At a glance:

Client

After the company was sold a complete security review was undertaken to meet PCI-DSS compliance and conform with the group security policy.

Engagement

OSI Security was contracted to perform an internal and external Penetration Test and reveal any security vulnerabilities that could expose the company to Information Security threats.

Outcome

Significant vulnerabilities were revealed that had the potential to seriously affect the company's ability to conduct on-line commerce. A detailed report assigned a risk factor to each threat and a structured remediation program was implemented based upon the actual and perceived threat rating.

"The OSI Team helped us achieve our corporate governance and security benchmarks . Our team gained knowledge that is proving invaluable in maintaining our security posture and threat readiness"

Group Chief Information Officer
Plastic Packaging Manufacturer
Sydney AUSTRALIA

OSI SECURITY
Securing your information assets, at every layer

www.osisecurity.com.au

OSI Security Case Study - Penetration Test

Compliance with global corporate standard and PCI-DSS reveals Information Security risks

Executive Summary

At the completion of a takeover a large plastics manufacturer requested their newly acquired business' IT infrastructure undergo a penetration test prior to integration of Information Systems. This was critical to ensuring compliance with current PCI-DSS standards. Upon completion of the testing, OSI Security identified critical vulnerabilities. Password policy was weak and access control to web facing resources was not strong enough to impede a malicious attack. The internal network was secure and only minor flaws were discovered. A seldom used legacy connection lacked any access safeguards, thus permitting attackers access to administrative resources. The wireless network was well designed and extremely secure, but it was discovered that intermittent unauthorised access to the company network was available via a "rogue" access point used by a team leader during training and team meetings. OSI Security made recommendations and assigned a risk rating to the weaknesses identified during the testing procedure. Remediation recommendations were provided in a comprehensive and detailed management report .

Business Driver

The core network had been upgraded to comply with the acquiring company's corporate standards. A migration to a single system was planned, but was not viable until some systems in production were replaced. A Payment Card Industry Data Security Standard or PCI-DSS is an industry benchmark designed to secure and protect bank and credit card information from inappropriate use. OSI Security was commissioned to perform an Internal and External penetration test to ensure security controls were granting access to company resources based on role employees role and responsibility.

PCI-DSS Risk Mitigation Program and Penetration Testing

Payment Card fraud is a security risk that the PCI-DSS standard is designed to eliminate. By restricting access and ensuring controls are effective, client privacy and financial security are protected. QSA's or Qualified Security Assessors are the first line of defence in ensuring the controls mandated by the PCI standards are compliant and standards are being maintained. By conducting penetration tests annually, organisations can ensure that security is protecting card holder data at all points within the infrastructure and meeting the guidelines recommended by the PCI governing body.

Client Overview:

Our client is a successful plastics manufacturer who was recently purchased by a global organisation. The business has maintained its competitive advantage by investing heavily in automated manufacturing and streamlined their supply-chain to improve efficiency. This has provided a competitive edge that sees over half of their turnover provided from exports.

Plastic Packaging Manufacturer

Annual Turnover (Australian $)

[A$40M]

Employees

[80]

Manufacturing Locations

[2]

Sales & Administration Offices

[9]

"PCI-DSS compliance is not a mandatory requirement for the business we transact, but we are reviewing how this can add value to our competitive value proposition. A number of our clients appreciate our proactive security stance and we hope this will pay dividends in the near future"

Group Chief Information Officer

OSI SECURITY

Securing your information assets, at every layer

Tel 1300 953 324
Fax 1300 956 840
Mob 0404 139 246
info@osisecurity.com.au
www.osisecurity.com.au

Internal Penetration Test

It was decided to begin the Penetration Test (pentest) procedures with an internal review. Not all employees were happy with the recent sale of the company and job losses were flagged by the new management team. Ensuring all critical data was protected and visible only to those whose role and responsibility required access was an important goal. Although sabotage was unlikely, disgruntled employees could act with malice and intellectual property could be appropriated without authority. Using a methodical discipline, all systems and divisions were tested using automated and manual testing procedures. The testing process sought to uncover oversights, errors and omissions in control measures and ensure data was accessible only by those whose role required it. The findings were consistent with first time testing. Passwords were weak and legacy systems were mostly unpatched with some users allocated administrative access that was outside their responsibilities. Of greater concern were numerous weak controls on Finance Department systems that permitted mid-level management access to online banking systems and payroll. This posed a significant risk to the organisation through potential fraud and misappropriation of company funds.

External Penetration Test

The goals for this testing were to ensure that access to specific systems and resources was limited to those with appropriate credentials and authority. The organisation had three tiers of exposure to public facing networks. Partners were granted access to inventory and pricing information for general enquiries. Accredited partners were extended greater access to order products and access account information. A public website offered webmail access to employees through a rudimentary interface. Links to a leading social media website were prominently placed on the site's landing page allowing direct links to "becoming a fan" of the company. Critical weaknesses were uncovered that permitted partners to view competitors account status and trading terms. Insecure and unpatched versions of leading web hosting application were in current production. This vulnerability had the potential to permit defacement of the website and bypass security controls altogether.

Solution Internal

OSI Security recommended deploying internal firewalls to separate Finance and Human Resource department systems. Password policy was changed with password complexity increased and the frequency of change reduced from monthly to quarterly. To safeguard confidential data and limit access to Salesforce.com client information, a two factor authentication solution was implemented. OSI Security suggested a review to refresh and simplify the company security policy. A user education program was also instigated to improve security awareness. Although out-of-scope, the market leading IP phone system was found to be using software two generations out of date.

Solution External

The public facing website was rebuilt with the latest version of the Operating System and denial of service mitigation measures put in place. A review of access logs was performed and inactive users were removed from access lists. Staff members had traditionally been granted access based on policy not their role or need. This was changed and strict conditions for remote access were enforced. A two-factor authentication solution was selected that used one-time-passwords delivered via SMS . This permitted business partners to securely access information. Employees and contractors were supplied software and hardware tokens to validate their credentials.

Conclusion

The company's IT team and OSI Security collaborated to reach a security posture that complied with the corporate PCI-DSS requirements. Specific areas of vulnerability were revealed, and by restricting access to specific resources, risks were reduced and security management was less of a burden for IT staff. Regular quarterly audits were scheduled as part of a managed service to ensure security expertise was available on-call as business needs dictated. The penetration test identified limitations in certain areas of the systems and infrastructure. They posed no immediate threat to the business, but were not in compliance with industry best practice. A twelve month remediation plan was initiated with budget and resources allocated. This would ensure completion of the goals based on priorities and a planned risk management strategy.

About OSI Security

The company was founded in 2010 by Information Security researcher Patrick Webster. Well known in the global Information Security community, Patrick has contributed more than 80 modules to the "metasploit security framework" and draws upon a broad experience of hands-on IT skills gained in IT Operation roles for leading Australian companies.