**Mitschrift**

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**

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. 5AHBGM - MIS Protokolle Jahr 2019/20 04.04.2020 Seite 37 von 37 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.