Vulnerability Management Article Anthology, vol. 3

Four Tripwire cybersecurity pros share their expertise on how to reduce risk from vulnerabilities and threats

Article 1: The 7 Habits of Highly Effective Vulnerability Management

Tim Erlin

On the surface, vulnerability management (VM) is nearly ubiquitous. If you ask someone whether their organization has VM, the vast majority will reply in the affirmative.

In fact, Tripwire asked that very question in a recent survey on the topic. Eighty-eight percent of respondents said yes. Beneath that surface of 'yes' responses, however, lies a varied spectrum of implementation ranging from periodic penetration testing to full-blown enterprise vulnerability management. As a VM vendor presenting your solution, you get used to the response (in a faux French accent) of "We've already got one!"

At the same time, the problem of vulnerability risk has hardly been solved. In the same survey, 27% of respondents indicated that they've experienced a breach as a result of an unpatched vulnerability. The VM market is growing, and that means that organizations are expanding and replacing the tools they have.

If you're going to increase investment, or make a replacement decision, you have to answer this most difficult question: how do you know your vulnerability management program is effective? In order to shed some light on that question and how it might be answered, let's look at seven habits of highly effective VM programs.

1. Executive Buy-In

It's easy to say that tone-from-the-top makes a big difference, but how do you actually determine if an initiative has executive buy-in? Start with the phrase 'buy-in' perhaps. If a VM initiative has the right level of sponsorship and visibility, then you should be able to articulate how the success or failure of the initiative impacts those executives. It might be that there's a specific compensation impact, or it might be less concrete, but when a program can succeed or fail without affecting someone, then that person definitely does not have buy-in.

2. Asset Discovery

Any limit you place on the scope of vulnerability management is a limitation on the risk to which you have visibility. That's why asset discovery has to be a core component of any vulnerability management program. If a VM program excludes assets or specific areas of the business, that's a sign that it's not going to be effective at risk reduction. You can't remove risk you don't know about. Likewise, if asset discovery isn't continuous or performed with frequency, it's likely to become stale and inaccurate.

3. Scan Frequency

You might think that the mantra here is something like 'scan continuously,' but that's a red herring. The reality is that you're conducting scans for two reasons: first, in order to drive remediation activity and second, in order to identify meaningful changes in your risk profile (e.g. find new, high-risk vulnerabilities). Your scan frequency should be, first and foremost, rational. That means it should be tied to those two objectives. If you remediate on a monthly cadence, then scanning daily

Article 1: The 7 Habits of Highly Effective Vulnerability Management (cont.)

isn't going to improve your outcomes. If, however, you have inadequate change management, then you might mitigate some of that risk with more frequent scanning in order to achieve the second objective. The ideal scenario is that scans occur in a similar cadence with remediation activities and automatically when changes occur.

4. Incorporating Business Context

Vulnerability risk isn't absolute, and if you're basing your remediation priorities on some notion of absolute risk, then you're likely leaving risk on the table. Highly effective vulnerability management incorporates the business context of the discovered vulnerabilities, and the systems on which they exist, into the prioritization mechanisms used to drive remediation activity. What does that mean in practice? It means that assets of higher value and higher risk to the business get addressed first.

5. Exceptions are the Exception

You can't manage risk you don't know about, and creating exceptions from scanning creates pockets of unknown risk. There may well be devices in an environment that can't be scanned, but they should be few and far between and hopefully on their way to retirement. Organizations that actively measure the total surface area they're missing are generally high-performing when it comes to VM.

6. Managing to Metrics

Panic is not a strategy, but it's a big part of the information security industry. There is a lot of fear, uncertainty and doubt to be had out there. Effective vulnerability management programs aren't built on FUD. They're built on metrics. Progress is inevitable if you simply start with the question "how do I know we're doing a good job?" That question leads to some definition of good, a requirement to measure it and likely a bunch of other metrics to help understand why you're not there yet. There are plenty of metrics to choose from and more than enough advice on which are the best. I'm always in favor of using the metrics that drive the right behavior in your organization.

