Advisen News

An Ignored Cyber Security Risk: Employee Access

Employee access an ignored cyber security risk

By Janet Aschkenasy, Advisen News

Companies often worry about outside hackers, but they face huge information security risks from the inside as well.

And this type of security risk can be easily, and even cheaply, addressed with proper planning.

Employee access is often forgotten when it comes to cyber security best practices, says a report from digital security provider Gemalto.

Exacerbating the problem, companies often fail to do proper background checks on individuals working for them—particularly after these employees are hired, Vince Rakoczy a forensics specialist with corporate security firm Investigative Management Group, told Advisen on January 4.

Small companies in particular often "fail to do proper due diligence and background checks on individuals not only at the beginning when they first hire the person but periodically", Rakoczy said.

In fact, top-level executives pose some of the biggest data security challenges.

"For IT professionals up against the significant challenge of keeping corporate networks and information secure, top level executives and board members present unique requirements" according to Gemalto's report. "Highly mobile and highly privileged, these individuals typically have access to the enterprise's most confidential information, from earnings outlooks to acquisition plans to new products.

Gemalto says the potential profit in accessing executives' information makes them prime targets and cyber criminals are willing to spend time and resources trying to hack the information.

Additionally, data can be leaked if a laptop is lost or stolen. Log-in credentials can be compromised by "spearphishing"—an attack mounted against a high-value target. Gemalto cites Juniper Research data indicating that mobile malware increased by 155% in 2011.

Despite these mounting high-tech threats, one of the most common culprits where proprietary information is stolen comes down to something very basic that can be very easily disabled—namely USB port access.

"USB ports are active all the time so an employee who wants to steal information can simply plug in a USB flash drive or other external storage media and download volumes of information," explained Rakoczy.

"When you set your computers up you can physically disconnect those ports," he added, however, "Most companies either don't think about this or they want employees to be able to take work home so they assume the risk."

Another risk Gemalto cites relates to outside directors.

"Since a company's board of directors is typically made up of senior executives of other organizations, anytime a board member is sent confidential information about your company, that data becomes vulnerable to leakage on the board member's company network," Gemalto said.

Gemalto recommends providing board members as well as executives and employees who travel frequently with a sandboxed workplace that is segregated from the host PC.

Keeping up-to-date network system logs is also of paramount importance.

Large companies with large volumes of information being passed back and forth internally and externally may not want to deal with the expense of having someone analyze all that logging and tracking of information, Rakoczy said.

Thus, it's often the case when an information breach occurs and Rakoczy asks if network logs are enabled, they have not been maintained or they have been overwritten, with only the last few weeks of information available.