BIZCOMMUNITY

The human firewall: turning the weakest link into the strongest ally

By Simeon Tassev

28 Oct 2015

Security has become a top priority for businesses in an effort to protect themselves from an ever-increasing variety of threats that continue to advance in sophistication and persistence. Many organisations have implemented costly and complex software solutions to assist them in mitigating the risk of hacks, data breaches and malware to name but a few. However, breaches still occur on an alarmingly regular basis despite this investment. The reason? Most frequently, the human factor is to blame, either as a result of human error or deliberate intent.

©arindam banerjee via 123RF

People are in fact the weakest link in any security chain, capable of bringing vulnerability to even the most sophisticated security system. Addressing this threat through a combination of appropriate technology, enhanced awareness and behaviour modification is essential to creating the 'human firewall', effectively turning this weak link into a strong security ally.

The risks that people pose

Organisations today are faced with a multitude of security risks and threats, most with the objective of stealing data and sensitive corporate or personal information. While sophisticated tools and malware can be developed to accomplish this, getting this software onto corporate networks is still essential for those with malicious intent. There are many ways of achieving this, from infected attachments and links sent via email or accessed online, to social engineering attacks that trick users into divulging information such as usernames and passwords or breaking security procedures and protocols.

Both hardware and software have limitations when it comes to truly securing an IT environment, which can be exploited by those with malicious intent. In addition, simple human error accounts for many incidents of data breaches - even something as simple as leaving a memory stick lying around or losing a mobile device with corporate data access can wreak havoc within an organisation. Security professionals and IT managers need to factor in the risk that people pose as part of the security chain, since even the most sophisticated security solution with all of the necessary layers can be compromised by a simple mistake on the part of an individual.

The first step

Creating awareness is the first step in mitigating the risk of human error. Many people today remain unaware of the threats that exist, how they are perpetrated, and what the consequences of a breach could be. In addition, not everyone makes use of password protection with devices such as smartphones. People need to be educated in areas such as how to spot malicious links and fake websites, and why they should not click on links sent by unknown persons in email, for example. They also often do not realise that their devices contain potentially sensitive information that could compromise an organisation or lead to it being compromised. Education of users for basic security practices is an essential first step.

How to turn the weak link into the first line of defence

However, awareness alone is clearly insufficient, as the on-going success of spear-phishing and social engineering attacks demonstrates. Aside from awareness, there are three key areas that need to be addressed to turn people from a weak link into an additional line of defence. Firstly cyber security technology remains critical and should be bolstered or prioritised in order to shore up any existing vulnerabilities. While technology may not be impervious to all threats, it is still essential in preventing any number of different attacks from reaching the organisation on a daily basis. With the right controls in place, fewer threats will enter the corporate network, where they could potentially cause harm as a result of the human factor.

Secondly, it is important to ensure employees receive on-going training and education so that they are up to date with the latest threats and techniques, including scams that employ spear-phishing and social engineering techniques as well as other emerging threats. In order to effectively form part of an organisation's defence, people need to recognise threats and potential threats. They must also be able to recognise the motivation behind the attack in order to understand the consequences. For example, the consequences of clicking on an infected link should be understood along with the objective of cyber criminals, be it compromising a network or obtaining personal details.

Finally, changing behaviour is potentially the most important aspect, but also often the most difficult to achieve. Understanding the nature of threats is an important part of this, however, people also need to acknowledge the consequences of their actions and flag potential threats for the attention of IT. Often it is a case of a lack of knowledge and training, combined with apathy of the consequences that result in people falling prey to many scams and cyber security threats.

People security

When it comes to cyber security, people are often the weakest link in an organisation, frequently without realising the dangers of their behaviour. A comprehensive approach to 'people security' including awareness, education and behavioural change, as well as appropriate technology, is essential in closing the gap on this particular vulnerability. If people can be turned from weak links into security champions, organisations will be in a far better position when it comes to defending their sensitive information, data assets and intellectual property from theft and other breaches.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa

- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...