http://sbr.com.sg/telecom-internet/exclusive/all-you-need-know-about-securing-cloud

All you need to know about securing the Cloud

13 Jan 14

The remedy of a private cloud attack is around $9 million, studies show.

Cloud security has become a buzz word in the information technology (IT) sector since the outbreak of information-sharing via the internet as a popular, and sometimes a necessary, activity not just for businesses but also for consumers.

Dr. Hongwen Zhang, Chief Executive Officer of Wedge Networks, said during the NetEvents APAC Cloud Summit held on November 20-21 that cloud is the biggest leap in connectivity since the Ethernet and it presents numerous opportunities both for businesses and consumers.

Since the introduction of cloud, issues have shifted from taking advantage of it to make information available to more end-users to protecting this available information from possible breach.

“I believe that cloud presents the biggest opportunity to impact the information security, the very industry of information security,” Dr. Zhang said.

This cloud initiative, he noted, provides the biggest opportunity to secure millions of small and medium businesses (SMBs), nearly one billion virtual machines, about 2.1 billion mobile devices, and around 18 billion other devices connected to the internet.

“But the fact is every year, globally we see almost several hundred billions security breach-related damage. Also, we spend almost $60 billion every year on security solutions. So, there’s something not quite working there,” Dr. Zhang raised.

Thus, he said security management is key to taking advantage of the benefits cloud can offer.

Sources of threats

Tim Dillon, Asia Research Director of Current Analysis, said the economic impact of security break to firms, especially those that are listed, is significant.

He cited some studies that suggest a public disclosure of breach knocks up to 5% off the organization’s share price. For instance, Dillon said Sony's outage back in 2011 was around $171 million of lost revenue for a month. Others, he noted, suggest that remedy of a private cloud attacked is around $9 million depending on the kind of breach.

“Cloud is both a concern and an enabler of security,” Dillon noted.

The influx of firms allowing higher degree of mobility to their employees poses security threats especially on information access from the outside of the office’s network.

According to Dillon, a survey recently conducted to organizations in Asia Pacific suggests that a small number of firms have mobile device usage o BYOD (bring your own device) policy. To be specific, there was a relatively low number of organizations approving BYOD use.

However, when asked if the firms allow employees to use their own equipment—mobiles, laptops, tablets, etc.—in the office, he said the number jumped to 80%.

“So organizations have this influx of consumer technology into their environment, and it's very difficult to deal with. The device environment is incredibly open,” Dillon stressed.

He added that the trend toward machine-to-machine (M2M) style devices and NFC (near field communication) also poses threats to information security. M2M, he said, has grown immensely in Europe and North America and more recently in Asia Pacific.

“And it is an area where organizations kind of forget about security, and that is going to be a big problem,” Dillon said.

The last source of threat, he mentioned, is third parties or outsiders that render services to several firms and are allowed to access internal information.

“So, you a vulnerability there, third parties coming into the organization,” Dillon emphasized.

Searching for the best security solution

“Security for the future is all about effective management,” Dr. Zhang noted.

In saying this, he mentioned the unrelenting demand for both convenience in using and making the most of internet-capable devices and assurance that information shared do not reach the unintended end-user.

However, he pointed out that though necessary, affordability of security solutions is still an issue for most users, whether businesses or individuals. This is seen as a single reason value-adding security solutions offered by various IT service providers are running with very limited success.

“Majority of under-protected SMB customers and consumer users would not have the resource to really procure the expensive solutions, the so-called managed security solutions from service providers,” Dr. Zhang said.

“The technology is too expensive to be used by the mass computing devices. So, we’ve got to find an easy way to allow the service provider to sell security services to the SMBs and consumers with affordable price. That’s really the key. That’s the technical challenge,” he added.
He explained that in order to entice SMBs and other end-users to avail of security solutions, they must be informed

of end-results.

“When they can easily comprehend what is the end-result of the security, it is proven that SMBs will open up their wallet and really pay the service provider for such services,” Dr. Zhang said.

He also said possible losses to the firm could also be cited in case a breach of information happens due to lack of information security.

According to him, statistics show that firms incur damages of $1 trillion a year due to attack amid spending of $60 billion on security.

“A cost-effective solution not only for now but the future really is a very challenging technical problem for the service providers,” Dr. Zhang stressed.

Moving forward

“We look at Cloud as being the great enabler of security. And it is in many ways but it also requires us to change the way we think about security, and I think that's the fundamental thing,” Bryce Boland, vice-president and chief technology officer for Asia Pacific of FireEye, said.

He discussed the human resource aspect of security and explained that most vulnerabilities are created by people who have created code and designed applications that may be flawed.

“[The networks and systems] are going to be administered by people who are also trying to use social networks and trying to use the latest mobile devices to get their job done more efficiently, so we know that we need to look at the people aspects of the problems as well as the infrastructure components,” Boland noted.

He also pointed to service providers’ band-aid solutions, which are easily considered by most clients due to affordability and straightforwardness.

“Traditional legacy solutions like Firewalls, IPS and others produce a lot of false positives and unfortunately, enable them to then spend even more money by providing investigation and breach clean-up services,” Boland explained.

Boland also raised the idea that attacks can also happen through security service providers which serve as repositories of the firm’s or several firms’ information.

“We see attacks taking place against organizations and data centre's repositories that provide real value. And that means that a service provider becomes a natural aggregation point,” he said.

Boland further explained that as that information is aggregated under a single point of control in a major service provider, that service provider becomes subject to all of the interesting interest of the attackers who would be otherwise going for the individual organizations.

“I think as a service provider, yes, you have a greater investment in security, but your threat profile is significantly greater and requires a real level of attention to detail, and continual maintenance in terms of the evolution of the

threat which is extremely difficult to continue to provide," he said.

Dr. Zhang agreed and service providers must make sure they have the security measures to prevent any privacy data leakage issues.

He added service providers also need to make sure that there is a unified standard to allow for connection of services provided by different providers.

"[Service providers have] to work together so you don't have the antibodies killing the other part, which typically happens when you have an over-strung security and your business continuity got impacted so that's our view," Dr. Zhang noted.

Boland concluded that just like other business issues—human resource management, accounting, etc.—cloud security or information security has become one of the key concern in most firms.

"I think in the organizations that we are selling to, we are increasingly finding organizations moving some of their processes into the Cloud just as normal part of business process outsourcing," he said.