Ongoing Penetration Testing & Vulnerability Scanning

Businesses face a constantly evolving threat landscape, with malicious actors devising new ways to breach systems and steal sensitive information. According to the 2023 Cyber Breaches survey cyber attacks on UK businesses nearly than quadrupled between 2022 and 2024, rising from 2.39 million to over 8.58 million incidents. Despite this, only 32% of UK businesses undertook a Cyber Security Audit to see if their business was vulnerable to modern threats. Maintaining robust cyber security practices through regular audits, vulnerability scanning and penetration testing is an essential defence against the more than 500,000 new threats discovered daily, and it also ensures businesses remain compliant with standards such as Cyber Essentials Plus and ISO 27001.

What is Penetration Testing & Vulnerability Scanning?

Penetration Testing (commonly shortened to “Pen Testing”) is a deliberate simulation of cyber attacks on computer systems, networks, web applications or cloud platforms, carried out to identify potential weaknesses that cyber criminals could exploit. Think of this as an extensive fire drill for cyber security, uncovering vulnerabilities before real criminals discover and exploit them. After the assessment, a report is compiled with detailed findings and recommendations to reinforce an business’s security posture. This allows us to work with businesses to be able to “patch” these vulnerabilities. Once vulnerabilities are patched it allows us to conduct a further penetration test to ensure that businesses are secure.

The Benefits of Penetration Testing for Your Business

Identifying shortcomings in a security strategy is key to preventing data breaches that could result in financial loss, reputational harm and legal consequences. Pen testing spots issues before attackers can exploit them, thereby allowing businesses to patch vulnerabilities and bolster defences. It is also vital for meeting the regulatory requirements imposed by data protection laws and standards such as Cyber Essentials Plus and ISO 27001.

This testing is not limited to revealing technical flaws. It also analyses real-world incident response capabilities. When incidents occur, well-drilled response procedures can minimise the resulting damage. By regularly probing systems, managers and IT teams gain insights into potential vulnerabilities and practice swift, efficient responses if an attack happens.

Why Businesses Shouldn't Overlook Penetration Testing

What was once regarded as a luxury to protect only highly sensitive data has become a necessity. Data from the UK Government's Cyber Security Breaches Survey 2025 suggests that attacks on UK businesses continue to escalate, with criminals adapting quickly to out manoeuvre conventional security measures. Regular penetration testing and subsequent improvements keep businesses one step ahead of emerging threats.

The financial consequences of a breach can be severe. A recent study found that the average cost of a data breach reached $4.24 million in 2021, and recent figures indicate an ongoing rise. Pen testing is a cost-effective way to reduce these risks and could save an business from catastrophic financial setbacks.

Maintaining customer and client trust also relies on demonstrable security measures. Meeting requirements under frameworks such as Cyber Essentials Plus and ISO 27001, both of which call for regular and ongoing pen testing, helps assure stakeholders that data is managed responsibly.

TwentyFour Crafting Comprehensive Cyber Security Solutions for Your Business

At TwentyFour we believe that ongoing penetration testing forms a critical element of any robust cyber security strategy. However, it is important that businesses understand that an effective strategy is not limited to ad-hoc tests. It should encompass continual assessments of findings and the deployment of further safeguards and best practices to defend against evolving threats

Our in-house Cyber Security Operations Centre (SOC) is staffed by skilled cyber security professionals and penetration testers, offering custom testing programmes aligned with each business's specific needs. Whether that be on-site infrastructure, cloud storage and database management, web and mobile applications, and much more. Adapting to persistent threats, the team helps safeguard the integrity, confidentiality and availability of your business' vital data.

Penetration testing is a foundational tool that equips businesses for both prevention and rapid response. Trust, customer loyalty and operational resilience are all strengthened when comprehensive testing and remediation strategies are in place. Knowledge and preparedness are key weapons in the fight against modern cyber threats, and ongoing penetration testing and vulnerability scanning delivers both.