

A Holistic Approach to Incident Prevention

by: Stephen Hendrie, 08/24/2004

<http://www.securitydocs.com/library/2468>

Introduction

As IT Security professionals struggle to respond to the increasing threats posed against their networks, too often, the approach taken consists of various silo projects aimed at eliminating one potential threat at a time. This often leads to a very disjointed security architecture that can leave the security professional no better off than when he started, with just a lot less money in the budget. The goal of this paper is to introduce the various components of Incident Detection and Prevention architecture and to show how taking a step back and looking at the big picture you can best leverage various solutions to protect your network. The term incident prevention in this paper is used to describe the complete array of technology used to avoid a compromise and is different from the concept of Intrusion Prevention.

Core Incident Prevention Components

There are five core components of a complete Incident Detection & Prevention strategy. Though many solutions are marketed with different package names, terminology and marketing buzzwords, they basically can all be placed into one of the following categories.

Vulnerability Assessment & Scanners: These tools are used to identify potential vulnerabilities or exploits on your network. Usually, they scan devices remotely looking for known exposures and are able to alert you to items that require action. They are an essential part of a proactive organization's efforts to minimize risk to their network.

Anti-Virus: Used to identify, prevent or remove known virus and worm signatures. Usually deployed on hosts (client or servers) but can also be incorporated into e-mail servers and web access systems like proxy servers or firewalls.

Firewalls: Used to regulate network traffic between network points. Firewalls are most widely deployed between a private corporate network and the Internet but they can also be used to control access within an intranet as well. For example they could be used to provide unwanted access to financial systems or manufacturing production control networks. Firewalls can also be deployed on client or server computers, providing a level of protection to or from the network directly on the client. Client computers that connect to the Internet for remote Access VPN are a prime case for implementing such a solution.

Network Intrusion Detection / Prevention: Also known as network based IDS or IPS, this technology relies on network sensors placed at strategic locations on your network. They have the ability to analyze network traffic for unwanted or malicious activity and alert you as to the potential intrusion attempt. In the case of IPS (Incident Prevention Systems), you gain the added benefit of having the system automatically stop this traffic when it sees it. Though this functionality is present, you should not confuse IPS as being the same as a firewall; rather IPS is potentially an extension to a firewall's functionality and, in fact, many firewall products have expanded their functionality to include IPS capabilities. Also important to note is that many products traditionally referred to as IDS now include IPS functionality as well. Having this understanding should help you separate fact from fiction in product marketing when evaluating your own solution.

Host Based Intrusion Detection: Host Based Intrusion Detection or Host based IDS is similar to network IDS with the difference being that it sits on a server or workstation. This allows for a layer of protection at the actual device should an attacker compromise it. These solutions typically allow for monitoring of such activity as account modification, file system changes, log file activity, application or system level configuration changes, etc. They can be very effective at identifying potentially malicious activity on controlled systems where these types of activities should not be occurring. Additionally, should a system be compromised, these technologies can provide a wealth of forensics information, making the assessment phase of your investigation easier.

The Holistic Approach

Now, as identified earlier, the problem we are facing is that too often we are forced to look at these solutions one piece at a time. This can be due to numerous factors such as budgeting constraints, prioritization or other resource issues. It is a normal part of business life that cannot be avoided. However, what can be avoided is having a hodgepodge of security tools at the end of it all that you would rather throw out the window than actually rely on for your networks protection.

Aside from the normal requirements for a solution (quality vendor, quality product, quality support, etc), there are three major items to consider when evaluating your solution:

- **Integration :** Most mature security solutions are now available as suites designed to cover multiple sections of the core components. Having solutions that can integrate with one another or with other systems on your network will be extremely beneficial in the long run. Examples of integration are IPS integration with firewalls, vulnerability definitions that are shared across multiple technologies for single sourced configurations or virus scanning integrated with e-mail servers or web proxies.
- **Administration :** Obviously, you want a solution that is as easy to administer as possible. Many vendors have taken this a step further by actually providing a means of central administration across numerous core category components. An obvious benefit can quickly be seen if the product allows you to configure host based, network based and access control policies from a central interface.
- **Correlation :** This is arguably the most important of the three categories. Any successful security product is going to gather a lot of information. Often times in security, the more information the better. Being able to tie this information together from various sources will allow you to get the most out of your security investment. This will be discussed in further detail later.

These three points are relevant even if you are only evaluating a small piece of the complete solution. Considering how you may be able to leverage or integrate this new component with your existing infrastructure is going to go a long way to reducing management issues down the road. Likewise, you should also consider your future requirements. Though you may only be looking at a single component at the moment, you want to make sure the solution that you select offers the ability to scale and integrate additional components at a later date to allow for new requirements that are bound to surface.

Correlation

Event correlation has been a dream of the security industry for years, but it has only recently begun to mature to the point that it is bringing true value to security solutions. As mentioned before, event correlation is probably the most important component of a holistic solution. This is where the true benefits of this approach can be realized.

The idea behind event correlation is to consolidate your logging information into one location so that it

can be analyzed as a whole. Many of today's security vendors offer varying degrees of event correlation.

Using the 5 core components identified earlier, it is easy to see how event correlation can be of extreme importance when troubleshooting an event. To put this together, let's look at a potential scenario with a network that has numerous security components installed.

Let's start by assuming that a vulnerability assessment tool has been deployed. This tool runs regular scans of your network devices, checking them for exposures that it is made constantly aware of through regular updates. It inventories all of your systems with known security exposures and alerts you to the action required for these devices. Let's also assume, for the moment, that you do not take the necessary action to correct these vulnerabilities immediately.

Next, a new worm is launched on the Internet that exploits this vulnerability. You get the call that there is suspicious activity on your network and you start your investigation. Assuming that your environment has been configured as described in this paper, you log into your central console to see what is going on.

With an integrated security solution, what you would see could very well give you the following information all from one location:

- You have 10 servers and 100 clients vulnerable to the attack
- Your anti-virus was unable to protect against this signature because it was network based.
- Your network scanners have recorded the activity and you now can see on exactly what networks the worm has been observed.
- Your host based scanners have recorded anomalous activity that matches the known attack signature and you now also know what machines have been infected.
- Your IPS enabled firewalls have been triggered and the worm has been contained.

As you can see, central administration and integration could play important roles in the above scenario too. The benefits of an integrated holistic solution are immeasurable when compared to an environment that has built each of these components individually, without regard to other technologies.

Worth mentioning as well are other bonuses of integration. For example, with an integrated solution, host based firewalls can automatically be configured to block an attack that was detected by other sensors or vulnerability scanners. This allows for your network to become smart and defend itself in the event of an attack attempt.

Summary

How you plan and implement various security tools is very important to the usability and effectiveness of these tools over time. It is important to keep your end goal in mind when evaluating even the smallest piece of your security tool arsenal.

Keeping integration, administration and correlation in mind will help to ensure that you are moving in the right direction from the start. Knowing that you are selecting a solution that is strong in these three categories will allow you to grow, manage and protect with ease.

Remember, any effective security practice requires more than technology. Policies and procedures need to be created, implemented and enforced. Additionally, no technology solution can ever replace user education and awareness. These components are instrumental under any circumstances and should always be considered a top priority for any organization looking to protect its networked resources.

[SteveHendrie.com Security Web Site](#)