ALLE PROTOKOLLE VOM SCHULJAHR 2019/20

MIS Hocheiser

5AHBGM

Inhalt

Mitschrift, am 09.09.2019

Allgemeines

- Protokollführung und Quellennachweise
    - Online quellen referenzieren und, wenn möglich, downloaden
    - Vasa-Syndrom:
        - Alle beteiligten arbeiten richtig. Passen sich aber nicht gegenseitig an

Vasa-Syndrom

Als Vasa-Syndrom bezeichnet man in Management- und Marketingkreisen ein Kommunikationsproblem, das zum Scheitern eines Projekts führt. Der Begriff geht zurück auf das schwedische Kriegsschiff Vasa, das 1628 infolge massiver Baufehler bereits bei seiner Jungfernfahrt sank. Unternehmen entgehen jedes Jahr Millionen, weil Projekte nicht effizient realisiert werden und ihr Ziel nicht erreichen. (Quelle)

Der König wollte herausfinden wer schuld war → Alle am Schiffsbau beteiligten Personen haben richtig gearbeitet, nur hat keiner die Gesamtheit im Überblick bewahrt hat. → Daher ist es in Abläufen in großen Gruppen wichtig einheitlich und ordentlich zu arbeiten.

Beispiel:
Vor 3 Monaten → israelische Forscher ist es geglückt Dicom Bilder so zu manipulieren, dass nach der Aufnahme des Lungenröntgenbilder ein Tumor injiziert wurde und es den Medizinern zur Befundung gegeben wurde.
→ https://www.spiegel.de/netzwelt/web/cyberattacke-im-krankenhaus-wie-forscher-eine-krebsdiagnose-manipulieren-a-1261330.html per 9.9.19

Daher ist es wichtig die **Integrität** von bestimmten Informationen sicherstellen.

Wie kann jemand in das System eindringen und mit den bestimmten Werkzeugen manipulieren.

Bundes ÖFP: **Spare Fishing Attacke** → Email wird so manipuliert, dass sie auf eine interne Website zeigt, damit das Opfer seine Identifikationsdaten preisgibt.

Optimale 3. Variante: **Zwei Faktor Authentifizierung** (Zwei unabhängige Elemente: Karte, Auge | Username, Passwort und TAN)

Zwei Faktor Authentifizierung

- Bei allen Onlinebanking Plattformen (Passwort & TAN)
- Stecken der O-Card, E-Card → Nur ein Mal am Tag (Er bleibt bestehen, bis der Tag abgelaufen ist oder die Verbindung abgebrochen wurde)
- Bankomatkarte (Karte und PIN)

Vorschriften, Gesetze für die Sicherheit der Patientendaten

DSGVO:

- Derzeit Übergangsfrist neue Medizinproduktverordnung
- EU-basis
- Verordnung (genaue Angaben zu halten)
- Alle sind von der DSGVO betroffen

Unterschied Richtlinie & Verordnung:

- Wenn ich eine **Richtlinie** in der EU hab müssen sich alle Mitgliedsstaaten daranhalten und durch eigene Gesetzgebung umzusetzen. → kann dazu führen, dass Interpretation zu einer nicht gleichen Gesetzgebung in der EU führt.
- **Verordnung** ist in allen Mitgliedsstaaten gleich. Hat den Vorteil, dass Firmen

NIS-RL:
fokussiert auf das Netz und Informationssysteme der Republik. Aber nur in den Bereichen, in denen es geht, die Infrastruktur der Republik zu schützen. Sektoren die zur kritischen Infrastruktur zählen. Einer davon ist der Sektor Gesundheitswesen. Alle beteiligten müssen Maßnahmen treffen, um diese Richtlinien gewährleisten zu können.

Informationsmanagementsystem

Informationsmanagementsystem: Es gibt Regen/Prozesse die regelmäßigen/unregelmäßigen Abständen zu machen sind. **Mutterprozess** eines Managementsystem ist der **Demenkreislauf → plan, do, check, act Zyklus).** Zählt in allen Managementsystemen. Welche Ziele will ich erreichen. Wie, welche Organisationseinheiten sind betroffen, welche Regulationen/Gesetze muss ich einhalten, wie habe ich diese in meiner Organisation technisch realisiert.

Jeder weiß was er wann wie zu tun hat, jeder wurde über die Vorgangsweise eingeschult. Wie die Vorgangsweise der Mitschriften. Grunddokument, wer ist wann dran, wie schauen diese aus, wo sind diese abzugeben, wie die Versionierung funktioniert, etc..

Zielt immer darauf ab, den Schutz, den wir erreichen wollen, so gut als möglich durch Maßnahmen aus technischer oder organisatorischer Sicht umzusetzen.

Da ich weiß dass ich keine 100% Sicherheit garantieren kann muss ich mir überlegen wie ich andere Geräte automatisch überprüfen kann.

Intrution-Detection System →(IDS):

- Host Basierend (Rechner basierend) oder Netzwerkbasierend
- Analysiert Anomalien

Intrution-Prevention (IPS):

- Reagiert auf diese Anomalien
- Teil von einem IDS wäre ein Antivirus am Rechner

Datenschutz

Datenschutz fokussiert sich auf das C und das I (Vertraulichkeit und Integrität). Beim NIS Gesätz kommt noch dazu, dass nicht die gesamte Gesundheitsdienstanbieter unter das NIS Gesätz fällt. Es wird ein Bescheid an alle vom NIS Betroffenen verschickt. Es gibt bedingt durch das Krankenanstaltsgesetz und das **Informationsmanagement System** die Notwenigkeit einer Krankenanstalt oder Gesundheitsinstitutes sich Gedanken zum Datenschutz zu machen. Im Gesundheitswesen haben wir wenn wir einen Bescheid haben, 3 Meldepflichten welche koordiniert gehören.

Beispiel für die Notwendigkeit eines **Informationsmanagement System**:

Montag 8 Uhr in der Früh AKH Wien. Bei der Kontrolle des Workflows, welche Patienten kommen in welcher Reihenfolge zum CT, fällt dem Bedienungspersonal auf, dass die Listen auch im Internet frei verfügbar sind. Die Daten können von Jedermann und Jederfrau im Internet aufgerufen werden.

Datenschutzbehörde ist zu verständigen. Eine Stunde später bei der Vorbereitung der entsprechenden Untersuchungsnotwendigkeiten stellt das Personal fest, dass der CT nicht so verhält wie er sich verhalten sollte und dass am Sonntag über das WE vom Hersteller und Betreiber ein Update durchgeführt wurde (Verdacht dass das Update schuld ist) gefacht besteht, dass das Personal oder Patient in Gefahr gerät. (Sollte ein Betreiber in Kenntnis eines nicht ordnungsgemäßen Ablauf, und es zu einem Schaden kommen kann hat er es an das Bundesamt für Sicherheit im Gesundheitswesen zu sagen. Diese können das Gerät aus dem Verkehr ziehen. Nicht nur bei Institutionen die es melden, sondern alle die zu dieser Installationsreihe gehören werden aus dem Verkehr gezogen - MPG§70). 12 Uhr Mittag nach erstmaligen Auftreten einer Anomalie fällt die IT des Ge… es Gibt den Verdacht dass weder ein Databridge war sondern es ein Hacker war. (NIS – Wenn ein Wesentlicher Dienst (Röntgen) in Mittleidenschaft gezogen wurde die Versorgung des Gesundheitswesen gefährdet wurde und die Störung dauert länger als 3 Stunden haben wir es der NIS Behörde zu verständigen).

Bemerkungen zum Beispiel:

- Im Gesundheitswesen ist Sehr oft das Restrisiko 1 (Nur einer ist betroffen und daher vernachlässigbar)
- **Trafik Light**: Ist die Ampel (Rot, Gelb, Grün)
    - Rot: Nicht weitererzählen (Vertraulich)
    - Gelb: unter bestimmten Bedingungen erzählbar
    - Grün: Alles ist erzählbar.

Mitschrift, am 16.09.2019

Risiko im Gesundheitswesen

Krankenhäuser erbringen als eine der tragenden Säulen unseres Gesundheitswesens vielfältige medizinische und pflegerische Dienstleistungen und zählen daher zu den Kritischen Infrastrukturen unserer Gesellschaft. Dabei ist die Funktionsfähigkeit dieser Einrichtungen selbst wiederum nicht nur von weiteren externen Kritischen Infrastrukturen, wie beispielsweise der Strom- und Wasserversorgung, abhängig, sondern auch bereits in hohem Maße von der vor Ort eingesetzten Informationstechnologie. Diese findet sich in zahlreichen Formen von Anwendungen zur Behandlungsdokumentation über Inventar- und Bestellsysteme bis hin zu medizintechnischen Geräten wieder. Sie unterstützt bei bisher papiergebundenen Arbeitsabläufen und erleichtert Diagnose- und Behandlungsprozesse oder macht diese sogar erst möglich.

Es gibt viele Belege dafür, wie verwundbar Krankenhäuser durch Naturkatastrophen oder durch den Ausfall wichtiger Ressourcen wie Strom oder Wasser sind. Mit zunehmender IT-Durchdringung wächst jedoch die Gefahr, dass Krankenhausprozesse nicht nur durch solche konventionellen Risiken, sondern auch durch Ausfälle oder Störungen der IT erheblich beeinträchtigt werden oder sogar komplett ausfallen können. Dass diese Risiken ernst zu nehmen sind, belegt nicht nur die Vielzahl an bekannt gewordenen IT-Sicherheitsvorfällen und IT-Störungen in Unternehmen und Behörden

NIS-Richtlinie

Die NIS-Richtlinie ist ein wichtiger Schritt für mehr Cyber-Sicherheit in Europa.
Die Richtlinie muss von den Mitgliedstaaten der europäischen Union in nationales Recht umgesetzt werden. Dafür haben sie bis Mai 2018 Zeit. Mit dem am 29.06.2017 verkündeten Umsetzungsgesetz hat der deutsche Gesetzgeber seine Hausaufgaben schon erledigt. Dabei war die Ausgangsposition hierfür denkbar gut: In Deutschland existiert seit Juli 2015 mit dem IT-Sicherheitsgesetz bereits ein einheitlicher Rechtsrahmen für die Zusammenarbeit von Staat und Unternehmen für mehr Cyber-Sicherheit bei den Kritischen Infrastrukturen (KRITIS). Dieser schreibt KRITIS-Betreibern vor, IT-Sicherheit nach dem "Stand der Technik" umzusetzen und erhebliche IT-Sicherheitsvorfälle an das BSI zu melden. Der Gesetzesentwurf zur Umsetzung der NIS-Richtlinie erweitert nun die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber KRITIS-Betreibern.

