Omni
CYBER SECURITY

Penetration **Testing**

Check the strength of your technical security before someone else does

About **OmniCyber Security**

At OmniCyber Security, we want to make watertight IT security and compliance accessible to every business. By sharing our knowledge of cyber security and rich industry experience, we help you to ensure your organisation is properly protected.

We offer a wide range of services to make your route to success as simple as possible. Our services include: CREST-accredited penetration testing, PCI DSS compliance, ISO27001 consultancy, and other INFOSEC services.

We're a boutique company, passionate about helping others. Our expert, friendly team are always on hand to offer advice and devise tailored solutions that meet your organisation's unique needs.

What is **Penetration Testing?**

Penetration tests are designed to discover whether there are any flaws in your technical security. Using real-world attack simulations, our world-class team utilises a complete range of penetration testing tools to check the full range of scenarios your security system may face.

Unauthorised attacks due to security flaws can lead to devastating large-scale breaches. It's easy to forget how much vulnerable information technical security must protect. Personal data, intellectual properties and cardholder information are all at risk from even the tiniest flaw in your defences.

Penetration testing makes it possible to identify any weaknesses in a safe, controlled way, and deal with them proactively to keep your business and assets safe.

Regular penetration tests verify that your cyber security measures are working, and can help you comply with globally-recognised security schemes like PCI DSS.

Penetration Testing Services

Hacking comes in all shapes and sizes, so there are a variety of penetration testing services available:

Web Application Testing

Web applications are often the hub of your digital landscape, and prime targets for cyber criminals. Web app tests audit the application from an unauthenticated, real-world scenario – using all the techniques that experienced malicious adversaries would.

Social Engineering

People are often the biggest weakness in an organisation's cyber security. By manipulating employees into disclosing sensitive information or installing malicious software within your organisation, hackers can attack with little technical involvement.

You are only as strong as your employees. Do they know the dangers to look out for? Social engineering tests will identify any weaknesses within your organisation and provide a starting point for further actions necessary to keep your company data safe.

Mobile Application

Our mobile app pen testing service evaluates the security of your mobile apps across both iOS and Android platforms. By simulating real-world attacks, we identify vulnerabilities in app code, authentication protocols, data storage, and more. This helps protect against risks like data breaches and unauthorised access, so your mobile applications are secure and resilient.

Internal Infrastructure Testing

By simulating an insider attack, we will discover how far an insider can get into your systems without detection. Testing internal controls and domain security will uncover the extent of information an insider could access and extract, exploring everything from unauthorised access, to confidential documents, to security levels for credit cards and customer data.

External Infrastructure Testing

Many perimeter devices are obtained from vendors and therefore vulnerable to attack due to internal default configurations that are easily exploited by hackers. Firewalls, file servers and other public-facing infrastructure as well as remote workers' connections can be checked using external penetration tests to ensure they are secure.

Red Teaming

Red teaming isn't a typical cyber secrity assessment. By emulating a full-scope, realistic attack, following the MITRE ATT&CK® framework our experts challenge your security measures across physical, digital, and human layers.

This advanced service goes beyond traditional testing to expose gaps in your unique security setup and prepare your team for real-world cyber threats.

Penetration Testing In Compliance

Penetration testing is a critical part of cyber security. As a result, many compliance schemes require the completion of a penetration test.

Cyber Essentials Plus

Cyber Essentials Plus is a requirement for businesses operating within the UK government supply chain. It's a government standard which also serves as a great introduction to cyber security for all types of businesses. At OmniCyber Security we provide comprehensive support for Cyber Essentials Plus, including vulnerability assessments or scans which are a requirement for the standard and can be undertaken by our penetration testing team.

ISO 27001

ISO27001 is necessary for supply chains for businesses of any size. Forming part of due diligence, ISO27001 provides an overview of information security management systems. ISO 27001 doesn't directly require a penetration test at present; however companies are required to prevent the exploitation of technical vulnerabilities in order to comply with control A12.6.1. Completing a penetration test will ensure this requirement is fully met and evidenced.

