

June 2, 2004

Marc Maiffret
Chief Hacking Officer
eEye Digital Security

Congressional Subcommittee Testimony on Security Threats to Public and Private U.S. Infrastructure

Vulnerability Management Strategies and Technology

For some time, security has been a race to create new protection mechanisms for a never-ending onslaught of vulnerabilities. Vulnerabilities are at the core of what makes systems insecure. However, the vulnerabilities that organizations face are not simply system/software vulnerabilities, but also social vulnerabilities in how people interact with technology. Until not long ago most organizations were winning the security race, because the “bad guys” were letting them. Things have changed though, attackers have become smarter, and the race is over. The “good guys” have lost, for now, and there has never been a better time to be a criminal.

One of the main reasons for the “good guys” losing this battle is due to the fact that security has always been reactionary. With the current trends in vulnerabilities, there is no time to react. It is important to emphasize the reactionary state of security to help better understand the dynamics of why we are failing.

Patches Aren't Always The Answer

If you casually look at the available studies and statistics you can easily point the blame at organizations for not patching their systems. Then again, you can also read newer studies which say patching is not enough - you cannot patch in a reasonable amount of time before new threats emerge (worms, viruses, exploits, etc.). Others say that it is not a problem of not patching or not patching fast enough, but there is an increase in “zero-day” vulnerabilities or threats that take advantage of non-public vulnerabilities which do not yet have patches. Keeping all of these dynamics in mind, you have to realize that the threat of vulnerabilities, which can be fixed through patches, is only one of a few different types of vulnerabilities that organizations face. Organizations are also vulnerable to various software/system configuration vulnerabilities, as well as social vulnerabilities.

Misconfigurations and social vulnerabilities are the most publicized types of attacks, and also the least. Virus attacks are one form of social vulnerability that is typically made very public. Viruses are able to propagate from system to system based on human interaction with software in a way that is harmful to the system the software is running on. The problem then escalates from one infected system to entire companies and groups of computer users. There are other types of vulnerabilities in software and systems that can be leveraged by attackers who take advantage of misconfiguration weaknesses in order to gain access to resources that attackers shouldn't otherwise have

access to. One recent example of this is when internal memos from the Senate Judiciary Committee were compromised. I'm sure you're all familiar with that particular instance. A solid Vulnerability Management plan will also cover the aspects of policy and compliance, user education and various other security facets beyond simple patch remediation.

Security According to Specific Needs

Vulnerability management should be at the heart of every organization's security strategy. Most organizations would love to have the single silver bullet for vulnerability management. While security companies will all claim that they offer it, there is no one solution. Instead, one of the most important aspects of creating a good vulnerability management plan is to first understand what is critical within your organization. From the private sector to the public, from financial services to health care, there are many differences in what is critical within an organization, and therefore different security requirements.

One of the first things to accept in securing a large enterprise is that the odds of being impervious to attack are against you. This is as good as a drunken road-trip to Vegas and betting your next house payment on black. There are no two ways around it; the odds that there will always be a way for a hacker to penetrate your network are against you. That is why it is important to understand what is critical within your organization and focus on those critical points first, before trying to tackle the security of your organization in its entirety. Obviously there are various levels of security a company can obtain, and with that, there are various layers of security that are required to advance to the next level. To understand what layers of security are required for your organization to reach various levels of security, you must first understand the types of threats your organization could possibly face.

Imagine for a moment that there are potentially thousands and thousands of people who live for "the thrill of the hack." From the young boy working all hours of the night to find that next vulnerable system to the next virus writer hoping to see their work made public around the world, there are many different types of computer criminals, and for the most part none of them seem to care which computers they target. Now take that image of computer "criminals" and never think of it again. Times have changed. Though some things have remained the same, the motivation and people behind computer intrusions has drastically changed.

As with any "free" and open system (computers, networks, Internet, etc.), that relies heavily on trust, the fun has to eventually come to an end. The "bad guys" have grown all too knowledgeable about the fact that technology is creating new opportunities to profit and proliferate from the same common criminal ideas that have existed for many years. This is all very evident by the investigations into various online fraud activities performed by the Federal Bureau of Investigation, many of which lead back to various countries where organized crime is able to operate more freely because of lax computer security laws and poor relations with the United States. There are other attacks, beyond simple online fraud, that are more sophisticated. Attacks that target specific companies and leverage things unique about an organization in order for an attacker to acquire whatever it is they are after. Regardless, if you want to believe the "boogeyman" stories

of organized crime or foreign nations breaking into your computer networks, the one attacker that almost all organizations have met with face-to-face is the computer worm.