Risikoanalyse

Die IT-Risikoanalyse umfasst eine Reihe von Teilschritten, die sich zusammen mit den vor- und nachgelagerten Aktivitäten in vier Aufgabenblöcke gliedern lassen:

- Vorbereitende Aktivitäten
- Kritikalität von Prozessen und IT analysieren
- Risiken identifizieren und bewerten
- Risiken behandeln

Als Maßstab für die Ermittlung kritischer Prozesse und IT-Ressourcen sowie für die Entscheidungen zur Risikobehandlung sind Schutzziele zu definieren, die sich an den übergeordneten Zielen der Einrichtung orientieren, beispielsweise an der aus dem Auftrag eines Krankenhauses abzuleitenden Verpflichtung zum Schutz der Gesundheit der Patienten oder dem Interesse an einer Aufrechterhaltung der wirtschaftlichen Existenzfähigkeit der Einrichtung. Für die IT werden die Schutzziele durch die im Rahmen der Informationssicherheit üblichen Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit konkretisiert. Aufgrund der speziellen Ausrichtung der IT-Risikoanalyse im Kontext Kritischer Infrastrukturen steht die Sicherung der Verfügbarkeit und Integrität der IT-Infrastruktur an oberster Stelle. Das Ziel der Vertraulichkeit wird in die Betrachtung einbezogen, da

durch dessen Verletzung sich in der Folge Verletzungen der Verfügbarkeit und der Integrität ergeben können. Eine mögliche Definition der IT-Schutzziele lautet beispielsweise wie folgt:

IT-Störungen dürfen nicht dazu führen, dass

- die medizinischen Versorgungskapazitäten nicht mehr in angemessener Qualität und Quantität aufrechterhalten werden können (**Verfügbarkeit**)
- Daten verfälscht werden, deren Richtigkeit für die Versorgung eines Patienten unbedingt erforderlich ist (**Integrität**)
- Daten, deren Bekanntwerden sekundär die Verfügbarkeit und Integrität der IT-Infrastruktur beeinträchtigen oder die Sicherheit eines Patienten gefährden können, unberechtigten Dritten zugänglich werden (**Vertraulichkeit**)

Staatliches Krisen- und Katastrophenschutzmanagement (SKKM)

Die Abwehr, Beseitigung oder Linderung der Auswirkungen drohender oder eingetretener Katastrophen (Katastrophenhilfe, Einsatzvorsorgen) ist in Österreich überwiegend eine Angelegenheit der Bundesländer. Die rechtliche Basis bilden die Katastrophenhilfegesetze der Länder, die vor allem die Feststellung der Katastrophe und die behördliche Einsatzleitung in den Gemeinden, Bezirken und Ländern festlegen.
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.

Im Krankenhaus gibt es Risiken, die beispielsweise verursacht werden durch

- die falsche Vergabe von Medikamenten
- die Verwechslung von Patienten
- mangelnde Hygiene
- schlecht ausgebildetes oder überlastetes Personal

Die IEC 80001 hat vergleichbare Schutzziele wie das Risikomanagement im Allgemeinen: Risiken für Patienten (körperliche Schäden, Verletzung des Datenschutzes) und das Krankenhaus zu minimieren.

Mitschrift am 07.10.2020

Analyse des Dokuments

Information richtig herleiten und Konzept aufbauen

Organisatorische Abläufe werden dargestellt

Sollen auch Menschen dann verstehen, die nichts damit zu tun haben

Aufgabenstellungen müssen irgendwie zusammengefasst werden, ein Gefühl dafür kriegen wie man sich an sowas Herantastet

Welche Maßnahmen würden wir einleiten, eine Beurteilung zu geben

Wie glauben wir, wie wir dort eine Risikoanalyse zu machen haben und wie wir diese bewerten?

BSI, Grundschutz, dort stehen Dinge für die Risikoanalyse drinnen

Weiters ist die Frage, wie wir diese Aufgaben aufteilen und diese Bereiche teilen und überlegen wie wir unsere Netzwerksicherheit, Risikoanalyse und Rechnersicherheit durchführen

Spezialbereiche in jeder Branche, als Beispiele: verschiedene Ambulanzen, OP-Stationen und Pflegebereiche

Intensiv-Stationen sind hochsensibel und müssen extra kontrolliert werden

Medizintechnik spielt eine wichtige Rolle bei Modalitäten

Ein kritischer Bereich sind die Apotheken

Das wurde im Dokument versucht zu beschreiben.

Die Gruppe soll aus der Summe der Informationen einen Abstract bilden, um eine einheitliche Sicht zu haben

Verweis auf die Seite machen, für jemanden der es nachlesen möchte, der eine bestimmte Seite sucht

Es muss von jemand der von außen darauf schaut, nachvollziehbar sein WIE EIN KOCHREZEPT

Ein Konzept finden, wer hat was zu tun und wie werden diese beschrieben und ebenso kontrolliert werden

Jeder Prozess, der beschrieben wird, kann im Reifegrad definiert werden, es gibt eine Norm dafür

Wenn es gar nichts gibt, dann wird das gemacht was die Person kann und macht

Ebenen und Beschreibungen

Ebene	Beschreibung/Messwerte
0: Nicht vorhanden – Unvollständig	• Kein Prozess definiert. • Prozessschritte nicht festgelegt (eher projekt- als prozessorientiert). • Input und Ergebnis nicht definiert. • Wiederholbarkeit nicht gegeben.
1: Sensibilisiert – Organisiert	• Bewusstsein für Arbeitsabläufe bei Mitarbeiterinnen und Mitarbeitern (MA) vorhanden • Prozess ist (in Teilen) organisiert. • Input und Ergebnisse definiert • Prozesse sind nicht abgestimmt.
2: Etabliert – Standardisiert	• Prozess ist dokumentiert und wiederholbar. • Prozesse sind aufeinander abgestimmt. • Rollen und Verantwortlichkeiten sind klar geregelt.
3: Gereift – Vorhersehbar	• Qualitätskriterien existieren. • Qualitätsziele sind definiert und werden gemessen. • Verbesserungen sind gezielt möglich. • Prozessergebnisse sind vorhersehbar und haben eine gute Qualität.
4: Optimiert – Exzellent	• Stärken und Schwächen der Prozesse sind transparent. • Prozesse werden kontinuierlich entsprechend den Messwerten an die Qualitätsziele angepasst. • Qualitätsziele werden fortlaufend an den Unternehmenszielen ausgerichtet. • Exzellenz der Prozesse resultiert in einer hohen Effektivität und Flexibilität des ITSM.

CMDP oder wie auch immer

Genau so ein Risiko bei dem, weil unterschiedliche Konfiguration

Bei einer Fehlkonfiguration sind alle Bereiche gefährdet

4-Augenprinzip, Überprüfung bei einer Konfiguration

Des is a Policy a Regelwerk

Wir brauchen Bewusstsein, bei jeder Arbeit

KVP (kontinuierlicher Verbesserungsprozess): es gibt Jemanden, der sich überlegt, welche Rahmenbedingungen verändert worden sind, wie muss ich Sie einpflegen ins System

Kommunikation ist wichtig

Heutzutage vieles durch Virtualisierung in einzelne Bereiche teilen

System einer Verwundbarkeit unterworfen und nach welchen Kriterien werden diese virtualisiert

Kann man die Netzwerke virtualisieren?

Virtualisierung ist auf unterschiedlichen Ebenen möglich

PaaS: Platform as a Service

Entweder eine komponente Lamp oder Wamp

Login muss selber erstellt werden

2.Variante vergessen/überhört

3. Variante

IaaS: Infrastructure as a Service

Bilde ich in meinem Rechenservice ein Cloud-Service ab

Es gibt Private-Clouds, Public-Clouds und Hybrid-Clouds

Kapazitätsengpass, wegen einer Überlastung des Rechners und mit dieser Möglichkeit eine Leistung von außen zu kaufen

Elastititäts-Management

So wie beim Car-Sharing, macht kauft die Hardware nicht, man mietet diese

Mitschrift, am 21.10.2019

Müssen wissen was in der Risikoanalyse kritisch ist.

2 Prozesse:

- Ambulante
- Stationäre Prozesse

Ambulanz Unterschied zu niedergelassenen Arzt:

Niedergelassen → First in first out

Ambulanz → Nach Kritikalität des Vorfalls wird Patient vorgezogen

IT unterstützt diese Prozesse

CIA-Triade beachten → Wenn Vertraulichkeit und Integrität nicht verfügbar sind → Auswirkungen auf Verfügbarkeit

Verfügbarkeit → Differenzierung Verfügbar oder nicht

In unserem Fall →

NIS → geht's nicht um den Datenschutz und die Vertraulichkeit

3 Meldewege:

- Databridge an Datenschutzbehörde melden
- MPG Paragraph 70 → bei beinahmen Unfall BVT informieren
- NISG → Wenn IT-Infrastruktur länger als 3 Stunden stillgelegt und Leistungen eingeschrängt sind → CERT-AT melden

Welche Bedrohungen gefährden unser System → Maßnahmen, Verantwortlichen

Wenn drei unterschiedliche Verantwortliche → finden keinen Zusammenhang zwischen bestimmten Vorfällen

Wenn eine Person für drei Sachen verantwortlich ist → findet einfacher Zusammenhang zwischen den Vorfällen

Beispiel:

Patientenbehandlung im Internet veröffentlicht (Databridge) → Analyse → Feststellung dass ein Update durchgeführt an einem Medizinprodukt wurde → Wahrscheinlichkeit wurde dadurch erhöht → „Bei nahe Unfall" muss gemeldet werden

2 Meldungen (MPG und Databridge Meldung)

Fall so eingegrenzt, dass die Wahrscheinlichkeit hoch ist, dass es ein Hackerangriff war.

NISG → Wenn Vorfall länger als 3 Stunden dauert, und Leistungen eingeschränkt sind → Meldung an BVT (NIS-Behörde)

Bis jetzt reine Risikoanalyse → Wie gehen wir mit einem Vorfall um?

KRITIS → Darstellung der Kritikalitäten in Ambulanten und Stationären Bereich um Maßnahmen zu setzen

Wie geht man um bzw wie ist der Plan B (Workaround, Alternativen) und wie schaff ich es das Personal zu informieren, dass Plan B angewendet wird.

2 Abläufe im Krankenhaus:

1.) Alles Funktioniert, alle kennen sich aus
2.) Wie geht man bei Fehlern bzw Ausfällen um. Wie informiert man das Personal

Katastrophenmanagement

SKKM (Staatliches Krisen und Katastrophenmanagement)

7 Stabsbereiche → S1 bis S7 (7 Personen)

Ausnahmesituation wird bzw muss von jemandem ausgerufen werden → Dann wissen wir wie wir in dieser Situation umgehen.

Kritikale Bereiche:

- Netwerk
- Rechenzentrum Struktur
- Stromversorgung
- Versorgungen für Patienten

Beispiel Spengerspital:

Kritikale Prozesse und Maßnahmen überlegen

Abhängigkeiten zur IT überlegen

Mitschrift, am 04.11.2019

- Im medizinischen Bereich muss sich immer die Frage gestellt werden: "Was wäre, wenn". Beispielsweise sollte man sich immer überlegen: "*Was wäre, wenn der Patient ein gewisses Medikament nicht vertragen würde?*"
- Man sollte sich immer die Frage stellen, was kann man machen, um eine Bedrohung zu verhindern, und was die Folgemaßnahmen wären.

Ransomware

Ransomware ist derzeit ein sehr großes Problem (auch im medizinischen Bereich)

- Dateien werden bei solchen Angriffen verschlüsselt, und dadurch den Ärzten unbrauchbar gemacht

Wie kann man dagegen vorgehen?

