Protecting information and services in a hyper-connected world

Every year, companies worldwide spend billions of dollars on security to protect their data center. Yet, security breaches happen. Clearly, the problem extends beyond what technology can offer.

At the recent NetworkWorld Asia Info Security Conferences in Kuala Lumpur and Singapore, industry experts and practitioners suggested as much.

In Kuala Lumpur, keynote speakers, discussion panellists and the audience alike raised the issue that management in many organizations are still in denial when it comes to security. Larger enterprises believe they have invested enough into building their defences, and want to simply focus on business growth.

But they have to take the evolving threat landscape and the changing role of IT into consideration. Cybercriminals are getting away with their sophisticated tools and ecosystem. IT infrastructures are going into the cloud, mobility and BYOD are entrenched into the enterprise fabric, social media networks have become employees must-have tools for both work and personal interaction, and we're heading into the uncharted waves of the 'Internet of Everything'.

Key issues

Dr Aswami Ariffin, vice-president and digital forensic scientist at CyberSecurity Malaysia, said in his keynote address that mobile phones and computers play a growing role both as tools and as targets of digital crime. They are also an important forensic tool in solving both digital and non-digital crimes.

Ravindra Krishna of Cyberoam emphasized the need to address the missing link in security in today's open and collaborative networking environment. Business networks are exposed to evolving threats, and BYOD and virtualization are creating security gaps and blind spots. "Organizations need to understand how their own users are adding to the threat potential, and if they are being used as attack vectors."

For keynote speaker Anthony Lim, vice-chairman of the Application Security Advisory Council at (ISC)2, the primary issue with security is not the hacker, WORM or advanced persistent threat (APT). "It's about other issues that will affect what happens to your data, which becomes a security issue," he said.

Lim also highlighted questions of governance. How was the vast store of confidential information handled after the collapse of financial services firm Lehman Brothers? Why couldn't the firewalls, the layers of security and the technical experts stop the high-profile

data breaches that hit retailers like Target?

Here, another problem lurks. "Hackers know you have firewalls, [certified security professionals], 10 appliances in a rack at the gateway," Lim explained. "They need a new place to attack and that is the software layer – your Java, Android, html5, SOA, Web 2.0, C++."

This problem has prompted (ISC)2 to offer the Certified Secure Software Lifecycle Professional program, which validates the application security competency of any IT professional involved in the software development life cycle.

Cricket Liu, chief infrastructure officer at Infoblox, spoke about a variety of threats, including cache poisoning and the frequent Distributed Denial of Service (DDoS) attacks on Domain Name System (DNS) servers. DDoS attacks also exploit DNS servers to become more potent. One example is a DNS amplification attack, which exploits servers that allow open recursion.

Among the ways to combat these attacks, "monitor DNS traffic and make sure you know what's happening in your DNS infrastructure," Liu said. "You'll be surprised how few people have any idea how many queries their name servers are processing."

Apt views

During a panel discussion, in response to a question on APT risk mitigation, Darwin Gosal, senior IT manager at YaleNUS College, said that it depends on the resources, money and time that the attackers have, their motive and their persistence.

"I don't really believe the products out there that claim they can prevent APTs because if the APT is persistent, it will continue trying for the next one, two or even 10 years," he said. "The only way is to keep monitoring what you find valuable and [invest the] necessary amount of money [in security that corresponds] to the value of asset that you are trying to protect."

"We have to be truthful to ourselves," said Alagu Karuppiah, head of technology at Diners Club. "We cannot prevent all the attacks. The question is how fast can you [brace your people, processes and infrastructure against] an attack?"

Lee Siew Kit, vice president of Information Technology at SATS, also noted that while APTs will happen because they can come in through many channels, "we definitely need proper processes, set ups and policies, and we need drills on how to properly respond to these threats."

In another discussion, Koh Juay Meng, president and chairman of Cyberguide Programme at RSVP S'pore, and Aaron Tan, founder and chairman of IASA Asia Pacific, pointed out a major source of corporate data leakage in the improper disposal of old computers and the data stored in them.

On the issue of privacy and spam, Philip Louis, chief marketing officer at Europlacer, urged organizations to have a clear value proposition, and understand why customers would want to receive the message they are sending. "If you don't do that, you are basically doing a leaflet drop," he said. "It's indiscriminate communication. That devalues the market for everybody and cheapens your brand. Technology can do everything but not everything is helpful." NWA