A computer worm is a program that leverages a “vulnerability” (typically found in software) to replicate itself from one computer to another without requiring any human interaction. Depending on the computer worm, there is sometimes a “payload” that is included with it. Payloads can be anything from malicious code that uses thousands of worms to create a coordinated attack against a target system, or a payload could simply attempt to disrupt or destroy data on infected systems. While the idea of computer worms sounds scary, the idea is nothing new.

Computer worms have been around for some time now. However, they are becoming more and more popular and seemingly easier to produce than ever before. One of the first known records of a computer worm stems all the way back to 1988 when Robert T. Morris Jr. released the first computer worm, seemingly by accident. One interesting aspect of the first computer worm was not specifically about the worm itself but more so about the author. The father of Robert T. Morris Jr., at the time the worm was released, was none other than Robert Morris who was then the Chief Scientist of the National Security Agency (NSA). Some would later speculate whether or not Robert T. Morris Jr. came up with the concept of the computer worm on his own. While there is interesting mystique surrounding the first computer worm, we must remember one thing. The first computer worm was written over 16 years ago. We have had 16 years to think about, analyze and create solutions to guard against computer worms. So why after all of this time, are businesses constantly impacted by computer worms? More so, why are businesses still impacted by vulnerabilities?

Vulnerabilities Are Typically A Known Quantity

Vulnerabilities in software and systems are what allow computer worms to propagate in the first place. When a vulnerability is discovered, typically that vulnerability is reported to the manufacturer of the software in which the vulnerability is found. At that point, the software vendor begins to assess the risk that the vulnerability poses to its customers. In some cases, the vendor also assesses the risk of embarrassment they will endure in the media. After some time, the vendor will eventually release a security patch and security bulletin to notify its customers of the new risk and that they need to apply the relevant patch. Parallel to that, the security researchers who discovered the vulnerability will also release a security bulletin that describes the vulnerability and gives possible mitigation information that can be put in place until a patch is deployed. At this point, a vulnerability has been made public. From the patch itself, enough knowledge has been disseminated that allows attackers to create worms and exploits, or programs that can take advantage of a vulnerability to compromise computer systems running the vulnerable software. This is when security starts to fall apart in the vulnerability life cycle. The reason being, vulnerabilities are being exploited faster than organizations are able to react to them and patch their systems. Therefore, even the most security-astute organizations are still going to be impacted by worms and computer attackers.

Some people have equated the current “vulnerability lifecycle” in relation to the term OODA Loop, or Observation Orientation Decision Action Loop, which was first

coined by Col John Boyd, USAF (Ret). In relation to vulnerabilities, the idea of the OODA Loop is that if an attacker can get “inside” your OODA Loop they will have the upper hand, as organizations will not be able to properly respond to attacks and instead be left in a helpless and disoriented state. All analogous jargon aside, if exploits and worms are being released before organizations can react, organizations will continue to be impacted by the ever-growing number of threats.

Coming around full circle we know that having good vulnerability management means good security policy and compliance, user education and technologies that will allow your organization to regain control of the vulnerability lifecycle. There are many technology solutions and service providers that cover the various areas of vulnerability management. One of the first steps an organization must take is determining a trusted source to help them along their path of creating a good vulnerability management plan. Many organizations actually do have a wealth of security knowledge within them just waiting to be tapped into. An outsider’s perspective can also be helpful for organizations in determining their current security stance and critical business processes.

Angles Of Vulnerability Management

When it comes to vulnerability management, there are a few basic technologies with varying levels of sophistication. Most of the technology related to vulnerability management can be separated into two functional groups: perimeter and endpoint, or host-based, security. There is, however, one technology that plays an important part in both perimeter and endpoint security - vulnerability assessment. The first place that companies typically make an investment in security is around the perimeter of their network.

Perimeter security is one of the older forms of security which for many years has been made up of two main types of security solutions: firewalls and Intrusion Detection Systems. Firewalls were created to provide access controls on how systems are allowed to communicate with one another. While firewalls worked very well for their intended purpose, they eventually were not enough to handle all the new emerging threats. Based on that line of thinking, the idea of the Intrusion Detection System (IDS) was born.

IDS created a way to monitor all network communications for various attack patterns and then create notifications based around those attack patterns. Those notifications were then interpreted by an organization’s IT staff to determine whether or not a system really had been compromised. This technology is no longer a viable option as most organizations have realized that IDS requires too many personnel resources without much return on investment. From this failure and various market analysts proclaiming, “IDS is dead,” there was the birth of Intrusion Prevention Systems (IPS).

