

Anti-Virus Defence In Depth

Ken Bechtel 2003-04-22

Lately it seems I can't open my inbox with out seeing a new article on defence in depth. This is fine: defence in depth is crucial to anti-virus protection. Unfortunately, most of the articles are missing two crucial components. To understand what is being missed, we need to look at what is meant by defence in depth as it applies in the malicious software world. For the purpose of this paper, when referring to defence in depth, we will be specifically talking about the utilization of anti-virus software, and other methods to provide a multi-layered anti-malware defence in a corporate environment.

In discussing defence in depth, we are really talking about protecting systems at three levels:

- desktop and remote users, which I like to call level 1 users;
- file and print servers, application servers, database, email, and web servers, which I refer to as level 2 devices; and,
- level three, or perimeter devices, such as mail gateways, proxy servers, VPN hosts, and other choke points.

I personally like to include home users with level one devices, and make it a point to negotiate this with my anti-virus vendor. After all, many people take work home with them and are encouraged to do so by management; what happens when they bring that work back to the office?

When I first became aware of the concept of defence in depth, the extent of depth was servers and workstations. At that time, most people felt that it was cost ineffective to protect both layers. I remember some very big, established names making very public statements of how we didn't need anti-virus software on servers, as it only added overhead, and offered little protection since a majority of viruses are boot sector infectors. These people were industry insiders and very respected "experts" at the time.

Today, security people are preaching to protect every layer of the infrastructure. Identify your choke points and possible virus entry points and make sure you have anti-virus installed and up-to-date. There's nothing wrong with that as far as it goes. For you and I this should be basic. Sorry to offend anyone, but this is entry-level anti-malware stuff. Two key components of proper defence in depth are often overlooked: the first being centralized reporting and control,

and the second is what I refer to as fishing with a net, not a line.

Fishing with a Net: Best of Breed and Content Filtering

Let's look at the second issue first as it's the more easily addressed. It is a well-known fact when you go fishing, you catch more fish with a net than you do with a line and pole. In computer science this is known as redundancy. When one part fails, you have a second system in place to pick-up where the first one left off. In terms of anti-virus protection, many people argue that you should pick the best of breed anti-virus software, so that if anything fails you only have one vendor to take to task.

This would be a fine approach if there were a clear leader in the market that was strong on all platforms. Unfortunately, this is not the case. For the purpose of this discussion, let's just look at organizations that employ Microsoft windows across the enterprise. Such an organization would rely on Windows file and print, as well as application servers, Windows is the desktop system and Exchange is the email. Based on independent reviews, we see several industry leaders that do all these platforms "well" or good enough; however, we can also see that one vendor is best of breed in the Exchange environment, while another vendor is better for the desktop, and a third vendor does is the most effective on server class machines. Add into the mix the fact that many medium and large companies, also use multiple flavors of *nix, and you totally upset the apple cart.

Further complicating matters is that different AV solutions use different approaches. Some anti-virus companies will detect "families" of viruses by using a strong heuristics base. These vendors may be able to detect and catch new viruses with out specific samples. Other companies prefer the scientific method of exact identification, which enables the AV program to be more precise, more rigorous. Heuristics has the drawbacks of increased overhead and more false positives, while exact identification will allow minor variations to slip through the net, not to mention 0-day viruses. Since our interest is in protecting corporate resources it is incumbent upon us to seek the best possible solution.

While it costs more money up front and it may require coordination with multiple vendors, the best approach I've found is to use the best of breed for each layer, or at least as many layers as possible. For example, you may employ one vendor's products on the proxy servers and mail gateway, while a second on the exchange servers, file and prints, and desktops. This is defence in depth at a very minimal level. This way if a virus slips through one product, a second one is

in place that prevents further proliferation within the company or, even worse, outside the company.

One of the worst tasks in security administration is cleaning a system after virus infection. Once the malicious code is in, it's there for a long time, and by depending on one anti-virus package it may be a while before the admin knows the system is infected. By using two or more products on different levels, you are increasing your chance of getting timely notification of infection, thus increasing your reaction time, and getting BOTH vendors to detect what ever is coming in.

Along with traditional virus scanning, true defence in depth requires some type of non-traditional anti-malware practices like content filtering. Although a non-traditional approach to anti-virus defence, blocking a list of known executable code such as .exe, .com, and .bat files has significantly limited the spread of computer malware. The average user has no need to receive this type of file, either through via email, zip files, or buy downloading from Web sites. Content filtering can make the file available to the end user without giving them the ability to automatically "launch" the potentially malicious code. Content filtering offers the added benefit of removing unwanted junkware that uses company bandwidth and consumes email storage space.