7. Remediation Workflow

The point of all this activity to find and measure vulnerability risk isn't a pretty report. The point is to make better risk mitigation decisions. The point is to take action. Effective vulnerability management has to result in effective remediation actions. No vulnerability assessment tool does this automatically for a variety of valid and invalid reasons. That means that effective VM programs integrate with the remediation workflows that drive action within an organization. The tricky part is that these workflows are likely to be unique, and there are usually multiple of them.

Article 1: The 7 Habits of Highly Effective Vulnerability Management (cont.)

If your VM program consists of generating a report and handing it off to another team, you might have some room for improvement. Start by finding out how work gets done inside your organization, then figure out how to get the right remediation work into those processes.

The evidence in the market is that there's plenty of vulnerability assessment out there but also room for improvement with effective vulnerability management. If you find yourself in a position of ownership for a vulnerability management program, these seven habits should help you get the most out of your efforts to manage and reduce vulnerability risk.

Watch 7 Habits of Highly-Effective Vulnerability Management

Article 2: The Five Stages of Vulnerability Management

Irfahn Khimji

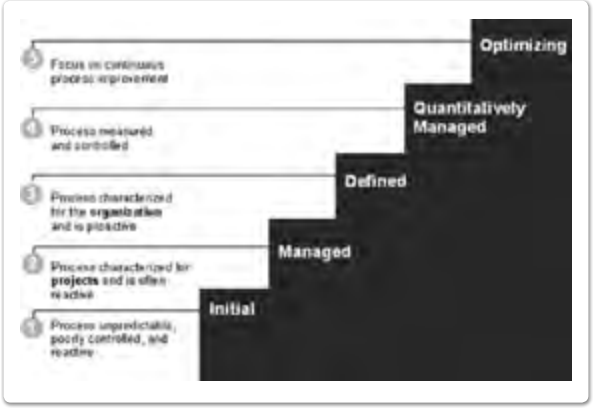
A key to having a good information security program within your organization is having a good vulnerability management program. Most, if not all, regulatory policies and information security frameworks advise having a strong vulnerability management program as one of the first things an organization should do when building their information security program.

The Center for Internet Security specifically lists it as number three in the Top 20 CIS Controls.

Over the years, I've seen a variety of different vulnerability management programs and worked with many companies with various levels of maturation in their VM programs. This post will outline the five stages of maturity based on the Capability Maturity Model (CMM) and give you an idea as to how to take your organization the next level of maturity. To read the full whitepaper, check out this link.

What is the Capability Maturity Model?

The CMM is a model that helps develop and refine a process in an incremental and definable method. More information on the model can be found here. The five stages of the CMM are:



Source http://www.tutorialspoint.com/cmmi/cmmi-maturity-levels.htm

Stage 1: Initial

In the Initial stage of a vulnerability management program, there are generally no or minimal processes and procedures. The vulnerability scans are done by a third-party vendor as part of a penetration test or part of an external scan. These scans are typically done from one to four times per year at the request of an auditor or a regulatory requirement.

The vendor who does the audit will provide a report of the vulnerabilities within the organization. The organization will then typically remediate any Critical or High risks to ensure that they remain compliant. The remaining information gets filed away once a passing grade has been given.

As we've seen over the course of the last couple of years, security cannot just be treated as a compliance checkbox. If you are still in this stage, you are a prime target for an attacker. It would be wise to begin maturing a program if you haven't started already.

Stage 2: Managed

In the Managed stage of a vulnerability management program, the vulnerability scanning is brought in-house. The organization defines a set of procedures for vulnerability scanning. They would purchase a vulnerability management solution and begin to scan on a weekly or monthly basis. Unauthenticated vulnerability scans are run, and

Article 2: The Five Stages of Vulnerability Management

the security administrators begin to see vulnerabilities from an exterior perspective.

Most organizations I see in this stage do not have support from their upper management, leaving them with a limited budget. This results in purchasing a relatively cheap solution or using a free open-source vulnerability scanner. While the lower-end solutions do provide a basic scan, they are limited in the reliability of their data collection, business context and automation.

Using a lower-end solution could prove to be problematic in a couple of different ways. The first is in the accuracy and prioritization of your vulnerability reporting. If you begin to send reports to your system administrators with a bunch of false positives, you will immediately lose their trust. They, like everyone else these days, are very busy and want to make sure they are maximizing their time effectively. A reliable and accurate report is critical to ensuring that remediation can occur in a timely manner.

