WHO CAN YOU TRUST?

Ian Glover *explains why more firms are turning to penetration testing to check their defences and why you wouldn't want just anyone trying to break into your company*

In the last few years, we have experienced cyber crime on a scale never seen before. In May 2017, WannaCry and Petya became national news and marked a tipping point for many that believed they were immune to cyber attacks. This virulent outbreak of ransomware began to infect organisations across the world and within hours over 75,000 victims were reported in 90+ countries from telecommunications companies in Spain to a Russian ministry. In total, 200,000 organisations were affected in over 150 countries. In the UK, the NHS felt the full force of attack across 48 trusts in England.

Ransomware, as the names suggests, is a malicious program that locks a computer's files until a ransom is paid, usually in the form of an online currency such as Bitcoin. But WannaCry ransomware attacks were different from any outbreak previously seen, exploiting a vulnerability in the Microsoft Windows operating systems to spread to neighbouring computer systems over networks once it had infected its original host.

US Deputy Attorney General Rod Rosenstein speaks at a press conference about Chinese hacking at the Justice Department

Picture credit: Getty

While WannaCry and Petya delivered a serious wake-up call for many companies and organisations, they also reflected a general increase in more sophisticated cyber attacks, from hacktivist groups, organised criminal gangs and state-sponsored cyber terrorists. In addition, the rise of ransomware-as-a-service and the ability to purchase malware on the Dark Web has lowered the barrier to entry and made cyber crime accessible to anyone.

GROWING THREAT

Two years on from WannaCry, there has been a string of high-profile breaches from British Airways and Marriot Sherwood Hotels to Facebook and Google+. The result is that no sector or size of company can ignore these targeted or indiscriminate attacks. Investment in products to improve cyber defences has risen rapidly and most large firms have specialist security teams to be able to achieve the security basics very well. Emerging 'zero-hour' technologies and the use of artificial intelligence can detect and identify threats that traditional anti-virus and other security solutions may not find.

It is more important than ever that all businesses understand what data is attractive to an attacker and discover where their security weaknesses are so they can fix them before someone else finds and exploits them. The best way to discover where vulnerabilities lie is to simulate malicious attacks, from inside or outside of the organisation, in order to see how easy it is to break into a network or computer system and steal valuable data or deny access to critical assets.

This is called penetration testing and the demand for this very skilled, technical and clearly very sensitive investigation and analysis has seen a rapid rise in demand. While penetration testing has traditionally been associated with government organisations and large financial institutions and corporations, it is now commonplace among medium-sized companies, NGOs and the wider public sector.

> **THE CYBER SECURITY INCIDENT RESPONSE SCHEME FOCUSES ON APPROPRIATE ACTION**

Penetration testing is sensitive work and companies using in-house or external resources need to be clear who they are dealing with and have confidence that they are utilising skilled, knowledgeable and competent individuals working under appropriate processes and methodologies to protect data and integrity and not cause harm. There needs to be confidence and trust in the specialist companies that deliver these services, regarding how information and knowledge is handled and processed. It is a common misconception that the once named 'ethical hacking' security industry is simply made up of ex-criminal hackers who most organisations would be reluctant to trust.

That is why CREST was established in 2006 by the technical security industry. CREST is a not-for-profit body representing the technical information security industry that provides internationally recognised accreditation for organisations and certification of individuals providing penetration testing, cyber incident response, threat intelligence and Security Operations Centre (SOC) services.

Importantly, all CREST member companies undergo a stringent accreditation process every year and sign up to a strict and enforceable code of conduct and code of ethics. Linked to these trusted suppliers, CREST-certified individuals must pass the most challenging and rigorous examinations in the industry worldwide, to demonstrate the highest levels of knowledge, skill and competence. They must be able to stay one step ahead of the cyber criminals and be well versed in the tools and techniques used in the most sophisticated attacks.

For example, CREST Practitioner entry-level examinations are aimed at individuals with typically 2,500 hours of relevant and frequent experience, while candidates for CREST Registered Tester examinations should have at least 6,000 hours – three years or more – and at a certified level 10,000 plus. All these individuals have to re-sit the examinations every three years reflecting the fast-moving nature of the industry.

