO**/IEC **27001** beschreibt ein Informationssicherheits-Managementsystem (ISMS). Ein Managementsystem besteht aus Leit- und Richtlinien, Prozessen und Verfahren, Dokumenten und Aufzeichnungen, Kontrollmechanismen und Leistungsbewertungen sowie aus Maßnahmenzielen und Maßnahmen.

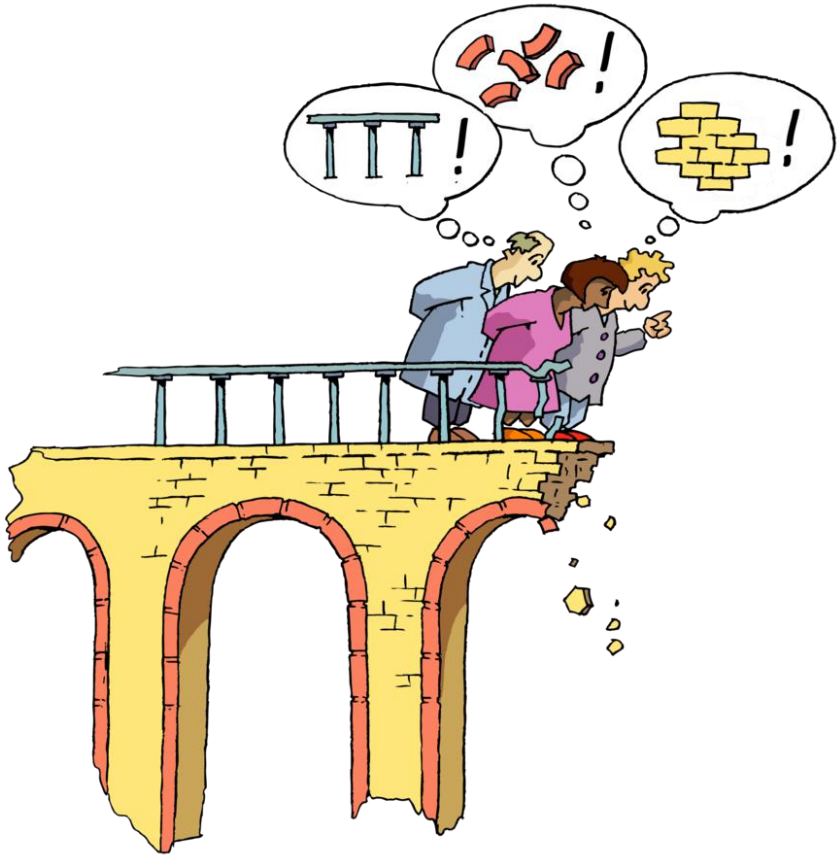
SKKM



Bei Krisen und Katastrophen besteht erhöhter Koordinationsbedarf, der in Österreich durch das SKKM gewährleistet wird. Die Geschäftsstelle ist im BMI angesiedelt. Das SKKM ermöglicht eine effiziente Katastrophenhilfe im In- und Ausland, durch die Zusammenarbeit aller zuständigen Stellen des Bundes mit den Katastrophenschutzbehörden der Länder sowie den Hilfs- und Rettungsorganisationen.

Protokoll MIS

Autor 1	Domenic Melcher
Autor 2	Leon Kosnar
Datum	22.09.2021
Thema	Risikoanalyse: Business Continuity Plan und Disaster Recovery Plan
Beginn	15:15
Ende	17:05



CIA-Triade

Das Confidentiality, Integrity, Availability Prinzip (deutsch: Vertraulichkeit, Integrität, Verfügbarkeit) bezeichnet in der Computerwelt drei wesentliche Grundbedrohungen der Informationssicherheit. Zu diesen drei Bedrohungen zählen der Verlust der Verfügbarkeit, der Integrität und der Vertraulichkeit von Daten. Um informationstechnische Sicherheit zu erlangen, ist die Abwehr dieser Grundbedrohungen durch angemessene, aber wirksame Maßnahmen zu verstehen.

SLA/OLA:

- SLA: extern
- OLA: intern
- Service level Agreement
- Organisation Level Agreement
- SLA: Wer hat welche Leistungen zu erbringen
- OLA: Welche Dienste sind notwendig, um sicherzustellen, dass Kernprozesse funktionieren.

