



Fact or Fiction Security Survival Guide: Clearing Up Misconceptions, Myths and Mistruths about Security

Thursday, June 26, 2008

www.lumension.com



The security space can be one of the most confusing territories to traverse as an IT decision-maker. These days there are just so many misconceptions about security's hot topics that it can sometimes be difficult to know what is true or false about security strategies and technologies anymore. Finding the right course of action can be difficult enough when the "map" has no key, let alone when that key is wrong.

When defining policies and reviewing different technologies it is imperative that you are making informed decisions, which is why we've endeavored to find some of the most shocking mistruths about endpoint security, vulnerability management and data protection. Here in this handy Fact or Fiction guide we've set the record straight about each misconception you're most likely to encounter while talking to colleagues or vendors.

Fact or Fiction – Breaking the Top 5 Misconceptions about Endpoint Security

Security experts have done a reasonable job over the past several years preaching to businesses about the increasingly porous nature of the enterprise network perimeter. Most organizations have gotten the message loud and clear, understanding the critical importance of enforcing security policies on the endpoints and shoring them up from attack.

Unfortunately, some enterprises have been less effective than others when acting on that message. This is because even in the wake of this increased enlightenment over the importance of endpoint security, there still remains many a misconception about the topic. We'd like to dispel a few of the biggest myths so that enterprises can better understand how to protect themselves from attacks against their clients.

Fiction: Endpoints are more secure today than they were before.

The Facts: Because most enterprises at this point have taken steps to protect their endpoints with traditional anti-virus, personal firewall, anti-spam and anti-spyware and other HIPS products, many within these organizations are under the mistaken impression that their endpoints are more secure today than in the past. The truth is that endpoints continue to be one of the elements within IT infrastructure most vulnerable to attack.



According to the SANS 2007 Top 20 Internet Security risks, "Critical vulnerabilities in software on personal computers inside and outside enterprises (client-side vulnerabilities) allowing these systems to be turned into zombies and recruited into botnets and also allowing them to be used as back doors for stealing information from and taking over servers inside large organizations" remain a top priority.

Unfortunately, traditional defenses that protect endpoints from attacks against these vulnerabilities are becoming increasingly ineffective as crafty attackers learn to beat them. According to Gartner, these signature-based technologies have less than a 50 percent chance of catching completely new threats and can miss up to 10 percent of old threats in the wild. The dilemma that these signature-based solutions face is that they try to block all of the bad processes from running rather than only allowing the good ones to operate. They simply can't keep up with all of the new attacks that crop up each day. And they certainly can't keep up with targeted attacks, for which signatures have not been created.

Fiction: Applications are becoming more inherently secure.

The Facts: As Microsoft and other experts have trumpeted the successes developers have had in hardening today's operating systems from attacks, hackers have gotten busy finding alternative attack vectors. Their particular favorite right now is through the application layer. The difficulty is that many organizations just don't understand how vulnerable they really are to application-based attacks. Many believe that because the OS is more secure today, so too are the applications.

The eye-opening truth is that attacks through applications are actually mushrooming. As it becomes more difficult to attack through the OS, crafty hackers are turning to lower-hanging fruit. Increasingly attackers are moving their bull's-eyes from the OS layer down to the application stack.

One of the best examples of this trend is the huge spike in attacks through Microsoft Office applications. Between 2006 and 2007, Microsoft Office vulnerabilities alone have grown by nearly 300 percent. Many hackers exploit these vulnerabilities by tricking users to open maliciously-manipulated Office files which then gives them a backdoor into the enterprise via the endpoint.

And Office attacks are only a fraction of the problem. The increasing prevalence of insecure Web applications within the enterprise only exacerbates the situation.



Fiction: All companies have a strong security policy.

The Facts: Even in this era of skyrocketing data breaches, many companies still fail to implement actionable security policies to protect their endpoints.

According to a recent survey conducted among 160 global enterprises, only 41 percent of firms have documented and ratified security policies in place and as many as 13 percent have no security policy in place at all.