- (beispielsweise) Firewalls konfigurieren, erstellen
- mehrere Kanäle/Komponenten müssen beschützt werden. Angreifer können heutzutage schon bei unterschiedlichen Modulen gleichzeitig angreifen
- Transdisziplinäre Betrachtung es sollen verbundene Module, die miteinander agieren, ersichtlich sein, und gemeinsam (bsp) geschützt werden
- Bei einem Zwischenfall hat man 72h Zeit Probleme der Datenschutzbehörde zu melden
    - dabei ist zu unterscheiden, ob eine Fehlkonstruktion, oder ein Angriff an einer Situation (bzw. Problematik) schuld ist
    - Wenn ein Labor Automat betroffen ist, muss nicht nur die Datenschutzbehörde, sondern auch der Sicherheitsbeauftragte des Krankhauses informieren werden

      ⇒ Meldeprozess (Wann habe ich zu informieren)

Meldeprozess

- Wer muss informiert werden?
- Wonach müssen die Personen reagieren (z.B. nach welchem Gesetz muss agiert werden)
- Welche Geräte sind betroffen
    - Welche Geräte wurden manipuliert?
    - Können Abläufe weiterhin durchgeführt werden?
- Wurden Daten manipuliert?
    - Können Folgefehler auftreten. Welche Risiken kann es geben (falsche Medikamente, etc.)
    - Integrität der Daten ist in Frage zustellen
- Können Daten noch immer manipuliert werden (ist der Angriff bereits vorbei?)
- Können Daten vertraut werden?
    - Wie kann man Korrektheit der Daten überprüfen?
- Müssen Gerätschaften Außerbetrieb genommen werden?
    - Wenn ja: ⇒ NIS Gesetz
- Wer meldet es bei einem Störungsfall?

  ⇒ Wer muss mit wem gemeinsam arbeiten (/kommunizieren)

Ansprechpersonen

- Datenschutzbeauftragte (aufgrund der DSGVO)
- Sicherheitsbeauftragte (wegen Medizinproduktegesetz, BVT)
- Bundesamt für Sicherheit im Gesundheitswesen (kurz BASG)

BVT und BASG können über einen Bescheid Entscheidungen treffen, welche umgesetzt werden müssen.

Zu überprüfende Faktoren

- Firewall
  kam es bei der Firewall vorbei?
  - Wenn nicht ⇒ Interner Angriff?
  - Wurden Geräte (Systeme) direkt manipuliert?

Folgemaßnahmen

- Präventive Maßnahmen
- Das "zentralen Logrepository" überprüfen

  jedes wesentliche Modul (von einem System) muss Log Dateien speichern. Diese sollen an einem zentralen Ort gespeichert werden. Auch können lokale Log Daten an einer betroffenen Maschinen (Systemen) überprüft werden

  - Werden betroffene Daten von Maschine zu Maschine weitergegeben?
  - Welche Maschine war zuerst betroffen?

  ⇒ Ziel ist, alle Log Daten gemeinsam abzuspeichern

  - in einem LOG soll es eine zentrale Zeit geben (alle Systeme sollten eine gemeinsame Zeit haben ⇒ optimaler Fall)
  - Es sollte eine eindeutige Nummer pro LOG-Eintrag geben
  - Systeme sollten immer einen "Fingerabdruck" hinterlassen Damit Systeme nachverfolgt werden können
  - Vergleichstest:

    Dieser Test ist nur dann durchzuführen, wenn sich eine Software auf einem Gerät nie verändert hat (z.B. durch Updates). Diese Tests können ungewollte Veränderungen an der Software feststellen.

    Ablauf:

    - Einen Test beim Einrichten durchführen
    - Einen Test zu späteren Zeitpunkt durchführen, und abgleichen, ob sich Daten bzw. Ergebnisse zum vorherigen Test verändert haben

      ⇒ Wenn ja, muss was vorgefallen sein

- Externer oder interner Zwischenfall?

NIS Gesetz

- Jene Einrichtungen, die unter dieses Gesetz fallen, haben die Behörde über das Meldeteam (CERT) innerhalb einer Frist (3h), der NIS Behörde mitzuteilen
- Verordnung der Frist (3h)
    - Der Gesundheitssektor hat innerhalb von 3h Informationen über einen Zwischenfall weiterzugeben
- Es gibt 3 unterschiedliche Zielrollen, die reagieren sollten
- Da man bei 3 unterschiedlichen Behörden eine Meldung abgibt, bekommt man auch drei unterschiedliche Rückmeldungen, die normalerweise vollkommen unterschiedlich verfasst sind

  ⇒ d.h. man bekommt drei unterschiedliche "Verbesserungsvorschläge"

  ⇒ Man soll gemeinsam agieren können, sodass keine mögliche Korrekturen vergessen werden

  ⇒ Standorte sollen die gleichen sein, sodass sie sich aufeinander abstimmen können (um einen Organisationsfehler entgegen zu wirken)

  ⇒ Beispielsweise die gleiche Probleme identifizieren

  (=Transdiszlipinäre Aspekte)

⇒ Ziel ist es der Schutz der Patienten

- BASK

Ergänzungen

Ergänzen von Herr Professor Hoheiser-Pförtner:

Der Gesetzgeber hat seit vielen Jahren Safety und Security im Gesundheitssektor in verschiedenen Gesetzen verankert, wie z. B. dem Gesundheitstelematikgesetz 2012 (GTelG 2012), dem Medizinproduktegesetz (MPG) sowie seit 2018 in der Datenschutz-grundverordnung (DSGVO) und im Netz- und Informationssystemsicherheitsgesetz (NISG). Besonders „Security & Privacy by Design & Default“ sind, neben den Abstimmungen der involvierten Personen (z. B. anhand der ISO/IEC 27000-Serie und/oder der ISO/IEC 80001-Serie), Voraussetzungen für Präventivmaßnahmen der IT-Sicherheit für Hersteller, Betreiber und Anwender im Gesundheitswesen. Mit der EU-Verordnung 2017/745 über Medizinprodukte (MDR) wird mit Mai 2020 das MPG durch ein weiteres, in der EU abgestimmtes Gesetz, ersetzt werden. Einerseits schützen diese Gesetze die Bürgerinnen und Bürger im digitalen EU-Binnenmarkt, andererseits bieten sie den Herstellern die Grundlagen und die Chancen, ihre Produkte einheitlich auf Safety, Security und Privacy auszurichten.

Bei der Anwendung des NISG werden im Sektor Gesundheitswesen nicht alle Krankenhäuser und Privatkliniken in Österreich betroffen sein. Das Gesetz sieht vor, dass die betroffenen Einrichtungen einen Bescheid (siehe NISV §16 Abs. 1) erhalten und dadurch Sicherheitsvorfälle an die NIS-Kontaktstelle melden müssen, wenn ein wesentlicher Dienst für die medizinische Versorgung mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist.

„Im Internet werden unerlaubte freigegebene Labor-Daten von Patientinnen/Patienten gefunden, die/der Datenschutzbeauftrage muss binnen 72 Stunden diesen Data Breach an die DSB[1][1] melden. Bei der Überprüfung dieser IT-Störung wird eine schwerwiegende Fehlfunktion bei der Integrität der Datenergebnisse von Labor-Automaten festgestellt und diese muss unverzüglich an das BASG[2][2] gemeldet werden. Dadurch ist die medizinische Versorgung eingeschränkt und nach 3 Stunden muss an das CERTat[3][3] eine IT-Störung abgegeben werden.“ Die Prozesse für die (IT-)Störfallbehandlungen in der Krankenanstalt habe auf diese 3 Meldewege Rücksicht zu nehmen, um die Koordination der Maßnahmen und die Abstimmung aller Betroffenen bestmöglich zu unterstützen. Es drängt sich die Frage auf: „Ob eine Abstimmung zwischen der DSB, dem BASG und dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) auch erfolgt?“ ***Eine mögliche Erleichterung würde nach Meinung des Autors die Gründung eines HealthCERT beim BASG schaffen, weil sich die Meldungen zum MPG und NISG treffen und die möglicherweise zusammenhängenden IT-Bedrohungen von Safety und Security leichter erkennbar wären.***

[1][1] DSB = Datenschutzbehörde – Meldepflicht lt. Art. 33 DSGVO

[2][2] BASG = Bundesamt für Sicherheit im Gesundheitswesen – Meldepflicht lt. § 70 MPG

[3][3] CERTat = Computer Emergency Response Team Austria – Meldepflicht lt. § 8 NISV

Mitschrift, am 25.11.2019

NIS BEHÖRDE:

Das Büro für strategische Netz- und Informationssystemsicherheit ist im Bundeskanzleramt als Teil der Abteilung I/8 zuständig für Angelegenheiten im Zusammenhang mit der Umsetzung der gesetzlichen Verpflichtung aus der Richtlinie (EU) 2016/1148 in Österreich und dem Bundesgesetz für Netz- und Informationssystemsicherheit.

Wenn wir einen Bescheid haben oder ein Bescheid vorliegt müssen wir die entsprechenden Maßnahmen durchführen. Nur der der einen Bescheid von den NIS Behörde bekommt muss auch das NIS Gesetz befolgen. Parameter kann schneller auf Veränderungen reagieren, in Deutschland wird es mit Parametern behandelt.

MELDUNG MACHEN:

Mann muss immer aufpassen und schauen in welcher Verordnung man sich bewegt. Bei uns beim Nis Gesetz ist es so: nach 3 Stunden, wenn ein Ausfall noch nicht behoben wurde, muss man das an die entsprechende Behörde melden. Wenn wir diesen Störfall entsprechend gemeldet haben, analysiert man es mit der Risikoanalyse, um zu schauen welche medizinischen Prozesse lebensgefährlich sind. Diese Prozesse sind für die Versorgung des Spitals notwendig, also auch IT Services, wie zum Beispiel Transportsysteme. Das Gesetz differenziert nicht ob der Ausfall von außen manipulativ erzeugt wurde (Hacker) oder durch das Personal der IT bei einer Fehlkonfiguration zum Ausfall geführt hat. Bei der Erstbeurteilung ist es wichtig zu beurteilen ob der Fehler manipuliert wurde oder intern ausgelöst wurde. Doch immer muss man es nach 3 Stunden melden „Das ist was passiert, die Eingrenzung der entsprechenden Fehler ist noch in Arbeit“.

DATENSCHUTZ:

Datenschutzverletzung hat man immer dann, wenn Personenbezogene Daten gehackt wurden, also wenn nicht autorisierte Personen Zugriff auf diese Daten bekommen. Das bedeutet intern darf man auch nicht die MailBox von anderen Kollegen sich anhören, weil das auch unter die Datenschutzverletzung fällt.