BIA:

- Welche Bedrohungen können Auswirkungen auf unsere Business-Abläufe haben (Impact) (zB: OP)
- -> Welche sind Schützenswerter?
- Zu beachten: Basisdienste, auf denen die Abläufe basieren

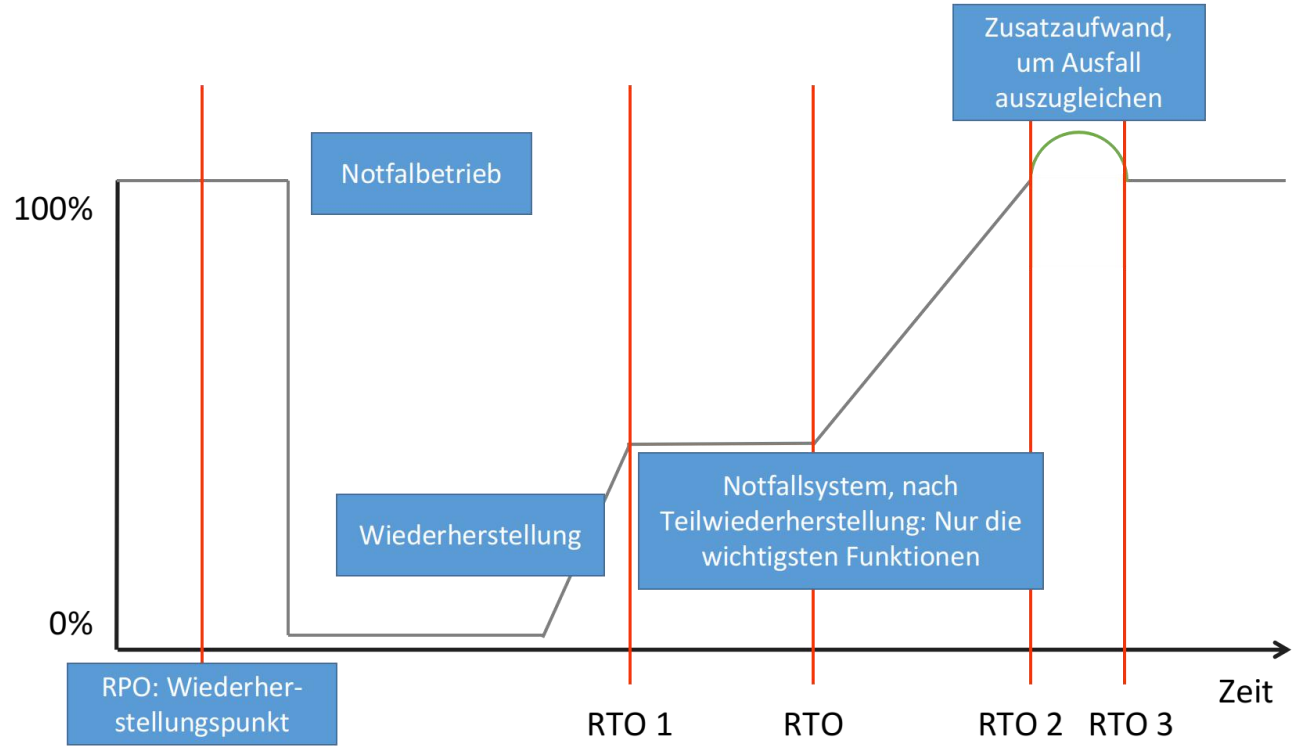
Vertikale und horizontale Ausfallsicherheit

- Ausfallsicherheit innerhalb eines Objekts
- Duplizierung der Einrichtung an einem anderen Ort
- -> Ausfall eines KHs: RTWs bekommen Anweisung zur Umleitung

PDCA-Zyklus:

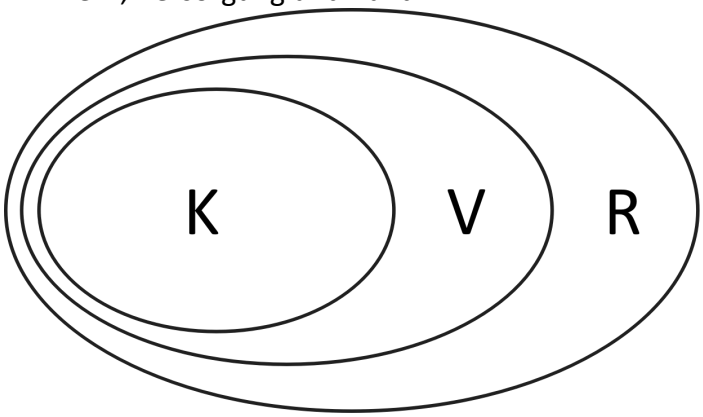
- Plan Do Check Act
- Planen, Durchführen, Überprüfen, Handeln

BCDR:



NISG verlang Zusätzlichen Katastrophenplan, falls BCDR nicht greift/reicht/funktioniert:

- Dynamische Lage
- SKKM: Wie kann man so eine Lage verhindern:
  - Krisenstab
  - Stabsoffiziere: S1 – S6 (in Österreich +S7):
    - S1: Personal: Wie viel Personal wird benötigt (mit Reserve), Personalmanagement, Befehlsweitergabe
    - S2: Infrastruktur: Betten, Wäsche, Nahrung
- Kern, Versorgung und Rand



  - Kern und Versorgung müssen aufrechterhalten werden, damit die Organisation funktioniert
  - Rand/Peripherie kann vernachlässigt werden

Quellen

- http://www.informatik.uni-oldenburg.de/~iug10/sli/indexd917.html?q=node/19, aufgerufen am 12.10.2021 um 11:25
- https://www.hanisauland.de/node/2133, aufgerufen am 12.10.2021 um 11:25

Protokoll MIS

Autor 1	Ardian Fetai
Autor 2	Nils Fischer
Datum	29.09.2021
Thema	Bedrohungen in Unternehmen (BIA) Planung, um Bedrohungen zu minimieren und um Verhaltensweisen beim Eintreten von Bedrohungen (BCP/DRP)
Beginn	15:15
Ende	16:05

Inhalt

Kurzzusammenfassung

Die Prozesse in Unternehmen müssen eingeteilt werden je nach Wichtigkeit und das Netz muss aufgeteilt werden in einzelne Netze, um bei Ausfällen von bestimmten Netzen die Funktionalität der anderen Netze zu gewährleisten.

Um Katastrophen Fälle zu minimieren, muss im Unternehmen vorher geplant werden (BCP) und wenn ein Katastrophenfall eintritt muss geplant worden sein wie man zu handeln hat um das System so schnell wie möglich wieder zum Laufen zu bringen (DRP).

Inhalt

Allgemein

Es gibt verschiedene Bedrohungen für die CIA-Triade und um diese Bedrohungen zu minimieren, braucht man einen Lösungskatalog.

Zuerst müssen die Prozesse (Prozess = Tätigkeit einer Firma) eines Unternehmens ihrer Priorität nach geordnet werden in:

- Kernprozesse (zb. Speichern von Daten, Kryptografie)
- Unterstützende Prozesse (zb. Apotheken, Sterilisation, IT)
- Vernachlässigbare Prozesse (zb. Darstellung des Unternehmens im Internet)

Die Einteilung wird mittels der Business Impact Analyse (BIA) durchgeführt. Durch diese wird klar welcher der Prozesse in einem Unternehmen ein Kernprozess, ein unterstützender Prozess oder ein vernachlässigbarer Prozess ist.

Beispiel anhand von AKH:

Das Netz des AKH kann eingeteilt werden in ein Verwaltungsnetz, ein Haustechniknetz und viele weitere Netze. Dieser Prozess wird **Separation** genannt.

Bei der **Mikroseparation** werden diese Netze nochmals in weitere kleinere Bereiche bzw. Netze eingeteilt.

Das Ziel dieser Separation ist es, dass wenn ein Netz ausfällt bzw. wegfällt die anderen Netze nicht vom Ausfall des eines Netzes betroffen sind und weiterhin problemfrei laufen.

Um so ein Netz zu planen wird der Zyklus des PDCA´s verwendet

PDCA steht für:

Plan
Do
Check
Act

Dieser Prozess muss regelmäßig durchgeführt bzw. Überprüft werden um ihn immer auf dem neuesten Stand zu halten. Das wird durch den **Kontinuierlichen Verbesserung Prozess** (**KVS**) gewährleistet.

