CSO
SECURITY AND RISK

From: www.csoonline.com

Cheap IT Security? The Tools Were There All Along

Fortunately, there are plenty of cheap tools to ensure a solid defense. Some of these tools have been in the arsenal all along, but you never knew it. (Part four in a series: How to Manage Security in a Recession)

by Bill Brenner, Senior Editor,

July 16, 2008

About this series: *Smaller staff. Deflated security budgets. In-store thievery. When economic times are tough, these are the things security pros must contend with. In this ongoing series, CSOonline looks at ways to ensure the best security possible during a recession.*

Jeremy Moskowitz calls himself the king of free. He's built an entire business around the notion that IT can be done on the cheap without damaging quality or security.

Given the current state of the economy, the self-described "chief propeller head" of IT consultancy Moskowitz, Inc. is finding that his do-it-for-free philosophy is a lot more popular than it was even a year ago, when there was more money to go around and companies were looking to buy top-of-the-line IT products - including the latest and greatest security tools.

With recession on the horizon, security pros in particular are searching for ways to control costs without letting their company defenses crumble in the process.

"Reducing the number of systems that require safeguards and controls means fewer anti-malware licenses, less patch management time, less backup space for recovery, and fewer security tokens"
Security Architect James DeLuccia
Many have found they can maintain strong security with a litany of low-cost or free software programs. But, Moskowitz says, many companies already have all the necessary security muscle without realizing it. And much of it resides in the Microsoft's Active Directory, which is being used by a vast majority of organizations.

"If you want cost effectiveness, you already paid for it. You have the Ferrari, now learn some stunts," he says. For example, he notes, Microsoft's Group Policy has 21 functions to manage access, lock down services and block malware. But most people don't know how use them very well. "That's why I have this job," he says, half-jokingly.

Microsoft security for the taking
Given all the attacks that have targeted Microsoft security holes over the years, some might find Moskowitz's position hard to swallow. Though Microsoft has poured an endless supply of money and manpower into security in the last six years, the bad guys are still finding ways to target the software giant's user base. Just last week Symantec Corp. was sounding the alarm over fresh attacks against a flaw in Microsoft Word.

Though the security challenges continue for the software giant, Moskowitz says it would be silly to discount the variety of ways Group Policy and other features can be used to bolster defenses for free.

One example of a tool waiting to be exploited is Microsoft's Group Policy Preference Extensions (formerly PolicyMaker Standard Edition and PolicyMaker Share Manager by DesktopStandard).

"Microsoft bought DesktopStandard last year and gave it to its Group Policy customers for free," he says. "It has tons of new functionality, one of which lets you change local administrative password accounts. It

can cost thousands of dollars to buy a tool to do that, but this is free."

Moskowitz has written two books on how to make the most of Group Policy, and he has made a believer out of Keith Gosselin, information technology officer at Biddeford Savings Bank in Maine.

"Group Policy, if properly utilized, is an effective way to lock down workstations that are typically your weakest security link," says Gosselin.

Gosselin has also come to rely on other Microsoft tools to maximize security without spending extra money. One is the Microsoft Baseline Security Analyzer (MBSA), designed to help small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations. Another is Windows Server Update Services (WSUS), which most Windows-based IT environments use for the automated deployment of Microsoft security patches.

Security through open source

As useful and cheap as Microsoft's embedded security has become, IT shops have turned to the open source community to flesh out the security arsenal without breaking the budget. Gosselin, for example, uses the open-source Nessus Security Scanner maintained by Tenable Network Security. "The free version of Nessus is a great way to get a handle on network vulnerabilities," Gosselin says.

Joseph Guarino, CEO and senior consultant for Boston-based Evolutionary IT, which specializes in security tools and management, is a big advocate of open source security. He notes that a free open source tool exists for just about every piece of the security market.

"Free and open source software has always had an essential role in information security," he says. "It's always been a building block for best-of-breed solutions as well as a source of innovation for things to come."

In an e-mail, he offered this list of examples:

- **Open BSD**, operating systems built with security as its primary objective.
- **Linux**, which has a history of high-quality, stable and secure code, making this OS a vital building block on which to build security infrastructure. Most security appliance solutions are built upon it, Guarino notes.
- **Snort**, the open source IDS tool maintained by Sourcefire, among the most widely deployed IDS tools around.
- **Wireshark**, a high-quality open source protocol analyzer.
- **OpenVPN**, a full-featured SSL VPN.

Eliminate complexity

As companies seek out cheap security tools to keep the bad guys at bay, some industry experts worry that the zeal to collect more technology has led to a bloated IT infrastructure. Atlanta-based strategic architect James DeLuccia is among those who yearn for more simplicity in security. A recession is as good a time as any to achieve that, he says.

"Organizations in hearty growth phases generally turn a blind eye towards the ability to leverage existing resources, which results in excess throughout the IT ecosystem," he says. "In times of belt tightening, technology teams should fully vet all of the ongoing IT services. This simple review will identify hardware and software that can be retired and simplify the amount of machinery that needs protecting."

He said the net effect includes:

- Reduced power bills because you are running fewer systems.
- Lower human capital costs - less systems to maintain, upgrade, and service.
- Reduced facility costs in hot/standby data centers that mimic primary data centers.
- Reduced number of software licenses that need to renewed, which means lower maintenance fees.

"Reducing the number of systems that require safeguards and controls means fewer anti-malware licenses, less patch management time, less backup space for recovery, and fewer security tokens," DeLuccia says.