CyberOne

Pen testing has moved on. Have you moved with it?

In ‘normal times’, many businesses would run their penetration test annually. But the world has changed dramatically over the past couple of years. The shift to hybrid working post-Covid has opened-out the threat landscape. Regular infrastructure changes are commonplace for many businesses. Threat actors and nation-states have accelerated their activity (think Ukraine, Russia, China, North Korea). And the attacker sophistication has gone to another level, driven by advances in technology and more organized and professional set-ups.

So standard approaches to pen testing are no longer sufficient to keep your cyber defenses water-tight year-round. Continually following the same pen testing formulas limits the creativity and scope of the findings. It leaves room for areas to be overlooked based on strong biases and produces predictable reporting, which does not keep pace with your adversaries.

This piece highlights how things have moved on to help you think differently about pen testing and what is needed for your business in today’s changing landscape.

Pace of the Testing Process

In today’s business environment, time to market is key. A critical release of new software, for example, can’t afford to be delayed by a slow and inefficient pen test. You need to pin your pen test provider down up-front to deliver to your required timescales. Some companies require a notice period of 4–6 weeks, whereas many others can do the job within a couple of days for a premium price. Variables such as the number and nature of tests should be agreed beforehand. Consider retained pen testing services, particularly where you have infrastructure changes planned to ensure reliable, timely delivery through multiple test phases during your projects. Don’t accept second best when it comes to the delivery of your project!

Automation Advancements

Automated testing has come on leap and bounds. The standard annual test may no longer be the best option for your business. Automation can streamline the process and improve the effectiveness of your test and gives you the option of either an on-demand service or continuous security validation, depending on your needs. However, automation can still be prone to false positives. Creating a mix that also involves a manual test can iron-out any irregularities that an automated test might leave behind. Whichever option you choose, we need to stop thinking of pen testing as a once-a-year exercise – at the least, you need to consider a test each time you upgrade an element of your infrastructure where security holes could appear.

Pen Testing Methodology

Methodologies continue to evolve and the one you choose needs to align with your current business environment and immediate needs. Many methodologies are now in existence, produced by many well-known organisations and research labs. However, each of these methodologies is made for a specific type of situation. Therefore, it is crucial to choose a provider who is fluent in a range of methodologies and will tailor the approach to you. Examples include PTES (with detailed technical guidance on the different test elements), OSSTMM (an open-source solution with test cases that result in verified facts), NIST (with a planning, execution and post-execution structure), OWASP (specific for web applications) and many more.

Quality of the Outputs

The quality of the final report is key to ensure you take the right actions to plug any gaps. It needs to align to the latest threats. Review a sample report from your provider up-front and ensure that your report will be bespoke to your specific engagement as opposed to something “off the shelf”, as well as in a format that works for you. Ask yourself if the information provided is detailed enough to help prioritise the remediation of weaknesses, both immediate and in the long term. As a bare minimum you need a business-focused executive summary, a thorough narrative of how the attacks or exploits were executed, clear recommendations and a risk rating against every stage. In short, will the provider work to your requirements and within your boundaries?

Expertise and Experience

There are a lot of new entrants into the pen testing space. It is essential your penetration testing partner is recognised by accreditation bodies such as CREST, but also take their own information security seriously by holding certifications such as ISO27001. A penetration testing provider should be able to demonstrate a long history of successful and well-received testing engagements backed up with client references. Expertise also extends to their availability, as well as their ability to communicate with you so check whether they outsource work to sub-contractors (who may be working in different time zones). Direct access to the actual engineer conducting the test is crucial.

Liability Insurance

Liability insurance is ever more vital to protect you from any uncertainty or side-effects of enduring penetration testing. For instance, if the penetration testing service provider causes any damage to your software during their testing and invasive activities, insurance will help remedy this damage. All the legitimate penetration testing companies have an insurance policy that protects you from any risk that a rigorous penetration test might involve so before hiring a penetration testing company, ask them whether they are covered.

Would you like to discuss how to evolve you pen testing approach to align with the changing threat landscape?

Get in touch →

About CyberOne

CyberOne strives to offer the most trusted cyber experience in the digital world. Founded in 2005 and based in Milton Keynes, our assessment, detection and response services empower you to stay one step ahead of the latest cyber threats. We are trusted by leading UK and global businesses and our people provide a service that is second to none.

www.cyberone.security
+44 (0)3452 757575
enquiries@cyberone.security