Datenschutz sagt ganz klar es reicht nicht nur dir Überlegungen u machen wie du Daten schützt, sondern auch die ganze Umgebung und Infrastruktur. Die Problematik in dem Bereich ist die Fragestellung: Prozessaufnahme gefährdet, welche Auswirkung hat es und welche Problemfelder betrifft es? Folgen: Bei Datenschutzverletzungen kann man Daten über den Patienten verlieren und man weiß nicht mehr ob die Daten der Patienten komplett sind. Man muss also einen WorkAround bauen, unser Job ist darauf hinzuweisen, damit der Patient behandelt werden. Kurz gesagt man muss ein Krisenmanagement aufbauen und berechnen wie lange welche Krise dauern kann. Wenn eine Krise mit der Patientenaufnahme nicht nach 30 Minuten repariert werden kann, sollte man die Patienten per Hand aufnehmen. Natürlich muss man das alles davor in der Risikoanalyse definieren. „Wenn dieses Service ausfällt, wie lange haben wir Zeit das zu reparieren“.

UNTERSCHIED:

In einem Spital kann das schwer sein, weil die Ärzte nicht alle Patienten kennen und es kann zu einem massiven Aufwand kommen. Anders bei Hausärzten, die kennen meistens all ihre Patienten, somit muss man die Risikoanalyse bei den beiden Fällen anders gestalten.

NETZWERK IM MEDIZINISCHEN BEREICH:

Bei dem einem Bild mit Netzwerk im Krankenhaus ist es so, dass man den Ausfall bei dieser Strecke durch die Redundanz sichern möchte. Was man dabei nicht weiß: Wie ist es mit dem Datenschutz?

Lichtleiterinfrastruktur: Länger Distanzen und redundant, gleichzeitig hat man eine Galvanische Trennung, wenn man die nicht hat braucht man Verbindungsstücke, die diese Galvanische Trennung sicherstellen. Also wenn etwas passiert schaltet sich dieser ab, beispielsweise bei einem Fehlerstrom. Diese Infrastruktur hat auch den Vorteil, dass man im Stock keinen Verteilerschrank braucht, also muss man da auch keine Überwachung, keine Kühlung und Notstrom-Aggregatoren einfügen. Man muss also die Sicherheit nur im zentralen rechnerraum genau organisieren (also am „Anfang“ und am „Ende“ der Leitung).

In der Risikoanalyse muss man definieren wie man vorgeht, wenn etwas ausfällt und wie man Angriffsvektoren minimiert. Bei der Planung einer medizinischen Infrastruktur ist das ganz wichtig und man plant für den Raum ein anderer Risikofaktor, am besten ist es alle Räume von einander zu trennen, dass bei einem Ausfall von einem nicht alle betroffen werden: Stromkreis trennen. Jedoch braucht man das nicht in jedem Stock, manchmal ist es so, dass man das Risiko minimiert, in dem es zentralisiert wird, weil es einfacher ist Räume, die nicht wirklich von Ausfällen betroffen sind, gleichzeitig zu überwachen.

SCHADPROGRAMME:

Problematik: Ransomware sind Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln. Die Täter erpressen ihre Opfer, indem sie deutlich machen, dass der Bildschirm oder die Daten nur nach einer Lösegeldzahlung wieder freigegeben werden. Da muss man entsprechende Intrusion Detection Systeme verwenden und Programme benutzen, die die Rechner beobachten und schauen ob die sich eh alle so verhalten wir sie sollen (überwachen ob es zu Kommunikationsanomalien kommt).

Mann muss sein Personal so schulen, dass diese nicht einfach jede Datei oder E-Mail öffnet, da es in diesen FakeMail sehr wohl Schadprogramme geben kann. Maßnahmen sind: Wenn das Personal schon zum 3.Mal eine FakeMail öffnet und das bewusste, kann man sagen das dieser beim Chef salutieren muss und sich rechtfertigen, wieso er nicht nachdenkt, bevor er etwas öffnet.

Deutschland:

Bestimmte Parameter → ausrechnen ob man im kritischen Bereich liegt

(Vorteile: kann schneller auf Veränderungen reagieren, Nachteile: verschiedene Ansprechpartner)

NIS-Gesetz

- NIS-Gesetz in Österreich: Bescheid für Gesundheitswesen definiert immer 3 Stunden
- Bei einem Ausfall von min. 3h oder mehr → **meldepflichtig!!!**
- Internen Prozess überlegen!
- Wie sammle ich die unterschiedlichen Störfälle, die dazu führen, dass eine medizinische Leistung erbracht wir oder nicht?
- Wenn Störfall erhalten → Zeit laufen lassen
    - Benötigt: Risikoanalyse (stellt fest, welche medizinischen Prozesse kritisch sind (Wertigkeit oben, A-Prozesse → für Versorgung des Spitals notwendig)
    - Wenn in A-Prozessen die IT ausfällt→ bestimmte Anforderungen (medizinisch notwendig) nicht umsetzbar → Problem!

- Gesetz differenziert nicht, ob der Ausfall von jemanden von außen manipulativ („Hacker“) (BVZ,.. müssen herausfinden, wer, was, wie dagegen vorgehen,...) hervorgerufen wurde oder durch das Personal (intern)
- Erstbeurteilung (3h) → Konfigurationsfehler oder Manipulation von außen → Melden!
- Datenschutzverletzung, wenn personenbezogene (z.B. Gesundheitsdaten → noch kritischer) Daten betroffen sind (nicht autorisierte Personen haben Zugriff auf die Infos erlangt) gilt auch bei internen Problemen
- Toms schützen (gesamte Umfeld, nicht Teile)
- Bewertungen von Fachabteilungen → auf Probleme hinweisen
- Problem: Risikoanalyse → Prozessaufnahme gefährdet
- Auswirkungen:
    - Kein Zugriff auf Informationen
    - Können Daten nicht abrufen
    - Informationen über Patient nicht im KIS
    - Niedergelassene Ärzte → Krisenmanagement
        - Verifikation nicht erkennbar
        - Versichert?
        - Zahlung erfolgt?
- Reparierbar? Wie lang dürfen wir warten bis wir melden? (in Risikoanalyse definiert → wie)

Prozesse sind in A-, B- & C-Prozesse geteilt

Wenn IT nicht funktioniert → technische & organisatorische Maßnahmen

<u>Technische & Maßnahmen</u>

- Für Netzwerk (Layer 1,2,3)
    - Funktionalität versucht Ausfall einer Strecke und aller notwenigen Komponenten durch Redundanz zu vermeiden
- Lichtleiter-Infrastruktur (redundant)
    - Galvanische Trennung
    - Abhörsicher
    - Höhere Bandbreite zu Verfügung gestellt
    - über längere Distanz nutzbar
- brauchen im Stock keine zusätzlichen Verteilerschrank → nicht notwendig vor unbefugten Zugriff zu schützen
- nicht kühlen, keine Notstromarchitektur
- Sicherheit nur an Endpunkten vorgesehen
- Rahmenbedingungen
- redundante Anbindung, Stromversorgung

<u>Organisatorische Maßnahmen</u>

- Mitarbeiter trainieren
- Definieren in Risikoanalyse (auch wie wir bewerten, welche Kriterien, etc.)
- Mitarbeiter müssen sensibilisiert werden, Gewährnesschulungen)
- Software: randsomwere
- Bewusstseinskampange → in welchen Abständen schule ich meine Mitarbeiter → Schulungsprogramme
- In regelmäßigen Abschnitten darauf hinweisen

Mitschrift, am 09.12.2019

Für Test relevant:

High Level Plan-Do-Check-Act Ablauf

Bsp. Kryptographische Mechanismen

In einem Dokument festgeschrieben wo und wie kryptografische Mechanismen im Unternehmen eingesetzt werden.

- Wer ist verantwortlich?
- Welche betrieblichen Maßnahmen müssen getroffen werden?
- Wie haben sich die Akteure und die Administratoren zu verhalten?

Werden die festgelegten Maßnahmen eingehalten?

- Stichprobentests
- Penetrationstests
- Logs zentralisieren

Sind bei dem CHECK neue Probleme aufgetreten oder war die Definition im PLAN unzureichend?

- ACT: Neue Maßnahmen definieren und einführen

  Kontinuierlicher Verbesserungsprozess

Dokumentenlenkung:

- Kopf- und Fußzeilen
- Autor (Bei PLF Familienname)
- Freigabe
- Formatierung

Angabe genau lesen, womöglich unnötiger Text, den man ignorieren kann!

Testbeispiel: Problemfall der CIA-Triade

Gesetzliche Texte die beim Text zu tragen kommen

- DSGVO
- Elektronisches Gesundheitsakte-Gesetz (ELGA-G)
- Gesundheitstelematikgesetz
- Netz- und Informationssicherheitsgesetz
- Medizinproduktegesetz

Überlegungen und Begründungen genau formulieren!

Juristik schreibt Rahmenbedingungen bei der Umsetzung vor

z.B.: Patient und Arzt brauchen ein Behandlungsverhältnis, um medizinische Daten auszutauschen (im Notfall kann ein Arzt für einen anderen Arzt einspringen)

Im niedergelassenen Bereich erhält der Arzt die Erlaubnis vom Patienten auf die Daten der ELGA zuzugreifen und im Spital erhält der Rechtskörper die Erlaubnis.

z.B.: Benutzerberechtigungen dürfen nicht über Sammeluser erfolgen (Alle verwenden Admin)

Komplexität des Environments minimieren:

Nur noch das verwenden, was notwendig ist, um die Betreuung der Patienten aufrecht zu erhalten

Tagesklinik ist hier einfacher als Stationäre Bereiche

Wir benötigen auf jeden Fall Infrastruktur sowohl innen als auch nach außen und Maßnahmen, welche die Sicherheit gewährleisten.

Vorteile Glasfaserleiter

- Schwieriger abzuhören und zu beeinflussen
- Nicht elektrisch leitfähig
- Schneller über größere Distanzen

Rechenzentren müssen in brandschutztechnische Abschnitte eingeteilt werden.

Kann ich dies nicht selbst verwirklichen stelle ich jemanden an der es kann.

Regeln und Verträge müssen ausgearbeitet werden, um die Arbeit mit dem Lieferanten zu definieren.

Überprüfungen des Lieferanten führe ich selbst durch Audits durch oder stelle wieder jemanden an, der diese für mich durchführt.

Aus rechtlicher Sicht ist der Gesundheitsdiensteanbieter immer der Verantwortliche und kann diese nicht an andere abtreten, auch wenn die Leistung selbst jemand anderer durchführt. Sonst ist mit einer Klage auf Fahrlässigkeit zu rechnen.

Mitschrift, am 13.01.2020

Dokumentenlenkung war gegeben bei der PLF, Autor eintragen

Öffentlich/intern/geheim
geheim heißt, wenn nur eine bestimmte Anzahl an Personen das Dokument sehen darf

Intern

- Wo wird das Dokument angewendet?
- Wer bekommt dieses?
- →Alles mit Vereinbarung

Öffentlich

- Alles ohne Vereinbarung

Was keiner hatte: Entwurf und Freigabe. Jener Teil, wenn man die Zeit hatte, wie wird das Dokument angewendet?

History

zum Dokument, Dokumente, die ich mal gültig hatte außer Kraft setzen (hatte Gültigkeit bis… oder Versionierung, am Besten irgendwo draufstellen und hinschreiben Gültig von…bis). Denn falls ein Problem auftritt, hat man einen besseren Überblick.