Simply having a security policy doesn't always guarantee that it is adequate, either. There are many organizations with policies in place that are too broad to be actionable, are outdated or simply make the end user apply their own judgment in questionable situations.

And even if a solid security policy is written, there is no guarantee that employees will know about it and follow it. In order to ensure this happens it is critical that organizations not only plan and budget for the development of the policy itself, but also for a robust awareness and training program to complement it. After all, a security policy is only as strong as its awareness and enforcement.

Fiction: Organizations can rely on end-users to follow endpoint best practices.

The Facts: Even companies with a strong security policy in place face endpoint security risks if they fail to adequately enforce their policies. Unfortunately, too many enterprises today still trust their users to self-police themselves while working on the endpoint.

Even the employees who should know better—IT professionals—are known to regularly break the rules. A recent survey of IT professionals by the Ponemon Institute found that more than half copied confidential company information onto USB memory sticks in spite of a company policy that banned the practice.

The issue of weak policies only exacerbates the problem. The hitch is that not only are employees likely to break a policy if they view it as inconvenient, but many conscientious users might also indulge in risky behavior when the policy is too vague to understand or enforce.

Clearly, organizations that leave it up to the user to implement endpoint security best practices are exposing themselves to increased risk. The only way to truly mitigate these risks is to not only



develop strong policies, but to also put measures in place that automatically enforce those rules. This takes the burden of security from the users' shoulders and allows them to work without worry.

Fiction: Isolating non-compliant endpoints from the network solves your security problem.

The Facts: The main idea behind most network access control (NAC) solutions is that by quarantining vulnerable endpoints from the network, an administrator can effectively mitigate the risk these non-compliant machines pose to the infrastructure.

The difficulty is that deployed in a vacuum, most NAC solutions are purely preventative—they simply deny network access to non-compliant or infected machines. While most NAC vendors position themselves as providing the overall solution to both quarantine and remediation capabilities, few actually offer the full framework for access control without working with partners that offer automated vulnerability assessment, remediation and continuous validation.

Without some way to automate the remediation of these machines, these NAC solutions can actually cause more problems than they solve. A lack of automated remediation puts these endpoints into 'PC purgatory,' putting users in a non-productive situation where they are unable to access company resources and must wait for IT personnel to fix their machine before reconnecting.

In order to avoid this black hole problem, administrators need an easy and seamless way to fix the problems identified and admit the user back onto the network with as little inconvenience as possible.

Lumension Security understands the inherent insecurity of traditional signature-based technology. Lumension Security's Endpoint Protection Solution allows organizations to proactively operate on the supposition that only allowing the known good applications and processes to run is more effective than trying to block all of the bad ones.

Lumension also understands the importance automation plays within a successful security management program. Combined with a strong and detailed endpoint security policy, Lumension can automate policy enforcement so that enterprises needn't rely on their users' word when it comes to following the rules. Plus, Lumension Security's vulnerability and patching capabilities



can automate the endpoint remediation process in order to prevent quarantined users from falling into that 'PC purgatory' which stymies so many when their endpoints aren't compliant.

Fact or Fiction – Debunking the Top 5 Vulnerability Management Myths

Vulnerability management can be a powerful means toward reducing the threat surface within an enterprise IT environment. But because vulnerability management technology has been around in some form or another for so long there has been plenty of time for the din of marketing-speak from various vendors to confuse users about the true nature of vulnerability management tools and practices.

The following are some of today's most common myths perceived about vulnerability management, along with explanations for why these beliefs are false. Understanding the true nature of vulnerability management will allow organizations to better mitigate risk and to ultimately strengthen the synergy between IT security and operations.

Fiction: All vulnerability management systems are created equally.

The Facts: One of the biggest myths held by those purchasing security solutions is that all vulnerability systems are alike. However, there are many details in each that can affect performance and, ultimately, usefulness of the system.

