Studiengang Informatik
apsi 2021

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

Lösungsblatt 11 — 06. Dezember 2021

Aufgabe 11-1: Zero Trust

Das Zero Trust Sicherheitsmodell geht weg von einem perimeterfokussierten Sicherheitsansatz.

(a) Isolierte, auf einen Perimeter fokussierte Dienste und Applikationen nehmen ab. Hybride Umgebungen mit On-Premises, Cloud Provider 1 und Cloud Provider 2 nehmen weiter zu. Workloads werden dynamisch verschoben und Mitarbeitende greifen von unterschiedlichsten Standorten auf ihre Businessprozesse zu.

(b) Unternehmen welche vor der Corona Pandemie bereits einen Zero Trust Ansatz gefahren hatte, konnten einfacher auf Homeoffice umschalten. Die anderen mussten z.B. in aller Eile ihre VPN-Gateways aufrüsten und VPN-Clients ausrollen.

(c) Zero Trust ist ein Sicherheitsmodell, bei welcher die Umsetzung nicht auf einen spezifischen OSI-Layer gebunden ist. Am effektivsten sind aber Ansätze, welche über alle Layer hinweg ihre Wirkung erzielen.

Aufgabe 11-2: Secrets Management

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

(a) Secrets Management ist im ganzen SDL relevant. Von der Entwicklung (Testzugänge Applikationen, DEV-Umgebung), über das Deployment (Secrets für die Deployment-Pipeline) bis in den Betrieb (Wartungszugänge, Logging).

(b) Bei Zero Trust wird jeder Zugriff auf eine Applikationen, einen Dienst explizit überprüft. Dynamische Secrets ermöglichen eine optimale Nachvollziehbarkeit.

(c) Dynamische Secrets (pro Zugriff, pro Identität, pro Applikation/Dienst) werden automatisch erst dann generiert, wenn diese gebraucht werden. Dadurch sinkt das Risiko, dass das Secret missbraucht wird. Dynamische Secrets können zudem unmittelbar nach der Verwendung widerrufen werden. Falls ein solches dynamisches

Secret geleakt wird, kann genau festgestellt werden, für was, wann und für wen dieses ausgestellt wurde.

Folgendes White Paper könnte für Sie hilfreich sein:

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

Aufgabe 11-3: Cloud Security

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

(a) Im Prinzip ist der Cloud-Anbieter für die Sicherheit der Cloud-Infrastruktur (DC, Server, Netzwerk, Virtualisierung, Basis-Services, ...) verantwortlich - resp. dass sie bezüglich C-I-A so funktionieren wie beschrieben, während der Cloud-Konsument für die Sicherheit innerhalb der Cloud verantwortlich ist (der Rest ;-)).

(b) Ja, bei PaaS und SaaS sind die angebotenen Services höherwertig und der Cloud-Anbieter ist damit für mehr verantwortlich (auch bezüglich Sicherheit). Bsp.: PaaS Datenbank-Service - Der Cloud-Anbieter ist dafür verantwortlich, dass nur der vom Kunden konfigurierte User tatsächlich Zugang hat (d.h. ein Attacker Access Control nicht umgehen kann).

(c) Alle (Security) Themen müssen weiterhin bearbeitet werden. Ansonsten kann der Kunde seriös analysieren, welchen Teil der Cloud-Provider übernimmt und welchen Teil ihm selber übrig bleibt.

Folgender Blog könnte für Sie hilfreich sein:

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