COVER STORY

CYBERCRIME: TESTING TIMES

by Joyrene Thomas

Cybercrime is booming. Banks and financial services companies are targets for criminals following the money and for nation-state actors and others looking to destabilise financial infrastructure. Ethical hackers, sometimes known as penetration or pen testers, are tasked with finding vulnerabilities before the bad guys. So, how bad is it out there? And what can financial services companies do to protect themselves?

Speaking on condition of anonymity, one technical director at a cybersecurity firm claimed never to have met a client his testers could not 'own'. That is to say, break into from the outside and secure full administrator access, from knowing only the IP address.

Sometimes this was done from a coffeeshop across the street from the target. Other times it was done within five minutes of opening the laptop. My guys get very upset if they haven't broken into somewhere before 12 o'clock on the first day, he declared.

Once inside, the testers move across the network. E-mail servers yield much useful information: staff and customer data but also passwords, including to the company bank account. We could have logged in remotely and emptied the account. It is frightening what we see — and that is just with the financial services clients, he said. Welcome to the world of cyber insecurity.

THE STATE OF CYBER INSECURITY

Cyber attacks and data theft appeared within the top five risks by likelihood for the first time last year, according to the *World Economic Forum Global Risks Report 2018*. The frequency, severity and disruptive potential of cyber attacks is increasing.

Attacks against businesses have almost doubled in five years. Incidents that would once have been considered extraordinary are becoming commonplace. For example, distributed denial of service (DDoS) attacks overwhelm specific IP addresses or web services with fake traffic to knock them offline. Attacks using 100 gigabits per second were rare but increased by 140 percent in 2016 alone.

In addition to corporate targets, the Austrian parliament and more than a hundred government servers in Luxembourg were affected by DDoS attacks last year. Banks and financial services companies remain the most attractive targets. Attacks are capable of causing such serious material and reputational damage that many organisations choose to pay ransom demands.

The financial impact of cybersecurity incidents is considerable. Some of the largest costs in 2017 related to ransomware. Notable examples included the WannaCry attack, which affected

300,000 computers across 150 countries. And NotPetya which caused quarterly losses of $300 million for a number of affected businesses.

Every company is a digital company to a greater or lesser extent. Many run complex, software-intensive systems, so vulnerabilities are almost inevitable. Moreover, devices increasingly connect to the internet, sometimes by default.

"A lot of organisations, including banks, will buy coffee machines or kettles for the staff room. They are a point of attack because they come with smart features out-of-the-box," explains Luke Potter, cybersecurity practice director at SureCloud, a cybersecurity solutions provider.

"We've done work with banking and financial services clients, where we've demonstrated attacking the network through the smart TV. Or using the smart TV as a way to listen to conversations within the contact centre. Or compromising the wireless communications on people's headsets and listening to the customer service agents talking," says Potter.

Criminals are hacking bank systems but also their processes and staff. They use social media, recce bank staff and strike via the supply chain. CEO scams as a form of phishing or social engineering are a good example. According to FBI estimates, bogus instructions to transfer funds have affected 40,000 businesses worldwide at a cost of more than $5 billion in the three years to December 2016.

TESTING, TESTING 1, 2, 3

Organisations can protect themselves against these vulnerabilities, but they need to be aware of them. This is one of the main drivers for organisations to conduct penetration testing, or pen testing for short. Others include greater use of outsourced services and suppliers, changes to business processes, and the need to achieve regulatory compliance.

Pen testing is a way of evaluating the security of a computer system by simulating an attack. Testers use a variety of manual and automated techniques to attack a client's applications, infrastructure or both. They look to exploit known vulnerabilities, plus use their expertise to identify specific weaknesses or unknown vulnerabilities in a client's security arrangements.

"Banks and financial services companies invest heavily in protecting information. They invest in anti-virus, firewalls, people, patching systems and hardware to protect information. If you don't test the controls you are investing in, how do you know that they are working efficiently?" says Potter.

He uses the analogy of installing a smoke detector, but never testing that the battery is operational and the mains working. Pen testing helps ensure that security arrangements are working effectively; it should not be confused with a vulnerability scan.

This uses automated tools only to identify known vulnerabilities, check if security settings are activated and consistently applied, and patches deployed. It does not exploit the vulnerabilities to simulate an attack, or assess the overall security behind a system.

"A pen test should be 80-85 percent manual effort from a human testing systems. There will be a level of automation, but that should cover no more than ten percent of the test time," says Potter. "The automation gives the breadth and the manual testing gives the depth. It's the depth which you are paying for — the physical consultant and the expertise," he says.

ETHICAL HACKING

Pen testing is highly specialised, technical discipline. It is also human one, which is where ethics comes in. How do pen testing firms manage ethics in the course of business?

"All of my consultants are background checked. I would never employ a hacker — that's just not what we're about. We are genuinely on the side of the organisation," says Potter.

For Daniela Perlmutter, vice president of marketing at Israeli cyber security firm Cyberint, ethics is as much about what testers do as how they do it. "It's using ethical tools and not doing anything that is not legal, unapproved or unauthorised. When you do testing, a lot of information comes out — personal or process information on the bank and how they work. We don't share that."

It is a difficult line to tread, because ethics and what constitutes ethical conduct differs from person to person. "Ethics is a very broad subject and extremely difficult to define, particularly internationally," says Ian Glover, vice president, CREST, a not-for-profit body that represents the technical information security industry.

CREST overcomes this by working towards codes of conduct. "We look at the policies, processes and procedures, which companies submit and we audit. Companies and anybody doing this type of work signs up to adhere to them. Any deviation can be identified and we can take action," explains Glover. This may include removing companies from the register of CREST-accredited suppliers, precluding them from certain types of work and client engagements.

