Cyber Security: Insider Threat Analyzed

Article

In a world where data breaches are quickly becoming commonplace, even the best security technology in the world can't help your organization to protect itself from security breaches unless your employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources.

In 2014, we learned the hard way that people are the biggest security problem we have today. In most cases, breaches occurred when an employee or third party gained access to the organization's internal IT systems access privileges.

The Vodafone and Telstra breach in late 2011 began when parties outside the control of internal IT security obtained credentials to access the organization's internal IT systems. Business users have more access than ever before to the critical data and services they need to do their jobs, and we can leverage this empowerment to engage them in ensuring the security of our most sensitive organizational assets. Said another way, it is precisely due to this unprecedented level of access to sensitive information that privileged users should be considered the first line of defense for our critical corporate assets.

An effective employee cyber security education should contain information about the most prevalent attack methods and actors of the current threat environment. In 2014, the expanding IT infrastructure that gives users easy access to sensitive data and services means that if a necessary security solution model is not implemented access to key organizational data can be accessed without any scrutiny. As an example of how internal user data is

targeted, Trend highlighted that Ransomware became a bigger and more sophisticated threat across regions and segments, and unlike older variants no longer involved simply issuing empty threats but actually encrypting files.

For example, training employees and key vendors in the use of Phishing email identification could have prevented the devastating Carbanak breach where hackers sent emails containing a malware program to hundreds of bank employees from different banks, hoping to infect administrative computers. Employing a Privileged Identity Management framework as part of an enterprise security model where all administrative access is monitored could potentially have highlighted these breaches a lot sooner.

In order for employees and the organization to truly benefit from cyber security education and for it to be embraced throughout the organization, cyber security education should be conducted frequently and made mandatory; but more importantly, easy to access and available on-demand.

Training employees is a critical element of security and the key to successfully implementing cyber security within the organization is to ensure the business user is seen as an extension of the security team. Only then can the impact of internally targeted data breaches affecting an organization be minimized and potentially avoided.

About ARCON

ARCON is a leading Information Security solutions company specializing in Privileged Identity Management and Continuous Risk Assessment solutions. With its roots strongly entrenched in identifying business risks across industries, it is in a unique position to comprehend and identify inherent security gaps in an organizations infrastructure framework and build and deploy innovative solutions/products to significantly mitigate potential risks.