Analysis of Risk: Penetration Testing Planet Home Lending

Zoë Medina

Professor Burke

CYBR-502 Cybersecurity Network Defense

Shiley-Marcos School of Engineering (SMSE), University of San Diego

Analysis of Risk: Penetration Testing Planet Home Lending

Planet Home Lending, LLC is a financial company that issues home loans to customers through means of purchase, refinance, cash-out, and remodel. Because of this, Planet Home Lending or PHL is responsible for maintaining and protecting their customer's personal and financial information in their data centers. As a United States company, it is under strict regulations and must follow a framework put into place by the Federal Financial Institutions Examination Council or FFIEC, who "aims to prescribe uniform principles of best practices for financial institutions" (Kost, 2023). It states that financial companies should perform risk assessments, create inventories of information systems and high-risk users, implement layered security and logging systems, and limit email and internet browsers. PHL also must protect its customers' data and inform its customers of any data-sharing according to the Gramm-Leach-Bliley Act or GLBA. Under the GLBA, a financial institution must disclose if they are sharing any personally identifiable information with a third party. Before sharing it, they need to provide customers with a timely "opt-out notice, a reasonable way to opt out, and a reasonable amount of time to opt out" (Vedova, 2022). Furthermore, customers must receive their full privacy notice each year until their relationship with the company is terminated.

In order to comply with all the federal regulations and protect the data, Planet Home Lending has implemented their own security measures. According to their website, "these measures include computer safeguards and secured files and buildings" (2015), but more can be implemented. In terms of physical security, the data centers that store customer financial information should be locked up with restricted access. Restricted access should be obtained through key card access and some variation of biometrics. Therefore, only those with privileged access should be given a key card to provide their identity and the biometrics will verify that

they are who they said they are. Furthermore, security guards who have received thorough background checks should be stationed around the data center and closed circuit cameras should be placed at crucial entrances. In terms of logical security, access to the data in the data centers should be restricted to those that need it to complete their job. Accounts that have access to the data should have two-factor authentication so that compromising the account is more difficult and should be logged when accessing sensitive data. Finally, all sitting and in-transit data should be encrypted so that it can not be read if compromised.

On top of securing their data, companies need to perform penetration tests on their systems to make sure their security systems work. Before hiring a third-party company to perform the penetration test, PHL would need to consider which areas of the system can be tested and which are off limits. With the recommended security measures in place, PHL would be comfortable letting a third-party test their employees through Social Engineering. This would include social engineering tactics to attempt to gain physical access to the data server room and gain logical access by compromising a privileged account. Employees can be tested to see if they fall for phishing emails or are victim to tailgating. Furthermore, penetration testers would be allowed to test out the security controls implemented such as finding exploits in the two-factor authentication, attempting to capture and decrypt in-transit encrypted data, or using port and vulnerability scans on the system to find openings. In order to keep their customer's information private, the official data servers should be off-limits to the third-party company. This means that during their penetration testing, the testers should be required to stop right before obtaining the actual information or be given fake data servers with the same security measures to test. While this could limit the thoroughness of the test, it would still reveal any vulnerabilities within the system that give access to the server while also ensuring the data remains private.

Two perspectives that need to be considered when creating security defenses are from a third-party penetration tester and from an outside hacker. As a penetration testing company, it is important to consider the scenarios that can cause issues for the company that hired them. Due to the nature of their data and the heavy federal regulations, the worst case scenario for PHL would be having their data leaked or stolen. This could be the result of a corrupt penetration tester stealing the data, a security measure being unknowingly broken during the test and not repaired, or a vulnerability found during the test being leaked to the public. Either way, the penetration testers need to take care that the security systems are only tested, not broken, during the test and that the results of the test are only seen by the company that hired them. As a hacker, they will most likely attack in a way that will be tailored to their target company. PHL is a big financial company that takes its responsibilities of protecting its customers' data very seriously. However, a big company means it also has many employees that are likely to be susceptible to social engineering. Therefore, a hacker would be inclined to exploit this weakness as it is the most likely means to compromise the system. Because of this, it is important for a company such as PHL to provide extensive training for its employees to avoid falling for social engineering scams.

While penetration testing is a crucial part of ensuring that a security system works, companies must also take note of the limitations and risk of performing such an intrusive test. Companies must determine and state strict guidelines for these tests and penetration testers are responsible for following them. These guidelines should always have the customer in mind since they are entrusting their personal information to these companies. Creating guidelines will also help keep security systems from breaking and allowing hackers to exploit them if the test needs to occur on official data servers.

References

Kost, E. (2023, March 31). Top 8 Cybersecurity Regulations for Financial Services: Upguard. Retrieved April 3, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-financial-industry

Vedova, H. (2022, September 13). How to comply with the privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act. Retrieved April 3, 2023, from https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act

What does Planet Home Lending, LLC do with your personal information? (2015, October). Retrieved April 4, 2023, from https://planethomelending.com/wp-content/uploads/2015/12/2015-2016-Consumer-Privacy-Notice.pdf