Business Continuity Plan (BCP):

Ein Business Continuity Plan (BCP) umfasst eine detaillierte Strategie und eine Reihe von Systemen, mit denen ein Unternehmen erhebliche Unterbrechungen des Betriebsablaufs verhindern oder notfalls eine schnelle Recovery durchführen kann.

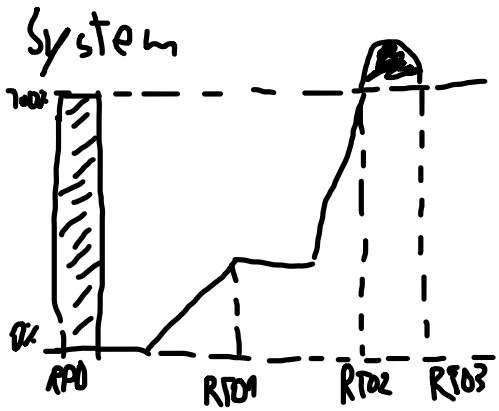
Disaster Recovery Plan (DRP):

Ein Disaster Recovery Plan (DRP) beschreibt die Technologie, den Prozess und das Verfahren zur Wiederherstellung kritischer IT-Geschäftsdaten. Ziel eines DR-Plans ist es, Ausfallzeiten von IT-Systemen im Notfall zu minimieren, damit ein Unternehmen so schnell wie möglich wieder geschäftsbereit ist.

Beim DRP wird geplant was für Situationen auftreten können und wie man sich in dieser Situation falls sie tatsächlich auftreten verhalten soll.

Fallbeispiel:

Eine oberösterreichische Firma für Cybersecurity wurde gehackt, da die Hacker eine Schwäche gefunden haben. Die Firma wollte das System mithilfe von einem Backup wieder aufsetzen, aber die Images der Backups waren auch schon kontaminiert und somit konnten diese Backups nicht verwendet werden, um das System neu aufzusetzen.



RPO = Recruitment Process Outsourcing

- hilft bei der Entwicklung einer Backup-Strategie

RTO = Recovery Time Objective

- befasst sich mit der Zeit bis zur Wiederherstellung und hilft bei der Entwicklung einer Disaster-Recovery-Strategie

RPO: System Fällt aus (Von 100 auf 0 % Systemfähigkeit). Man braucht Zeit es zu bemerken (RTO). Dann geht man in einen Not Modus (cirka 40-50% der Systemfähigkeit (RTO1)) und dann dauert es wieder bis das System ganz funktioniert (100% (RTO2)).

Tag der Mitschrift	06.10.2021
1.Autor	Fabian Freudenthaler
2.Autor	Nour Nassar

Mund-Nasen-Schutz -> Schützt Personal und Patienten

CIA – triad -> **confidentiality, integrity,** and **availability**

Welche Aufgabenbereiche gibt es im kritischen klinischen Pfad?

- Identifikation von Objekten
- Identifikation von Bedrohungen
- Verminderung von Gefährdungen
- Gewährleistung der Ausfallsicherheit

Es können 3 verschiedene negativen Ereignisse auftreten:

- Störfall – wir gehen davon aus, dass dies auftreten, kann
- Notfall – wenn man selbst in der Lage ist dieses Problem zu lösen
- Katastrophe – wenn äußere Hilfe benötigt wird oder Menschen in unmittelbarer Lebensgefahr stehen

Es gibt Definitionen innerhalb einer Organisation, jene besagen, wie lange Systeme stillstehen dürfen.

OLA (Operational Level Agreement)

- Definitionen innerhalb einer Organisation, jene besagen wie lange Systeme stillstehen dürfen

SLA (Service Level Agreement)

- Definitionen außerhalb einer Organisation, jene besagen wie lange Systeme stillstehen dürfen

Hot-standby -> Wenn eine Komponente abstürzt, dann übernimmt dieses Gerät die Funktionen dessen.