Organisations worldwide wishing to buy penetration testing services can now have the confidence that the work will be carried out by trusted companies with the appropriate policies, processes and procedures for the protection of client information, using qualified individuals with up-to-date experience and understanding of the latest vulnerabilities and techniques used by real attackers.

Another result of the rise in the threat of cyber attacks and breaches is the increase in regulated schemes designed to provide assurance that the technical controls in place are commensurate and proportionate to the level of risk.

WORKING WITH CNI PROVIDERS

For example, CREST works particularly closely with the UK's critical national infrastructure providers where cyber attacks could do the most damage – from energy and utilities companies to major financial institutions. Working alongside the Bank of England, Government and industry, CREST developed the CBEST framework to deliver controlled, bespoke, intelligence-led cyber security tests for the UK's most important financial institutions. Following on from this initiative, TBEST and GBEST schemes have been developed for UK telecommunications firms and Government bodies. A number of other Regulators in the UK are also starting to follow this model, while international demand for these types of service is increasing dramatically.

At the other end of the scale, it is clear that cyber criminals are turning their attention to small and mid-size companies – maybe because they are seen as 'low-hanging fruit'. CREST was instrumental in developing the technical assessment and certification framework for the UK Government's cyber security standards, Cyber Essentials and Cyber Essentials Plus. These set down baseline requirements for cyber hygiene and are now mandated for some Government contracts dealing with sensitive data.

The scheme provides organisations with clear guidance on implementation, as well as offering independent certification for those companies who want to demonstrate to their customers that their data is adequately protected and that they take cyber security seriously.

CREST accredits companies to deliver Cyber Essentials certifications and while Cyber Essentials will not stop the determined attacker, it has been shown that organisations with a basic level of cyber hygiene have not been affected by random attacks such as WannaCry.

Despite best endeavours, it is impossible to be 100 percent secure and if your business does fall victim to a malicious cyber security incident, your immediate task is to act as quickly as possible to limit the impact and damage. An Information Security Operations Centre (SOC) is often the first line of defence so there is an increasing demand to ensure that they are operating effectively.

THE ULTIMATE WAY TO DISCOVER WHERE ANY VULNERABILITIES LIE IS TO SIMULATE ATTACKS

The SOC is a facility where enterprise information systems – websites, applications, databases, data centres and servers, networks, desktops and other endpoints – are monitored, assessed and defended. Some companies and organisations run their own SOCs, while others outsource this function. Depending on the nature of the SOC, organisations may offer a variety of services including monitoring, detection, threat hunting, incident management, log analysis, forensic imaging, malware analysis, reverse engineering, mitigation advice and general good practice guidance.

