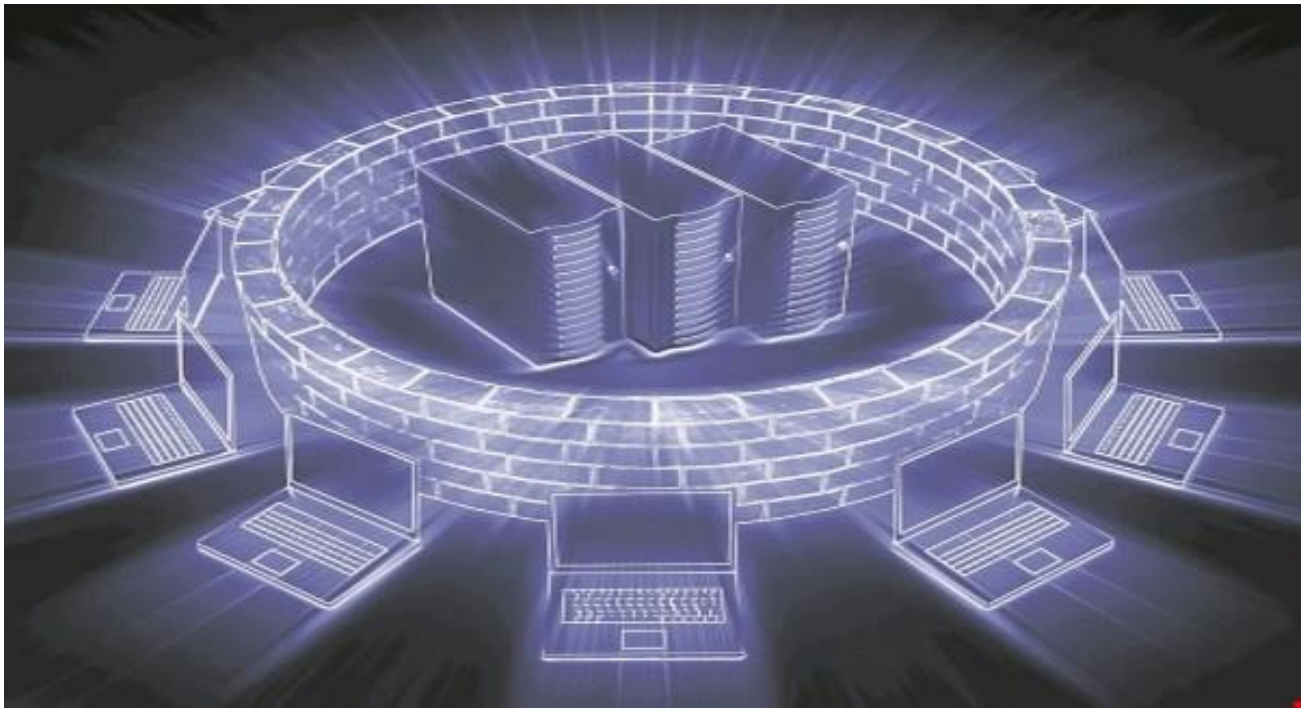
Putting up a cyberwall is not enough anymore

Friday, November 13, 2015
by Bob Griffin

Changes in attack strategies and regulatory policies mean that Irish businesses need to build a process-based cyberdefence that pays attention to changing threats, writes **Bob Griffin**.



The EU Court of Justice issued a landmark ruling last month, declaring the US Safe Harbour provision set up by the European Commission 15 years ago — which oversees the transfer of personal data between EU member states and the US — invalid due to surveillance of European citizens by American intelligence agencies.

The decision has resulted in a great deal of uncertainty regarding the transfer of data between the two. One implication of the decision is clear: It points up a fundamental shift in perspective regarding cybersecurity strategy.

For many years, cybersecurity has been regarded as a simple rote application of technologies like anti-virus, firewalls, intrusion detection systems, and so on. Meanwhile, attackers have shifted to a focus on users, rather than technology, as the weak link in cyber-security.

RSA recently published joint research performed with the Information Systems Audit and Control Association on the current state of cybersecurity that sheds important light on the dangers of social engineering attacks.

The report provides the results of a survey of cybersecurity professionals, conducted in the first quarter of 2015, showing that phishing and other kinds of social engineering attacks targeting users were the most common attacks within enterprises in 2014, with nearly 70% of respondents citing phishing as having resulted in exploits in the enterprise, and 50% citing other social engineering attacks.

Research by Intel shows more than eight in 10 Irish businesses have been targeted by cybercriminals in the last 12 months. Further research by William Fry shows 81% of Irish businesses experienced an attack in the last year, while just under half (46%) of these attacks took over four months to be detected.

And it's not just businesses. According to recent data from Eurobarometer, Irish people aren't doing enough to protect themselves online. More than half (57%) of Irish people admit to opening emails from people they don't know — and many will go on to download and open seemingly harmless email attachments that execute malware and infect their devices. Other findings include:

- 75% use the same password across different sites and online services;
- 26% regularly change their passwords;
- 7% have been the victim of a particularly sinister type of malware, called "ransomware", which can permanently lock down a computer's hard-drive unless a ransom is paid to a criminal racket.

These changes in attack strategies and regulatory policies mean Irish businesses in particular need to build a process-based cyberdefence that pays attention to the changing face of cyberthreats and regulatory issues. This "advanced cyberdefence" combines effective governance and intelligence-driven security solutions.

To start, a company needs to understand the potential for attackers to exploit the vulnerability of its users, the interest of attackers in taking advantage of that potential and the impact that such an attack could have. Indeed, cyberattacks are more a case of when, not if. Having the right defensive tools, and the right organisational protocols in place, can be the difference between a glancing blow and a devastating breach.

Companies need to think beyond traditional cyberdefence tools. For organisations that deal in e-commerce and sensitive data, like customer information, reliance on a standard anti-virus suite is not enough. Using intelligence-driven security software, on the other hand, provides a proactive line of defence against attack.

Think of a traditional anti-virus as a perimeter wall. For determined hackers, this wall can be scaled easily, often before anyone notices. An intelligence-driven security solution, the kind we pioneer at RSA, is more like a patrolling sentinel, actively checking for intrusions and questioning those who seem suspicious.

If I'm a hacker somewhere in South America trying to access a company's server in Dublin using stolen credentials, an intelligence-driven security solution would analyse my location, credentials, and computer, in addition to other variables, to check my identity.

For someone who's not who they're pretending to be, passing through this gauntlet of checks is extremely difficult and thus, access to private information is denied. In general, these

intelligent solutions can be scaled to fit a firm's specific data protection and security policies, making them agile and flexible.

But a company's cybersecurity cannot depend entirely on technology. Effective governance and "security hygiene" among all staff, not just the IT department, is vital to protect assets.

This can be as straightforward as a company-wide training day on the importance of updating software when prompted, creating strong, unique passwords and deleting unsolicited emails with suspicious attachments.

Companies must also put in place a defined structure and hierarchy to deal with security breaches quickly and effectively. This "critical incident response team" must know how to act, who to contact, and which assets to secure in a time of crisis.

As the Court of Justice ruling shows, it's difficult to find a safe harbour in the storm of cyberattacks, but there are ways to protect against damage and mitigate risk. An advanced cyberdefence policy combines intelligent technology with sensible, proactive governance, and it's an essential strategy for Irish companies to safeguard data. Often, security breaches can be found and fixed in a short space of time, but they can have long-term, sometimes permanent, effects on a business's reputation and viability.

Robert Griffin is chief security architect at RSA, the security division of EMC