Pentesting in the financial services industry: adapting to changing threats

BY ANNA HAMMOND · FEBRUARY 26, 2024 · LAST UPDATED ON MARCH 6, 2025

Cybercriminals frequently target the financial services sector due to the abundance of confidential client information it carries. These attacks can be highly damaging, leading to monetary losses, harm to reputation, and damage to customer confidence. It is imperative for financial organizations to prioritize cybersecurity and take proactive steps to defend against constantly evolving threats.

A crucial method for enhancing cybersecurity readiness is through the implementation of penetration testing (pentesting). This article discusses the growing issue of cybercrime in finance and the challenges of pentesting in the financial sector. We will also cover the importance of continuous security testing and how financial institutions can proactively protect themselves from evolving threats.

The rising tide of cybercrime in finance

The financial services industry's reliance on technology and the vast amount of sensitive data it handles makes it an attractive target for malicious actors. One notable cyber attack of recent was the SolarWinds supply chain attack, which was discovered in December 2020 but still makes headlines today. SolarWinds is a provider of IT management software. However, attackers breached their systems, resulting in the compromise of multiple government agencies and private companies, including financial institutions.

Furthermore, the sector as a whole is facing a significant financial burden due to cybercrime. According to recent estimates, global cybercrime costs the financial services industry billions of dollars annually. These losses stem from various factors, including stolen funds, business disruption, regulatory fines, and the cost of implementing cybersecurity measures. Cyberattacks can also lead to a loss of customer trust, which can further damage an organization's reputation and profitability.

Pentesting: A critical tool for financial institutions

Pentesting is a critical tool for financial institutions to protect themselves from cyberattacks. By simulating real-world attacks, pentesting helps financial institutions identify and fix vulnerabilities before they can be exploited by malicious actors. In addition to identifying vulnerabilities, pentesting can also help financial institutions to:

- Comply with industry regulations and standards
- Demonstrate their commitment to security and compliance
- Build a stronger security posture by identifying and addressing security gaps.

Regular pentesting is essential for financial institutions to keep pace with the evolving threat landscape and protect their sensitive data and systems.

Unique needs for financial services pentesting

The financial services industry have many unique needs when it comes to penetration testing. These include:

1. Compliance and regulatory requirements

Financial institutions are subject to a variety of compliance and regulatory requirements, including the Payment Card Industry Data Security Standard (PCI DSS), Digital Operations Resiliece Act (DORA), and TIBER-EU Framework. These regulations require financial services companies to protect customer data and financial information, and to have robust security measures in place. Pentesting can help to meet these requirements by identifying vulnerabilities that could be exploited by cybercriminals.

2. Interconnected systems and complex IT environments

The financial services industry is also characterized by its interconnected systems and complex IT environments. This can make it difficult to identify and test all of the potential entry points for cyberattacks. Pentesting can help financial institutions identify these vulnerabilities and develop strategies to mitigate them.

3. High volume and sensitivity of financial data

The high volume and sensitivity of financial data is another challenge that financial institutions face regarding pentesting. Financial data is a prime target for cybercriminals, who can use it to commit fraud, identity theft, and other crimes. Pentesting can help financial institutions protect this data by identifying vulnerabilities that could allow cybercriminals to access it.

4. 24/7 operations with the need for minimal disruption

Finally, financial institutions operate 24/7, and any disruption to their operations can have a significant impact on their customers and their bottom line. This makes it challenging to conduct pentesting without disrupting operations. However, there are several techniques that can be used to minimize disruption, such as scheduling pentesting during off-peak hours or using non-invasive testing methods.

Best practices: pentesting for financial services

Pentesting is a critical security measure for financial institutions to safeguard sensitive data and comply with industry regulations. Here are some best practices to ensure effective pentesting in the financial services sector:

1. Stay updated on the evolving threat landscape

Be vigilant in checking for potential threats, vulnerabilities, and attack vectors that are relevant to the financial industry. Stay informed about the latest cybersecurity trends by subscribing to security advisories, threat intelligence feeds, and industry forums. Keep pentesting tools and techniques up to date to effectively address new threats and maintain a proactive security approach.

2. Combine automated and manual testing

Combining automated and manual testing methods will help achieve more comprehensive coverage. Additionally, organizations can identify vulnerabilities that may be missed by relying on only one approach. Automated tools can efficiently scan large networks and systems for common vulnerabilities. Conversely, manual testing allows skilled security professionals to conduct targeted and in-depth analysis.

3. Switch to crowdsourced pentesting to tap into thousands of experts

Access a vast network of security professionals who possess significant expertise and experience in pentesting, and are further motivated by the potential of receiving bounty rewards. For example, Intigriti's Hybrid Pentest solution combines the pay-for-impact approach of bug bounty programs with the dedicated resourcing strategy found with classic penetration testing.

4. Conduct regular risk assessments

Conduct risk assessments regularly to identify potential vulnerabilities and prioritize testing efforts. Pay attention to critical assets, sensitive data, and systems that are highly vulnerable to external threats. Keep risk assessments up-to-date by considering changes in the threat landscape, regulatory requirements, and internal security policies.

5. Implement a robust incident response plan

Create a thorough incident response plan that outlines the necessary actions to be taken in the event of a security breach or vulnerability exploitation. This plan should clearly define roles and responsibilities, communication protocols, containment strategies, and remediation procedures. It is important to regularly test and update the plan to ensure its effectiveness in handling real-life security incidents.

Staying ahead with continuous security testing

Financial institutions have traditionally used periodic penetration tests to evaluate their security stance. However, this approach is no longer enough to combat the constantly changing threat landscape of today. Combining traditional pentesting with continuous testing, by running a bug bounty program, for example, is a proactive security approach.

Watch Intigriti's on-demand webinar on how to optimize security testing budget.

Bug bounty programs and penetration tests both aim to identify vulnerabilities that hackers could exploit. However, there are some key differences. Pentests focus on one moment in time, whereas bug bounty programs are continuous. After a penetration test is performed, you will receive proof of attestation and an overview of any vulnerabilities found within a specific time frame. However, it is important to note that your security posture may change as you release new features or updates. This is where bug bounty programs work well as a follow-up, further strengthening your security posture.

A combined approach to security testing is a must for financial services

Implementing a sufficient security testing strategy can be a complex and time-consuming process. However, it is an essential investment for financial institutions that want to protect their sensitive data and comply with industry regulations. By following these best practices, financial institutions can ensure that their continuous pentesting program is effective and efficient.

To learn more about bug bounty programs and pentesting for financial services, get in touch