When evaluating a system it is critical to look at the source of vulnerability definitions used to assess the environment, how well the system integrates with the IT infrastructure and how actionable the information is that is produced by the system. Ideally a system should link vulnerabilities to as many standard vulnerability classifications as possible, such as CVE, BugTraq and IAVA codes. And most importantly, it should be integrated within the architecture to be able to automate and report on remediation to the greatest extent possible. Unfortunately, many vulnerability management systems on the market today fail to include this key element of automated remediation, making it an arduous task to actually fix the vulnerabilities found during assessment.



Fiction: Patching is the only way to remediate vulnerabilities.

The Facts: Even non-security experts understand that many of the vulnerabilities within an organization's infrastructure come by way of bugs and coding problems in their vendors' software. As a result patch management rightfully gets a lot of attention as a powerful means to remediate vulnerabilities.

But patch management is only half of the vulnerability management picture. The other half is configuration and change management. According to both Forrester Research and Gartner analysis, more than 40% of application downtime is caused by configuration problems. Vulnerability management best practices call for both up-to-date patches and flawless configurations to mitigate risks that can cause downtime or potential data breaches.

Sound configuration management tools and processes will not only address certain vulnerabilities left untouched by patching, they can also be a way to reduce risk when a patch cannot be administered. For example, take a certain little-used process that is always on by default. If that process is found to be flawed but the patch to fix it causes some other unrelated but vital process to break, it might make sense to change the default and turn that process off rather than installing the patch. For this reason the best vulnerability management tools will marry both patch management and configuration management in a single package.

Fiction: You must choose between agent-based or agent-less systems.

The Facts: Over the years the debate over vulnerability management system agents on the endpoint has raged, spurred on primarily by rhetoric from vendors who only offer one choice of assessment method.

Those in the agent camp say an agent is a best way to enforce patch and configuration levels on a consistent and ongoing basis. Those for agent-less systems believe that network scanning can offer a better view of a dynamic network environment, examining and discovering new machines that may not have agents and other vulnerabilities that might not be found with an agent. The truth of the matter is that both sides are right—both agents and network scanning offer their own intrinsic strengths. So why should an organization have to choose between these methods?



A truly thorough vulnerability management system should be able to offer both agent and agent-less assessment and remediation capabilities. Without both methods, an organization is bound to leave a gaping hole within their vulnerability management activities.

In the case of solely relying on agents, an organization can potentially be blindsided by devices and laptops without agents installed that connect to the network. Working only with an agent-less system leaves the possibility open that a device or laptop may not always be connected during a scan, thereby falling through the cracks. Taking advantage of both techniques takes advantage of each side's strengths while eliminating their weaknesses.

Fiction: Vulnerability management technology will always give you a big-picture view of risk.

The Facts: Because all vulnerability management tools are not created equally, many of them can fail to offer their purchaser a fully fleshed view of the risk suffered due to vulnerabilities.

Many tools that are evolved from the old guard of what was once the vulnerability assessment market are often guilty of producing long and detailed vulnerability reports that tend to offer a myopic look at the flaws in an environment. These reports are often not correlated to the configuration controls in place within the network environment. This makes it difficult to creatively mitigate risk through change and configuration management without the vulnerability system indiscriminately throwing up a red flag because a patch has not been installed.

Additionally these laundry list reports offer little in the way of actionable or prioritized information. They are meant to be produced by the security team, which then typically lobs the reports over to an already beleaguered operations team to handle the problems in a 'firefighting' mode. Without that integration of automated remediation these tools make it difficult to not only evaluate and prioritize risks posed by vulnerabilities, but to also act upon that information.

Fiction: Installing vulnerability management system solves all of your vulnerability problems.

The Facts: A good vulnerability management system can provide the make-or-break difference for a successful security program. But it is not a panacea.

Risk cannot be solved, it can only be mitigated. And because vulnerabilities and the threat surface changes every day, that risk is a moving target. Which means that vulnerability management systems at their very core are not install-and-forget tools.