The second problem is that even if you verify that the vulnerabilities are in fact vulnerable, how do you prioritize which ones they should fix first? Most solutions offer a High, Medium, Low or a 1-10 score. With the limited resources system administrators have, they realistically can only fix a few vulnerabilities at a time. How do they know which 10 is their most 10 or which High is the most High? Without appropriate prioritization, this can be a daunting task. Granted, an industry standard such as CVSS is warranted for a common communication mechanism. Being able to prioritize in addition to this provides tremendous value.

Stage 3: Defined

In the Defined stage of a vulnerability management program, the processes and procedures are well-characterized and are understood throughout the organization. The information security team has support from their executive management as well as trust from the system administrators.

At this point, the information security team has proven that the vulnerability management solution they chose is reliable and safe for scanning on the organization's network. As recommended by the Center for Internet Security, authenticated vulnerability scans are run on a, at minimum, weekly basis with audience-specific reports being delivered to various levels in the organization. The system administrators receive specific vulnerability reports, while management receives vulnerability risk trending reports.

Vulnerability management state data is shared with the rest of the information security ecosystem to provide actionable intelligence for the information security team. For example, if an exploit is detected on the external firewall, a quick correlation can be run in the Security Incident and Event Management (SIEM) tool to identify which systems are vulnerable to that exploit.

The majority of organizations I've seen are somewhere between the Managed and the Defined stage. As I noted above, a very common problem is gaining the trust of the system administrators. If the solution that was initially chosen did not meet the requirements of the organization, it can be very difficult to regain their trust.

Article 2: The Five Stages of Vulnerability Management

Stage 4: Quantitatively Managed

In the Quantitatively Managed stage of a vulnerability management program, the specific attributes of the program are quantifiable, and metrics are provided to the management team. The following are some vulnerability metrics that every organization should be tracking:

- What is the percentage of the organization's business systems that have not recently been scanned by the organization's vulnerability management system?
- What is the average vulnerability score of each of the organization's business systems?
- What is the total vulnerability score of each of the organization's business systems?
- How long does it take, on average, to completely deploy operating system software updates to a business system?
- How long does it take, on average, to completely deploy application software updates to a business system?

These metrics can be viewed holistically as an organization or broken down by the various business units to see which business units are reducing their risk and which are lagging behind.

Stage 5: Optimizing

In the Optimizing stage of a vulnerability management program, the metrics defined in the previous stage are targeted for improvement. Optimizing each of the metrics will ensure that the vulnerability management program continuously reduces the attack surface of the organization. The Information Security team should work with the management team to set attainable targets for the vulnerability management program. Once those targets are met consistently, new and more aggressive targets can be set with the goal of continuous process improvement.

Vulnerability management, combined with asset discovery, cover the top three of the Top 20 of the CIS Controls. Ensuring the ongoing maturation of your vulnerability management program is a key to reducing the attack surface of your organization. If we can each reduce the surface the attackers have to work with, we can make this world more secure, one network at a time!

Learn more about Tripwire's vulnerability and risk management solutions, here.

Article 3: How to Avoid Common Software Vulnerability Management Mistakes

David Bisson

Vulnerability management (VM) is an essential process through which organizations can reduce risk in their environments. But myths and misconceptions surrounding VM abound. For instance, organizations commonly approach vulnerability management in the same way as they do patch management. Others are guilty of believing that all attacks rely on vulnerabilities, while others still are under the false impression that all software patches will work without a hitch.

When held by digital security teams, these and other misconceptions can lead to mistakes in the vulnerability management process. Such errors, in turn, undermine organizations' digital security posture more broadly. Provided below are three of the most common of these slip-ups.

Mistake #1: Not prioritizing risk properly

If there's one thing that's for sure in information security, it's that there's no shortage of known software vulnerabilities. Software providers rightfully respond to these flaws by routinely releasing dozens and dozens of patches in their security bulletins. For instance, Microsoft's Patch Tuesday for June 2019 included fixes for a whopping 88 security vulnerabilities in the Windows operating system and related software. Meanwhile, Oracle Technology Network's Critical Patch Update Advisory pushed out patches for 334 security flaws in July 2018 alone.

