Case Study – Education Sector

April 2024

WhiteRook Cyber

WRC Case study brief: Education Sector

Topic: Building cyber resilience enhances trust among parents, students and staff at a private Queensland school.

Case study

A prominent Queensland Private School, renowned for its exceptional education and cutting-edge technology, prided itself on being ahead of the curve. After a data breach at a similar prestigious school resulted in exposed student records and public concern, the school's leadership recognised the urgent need for pre-emptive measures. The breach was traced back to phishing scams targeting staff, insufficient access controls, and outdated software, allowing hackers to navigate the network and access sensitive data.

Determined to avoid such a fate, the school leadership and IT team took decisive action. They partnered with White Rook Cyber, experts in cyber security services in the education sector.

Challenge

Private schools are custodians of a wealth of sensitive information, including personal details of parents, students and staff, as well as financial records, academic transcripts, and admissions data. A breach in this data can lead to severe consequences, such as financial losses, reputational harm, legal action, and emotional distress for the families involved.

Solution

Penetration testing (pentesting) simulates cyberattacks to pinpoint weaknesses in a school's IT infrastructure and security measures, enabling timely rectifications. Security reviews, particularly of Active Directory – a known vulnerability post-perimeter breach – ensures that school technology and applications are secure and correctly configured.

White Rook's ethical hackers conducted a comprehensive assessment, utilising:

- Network pentesting: Testing network components like firewalls, routers, and servers, to identify potential vulnerabilities.
- Web application pentesting: Examining ACME's online systems for weaknesses.
- Social engineering: Assessing staff response to phishing attacks through personalised emails and phone calls.

The results were eye-opening. White Rook Cyber uncovered several vulnerabilities, including:

- Weak password policies: Many staff used simple or easy-to-guess passwords, providing easy access for hackers.
- Unpatched software: Outdated software versions contained known security flaws, offering a backdoor for malicious actors.
- Limited access controls: Lax permissions on sensitive data exposed it to unauthorised users within the school network.
- Susceptible staff: Some staff members fell victim to phishing simulations, highlighting the need for cyber security awareness training.
- Misconfigured Active Directory: The Active Directory environment was misconfigured, allowing for easy lateral movement and privilege escalation within the environment.

The school's response was swift. Working closely with White Rook Cyber, they:

- implemented stricter password policies and enforced mandatory complexity requirements
- patched all software and systems to the latest versions, eliminating known vulnerabilities
- introduced stricter access controls, restricting access to sensitive data based on roles and responsibilities
- undertook technical security services to reconfigure Active Directory securely
- provided comprehensive cyber security awareness training for all staff, faculty, and students

Outcomes

The outcome was transformative. By tackling the vulnerabilities revealed through pentesting and prioritising a comprehensive body of remediation work, this Queensland-based private school significantly strengthened its cyber defences. They gained a new level of confidence in the security of their critical data and built stronger trust with parents who deeply value the privacy of their children.

Additionally, the school achieved the following:

- avoided potentially crippling costs associated with data breaches
- reduced their cyber insurance premiums reflecting a stronger security posture
- established themselves as a leader in student data protection

Conclusion

This experience underlines the value of regular penetration testing and incorporating technical security into IT infrastructure and applications. Realistic attack simulations can strengthen the digital environment, ensuring a secure educational setting. In a world increasingly reliant on technology, cyber security must be a top priority, and pentesting is the key to achieving a defensible and trustworthy digital ecosystem.

Contact Integral/White Rook Cyber today and take control of your school's cyber security.

E: contact@whiterookcyber.com.au

P: 1300 794 777

W: whiterookcyber.com.au