MIS-Protokoll vom 27.09.2022

Thema: Schutzziel

Das Schutzziel fokussiert sich immer auf die CIA-Triade.

CIA-Triade → Vertraulichkeit, Integrität und Verfügbarkeit - Schutzziele der Informationssicherheit.

Ich muss mir bewusst sein das immer gewisse Bedrohungen vorhanden sind.

Normenwelten (Management System für Informationssicherheit). Die Aufgaben eines Management System sind die Verbesserung der Kundenzufriedenheit und -loyalität, die Verbesserung der Unternehmens-prozesse im Hinblick auf optimale Produkte und Arbeitsergebnisse, Einsparungen von Ressourcen und Entsorgungskosten.

ISO26000 Serie – Vielzahl von Dokumenten – definiert Managementsystem für Informationssicherheit

➔ **Dabei unterscheiden wir zwischen:**

- *Präventiven Maßnahmen* (Ein Problem einschränken), es gibt entsprechende Maßnahmen, die agieren sollen. Warum wird es ein Problem geben und wie Stelle ich mich dem?

- Wenn diese präventiven Maßnahmen nicht greifen, muss ich mir überlegen, was meine Prekativen Maßnahmen sind.

- Unterschied zwischen *Normalsituation (Normalfall vs. Ausnahme).* Die Ausnahme hat 2.Arten: Krise (Krise die länger andauert oder bestimmte Rahmenbedingungen hat bzw. Katastrophe)

Beispiel → Notebook fällt aus → etwas womit wir rechnen müssen, welche alternativen dazu gibt es?) → Lösungswege betrachten und einen Ausweg entscheiden→Lösung nicht mit eigenen Mitteln realisierbar – dann Krise (Hilfe von außen usw.)

Gesetz: Netz und Informationssicherheitsgesetz und Verordnung

➔ Basiert auf Netz und Informationssysteme
➔ Alles verläuft planmäßig – Normalfall
➔ Ausnahmesituation in Normalfall umwandeln

Wenn etwas passiert, überlegen wir wie wir das bewältigen wollen.

Wenn wir das nicht machen, dann kommen wir in die Krise.

Wenn wir das nicht regeln können, dann sind wir in der Katastrophe

Beispiel: Applikation

- ➔ DB-System mit gespeicherten Informationen
- ➔ System kann defekt gehen
- ➔ Bedrohung
- ➔ Hacker verschlüsselt DB – wenn sowas passiert – Daten wiederherstellen – Strategie – Backup
- ➔ Wiederherstellung der Daten ist nicht möglich
- ➔ Backup nicht möglich -> Plan wie wir damit umgehen müssen

Normalfall vs. Ausnahmefall

- ➔ Desaster – welche und welche Möglichkeiten zum beseitigen
  Betrieb würde „eingeschränkt" funktionieren

Welche Prozesse haben wir und wie wollen wir diese schützen? Und wenn, wenn der Schutz nicht greift – Plan B (Desaster Recovery)

Beispiel:

Klinik – wenn System ausfällt – Auswirkung auf Klink

Business Impact Analysis ➔ Eine Business-Impact-Analyse ist im Business Continuity Management eine Methode zur Sammlung und Identifizierung von Prozessen und Funktionen innerhalb einer Organisation, um die den Prozessen zugrundeliegenden Ressourcen zu erfassen.

Wenn ein Ausfall des Systems passiert, kann man Patienten trotzdem behandeln.

Labor, Röntgen, Apotheke können weiter Arbeiten nur auf Blatt Papier.

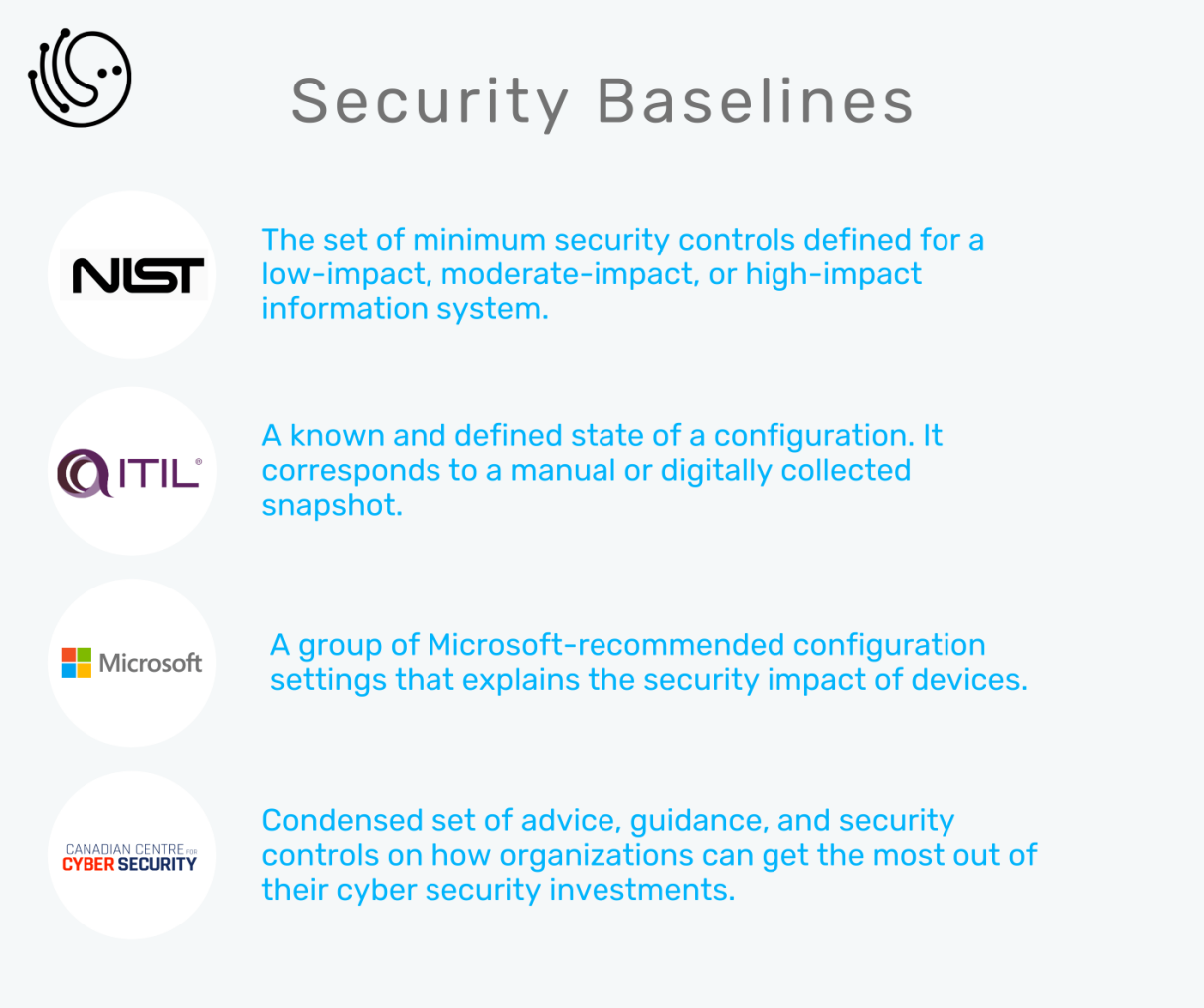
Wichtigste Prozesse: alles mit GIS, Aufnahme, Verrechnung, Entlassung

Notfall: INFOS mit Hand mitschreiben können für Verrechnung

Nicht betrachtete Dinge: Mediziner Reaktion gegenüber Patienten

Wichtig: Apotheke, Aufnahme von Patienten, Essen, Wärme, Nahrung und Küche damit alle versorgt werden können

Baseline Security (Basisschutz) → MBSA ist ein kostenloses Werkzeug, das Windows auf Sicherheitslücken untersucht. Es soll etwa typische sicherheitsrelevante Fehlkonfigurationen in Microsoft-Produkten und Windows ausfindig machen.



Quellen:

Baseline Security (Posture) Monitoring is the New Breach Monitoring (octiga.io)

Was ist Business Impact Analysis (BIA)? - Definition von WhatIs.com (computerweekly.com)