In order to maximize the power of a solid vulnerability management system, an organization must set the right policies and procedures in place. Ideally the organization should get a picture of the current landscape and the risks posed by known vulnerabilities and then set a configuration baseline that mitigates the risks deemed most important to that enterprise based on threat relevance and the importance of affected systems. The organization then needs to be constantly adjusting the baseline to new vulnerabilities and threats that crop up. The trick is to pick the tool that most easily allows the organization to automatically enforce that baseline policy once it has been set.

Lumension Security offers enterprises with a comprehensive Vulnerability Management Solution that addresses vulnerability assessment, patch and configuration management. Its technologies provide a proactive way for enterprises to continuously assess vulnerabilities through both agents and network scanning in a seamless process that evaluates an environment against vulnerability definitions from all of the major standardized databases. It provides automated remediation and the means to enforce a security baseline set by each individual enterprise.

Fact or Fiction – Clearing up the Top 5 Data Protection Mistruths

One of the latest trends in IT security has been the shift in focus toward data-centric protection. Data is the most valuable asset an IT department must protect, and technology has evolved to meet this requirement. Encryption technology and data leakage protection solutions, which tend to rely heavily on content filtering technology, have helped shore up many organizations' data stores, but the problem is that as companies adjust their data protection strategies they have fallen prey to a number of misconceptions about data protection. Security officers should do their best to learn the truth so that they can develop a well-balanced data protection program.

Fiction: The outside threat is a greater threat than the inside threat.

The Facts: Data leakage risks can be broken down into two major categories: data loss and data theft. Most of the news stories out today usually relate to the former, typically reports of data missing through lost laptops, back-up tapes and devices.



While the loss of a laptop with thousands of personal records is certainly enough to raise an eyebrow, the likelihood that it will fall into the hands of someone who knows what to do with that data is relatively low. Even if a device or laptop is stolen, it is far more likely that the outsider that gains possession is really just in it for the value of the hardware rather than the data. The appropriate use of encryption can further diminish the risk that an opportunistic thief takes advantage of the valued information contained within.

That leaves us with the second category of data leaks. Data theft is far more hazardous to the enterprise, because in these cases the criminal understands the value of the data and hopes to steal it for their use. These malicious parties, whether they are inside or outside the organization, seek ways to gain access to the data and use it to their advantage. From the outside this is typically achieved through malicious programs designed to install backdoors into the enterprise. From the inside it might be as simple as loading several gigabytes worth of data onto an external device and taking it home.

These days most enterprises have full protection from the outside assaults. It is the threat from the inside that leaves them truly vulnerable. Most organizations have no methods in place to prevent trusted insiders from loading data onto external devices and walking away. And yet, this method of data leakage is perhaps the most dangerous risk among all types of data leaks. Not only does the trusted insider have access to the data, but they usually know the value of the data and what to do with it. If organizations are serious about prioritizing security based on the severity of risk, they must put insider threat protection on top of their list.

Additionally, organizations also need to be able to automatically audit this protection process. Without the visibility of auditing, businesses will be unable to quantify the risks posed by data leaks. They won't know whether data has moved between endpoints, what data it was or how much of it was potentially leaked. It is critical that auditing be baked into the data protection technology to fully realize its benefits.

Fiction: Data leaks are the only aspect of data protection that enterprises must worry about.

The Facts: Sure, data leaks have the potential to be devastating. Even if the data itself never makes its way into the hands of wrongdoers, the public relations nightmare that manifests itself after such an event can be harrowing. However, protecting the confidentiality of data is only one



facet of safeguarding this information. There are two other huge components as well, namely protecting data integrity and availability.

A well-rounded data protection program should not only be able to mitigate the risk of data leaks, but also to minimize the threat of the data being tampered or destroyed. Failing to address the data integrity component of data protection leaves an organization highly vulnerable.