Given this number of vulnerabilities, organizations might feel inclined to fix as many vulnerabilities as possible. But this desire does not work in the favor of organizations' digital security postures, as bad actors don't develop exploit code for all vulnerabilities. In fact, a research study led by Kenna Security and the Cyentia Institute found that malefactors actively exploit less than two percent of vulnerabilities in the wild.

Kenna Security's research finding reveals that digital attackers tend to craft exploit code for an extremely small percentage of known security holes. It, therefore, doesn't make sense for organizations to treat all vulnerabilities the same. Nor is it beneficial for organizations to drop everything that they're doing and direct all their focus to a flaw which the media has hyped up for no meaningful reason.

Instead, organizations should look to prioritize their vulnerability management efforts. TechBeacon recommends that organizations specifically focus their efforts on vulnerabilities that enable access over the network and from outside threat sources. Additionally, organizations should use a risk formula to calculate each vulnerability's severity based on the threat it poses to their environment. This calculus should take related threat information, threat relevance, business value and role info of the target system into consideration.

Mistake #2: No accounting for zero-days

Organizations don't just have to worry about wasting time while patching known vulnerabilities which digital attackers aren't exploiting in the wild. They also need to concern themselves about security flaws of which they know nothing. Signature-based detection technologies don't work against these zero-day vulnerabilities. Digital attackers know this, and they know that

Article 3: How to Avoid Common Software Vulnerability Management Mistakes (cont.)

many organizations have no way of accounting for zero-day threats. That's why these bad actors are increasingly leveraging such "undiscovered" security holes to devise increasingly clever ways to penetrate organizations' networks without them knowing any better before it's too late.

Traditional security measures clearly don't work against zero-day vulnerabilities. Consequently, organizations need to outfit their vulnerability management programs with monitoring capabilities. Specifically, these features should monitor for suspicious activity involving their endpoints and the network as a whole. Organizations also need to balance these monitoring capabilities with a host-based intrusion prevention system that uses threat intelligence to stay on top of the latest threats. Finally, they should make sure they have robust incident response plans in place that can help them quickly address an instance where bad actors exploit a zero-day flaw.

Mistake #3: A disjointed approach to VM

It's not easy for organizations to coordinate their VM efforts towards mitigating both known and unknown vulnerabilities. This is especially the case when organizations practice a disjointed approach to vulnerability management. More often than not, this mistake boils down to issues involving people and process rather than technology. TechBeacon explains that organizations commonly slip up by dumping loose vulnerability management duties onto the desks of already overworked IT security professionals. In many cases, organizations often complement these ineffective duty assignments with weak policies and an abundance of disparate solutions.

To avoid these problems, Trace Security and TechBeacon both support the idea of organizations assigning firm responsibilities to individuals who have time to make VM an essential part of their jobs. Organizations should also create an incentive plan for system owners based on the vulnerability scores of the assets they manage. As we explained for The State of Security:

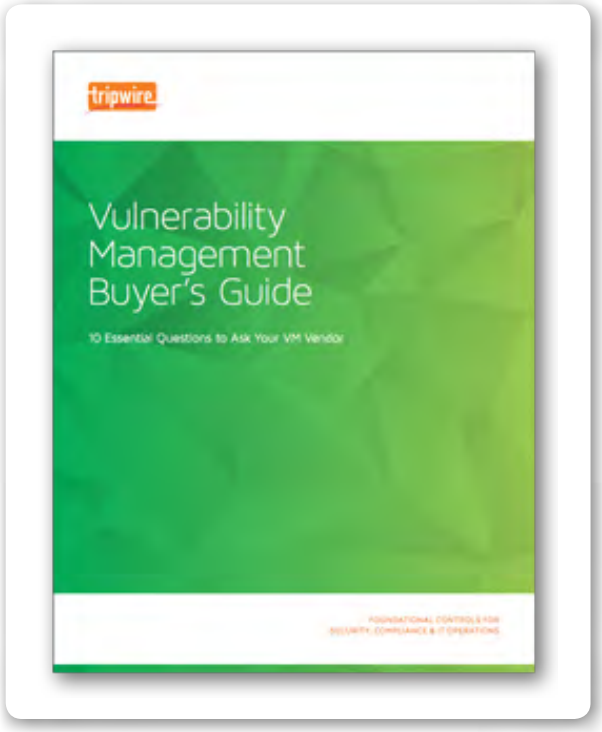
> People are often motivated by carrots, and there is nothing like presenting an award to an employee to make them feel good about their work and contribution. Besides, a little competition among peers is a good thing. Make sure you're using workflow in the tool to assign remediation to system owners and track their progress fixing problems.

