

APRIL 13, 2006

Expert Advice

Enemy at the Watercooler: Insider IT Threats Increasing

By: Brian Contos

IT security and information risk management has been high on the agenda of financial institutions for the past decade. It's little wonder due to the regulatory and organizational repercussions of a wholesale breach. Historically executives have concentrated on threats from "beyond the firewall," protecting the company and its data from attacks by unknown parties from outside the company.

However, we are now seeing a sharp rise in attacks from inside the organization; individuals within the protective firewall dropping bombs into the network to take the system down, or misusing company data for personal gain. The image of an employee accessing the corporate network and stealing confidential data using an iPod-type storage device is no longer simply a threat scenario — today it has become a well-documented reality.

Organizations' focus on perimeter attacks such as viruses and spyware has detracted attention from the challenges posed by internal threats, often resulting in insider threat policies that are loosely adhered to and routinely skirted. However, best practices and increasing regulation are forcing institutions to look at the whole picture, to recognize their internal enemies and understand that threats from inside the organization are rapidly becoming more dangerous than those from the outside.

Insider Profiles

Managing the risk associated with insider threats poses some very specific practical and philosophical challenges, precisely because the enemy's identity is murky and the politics can often get nasty. Indeed, determining whether the biggest threat to the company may actually come from your trusted employees, contractors and partner organizations can be a difficult task for many employers. As painful as it may be to grasp, however, in an age where the average worker changes jobs every two years and company loyalty is often replaced by financial ambition, this is becoming the reality.

Perpetrators of insider threats can be placed into two main groups. The first group includes employees who become

disenchanted in their role or angered by the company — more often than not as a result of a disciplinary event. These are individuals who may want to harm, rather than rob, the organization.

In terms of profiling such perpetrators, the "Insider Threat Study" carried out by the Carnegie Mellon Software Engineering Institute in May 2005 suggests that there is a recurring pattern among the majority of insider attacks. The study examined 49 incidents across critical infrastructure sectors between 1996 and 2002, in which the goal of the attack was sabotage or harm to the company or an individual. In these cases, the study found that almost two thirds of the perpetrators were former employees, of which almost half were fired.

These results are not far from what one might expect, but the study also identified that 86 percent of the perpetrators were employed in technical positions (systems administrators, programmers, engineers), suggesting that the greater the knowledge of the system, the greater the risk of a threat from a disgruntled employee. This makes an overwhelming case in favor of regular employee reviews and careful hiring policies.

Personal Gain

The second and fastest growing group consists of individuals who join the organization and intentionally limit their tenure — either with a view to move on and up more rapidly, or to build a contact list, either legitimately or otherwise, before moving on. These people are almost impossible to spot.

Before 2002, the most common insider threat came from the disgruntled employee, a passed-over systems administrator, for example, dropping a "logic bomb" into the system to take down the desktops inside his/her department. On the whole, situations like this were not about about personal gain. However, with the growth of "data supermarkets" — online sites where personal details are auctioned to the highest

Continued...

bidder — information theft has suddenly become a much more common and much more lucrative event.

Recently, eight Bank of America employees were caught stealing more than 700,000 customer records with the express purpose of profiting from the action. Unfortunately, we live in an age of identity theft where it is all too easy for individuals to make money out of raw data such as names, addresses, account numbers, insurance IDs and social security numbers. The impact on an institution's risk management procedures can be immense.

Hard to Find

There are also suggestions that detected insider attacks are underreported, which makes it difficult to establish just how many incidents occur. You can't report on what you don't know about; however, it is safe to assume that these are becoming at least as common as known perimeter threats. Both kinds of attacks carry the same risks: loss of confidential data and intellectual property, along with compromised personal integrity, including exposed personal or private information, damaged or destroyed critical information assets, severed communication and costly downtime. However, insider threats remain more difficult to detect and prevent than their external cousins.

When dealing with employee access to hugely complex and wide-ranging global IT networks, the vast majority of attacks go undetected. For example, if a door entry key-card is used at a company site in Rio de Janeiro, and on the same day the same user identity is used to access the IT system in New York, one of the events is likely to be suspicious. However, there is very little chance that this will be identified in a manual environment where the most common analysis method is diving into disparate device logs looking for the suspect needle in a stack of needles. Similarly, if an employee uses his own, or a colleague's password, to download sensitive records onto his portable USB key-fob, this is, again, likely to pass unnoticed.

The most effective way to detect insider attacks, and to reduce the potential risk to the institution, is to automate the process — just as is most often done at the perimeter level. New automated enterprise security management systems, for example, work in tandem with existing best practices to create a single, comprehensive view of the organization's IT risk, employing advanced correlation and pattern discovery techniques able to match, for example, two apparently

unconnected events in two geographic locations, while making security and compliance officers aware of suspect activities like massive downloads or data copying.

Protecting Your Data

It is the sheer number and diversity of security devices and events — both internal and external — that makes correlation of data so imperative when it comes to detecting any kind of security threat. After all, the typical FTSE 250 company gets around 4 million attacks on its firewall every day. Multiply this by the number of additional perimeter defenses — AV, authentication & verification layers, anti-spam appliances, etc. — and there is an incredible number of security devices to manage. Add all the internal protections, password authentication, swipe card readers, anti-ID theft devices, applications, databases, operating systems and executives begin to lose control.

While managing a security portfolio — including event logging, monitoring, and alerting analysts to potential attacks — is central to protecting against insider threats, it is this real-time

correlation that holds the key to reducing and managing risk. Individual security events may pose no obvious threat, yet by checking them against one another, potentially innocent network occurrences become highly malicious attacks, and vice-versa.

Disappearing Perimeter

Ironically, the most effective way for organizations and institutions to protect themselves is to move their focus away from both perimeter and internal threats. While this sounds illogical, the simple truth is that an attack is an attack, regardless of where it originates. Organizations must start with pro-

tecting their IT assets from the ground up, from every threat, identified or potential. This is the theory of the disappearing perimeter — to start with the application and work outwards.

Overall threat awareness is much greater now than just 18 months ago, and many organizations have much more mature policies in place. Yet while the drive towards reducing corporate risk through IT security is vital, it is part of a larger picture that includes compliance regulations, company policy and organizational procedure. The adoption of enterprise security management tools and the corresponding security policies and procedures could most certainly give institutions the upper hand. **ECT**



ArcSight, a leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM(™) enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently.

ArcSight's customer base includes leading worldwide companies across many verticals-and more than 20 of the largest U.S. federal agencies.

For more information, visit www.arcsight.com