Penetration Testing Services

What is it?

Penetration Testing Services from **norm.** assess an organisation's networks, systems, applications and people to identify and address security weaknesses.

Our highly trained security analysts help your organisation to manage cyber security risks by identifying, safely exploiting, and supporting the remediation of weak points in your environment. Left unchecked, these vulnerabilities could lead to data and assets being compromised, lost to malicious attackers and potentially other direct and indirect collateral damages and losses.

The purpose of Penetration Testing is simple:

* To identify and exploit weaknesses in your corporate environment through a combination of vulnerabilities, exploits and social engineering techniques
* To deliver a final incident report which gives detailed findings and recommendations to prevent similar incidents in the future

Why now?

As data breaches become increasingly common, even amongst the world's largest companies, maintaining the security and privacy of customers is a growing area of concern for businesses and the IT organisations that support them.

Technology is consistently evolving, and cyber-attackers are continuously developing new techniques in order to breach an organisation's defences. New vulnerabilities are being identified on a constant basis, and they are present in all software and devices including laptops, desktops, servers, IoT devices and web applications.

Penetration tests form part of an industry-recognised approach to identifying and quantifying risk. They actively attempt to exploit vulnerabilities in a company's infrastructure, applications, people, and processes. By simulating the techniques used by cyber criminals and hackers, **norm.** provides context around the extent of vulnerabilities and the likelihood and impact of the breach of an information asset.

What's included?

* Deployment of **norm.** cyber security experts to identify and exploit weaknesses in your corporate environment through a combination of vulnerabilities, exploits and social engineering tactics
* A range of assessment services including External Pen Testing, Internal Pen Testing, Web Application Pen Testing and Vulnerability Assessments
* A final incident report providing detailed findings from the assessment(s) and recommendations to prevent similar incidents in future

Want more detail?

For the full Service Description of our Penetration Testing Services <<ClickHere>>.
To register your interest and get one of the team to call you <<ClickHere>>
or just give us a call on **+44 (0)20 385 55242.**

***Reassuringly dull cyber security**

norm.

In a nutshell…

Regular penetration testing is vital to assessing the effectiveness of an organisation's cyber security defences. It is a well-recognised means of discovering how vulnerable a company is to becoming the victim of a data or cyber security breach, and customers and suppliers are increasingly specifying this as a condition of doing business.

norm. offers a variety of penetration testing services, and our team has extensive experience of conducting them for organisations in a wide range of industries. We also work closely with our clients to address any issues found on an ongoing basis.

How does it work?

The **norm.** team will work alongside you throughout the penetration testing process. We will:

* **Arrange a technical scoping call** between a member of norm's Red Team and your organisation's IT team (or your managed service provider (MSP)) to confirm the configuration of your network and your exact requirements
* **Document the scope** of the penetration test assessment service and ask you to agree and sign off
* **Agree a testing window,** during which the testing team will be on call throughout and available for any questions that may arise during the test
* **Provide you with a report** detailing the findings, as well as remediation steps and/or best practice recommendations to address any issues found

We will offer you the opportunity to review the results of your test with the testing team to help you understand exactly what vulnerabilities were discovered, how they could be taken advantage of, and the steps that need to be undertaken to resolve any weaknesses.

If requested, will can conduct a free re-test on all 'Critical' and 'High' category vulnerabilities to ensure that they have been addressed. Re-tests must occur within 90 days of the date the report was provided.

FAQs…

I've had a penetration test in the past, why do I need another one?

Things change over time, additional users, software and infrastructure can all impact your cyber security posture. There are two ways to test how robust your cyber security is – penetration testing from a company like **norm.** with clear results to help you improve your defences, or actually getting breached.

I only use cloud-based services now, so is there any point in penstration testing?

Firstly, you need to make sure that you've asked your SaaS providers for their penetration test results. Secondly, it's not just your data that is at risk, penetration testing helps to identify the weakness that could open up access to those SaaS platforms or lead to ransomware attacks.

How do you define the scope of the test?

We work with you to best define the scope of the testing, to ensure that not only have we thoroughly tested everything, but that the results are as clear and relevant as possible.

How frequently do you recommend we run penetration testing?

Penetration testing is usually run annually. However, if you are developing your own web applications or are making large-scale changes to your network, we offer change-based testing. This could be a subset of the full testing designed to check those areas of software or hardware that have been changed.

In addition to the obvious benefit of understanding how protected we are, are there any other business benefits to this service?

Investing in robust and effective penetration testing demonstrates that your organisation takes data and cyber security seriously. It reduces your operational risk, builds your reputation with customers, suppliers and regulatory bodies (such as the ICO) and ultimately improves the value of your business. In addition, some customers and suppliers may insist on seeing up to date penetration testing results as a requirement of doing business with you.

norm.