CheeseHead Hosting

# Cheesehead Hosting

## Security Management Analysis

Author: Group 1 Date: 15/01/2024 Version: 1.0

# Contents

# 1. Threats

In this chapter we will list what we believe to be the biggest threats to our systems.

**Unauthorized access**

Because the majority of our system is located in the cloud, the biggest threat there will be clients, personnel or hackers getting unauthorized access to components of the network they should not have access to. In this scenario think of a client being able to gain administrator privileges for their account.

**Data Leaks**

Another threat is a data breach into one of our systems which causes access keys, passwords or sensitive data to be compromised. Malicious actors can then get access to the backend etc.

**DDoS and SQL injection**

These are both very common attacks performed by hackers trying to break a system. Ours is also not safe from it, although AWS has quite a few protection measures in place to combat this, the risk is never 0%.

**Misconfigurations**

AWS components can be misconfigured. For example, security groups, ACL's or IAM roles and policies, these are all ways for a malicious actor to breach the system.

**Resource Exhaustion**

The system being overloaded with requests is also a risk that can break the system. If its due to increased demand or a malicious actor trying to crash the site.

**Third party risks**

Although highly unlikely, AWS experiencing trouble at one or more of their datacentres also poses a risk as our system relies heavily on AWS.

**Port scanning**

AWS has a few methods to combat this but there is a risk of some network components being port scanned.

**Brute force Attacks**

Some malicious actors can try to force his way into our environment or website by brute forcing.

# 2. Vulnerabilities

### Insecure API's

The first big vulnerability that our system has is the API. Our system uses an AWS API gateway, but this is not tightly secured. For example, no authorization is performed when the API is called.

### Insufficient Monitoring

The second vulnerability is monitoring, our system is pretty closely monitored, almost every component is watched by AWS CloudWatch. However, there is always a risk that there is a component of the network not that closely watched in which an attacker can get in.

### Container Security

Our system also works a lot with containers to run applications. The risk that comes with this is that these containers, depending on their configuration can be exploited. Containers that are outdated can also be a way in for malicious actors.

# 3. Repressive

Starting with this chapter we will explore the security actions we can take to combat the previously mentioned threats and vulnerabilities of our system. As for the first category, we will talk about repressive actions to take. These are actions that need to be executed when an incident occurs.

### Incident Response plan

The first and really important preparation to have for dealing with incidents is having a predefined, well planned out response plan. The implementation of such a plan minimizes the damage and allows for a faster analysis and solution to a given incident.

### Forensic Analysis

This ties into the incident response plan but is still a big part of repressive actions that need to be taken. When an incident occurs, a forensic analysis must be done to understand how the incident occurred, to what extent the malicious actor has gotten into the system, and the overall damage of the incident. Based on this we can start to act and handle the incident.

# 4. Preventive

We now move on to preventive measures that can be taken to keep the systems safe.

**Identity Access Management**

For our system this might be the most important measure that can be taken when you take the threats into account. We would need to make sure that the IAM policies are properly configured for each AWS components but also every user should have the proper rights.

**Network Security**

This might be an obvious entry, but network security is important, our environment uses security groups and a well-orchestrated network design to keep the network secure. Customer and Cheesehead hosting VPC's are separated as well as public and private subnets. The network also makes use of a NAT gateway, so the network is not exposed to the internet for the most part.

**DDoS Detection**

As a security measure implantation, we used a stream of vpc flow logs to detect our network activity with Athena. It was a bit difficult to understand the regular flow of traffic because it may vary depending on the size of the company. As a preventative measure, a lambda function checks for a very high number of packets received in a short amount of time and if there are multiple calls of the same thing. Usually, these attacks are done through the HTTP and HTTPS ports, but UDP flooding is also checked for in our preventative measure. Once it detects this unusual activity, an alarm is set off which notifies the system administrators.

# 5. Detective

This section will contain the measures that need to be taken to detect an incident or some other problem within the system as soon as possible.

