aztech

Cyber Security Services

Penetration Testing

Taking a deep dive into your systems to uncover issues, vulnerabilities & test your security's effectiveness against cyber-attacks.

about the service

Penetration testing, also known as Pen testing or ethical hacking, is an authorised simulated cyberattack on your IT infrastructure. Having the right security tools for your organisation is step 1, but without testing those security tools, you cannot be 100% confident that your organisation will be protected, able to detect, defend or respond to an attack effectively. Identifying vulnerabilities in your computer systems is essential to your organisation's security - our Penetration Testing Service provides you with a realistic understanding of the security issues you may face.

how it works

Our Penetration Testing service take a deep dive into your systems to uncover any issues, vulnerabilities and test how effective your security solutions would be against a cyberattack. Penetration testing, also known as Pen testing or ethical hacking, is an authorised simulated cyberattack on your IT infrastructure which we use it to evaluate the security of your networks and applications and look for weaknesses. We will analyse the current security level of your IT infrastructure, discovering where the gaps are and how it could potentially impact your organisation. Our experts will then provide a report of the findings with recommendations for improvements.

key benefits

Best Practice

Our Penetration Testing configures your security controls in accordance with best practices so you can gain confidence knowing that there will b no common or publicly known vulnerabilities at the time of testing.

Cost savings

By utilising our Penetration Testing service you can help prevent a breach before it's even happened saving your organisation the cost of recovering from a data breach.

Compliance

Our service will analyse your current security regulations and advise on where the improvements can be made to ensure your organisation is fully compliant with leading security standards.

Expertise

Our specialist teams have a broad understanding of a cyber criminal's strategies, tactics, tools and motivations allowing them to keep your IT infrastructure fully protected with their in-depth knowledge.

features

Vulnerability Assessment
We will identify and assess vulnerabilities within your organisation's IT infrastructure, including networks, applications, and systems.

Exploitation
Our team of experts will actively attempting to exploit identified vulnerabilities to determine the extent of potential damage or unauthorised access an attacker could achieve.

Risk Analysis
We will evaluate the potential impact and likelihood of successful exploitation of vulnerabilities, prioritising them based on the level of risk they pose to your organisation.

Reporting
Our team will also provide detailed reports outlining discovered vulnerabilities, potential risks, and recommendations for remediation to improve your overall security posture.

Compliance Validation
Our Penetration Testing service ensures compliance with industry standards, regulations, and best practices by assessing yout organisation's security controls and identifying any gaps that need to be addressed.

Social Engineering Testing
We will assess the susceptibility of your employees to social engineering attacks, such as phishing or pretexting, to evaluate the effectiveness of security awareness training and policies.

Post-Exploitation Analysis
Once completed, our team of experts will conduct thorough analysis after successful exploitation to understand the attacker's potential actions, identify any additional vulnerabilities exploited during the test, and recommend appropriate remediation measures.

why you need it

- You want to ensure your IT environment is secure and protected.
- You are looking to test your current security tools for your organisation to determine the correct ones.
- You're looking to leverage some expert advice from experienced professionals for future security enhancements.
- You want to be confident that your organisation can detect, defend, and respond to cyber attacks effectively.
- You are worried about vulnerabilities in your IT infrastructure.

other useful services

Cyber Security Operations Centre (CSOC) Services
Monitoring and scanning your systems to identify suspicious activity using the most up to date tools & industry experts for your maximised protection.

Cyber Security Awareness Training Services
Educating your employees on cyber security, how to stay vigilant against cyber threats and warning signs/risks of potential cyber-attacks.

Dark Web Monitoring Services
Continuous monitoring of the Dark Web to ensure your business' credentials are safe from cyber threats whilst letting you know which credentials have been compromised.

aztechit.co.uk
info@aztechit.co.uk
0330 0949 420