Security

Online security has become a very diverse topic. It can split into multiple angles such as keeping away intruders, making sure data is not compromised, and even legislation. We must be able to protect our physical infrastructure, data, and users. Security is more important than ever, and we wanted our architecture to reflect that.

Several security features have been discussed already in this document, such as DDoS protection and private subnets. The following features are implemented with only security in mind.

We use features that AWS offers to make sure our servers remain untampered with. Our network implements ACLs to restrict traffic into a specific type. In our case this would be to only allow TCP traffic into our subnets. ACLs help us avoid giving access to malicious entities and if they gain access, ACLs limit what they can accomplish while inside our network.

Another method of limiting access to our VPC is the use of security groups. Security groups allow a more granular control of traffic to specific instances within our network. They can be used to create rules that allow for example a specific IP address to connect via PuTTy to do maintenance on EC2 instances.

As we are an organization, several people will need to have access to our AWS management console. This can create vulnerabilities as each person has different skillsets and expertise. One way to avoid mistakes that can be made with good intentions in mind is to use IAM roles. IAM roles can limit access to which parts of the architecture each person can modify. Principle of least privilege is applied making sure accessors only have access to what they need. Additionally, for IAM users, we enforce multi-factor authentication. While we use IaC to manage our environment, IAM roles should still be in place. Another benefit of IAM roles is it can be used to limit AWS services access rights. This can be used to avoid any unintended interactions that an EC2 instance, for example, tries to do.

We must also be able protect users and their accounts. We use Cognito service to connect users to their accounts. Cognito is a user management – service that grants a temporary privilege for users to access our application in the AWS environment.

Cognito is the AWS way to leverage user pools and identity pools. These can help simplify the user creation process from the developer's standpoint. Cognito supports signing in using Google, Facebook and Apple accounts which makes it a viable solution. Additional security comes from the support of multi-factor authentication. This is not something we are mandating from the users, at least not at first.

Using Cognito, user information is encrypted. Encryption is a vital part of data security. In addition to Cognito, our architecture leverages encryption in two ways. First is to use HTTPS protocol when communicating with a user's browser. HTPPS encrypts data in transit, which means that even if captured mid transit, it cannot be read. Another encryption resides in our RDS. RDS database data is encrypted at rest to protect it from prying eyes. Proper encryption is required by several government agencies.

Since our application handles user data, under the EU laws, users have several rights pertaining to them. The data we handle can be very sensitive as at some point, we may need to verify a user's identity. This can arise if event organisers demand to know exactly who they are enlisting from our application. GDPR is a vast collection of rules that govern data privacy. We must be able to implement notifying users about the information we collect, right of access to your data, right of erasing the data, and many more rights.

With all these security features implemented, we will have a good starting point for the security element. We must be able to set up monitoring and logging for many parts of the application to know if a breach has occurred. If a malware manages to attach itself and monitor or steal information, we must be able to detect it and figure out how it got there. Security is an ever-changing landscape that must be maintained diligently.