RTO – recovery time of the objective -> mögl. Gering

Cold-standby – Dieses Gerät ist einmalig und muss deshalb nachgekauft werden -> recovery time sehr hoch

1st Level support – einfache und sofortige Problembeseitigung mit einfacher Dokumentation

2nd Level support – Die aufgetretenen Probleme werden behandelt und eingegrenzt.

3rd Level support – Change request -> Die Probleme werden behandelt und so gelöst, dass sie nicht mehr auftreten. -> Programmierebene

Falls ein Fehler auftritt, der gegen die Datenschutz Grund Verordnung verstößt, dann haben wir nach einer Meldung bei der Datenschutzkommission 72 Stunden Zeit diesen Fehler zu beheben.

Fallbeispiel:

Patientendaten wurden Publiziert und wir melden es sofort der Behörde.

Anschließend führen wir eine Analyse durch, um ein Leak zu finden.

Dabei finden wir heraus, dass unsere Radiologie Geräte fehlerhaft sind, deshalb Melden wird es dem Bundesamt für Sicherheit im Gesundheitswesen.

Welche Maßnahmen müssen getroffen werden, um diesen Fehler zu beheben?

Benötigen wir äußere Hilfe?

Protokoll MIS

Autor 1	Harald Schild
Autor 2	Elias Schartmüller
Datum	11.11.2021
Thema	Österreichisches Informationssicherheitshandbuch
Beginn	15:15
Ende	16:05

Österreichisches Informationssicherheitshandbuch

2 Informationssicherheitsmanagementsystem

4 Risikoanalyse

Erst grundschutz dann detailiert oder nur eines von beiden

bsi.bund.de

BSI 200-1

VergANGENHEIT 100 version 100-1,100-2,100-3,100-4

Österreich verweist auf den grundschutz der aus Deutschland kommt welcher im dokumet **BSI 200-2** zu finden ist.

Grundschutzmethode = Baselinesecurity

Alles was unter der Linie ist muss Regenln einhalten

Bsp.:

Grundschutz: Auf allen Endgeräten wird ein Schutz installiert

Warum ist das aber kontraproduktiv: nicht jedes System benötigt die selbe Art von Schutz, alle Systeme haben die gleiche Schwachstelle, vielleicht braucht nicht alles ein Anti Virus, vielleicht erlaubt der Hersteller nicht die Installation auf bestimme Geräte wie zb von Medizin Geräte

→Deswegen detaillierte Risiko Analyse

→kern Prozesse analysieren und diese unterstützen

Früher gab es einen Bedrohungskatalog die frage ob es auf unseren Objekten ein Risiko gibt

Sandboxing: Man konfiguriert was durchgeht durch ein System

Mitarbeiter Schulen,

NOC: Network Operation Center→ Alle Mitarbeiter die verantwortlich sind für das Netzwerk

SOC: Security Operation Center → Kümmert sich um die Sicherheit im NOC

Detaillierte grundschutz

Schaut jedes einelne objekt dezitiert an ist ber zeitaufwendig und ineffizient

Lso evrwendet man den Kombinierten Ansatz

Alles was aus dem Grundschutz heraussticht weil sie kritisch sind müssen detailliert geschützt sein aber die administrativen Geräte werden wahrscheinlich alle gleich auf der Grundschutzmethode sein also alle Windows+Microsof+Antivirus

Damit wird versucht die breite Masse zu schützen

Antivierenschutz kann kontraproduktiv sein weil dadurch alle systeme die gleiche schwachstelle haben können, daher auf server andere Antivirus als auf Nutzerendgeräten. Und wenn nicht jedes Gerät einen Antivirus braucht oder der Medproduktehersteller erlauben nur bestimmte Antivirusprodukte auf ihren Produkten

Möglichkeit:

Wir bekommmen kein Ok für antivirus

Brauchen detaillierte Risikoanalyse

Die grundschhutzmethode kann man nicht überall verwenden deshalb hat deutschland gesagt man muss die Kernperipherie schützen, also Gastwlan muss nicht geschützt werden kann im notfall einfach abgedreht.

