CMPE 220 – System Software

Assignment 8 – Security

First Name: **Harish**

Last Name: **Marepalli**

SJSU ID: **016707314**

Professor: **Robert Nicholson**

Securing a software service:

The short description of all the things I will be doing to secure my service is as below:

1. *Strong Passwords and Two-Factor Authentication*: All user accounts will be required to have strong passwords, which will be enforced using password policies. This will help prevent brute-force attacks and other password-based attacks. Additionally, two-factor authentication (2FA) will be implemented to provide an extra layer of security. 2FA requires users to provide a second form of authentication, such as a code sent to their phone, in addition to their password.
2. *Data Encryption*: All data handled by the service will be encrypted both in transit and at rest. This means that any data sent between the user's device and the service, as well as any data stored on the server, will be encrypted to prevent interception by malicious actors. The encryption algorithm used will be strong and industry-standard to ensure maximum security.
3. *Access Control*: Access to the dedicated server will be restricted to authorized personnel only. This means that only individuals who need access to the server to perform their job duties will be granted access. Additionally, access will be controlled using role-based access control (RBAC), which means that users will only be able to access the parts of the system that they need to do their jobs. Access logs will be regularly monitored to detect any unauthorized access attempts.
4. *Regular Software Updates and Security Patches*: Regular software updates and security patches will be applied to the system to address any known vulnerabilities. This will help prevent any potential security breaches from being exploited by attackers.
5. *Penetration Testing*: Regular penetration testing will be conducted to identify any potential weaknesses in the system. This involves simulating an attack on the system to identify any vulnerabilities that could be exploited by attackers. Any vulnerabilities discovered will be promptly addressed and remediated.
6. *Employee Security Training*: All employees and contractors will undergo thorough background checks and security training to ensure that they understand the importance of data security and are equipped to handle sensitive information appropriately. This will include training on how to identify and respond to security threats, as well as best practices for data security.
7. *Use firewalls and intrusion detection systems*: Firewalls and intrusion detection systems help prevent unauthorized access to the server. Implement firewalls to restrict incoming and outgoing network traffic and intrusion detection systems to detect and respond to suspicious activity.
8. *Limit access to the server*: Limit physical access to the server by storing it in a secure location and only granting access to authorized personnel. Implement physical security measures such as security cameras and access controls to prevent unauthorized access.

9. *Implement role-based access control*: Implement RBAC to restrict access to sensitive data based on job roles. RBAC helps ensure that only authorized personnel have access to sensitive data and that they only have access to the data they need to perform their job functions.
10. *Monitor server activity*: Monitor server activity to detect suspicious activity, such as unusual login attempts, and respond appropriately. Server activity monitoring should include log analysis, real-time alerts, and incident response procedures.
11. *Train employees on security best practices*: Provide regular training to employees on security best practices to ensure that they understand how to safeguard sensitive data and avoid common security pitfalls. Security training should cover topics such as password hygiene, social engineering, and safe browsing practices.
12. *Conduct vulnerability assessments*: Conduct regular vulnerability assessments to identify weaknesses in the system and take steps to address them. Vulnerability assessments should include penetration testing, vulnerability scanning, and threat modeling.
13. *Use a reputable hosting provider*: If you are not hosting the service on your own dedicated server, use a reputable hosting provider with a strong track record of security. A reputable hosting provider will implement security best practices, provide regular software updates and security patches, and monitor the server for suspicious activity.
14. *Implement data encryption in transit*: Implement secure communication protocols such as TLS/SSL to ensure that data is encrypted in transit and cannot be intercepted by unauthorized parties. Data encryption in transit is essential to prevent man-in-the-middle attacks and other forms of network-based attacks.
15. *Implement intrusion prevention*: Implement intrusion prevention systems (IPS) to detect and prevent malicious activities before they can cause damage to the system. IPS helps detect and block suspicious network traffic, such as malware downloads and brute-force attacks.

By implementing these measures, we can ensure that our software service is safe and secure for all users.