

21.12.2011. – SC Magazine UK

2012: security predictions for the future of mobile, cloud, attacks, data loss and big data

Over the past few weeks I have been inundated with 'predictions' for what 2012 will bring to the security market.

I really have to take these predictions with a pinch of salt as all trends can be predicted, but headlines cannot. Looking back at the article I wrote last year, it could be argued that the mobile threat came true, as did the consumerisation of IT, but we didn't hear much about advanced biometrics. Hackers were caught and arrested as cyber crime became more industrialised, there was some advanced malware, and the launch of Google+ ticked the box for social networking.

So to do kind of a summary of the 20,000-plus words I have received from security vendors and analysts, let's start with the main trend: mobile. Analyst Ovum claims that smartphones and tablet computers will continue to be deployed by the enterprise for specific roles, particularly for customer-facing staff in service industries.

Imation Mobile Security claims that the bring your own device (BYOD) policy will grow in popularity in the workplace, but at the same time create potential compatibility headaches for the IT department and increase the need for tracking capabilities and usage metrics.

Melvyn Wray, SV-P of product marketing EMEA at Allied Telesis, agreed that there will be a shift towards BYOD policies, as network staff will look to reduce maintenance issues by encouraging commoditisation of the network, whereby network staff will encourage employees to self-regulate their equipment to access the network.

According to PandaLabs, 2012 will bring attacks on the Android platform on a small scale, but tablets will be soon targeted by the same malware as that for smartphone platforms. In addition, it said tablets could draw a special interest from cyber criminals as people are using them for an increasing number of activities and they are more likely to store sensitive data on them than they are on a smartphone.

Among a stack of predictions from Lookout Mobile Security were new methods of malware 'monetisation', including mobile pickpocketing with SMS/call fraud via malicious applications, an emergence of and increase in mobile botnets, malvertising via in-application adverts, and mobile fraud through web-based distribution such as email, text messages and fraudulent websites.

FortiGuard Labs at Fortinet believed that new worms and polymorphism would emerge in mobile malware, along with ransomware (where an infection holds a device 'hostage' until a ransom payment is delivered).

Eddy Willems, security evangelist at G Data, said: "2012 is not just going to see an increase in mobile malware, but will also witness new types of mobile malware entering the space. We must remember that mobile malware requires a new and different business

model to traditional malware, and perpetrators are still experimenting with it; there is a lot more room for creativity.

“Cyber criminals have been mainly using backdoors, spy programs and expensive SMS services, but 2012 will bring more additions to this list. As cyber criminals become more knowledgeable and confident, mobile botnets are one type of attack we predict gaining popularity, especially because they can be used as a tool to obfuscate the source of an infection and keep the criminals 'safe'.”

No doubt there are plenty of challenges there, but what about another trend that has hung around security for a few years now: cloud. It has long been the discussion point on its security, but is that conversation over? If so, what will be the next key points?

James Lyne, director of technology strategy at Sophos, told SC Magazine that people will get over the fear, uncertainty and doubt around cloud, and 2012 will be about protecting data on systems that one has no control over. He predicted a focus on cloud to see legal and IT combine to work with new concepts.

Patrick Graf, general manager at NCP engineering, told SC Magazine that everyone is talking about cloud but most people do not understand what it means; yet it will be especially beneficial for those companies without a specific IT department. “If you integrate processes into the cloud then everything makes sense,” he said.

Ovum said 2012 will be the year of Platform-as-a-Service (PaaS), where organisations' approach to cloud will shift from a low-level Infrastructure-as-a-Service/cost-cutting discussion to a higher-level one.

Denis Martin, CTO at NaviSite, predicted the cloud will transform disaster recovery services by extending disaster recovery options that yield significant cost savings and flexibility for businesses. He said cloud-based Recovery-as-a-Service (RaaS) will include the ability to completely replicate virtual environments in multiple data centres worldwide.

He also predicted that organisations will move toward cloud-based security in order to enable the cloud environment to grow through compliance at the same rate as business growth. Finally, he believed that 2012 will be the year that IT moves to the cloud as the core delivery for key in-house applications, rather than infrastructure augmentation.

