economia

http://economia.icaew.com/business/october-2016/cyber-threats-ghost-in-the-machine

Cyber threats: ghost in the machine

06/10/16

06 October 2016 Comments (0)

It takes more than a firewall to stop a virtual virus these days, so what can you do and are the solutions effective? Manek Dubash looks at how firms can protect their business from the latest threats to their IT systems

There can be no doubt that the numbers and scope of threats to the privacy of information belonging to organisations and individuals across the globe are increasing. As the European Union Agency For Network and Information Security (ENISA) notes in its report, Information security and privacy standards for SMEs, a fast-growing and increasingly complex cyber-threat landscape poses a greater risk than ever. Those vulnerable to attack include organisations of all types and sizes, according to ENISA.

The threat landscape

Bob Anderson is managing director of security firm Navigant, and prior to that, executive assistant director of the FBI's Criminal, Cyber, Response and Services Branch.

He describes the threat landscape as sophisticated, with a wide range of attacks, origins, and targets. Hackers' motives are primarily financial so, for example, they will mount distributed denial of service (DDoS) attacks that cut the organisation off from its customers and the rest of the world by flooding its servers with heavy bursts of data, with the aim of extracting a ransom in return for halting the attack.

> Many companies dedicate lots of money to IT infrastructure – they have anti-malware software installed, and some monitor endpoints, but that's not the way to go now
>
> *Bob Anderson, managing director of security firm Navigant*

Similar motives lie behind hackers who threaten to expose stolen customer databases and other sensitive information. They inveigle malware into a company's systems. It then sits dormant, monitoring transactions and acquiring credentials, and forwarding the data on to the hackers. While detailed specifics are understandably hard to come by – hacked companies tend to be reticent – security vendors say they are seeing growing numbers of customers who just pay up in order to avoid the business being seriously damaged. These types of attacks seem likely only to increase, given their profitability.

The vector, or route, into the organisation varies. Threats can come from not just disgruntled employees, but, for example, smartphones, laptops, USB memory sticks, social media and malware-laden emails and infected web pages. As businesses move their data into the cloud, this potentially exposes them to further attacks. As IT industry analyst Nikhil

Batra said at a recent NetEvents conference: “Security is moving away from the perimeter. It’s moving into the cloud and there’s a much larger number of devices, networks and cloud servers that we need to protect.”

Examples of such attacks include spear-phishing, which is a digital con game using a spoofed web page or email to persuade victims to enter sensitive information such as bank authentication details. These are then captured and money stolen.

Whaling is a more targeted form of spear-phishing, involving the targeting of C-level executives, using content resembling a subpoena, customer complaint, or other executive issue. Whaling works, too. In 2008, 20,000 CEOs were attacked using a spoofed FBI subpoena, 10% of whom downloaded and installed malware that pretended to be software required for viewing the document. In fact, it was a keylogger that captured passwords, and resulted in further attacks on those 2,000 individuals. According to the FT, $800m was stolen using whaling attacks in the six months to March 2016.

What can you do?

All is not doom and gloom. Anderson says that globally, banking and accounting firms tend to be better prepared. This is not just because financial institutions have – in the main – been in the front line of cutting-edge cyber-attacks, but also because the regulatory regimes under which they operate mandate information protection. Note that the regulatory regime is about to change.

However, ENISA research has found that although small to medium-sized businesses – which means most companies – are slowly becoming aware of both the potential impact of such business disruption and of how security management can protect them, only 49% of those surveyed by the UK government in 2015 had conducted a risk assessment in the previous year.

So there is no room for complacency. Anderson agrees that many organisations are poorly prepared: “Many companies dedicate lots of money to IT infrastructure – they have anti-malware software installed, and some monitor endpoints, but that’s not the way to go now,” he says. “Rather, you need to look at your infrastructure and the business and match it to the adversary.”

What does this mean? From a conceptual perspective, a traditional view of security has been likened to a chocolate-covered marshmallow: crunchy on the outside, soft on the inside. In other words, defences such as a firewall were set up at the perimeter, but little else prevented hacks once the attacker breached the firewall.

ICAEW’s advice on GDPR

While the commercial consequences of a data breach can be disastrous, the regulatory authorities are slowly catching up. The EU’s General Data Protection Regulation (GDPR) is due to come into effect in May 2018 and aims to help simplify cross-EU working by harmonising data protection regulation.

Kirstin Gillon, technical manager at ICAEW’s IT Faculty, says: “GDPR represents a step change in the requirements for businesses around personal data, and there are many positive aspects. It aims to provide consistency in approach to personal data across the EU, which will be helpful to multinational businesses in particular. It incorporates a number of leading practices, such as privacy-by-design, which will encourage a more proactive approach to the use and security of personal data. The increased level of fine and breach reporting will also focus boards’ minds on the issues.

“However, a lot still depends on how it is implemented in practice, particularly in areas such as breach reporting. In the UK, the Information Commissioner’s Office is still developing a lot of the detailed requirements, and effectiveness will depend a lot on that work.

“While some large businesses have been preparing for a while, most businesses still have a long way to go to comply with some
of the requirements. Part of the difficulty has been that the regulation has been under negotiation for a long time and the specific requirements have only recently become clear.

“However, we urge businesses to look at the new requirements and consider what they need to do in order to be compliant by 2018.

“Even though this is a piece of EU legislation and therefore could be impacted by the Brexit vote, at the very least, businesses who hold any data regarding EU citizens will be required to comply. The current expectation from bodies such as the ICO, though, is that the UK will enact very similar legislation, regardless of the formal position with the EU.

ICAEW has a helpsheet, and other resources, which can help our members get up to speed (icaew.com/cyber).

Today’s threat landscape means this is no longer a tenable model.

A modern security model deploys defences throughout the organisation, on every endpoint, and mandates a regime of constant vigilance, according to Anderson. “You need to put together an adequate security infrastructure that you’re monitoring constantly, because they [attackers] are always refining their attacks,” he says.

“If you let it stagnate for even six months, with crypto-locker [ransomware] and APT [advanced persistent attacks], you get behind the curve. Those who do it well are constantly reviewing their systems. It’s like deciding whether to bring a knife or a sword to a fight – you need the right weapon.”

However, technology alone cannot keep a company secure. It needs awareness and education across the organisation. As we have seen from the success of whaling and spear-phishing, people remain the weakest link.

One thing that most security technology vendors will agree on is that the attackers are one step ahead almost every time. However, security technology is evolving.

Most security technologies use a form of pattern recognition, or signatures, of previously-captured malware, but this leaves an opening for developers of new malware – which is why malware constantly evolves. Some companies, though, are trumpeting new ways of being smarter about catching fresh malware, such as those who use what they describe as artificial intelligence running in the cloud.

Every cloud...

Bryan Gale, VP of marketing at Cylance says: “We don’t use signatures, we don’t use a DAT file, we don’t require system scanning. Everything we do is based on machine learning and artificial intelligence. We use Amazon’s cloud, a massive computer cluster, to essentially train our machine learning models.”

An alternative to keeping up by buying technology is to rent it from cloud-based security service providers. They can draw on expertise that few SMEs could afford by exploiting their economies of scale. Frank Wiener, VP of marketing at Wedge Networks says: “What we’re seeing is a tremendous initiative by service providers who ... offer security at that cloud layer of the network as a service for both large enterprises, but primarily small and medium-sized enterprises who lack the sophistication and the resources to do that on their own.”

Manek Dubash