Wenn das KH internetservices anbietet wird es zum porvider und muss die ganzen regulierungen einhalten nud adblocker einstellen usw. d.h. lieber einen externen provider frage ob die Internet anbieten wollen

In Ger doc 200-2

Es gibt einen bedrohungskatalog, der einstuft wlches objekt in welche risikoklasse es fällt

Grundschutz ist überall anzuwenden aber was machen wir dort wo wir den Grundschutz nicht wanweden können, wir machen ein Vlan also wir separieren alle komponenten nach Abteilung wir versuchen also die Komponenten von einander ,abzuschotten.

Also firewall zwischen den Vlans dort wird nur jene kommunikation durchgelassen die notwendig ist

Andere Löung

Snadboxing

Man kann konfigurieren was man durchlässt und was nicht

Firewall mit Snadboxing versucht den aufrufenden client zu simulieren und darin schaut ob ein visrus drauf ist wenn nicht wird die nachricht weitergegebn wenn schon wird sie zurückgesendet oder gelöscht

Kap. 6 Oragnisation

Wer tut was

6.1.1 sit leider veraltet also missmatch oder Gap

Was macht man wenn man für das Netzwerk verantworktlich ist. Was macht man um ein Problem organisatorisch in den Griff zu bekommen zb Mitarbeiter schulen man hat so aber leute die nur auf das Netzwerk spezialisiert sind, wird geannt ***NOC*** Network operatioin Center

Zur sicherheit ***SOC*** security operation center

Firewall

Antivirus

Verwendet **SIEM** (security information event management)

Server, client, switch – event iwas ist passiert zb Brandmelder

NOC und SIEM arbeiten eng miteinandere zusammen

Ergänzung

Protokoll MIS

Autor 1	Ardian Fetai
Autor 2	-
Datum	23.02.2022
Thema	Traffic Light Protocol, GRC, Einteilung Primär- und Sekundärprozesse und TOM
Beginn	15:15
Ende	16:45

Inhalt

Kurzzusammenfassung

Dokumente in Organisationen müssen mit dem Traffic Light Protocol versehen werden um die Zugangsberechtigung/Leseberechtigung festzulegen.

Prozesse im Unternehmen müssen in Primär und Sekundärprozesse eingeteilt werden, um die Sicherheit durch individuelle Anpassung zu erhöhen. Außerdem müssen Technische und Organisatorische Maßnahmen definiert werden um die Sicherheit der Verarbeitung personenbezogener Date zu gewährleisten.

Inhalt

Allgemein

Jedes Dokument in einem Unternehmen, dass an Mitarbeiter versendet wird, muss am Anfang von Dokument das Traffic Light Protocol (TLP) verwendet werden. Das TLP ist eine standardisierte Vereinbarung zum Austausch von schutzwürdigen Informationen und wird in 4 Farben eingeteilt.

Rot:

Das Dokument darf nur von dem Empfänger selbst gelesen werden. Dieser darf das Dokument nicht an andere weitergeben.

Gelb:

Der Empfänger darf bei „gelbem Licht“ die Informationen an andere Personen innerhalb der Organisation weitergeben, jedoch nur nach dem „need-to-know“ Prinzip. Also nur die Personen in der Organisation die die Informationen wirklich brauchen und kennen müssen sollen sie auch bekommen.

Grün:

Die Informationen dürfen innerhalb der Organisation und deren Partner weitergegeben werden, sie dürfen aber nicht veröffentlicht werden durch die Presse.

Weiß:

Diese Informationen können an alle Personen weitergegeben werden einschließlich der Presse.

Stufe	Bedeutung	Bestimmungen
TLP-White	**Unbegrenzt**	Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP-White ohne Einschränkungen frei weitergegeben werden.
TLP-Green	**Organisations-übergreifende Verteilung**	Informationen in dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Information darf jedoch nicht veröffentlicht werden.
TLP-Amber	**Organisationsinterne Verteilung**	Informationen in dieser Stufe dürfen innerhalb der Organisationen der Empfänger weitergegeben werden, jedoch nur auf der Basis „Kenntnis nur wenn nötig“. Der Ersteller der Information muss zusätzlich beabsichtigte Einschränkungen der Weitergabe klar spezifizieren.
TLP-Red	**Persönlich, nur für benannte Empfänger**	**TLP-Red-Informationen** sind auf den Kreis der Anwesenden in einer Besprechung oder einer Video-/Telefonkonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. In den meisten Fällen werden Informationen der Stufe TLP-Red mündlich oder persönlich übergeben.

