Studiengang Informatik
apsi 2020

Fachhochschule Nordwestschweiz
A. Wagner, M. Schläpfer, R. Wagner

Übungsblatt 10 — 16. November 2020

Aufgabe 10-1: Zero Trust

Das Zero Trust Sicherheitsmodell geht weg von einem perimeterfokussierten Sicherheitsansatz.

(a) Wieso ist der perimeterfokussierte Sicherheitsansatz nicht mehr zeitgemäss?

(b) Was hat Zero Trust mit dem Corona-Virus zu tun?

(c) Ein Freund erzählt Ihnen, dass Zero Trust auf Netzwerkebene gelöst werden muss. Was antworten Sie ihm?

Aufgabe 10-2: Secrets Management

Secrets Management erlaubt den sicheren, automatisierten Umgang mit Secrets wie Tokens, Passwörter, Zertifikate, Privat Keys und anderen sensiblen Daten.

(a) Wo trifft man auf Secrets Management im SDL (Software Development Lifecycle)? Nennen Sie Beispiele.

(b) Wieso ist Secrets Management im Zero Trust Sicherheitsmodell ein wichtiger Faktor?

(c) Was machen dynamische Secrets aus und was sind die Vorteile / Nachteile?

Folgendes White Paper könnte für Sie hilfreich sein:

`https://www.hashicorp.com/resources/unlocking-the-cloud-operating-model-security`

Aufgabe 10-3: Cloud Security

Cloud Security lässt sich aufteilen in Security in the Cloud und Security of the Cloud.

(a) Welche zwei grundsätzlichen Parteien gibt es in dieser Aufteilung und was sind deren Verantwortlichkeiten?

(b) Sind die Verantwortlichkeiten anders bei SaaS, PaaS und IaaS? Wenn ja, in wie fern?

(c) Wieso stimmt diese Behauptung (nicht): 'Ich nutzte SaaS - darum brauche ich keine Konzepte mehr für Access Management, Datenintegration oder Backupz.B. für Backup'?

Folgender Blog könnte für Sie hilfreich sein:

`https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/`