PCI Consulting Australia

Penetration Testing & Vulnerability Scanning

PENETRATION TESTING

- The most comprehensive of all testing and requires the most time.
- The most effective test to identify all vulnerabilities.
- Testing is designed to be non intrusive.
- Full reporting provided with all vulnerabilities ranked.
- One free re-test is inclusive of pricing once all issues have been addressed.

INTERNAL SCANS

- Use of tools such as Nessus.
- In most cases, can be performed remotely but onsite tests can be facilitated if preferred.
- Non intrusive and completed in much shorter timeframe than penetration testing.
- Full reporting provided similar to penetration testing.

EXTERNAL SCANS

- Utilises third party web based software with a portal for ongoing management.
- PCI Consulting Australia assists in setting up a licence and providing instruction on how to use the portal.
- An initial report will be generated after a scan marked 'Not Certified'. You must login to the portal and validate to receive the full compliant report.
- Must receive a compliant result each quarter.

ALL SCANS/TESTS

Missing a scan or test will affect your compliance! Set calendar reminders to ensure these activities are not missed.

Confusion can reign between PCI DSS Requirements 11.2 and 11.3. Here are some key facts on PCI Consulting Australia's testing services:

- Penetration testing (11.3) is the most comprehensive testing using both manual and automated techniques. It's an **annual** test of both applications and infrastructure.
- Internal scanning (11.2.1) is mainly automated testing and probes for vulnerabilities without exploiting them. It's a **quarterly** exercise.
- External scanning (11.2.2) must be completed by an Approved Scanning Vendor (ASV). We offer 12-month Qualys licences to facilitate. They must be completed **quarterly**.
- CLARIFICATION: A full penetration test can count as 1 x quarterly internal scan (so 3 more required per annum). However, an external scan MUST be completed independent of the penetration test, even if fully compliant. So 4 must be completed per annum. An ASV scan is a completely separate requirement to penetration testing.

Do I need all these tests?

When we complete an initial scope determination and gap analysis of your Cardholder Data Environment (CDE), we determine which tests are necessary. In some environments, none of these are required. If you have a website- even if payment processing is fully outsourced- we always recommend some level of regular testing to protect your site and brand which is likely to be an external scan.

Further Information

1. **Penetration testing** - In most cases needs to be performed on an annual basis and combines both **manual and automated** testing techniques in order to simulate real-life hacker scenario trying to breach your CDE. This involves testing both internal and external applications and infrastructure that exists within the defined CDE. The last part of the testing is segmentation testing which verifies that the CDE is separated from other segments of the network and it is not possible to connect from e.g. office DHCP vlan to CDE.
2. **Internal quarterly scans** - Should be performed on quarterly basis via VPN or on-site. It is mostly automated testing which is probing the CDE for the most common vulnerabilities that may have risen from small network changes or missing latest security patches and misconfigurations.
3. **External quarterly ASV scans** - This testing has to be performed using an ASV scanning tool. PCI Consulting Australia can help organise such a licence. It is targeting external interfaces/IP addresses of the CDE and is mostly automated.

If there is a significant change within your CDE, all these tests must be completed notwithstanding the regular schedule.

PCI CONSULTING AUSTRALIA SERVICES AVAILABLE

Advisory Services
Assisted SAQ Assessments
Full ROC Assessments
Acquiring Bank liaison
100% vendor independence
Penetration Testing
Vulnerability Scanning

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

1300 997 290
www.pciconsultingaustralia.com.au
info@pciconsultingaustralia.com.au