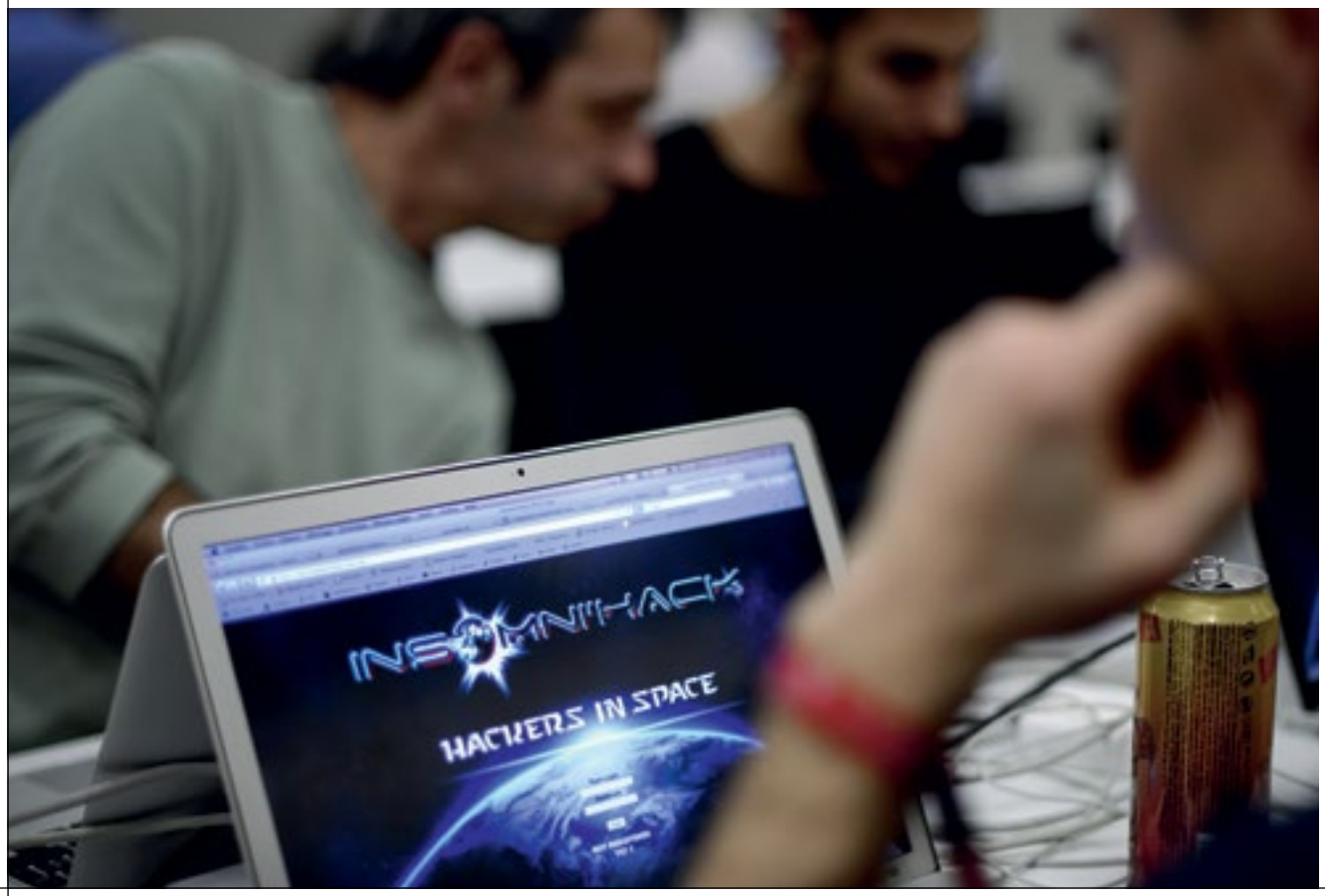
ASSESSING EFFECTIVENESS

The difficulty is how to assess if the SOC is operating effectively. It is impossible to assess capability based on marketing material and almost impossible to assess capability through a procurement process. To help to resolve this issue, CREST has worked with the suppliers, buyers and influencers to develop a SOC accreditation process. This includes procedural audits, physical audits and technical assessments. The SOC is the first line of defence and therefore it is essential that the capability is measured and reported.

If all else fails and a breach occurs, your company effectively becomes a crime scene and the requirement for evidential integrity and rigour can conflict with the need to resume business as usual, let alone budgetary and time constraints. The CREST Cyber Security Incident Response scheme focuses on appropriate standards for incident response to help companies have in place effective policies, processes and procedures to plan for, manage and recover from significant cyber security-related incidents. Where there is a major risk of reputational damage in the aftermath of an attack, companies will want assurances that their data is not compromised.

As client organisations significantly improve the security of their networks, businesses must ensure they do not become the weak link in the protection of data. As we have seen, the results of a successful cyber attack can be devastating for business and individuals, so companies need a professional cyber security industry they can trust and rely on ●

Ian Glover has worked in information security for the last 36 years. As President of CREST he has been instrumental in many major UK Government and industry initiatives, while working with international governments and regulators to build CREST chapters in Singapore, Hong Kong, Malaysia, GCC, Australia and the USA.



Participants compete behind their computers during the ethical hacking contest Insomni'hack

Picture credit: Getty