Auditing and content monitoring capabilities play an important role in this process of ensuring data integrity. Keeping tabs on where data is flowing and being changed can ensure greater control over malfeasance. Additionally, managing vulnerabilities and patches and securing endpoint configurations play a critical role in ensuring data integrity because unmanaged applications and machines can easily allow the propagation of malware and keyloggers, which could compromise the integrity and availability of data.

Fiction: E-mail protection will plug all potential data leakage problems.

The Facts: These days most enterprises have taken heed of the warnings of risk surrounding e-mail data leaks. Security experts have long understood the hole that unmonitored e-mail can present an organization should an insider choose to transmit sensitive information outside the organization, which is why most organizations have endeavored to plug that gap with e-mail monitoring and filtering tools.

Unfortunately, though, some people are under the mistaken impression that e-mail is the only channel they need to guard from unwanted leaks. The truth is that there are plenty of other ways for data to make its way outside the security perimeter. Users can potentially click on malicious links on the Internet that can cause undetected backdoors to be installed on their system. Or more devastatingly, the users themselves can walk out the door with endpoints or devices under their arms, loaded with sensitive information.

Clearly, the matter of shutting off data leaks expands much broader than just e-mail.

Fiction: Enterprises can control data leakage through removable media by banning it.

The Facts: When analysts first began warning of the enterprise risks posed by removable media, some IT executives reacted quickly with Draconian policies banning the use of optical drives and USB devices. Once it became clear that users were ignoring these policies, IT departments



responded by picking up technology that completely blocks access to these devices or even going so far as to glue shut USB ports.

Security staff that employ such tactics fail to understand why users rebelled in the first place. The outright ban of devices was bad policy because most of the banned devices are useful tools that enable users to more effectively do their jobs.

Banning removable media in order to battle the risks associated with its use really hampers daily business activities. Effective organizations should develop security policies that only ban the risky behavior that makes removable media a threat, then implement technology flexible enough to enforce these policies.

Fiction: Encryption and content filtering are all you need to protect your data.

The Facts: While content filtering has certainly improved the state of data protection today, it does have one glaring blind spot. The typical content filtering solution monitors network or e-mail activity, but once information is moved to the local machine it will usually lose oversight of what the user is doing with the data. A user with malicious intentions could easily move data to the local machine and copy it to a USB thumb drive without the content filtering system ever notifying security experts of the problem.

Similarly, encryption also has its own weaknesses. Most encryption solutions do a great job protecting information should a device or endpoint be lost or stolen. Encrypting these devices will prevent someone on the outside from accessing the data they contain. However, once an authorized user enters their password they have unimpeded access to this data. Encryption does not protect the data on the endpoint once that user has authenticated.

In order to achieve truly balanced protection, organizations must supplement encryption and content filtering with a sound endpoint solution that can monitor users and enforce policies on the endpoint.

Endpoints have become the new targets to get unfettered access to data as many organizations do not have enforceable policies and many cannot quantify their exposure to data leakage. While managing removable device usage and data flowing to and from these devices protects an



organization from the greatest data leakage outlet, a complete data protection strategy must incorporate other technology to secure data-in-motion and data-at-rest.

Lumension Security's Enterprise Data Protection Solution proactively enforces data protection policies by delivering platform, user and data security to protect against loss and/or theft. By securing endpoint configurations and enforcing patch management policies, and by delivering granular controls around the use of removable devices and policy enforcement of data access and transfer, Lumension Security effectively protects organizations from both the external and insider data threats. Lumension puts management and control back in the hands of administrators who can not quantify the data leakage problem via the mass usage of external devices.

Additionally, Lumension has extended its data protection capabilities through best-of-breed partnerships with some of the leading endpoint encryption and data leakage prevention vendors, to deliver total data protection at the endpoint.

Conclusion

Whether you're choosing the appropriate endpoint security technology, setting the right vulnerability management policies, or deciding how a data-centric protection strategy fits into your organization's security plans, we hope this guide serves as a good first step to preparing you from falling into the trap of security misconceptions.