Are you satisfied that your network is adequately secured against a malicious hacker?

Would your externally-facing systems stand up to an attack?

Is your network leaking confidential information into the public domain?

Is your mail server securely configured?

Have you been infected by malware?

Perimeter security technologies such as firewalls are paramount to a business’s defence against attack, but cannot be assumed to be impenetrable. In fact, the ever increasing expansion of the internet is eroding the boundaries of the traditional perimeter, allowing new services and interaction to be delivered direct to the desktop, tablet or mobile phone, bypassing what was once the primary (physical) line of defence.

**What is Penetration Testing?**

“Penetration Testing” or “Ethical Hacking” is the process of identifying vulnerabilities in your technology environment and assessing the exposures they create. This is performed in the same way as a malicious attacker would, with the same techniques and tools, however, without the malicious intent. This allows the enterprise to understand the level of exposure that it has to the various forms of attack and is the only real test that uncovers hidden vulnerabilities. It is a convincing tool in planning remediation activity and security spend effectively.

It is important to understand that not all attackers are actually persons; in fact the majority of attacks today are facilitated by automated technologies and malicious software agents that have been specially created to exploit common known weaknesses. These attacks are arbitrary in nature, and attack everyone and anyone with a vulnerable connection to the internet, regardless of who they are or what data they have.

A continuously changing technology and threat landscape means that penetration testing should not be a one-off exercise, but rather, a strategic process designed to assess exposures on a regular basis to design better controls and understand risk in more detail. It also serves as for peace of mind – to confirm that the defences are holding up as intended.
“Penetration Testing” is typically associated with the process of attempting to identify and exploit vulnerabilities on externally facing systems. However, different penetration testing exercises address different threats:

1. **External Penetration Testing**: The focus of this testing is to assess whether someone outside your organisation is able to access your core information assets from the internet through weaknesses within your perimeter.

2. **Internal Penetration Testing**: The objective is to assess whether internal staff or someone with access to your physical premises can access information assets they are not privy to.

3. **Web Application Security Assessment (WASA)**: The focus of this exercise is to assess and identify what vulnerabilities can be exploited through web applications and services made available to clients, employees, etc. Such vulnerabilities may allow an attacker to exploit the application and extract its data or to further elevate their privileges.

**Why do I need this?**

Although the organisation may have invested in significant security safeguards, a penetration test carried out by an independent third party can provide assurance that the safeguards in place are effective and thus protecting the organisation’s reputation with customers, business partners and regulators – ultimately acting as a business enabler. Used properly, a penetration test can also address specific compliance objectives in regulated sectors and help the organisation’s IT department to take the necessary corrective measures (e.g., by patching vulnerable systems) and ensure continuity of critical business operations that rely heavily on IT systems.

As outlined above, penetration testing provides detailed information on actual, exploitable security threats. Through the execution of periodical penetration testing exercises, an organisation can derive business value by proactively identify which vulnerabilities are most critical and plan a response procedure to ensure that information system resources are available when and where they are needed most.

**Typical Test Process**

Testing involves five key stages, with the option to “penetrate” during an assessment if there is sufficient need, risk appetite and potential reward.

1. **Scan** Passive and active scanning techniques are used to identify possible targets.

2. **Analyse** Analysis and cross-referencing of vulnerabilities found on the targets.

3. **Follow up** There is no substitute for the experience of a seasoned tester; any findings from the prior stages are manually verified to eliminate false alarms.

4. **Penetrate** During the manual follow up of findings, our test teams may discover vulnerabilities that if exploited, could bring further levels of access. If this is the case, a full risk and business impact analysis is performed and presented to you, so that you can decide if the potential value outweighs the likely risk.

5. **Report** The key to value is a report the business can understand, with practical recommendations of deeply technical issues, analysis of potential root causes and a clear explanation of the risks.

**Our Approach**

At PwC, we ensure that a true, reflective threat scenario is the starting point for any testing. This allows us to tailor the testing performed to maximise value for you. All of our testing is bespoke and in response to the real world threat scenarios that the business could face.

**Our Experience**

Globally, PwC has performed this service for clients for over 18 years, and has developed a mature and robust methodology that ensures all client risk is adequately managed. We have secure laboratory environments to ensure that all testing activity is controlled and contained, and that your data is adequately secured.

Locally, we have experience in successfully performing penetration testing on online banking services, online retail shops and online workflow systems for our clients.

**Have you assessed and addressed the risks that your business is facing?**

**Contacts**

George Sammut
george.sammut@mt.pwc.com
+356 2564 7608

Gordon Micallef
gordon.micallef@mt.pwc.com
+356 2564 7014

Nathan Gatt
nathan.gatt@mt.pwc.com
+356 2564 7035