This story appeared on Help Net Security at
http://www.net-security.org/article.php?id=1289
9/17/09

The threat within: Protecting information assets from well-meaning employees
by Jagat Shah - CTO of Prism Microsystems -

Most information security experts will agree that employees form the weakest link when it comes to corporate information security. Malicious insiders aside, well-intentioned employees bear responsibility for a large number of breaches today. Whether it's a phishing scam, a lost USB or mobile device that bears sensitive data, a social engineering attack or downloading unauthorized software, unsophisticated but otherwise well-meaning insiders have the potential of unknowingly opening company networks to costly attacks.

These types of internal threats can be particularly hard to detect especially if a company has placed most of its efforts on shoring up external security. For instance, some cyber gangs in Eastern Europe have come up with a pretty clever method to swindle money from small US companies. They send targeted Phishing emails to the company's treasurer that contains a link which, when opened, installs malicious software that harvests account passwords. Using this information, the criminals initiate wire transfers in small enough amounts to avoid triggering anti money laundering procedures. In cases like these, traditional defenses (firewalls, anti-virus etc) prove to be useless as legitimate accounts are used to commit fraud. This story is not uncommon. In a study conducted by Ponemon Institute earlier this year, it was found that over 88% of data breaches were caused by employee based negligence. In another survey of over 400 business technology professionals by Information Week Analytics, a majority of respondents stated that locking down inside nodes was just as vital as perimeter security.

Employees, the weakest link

Let's take a look at some of the easy ways that employees can compromise a company's confidential data without really meaning to.

Social engineering attacks – In its basic form, this refers to hackers manipulating employees out of their usernames and passwords to get access to confidential data. They typically do this by tracking down detailed information that can be used to gain the trust of the employee. With the growing popularity of social networking sites, and the amount of seemingly innocent data that a typical employee shares on these sites, this information is not hard to track down for the resourceful hacker. Email addresses, job titles, work-related discussions, nicknames, all can provide valuable information to launch targeted phishing attacks or trick emails that lead an unsuspecting employee to hand over account information to a hacker posing as a trusted resource. Once the account information has been obtained hackers can penetrate perimeter defense systems.

Weak passwords - Most employees do not choose passwords that are secure enough against modern password attacks. For instance, the Conficker B. worm that spread like wildfire across the internet early this year worked primarily by cracking administrator passwords on networks. Considering that the worm used a list of only about 200 common passwords, the breached admin/employee accounts must have had really easy to guess passwords!

While some companies combat this by forcing users to choose complex passwords - minimum lengths, special characters, combination of alpha-numeric characters - and have them change these on a periodic basis, users often respond by writing passwords down or reusing passwords that they use on other less-secure websites. Some simply forget their password which poses a

security risk in itself since backup authentication systems like “secret question” are easily guessable

Employee negligence – Many employees unwittingly violate security policies simply to get their work done. For instance, employees without remote access may mail confidential documents to a yahoo or gmail account so they can work from home, or access company documents over an unsecured connection (free wi-fi at the local coffee shop), or copy data on a USB device only to realize later that they misplaced the device. Other cases of employee negligence may include downloading unauthorized software that hides malware which renders networks vulnerable to attacks, or use of applications such as Skype or Instant Messengers that open up security holes and let Trojans into a company’s network- In all these incidents there is potential for data loss.

Countermeasures

Security is only as good as its weakest link and unless companies address the human side of security, the hundreds of thousands of dollars spent on antivirus, firewalls, encryption and secure access devices, are essentially wasted. Drafting comprehensive security and privacy policies and educating employees on safe practices is a necessary first step to improving security; however, as we have seen above, these practices may easily be neglected or avoided. And punitive, brute force methods such as prohibiting the use of USB devices entirely, can be counter-productive and lead to employee dissatisfaction. The dilemma for companies then is to balance usability with security. Log Management can be instrumental in reducing risks associated with day-to-day employee decisions while still allowing them to perform their work with minimal intrusion. This can be done in a number of ways:

User behavior correlation: Companies are literally sitting on a gold mine of log data that can be used to detect abnormal or inconsistent user activity. Automated log management solutions can filter out potential security issues from the normal chatter of day to day operations by analyzing normal user activity patterns and alerting staff when inconsistent usage is detected. For instance, if Susie normally logs on between 9am and 10 am on weekdays, a logon at 2am or over the weekend could indicate that her account has been hijacked. Or, if Tom’s account typically sees a certain amount of network activity, a significant spike in his activity could mean that his account has been breached.

User activity monitoring: If a hacker gets access to an employee account and uses it to access privileged data that the employee is not authorized to access, or install a malicious program, an automated log management solution can alert staff of this violation. Log data can also provide valuable information on employee activity such as internet access, application usage, software install/update, file sharing traffic, instant messaging, files accessed/modified/deleted, network drives accessed and more with minimal intrusion. This helps security personnel detect critical policy violations and security holes that can result from the use of certain applications or websites.

Administrator account monitoring: Most hackers will typically target administrator accounts since a breach at this level provides them with the keys to the kingdom. Keeping tight control over this group is vital and knowing about any change (add or delete) is a must. Having event log monitoring in place can alert the appropriate personnel when a user is added to an admin account, which facilitates further investigation on the legitimacy of the addition.

USB device tracking: When it comes to data leakage, USB devices can be some of the hardest to detect. There is little that a company can do if a USB device containing sensitive information is lost by an employee, however, a company can take proactive measures by monitoring logs to track data that is written to, deleted from, modified or copied on to these devices. Rather than banning the usage of USB devices (a policy that can severely impact productivity), a log

management solution can be used to monitor what employees are actually doing with the USB devices and in many cases, remedial actions can be automatically launched to block a device if its use is not authorized.

The key thing to keep in mind when addressing the human factor of security is that employees will typically find ways around security policies if they find their day-to-day operations hindered or if they know that policies will not be enforced. Event log monitoring can not only provide companies with a safety net while letting their employees go about their work with minimal intrusion, but also help detect policy violations for enforcement.