Security predictions for 2013

As you round out your 2013 business and IT plans, cybercriminals are resolving to implement increasingly sophisticated threats targeting specific computer systems and organisations big and small.

By Doros Hadjizenonos 13 Feb 2013

Last year, businesses suffered from several serious hacks and breaches. As the arms race between attackers and businesses continues to evolve in 2013, IT departments and security professionals will need to stay on top of the changing tactics and approaches used by criminal hackers in order to protect their organisations.

Here's our take on what security threats and trends we expect to see in 2013:

Threat 1: Social engineering

This begins with focusing on a tried-and-true black-hat tactic in both the physical and digital worlds - social engineering. Before the computer age, this meant sneaking one's way past a company's defences with the gift of gab as opposed to a cleverly worded email. Now, social engineering has moved on to social networks, including Facebook and LinkedIn.

Attackers are increasing their use of social engineering, which goes beyond calling targeted employees and trying to trick them into giving up information. In years past, they might call a receptionist and ask to be transferred to a targeted employ so that the call appears to be coming from within the enterprise if caller ID is being used. However, such tactics aren't needed if the details the cybercriminal is looking for are already posted on social networks. After all, social networks are about connecting people and a convincing-looking profile of a company or person followed by a friend or connection requ can be enough to get a social engineering scam rolling.

Threat 2: APTs

Being aware of social engineering is important, of course, because it can be the precursor for a sophisticated attack mea to breach the wall of your organisation. This year had a number of high-profile attacks (think: Gauss and Flame) targeting both corporations and governments. These attacks are known as Advanced Persistent Threats (APTs). They are highly sophisticated and carefully constructed. The intention behind APT attacks is to gain access to a network and steal information quietly. They take a low-and-slow approach that often makes them difficult to detect, giving them a high likelihc of success.

Additionally, APTs need not always target well-known programs, such as Microsoft Word; they may also target other vecto such as embedded systems. In a world in which a growing number of devices have Internet protocol addresses, building security into these systems has never been more important.

APTs will continue as governments and other well-funded organisations look to cyberspace to conduct their espionage. In fact, APT attacks are running as we speak, so look out for those anomalies in your network traffic.

Threat 3: Internal threats

But some of the most dangerous attacks come from the inside. These attacks can be the most devastating, due to the amc of damage privileged users can do and the data they can access. In a study funded by the US Department of Homeland Security, the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute and the US Secre Service, researchers found that malicious insiders within the financial industry typically get away with their fraud for nearl 32 months before being detected. Trust, as they say, is a precious commodity - but too much trust can leave you vulnerat

Threat 4: BYOD

The issue of trust comes into play in the mobile world as well, with many businesses struggling to come up with the right m of technologies and policies to hop aboard the bring-your-own-device (BYOD) trend. Users are increasingly using their devices as they would their PCs and, by doing so, are opening themselves up to web-based attacks the same as they wou if they were operating a desktop computer.

For attackers, it is likely as well that there will be more attempts to circumvent the app review and detection mechanisms th mobile vendors use to guard their app markets. All this means that the flood of iPhones, Google Android phones and other devices making their way into the workplace are opening up another potential gateway for attackers that needs to be secured. Think about it - your smartphone has a camera. It has a microphone. It can record conversations. Add these features to the ability to access your corporate network and you have the ideal stepladder to climb the walls we are talking about.

Threat 5: Cloud security

BYOD is not the only thing changing the walls that corporations must build around critical data, however. There is also a lit trend called cloud computing. With more companies putting more information in public cloud services, those services become juicy targets and can represent a single point of failure for the enterprise. For businesses, this means that securit must continue to be an important part of the conversation that they have with cloud providers, and the needs of the busine should be made clear.

Threat 6: HTML5

Just as the adoption of cloud computing has changed the vulnerability surface, so will the adoption of HTML5. Earlier this year, it was noted at the Black Hat conference, a place where security pros can get a sign of attacks to come, that HTML5 cross-platform support and integration of various technologies opens up new possibilities for attack, such as abusing Web Worker functionality. Even with an increasing amount of attention being paid to HTML5 security, the newness of it means that developers are bound to make mistakes as they use it, and attackers will look to take advantage. So, expect to see a surge in HTML 5-oriented attacks next year, hopefully followed by a gradual decline as security improves over time.

Threat 7: Botnets

But even though the arms race between researchers and attackers favours innovation; expect cybercriminals to spend a lo of time perfecting what they know best, such as making sure that their botnets have high availability and are distributed. While the legal takedowns being launched by companies such as Microsoft succeeded in temporarily disrupting spam and malware operations, it is naïve to assume that attackers aren't taking what they have learned from those takedowns and us it to shore up their operations. Botnets are here to stay.

Threat 8: Precision-targeted malware

Attackers are also learning from the steps that researchers are taking to analyse their malware, and techniques were recently demonstrated that can help render analysis ineffective by designing malware that will fail to execute correctly on a environment other than the one originally targeted. Examples of these attacks include Flashback and Gauss. Both have be successful, especially Gauss, at stopping researchers from automated malware analysis. In the coming year, attackers wi continue to improve and implement these techniques and make their malware more dedicated so that it only attacks computers with a specific configuration.

One thing is for certain - 2013 is sure to bring an army of exploits and malware through vectors ranging from social netwo to mobile devices to employees themselves. As computer and operating system security continues to improve, so will cybercriminals' new techniques to bypass these defences. All the more reason to make security one resolution we keep.

ABOUT THE AUTHOR

Doros Hadjizenonos is the South Africa sales manager of Check Point Software Technologies.