BIZCOMMUNITY

Face 2016 with a proactive attitude of security awareness

By Carey van Vlaanderen

22 Jan 2016

It is a fact that cyber attacks are growing more sophisticated. Protecting a company's information and data seems to be an arduous and complicated task, and finding trained personnel willing to combat continuing attacks gets more difficult all the time.

©Buchachon Petthanya via 123RF

However, the good news is that it is possible to protect individuals and businesses, and that technology, management and education, combined together, are key factors for security.

Technological advances bring new possibilities for individuals and for businesses. And cyber criminals are well aware of this fact. Given that technology affects so many aspects of everyday life, insecurity could be 'everywhere'. Consequently, we believe instead that security should be everywhere, and insecurity banished. And therein lies the challenge for businesses, governments and individuals.

The challenges for the future are not impossible to accept: the fact that in five years there will be 25 billion devices connected to the internet, according to Gartner, does not mean that users must become paranoid about their privacy and information security.

Factors to be considered

As well as needing to continue investing in security, companies will have to assess the technologies they use to detect and eliminate the threats from their networks. The implementation of layers of protection, or technologies able to detect an attack, in its various stages, to minimise the exposure to cases of information leakage and data hijacking, to reduce the exposure gap and the response time of each incident - all these factors need to be considered.

Employees' ability to detect possible attacks, which occur mainly through emails, help to reduce the time needed for identification of such attacks. This ability is not possible, though, without education and training in information security.

However, this will not be developed if the organisation does not see user involvement in security as an important aspect of its business. In other words, if the company does not care about the education of its employees and the correct implementation of protection technologies, it will be a lot more vulnerable to cyber attack.

Based on what we expect to see in the future, it is important to stress that information security does not wholly depend on advances in cyber criminals' attack methodology, but also on the measures taken by individuals, governments and companies to defend their information, systems and infrastructure. Indeed, each group has to accept the challenge and assume responsibility for improving and maintaining information security.

Different challenges

There are different challenges for the years to come: from users' demands for higher levels of security and privacy, the importance of keeping children safe on the Internet, and the actions that security agencies should take to combat cyber crime, to the implementation of millions of new devices that interconnect the lives of individuals, businesses and governments.

Security software companies, protection technologies and the education of consumers and end-users will play major roles in the understanding, analysis and protection of the most diverse technologies. The role of the user is becoming more important and this is a trend that will continue to grow. For some years now, users have been demanding that companies provide more and better security to protect their data and information.

But beyond these demands, it is more important to educate individuals about internet security and how to be protected. In other words, users can no longer be indifferent towards their information since most of it is stored in different digital formats and in many different places far beyond the borders of their own systems.

In 2016 and the years to follow, users will have to play a more active role regarding their own security, by continually learning to protect their data as well as relying on the protection afforded by software security companies and the services they use.

Three pillars

Companies will have to base their strategies on three pillars: technology, management and education of employees. That said, the roles of the state and the security agencies should be stressed as well, in terms of passing laws that serve to encourage the secure evolution of new technologies, defining standards and rules that promote respect for users' privacy, and ensuring that services and infrastructure continue to serve to facilitate countries' development.

In addition, investment in research and development into new technologies must be accompanied by a security plan that assesses and describes the security measures to follow.

Therefore, with a larger potential attack surface and new vulnerabilities emerging in widely-used technologies, the greatest challenge of 2016 will be to focus on protecting networks, internet access and the way in which devices are interconnected. From the router that provides access to the internet in the home to the infrastructure of the most modern cities, the best security practices should be applied to protect data, information and privacy.

This is collaborative work that requires more active participation from users, companies with a critical understanding of information protection and a proactive role in security strategy, and governments promoting economic development while ensuring the establishment of (and compliance with) standards, so that both companies and individuals will be protected in the event of a cyber incident.

2016 will be a most challenging year and we must face it with a proactive attitude of security awareness.

ABOUT CAREY VAN VLAANDEREN

Carey van Vlaanderen is CEO of ESET Southern Africa. ESET is a global provider of security software for enterprises and consumers and is dedicated to delivering instant, comprehensive protection against evolving computer security threats.

- 4 ways to manage the human threat to cybersecurity - 18 Jul 2023
- A cybercriminal's tricks and trades to get into your phone - 23 Mar 2018
- What is encryption, how does it work and why is it important? - 6 Mar 2017
- Five common security threats that demand attention - 9 Mar 2016
- Face 2016 with a proactive attitude of security awareness - 22 Jan 2016

View my profile and articles...

For more, visit: https://www.bizcommunity.com