Demystifying IT security buzzwords

Summary: *Cloud security and APTs are some of today's most used industry watchwords, but it is important to understand the terms beyond the hype to better secure companies' data networks.*

By Ellyne Phneah | October 3, 2012 -- 10:39 GMT (03:39 PDT)

The IT industry is not averse to indulging in acronyms and jargons when describing security issues and threats. But in an era when high-profile security breaches and incidents seem to occur on a daily basis, companies should make the effort to make sense of commonly-used security terms to know what they are defending against.

Roman Foeckl, CEO of security firm CoSoSys, for one, said as more individuals and organizations experience seeing their accounts and corporate networks getting hacked into and the onslaught of security offerings introduced to the market continues, confusion regarding certain security terms is inevitable.

When these terms are misunderstood, this can lead to organizations being wrongly informed and opt for a security package that is unsuitable for their needs, Foeckl added. Implementing the wrong tools, in turn, could result in putting corporate data at risk, affect companies' overall budgets, and impact their risk management strategies, he noted.

To prevent this, ZDNet Asia takes a closer look at four commonly-used security buzzwords to find out what they really mean.

Cloud security

Many confuse cloud security with cloud-delivered security-as-a-service tools, and the situation is not helped by the fact that the original term has evolved to describe many different issues, Foeckl pointed out.

These days, cloud security can mean the data stored in cloud repositories and the related security measures to safeguard the information, such as encryption. Another take would be from a disaster recovery standpoint where backup tools are the focus to prevent data loss should the cloud service goes down, he explained.

Then there is the access management component that focuses on which employees can access what types of information stored in different cloud services, the CEO pointed out, adding this would creep into compliance regulations and other related issues.

All these add up to make defining cloud security a hazy endeavor.

Advanced Persistent Threat (APT)

APTs (http://www.zdnet.com/symantec-apts-can-afflict-anyone-2062304681) are a very targeted attack that typically takes place over a long period of time, exfiltrating intellectual property, economic and political information without the victim knowing it is happening, Michael Sentonas, CTO of McAfee Asia-Pacific, observed.

The term is overhyped and misused (http://www.zdnet.com/hacktivism-against-apac-govts-to-rise-7000004701/) in many cases, especially in common attacks conducted to achieve quick financial gain or fraud, Sentonas stated. Such in-and-out attacks using simple intrusion tools can be stopped with strong security architecture and a layered defense, he said.

The level of skill required to conduct an advanced persistent attack, on the other hand, is higher and hackers will need to be well-resourced, highly motivated and patient in trying numerous attack vectors until they succeed in breaching the target's accounts or network, the executive said.

So, the motives and level of skill and resources are the main differences between run-of-the-mill hacks and APTs.

Mobile Malware

The implications of mobile malware tend to be obscured behind figures and statistics of how rapidly such programs are growing (http://www.zdnet.com/trend-micro-mobile-malware-apps-up-five-fold-in-q2-7000001259/) , and which platforms are being targeted the most, Sentonas said.

Looking deeper, the issues related to mobile malware (http://www.zdnet.com/mobile-apps-pose-biggest-threat-7000002093/) center on the risks that is changing dramatically over a short period of time, he said. This is due to the convergence of networks and increasing use of sophisticated devices, the executive stated.

As more valuable information gets stored on mobile devices, this also increases cybercriminals' motivation in targeting mobile devices, he added.

"The challenge and risk is many people are not adopting protection [for their mobile devices] and choose to wait and see instead of fully understanding this risk [posed by mobile malware]," Sentonas noted.

Mobile device management (MDM)

There are many terms used to describe the introduction of consumer-grade devices into the workplace, such as bring-your-own-device (http://www.zdnet.com/asians-more-dependent-on-byod-7000000104/) (BYOD), and the measures companies are taking to address the challenges posed by this phenomenon.

Mobile device management (MDM) was thrown into the mix to address the latter point, and this term has since been used to describe many different aspects of working with and securing end-users' mobile devices, Foeckl noted.

The term is still evolving currently, but the definition is being broken down granularly to focus on different aspects of the BYOD trend, he added. Mobile app management, for instance, is a term dealing specifically with measures to safeguard how corporate apps are used and policies to follow, while MDM will specifically address the security of data stored on one's device.

IDC Asia-Pacific's Tim Dillon thinks otherwise, though. The analyst previously mentioned MDM had morphed to now include identity and access functions (http://www.zdnet.com/mobile-management-requires-holistic-granular-approach-2062304794/) , and would eventually need to evolve to become a multi-faceted solution that addresses device, applications and data access.

Topics: Security, Cloud, Malware, Mobility

About Ellyne Phneah

Elly grew up on the adrenaline of crime fiction and it spurred her interest in cybercrime, privacy and the terror that exists in the dark side of IT. At ZDNet Asia, she has made it her mission to warn readers of upcoming security threats, while also covering other tech issues. Elly enjoys growing her already-huge wardrobe, photography, the performing arts and planning her travel escapades. She dreams of leaving her footprints all over the world.

Talkback