Case Study – Local Council Sector

April 2024

WhiteRook Cyber

WRC Case study brief: Local Council Sector

Topic: Prioritising data security through regular penetration testing in local government.

Case study
A medium-sized local council implemented a comprehensive penetration testing program following a phishing attack that put citizen records at risk.

Challenge
Local governments hold sensitive citizen data, which makes them prime targets for cyberattacks. Data breaches can lead to the exposure of personal information, disruption of essential services, and erosion of public trust.

Solution
Penetration testing (pen testing) simulates real-world cyberattacks to detect and address vulnerabilities in IT systems before they are exploited. This proactive approach strengthens cyber security posture and minimizes the likelihood of costly data breaches.

Key findings

- More than fifteen (15) critical vulnerabilities were identified in the council's IT systems, including web applications, databases, and network infrastructure.
- The potential impact of these vulnerabilities included exposure of Social Security numbers, financial information, and medical records.
- The cost of fixing these issues proved to be substantially lower than the potential damages and reputational losses that could have resulted from a real-world attack.
- The benefits included enhanced data security, increased trust from citizens, and more effective cyber risk management.

Implementing cyber security vigilance and resilience

- Implement a regular pen testing program to evaluate IT systems for vulnerabilities every 6-12 months.
- Partner with experienced pen testing professionals who are well-versed in government infrastructure.
- Invest in ongoing cyber security training: to ensure employees are aware of cyber threats and understand the best practices for prevention.
- Make data security a priority to protect citizen information and maintain public trust.

Data Points

- A 399% increase in cyberattacks targeting local governments was reported in 2022 (Source: Verizon Data Breach Investigations Report).
- The average cost of a data breach for local governments is estimated at $4.24 million (Source: Ponemon Institute).
- It's possible to remediate 93% of issues found during pen testing within 90 days (Source: SANS Institute).

Conclusion

By actively identifying and addressing vulnerabilities through pen testing, local governments can establish solid cyber security defences, protect sensitive data, and retain the trust of the public in an increasingly digital world.

E: contact@whiterookcyber.com.au

P: 1300 794 777

W: whiterookcyber.com.au