Means Business

Datasheet

Our Network Vulnerability Assessment services

Our team of ethical hackers can identify security vulnerabilities within your network infrastructure before the cyber criminals do and provide valuable remediation advise.

Safeguarding your network infrastructure with ethical hacking can improve your security posture.

Your organisation faces complex challenges every day. Keeping focused on business objectives whenever and wherever you are across the globe requires a secure network infrastructure to support you.

Exciting new ways of working and new channels to market mean the company board are delighted, but will security be an enabler to this strategy? How vulnerable is your business today and into the future?

Is it a straightforward process to find weak spots in your business-critical systems, procedures, policies and behaviours of your employees? Or does the news of a new piece of regulation or legislation mean significant work which will cost time and money and potentially introduce new security weaknesses?

What do you get out of this?

It's about ensuring proactive protection of your brand, reputation and valuable electronic assets around the clock worldwide.

Secondly, it's about having a clear view of your overall risk profile from any potential financial impact, or as loss of customer trust which is very hard to recover.

At an operational level, it's also about understanding the countermeasures and actions that you may need to take if your information or services were compromised, as well as about having full visibility of your own security estate, your service providers and the services they are managing.

All of these combine to better support your organisation's business strategy.

Assessing your network

We've developed a standard way of testing network infrastructures. It's based on advice from NIST (National Institute of Standards and Technology) and the PTES (Penetration Testing Execution Standard), the current thinking from tech forums and publications and our many years of experience.

Identifying vulnerabilities in your network infrastructure is key to keep your sensitive data secure and your reputation intact. If these vulnerabilities go unnoticed, you run the risk of compromise and impact to your reputation.

Our assessment is made up of a few different test phases, each helping to paint a better picture of the strength of your network infrastructure. Altogether, there are three phases.

1.We identify and map active devices

We will enumerate the devices and services available on the target network and determine the network architecture as well as security mechanisms that are used to protect your network resources. We'll also identify as much information about the target area as possible using various sources.

2. We scan your network for vulnerabilities

We'll focus on scanning devices determined during the first phase for potential vulnerabilities. We will test all TCP and UDP services to include all common services, such as HTTP(S), FTP, Telnet, Sendmail, DNS, SMTP, SNMP, etc. as well as all 65,535 TCP and UDP ports.

We'll check the following types of devices:

- Router(s), load balancers, proxy appliances and switches
- firewalls and/or other screening devices
- mail servers (SMTP, POP3 and IMAP)
- web, name and file servers
- desktops and network multifunctional devices
- network attached storage appliances
- IP cameras, DVR's and other video communication appliances
- WAN optimization and management appliances
- other IP connected systems which are identified during the testing.

Where applicable, bypassing segmentation controls may be used depending on the scope.

3. We check our results

We'll perform manual testing to validate whether a vulnerability is applicable to your network infrastructure and thus a threat to your business exists.

Exploitation of vulnerabilities

Once we've gone through the above phases and have an accurate picture of your network infrastructure and its security posture, our hackers can try to exploit the vulnerabilities they've found. Why? To show the business impact of having vulnerabilities in your network infrastructure.

This could include:

- getting access to certain systems by exploiting configuration or software issues
- escalating privileges, including the extraction of credentials
- evaluating any data from the attack (like social security numbers, personally identifiable information, bank account details, corporate information)
- investigating whether hacking tools can be uploaded and installed on the target host
- pivoting to understand the overall business impact of an exploited vulnerability.

Banking on trust

Over the next five years, our ethical hackers will be running assessments for a large bank with European headquarters. We're testing the systems that manage billions of euros every day, on a global and local scale.

It's so they can show their auditors they've carried out the right checks. And so they can show their customers that they're a trustworthy brand. The bank remains compliant and in control of their infrastructure and applications; they've got a lot of both, and they're often classified.

Why us?

We're experienced

In fact, we're one of the biggest security and business continuity practices in the world. We've got 3,600 security professionals working for us across the globe. And when it comes to ethical hacking, our team has more than 30 years' experience.

We operate across many industries, including industries that are significantly more advanced in dealing with cyber threats. This means we are ideally placed to bring expertise and know-how acquired with customers on the leading-edge of cyber security.

We're recommended

We're recognised as a Leader in ISG Provider Lens™ – Cyber Security – Solutions and Services 2024 in the UK. The report highlighted our strengths in managed security services, strategic security services, and technical security services in the UK.

BT has been named a Leader for the 20th consecutive year* in the 2024 in the Gartner Magic Quadrant™ for Global WAN Services based on its "Ability to Execute and Completeness of Vision".

*Magic Quadrant for Global WAN Services was previously named Magic Quadrant for Network Services, Global

We're qualified and security cleared

Our consultants hold industry certifications like CISSP, CISA, OSCE, and OSCP.

Where appropriate, our consultants possess national security clearance for delivery to government customers.

We're accredited for ISO27001:2013 covering our security testing services to both internal and external customers. Next to our ISO27001 accreditation we're also accredited for global consulting by Lloyd's Register Quality Assurance for the ISO9001 quality management system. We've held that since 2003 – proof of our long-term commitment to improving our services.

We have first-hand experience

As a large organisation, operating in around 180 countries, we know all about keeping our intellectual property, customers, people and premises safe.

We work hard to protect our networks, systems and applications – our ethical hackers and red team specialists test everything. Additionally, we work closely together with our blue team to test the effectiveness of our defences by carrying out multi-layered simulated attacks against both our physical and cyber security infrastructure.

This unrivalled experience, gained over many years of full spectrum testing of our policies, processes and defences, keeps our brand safe.

Find out more about ethical hacking

Learn more

Offices worldwide

JN: 1611673531 | November 2024.