Beyond that, organizations need to develop an appropriate strategy by which they can uniformly approach vulnerability management. They can complement this approach by investing in a VM solution that's right for them. This buyer's guide can help in that effort.

Just the Beginning

Everything we described above will help set organizations in the right direction towards augmenting their vulnerability management programs. But organizations should not pursue these steps with the expectation that they'll then be done. They

Article 3: How to Avoid Common Software Vulnerability Management Mistakes (cont.)



Download Vulnerability Management Buyer's Guide

need to realize that vulnerability management is an ongoing process, and they need to treat it as such.

Learn more about how Tripwire can help with your Vulnerability Management program, today!

Article 4: Steps for Successful Vulnerability Management: Lessons from the Pitch

Anthony Israel-Davis

When I was younger, I played a variety of team sports and enjoyed competing against opponents with my teammates. Winning was always a matter of applying sound tactics and strategy, attacking and defending well and using a blend of skill, talent and luck. Now that I'm older, I watch more than I play, and I'm able to appreciate the many lessons team sports teach, especially at the professional level. With sports, we can tackle technical topics in a relatable way. In this post, I take on vulnerability management (VM). The key word here being "management," an active and continuous approach to dealing with risk. Like the dynamic action on a ball field, vulnerability management is something that is always changing and rarely predictable. It also requires active participation.

There is an aphorism in sports that defense wins championships. While there is some debate about this in the sporting world, defending the enterprise against a data breach is a required business practice. Continuous vulnerability management remains Number 3 in the CIS critical security controls; it contributes to the defense that wins business.

To understand vulnerability management, it helps to have a common definition of vulnerability. A misconception about this term is that it is monolithic and binary. How often have we heard someone say "We need to patch a vulnerability"? This framing is dangerous as it assumes a vulnerability is a singular thing that can be fixed and forgotten. Shifting the focus to what it is we want to protect rather than any specific weakness changes the question to "how vulnerable are we?" In other words, "how likely is it that a threat can cause harm to my critical asset?" Soccer offers a good analogy: the critical asset is the goal, and the threat is the opposing team attempting to score. The goal is always vulnerable to attack; it is less vulnerable when there are defenders and a goal keeper and more vulnerable when those people are absent (which doesn't mean an attacker can exploit that vulnerability, it's just more likely).

Managing vulnerabilities is the process of decreasing the likelihood a threat can cause damage.

SANS has developed a simple framework which outlines the steps for successful vulnerability management: Prepare, Identify, Analyze/Assess, Communicate and Treat (PIACT).

Prepare

In sports, preparation is vital — practicing, fitness conditioning, studying tactics and strategy are all part of creating a winning team. Vulnerability management is the same — Identify key assets to protect, determine their level of importance, develop a plan to evaluate their weaknesses and know how to respond when weaknesses are found.

Like a successful sports team, a business team will need to come together to identify critical assets, determine their risk tolerance and determine a plan to identify and treat vulnerabilities. The players are IT and security professionals, systems owners and executive leadership. With a full team effort, assets can be appropriately classified, and patching and remediation plans won't conflict with business objectives. The team itself is part of the risk management process.

Article 4: Steps for Successful Vulnerability Management: Lessons from the Pitch (cont.)

Identify

Identification is the first step of enacting the plan. A football coach needs to know which players are ready for the game, which are injured and which match up well against an opponent. Similarly, a VM team will be looking to identify which assets need protecting and begin to prioritize them. Which assets have critical uptime requirements? Which hold the most valuable data? Which sit in exposed locations?

Every place critical data is stored or valuable processes occur need to be identified. This includes cloud, servers and even mobile devices. Access paths to those assets also need to be evaluated as potential points of exposure.

