TECH STARTER

1.7.3. VPC - Ausgangssituation

Beschreibung: Cloud-Infrastruktur für ein Startup

Szenario: Ein aufstrebendes Startup hat eine App entwickelt, die eine Vielzahl von Nutzern anziehen soll. Die App muss sicher und skalierbar sein, da täglich sensible Benutzerdaten verarbeitet werden. Das Startup hat sich für AWS als Cloud-Anbieter entschieden, um die Infrastruktur aufzubauen, möchte jedoch Kosten gering halten, ohne auf Sicherheits- und Netzwerkstandards zu verzichten.

Was brauchen wir also?

1. Einrichten eines VPCs für die App:
    - Das Team wird eine VPC in der Region ihrer Wahl erstellen, um die App-Server und Datenbanken in einer isolierten Umgebung zu betreiben.
    - Die VPC sollte mindestens zwei Subnetze haben – ein öffentliches und ein privates Subnetz. Im öffentlichen Subnetz soll ein Webserver platziert werden, der Benutzeranfragen entgegennimmt, während im privaten Subnetz eine Datenbank läuft, die sensible Daten speichert.
2. Subnetze und Routing:
    - Im öffentlichen Subnetz wird ein EC2-Instance (Webserver) gestartet. Diese Instanz soll nur über das Internet zugänglich sein, um Benutzeranfragen entgegenzunehmen.
    - Die Datenbank im privaten Subnetz darf nur vom Webserver aus zugänglich sein und sollte keinerlei direkten Zugang vom Internet haben.
    - Ein Internet Gateway soll an das öffentliche Subnetz angeschlossen werden, während das private Subnetz über ein NAT Gateway auf das Internet zugreifen kann, um Updates und Patches zu erhalten, ohne direkt zugänglich zu sein.
3. Sicherheitsgruppen und NACLs:
    - Erstelle Sicherheitsgruppen, um den Zugriff auf die EC2-Instanzen zu steuern:
    - Die Sicherheitsgruppe des Webservers soll nur HTTP- und HTTPS-Zugriff von überall und SSH-Zugriff nur von spezifischen IP-Adressen (z. B. Büroadressen) zulassen.
    - Die Datenbank-Sicherheitsgruppe erlaubt ausschließlich Verbindungen vom Webserver.
    - Implementiere Network ACLs, um zusätzlichen Schutz auf Subnetzebene zu gewährleisten und potenzielle unberechtigte Zugriffe abzuwehren.
4. Überwachung und Logging:
    - Aktiviere Flow Logs für die VPC, um den Netzwerkverkehr aufzuzeichnen und potenzielle Sicherheitsrisiken zu überwachen.
    - Nutze AWS CloudTrail, um API-Aktivitäten in der VPC zu verfolgen und sicherzustellen, dass keine unerlaubten Änderungen vorgenommen werden.