IPS is the next wave of perimeter security that aims to protect organizations from both known and unknown attacks. Unlike IDS, IPS is supposed to actually stop attacks, and not just notify organizations about them. Therefore, giving an increased level of security by blocking attacks around the perimeter of your network. The problem though is that many IPS solutions are nothing more than repackaged IDS solutions that have been repurposed to “block attacks” instead of just notifying organizations about attacks.

One of the fundamental flaws of IDS/IPS systems, regardless of whether or not they are able to block attacks, is that they protect against exploits and worms which are not necessarily the core of the security problem organizations face. Again, the core of the security problem is the vulnerabilities. Since IDS/IPS systems are protecting from exploits and worms, the threats, and not vulnerabilities specifically, they fall into the same vulnerability lifecycle trap that was described earlier. Again, your security is only as good as how quickly your IDS/IPS system can be updated. You might have gained a little bit of time in the race against attackers; however, in most cases you still have not gained enough time to win the race. In general, firewalls, IDS and IPS, do have their applicable uses and every company should, at the very least, be investing in perimeter security. It should, however, be understood very clearly that perimeter security is not enough. One of the reasons why perimeter security, no matter what kind (firewall, IDS, IPS, etc.), is not enough is because the dynamic nature of threats and business processes has created a plethora of ways that attackers, worms, etc. are able to find their way inside an organization's network.

Companies who have invested heavily in perimeter security are still being affected by various security threats for a few reasons. One of the reasons is that of remote and rogue computer users. Whether it's a user traveling with a laptop on the road or logging in from home, all too often, remote users' machines are being infected with worms, or "back-doored" by attackers. Eventually those remote users bring their systems back inside the organization, at that point, bypassing any perimeter security that is in place. Remote and rogue users are not the only ways perimeter security is being unknowingly bypassed these days. Other breaches in perimeter security are commonplace in relation to business processes that require two organizations to communicate between one another, often times from within each organization's perimeter. From these various deficiencies in perimeter security came the idea of endpoint security solutions.

Endpoint Security

Endpoint security will receive a great deal of attention over the next few years. This is because endpoint security solutions are providing security at the closest point to the digital assets that organizations are trying to protect. There are many types of endpoint security solutions and many of them are similar, if not identical, to some perimeter security solutions. Patch management solutions are also a part of endpoint security and are growing in popularity.

No one can deny that one of the most crucial things an organization needs to be doing for security is installing the latest security patches. There are many adequate solutions on the market today that allow for organizations to deploy patches across their environment with relative ease. When looking at patch management solutions, organizations need to be careful about the scalability of certain patch management solutions. While a patch management solution might seem like a great idea in concept or in a lab, many patch management systems start to break down and have problems when they are used on a network of any sort of large scale. Another deficiency in most patch management solutions is that their management capabilities, beyond even scalability,

have not been built with large organizations in mind. Patch management and remediation is not as simple as clicking a button and blasting a patch out to all the systems that need it, although that's how most patch management solutions work. Patch management is very much process-related, and the process of deploying patches changes depending on each organization. Even a scalable and process-oriented patch management solution is not going to be enough to protect your organization. Again, the current vulnerability lifecycle does not allow organizations enough time to patch before a new threat emerges. That does not mean you should not be looking into patch management or patching your systems...just don't bet the farm on it.

One security technology that has been pioneered recently has been that of Endpoint Vulnerability Protection. Endpoint Vulnerability Protection works by being able to understand the vulnerabilities that are used by exploits, worms and attackers. By truly protecting systems from vulnerabilities and not threats, EVP systems are able to protect systems automatically from new threats, before they arise. That is to say that when a vulnerability is released, an EVP system is then able to specifically protect a system from that vulnerability. So no matter what new threats, worms or otherwise, are released, your systems will already be protected ahead of time; therefore, giving you the advantage in the vulnerability lifecycle. This then allows you to deploy patches throughout your organization when it makes sense for your business. Your systems remain protected even without patches installed.

While endpoint security in some ways sounds like the silver bullet to security you must keep a few things in mind. First, there are many different types of endpoint systems that organizations need to protect: Windows, Linux, Apple, Unix, routers, and various other devices. Most endpoint security solutions do not offer support for all of these different platforms, and some platforms are simply impossible to create endpoint security solutions for, as they are proprietary. Also, endpoint security solutions are only going to protect systems that organizations know about and systems on which they can install endpoint agents. There is still the threat of rogue machines, machines that can't run the endpoint agent software, and various other instances where endpoint security is not applicable. These are just a few of the reasons that some of the largest organizations in the world rely on one of the oldest type of vulnerability management tools ever created: vulnerability assessment.