**Monitoring**

This is something that already has been highlighted in the previous section but is also applicable here. Monitoring is a detective measure to ensure the components of the system are healthy, but in this context its more about when a system or component is not. Good monitoring will ensure that we detect suspicious activity as early as possible, and we can have a fast response time for dealing with these threats.

**User Behaviour Analysis**

Something that also might be a good measure regarding our system threats is UBA, this way we can monitor the AWS accounts and see if some accounts may act in an unusual way to spot potential malicious actors.

# 6. Corrective

The actions mentioned here are things that can be done when an incident has occurred. The actions will help with restoring the system to its healthy state and repair damages.

**Patch system components**

After an incident has occurred you know what went wrong within your system and one straightforward way to fix this is by patching the weak component.

**Restoring from Backup**

If a backup from the system or system component has been made, a rollback can also be done to a state where the system was not infected or compromised yet. A prerequisite for this is that timely backups are made and that these are reliable.

In the project the MySQL database is backed up because it is connected to EFS which performs backups of the data stored inside the database. As for the containers they will always be running because of the ECS service.

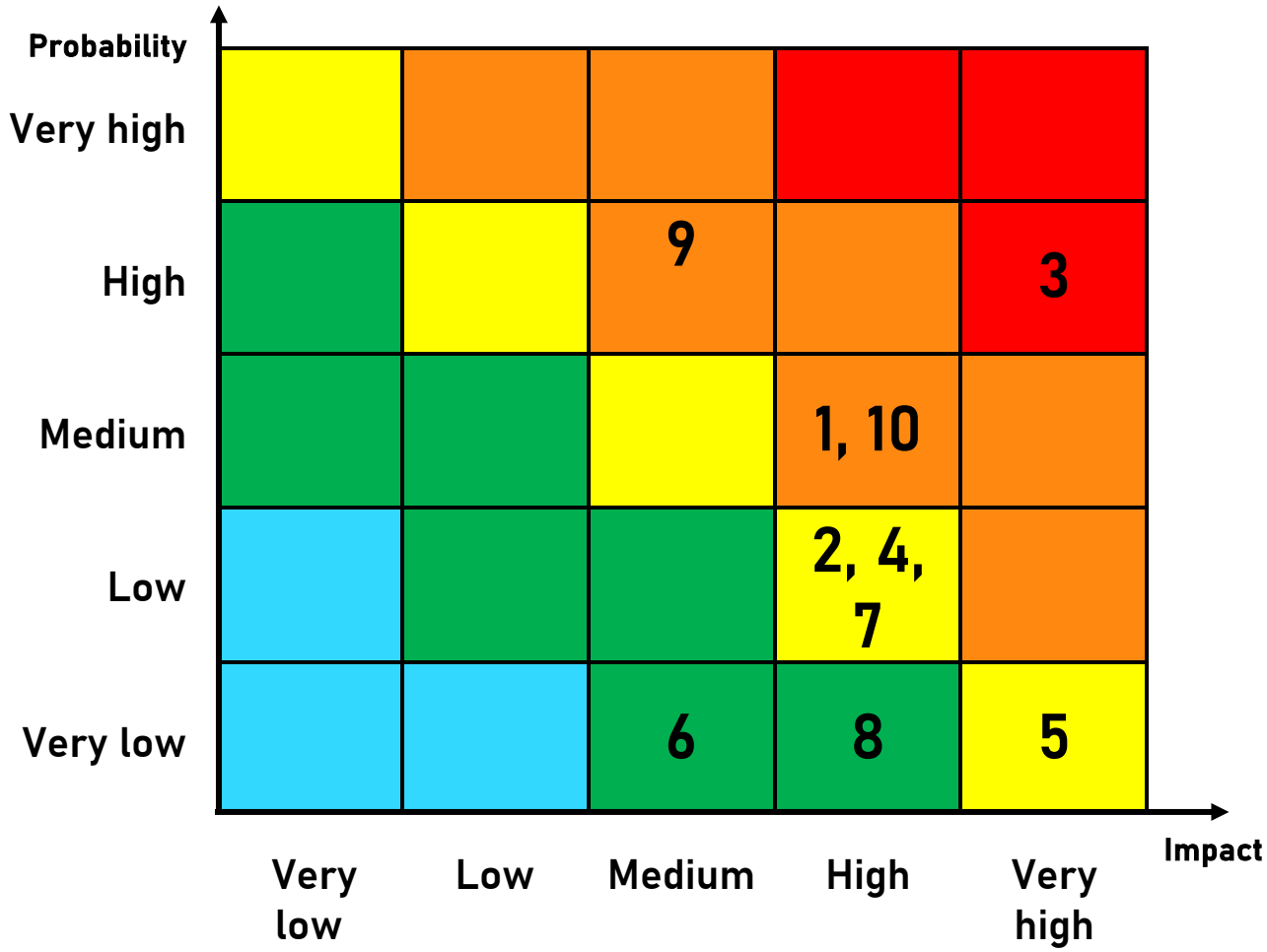
