PENETRATION TESTING

logically secure

The penetration test always starts with us working with you to establish a goal of the test and determining the best possible services as well as their depth. This is followed by scoping in which we further set up ground rules and test boundaries. Our aim is to protect you and place you in a comfortable position in which you are fully aware of all risks associated with the chosen set of technologies or processes.

Logically Secure utilise skilled testers to ensure no information is missed in the process. We test against well-recognised standards such as OWASP TOP 10, ASVS, CIS, NIST and others to ensure our testing is catching all the latest risks in a way that can be categorised.

We are flexible regarding our process of penetration testing to fit your needs; however, a typical penetration testing methodology is usually utilized.

We also cover typical scenarios when carrying out penetration tests:

- Would an attacker with no knowledge about your company be able to gain access to your systems? (Black Box Test)
- Would an attacker with valid standard credentials be able to gain further access or take over your systems, for example, a supplier? (Grey Box test)
- Is using open source tools, libraries of which code is available to potential attackers placing you at risk? Is an internally developed code secure enough? (White Box/Source code review)

In addition, there are other services which help with different aspects of information security:

- Social Engineering – Vishing/Smishing/Phishing/ Physical Penetration Test (Have you thought of lost laptop scenarios or unlocked internal workstation left unattended?)
- Internal Infrastructure testing (If an internal system is compromised, could compromise of other systems and data happen?)
- Cloud Review (What would happen if someone gained any access at any level to cloud systems or panels you use?)
- Mobile Application testing (Do you have mobile applications for users or suppliers to utilise your services while they are on the go? Could that lead to exposure of data or create a potential route to your other systems?)

It is important to keep in mind that the threat is not only external, but some of the most highly damaging cyber-attacks have also been attributed to weak internal controls. Threats may also appear through employee negligence, or even accidentally.

Each member of our team has a strong technical understanding, as well as a consultative, risk-management focus. Logically Secure testing team engages with various types of work throughout the organisation to ensure they are skilled and up to date in all areas.

FURTHER INFORMATION

For general information on Products & Services please email:

info@logicallysecure.com

Or please visit our websites:

www.logicallysecure.com
www.cybercpr.com