Vulnerability assessment is a solution that can provide organizations with a clear view of their current security stance, whether it is perimeter security, endpoint security, rogue devices, or security policy compliance. Vulnerability assessment allows you to view the security of your network from all angles and create a real-world view of how your organization is doing in terms of its risk to malicious attackers. Years ago, Vulnerability Assessment (VA) was mostly thought of as a quick-use security-consulting tool, and for the most part it was. Over time, VA solutions have evolved into enterprise-class security solutions that provide companies the real-time information they need to properly assess their security posture when new threats are discovered. Beyond that, VA solutions have evolved into more process-centric solutions that allow organizations to track vulnerabilities from their initial discovery all the way through their remediation. This allows organizations to have a better understanding of the types of vulnerabilities

they are facing, as well as management of the personnel and resources that are required to ascertain various levels of security.

One of the last technological building blocks of vulnerability management is a solution to manage the many processes that make up vulnerability management. Whether it's your perimeter security, endpoint intrusion prevention, or patch remediation, the various solutions for vulnerability management alone are not enough. Having the various tools to perform vulnerability management does not necessarily mean you have created the business processes to verify that everything is in compliance to your set standard. The end-to-end vulnerability management plan should include a solution to manage the process as a whole. Simply having vulnerability assessment, firewall, patch remediation tools, etc. is not enough. You need to have a process to track your organization's progress and verify that you are at some level of compliance relative to your business goals. Organizations must also remember that one of the most important natural resources and backbones of security and vulnerability management is the security researcher.

Security researchers come in many forms from the hobbyists staying up all hours of the night finding security bugs for fun to the paid employee working for a security company researching new vulnerabilities. No matter what type of security researcher, security researchers are critical assets in helping organizations gain a level of security. That is not to say every organization must have their own security researchers on staff, but organizations must remember that by wanting their systems to be secure, they are in part joining a security community made up of all types of people. Organizations must be wise in knowing what people and movements/ideas they should support. There are many battles that are waged between big business and the security researcher. The majority of time "big business" is the very companies who are writing insecure software and putting organizations/customers at risk, who would rather security researchers went silent. If no one talked about the problem, then there wouldn't be a problem.

Thinking Like A Criminal, For Greater Security

Looking to the past we can find instances where battles were staged. Organizations, researchers, companies, and even government, all took sides on debates about security. Had some of these debates gone truly sour, we would have seen a rippled effect that would have caused a giant set back to the security of organizations today. So what was one of these historical turning points where community decisions on security could have caused things to go horribly wrong? The birth of vulnerability assessment. One of the very first vulnerability assessment tools ever created was SATAN. When SATAN (System Administrators Tool for Analyzing Networks) was first created many organizations and institutions went into a bit of a panic. Some people got the idea in their head that the creation and public release of vulnerability assessment tools would allow for the "bad guys" to use the tools against organizations and therefore help the "bad guys" in their efforts to break into systems. The creators of the tool argued that the tool was needed by the "good guys" in order to be able to identify all the ways that the "bad guys" could break into systems and have information on how to fix those insecurities. The creators believed so strongly that they were doing what was right for security that at least one of the creators put their professional career at risk. A long time

before SATAN was created, “bad guys” had been using these types of tools to break into computer networks, but the “good guys” were never clued in to have the same tools as the “bad guys.” The idea of thinking like a criminal, to stop a criminal seemed a hard pill to swallow at the time. If you look at present day security you will see that vulnerability assessment tools are very common-place within organizations and are widely accepted as being one of the greatest network security tools. This is just one example that hopefully illustrates the need for organizations to stay in touch with security researchers, their ideas and their motivations. Where would organizations be now if vulnerability assessment tools had been outlawed? Where will organizations be tomorrow if free thinking and publication of vulnerability research and exploits were outlawed? Shouldn't we be more concerned, first and foremost, with the accountability of companies creating the insecure software? When the battle is waged between researchers and software vendors for accountability on both parties' parts (researches for their information and software vendors for their insecure software) where will your organization stand? Or will you not be informed enough to lend a hand in making sure computer security keeps progressing ahead of the “bad guys?”

This is a small taste of the world of vulnerability management, the many technologies that drive it and the social intricacies that will continue to mold it. Everyone is talking about security until we are all blue in the face. At the end of the day, I fear too many people are doing just that, talking. Security in my mind is still not a true priority for organizations. Organizations will all admit that security is the most important thing to their business, but when push comes to shove and business decisions are made, security still remains riding in the backseat of a broken down vehicle that is riding the information highway to nowhere.

Signed,
Marc Maiffret
Co-Founder/Chief Hacking Officer
eEye Digital Security