Protokoll 31.01.2023

Kurzzusammenfassung

In der Stunde vom 31.01.2023 haben wir uns mit dem Thema der Erarbeitung einer Aufgabenstellung beschäftigt.

Inhaltsverzeichnis

Inhalt

NIS-Gesetz: Separation (Unterteilung)

- Zielsysteme in mehrere Netze Aufteilen und nicht in einer flachen Architektur (alles in einem Netz)
- Konzept überlegen wie können die verschiedensten Systeme so unterteilt werden, dass wir unterschiedliche Zonen haben. (verschiedene Modelle)

Zonenmodell (Sicherheitsklassen/Zonen absichern)

Vertikale und horizontale Betrachtung (Sicherheit geht in die Tiefe). Beim Zonenmodell habe ich unterschiedliche Sicherheitsklassen, wo die äußerste Schicht immer weiter in mein COR-System kommt. Jede Zone hat einen Übergang. Der Übergang von außen nach innen, wird nach bestimmten Kriterien abgesichert.

- 1.Kritierie (Variante): Verwendung einer FIREWALL (bestimmte Kommunikationen zulassen/nicht zulassen)
- 2.Kritierie (Variante): Zonen untereinander Absichern [unterschiedliche Zielmaschinen (Patienten, Buchhaltung…..)]

DMZ → demilitarisierte Zone

Firewall

Unterschiedliche Zonen setzen Richtlinien um (= Schutz in die Tiefe!). Einer der ersten Schutzmechanismen ist, dass ich gewisse Kommunikationen zulasse, und gewisse Kommunikationen nicht zulasse.

- „alles ist erlaubt was nicht verboten ist“ → Probleme aufgeworfen, ich muss wissen was verboten ist.

DESWEGEN: „alles verboten was nicht erlaubt ist“ → wir wissen was erlaubt ist.

Jump Host (außerhalb Berechtigung)

Richtlinien durchqueren (Zugriff und Berechtigung = ROLLEN)

Jump Host geht auf Zielmaschinen (jemand von außen bekommt eine Berechtigung und von diesem Jump Host aus geht er anschließend in die Zielmaschine). Der Jump Host kennt die Passwörter der Zielmaschine, der Admin jedoch NICHT.

Auch bei unseren Clients möglich:

- Keine Applikationen auf Rechner
- Keine Daten auf Rechner
  - ➔ Nur per Stream möglich [Terminalserver = (hat alle Programme, die der Mitarbeiter benötigt, alle Daten von Mitarbeiter werden gesichert)]

SSO → „Single Sign On“ (einmaliges Anmelden erforderlich)

Terminal Server

Informationen werden am Bildschirm angezeigt, alles wird ferngesteuert.

➔ Terminal Server Vorteil:

Vielzahl an Mitarbeitern, jedoch brauche ich nicht alle Rechner servicieren.

1.) **Thin Client**: Ist ein Rechner der aus Prozessor, Memorie, Speicher, Bildschirm und einer Maus besteht. Der Thin Client bekommt die Daten vom Terminal Server.

2.) **Clients**: Lokale Daten Gefahr
- Device Management verwalten
- Verschlüsselung

→ *bei Verweigerung*: **Verantwortung übergeben!** (Strafbar bei Verlust), End Point Protecting (von Ferne lösen) oder wenn das nicht gemacht werden kann (med. Gerät)

Separation of Duty: Rollen Modell welches auf Aufgaben spezifiziert ist. Minimale Rechte (nur wenn notwendig)

3.) **Virtuelle Maschine**: 1-1 Beziehung zum Nutzer
Terminal Server: 1-n Beziehung zum Nutzer

- PAAS → Plattform as a Service (Gesamtheit des Systems als Service)
- NAMP/LAMP → Windows Apache MySQL PHP, Linux Apache MySQL PHP
- Provisioning System → einfache Installation von VM oder System.

In Amerika? → Nein, da die Daten den europäischen Boden nicht verlassen dürfen