Echoing comments made by LogLogic CEO Guy Churchward this week, WatchGuard predicted that a major cloud provider will suffer a significant security breach as organised criminals will target cloud services and "significantly breach" at least one well-known firm.

It also said to expect smarter, trustworthy cloud providers recognise the risks and add premium security to their offerings.

Andrew Wild, chief security officer at Qualys, said cloud services are maturing to the point where security can be reliably deployed and implemented to protect both the devices and the networks they are connecting to.

Elsewhere, Webroot predicted that the masses will migrate to cloud platforms due to the launch of iCloud, as the appeal of file sharing and remote access will be a major draw for an increasingly tech-savvy population that connects to the internet from tablets, smartphones and multiple PCs.

Mak Seager, vice-president of technology EMEA at Informatica, believed that 2012 will feature an upturn in cloud adoption as it is driven by the need for organisations to be more agile, as well as the need to cut costs.

However, Richard Moulds, V-P of product strategy at Thales e-Security, said enthusiasm for the cloud will wane if companies are concerned about placing sensitive information in it, so greater understanding of what is sensitive is needed.

He also believed that the cloud and compliance are on a collision course; as, if a cloud computing vendor houses regulated data, that vendor is now part of the scope of a compliance audit. "Given how multi-tenancy works, the provider will not be able to know what part of their infrastructure touched the regulated data," he said.

Trend Micro said the real challenge for data centre owners will be dealing with the increasing complexities of securing physical, virtual and cloud-based systems. It said that while attacks specifically targeting virtual machines (VMs) and cloud computing services remain a possibility, attackers will find no immediate need to resort to these because conventional targeted attacks will remain effective in these new environments.

So with that, let's pick another trend: attacks. Targeted or untargeted, what's your flavour?

Imation Mobile Security said financial services will be hit by an increase in malicious attacks and internet threats as these become more sophisticated, while Raj Samani, CEO EMEA at McAfee, predicted that attacks will become more complex along with an increase in the volume of threats in 2012.

"It's the complexity of attacks that will astound the industry. The high levels of malware produced every day can obscure its sophistication – which lies buried beneath the big numbers. Cyber crime will track our own use of technology, hence the recent rise in mobile malware. This is set to continue in 2012," he said.

WatchGuard said it expects geolocation data to be used to customise attacks, while it also expects an attack against physical infrastructure or equipment that will have a significant repercussion.

It also said that it expects organised criminals to leverage advanced malware techniques in targeted attacks against businesses as advanced persistent threats (APT) to create more advanced malware targeting smaller businesses and even consumers.

Peter Davin, CEO of Cryptzone, said that following targeted attacks in 2011, the trend will continue and, rather than hackers attacking randomly, they will have specific targets, whether political or personal. He said attacks against well-known brands will become more common as unsuspecting recipients are sent malicious emails containing hostile code.

Ash Patel, country manager for UK and Ireland at Stonesoft, said: "In 2012, I believe that we will hear a lot more about APTs and advanced malware. Using the term 'APT' alone gives little or no information as to what the problem is/was, and I believe further details will be given on these types of attacks.

"Both the media and vendors will begin to communicate more information about the actual type of hacking method, such as advanced evasion techniques. I also feel that DDoS attacks will continue to be a major problem. Furthermore, I feel we will hear a lot more about 'state on state' hacking."

FortiGuard Labs predicted that there will be an increase in 'Crime-as-a-Service' (CaaS), where criminal syndicates will offer illegal and detrimental services; instead of hiring a CaaS outfit for blanket attacks, they will provide more strategic and targeted attacks on companies and individuals. It also believed that more hacktivist groups will come to the fore in 2012, as LulzSec did in 2011.

Imperva believed that DDoS attacks will increase in sophistication and effectiveness by shifting from the network level to the application level, and even to business-logic-level attacks.

In agreement was Bradley Anstis, vice-president of technical strategy at M86 Security, who said targeted attacks will become more complex and public, similar to those against Sony and RSA. "Cyber criminals will exploit stolen digital certificates and use zero-day and multi-stage attacks to infiltrate organisations and access personal, corporate and, in some cases, classified government information," he said.