Governance, Risk & Compliance (Governance, Risk Management and Compliance – GRC) fasst die drei wichtigsten Handlungsebenen eines Unternehmens für dessen erfolgreiche Führung zusammen:

- **Governance** ist die Unternehmensführung durch definierte Richtlinien. Dazu zählt die Festlegung von Unternehmenszielen, die darauf angewandte Methodik zur Umsetzung und die Planung der notwendigen Ressourcen für das Erreichen der Ziele.

- **Risk** steht für das Risikomanagement mit bekannten und unbekannten Risiken durch definierte Risikoanalysen. Ein wichtiger Faktor dabei ist das frühzeitige Auseinandersetzen mit Risiken, der Bereitstellung von Strategien zur Risikominimierung und dem Vorbereiten von Schadensfallpuffern bei Risikoeintritt.

- **Compliance** ist das Einhalten interner wie externer Normen für die Bereitstellung und die Verarbeitung von Informationen. Diese beinhaltet unter anderem Vorgaben aus Normierungsbestrebungen und die Zugriffsreglementierung für die Daten sowie die gesetzlichen Rahmenbedingungen für deren Verwendung.

Quelle:
„https://de.wikipedia.org/wiki/Governance,_Risk_%26_Compliance#:~:text=Governance%2C%20Risk%20%26%20Compliance%20(Governance,die%20Unternehmensf%C3%BChrung%20durch%20definierte%20Richtlinien. , Stand 24.02.2022“

Die unterschiedlichen Fachbereiche eines Krankenhauses (medizinische Versorgung, technische Versorgung) müssen darauf überprüft werden, ob sie Schnittstellen zu uns (der IT/IT-Sicherheit) haben. Unser Hauptfokus liegt dabei auf den IT-Systemen wie, IKT-System, Medizintechnische-Systeme und Kontrollsysteme die elektrisch sind.

Daraufhin müssen Schutzziele definiert werden. Um die Sicherheit in den verschiedenen Bereichen zu erhöhen und um sie an den jeweiligen Bereichen anzupassen, müssen die Bereiche Segmentiert werden. Durch die Segmentierung kann auch der Ausfall aller Systeme verhindert werden, wenn ein einzelner Bereich ausfällt. Hierbei schreibt das NIS-Gesetz vor Bereiche zu unterteilen in die nur Personen mit Berechtigung hineinkommen und Bereich zu denen jeder Zutritt hat.

Durch „Shared-Arbeitsplätze“ (1 Hard- und Software, die von mehreren Personen verwendet werden) wird das Fehlerrisiko erhöht. Auch durch die zunehmenden E-Health Anwendungen werden die Bedrohung und die Komplexität für die IT-Sicherheit erhöht.

Durch Organisatorische Maßnahmen und Separation der einzelnen Bereiche werden sowohl die Bedrohungen als auch die Komplexität verringert.

Primär und Sekundärprozesse:

Um die Primär und Sekundärprozesse einteilen zu können müsse wir mit den jeweiligen Fachexperten der medizinischen Prozesse Gespräche führen. In diesen Gesprächen wird ein vorgefertigter Fragenkatalog durchgearbeitet.

Im zweiten Schritt werden die Sekundärprozesse erfasst die für die Primärprozesse nötig sind. Zum Schluss wird beschlossen welche Bereiche/Prozesse IT benötigen.

TOM- Technische und Organisatorische Maßnahmen werden in der DSGVO definiert.

Technische und organisatorische Maßnahmen sind die vorgeschriebenen Maßnahmen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten.

Im Fall eines sogenannten Data Bridge (Veröffentlichung personenbezogener Daten) muss laut der DSGVO innerhalb von 72 Stunden ein Ticket geschrieben werden bzw. das Datenleck gemeldet werden, wenn innerhalb von 72 Stunden keine Lösung gefunden wird.

Das NIS-Gesetz schreibt vor, dass wenn ein wesentlicher Dienst ausfällt, aus welchen Gründen auch immer, sowohl durch äußere Faktoren (Hacker) oder Eigenfehler (Updates, die nicht funktionieren), muss das innerhalb von 3 Stunden gemeldet werden.

ergänzende Informationen: