Antonela Cabro
Djordje Jovanovic 13.09.2022

PROTOKOLL

Unser oberstes Ziel in einer Klinik ist der Schutz der CIA-Triade. Der Schutz bedeutet, dass wir uns überlegen müssen welche Maßnahmen umsetzen damit Verträglichkeit, Integrität und Verfügbarkeit in einer bestimmten Konsultation gewehrleistet wird.

Vorgangsweise, diese Vorgangsweise bedient sich im Internationaler Umfeld alle Organisationen, weil sie dasselbe Problem lösen wollen. Das Problem, welches gelöst werden soll, ist, wie schütze ich mich vor Manipulation, immer im Fokus auf unsere Informationen und digitalen Prozesse. Die Vorgangsweise ist, die man führt, ein ISMS ein. Für das ISMS gibt es eine Norm, die ISO-Norm lautet 2700 Serien.

Wie geht man an so ein System heran?

Zuerst Analysieren, welches Problem gibt es? EIN BEISPIEL DAZU:

- University of Hiver hat einen Hackerangriff auf dem Computertomographen simuliert und hat die Bilder des CTs, durch Software so manipuliert, dass ein Nicht-vorhandener Tumor in die Lunge eingepflanzt wurde.
- Diese Bilder wurden dem Arzt vorgelegt, die Ärzte hätten anhand der Bilder sofort eine Notoperation des Patienten angesetzt
- In diesem Fall gibt es eine Bedrohung, was ist in der CIA-Triade bedroht?
    - Vertraulichkeit, wahrscheinlich, aber eher vernachlässigt, weil, wenn ein Unberechtigter auf ein System zugreift und die Infos liest, ist die Vertraulichkeit komplementiert aber Manipulation der Information wiegt schwerer
    - Integration: Problem, weil Indignität von Informationen kann nach bestimmten Mechanismen überprüft werden, hängt ab vom Sender der Information die Integrität in dem System aufrechterhaltet.
        - Risikoanalyse haben wir, Risko ist, dass die Daten verändert werden
        - Wie schützen wir die Integrität

Wie schützen wir die Integrität:

Verschlüsselung von Daten, wäre eine Variante, wenn wir nur Berechtigte drauf zugreifen lassen, aber Integrität kann damit nicht überprüft werden. Wir können auch signieren.

Antonela Cabro
Djordje Jovanovic 13.09.2022

Wie kommen wir die Manipulation der Daten aufhalten?

Wir benötigen PKI; heißt es muss jemanden geben, der die Zertifikate ausstellt. Wenn wir es selbst sind, müssen wir PKI selbst betreiben

Den wichtigsten Zertifikaten

- Kann man ihnen vertrauen? → ob das Zertifikat abgelaufen ist, Datum.
- Zertifikate laufen ab
- Zertifikate hat über eine bestimmte Zeit eine Gültigkeit
- Meistens laufen es nach 1 Jahr ab
- Müssen dem Stand der Technik entsprechen

Stand der Technik

Der Stand der Technik ist eine Zusammenstellung der zurzeit gewährleisteten technischen Möglichkeiten und basiert auf wissenschaftlichen und technischen Erkenntnissen.

INOFORMATIONSMANAGMENTSYSTEM

- man spricht von Policies → Entscheidungen treffen, wir bezeichnen es als Regelwerk
- Im Regelwerk definieren wir eine Vorgehensweise für das Zertifikat
- Zertifikate, die wir selbst erzeugen, dann muss es jemanden geben der regelmäßig überprüft, ob die Zertifikate dem Stand der Technik entsprechen
- Plan, do, check, Act: Planen, machen, kontrollieren und agieren
- Regelwerk definieren: prüfen, ob alles passt, z.B. jedes Jahr, Dokument anpassen → Prozess wird Kontinuierlicher Verbesserungsprozess (KVP) genannt
    - Regelmäßig berichten lassen wir man das verhindern kann, Versionen zum Richten stand

ISME→ verantwortlichen Personen einer organsaton ahben personen bestimmt, dass bestimmte Tätigkeiten in einem Handbuch niedergeschrieben werden und erklärt werden, warum wir es machen, wie wir es machen, Kontrollen anwenden (Plan, Do, Check, Act)

Beschreibung von System, Die Norm versteht darunter eine Systematik, also eine Beschreibung:

- Diese Beschreibung ist keine Lösung des Systems
- Management muss überlegen, welche Bedrohung es hat, anhand der risikoanalyse sich überlegen welche Maßnahmen man einsetzen möchte
- Nich wie etwas umgesetzt werden soll, sondern den Weg dahin, wie man draufkommt

Wichtiges Regelwerk:

- SOA (Statement of applicability) → Dokument herausgeben, nach welchem Gesetzt wir agieren müssen

Welche Risiken können eintreten das cia komplementiert wird, kann Integrität, Vertraulichkeit, Verfügbarkeit komplementiert werden: ja

Verfügbarkeit: Netz und Informationssysteme Gesetz: Zuerst muss das Netzwerk betrachtet werden

Das Netzwerk einer Klinik kann ausfallen, was kann man dagegen tun?

- Wir betrachten Layer 1-3
- Die einfachste Lösung sind Redundanzen bilden, dies führt zu Ausfallssicherheit
- Redundanzen bauen: vertikale und horizontal Verkabelung einbauen
  - Horizontale Verkabelung: .
  - Vertikale Verkabelung:
    - sind die Drähte, die von Stock zu Stock, über eine Telekommunikation zu einem Geräteraum erweitern.
  - Bei Verkabelung mit VLAN
    - VLAN: ein kleines Segment innerhalb eines größeren kabelgebundenen Netzwerks. VLANs ermöglichen eine ortsunabhängige Konnektivität innerhalb desselben LANs.