

## A QuickStart Guide to Proactive Network Security

by Gary S. Miliefsky, CISSP®, September, 2005

Commentary--Behind our daily barrage of hacker attacks, announcements of new viruses and worms, and frequent risk of downtime is an opportunity. This is your opportunity to step away from the noise, for a moment, and take steps to build a more proactive network security model for your organization.

Countermeasures like firewalls or anti-anything (antivirus, anti-spam, anti-spyware, etc.) are all reactive security tools. They are necessary countermeasures and a part of a comprehensive security system, but you must also take action, be proactive, to ensure the highest level of network security. Daily vigilance is key. But it's nearly impossible to watch your network all the time.

Before you pursue proactive network security, you need to understand the commonly used four pillars of network security. These pillars are firewalls, VPNs, antivirus software, and intrusion detection systems (IDS). Firewalls inspect packets and attempt to block bad packets, but they cannot recognize an attack or may block legitimate access. VPNs create secure tunnels between insecure computers, but they don't protect network assets. Antivirus has its role and, vital as it is, it cannot close the vulnerabilities that would prevent an attack. Finally, intrusion detection systems (IDS) are purely reactive, dealing with an attack after it has occurred.

While these four pillars of network security are critical to your organization, the fact is, a single enterprise can spend thousands on firewalls, VPNs, antivirus and IDS systems, while the real network security culprits, "Common Vulnerabilities and Exposures" (CVEs), go



PREEMPTIVE, PROACTIVE PROTECTION.™

largely undetected. CVEs are essentially holes in applications that can be attacked by hackers and cyber terrorists to steal information or bring down networks. CVEs are a real problem and according to the 2004 E-Crime Survey are the systemic cause of over 90 percent of all network security breaches.

Proactive network security is the act of managing the four pillars of network security so that you get the most performance from them while at the same time augmenting your system with a vulnerability management system. A more effective firewall is going to block the right traffic. A more effective antivirus program is going to have less work to do, because viruses will have fewer opportunities to attack your systems. The IDS will become a backup system, rarely forced to sound an alarm that someone has actually gotten past your secure threshold. But preventing the attack with a vulnerability management system to eliminate CVEs is the most important component.

Why? According to the same survey 95 percent of all security breaches result from known vulnerabilities and misconfigurations. In reality, it just plain makes more sense to lock the doors and keep intruders out than to solve the problems after intruders have already broken in. You wouldn't leave your house unlocked, so why leave your network unlocked?

#### *Achieving proactive network security*

So as an organization how can you protect your network? There are many simple steps you can take to proactively secure your network. First you should develop a security policy and force folks to adhere to it. To do this, you should lock down all mobile devices and turn on wireless encryption to utilize inherent security technology. Patching your wireless router is critical and you should work with your firewall to ensure it is secure. Then move onto common vulnerabilities ensuring you know which vulnerabilities exist on your network and closing them immediately so that hackers can't access your business critical information or take down your network preventing you from doing business.

Detail of these steps is below:

### *Develop a security policy*

Good network security always starts with a living security policy. Even if it is one page, it should be an outline of security practices that every executive in the organization agrees to live by. Basic rules should include guidelines for everything from user access and passwords to business continuity planning and disaster recovery planning (BCP and DRP). For example, you should have policies in place for backing up financials and confidential customer records as well as mirroring systems to be better prepared, proactively, in the event of a disaster. In some cases, your BCP and DRP may even require a 'cold' or 'warm' site where you can quickly relocate your staff to continue operations after a disaster or terrorist attack. Implementing a corporate security policy is the first step in achieving proactive network security.

### *Reduce violations of security policy*

Violations of good security policy that commonly occur in wired systems as well as on laptops and wireless devices are a lack of antivirus software, no firewall, peer to peer programs installed (such as Kazaa, Napster, or Gnutella), and instant messaging all capable of creating security holes. You need to install antivirus, turn on the built-in firewall in Windows XP or purchase and install a commercial grade desktop firewall and be sure to remove peer-to-peer programs and instant messaging software.

### *Lock down mobile devices*

One of the greatest threats to security is laptops and other mobile devices that need and deserve legitimate access to your network, but often pose a threat to that network because of the very characteristic that gives them value--their mobility, which allows them to plug in to other networks and be exposed to threats. Wireless devices fall into the same category as laptops.



According to Forrester Research, there will be 35 million remote users by 2005 and 15 billion devices on the Internet by 2010. You don't have to be a mathematician to see that the numbers indicate multitudes of possible interconnection paths will exist, increasing the magnitude of a potential attack. And every system is potentially susceptible to access by unauthorized individuals.

You need to lock down your network by having a policy and systems in place that quickly determine that mobile devices have plugged in, then audit those devices for violations of the security policy and known vulnerabilities as soon as possible.

### *Turn on wireless encryption*

On wireless systems, Wireless Encryption (WEP) should be turned on and set at the highest level. Administrative username and passwords need to be changed immediately and frequently. However, even this may not be enough to stop hackers and cyber hijackers from breaking into your physical LAN through the wireless router. The reason is that there are specific CVEs in most wireless routers that have not yet been fixed. Good hackers can download free tools to take advantage of these weak spots and break through your security.