Content filtering is also advisable on the proxy server level, as there are an increasing number of hostile Java Script and Active-X components. Blocking them at the proxy level keeps them from potentially infecting a host system and spreading to other systems within the company.

Centralized Reporting and Control

Now the biggest issue, in my mind, is the lack of central control. I can no longer count how many times I've heard that a certain workgroup needs to be in control of the anti-virus product because they are responsible for the application or the servers. They typically argue that they're the ones called on the carpet when it's unavailable. Yet these same people are not held accountable when a virus gets into the company and becomes an outbreak, even though it may have entered the system because they did not keep the virus definitions up-to-date, disabled the anti-virus software for one reason or another, or created issues because they failed to follow established procedures.

Many companies do not have a central point of contact for malware issues. They may have an

experienced desktop support person who is the "go-to" guru for virus and anti-virus issues on that platform, but no corporate "architect" to oversee the strategy. There are even some companies who have an individual in the computer security division, but who has no authority for enforcement. These companies do not have the information to tell them where the viruses are coming from, and do not have a clear goal or information to formulate a strategy to protect corporate assets. More importantly, they do not have a central person or group to ensure that all necessary anti-virus provisions are in place. Nor do they have any central person or group who is charged with detecting, containing and responding to an incident.

In this environment, it is easy to become complacent. Since each workgroup is responsible for its own policies and procedures, it becomes easy to assume that they are surely maintaining them. In fact, the reverse is often true. To ensure "availability" of the services required to fulfill the work group's objectives, it is often easier to shut down the anti-virus service than to troubleshoot any issues arising with the AV. For example, a work group may notice that the anti-virus is taking up 80% of CPU usage. Is this because that machine is having to work extra hard cleaning/ preventing infections, or has something happened to cause the software to "break"? Rather than taking the time to determine the root cause of the problem, the first reaction is disable or uninstall the anti-virus software, then spend several days weeks or months in a test environment to determine the cause. During that timeframe the systems are unprotected and becoming a very virus rich environment.

When building a defence in depth, this must be taken into account. Almost all AV vendors now have a central console that allows reporting to an anti-virus administrator. These consoles can generate reports on issues as mundane as the number of machines that are running current anti-virus and how many have not communicated to the central server in a defined period of time, as well as the strategically important virus infection information. By evaluating the detection reports you'll be able to determine the weak points in your defences. You'll also have the ability to detect workgroups that are disabling or misconfiguring the software. The offending parties must then be held accountable. This can be justified by showing management that it takes more than three times the manpower hours to clean an infection as it does to prevent it.

When you look at centralization, you also gain several strengths, in addition to offsetting the negatives we've already discussed. One of these is the ability to perform patch management, or identify the machines that need to have patches applied. Some may not think this is part of an anti-malware strategy, but keep in mind that 80% of viruses use exploits that have had patches released for three or more months. SQL Slammer is one example, companies using a

centralized structure that knew their patch level, suffered less than organizations that did not.

Centralized reporting offers administrators the ability to report with confidence to their management the current level of compliance. With this, I challenge anyone to tell me, or anyone else, with a degree of reliability, what is the percentage of their machines that are up-to-date with their anti-virus product? The centralized reporting scheme gives us current data, to show us how protected we are, rather than how protected we think we are.

Having an established central point of contact also establishes a single authority responsible for protecting corporate assets in case of virus infection. By making this an item of responsibility, it is now quantifiable, and since no one likes to fail, steps will be taken to prevent outbreaks, as well as holding everyone to the established policies and procedures, cutting the losses from outbreaks. By appointing a central authority, the organization can establish a standard response to viral incidents, thereby ensuring that in case of infection, the damage can be mitigated and the infection contained.

Conclusion

Defence in depth is more than protecting at every layer of potential penetration. It is a concerted effort of using the best of breed on each platform and at every level of the organization's systems, using content filtering to reduce the risk of non-traditional malicious code infection, and using a centralized reporting and authority to manage the anti-virus protection strategy.

One final point I'd like to discuss, as it can't be said enough is user education. While this is often considered not a part of a formal defence in depth, user training may also be considered your first line of defence. There will always be users who can't be bothered to learn, or apply their knowledge; but many more are willing, and this will pay off in volumes. While not all companies have "experts" in malware as employees, the best practices will still protect them, and defence in depth is required even more for them. The only way to ensure that these requirements are fulfilled is through thorough, effective user education.

Ken Bechtel has been involved in Anti-Virus research and corporate support since 1988. He is a founding member of [AVIEN](#), a [WildList](#) reporter and a member of [AVAR](#). He likes to work outside the "established field" to bring maximum payoff to his clients.

[Privacy Statement](#)

Copyright 2006, SecurityFocus