gulfnews.com

Rise in IT security training and awareness

Companies not only improve their security posture but also gain in terms of savings and competitive advantage

Jyoti Lalchandani
Published: 21:34 July 3, 2014

GULF NEWS

One of the major challenges cited by IT department heads when it comes to managing IT security is not just the growing sophistication and frequency of threats but also the fact that employees do not adhere to policies.

While IT departments would like to put this down as employees not following guidelines, the majority of the mistakes that occur around data loss and processes that lead to malware issues are purely accidental or due to sheer ignorance. Companies often do not even have security policies in place, and are typically very reactive when it comes to dealing with incidents or managing security issues. If companies do have policies in place then employees are usually not aware of them, or communication of the policy is so ineffective that it is ignored.

Growing number of endpoints

While IT departments are making efforts to secure the ever-growing number of endpoints, employees can cause problems by contributing to data loss through sheer ignorance (e.g., an employee not aware of what information can and cannot be shared with external parties), by accidentally deleting/changing information that they should not have access rights to in the first place (e.g., a lack of proper identity life cycle management), or by bringing malware into the organisation (e.g., through an infected USB device).

While insufficient training standards are already a major problem, technologies such as mobility and social compound the situation by adding to the complexity of data security policies and strategies.

Given the increasing number of attacks being experienced by organisations within key sectors of the UAE economy, companies have begun to take more proactive steps toward ensuring their security. In addition to deploying advanced solutions, the more proactive ones are updating their existing policies, while others have started to put security policies in place. IT decision makers are also increasingly realising that their policies can no longer be static and must be updated based on new solution rollouts, technology adoption, and audits. However, to be a secure organisation, companies must adequately train their employees around the security policies being put in place.

Traditionally, IT security training and policy is seen as the responsibility of the IT department, which should never be the case. A successful security training programme requires a few key processes to be put in place.

Firstly, there should be buy-in from the executive board for IT security training to be made mandatory for each and every employee across the organisation. Secondly, the training sessions must be conducted in collaboration with HR and the various lines of business (LoBs). Indeed, it is imperative that this level of training should be supported by HR.

The training should not only cover the key points of the policy but should also train employees on basic security practices that they can utilise themselves to prevent or mitigate an attack. This aspect can cover aspects around web security, how to avoid social engineering attacks, and secure information-sharing policies. It should be kept in mind that companies can also implement data-loss-prevention systems to automate information sharing policies and block USB ports as well. In addition to getting the support of HR and LoBs, the training should be modular, and metrics need to be put in place to evaluate the success of the program. These metrics will be critical for justifying further investment from the board for the continuation of the program. IT departments should also continue to prompt users if there any major security threats that can impact them on an organisational or even on a personal level. Also, security training programs need to be updated to accommodate the proper secure practices for the use of cloud, mobile, and social technologies within the organisation.

A growing trend in the UAE is that several IT services providers are establishing security awareness training practices. At times the IT and HR departments within organisations are not equipped enough to conduct the training processes themselves, and therefore seek out security awareness training services from external parties. The IT service provider then works with the organisation’s IT and HR departments to conduct these training sessions.

The major benefits of a proper IT security awareness training programme is not just limited to making employees more aware of how they can protect their data at a corporate level; it also benefits them on a personal level, since such training can help increase their awareness of how to protect themselves against identity fraud and phishing attacks. Companies also benefit in terms of cost savings, since they not only reduce the number of incidents that could have incurred previously, they also reduce the chances of downtime. By establishing a strong security culture, companies will be able to reduce the chances of failing to comply with regulatory requirements. There is also a benefit in terms of improving their overall reputation with customers, and thereby gaining a clear edge over the competition; this is particularly beneficial for those organisations tasked with handling large volumes of customer information. By implementing a security training programme, companies not only improve their security posture but also gain in terms of savings and competitive advantage.

The columnist is group vice-president and regional managing director for the Middle East, Africa, and Turkey at ICT market intelligence and advisory firm International Data Corporation.