subrosa

A Case Study:

Securing PHI With Network And Application Penetration Testing

Contents

The core mission of cybersecurity

The core mission of cybersecurity in any business is to secure its digital assets and infrastructure. For the healthcare industry, protecting and securing sensitive health data is the topmost information security priority. As the impact of a malicious attack can go far beyond financial damage or loss of corporate information, the stakes are very high for healthcare industry operators.

The U.S. Department of Health and Human Services points out that as health care providers and other entities dealing with Protected Health Information(PHI) move to computerized operations, including computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems, necessary data protection measures are paramount. The major aim of the regulatory systems is to protect the security and privacy of individuals' digital information in the modern healthcare industry.

While healthcare providers rely on technology every step of the way to ensure better healthcare. This level of reliance and criticality compounds the cyber risk factor manifold. Regulations and compliance standards are highly-rigorous and complex to implement. Tenacious information security challenges arise every day. All these factors add up to making cybersecurity implementation and management a particular challenge in the healthcare industry.

The paramount need to safeguard patient health data and healthcare providers' reliance on technology are interlinked and fundamental to the healthcare industry now and always.

The challenge

Our client is a major healthcare provider located in the US that provides healthcare services to state and federally referred clients. As part of their cybersecurity plan geared towards ensuring and maintaining HIPAA compliance, they decided to conduct penetration testing to test and bolster the security of protected health information (PHI).

The Health Insurance Portability and Accountability Act (HIPAA) is a set of governing rules and regulations that set the standard for sensitive patient data protection. Any healthcare service provider or organization dealing with protected health information (PHI) is required to implement physical, technical and administrative safeguards to ensure the necessary standard data protection. To this end, our client required application, external and internal network penetration testing in order to maintain compliance with HIPAA.

An integral challenge of cybersecurity operations in the healthcare industry is the rigorous attention to detail required in ensuring adherence to regulations, ethics and confidentiality at every step.

The crux of the challenge

- An important part of their organizational infrastructure was a complex, custom-developed billing software application. It presented a unique set of challenges. Specialist knowledge was required to properly test the application including manual review of its source code, the live application environment lacked several security controls that were part of the production environment and lastly, any exposed critical vulnerabilities had to be remediated simultaneously to the testing process.

- The client required robust and thorough testing of both internal and external resources to assess all-around security. The internal employee team consisted of multitudes of internal members with varying access and privilege levels. The organizational application and network infrastructure required in-depth penetration testing at multiple points and with varying techniques and methodologies. All this had to be taken into account in order to formulate an effective testing solution.

- The developer team did not have an established procedure to quickly and effectively remediate vulnerabilities. Another critical cybersecurity challenge was that the developer team did not follow secure developmental practices in building the application. This posed a severe threat due to the heightened risk factor and the potential number of attack vectors.

Our solution

We utilized our penetration testing scoping methodology to identify the network topology, IP addresses and external and internal resources that are required to be in scope. Special attention was given towards testing the integrity of the areas of the network that store patient health information. Considering that multiple factors had to be taken into account, a two-step solution was devised. This was imperative to test the level of risk that PHI was exposed to under different scenarios.

To ensure this, we undertook the following measures:

Testing workforce awareness and security:

A crucial component of an organization's cybersecurity defenses is the level of training and preparedness its internal employees are equipped with.

To test this we conducted sophisticated social engineering tests which also leveraged insider information. These tests were intended to simulate internal communications with a high degree of accuracy. This included simulating phishing attacks and attempts to escalate privileges. Multiple rounds of social engineering tests revealed that the target firm's employees were well-trained to spot potential social engineering attacks and to deal with them appropriately.

Testing the network and application infrastructure:

The digital infrastructure of the client organization was the next resource to be put under scrutiny.

Application testing: We utilized the OWASP top 10 application security vulnerabilities as our guide in assessing the security level of the client organizations's applications. The application testing process also included complete source code review and the testing of the infrastructure upon which the application was hosted. This thorough testing process yielded exploitable vulnerabilities at multiple points.

Internal and external network testing: For the network testing, we utilized the CIS penetration testing framework and NIST 800-115 guide to information security testing and assessment. Penetration testing conducted on the external network revealed that resilient security measures were in place. Testing the internal network revealed that it had the most critical vulnerabilities among all of the target test areas. Despite the vast scope of the internal network, it lacked the required security controls, which if exploited successfully would have presented the highest risk factor.

As listed above, exhaustive two-stage testing was conducted on the client organization's internal and external resources to discover vulnerabilities. In the application and network testing process, once vulnerabilities were identified our team developed exploits and ran them against the vulnerabilities. Based on this process, the several vulnerabilities that were exposed and their respective risk levels were formulated into a detailed report to enable remediation at the earliest.

One of the key challenges with this project, as mentioned previously, was that the developer team lacked a standard procedure to remediate vulnerabilities. Our team worked closely with the developers to establish a standard remediation procedure to quickly and effectively patch up any vulnerabilities. Constant guidance was provided to the client to ensure that all the exposed vulnerabilities were remediated. Several advisories were also furnished to enable our client to put in place preventative measures so as to reduce the overall cyber risk level.

Key insights

Our solution enabled the client organization to:

- Have critical insight regarding the information security levels across every aspect of their entire organizational chain that processes or stores PHI.
- Have a clear picture of the potential vulnerabilities that could compromise PHI across their application and network infrastructure and the risk level posed by each vulnerability.
- **Have a detailed plan of action to remediate the said vulnerabilities to prevent them from being exploited by an actual threat actor with malicious intent.**
- **Establish and maintain a standard procedure that enables the developer team to effectively and quickly remediate any vulnerabilities that may arise in the future**

The impact

Key metrics

2 **Million active records protected**

44 **Attack vectors tested**

100 **Thousand patients data protected**

Conclusion

As a result of the robust testing process undertaken, the client organization now has a clear understanding of the cyber risk and exposure level that PHI hosted on their platform was under. More importantly, they are equipped with actionable input and an established procedure to remediate those vulnerabilities and minimize the said risk.

Adhering to HIPAA compliance is critical to every firm that deals with PHI. Whether willful or not, the risks of non-compliance with HIPAA ranges from criminal charges to severe penalties to the threat of sanctions. The potential impact of cyber attacks ranges anywhere from exposure of sensitive health information to the financial brunt of dealing with a ransomware attack. Healthcare industry operators are exposed to risks from multiple fronts. These severe risks cement the need for increased vigilance and better enterprise-grade cybersecurity defenses.

Comprehensive penetration testing has furnished our client with the knowledge to mitigate the risks associated with storing and managing healthcare data. And, they are now able to focus on their life-saving mission while simultaneously ensuring that their patient health information (PHI) is secure and reinforcing overall cybersecurity.