PENETRATION TESTING

WHY PENETRATION TESTING IS IMPORTANT

The risk is real

More and more companies are under threat by malicious criminal organisations. The number of attacks, as well as the type of attack, is increasing weekly and it really is becoming a case of 'when' rather than 'if' you are attacked.

Cyber attack – it's not if, but when

Establishing a baseline

Conducting an external, third-party penetration test is the best way of precisely establishing what your real-time security posture looks like. It is the best place to start on your journey of protecting your business, its assets, reputation and overall business continuity.

Risk assessment

How much is your business going to lose if your systems are compromised? How much would your clients lose? You also need to be aware of fines for non-compliance or preventable breaches.

Regulation and compliance

Non-compliance to regulations may cost you a hefty fine, lose you your license to operate, or even worse, get you jail time.

Even though penetration testing may not directly address the concern of data privacy, it helps to reduce the risk of a data breach from software vulnerabilities.

Reputation

A company's reputation will suffer when a data breach is announced. Share prices will almost certainly be affected and may cause a loss of customer confidence and subsequent loss of revenue.

Financial

In addition to the loss of revenue, if your organisation is hit by a malicious criminal, a ransom is often associated with the attack.

Most cyber insurance policies do not cover ransom payments.

If you decide as an organisation that you will pay ransom, your insurance premium will become very expensive, as ransom demands are increasing rapidly.

Competition and rivalry

Breached information may end up in the hands of competitors – a disastrous consequence.

Your competitors will likely use a breach against you to attack your credibility.

Professional advice on remediation requirements

Identifying a threat risk is the first step. Providing a remediation strategy is the most critical step. Cyber Citadel takes pride in providing clear, concise advice on what your technical staff need to do to patch the threat. If required, we are also able to make the changes on your behalf.

Penetration Testing vs Vulnerability Assessment

Vulnerability Assessments

Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to and those that cannot.

Penetration Testing

Penetration tests find exploitable flaws and measure the severity of each. A penetration test is meant to show how damaging a flaw could be in a real attack.

See over for common business concerns and FAQs

It may disrupt our systems

At Cyber Citadel we protect against this by ensuring:

- All tests are carried out during pre-approved hours only
- We work directly with your staff in coordinating what and when testing is executed
- We do not exploit the system with denial-of-service attacks unless specifically requested to
- We do not automate any of our scans – they are all manually controlled

It may cause loss of data

Cyber Citadel takes pride in our successful track record, the feedback we have had from our existing partners and, above all, our highly skilled staff. The risk of data loss through penetration testing is significantly less than via cyber attack.

It costs too much

We repeatedly see tests that have been carried out using tools that are run automatically and are therefore cheaper than a manual penetration test. It is important to note that these are vulnerability assessments. Such automated tools only point out where vulnerabilities may occur; they do not show or explain how the vulnerabilities can be exploited. Vulnerability assessments do not replace or even begin to compete with a full penetration test.

A breach could cost your company many multiples of a penetration test cost – think of it as insurance.

Where should I start?

Ascertain your security posture

- A simple way to start your journey is to engage Cyber Citadel to conduct a basic security posture assessment known as Next Generation Vulnerability Assessment (NGVA)
- A vulnerability assessment is a 'look but don't touch' scan of your entire network to identify security weaknesses and priorities. A common issue in many vulnerability assessments is a large number of 'false positives': vulnerabilities highlighted which have already been addressed by other means that the scan does not detect. False positives can often lead to your internal IT team wasting significant time chasing down imaginary vulnerabilities. Vulnerability assessments can be followed up with a targeted penetration test if the assessment highlights a moderate amount of security issues.
- Once we have established your baseline security posture, we can jointly plan where you should focus to significantly improve your company's cyber security.

We can do it in-house

It is unlikely that in-house staff will have the requisite skills needed to perform a successful penetration test. A specialised external partner, like Cyber Citadel, is far more likely to find all the vulnerabilities within your company infrastructure. We will carry out a manual deep dive into your whole environment to find not just the obvious vulnerabilities, but the complex vulnerabilities: those that may not exist now, but that could become critical and or high risk if a lower-risk vulnerably were exploited.

Keeping abreast of the threat landscape is time-consuming specialist work. Via our network of contacts within the worldwide cyber research community, Cyber Citadel are aware of any new risk as soon as it is executed and can offer important early detection to our clients.

Risks of doing it in-house

Using a less-experienced tester presents a number of disadvantages:

- Testing might result in unscheduled system downtime that badly disrupts the business, and they may unwittingly cause a total system crash
- Testing may slow down the network, affecting business productivity, potentially incurring costs
- The tester might automate the test, which has a high probability of producing a false positive and/or a false negative result
- A Distributed Denial of Service (DDOS) may be triggered
- Scenarios arise that the tester does not have the breadth and depth of knowledge needed to address quickly
- Findings are not reported in a way that all levels of staff can clearly understand – for the safety of the whole organisation, it is just as important for Fred in accounts to realise the vulnerability of opening an email attachment as for IT to know where there is a cross-site scripting vulnerability
- Employing a full-time cyber security team member and keeping them fully trained would be more expensive than utilising a Cyber Security partner only when needed
- Lack of access to a security consultant who can provide a detailed report on how you can remediate the threat once identified – this is a core strength of Cyber Citadel.

Engaging Cyber Citadel is simple

All we require is a confirmation email and we will get to work immediately.

The more quickly you determine your baseline security posture, the more likely you are to be able to improve the security of your entire network and remove the risks of financial and brand damage. Get in touch now.