### *Patch your wireless router, use its firewall*

Another strong recommendation would be to get the latest patch or firmware upgrade for your wireless router and, if you can buy one that comes with a built-in firewall, learn how to use it and properly configure it. You can also limit the number of users allowed in through your wireless router at any one time. If you have only a few employees, why leave it set at the default (which might be unlimited)? Set it to as low a number as possible so that only your staff should have access.

### *Work with your firewall*

Although firewalls are not going to implement proactive security for you, they can certainly be employed in the best ways possible to do their part.

You should have intelligent firewall rules that help close traffic to potentially vulnerable ports. For instance, Port 1045 was (and still is) used by the SASSER worm, so you should be sure to have a firewall rule that closes traffic to that port on all systems. It also needs to be a dynamic rule that closes traffic to that port on laptops and wireless devices when they plug in.

### *Download/Install commercial grade security tools*

There are many free tools available for download that can help you secure your network. They range from policy templates to antivirus scanning and anti-spyware. Microsoft also offers vulnerability management updates. All of these tools can be an effective augmentation to your existing security measures and should be utilized to their fullest extent.

### *Disable potentially exploitable objects*

A "Browser Helper Object" is utilized by browser developers to do things like monitor page navigation and monitor and control file downloading. These BHOs are often installed on your system without your knowledge and because they pull information from the outside onto your computer, they are a threat to your security. Some companies go out of their way to hide the presence of the spyware BHOs that they install. They go so far as to find ways around the most popular detection tools by changing their product regularly just enough to avoid detection until the next version of the detection software comes out. To see all BHOs you have installed on your machine right now, you can install [BHODemon](#) from Definitive Solutions.

The ADODB stream object is the engine that allows BHOs to work with Internet Explorer. You should disable the ADODB stream object to stop BHOs from being able to write files, run programs, and take virtually any action on your host. To disable the engine, visit

<http://support.microsoft.com/default.aspx?kbid=870669>



PREEMPTIVE, PROACTIVE PROTECTION.™

*Keep up with the latest threats*

According to the Computer Security Institute (CSI), the results of the 2002 CSI/FBI Computer Crime and Security Survey indicate that "the threat from computer crime and other information security breaches continues unabated and the financial toll is mounting." You need to keep up with the latest threats to networks to keep your business safe. They are posted in many places on the web, starting with [www.us-cert.gov](http://www.us-cert.gov) and [www.sans.org](http://www.sans.org).

*Close known vulnerabilities.*

Known weaknesses in systems are called Common Vulnerabilities and Exposures (CVEs), compiled and documented by the MITRE organization. These vulnerabilities should be eliminated from every system on your network by applying patches or taking other actions, as required. Technology is available to automatically detect and eliminate CVEs®. More information is detailed at the [cve.mitre.org](http://cve.mitre.org) web site.

In summary, proactive network security for your business starts with good security policies. Next, you need to make sure you take action and implement these policies. Finally, as your business and network are dynamic in nature and ever changing, you need to be one step ahead of the hackers, worms, malicious insiders and cyber terrorists that are lurking around every corner of cyberspace. To do this, you must proactively enforce and update your policies, then make sure you have the proper countermeasures installed and running to thwart their every attempt.

You will never be 100 percent secure, but you will be standing on solid ground.

A handwritten signature in black ink, appearing to read "Gary S. Miliefsky".

Gary S. Miliefsky, CISSP®



Gary Miliefsky has over 20 years of experience as an entrepreneur, computer scientist and trained security professional. He has been CEO and/or CTO of 3 start-up ventures. At QuickBuy, Inc. he raised over \$10M in strategic and venture funding, personally recruited key team members, filed 6 patents, sold a \$0.5 million technology license deal to the president of Computer Associates, Inc. and drove revenues to over \$1M in the first year. At Netwave Technologies, he co-developed an Internet security technology that was licensed to N2H2, subsequently acquired by Secure Computing (NASDAQ:SCUR).

Mr. Miliefsky has also successfully brought new products and technologies to market for Fortune 500 companies, including a multi-million dollar executive information system for AIG, Lotus and DEC. At Wang Laboratories, Inc. he led a team to deliver in record time his new Internet fax invention for the Wang Open/image product line, deployed in over 40 countries in 14 languages and subsequently acquired by Kodak.

Mr. Miliefsky received his undergraduate degree from UMASS Lowell in Computer Science, and has subsequently earned certification as a CISSP®. He helped the White House develop their Internet Safety program for families and the recent National Strategy to Secure CyberSpace, advising the President's Critical Infrastructure Board. He is a Founding Member of the Department of Homeland Security and a member of MITRE's CVE/OVAL advisory team. He holds six e-commerce patents and has 3 network security patents pending. He has been written about twice in *Fortune magazine*, and has been seen and heard in *CIO magazine*, *Red Herring*, *Information Week*, *USA Today*, *the Washington Post*, *Washington Times*, *the New York Post*, *ZDNet*, *PCWeek* and *PCWeek Radio*, *Into Tomorrow* radio talk show, *the Boston Business Journal*, and *Mass High Tech*.