External Testing Methods

Daniel DeGouveia

Southern New Hampshire University

CS-405bye

**Summary of Breach**

In March 2017, Experian experienced a security breach where the personal data of millions of clients was stolen. The personal data in this case comprised of people’s identities and their credit card information. This was a result of the company failing to follow security policies, keep software patched, and keep security certificates up to date. Once discovered, Experian failed to respond to the attack quickly. Further, the leadership of the organization was accused of corruption and their potential involvement in the breach. The hackers managed to get access to the company’s web portal and pull data through encrypted means without getting recognized. This breach went on for months without being detected by the security protocols installed in the company’s system.

**Encryption Strategies**

Encryption is one of the most important security features since it protects a system from malicious users accessing private data. There are multiple types of encryption that can be used to add protection to the data stored in the system. One example is symmetric encryptions, this method uses a single key for both encryption and decryption of data. This key is only made available to authorized personnel. Another method is asymmetric encryption that provides two keys, one that is shared with the public and one that belongs to the key generator. With these keys, a company can use resources such as advanced encryption standards (AES), Rivest-Shamir-Adleman (RSA), Twofish, and triple data encryption standards (TrippleDES) (Gai et al., 2016). AES could be the best solution for the company since it requires a hacker to go through multiple steps before they can access data. It also provides encryption for data that is in rest and in transit.

**AAA Framework**

The use of AAA Framework would be essential in identifying security issues around people’s capacity to access the company’s intellectual property. The 3As stand for Authenticate, Authorize, and Account. With authentication, a system identifies a person’s password and can also require biometric tests, and access cards to be provided to grant access. In the case of mobile and web applications, a 2-factor authentication process is used to verify a person’s identity. Once a user has been identified, they are then provided authority to specific features. There are options such as Mandatory Access Control (MAC), role-based access control (RBAC), and discretionary access control (DAC). In the case of Experian, MAC and RBAC best fit the security needs of the company since only specific functions of the company provide access to a user’s credit information. For instance, if a client wants to make a transaction, this function is handled by the billing department. For this reason, only personnel in this department should have access to this information. Lastly, accounting identifies any logging and usage activities in a system. This function could be handled using Security Information and Event Management (SIEM) in Experian to ensure that everyone that has access to the system was authenticated correctly. This feature could have helped identify the data breach sooner.

**Unit Testing**

The unit testing used for the company will depend on the type of application and programing language used to build the system. For instance, if the company requires to counter problems in android applications, the best option would be J-Unit testing. The advantage of unit testing is that it helps with identifying if web apps, websites, and mobile applications perform as is required by functionalities. This fact ensures that there are no faulty functionalities in a system. For instance, before a person is given access to data in a client’s billing information; they have to provide different data in fields provided in the authentication form before they proceed to gain access to other aspects of the application.

**Conclusion**

Ultimately the data breach could have been avoided if Experian was following a security policy. The details that have been laid out in this plan can help prevent attacks and protect data by using secure coding best practices. Implementing strict rules for encryption such as AES, using AAA framework, and implementing J-Unit testing will help ensure that data will be secured and there will be limited risk and vulnerabilities in the system. Overall, security should be thought of as a priority and not an afterthought.

**References**

Gai, K., Qiu, M., Zhao, H., & Xiong, J. (2016, June). Privacy-aware adaptive data encryption strategy of big data in cloud computing. In *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 273-278). IEEE. <https://ieeexplore.ieee.org/abstract/document/7545931>

Bouganim, L., & Pucheral, P. (2002, January). Chip-secured data access: Confidential data on untrusted servers. In *VLDB'02: Proceedings of the 28th International Conference on Very Large Databases* (pp. 131-142). Morgan Kaufmann. <https://www.sciencedirect.com/science/article/pii/B9781558608696500202>