Penetration Testing for Critical Web Application

Customer success story

CLIENT: **BRIMBANK CITY COUNCIL**

INDUSTRY: **LOCAL GOVERNMENT**

SOLUTION PROVIDER: **BORDERLESS CS**

SERVICE: **PENETRATION TESTING FOR CRITICAL WEB APPLICATION**

Overview

Brimbank City Council, a local government authority based in Melbourne, Australia, oversees critical services and sensitive data that require robust security measures. To protect these assets and ensure compliance with government regulations, the council turned to **Borderless CS**, a leading Australian cybersecurity company, for **penetration testing** of one of its most critical web applications. The goal was to proactively identify and remediate potential vulnerabilities that could put their systems, sensitive data, and overall reputation at risk.

The Challenge

As a local government entity, Brimbank City Council hosts and manages multiple online services, including citizen portals, payment systems, and access to internal applications. These web applications are crucial for the council's day-to-day operations and for providing services to the community. However, as with any online platform, there is always the risk of cyberattacks targeting weaknesses in these systems.

Brimbank faced several challenges:

1. **Critical Application Exposure**: The web application was a high-value target, as it handled sensitive data and provided access to key services, making it a prime candidate for cyberattacks.
2. **Complex Threat Landscape**: The growing sophistication of cyberattacks, including SQL injection, cross-site scripting (XSS), and other vulnerabilities, made it essential to perform thorough security testing.
3. **Regulatory Compliance**: The council needed to comply with strict security and data protection regulations, ensuring that their applications met government standards and provided adequate protection for citizens' data.
4. **Proactive Risk Management**: Brimbank wanted to identify vulnerabilities before malicious actors could exploit them, ensuring that any weaknesses were addressed before they could impact service delivery.

The Solution

To address these concerns, Brimbank City Council engaged **Borderless CS** to conduct a comprehensive **penetration test** of its critical web application. The goal was to simulate real-world cyberattacks to identify any vulnerabilities that could potentially be exploited by attackers.

Key Penetration Testing Features:

1. **Simulating Advanced Attacks**: Borderless CS's team of ethical hackers performed advanced penetration testing to mimic the tactics, techniques, and procedures (TTPs) of cybercriminals. This included attempting to exploit known vulnerabilities and attempting to breach the web application from various attack vectors.

2. **Comprehensive Security Assessment**: The penetration test covered multiple aspects of the application, including authentication mechanisms, session management, user input validation, and data encryption practices. It also included network infrastructure and server configuration testing to ensure all layers of the system were secure.

3. **Vulnerability Scanning and Exploitation**: The team used automated vulnerability scanning tools, as well as manual testing, to identify weaknesses such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and insecure direct object references (IDOR).

4. **Application-Specific Security Testing**: Special attention was given to the application's business logic and custom code, as these areas often present unique vulnerabilities that are not always covered by standard security tests.

5. **Risk and Impact Analysis**: Borderless CS identified and ranked vulnerabilities based on their potential impact, providing Brimbank with a clear understanding of which issues required immediate attention.

6. **Detailed Reporting and Remediation Guidance**: Following the testing, Borderless CS provided Brimbank with a comprehensive report detailing the vulnerabilities discovered, the risk associated with each finding, and clear recommendations for remediation.

Results

The penetration testing engagement delivered numerous benefits for Brimbank City Council:

1. **Identification of Critical Vulnerabilities**: The penetration test uncovered several significant vulnerabilities, including issues with input validation and weak session management, that could have been exploited by attackers to gain unauthorized access or execute malicious code on the web application.

2. **Reduced Risk of Cyberattacks**: By identifying and remediating the vulnerabilities before they could be exploited, Brimbank significantly reduced the risk of a successful cyberattack, including potential data breaches or service disruptions.

3. **Improved Security Posture**: The penetration test not only identified specific weaknesses but also helped Brimbank strengthen its overall web application security practices. By implementing Borderless CS's recommendations, the council was able to implement stronger encryption, improve input validation, and harden its authentication protocols.
4. **Regulatory Compliance**: With the penetration test findings, Brimbank was able to demonstrate to regulatory bodies that they were proactively managing risks and complying with local government cybersecurity and data protection standards.
5. **Enhanced Trust**: By proactively testing and securing its web application, Brimbank was able to maintain and even strengthen public trust. Citizens and stakeholders could feel confident that their data was protected when using the council's online services.
6. **Ongoing Security Improvements**: Borderless CS provided Brimbank with a roadmap for ongoing security improvements, including best practices for future development, ongoing security testing, and the implementation of regular vulnerability scans.

Conclusion

The **penetration testing** conducted by **Borderless CS** for Brimbank City Council was a success, providing critical insights into vulnerabilities within one of the council's most important web applications. The thorough testing, performed by a team of cybersecurity experts, helped identify weaknesses and provided Brimbank with guidance to address these issues proactively.

As a result, Brimbank was able to mitigate the risk of potential cyberattacks, ensure compliance with government regulations, and provide enhanced security for its citizens. This success story underscores the importance of proactive cybersecurity measures, such as penetration testing, to protect critical systems and ensure the continued safety of sensitive data in the public sector.

Borderless CS's expertise in penetration testing and its commitment to identifying and remediating vulnerabilities helped Brimbank City Council strengthen its cybersecurity framework, providing greater resilience in the face of evolving cyber threats.