PCI DSS

Any company that wishes to process card payments must demonstrate their PCI compliance annually. If compliance is not achieved, the merchant may receive non-compliance fines from their acquiring banks or even the revocation of their payment card privileges for continued non-compliance.

To be PCI compliant, that company must complete a penetration test every year if they are a Merchant, or every six months if they are a Merchant Service Provider. The requirement is part of the PCI-DSS standard for card payment services. Quarterly ASV scans and another penetration tests are also necessary after any major change to a technical environment.

PSN ITHC

PSN IT Health Checks ensure non-central government organisations are following all public sector guidance. They are carried out once a year by a CREST-accredited organisation like OmniCyber Security.

Omni
CYBER SECURITY

Case Studies

Client: Global Organisation

Discovered critical physical security weaknesses

During a physical social engineering engagement, OmniCyber Security gained unauthorised access to restricted areas within the client's head office, bypassing multiple security controls, both digital and physical. This exercise revealed critical gaps in the client's security posture, highlighting the potential risks of insider threats and physical breaches.

Client: Finance

Multi-layer security gaps in red team engagement

Through a comprehensive red team engagement, OmniCyber Security identified several critical points of entry that an adversary could exploit, including spear-phishing and network vulnerabilities. By reinforcing employee training and improving access controls, the client reduced the risk of targeted cyber attacks.

Client: Transport

Identified email security gaps through phishing simulation

OmniCyber Security conducted a social engineering test that resulted in a significant number of employees falling victim to simulated phishing emails., including the Domain Admin, handing our team the keys to their digital kingdom.

Client: Retail

Demonstrated denial of service attack vulnerabilities

Our team conducted a DoS assessment to identify potential disruption points in a client's network. We simulated attacks that demonstrated how an adversary could overload systems, leading to service unavailability. Based on our recommendations, the client took action to improve service availability and resilience based on our recommendations.

You can find the full story of each of these case studies and more [on our website.]

Why Penetration Test?

Cyber attacks are an ever-increasing threat to organisations all over the world. For so many companies, large or small, cyber security simply isn't something they have the capacity to manage properly. It's a persistent task which requires time, commitment and expertise.

Modern threats are imaginative and wide ranging, beyond your internal systems there are so many external factors to address. The serious risks to your business are multi-layered and complex, from stakeholders to an employee opening an email attachment or a USB device found in a car park. Simply running the latest technology or updating software isn't enough.

It's for these reasons, businesses are often slow to take the precautions they need before it's too late. With our help, you can learn about your weaknesses before they become a problem.
Working alongside you, we'll give you the time, dedication, services and expertise you need to put plans into action.

That's why we love penetration testing. With penetration testing, you get to see exactly what your enemies will do before they do it. As they say, you have to act like a thief to catch a thief.

We're driven by a desire to see your organisation protected and your knowledge of cyber security grow. We believe it's important everyone understands how to stay safe, and that's why we promote basic security awareness training for all staff.

We're proud to have a sensational team of forward-thinking, dedicated experts in their field. With some of the best minds in the industry amongst our staff, we know we can deliver an exceptional service to you. Commitment, passion and enthusiasm mean we're always driving each other forwards and swapping ideas and new techniques to aid testing. Our company has a warm, positive, family atmosphere that extends to our customers. We'll get to know you and your business inside out and are always here to help you in any way you need.

Communication is key for penetration testing, and at Omniwe're experts at providing transparent services and easy methods of communication. We'll always be open and honest with you, explaining everything clearly using language you understand.

Whatever your needs are now and in future, we're always here to help.

Stuart Joce
CEO
OmniCyber Security

OmniCyber Security
Grosvenor House
11 St Paul's Square
Birmingham
B3 1RB

Call us on
0121 709 2526

Email us at
info@omnicyber security.com