EINPRESSWIRE

Why is penetration testing necessary?

ELY, UK, September 5, 2013 /EINPresswire.com/ -- With cyber attacks becoming the norm, it is more important than ever before to undertake regular vulnerability scans and penetration testing to identify vulnerabilities and ensure on a regular basis that the cyber controls are working.

Geraint Williams, Senior Consultant at cyber security experts IT Governance, explains: “Vulnerability scanning examines the exposed assets (network, server, applications) for vulnerabilities – the down side of a vulnerability scan is that false positives are frequently reported. False positives may be a sign that an existing control is not fully effective, i.e. sanitising of application input and output, especially on web applications.”

Penetration testing looks at vulnerabilities and will try and exploit them. The testing is often stopped when the objective is achieved, i.e. when an access to a network has been gained - this means there can be other exploitable vulnerabilities not tested.”

Organisations need to conduct regular testing of their systems for the following key reasons:

- To determine the weakness in the infrastructure (hardware), application (software) and people in order to develop controls
- To ensure controls have been implemented and are effective – this provides assurance to information security and senior management
- To test applications that are often the avenues of attack (Applications are built by people who can make mistakes despite best practices in software development)
- To discover new bugs in existing software (patches and updates can fix existing vulnerabilities, but they can also introduce new vulnerabilities)

Geraint adds: “If people are attacked through social engineering this bypasses the stronger perimeter controls and exposes less protected internal assets.

The worst situation is to have an exploitable vulnerability within infrastructure, application or people that you are not aware of, as the attackers will be probing your assets even if you are not. Breaches, unless publicised by the attackers, can go undetected for months.”

Vulnerability scanning and penetration testing can also test an organisations ability to detect intrusions and breaches. Organisations need to scan the external available infrastructure and applications to protect against external threats. They also need to scan internally to protect against insider threat and compromised individuals. Internal testing needs to include the controls between different security zones (DMZ, Cardholder data environment, SCADA environment etc.) to ensure these are correctly configured.

How often to conduct pen testing?

Pen testing should be conducted regularly, to detect recently discovered, previously unknown vulnerabilities. The minimum frequency depends on the type of testing being conducted and the target of the test. Testing should be at least annually, and maybe monthly for internal vulnerability scanning of workstations, standards such as the PCI DSS recommend intervals for various scan types.

Pen testing should be undertaken after deployment of new infrastructure and applications as well as after major changes to infrastructure and applications (e.g. changes to firewall rules, updating of firmware, patches and upgrades to software).

IT Governance provides comprehensive pen testing and PCI QSA services. The company can be contacted on 0845 070 1750 or by email at servicentre@itgovernance.co.uk.

More information on IT Governance's pen testing packages is available here: www.itgovernance.co.uk/penetration-testing-packages.aspx.

- Ends -

NOTES TO EDITORS

IT Governance Ltd is the single-source provider of books, tools, training and consultancy for IT governance, risk management and compliance. It is a leading authority on data security and IT governance for business and the public sector. IT Governance is 'non-geek', approaching IT issues from a non-technology background and talking to management in its own language. Its customer base spans Europe, the Americas, the Middle East and Asia. More information is available at www.itgovernance.co.uk.

Desi Aleksandrova
IT Governance
+44 (0) 845 070 1750
email us here