Computing Security
Secure systems, secure data, secure people, secure business

2013 - Where Will It Take Us?

Search

Related Topics: Security Malware BYOD Phishing INDEX
Related Companies: Wick Hill Group Clearswift CoSoSys FireEye SafeNet INDEX
Related Product: INDEX
Article Type: Feature INDEX
Published: Jan-13 INDEX

PREVIOUS ARTICLE NEXT ARTICLE

"We will also see the emergence of the Information Map, enabling organisations to better understand where their critical information is, and how it flows between people and organisations. This greater understanding will lead to improved security against the threats we know are out there and the new ones that will appear."

BYOD-iOS challenge
According to Roman Foeckl, CEO and founder of CoSoSys, organisations will continue to face the BYOD challenge in 2013, meaning adapting to it and implementing solutions that allow them to deal securely with devices brought by users.

"Those devices are mainly Android and iOS smartphones and tablets, along with more Mac OS X MacBooks and other portable PCs. New PCs brought by users will come with Windows 8 since it started to be sold and comes now with every new PC that is sold. Naturally, people will take their new PCs and tablets to work and companies will have to deal with a new operating system in their network. The BYOD trend will demand a focus on apps downloaded on iOS, with an emphasis on Android devices which are loaded by employees with all kind of apps, without paying attention to the damage that these apps could cause, since more of them will be compromised with malware that is distributed and disguised as mobile apps.

"It is just a matter of time before security breaches caused by apps will come to the surface, so IT departments have to be prepared how to deal with these through mobile device management and mobile application management solutions put into place. We also expect for 2013, even more than in the past years, that Macs will make their way into organisation's IT infrastructures. More than 50% of the companies we speak with will issue Macs, giving IT administrators an additional OS to manage and secure.

Inadequate defences
Meanwhile, Paul Davis, director of Europe at FireEye, is scathing about many organisations' ill preparedness to counter attacks. "Despite the fact that the stakes have never been higher, with regards to the consequences of falling victim to a cyber attack, there remains a woeful inadequacy in the level of security architecture in place in the vast majority of organisations today," he states "Traditional security defences, including perimeter-based defences and anti-virus, are insufficient as stand-alone methods of protection, and should instead form the foundation of a holistic and integrated defence strategy.

"While the heightened media attention around international cyber attacks and data breaches has signalled a new era of awareness around the realities of the IT security threat - for instance, with the Olympics providing a focus of much concern over the potential for cyber attacks to wreak havoc on a significant, global event - there is still a worrying gap between what is now known of the threat and what is proactively being done to secure against it.

"Quite simply, there is no room for complacency when it comes to this issue and, in 2013, network security and data protection really should be front of mind, right to the highest echelons of an organisation," he cautions.

Watershed year

Jason Hart, VP Cloud Solutions at SafeNet, believes 2013 should be a watershed year - "when enterprises and governments consider a wholly new approach to data protection, founded on the concept of the secure breach. What the experiences of 2012 (and 2011, too) teach us is that perimeter defence strategies aren't working sufficiently. Indeed, it can be argued that these long-held strategies are coming to the end of their useful life."

In part, this is because hackers and e-criminals have become more persistent and inventive in their use of social engineering to undermine defences. "In 2013, these threat actors aren't going to let up," he stresses. "They're going to take advantage of new vulnerabilities, especially as enterprises embrace mobility and virtualisation on a wider scale."

Page 1 2 3 4

Email The Editor With Your Thoughts! Go Top

PREVIOUS ARTICLE NEXT ARTICLE