Wichtig
weil: neues NIS Gesetz, eine Besonderheit macht, wählt Firmen aus, welche dann die Berechtigungen des Innenministeriums bekommen, die kommen in das Haus der Organisationen und schauen ob das NIS Gesetz und seine Lenkungen richtig eingehalten werden

Anmerkung machen: Kritikalität setzen. Wo es hoch kritisch wird verwendet man das Dokument in dem beschrieben wird was gemacht wird, wenn es hoch kritisch ist. → Macht man idealerweise nicht so, sondern fasst alles in ein Dokument zusammen.

Klassifizierung

juristisch betrachtet sind es zwei verschiedene Personen, die die ein und dieselbe Sache verwenden → Mandantenfähig→Gelderspart, aber man darf nicht auf gleiche Sachen zugreifen, sondern jeder seines. Rechtlich ist dies nicht erlaubt. Virtuell getrennt, Admin hat zwei Berechtigungen, eines für Radiologie, eines für die Klinik.

Rechtskörper muss man trennen → Mandantenfähigkeit

Technisch = Virtualisierung, saubere Trennung, Rollen und Berechtigungskonzept in beiden Systemen

Terminus

- bestimmte Rollen genau definieren
    - z.B. Notfallbeauftragte, dieser hat bestimmte Rechte
    - Mitarbeiter
    - Techniker
    - Medizintechniker
    - etc.
    - →Alle haben verschiedene Rollen und Berechtigungen

Tipp: Die Begriffe/Definitionen, wenn man weiß, dass man was beschreiben muss zb eine Rolle, dann irgendwo markieren, dass man es später noch machen soll oder CIA Triade erwähnt, oben schreiben unten dann Referenz. → löst Verständnisprobleme, zum Nachlesen

3 Meldewege beschreiben

- **1.** Data Bridge Notifikation nach 72h (stimmen grundsätzlich, wenn es keinem Aufgefallen ist, wenn Medien es merken, dann sollte man es gleich machen
    - Wann ist wo was anzunehmen (PDCA, was passiert dort?)
- Sofort, wenn man bereits drüber spricht

Es bleibt frei überlassen, wen man verantwortlich macht es dem Datenschutzbeauftragten sagt bzw. was er genau machen soll.

Im Zuge der Situation ist es kein Regelfall. Theoretisch sagen, es ist ein Notfall und daraus versuchen Personen freizuspielen. Data Bridge ist abgesetzt und übers WE merkt man, dass ein Softwareupdate eingespielt wurde und das System verhält sich nicht dementsprechend, sondern es treten Probleme auf. Man hat einen Notfallverantwortlichen festgelegt, 2. Meldung absetzen, Bundesamt und Sicherheit Bescheid geben, sofort, keine Stunden, Minuten. → Ist der Gefahr im Verzug? daher geben wir intern folgendes hervor, es wird nichts mehr an diesen Geräten gemacht. Wenn man Geräte von anderen Herstellern hat, dann verlegt man die Untersuchungen auf die anderen Geräte, auf die kein Update gespielt wurde. Wir können uns aber nie auf die Firmen direkt verlassen. Wir müssen sagen Netzwerk, Medizintechnik in Ordnung oder nicht. In Unserem Notfall betrachten wir nur wie geht es weiter, weitere Analysen, Spezialisten herholen, bestimmte Sachen nicht mehr machen. Man schaltet es nicht ab, sondern einfach Trennen vom Netz, wegen der Fehlersuche, sehen was wirklich passiert ist. Man kann da noch vielleicht spuren finden→**Beweissicherung**. So lange wie möglich Beweise aufrechterhalten.

- 2. Bundesamt für Sicherheit melden
- 3.

Bei allen diesen Vorgängen hat der Notfallbeauftragte die letzte Kompetenz, und das muss irgendwo stehen und alles genau beschreiben. Wenn jemand unten nichts versteht bei den ganzen Kürzeln, muss man oben alles beschreiben.

PLAN DO CHECK ACT

selbst entscheiden und festlegen was was ist. Besonderheit, irgendwo sollte man auch dazuschreiben, was ist das wichtigste, wenn man eine solche Situation hatte: Lessons Learned!

Es muss jemanden geben, der muss die Ausnahmesituation ausrufen und sagen „wir bearbeiten nicht den Normalregelfall." Notfall muss beendet werden.

Als Erinnerung: Das Problem bei diesem Prozess, KVP ist ja auch plan do check act, es geht nicht darum zu beschreiben, was hat wer zu tun, wenn ein notfallpassiert, sondern auch Anwendungsbereich und auch Überarbeitung. Zu Änderungen, wenn sich was gesetzlich ändert, oder wenn das Bundesministerium kommt und dort kontrolliert einmal im Jahr schauen ob sich das Dokument ändert. Regelmäßiger Ablauf Kontrolle vom Dokument ist wichtig, wenn ja nichts passiert, schön und gut aber das Dokument steht. Es kann ja sein, das bestimmte Dinge wegfallen. Wie kommt es zu dem Dokument und welche Kriterien gibt es, es zu überarbeiten. In dem Zusammenhand immer zwei PDCA, der der es tut und der der es schreibt (das Dokument).

Zweites Dokument:

- logischer und physikalischer Zutritt
- Dokumentenlenkung → Detto
- Differenzieren der Räume, Klassifikation
- Technikraum muss man externen Personen zustimmen
- Wenn man aber eine externe Firma hat, er muss auch reinkommen
    - Variante 1: es kommt immer wer mit
    - Variante 2: Vertrauen
- Bei einem internen Mitarbeiter sind wir verantwortlich
- Beim anderen hat die Firma die Verantwortung, Nachweisen müssen sie auch können, wer da war
- Eine Möglichkeit wäre der Schlüssel→Schlüsselbuch
- Karte kann man sperren, wenn ich Schlüssel habe, dann muss ich alle Schlösser tauschen (Kosten!)
- Wichtig ist nachzuweisen: wer war wann in welchem Raum, sei es jetzt Schlüsselbuch oder System, ist egal.
- Irgendwo muss es ein Zentrales Log System geben, um alles nachzuweisen können.
- Wie dokumentiere ich das im System?
- Alle Leute aus meiner Organisation auf alles zugreifen können auf die sie die Berechtigung haben.
- Beispiel wenn ein Administrator betritt einen Raum, irgendwo muss vermerkt sein, für welche Organisation er es macht.
- Wichtig bei solchen Rollen Berechtigungsschein ist die Kontrolle, irgendwo im Zyklus beschreiben, dass ich regelmäßigen oder unregelmäßigen Zyklen des Zutrittes(physisch) oder Zugriffs (logisch) Dinge kontrolliere

Zum Ersten noch: Die Beschreibung des Systems. Wie erreiche ich die Ausfallssicherheit? Redundanzen, etc. (Besonderheit: externes Rechenzentrum) intern Ausfallsicherheit und nochmal extra Absicherung mit dem externen Rechenzentrum.

- Dokumentenlenkung
- NIS-Gesetz
    - Besonderheit: wählt Firmen aus, die dann die Berechtigung von Innenministerium bestätigen. Werden über das NIS- Gesetz kontrolliert.
        - Welche Dinge müssen, wo umgesetzt werden
- Kritikalität: niedrig – mittel – hoch
- Statt drei Dokumente nur noch ein Dokument verwendet. Definieren welche Besonderheiten verwendet werden.
- Zwei Rechtskörper
- Einmal die Klinik und einmal die ausstehende Radiologie
    - Man darf es nicht gleichmäßig benutzen
    - **Mandantenfähigkeit**
    - Zwei verschiedene Berechtigungen
    - Man muss schauen, dass man den richtigen Administrator benutze.
- Ein Mitarbeiter kann z.B. zwei verschiedene Rollen einnehmen
    - Entweder ist er ein Mitarbeiter der Klinik
    - Oder er arbeitet für die Radiologie ausstehend
- Man braucht unterschiedliche Berechtigung
- Kann zu einem rechtlichen Problem kommen, wenn man sie nicht einhaltet

- **Rollenkonzept -> einen Notfallverantwortlichen**
    - Kann bestimmte Dinge tun und nicht tun
    - Wie verwende ich diese Person
- Begriffe referenzieren
    - Z.B. CIA-Triade -> oben Anmerken / unten dann auf den Begriff referenzieren
- Meldeprozess
    - 72 Stunden ist man verpflichtet
    - Man hat das Problem sofort zu melden, wenn die Sache sehr heikel ist.
    - Man muss es definieren
- 1. Meldeprozess: DatenbridgeNotification - > Patienten, die im AKH heute dran sind, sind im Internet ersichtbar. Sofort melden.
- Erste Analyse: Ein neues Softwareupdate wurde eingespielt.
    - Meldung abgesetzt
- 2.Meldeprozess
    - Gefahr im Verzug §17
    - Andere Klinken können dasselbe Problem haben, wenn dieselbe Software verwendet wurde.
    - Keine Nutzung von Gerät
    - Die Techniker, wir mit dem Problem nicht zu tun
    - Versuchen das System zu separieren.
    - Beweissicherung, wer dafür verantwortlich
- Checkliste zu Hand haben, um eine Anweisung zu haben, was zu tun ist falls es zu einem Problem kommt.
- 3.Meldung: Man stellt fest, dass es ein Cyberangriff ist.

PLAN, DO, ACT, CHECK

➔ Ablauf des Gesamtverlauf, ein Notfall muss aufgerufen werden, Notfall beenden

Während dem Durchlauf

- Nächste Woche Montag- > schriftlicher Teil nachholen
- Mitarbeitsaufgabe bis Freitag -> eine verbesserte Aufgabe von letztem Test
    - Eines der Dokumente aussuchen!
- Kontinuierliche Verbesserung
    - Wo wird es angewendet, wo kommt es zu einer Änderung
    - Neues Gesetz
    - Einmal im Jahr sollte das Dokument überprüft.
        - Wird dem Lenkungsausschuss niedergelegt
- Betrifft das Dokument
- Die Handlungsweise für die Person die es ausführt

➔ Große Fehler: Dokumentenlenkung , nicht vorhandenere Prozess fürs Ausrufen(Meldeprozess)

- Zutritt: Klassifizierung der Räume. Wer darf in den Raum rein?
    - Technikraum darf nicht vom Arzt betreten werden außer es herrscht eine Ausnahme.- > muss geregelt
    - Bei interem Personal ist die Technikbetrieb verantwortlich , wenn es extern ist.
- Organisatorisch zu achten: Wer war wann in einem Raum? ANALOG auf die Systeme, es gibt einen User. Wir brauchen einen Rollen und Berechtigungsgesetz

Mitschrift, am 10.02.2020

NIS Gesetz:

- Gesundheitsdienst muss aufrechterhalten werden
- Kommt dann zu tragen, wenn das Haus zur kritischen Infrastruktur des Gesundheitswesens zählt
- Nach 3h Beeinträchtigung

Vorgang:

- Krankenhaus in Fachbereiche unterteilen -> überschaubar Menge minimieren -> Sicherheitszonen
- Rahmenbedingungen für diese Zonen
- Entscheidungskompetenzen definieren
- Personal für Aufgaben in Sicherheitszonen
    - Wenn Notfall ausgerufen wird - > Regeln des Normalfalls gelten (teilweise) nicht mehr

Problem in medizinischen Einrichtungen: sehr viel zwischenmenschlicher Kontakt -> „Eindringling“ könnte als Besucher getarnt sein -> lokaler Angriff

3 Zonen:

- Kernzone
    - Große Problematik bei teilweisem oder ganzem Ausfall von Systemen
    - Notwendig um medizinische Versorgung und alle unterstützenden Systeme aufrecht zu erhalten
    - z.B. Serverraum, …
- Mittelzone
- Randzone

SKKM (Staatliches Krisen- und Katastrophenschutzmanagement)

Die Abwehr, Beseitigung oder Linderung der Auswirkungen drohender oder eingetretener Katastrophen (Katastrophenhilfe, Einsatzvorsorgen) ist in Österreich überwiegend eine Angelegenheit der Bundesländer. Die rechtliche Basis bilden die Katastrophenhilfegesetze der Länder, die vor allem die Feststellung der Katastrophe und die behördliche Einsatzleitung in den Gemeinden, Bezirken und Ländern festlegen. 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. (Entnommen aus https://www.bmi.gv.at/204/skkm/start.aspx, 10.02.2020)

- Struktur über Rollen
    - Einsatzleiter/in
    - Stabsfunktionen (S1 – S7)
        - Personal,
        - Logistik, …

NIS Gesetz: Dienst aufrechterhalten (Gesundheitsdienst)

Verantwortung: so gut wie möglich für uns zu unterteilen

Ziel: Gefahren auf überschaubare Menge minimieren → Einführung der Sicherheitszonen

Rahmenbedingungen definieren

Hauptproblem: Wir sind Spital → mehrere Bereiche

starker Patientenkontakt + Angehörige

Überwachungsmonitore usw. → lokaler Angriff durch Tarnung als Patient, Besucher, externer Medizintechniker

Zonen mit Kritikalitätsgrenze

- **Kernzone**: Serverraum, OP-Räume, Verwaltung (Planung der OP, Materialverwaltung), große Teile des technischen Bereiches (Strom - USV, Klima, Heizung, Lüftung), Radiologie

  Katastrophenplan SKKM (Staatliches Krisen und Katastrophenmanagement)
  Landeshauptmann/ -frau verantwortlich
  Innenminister wenn Regionsübergreifend
  Bundesministerium für europäische und internationale Angelegenheiten
  dabei immer Bundespräsident + Bundeskanzler

  Wer nimmt welche Rolle wahr (**Stabsfunktionen** S1 – S7 (international 7 nicht vorhanden, nur Österreich)) → Einsatzleiter für Katastrophenfall in Krankenhaus verantwortlich

  - **Personal** (welches Personal brauche ich wann wo, in welcher Konzentration)
  - **Logistik** – Material (was brauche ich, wie viel, von wo können diese an die entsprechenden Stellen geliefert werden)

  Katastrophe: Notfall ausgerufen → kein gewöhnlicher Ablauf mehr → Notfallstrategie
  Data Bridge Einfluss auf Ablauf? → kann zu einem Risiko werden
  → der Sache auf den Grund gehen
  z.B. Medizinprodukt CT (verantwortlich Technischer Leiter)
  Medizinproduktegesetz: Situation muss an Bundesamt für Sicherheit im Gesundheitswesen gemeldet werden, da andere Krankenhäuser dieselben Medizinprodukte verwenden könnten

  mit Mai 2020 → Medizinproduktegesetz durch Medizinprodukteverordnung abgelöst

  Agentur für Sicherheit im Gesundheitswesen (AMA) in England (international)
  DSGVO: Data Bridge Meldungsfrist 72h
  Definition von „Beeinträchtigung“:
  - CERS (Computer Emergency Response Team)
  - Trouble Ticketing System (für organisatorische Handhabung)
  - Zentrale Stelle für Problemmeldungen

  Derzeitige Lösung: DSGVO + NIS Gesetz + Medizinproduktegesetz beachten

  an wen haben wir gemeldet, von wem kriegen wir was zurück → Zentrales Katastrophenschutzteam die alles Sammeln mit Stabsfunktionen → Verarbeitung und Reaktion auf einfließenden Informationen → dynamische Lage, d.h. als Einsatzleiter laufender Prozess Informationen über Zustand

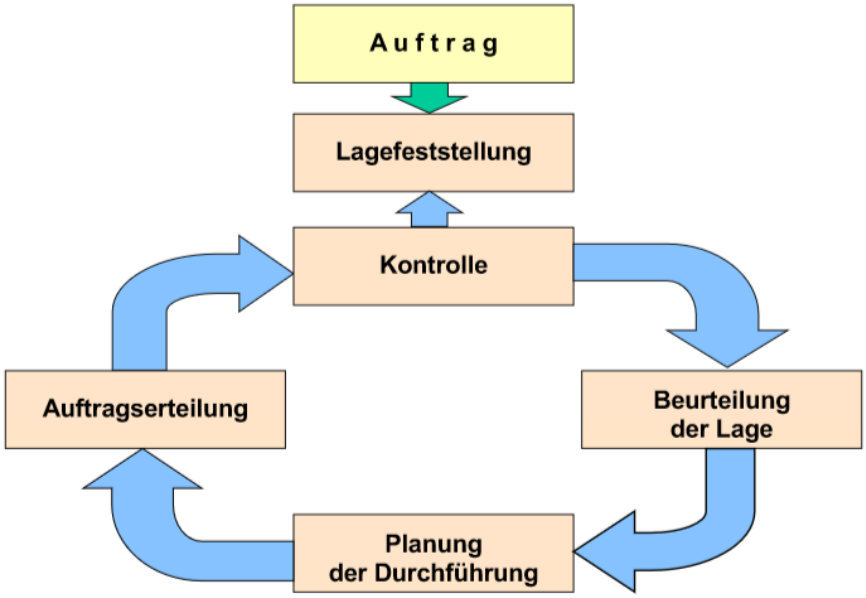
Mitschrift, am 17.02.2020

Wenn ich mit den vorgefertigten Plänen nicht zurechtkomme habe ich eine Ausnahmesituation, dann **SKKM→ Staatliches Krisen- und Katastrophenschutzmanagement**

Es gibt eine Person, die für alle sagt, es gibt eine Katastrophe. (Person braucht gewisse Qualifikationen und Informationen, um Entscheidungen treffen zu können)

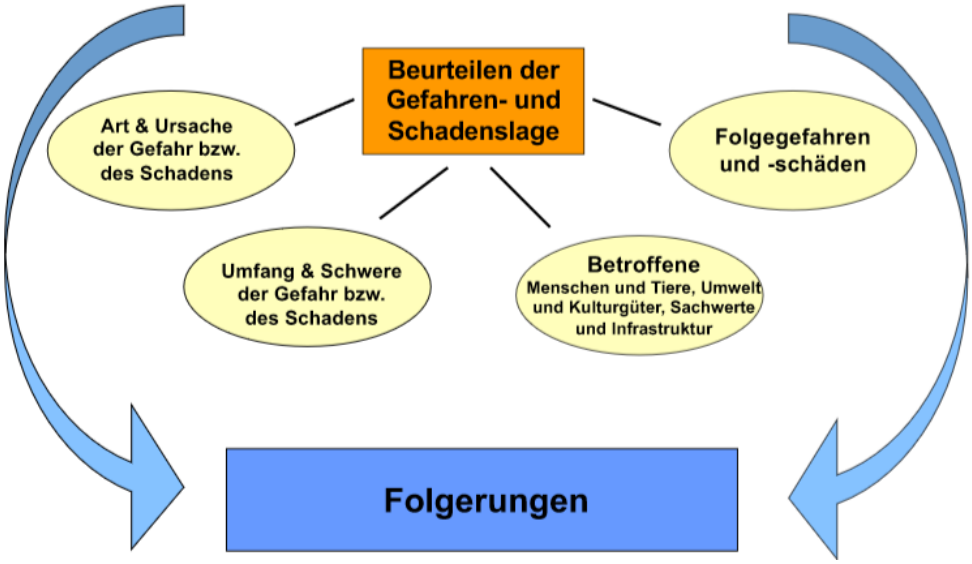
Sobald eine Katastrophe ausgerufen wird sind die normalen Verfahren ungültig.

Regelkreis der Führung:



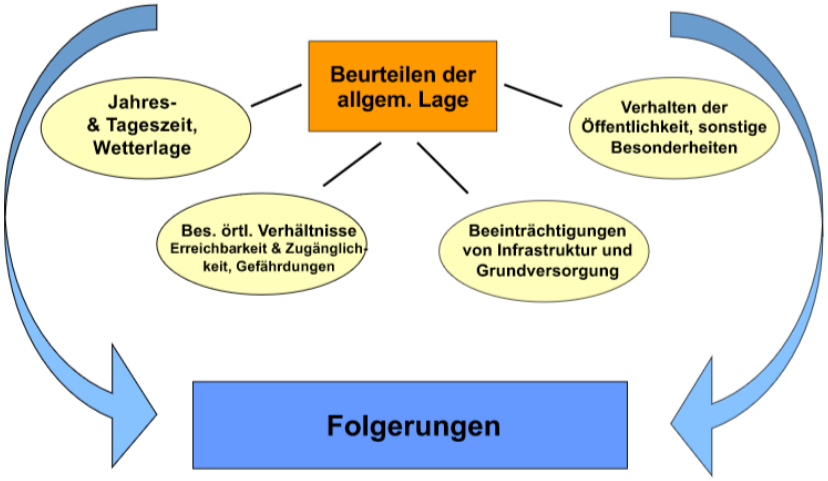
Auftrag → Plan Do Check Act

Beurteilung der Gefahren- und Schadenslage



Was bedeutet das für uns → welche Kraft muss ich in welcher Zeit liefern

Beurteilung der allgemeinen Lage:



Bin nur ich oder z.B. ganz Österreich betroffen → Kann ich auf Hilfe von außen hoffen

Entschlussfassung:

Festlegung von:

- Kräfte und Mittel (Einsatzelement)

- Wesentliches der Durchführung

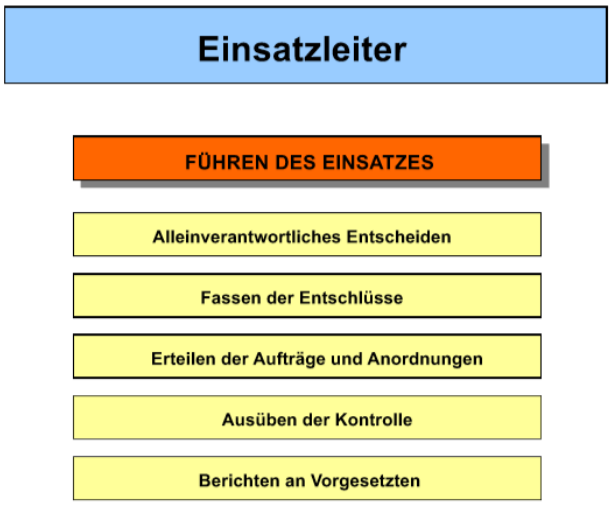
- Ziel

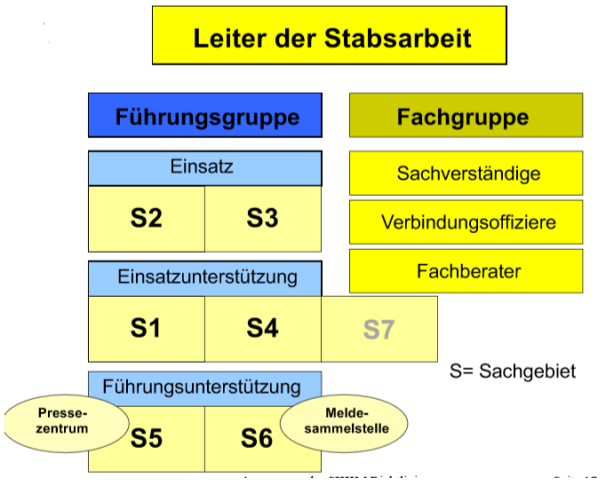
> Wer macht

> wann und > wo> was und > wie

> warum

Stabsarbeit:





S → Sachgebiet

S1: Personal

Kümmert sich um das Personal (Wie lange ist wer schon im Einsatz)

S2: Lage

Informationen sammeln und bereitstellen

S3: Einsatz

Kurzfristige Erstellung eines Prozesses

Hat der Prozess was gebracht

Dokumentation

S4: Versorgung (International auch für die Psychologische Betreuung)

Kümmert sich um die Ressourcen

S5: Öffentlichkeitsarbeit

Für die Presse zuständig

S6: Kommunikation

Stellt Telefonnummern zur Verfügung

Sicherstellung der kompletten Kommunikation (intern/extern)

Kommunikationsplan

S7: Ganzheitliche Betreuung

In Österreich für die Psychologische Betreuung

ENISA → European Union Agency For Cybersecurity

Richtlinie bei Großschadensereignissen für österreichische Blaulichtorganisationen, Katastrophenschutz laut ÖNORM – siehe Moodle. Norm richtet sich nach internationalen Richtlinien. Hilfreich für Bewertung, Bewältigung von solchen Ereignissen.

Ausnahmesituation bedeutet, daß man nicht mit herkömmlichen organisatorischen Mitteln auskommt. Anwendung von SKKM (staatliches Krisen- und Katastrophenmanagement). Überlegung: Wie gehe ich mit der Situation um?

Derjenige, der das Ereignis zur Kenntnis nimmt, muß die Krisensituation ausrufen und die Führung übernehmen. Innerhalb der Organisation soll es einen geben, der eine Krisensituation ausrufen kann. Wird ein Notfall ausgerufen, ist die herkömmliche Organisation außer Kraft. Es soll festgehalten werden, welche Kompetenzen/Befugnisse der Verantwortliche hat.

Einheit der Führung: Einer ist verantwortlich, Aufgaben sind definiert. Hierarchische Struktur, weil man im Notfall keine Zeit verlieren darf.

Ziel der Richtlinie: Medizinische Versorgung im Sinne von Integrität, Vertraulichkeit, Verfügbarkeit gewährleisten.

Wir haben nur begrenzte Ressourcen zur Verfügung, egal ob personell, materiell. Wichtig: Reserve bilden, um im Notfall Kapazitäten zu haben.

Lagefeststellung: Wo befinden wir uns gerade, welche Situation haben wir? Bild von der Lage verschaffen, immer wieder neu bewerten. Bewertung der eigenen Lage; bin nur ich betroffen?

Regelkreislauf: Organisation gibt Auftrag (Lagebild, Handlungsanweisung) -> Plan Do Check Act

Kräfte-Raum-Zeit-Kalkül. In welcher Zeit muß ich welche Kräfte (Ressourcen) aufwenden, um ein Ziel zu erreichen?

Allgemeine Lage: Wer ist betroffen? Nur ich? Die ganze Stadt? Abhängig davon Hilfe zukommen lassen, je nach Kritikalität.

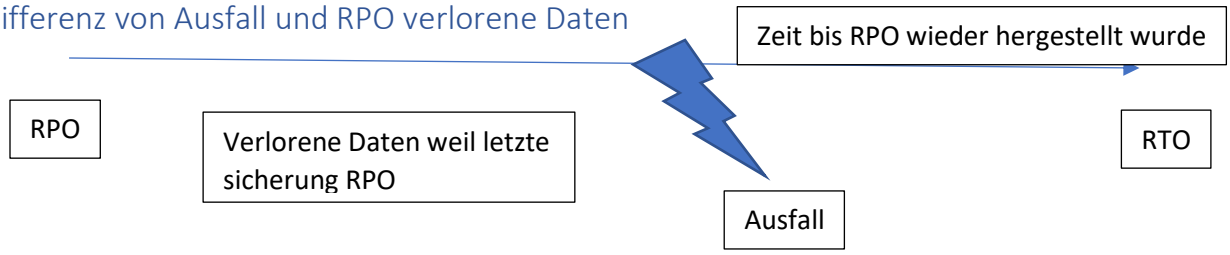
Entschluß treffen: Kräfte, Ressourcen einteilen. Wer macht wo wann was, wie und warum? Aufgaben einteilen.

Aufgabe des Einsatzleiters: Führt, trifft Entscheidungen, Kontrolle. Weitere Organisation: Fachgruppen, Stabsfunktionen S1-S7. Leiter des Stabes: Vertretung des Einsatzleiters, Kommunikation mit Leiter anderer Organisationen.

Mitschrift, am 24.02.2020

- Sachen schnell eskalieren
- Skkm = Staatliches Krisen- und Katastrophenschutzmanagement
- Österreich
- Wichtig in dem Bereich Schutz der kritischen Infrastruktur (Austrian Programm for Critical Infrasturcure Protection = APIP)
- Wichtig ist die Infrastruktur = alle Dinge, die wir benötigen um über Kabel oder mobil daten/daten austauschen
- Dieses Jahr Übungen (= weniger Energie 70%) Erfahrung aus Schweiz die Protektion greift nicht
- Auf uns umlegen auf KH, ähnlich BCM, DRP
- Zonen (Kernzone) Menge der betrachteten Objekten (HW, SW) um für uns ein Modul zu schaffen welches in einer Ausnahmesituation umgegangen werden kann Business Continuity eine Widerstandsfähigkeit zu schaffen (wie bei einer Impfung) beim Technischen wird dies durch Ausfall Sicherheit und Redundanzen geschaffen und so kleiner das ist desto leichter zu betrachten
- Bei der Planung muss all dies festgelegt werden auch Überwachen Plan Do Check Act
- In Wirklichkeit nicht planbar, weil mit BCM wollen wir Risiken vermeiden doch ist ein Rest Risiko immer vorhanden
- Verschieden Technische und Organisatorische
- Vorbeugen durch Überlegen
- Falls doch in Ausnahmesituation SKKM und BCM greift nicht mehr
- Theoretische Abhandlung der Regeln und des PDCA
- Bei Ausfallübungen können die Maßnahmen überprüft haben
- RPO (Recovery Point of Objective) links auf zeit achse
- RTP (Recovery Time of Objective) rechts auf zeit aches
- Irgenwo auf Aches Ausfall

Differenz von Ausfall und RPO verlorene Daten



- Notfall System keine gespeicherten Informationen zugriff Real Time Parameter vorhanden in einem Medizinischem KH System
- In Stresssituation höhere Chance auf Fehler deshalb Ausfallsicherheit, um nicht in Stress zu kommen
- Hoch Sensible Informationen schwierig, wenn dritte helfen
- Rot, Grün, Gelb, Weiß sagen über die Kritikalität des Inhalts aus sozusagen Zugriffs Berechtigungen wer darf das Wissen und wer nicht
- Andere Organisationen sind da zum Helfen meißt deshalb gelb und grün
- Wir benutzen Traffic light protocoll ERHÖT PUNKTEZAHL BEI TEST (weiß, grün, gelb, rot)
- Rot: nur eigene Info
- Gelb: mit anderen
- Grün: offen

Mitschrift am 02.03.2020

Zusammenfassung

In dieser Mitschrift werden auf die Zonen eingegangen, die wir beachten müssen und welche Regeln bei extern und intern gelten müssen. Des Weiteren wird erklärt, wie man diese am besten schützt, und wie diese Architektur aufgebaut werden kann.

Zonen

Zonen sind ein wichtiger Aspekt für unser Konzept
bildlich betrachtet können wir dies so sehen

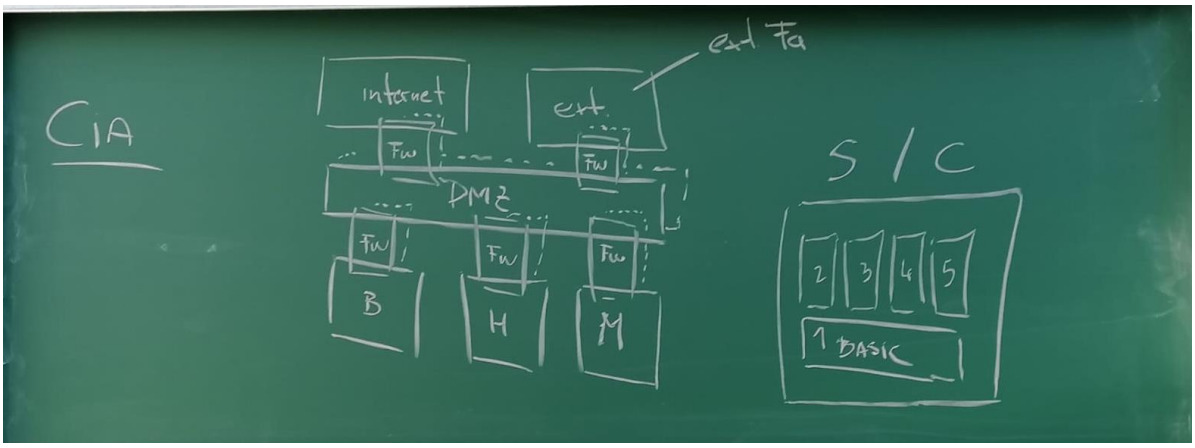
|internet| |extern|

Wir haben bestimmte Regeln, die bei Intern und Extern gelten
Bei externen Firmen müssen wir sicherstellen, dass es keine Querverbindung zum Intranet gibt. Wir könnten zum Beispiel einen externen Rechner nehmen, wo sich die Externe verbinden kann.

Extranet = alle Organisationen mit denen wir einen Vertrag haben

z.B. Wartungsaufträge am System

3 Zonen, die wir bedenken müssen



Büro

Haustechnik

Medizin Technik - Labor, Röntgen, OPs, Stationen, Ambulante Bereiche

…definieren bestimmte Dinge, die in der Zone passieren dürfen oder eben nicht.

DMZ (Rechner), bei diesem wäre es wichtig, wenn bei all diesen Strukturen Firewalls existieren

DMZ: jump host damit nicht direkt aufs Interne Netz zugegriffen werden kann

Ob das eine zentrale Firewall ist ist egal, allerdings ist eine Reduanz wichtig
Bei den Rechnern ist dies auch wichtig
Je nach Fall ist dies auch bei Büro, Haustechnik, Medizin Technik notwendig
In einer OP oder in einer Intensivstation ist ein kritikales Problem, dadurch benötigt man bestimmte Sicherheiten

Für jeden Bereich gelten anderen regeln die auf Verträgen beruhen und durch u.a. Firewalls umgesetzt werden.

