Cyberity

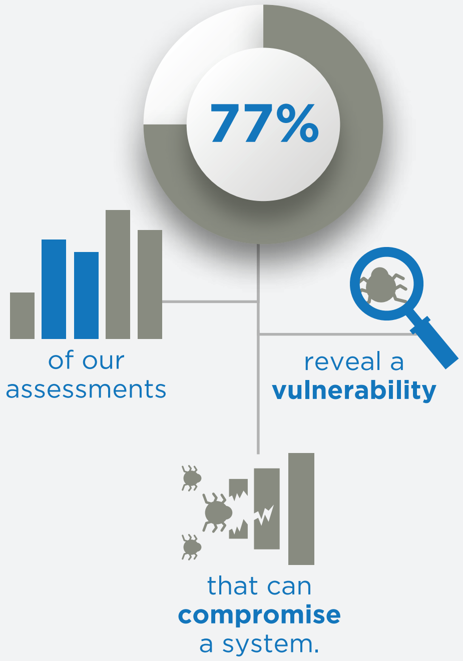
VULNERABILITY ASSESSMENT & PENETRATION TESTING

DETERMINE YOUR IT RISK EXPOSURE AND THE EFFECTIVENESS OF YOUR SECURITY CONTROLS.

Cyberity provides you with reassurance and facilitates regulatory compliance by delivering a comprehensive list of vulnerability assessment and penetration testing services.

Regular assessment of your system's vulnerabilities and testing of its security controls will reveal how vulnerable your infrastructure is from an attacker's perspective.

Depending on your organisation's requirements, these services can be customised for specific scenarios, such as API and web applications, hosted infrastructure, internal LANs, and any other specific environment in which uptime is critical or where a compromise could place sensitive data at risk.



ASSESSMENT AND TESTING OBJECTIVES

Knowing your objectives for conducting a vulnerability assessment or penetration test will enable Cyberity to design an assessment or test that will best deliver on your requirements.

CONSIDER THE FOLLOWING POSSIBLE OBJECTIVES:

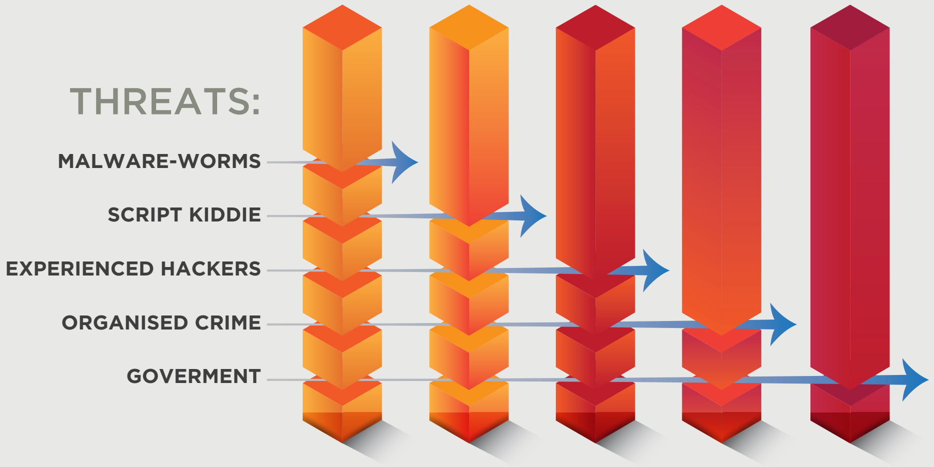
- Is the assessment purely to meet regulatory or auditing requirements?
- Has there been an attack on your systems and do you now require assurance that security gaps have been closed?
- Has your organisation reached the next security maturity level, which necessitates (deeper) assessments and testing being done?
- Do you have a new system that requires a level of security vetting before being implemented into production?

WHO DO YOU WANT TO DEFEND AGAINST?

Threats vary in sophistication, intensity and stealth – ranging from concerted efforts by governments to “script kiddies” experimenting with hacks.

Our vulnerability assessment and penetration testing will highlight at what risk your infrastructure is, and to what level your existing defences will protect you.

For instance, will a “script kiddie” be capable of compromising your environment, or will compromise require the extensive resources and expertise of organised crime?



Cyberity

THE DIFFERENCES BETWEEN

VULNERABILITY ASSESSMENT and PENETRATION TESTING

VULNERABILITY ASSESSMENT

A Vulnerability Assessment is designed and conducted to reveal as many security vulnerabilities as possible in an environment.

When is it advisable?
When you suspect or know you have security issues, and need to ascertain what these are and how they should be corrected.

Deliverables of the assessment
A complete and prioritized list of vulnerabilities, plus recommendations for remediation.

PENETRATION TESTING

A Penetration Test is designed to simulate the actions an attacker would take to achieve a specific malicious goal, for instance to access a database or to modify sensitive salary details in the HR system.

When is it advisable?
When you believe your security is strong, and would like to confirm this assertion. (Typically when there are no known vulnerabilities.)

Deliverables of the test
A report detailing how security was breached to achieve that one, specific goal, plus recommendations for remediation to prevent that same goal being achieved in reality.

ASSESSMENTS AND TESTS TO DETERMINE THE LEVEL OF PROTECTION REQUIRED

VULNERABILITY SCAN

A cost-effective, usually automated, scan to determine vulnerabilities of a system or part of a system. This is the foundation for creating visibility of the vulnerabilities that may exist in an environment.

More mature organisations may already perform these scans as part of their regular or routine vulnerability management process.

VULNERABILITY ASSESSMENT

The objective here is to find as many vulnerabilities as are present in an environment, in order for them to be remediated – thereby rendering the client more secure. The assessment can be very broad or it may target a specific set of systems, such as web applications.

The assessment provides a prioritised list of vulnerable areas. The client can then have these remediated.

PENETRATION TEST

Each penetration test has a clear goal set as the deliverable. The test mimics the actions a hacker might take. The goal could be to obtain some defined confidential data, gain access to a particular system or even gain physical access. Penetration tests are ideally suited to organisations with high security maturity.

These organisations may have complete trust in their existing defences. Penetration tests allow for the validation or disproof of the efficiencies of these defences.

WIRELESS NETWORK SECURITY ASSESSMENT

Most wireless network security mechanisms can be breached in a matter of minutes, allowing hackers to access the network.

A wireless network assessment by Cyberity will provide an organisation with insight into the level of risk exposure its wireless network introduces to the organisation's infrastructure.

SOCIAL ENGINEERING ASSESSMENT

Organisations often overlook this attack vector (or path of attack). Social engineering can be very effective and crippling. Most breaches today include elements of social engineering as part of the attack. Phishing is the most prevalent type, but there are many other forms of social engineering.

A social engineering assessment will provide your organisation with insight into how vulnerable it may be to social engineering attacks.

WEB APPLICATION ASSESSMENT

Web applications are a common attack vector (or path of attack). More often than not these applications are vulnerable in one way or another. Most web application design briefs do not include security as part of the specifications. Instead they focus on ease of use, development timelines and features. This leaves most applications vulnerable.

Cyberity's assessments identify weaknesses in web applications and APIs, in order for these to be secured.

GET IN TOUCH AND GAIN INSIGHT INTO YOUR VULNERABILITY STATE

Phone: 02 8971 4548 | Email: Security@cyberity.com.au | Web: www.cyberity.com.au