However, Andrew Wild at Qualys said it was his "fervent hope" that in 2012, organisations will realise that APT prevention products are simply the latest 'silver bullet solution', as most such attacks (RSA, Sony, Epsilon) were caused by human failings; if your organisation wants to protect itself against APTs in 2012, he said, then you need to design and implement a serious user education programme, deploy patches and upgrades in a more timely fashion, and consider outsourcing at least some elements of your security infrastructure.

He said: "In an ideal world, much of the above would become part of compliance requirements (especially the user education part) and APT will go the way of many other announcements before it and never be heard of again. We can all live in hope; just remember that hope is not a security strategy."

This year featured the Information Commissioner's Office (ICO) dishing out a number of fines, and next year it will enforce new rules on cookies. So here's another trend: data loss and breaches.

Many predicted that the number of data breaches will continue to rise in 2012, while Trend Micro said more hacker groups and the social networking generation will pose a bigger threat to organisations that protect highly sensitive data. It also predicted that more high-profile data loss incidents will occur via malware infection and hacking.

Tony Dyhouse of the ICT KTN said he had no reason to believe that the number of data breaches will reduce over the next year as, while there have been "many positive moves in raising awareness and bringing more people into the industry", too much data is "in the wild" and attacks are increasingly moving to mobile.

He said: "We're probably not going to get a grip in the short term. There is no clear endgame; but if governments, companies and individuals keep upping their game, and there is good evidence that they are doing so, we can at least stay on top of things."

Dan Hubbard, chief technology officer at Websense, said: "One thing we do know from the explosion of breaches, amplification of advanced malware and propagation of exploit kits is that the common factor here is, very simply, the web.

"The most advanced criminals are going to ride the waves of personal devices, personal social media use and personal web activities of employees to create more advanced, social engineering attacks to get in. Many of the business and government attacks in the coming year won't necessarily be about how complex the code is, but how well they can convincingly lure unsuspecting victims to click."

Imation Mobile Security said compliance will continue to drive data protection, especially as the European Union is planning to fine companies up to five per cent of their global turnover as punishment for the most severe data breaches.

Mark Seager said: "With regulatory bodies under pressure to up their game in 2012, companies will continue to feel the sting of hefty fines unless they address the challenges they face when it comes to protecting data, whether in the cloud or on premise.

"Poor management of customer data, resulting in errors, loss and theft, will continue to be a stumbling block unless organisations make themselves equipped to deal with it. With regulators set to continue to wage war against businesses failing to implement the right information management procedures, businesses must act quickly to ensure they aren't in the firing line for a hefty fine."

Let's look at one final trend for this lengthy summary: big data. It was recently claimed that the problem of 'big data' can be solved if the right techniques are used to manage and search the 'digital landfill'.

Chief technology evangelist at Quantum, David Chapa, acknowledged that massive amounts of data will need to be managed across multiple tiers of storage, while Wray said the key factor will be how businesses manage big data and optimise their network to deal with the growing use of social media, mobile and cloud services.

Ovum said big data will create transformation opportunities as, by applying analytics to social media, machine-to-machine and location data will create new business opportunities and drive new investment in business intelligence and data warehousing infrastructure. Seager believed that this is a generational thing, as today's youth is sharing everything they do, at every moment of the day, via social networks.

“As thousands of consumers are sharing more of their identity online, for businesses in 2012 the matter of data privacy will continue to shake up process and protocol. With increasing volumes of intelligence on consumers now available, brands must tread a very fine line when it comes to what data they gather and how they manage it, to avoid overstepping the mark or making critical errors,” he said.

Is that everything you expected, or was there something that the experts missed? It is possible that the above will be the key trends for 2012, or it could be something different altogether – this is based on predictions, after all. Either way, after a busy 2011, I expect that information security is set for another big year next year.

<http://www.scmagazineuk.com/2012-security-predictions-for-the-future-of-mobile-cloud-attacks-data-loss-and-big-data/article/220301/>