Threat Model:
BeavDMS

Dam Security
Sunwoo Kim, Billy Endicott, Ian J Delgado, Alanna Croysdale
26 January 2023
CS 46X

Success Measures

Identification of any possible threats to our clients software available to the public. The threat modeling process will include identifying threats at each level of the web application from users to the backend to cloud services. Proper threat modeling can help identify countermeasures for each attack surface present in a web application environment. The focus of the threat modeling process on BeavDMS will be to identify the most probable threats and attacks to this web application. Below is a list of expected threats at each level starting from the user accessing the web application. The BeavDMS application deals with any array of information that can be used in social engineering. The goal of threat modeling will be to minimize the risk of this information being exploitable.

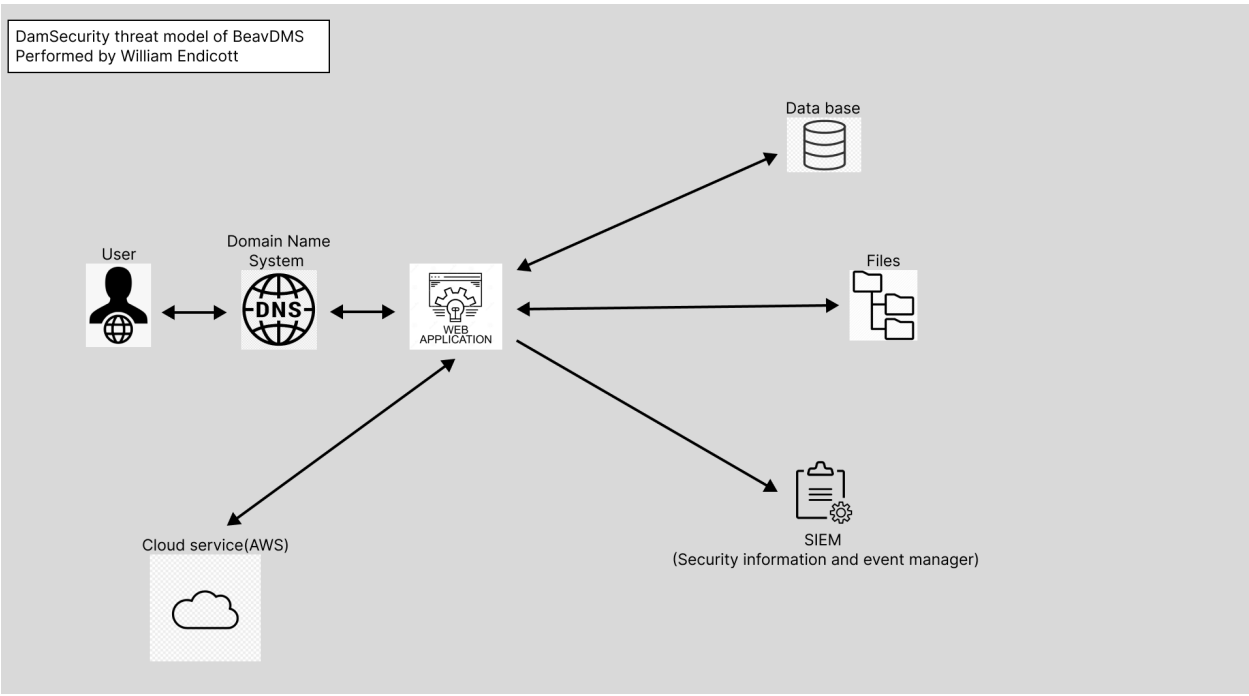

Figure 1. Basic outline of the architecture for the web application based on a very simple diagram from the BeavDMS team.

Users

Social engineering remains one of the most damaging aspects to businesses and companies. Simple social engineering can lead to malware, ransomware, leaking of credentials, and loss of digital assets. Given the importance of protecting user and employee data, it is necessary to at least minimize phishing attempts via email, phone, and even physical mail. On OWASP's top ten list of security risks, the second vulnerability listed is cryptographic failures. Cryptographic failures can lead to insecure communication. The craft team's project will be dealing with the use of users' credit cards, banking information, and shipping addresses. The use of this personal information of the users can lead to a man in the middle attack and subsequently a social engineering attack. Assets at risk in a social engineering attack on the BeavDMS include customer and employee data and availability of service.

DNS

Domain Name System is an attack surface that adversaries use to redirect traffic to malicious websites that can be used to attack users in various other ways. DNS can also be attacked in the form of a DoS (denial of service) attack which will cause a congestion of traffic from malicious bots; consequently, the app will be down, as it will be unable to respond to legitimate requests from the users. The main asset at risk for BeavDMS is availability of service.

Web Application

The third listed vulnerability on OWASP's top ten is injections. SQL injection (SQLi) and cross-site scripting (XXS) are the most dangerous and common weaknesses in online

applications. DoS attacks and attacks involving authentication methods are also common threats. If a website has weak authentication recommendations for its users, that can lead to a higher than normal amount of accounts being compromised.

Identification and authentication failures are listed as seventh on the OWASP's top ten. Insecure communication and platform misconfiguration will also lead to various other attacks. Security misconfiguration is the fifth vulnerability listed on the OWASP's top ten. Having all the security in the world will be useless if the application is misconfigured and vulnerable ports remain open. BeavDMS assets at risk include user and employee data, user and employee authentication credentials, and sensitive material that may be stored.

Files/Database

Files will have similar threats that are included in the database section. Improper encryption of data while at rest and in transit is the greatest concern for this section. A great majority of the threats from the web application section also apply here, including SQLi and improper platform configuration. The assets at risk are files storing employee credentials, admin credentials and customer data.

Logs

Logs are an important part of running a service online. Maintaining proper security logs and event logs will help later identify if someone did something malicious on the website. It will be important to log and maintain a running file of documents that are updated and by who, as well as any information that can be obtained from the interaction. If someone uploads a malicious file and an offensive file, we would want the ability to find that person and hold them responsible. This is where one of the key pillars of information security comes into play.

Non-repudiation will allow the administrators of the website to log the sender's information that is provided from the network traffic as well as the credentials associated with the traffic.

Cloud services(AWS)

Most of the AWS-related threats will be due to customers of AWS misconfiguring the security services. Misconfiguring of access control S3 buckets and privilege escalation of credentials are some of the biggest threats other than the misconfiguration. Assets at risk include administrator credentials and employee or customer login credentials.