**Security Awareness Training**

On the human resources side of security, we can provide security training to employees or clients about past security incidents to minimize the human error side of your security. Given the threats of our project we can use this so AWS accounts do not get compromised by phishing attacks.

## Security table

The mentioned risks are classified by their likelihood and severity of the impact they pose on the infrastructure.

| RISK ID | RISK NAME | PROBABILITY | IMPACT |
|---|---|---|---|
| 1. | Unauthorized access | MEDIUM | HIGH |
| 2. | Data Leaks | LOW | HIGH |
| 3. | DENIAL OF SERVICE | HIGH | VERY HIGH |
| 4. | SQL INJECTION ATTACKS | LOW | HIGH |
| 5. | NATURAL DISASTERS | VERY LOW | VERY HIGH |
| 6. | Misconfiguration | LOW | MEDIUM |
| 7. | Resource exhaustion | MEDIUM | HIGH |
| 8. | Third party attacks | LOW | HIGH |
| 9. | Port scanning attacks | HIGH | MEDIUM |
| 10. | Brute force attacks | MEDIUM | HIGH |


Probability
Very high
High
Medium
Low
Very low
9
3
1, 10
2, 4, 7
6
8
5
Very low
Low
Medium
High
Very high
Impact

# Conclusion

We have addressed all threats surrounding our system, the vulnerabilities it has and the four types of controls that can/need to be taken into account when talking about these threats and their incidents. We can see a clear overview of this in the figure below.

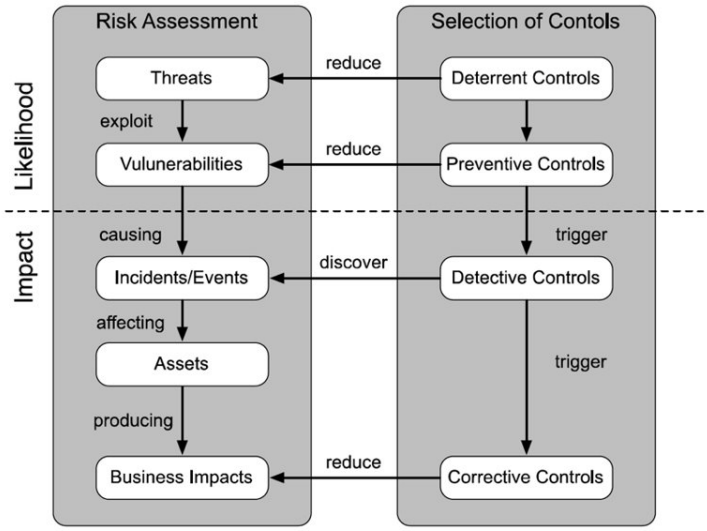



*Figure 1, Controls overview.*

| Threat/Risk | Repressive | Preventive | Detective | Corrective |
|---|---|---|---|---|
| Physical | -- | Group member devices are secured | -- | -- |
| Technical | -- | Identity acces management and network security | Monitoring | Restoring for backups |
| Organizational | -- | Security training | -- | Security training |