- Datenschutzvertrag: DSGVO, med. Umfeld -> Daten werden gespeichert
- Verschwiegenheitspflicht: z.B. externer Berater / Systemtester -> Daten werden eingesehen

Ziel: Systematische Herangehensweise der Soft und Hardwarekomponenten (so einfach wie möglich Hantierend) dh. Ziel ist es, die verschiedenen Komponenten (Hardware und Software) zu differenzieren, während das Arbeiten (und bearbeiten) mit den Komponenten so einfach wie möglich gehalten werden soll.

Einheitliche Architekturen werden geschaffen: Basiskomponenten + Zusatzmodule

Differenzierung ist relevant!
Unterscheidung der Elemente sollen beachtet werden und eine einheitliche Architektur ist wichtig

Überlegungen unbedingt niederschreiben, damit es auch für andere klar ist! (BSP: Verhalten im Brandfall)

Je besser unsere Architektur ist, desto weniger Aufwand wird man später haben.
Alle Komponenten auf einem Server zu implementieren die ausfallsicher sind bzw. mehrere Zentrale Instanz virtueller Zugang → Daten sind nicht lokal gespeichert oder auf dem System Die Gefahr wenn hier etwas ausfällt, ist dies sehr groß - argumentieren was man empfehlen würde: Dinge so niederschreiben, dass es in einfachen Sätzen nachvollziehbar ist, was haben sie sich dabei gedacht, welche Überlegung, warum so trennen, welche Sicherheitsüberlegungen haben sie gemacht - hierbei geht es darum das sie ein Architektur oder ein Sicherheitskonzept haben

Gesetzliche Rahmenbedingungen müssen auch realisiert werde - Rollenverteilung, Datenschutz Verträge (DSGVO - medizinisches Umfeld, Aufgabe etwas zu verändern), Verschwiegenheitserklärung (Systeme auf den neusten Stand überprüfen- hat alle Daten aber hat sie nicht gespeichert) → bei beiden kommen Personengruppen, die etwas für uns machen

Bei Fernwartung zb.: wenn sein eigenes Netz bei einem Cyberangriff in Mitleidenschaft gezogen wurde und einen Virus hat dann soll er uns benachrichtigen

NEWS: Nicht so wie bei Microsoft - seit 5 Jahren ein Problem

DataLeek - darum so wichtig, weil dann im Internet alle Daten frei im Internet einsichtig sind, zb.: wer hat welche Krankheit, gerade eine Geschlechtsumwandlung hat, etc.

Optimal wäre, wenn wir Logfiles oder Dump übermitteln prüfen wir ob Personenbezogene Daten drinnen sind und wenn dann geben wir sie raus

Differenzierung zwischen Datenschutz und Verschweigenheitserklärung ist wichtig und es muss auch einen Vertrag zur Absicherung geben

Regeln: Governence

Überlegt wo die Gefahren sein können

GRC - Control (Nachweis, zb.: mittels eines Konzepts, welches die Sachen von Oben beachtet/ Steuern soll man hier auch - werden die Dinge umgesetzt, so wie wir wollen - Prüfung in regelmäßigen Abständen zb.: Penetrationssoftware (dort wo das Eindringen gelingt sollte man etwas ändern)

Die Mitarbeiter die die Firma verlassen, müssen alles abgeben (die Accounts sollen inaktiv werden, Schlüssel abgeben, Handy abgeben) Außerdem muss nachweisbar sein, wer Zugriff hatte, deswegen werden die Accounts nicht gelöscht, zusätzlich gibt es UIDs, welche eindeutig vergeben sein soll Die User werden aus dem System ausgetragen, verschlüsselt werden die Originaldaten gespeichert, bei Bedarf wieder gezeigt

Wenn man diese nicht verschlüsselt ist, kriegt man eine Strafe (weil die Daten nicht mehr benötigt werden eigentlich)

Prüfroutinen (PDCA)

TODO

- Unterlagensammlung!

Anmerkungen

5G - Netz Höhere Bandbreite lässt komplexere Dinge leichter machen

Thin Clients: nur Image übers Netz: kein OS, keine Datenspeicherung auf dem lokalen System (geht z.B. bei Büroautomatisation) (wird bei vielen Geräten allerdings nicht funktionieren)

GRC: Gesetzliche Rahmenbedingungen und Control

Mitschrift, am 09.03.2020

YouTube Video : Hackerangriffe auf Krankenhäuser | W wie Wissen

Das Öffnen von Attachments - Ransomware - schleicht sich auf den Rechner ein und greift ihn von ihnen an. Das Wichtige ist, dass man nur Maßnahmen treffen kann, diese schützen einen aber nicht zu 100% vor einem Angriff. Deshalb muss man es in verschiedene Sektionen unterteilen, Zum Beispiele mehrere virtuelle Rechner. Auf einem lokalen Rechne sollten nicht die Systemarchitekturen, etc. gespeichert werden. Security bei Design bedeutet, dass die Sicherheit durch einen speziellen Aufbau der Systemarchitektur gewährleistet ist.

Die Medizinproduktkomponente wird vom Hersteller produziert, welcher mit den etwaigen Risiken rechnen muss und jeweilige Maßnahmen treffen muss.

Zum Beispiel: Galvanische Trennung - Sicherheitswiderstand
Unter galvanischer Trennung (auch galvanische Entkopplung) versteht man das Vermeiden der elektrischen Leitung zwischen zwei Stromkreisen, zwischen denen Leistung oder Signale ausgetauscht werden sollen. Die elektrische Leitung wird dabei durch elektrisch nicht leitfähige Kopplungsglieder aufgetrennt.- Wikipedia

Praxisbeispiel

Station mit 12 Betten, die bestimmte Anzahl an Zimmern mit Betten muss die benötigten Monitorfunktionen aufweisen. Wichtig Notstromversorgung. Diese Informationen werden weitergeleitet auf Server, etc. Die Daten die aufscheinen am Monitor, werden auch in einer zentralen Überwachungsstelle sichtbar -> zB Schwesternnotruf, Telefon mit Notrufknopf

Zentralkomponente fällt durch Virus aus, deshalb gibt es keine Überwachung mehr -> Andere Überwachungsmöglichkeit (Person in jedem Zimmer, etc.), Notplan wird benötigt um Überwachung zu gewährleiten, welche Personen können welche Aufgaben übernehmen.
Zimmer (Sektor) muss erhalten werden, obwohl Zentralkomponente ausfällt. Dafür wird ein Konzept benötigt.

YouTube Fall: 14 Tage zuvor wurde ein Award überreicht, für den Umstieg auf elektronische Verwaltung, etc. Wie hätte es verhindert werden können? Mitarbeiter informieren, Schulung, Nicht an die Öffentlichkeit gehen, …, TEST (Leute anheuern die versuchen das System zu hacken)

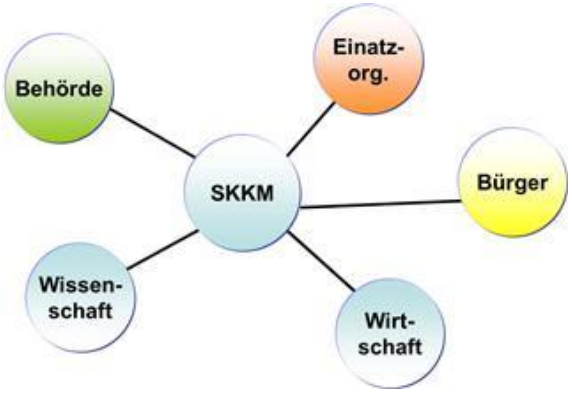
PLAN DO CHECK ACT - Vorgaben unterliegen einem Alterungsprozess
Die Vorgaben sind auf den zu dem Zeitpunkt aktuellen Stand angepasst, es kann aber sein das diese Vorgaben nach einigen Monaten oder Jahren nicht aktuell sind und dadurch nicht auf etwaige Bedrohungen vorbereitet sind.

Business Continue & Desaster Recovery - versuchen mit Maßnahmen den laufenden Betrieb zu erhalten und einen Plan für den Ernstfall haben.
Im Notfall: Zonen voneinander trennen -> Ausbruch eindämmen

Die Problematik wird aus der Technischen, nicht aus der medizinischen Sicht betrachtet. Die Entscheidungen medizinischer Natur, unterliegen dem medizinischen Personal. Die Aufgabe der IT ist es die Daten zur Verfügung zu stellen. Wichtig: Der Fehler ist schnell aufgefallen, deshalb konnten sofort Maßnahmen ergriffen werden. Es ist wichtig das die Personen rechtzeitig informiert werden, damit man weiß ob die Daten noch richtig sind.

In dieser Situation muss man dann alles auf Papier erfassen, dass ist wichtig / besser auf Formularen, ansonsten ist es zu unübersichtlich. Anweisungen an das Personal sind wichtig, damit der Prozess effizient bleibt, sowie Engpässe vermieden werden.

Verfügbarkeit und Integrität sind in diesen Situationen besonders wichtig. In diesem Momenten muss man wissen was eine Notsituation ist, welche Personen informiert werden müssen, welche Maßnahmen müssen getroffen werden. SKKM - Staatliche Krisen und Katastrophen Management



Krisenschutz - > Krisenschutz wird zusammengestellt und jede Person hat eine eigene Rolle zum Beispiel IT Sicherheit, etc. In bestimmten Zeitabständen, zum Beispiel 2 Stunden, werden neue Informationen eingeholt, um zu sehen ob die getroffenen Maßnahmen wirksam sind.
Beispiel Krisenstab Coronavirus
Wenn eine Krise beim Coronavirus ist und eine Krise im IT Schutz gibt es zwei individuelle Krisenstäbe, aber diese müssen miteinander kommunizieren. Kommunikation ist sehr wichtig, was ist zu tun, was ist betroffen, was darf ein/ausgeschalten werden, Reaktivierungszeit?

Alle Ausarbeitungen werden so bearbeitet, dass nur der IT-Teil betrachtet wird, mit dem Teil, dass mit der Medizin kommuniziert werden, bzw. einem Krisenstab.

BVT -> Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

LVT -> Landesamt für Verfassungsschutz und Terrorismusbekämpfung

Wo sind die Schnittstellen. Gesetze: Datenschutz, Medizinprodukte, RIS Gesetz. Was für ein Problem ist es? Labor, MRT,…?

Wenn man auf ein Problem stößt, muss analysiert werden was es für ein Problem ist. Man muss sich überlegen, wann zum Beispiel ein System Alarm schlagen soll und unter welchen Umständen. Je nach Gesetz und um was es geht ist es wichtig wann der Alarm ausgelöst wird, zum Beispiel 72 h Datenschutzgesetz. Meldungen müssen ans CERT gehen, wenn ein Bescheid vorliegt, aber auch auf freiwilliger Basis kann gemeldet werden (sehr selten).

Ein Coreswitch ist ein verbindendes Gerät in Computer-Netzwerken. Coreswitches sind sehr leistungsfähige Switches, die das Rückgrat (Backbone) eines Netzes bilden.