"We are trying to tie the elements of ethics that we think are important in the industry into our code of conduct, which makes them enforceable. A lot of ethical codes are if you call the industry into disrepute, we will take action. How can you measure that? You cannot really work to that and you certainly cannot internationalise it," says Glover.

CREST codifies specific examples of behaviour pertaining to ethical conduct. For example, the type of attack tools to be used; that vulnerabilities discovered during a contract must not be publicised or sold; that no research must be done on companies that have not requested or signed up to a contract.

HACKING BACK

It is a predicament though. Companies collectively spend billions on cybersecurity. Law enforcement agencies investigating digital crimes are overwhelmed. While ethical hackers follow the rules, black hat hackers do not. This has sparked renewed interest in 'hacking back', particularly in the US. Two US politicians have proposed draft legislation that would allow cyber victims to engage in active defence. That is to say, use limited defensive measures to monitor, identify and stop attackers.

Today such digital vigilantism would breach the Computer Fraud and Abuse Act (CFAA), which makes it illegal to access third party computers without authorisation. Companies and individuals may protect their computers and data only by taking measures within their own network. For example, installing anti-virus, using encryption or strong authentication, or monitoring unusual traffic patterns.

The Active Cyber Defence Certainty Act (ACDC) would enable authorised companies and individuals to go outside their own networks to establish attribution or disrupt an attack. They could also retrieve and destroy any files stolen during an attack and monitor attacker behaviour.

However, there is understandable nervousness around the proposals. It is a very slippery slope as attribution within cyberspace is so difficult.

There are so many false flags as attacks can be staged via remote servers and, in the case of DDoS attacks, via thousands of compromised computers and IoT devices. Who does a victim go after? How sure can they be about the identity of their attacker if they cannot trace messages back to their original source?

The ACDC only allows retaliatory action against computers based in US territory. This limits the scope of what is possible for victims. There are concerns that hacking back may lead to an escalation of online hostilities and collateral damage with uninvolved parties caught in the cross-fire.

Information security professionals also warn that the process of hacking back can in itself taint forensic evidence at the scene of the attack. If analysed properly, this could yield more valuable results than a retaliatory strike.

It is also a moot point that if a victim's cybersecurity posture was such that they were attacked in the first place, what are their chances in hacking back against an attacker who is better armed, trained and may be expecting them?

PUTTING IT RIGHT

Cybersecurity evolves with cyberthreats. Initially the focus was securing an organisation and its data from the outside in. When it became increasingly unlikely that perimeter controls alone could prevent all attackers all of the time, focus shifted to defence in depth. This used several independent controls to offer protection greater than the sum of its parts. Thinking has now moved towards a defence in breadth approach, which builds a systemic fabric of protection by integrating various controls across a platform.

These shifts in focus also reflect greater pragmatism in how to deploy both technical and human resources. When being breached is the new normal, companies must move from prevention to building resilience to mitigate risk. This involves building up detection, response and recovery controls. These include technical controls, naturally, but also procedural and human controls.

Awareness is the first step for banks and financial institutions in protecting themselves, according to Perlmutter from Cyberint. Then comes employee training and ensuring that the right mechanisms are in place to detect and identify threats. Processes, such as immediate response and mitigation plans if there is a compromise, are critical, she says. Similarly, continuous detection using various tools and models, which are also integrated with others to identify when a threat is imminent.

There are no silver bullets in the fight against cybercrime — there never are with security. It may be unglamorous and unsung, but business-as-usual security is bedrock of any effective security approach. "It all boils down to the same things that the industry has been saying for a while now. It's all down to people, processes and technology. If you focus on those, then you can start to identify, detect and respond quicker," says Elad Ben Meir, vice president, strategic accounts, Cyberint.

That notwithstanding, pen testing is evolving in line with cyberthreats. Firstly, is the attempt to automate simulated attacks against corporate networks or staff to validate the organisation. These attacks are increasingly informed by threat intelligence and are continuous. Pen testing should no longer be regarded as an annual exercise, rather as an ongoing activity when things change within the business and externally in the threat landscape.

Secondly, the next generation for pen testing is to run red team and blue team activities — what the industry now calls purple teaming to test the defenders and as well as defensive measures (see box). This does not stop at penetrating the network. It expands to getting at the organisation's crown jewels and testing how quickly it responds to an attack. After all, next time it may not be a test.

HACKING IN COLOUR

'Hacking' tends to be a word associated with illegal activity. But it actually means understanding something, breaking it down and finding out how it works. The original hackers were those who delighted in having an intimate understanding of the workings of computers and networks.

The information security industry has colour-coded hackers and hacking behaviour for ease of reference.

Black hat hackers violate computer security or act illegally for personal gain or maliciousness. For example, stealing card or personal data or performing DDoS attacks.

White hats also known as ethical hackers, use their abilities for good and legal purposes. They are employed within the legitimate cybersecurity industry.

Grey hats fall somewhere in between. They may not look to benefit financially or cause disruption, but may access systems without permission or sometimes behave illegally or unethically.

This terminology is said to come from American westerns, where black and white attire denotes the villains and the heroes among cowboys. The same three colours are used to describe styles of penetration testing.

Black box is where no information is provided to the tester. External attacks are simulated with no prior knowledge of the target environment to understand what an uninformed attacker can achieve.

White box is where full information is provided, e.g. network maps and access to client staff. This supports a targeted test on a particular application or system from many angles.

Grey box is where limited information is provided, e.g. system logins or visitor access to a building. This evaluates the possible damage someone with some knowledge and access can do.

US military terminology has been adopted to describe types of penetration testing.

Red teaming simulates attacks to test an organisation's information security.

Blue teaming designs defence measures against such red team activities.

Purple teaming has been added by the information security industry, which essentially helps blue team defenders get the most out of a red team or pen test exercise.