***Group Project***

Group 1

Astha (8912446)

Anmol Singh (8975825)

Panth Patel (8975227)

INFO2350 – Advanced Cloud Infrastructure Administration

Nikola Cedic

(Document Contains Security Consideration (Task 4) and brief report on security decisions and trade-off)

**Task 4: Security Considerations**

**Brief Report on Security Decisions and Trade-offs**

* The Following important security configuration and considerations were made when creating a scalable and secure AWS infrastructure:

**Problems and Solutions in Security**

1. Making the database server private

**Challenge:** To prevent exploitation or data breaches, the database must be made private.

**Solutions:**

* The database (DBServer EC2) was positioned in a private subnet without a public IP address as a solution. All incoming traffic from the public internet is blocked, and the VPC can only communicate with its internal resources.

1. Safe Interaction Between Database and Web Layers.

**Challenge:** Only allow secure communication between database and web servers.

**Solutions:**

* The DBServer security group was configured to only permit traffic from the WebServer security group for MySQL port (336), not from any public IP address.

1. Enabling Private Subnet Internet Access Without Exposure.

**Challenge:** Let the private DBServer download dependencies or updates without making it accessible to the public online.

**Solution:** To allow the private subnet to route outgoing internet traffic while blocking incoming traffic, a NAT gateway was set up in the public subnet.

**Security Decisions Summary:**

* Region\Security Mechanism
* Only WebServer EC2 allows public access.

**Database Protection**: Private subnet, no public IP address, access control, traffic managed by security groups internet for Private Subnet NAT Gateway for outgoing internet access only.

**Trade-offs Made:**

**Security vs. Complexity:**

* Although they increased architectural complexity, the use of NAT Gateway, public and private subnets, and multiple security groups greatly enhanced network separation and security.

**Cost vs. Protection:**

* Adding a NAT Gateway costs money on AWS, but it is necessary to protect the DBServer while permitting outgoing internet access.

**Control vs. Accessibility:**

* By preventing direct SSH access to the DBServer, extra steps are created (Such as using the WebServer as a jump host), which hinders debugging but also grants least privilege.

The Safety Structure aligns with AWS best practices and successfully lowers the attack surface without compromising backend database and web application functionality.