One way to automate this process is asset discovery. Running a scan to find all the devices with IPs on your network is one way to reconcile (or create) your asset inventory (CIS control number one). This can also become an integral part of the next phase, which is to analyze and assess the environment.

Analyze / Assess

Elite sports teams utilize advanced techniques to analyze the fitness and health of the athletes. I heard a story of a Tour de France cyclist who had every aspect of his day managed during the race – when to eat, what to eat, how much, when to drink and when to...everything else. The nutritionists and specialists had studied the cyclist during training to the point that they knew exactly what he needed and when to produce the fastest ride.

That same level of rigor needs to be applied to our most critical IT assets when evaluating risk. Understanding what controls are currently in place, what controls need to be implemented and what impact an exploited weakness would have can certainly help determine an asset's security posture. The assessment results in a prioritization and a recommendation for how to proceed.

Performing a risk assessment can be as simple as running a vulnerability scan or as complex as evaluating all the controls affecting the asset. The deeper the analysis, the more complete the view, so doing as much as is reasonable is recommended. A good start would be to evaluate access controls and who has access and to then run an authenticated vulnerability scan with something like Tripwire IP360 and a CIS configuration benchmark with Tripwire Enterprise. This will provide a good start for evaluating the technical control in place.

Communicate

It's tempting to jump right into treat phase at this time, and that would be a mistake. Before taking on the remediation, it's important to communicate the analysis to the appropriate parties. The assessment phase results in recommendations, prioritization and potential impacts for each asset. Because this entails work from various groups, possible expenditure for tools and changes in processes, the assessment team needs to present the results to IT operations, system owners and executive staff. Risk is a business decision, and how to address it is balanced against other strategic goals. Additionally, developing a means to communicate risk posture over time will help fund future

Article 4: Steps for Successful Vulnerability Management: Lessons from the Pitch (cont.)

efforts and give executive leadership a scorecard to understand the effects of ongoing initiatives.

In the sporting world, I think of this like the starting line-up. The specialists and trainers have watched practice all week, and now the manager needs to choose who starts, who is on the bench and who doesn't make it all. All teams have more players than can start, so just like managing IT assets, the head coach needs to decide who gets priority and who doesn't. Which brings us to game day.

Treat

Ultimately, this is the goal of vulnerability management. Reduce the risk by treating the weaknesses. And like vulnerability management itself, this is a continuous process, not a single event. This may mean putting in patching processes and policy, updating practices such as change control and running regular scans and assessments to ensure the appropriate controls are in place are functioning well. And then starting the cycle over again.

Train, play, compete week in and week out all season and maybe win a championship. And when the season is over, another season is right around the corner. With vulnerability management, it's no different – stay one step ahead of the adversary and play to win.

Looking for Help in Vulnerability Management?

Tripwire can be part of your vulnerability management team. With Tripwire ExpertOps, we can provide you with the tools and expertise to jump start your vulnerability management program. If you need the skills and would like someone else to manage administer your security toolset, it's the perfect choice. For those who have the skills and would like to manage it themselves, Tripwire has a suite of vulnerability management, file integrity management, secure configuration management and malware detection tools as well as professional services and penetration testing services for commercial and industrial systems. Tripwire is ready to be part of your security team!

Download Tripwire ExpertOps VM Services Brief

Article 5: Vulnerability Management and Patch Management Are Not the Same

Lamar Bailey

Vulnerability management and patch management are not products. They are processes – and the products are tools used to enable the process.

You cannot buy a hammer, nails and wood and expect them to just become a house, but you can go through the process of building the house or hire someone to do it for you as a service.

Vulnerability management and patch management products are often lumped together and assumed to be part of the same product. While they have a compatible relationship, they are not the same. Vulnerability and patch management products are distinct products with different purposes and goals that are used to support these processes.

Patch management is a process used to update the software, operating systems and applications on an asset in a logical manner. The purpose of a patch management system is to highlight, classify and prioritize any missing patches on an asset.

For the purpose of specificity, patches are updates from the vendor; they can contain anything from security fixes to new features. The vendor sets their policy for what can be in a patch, and they should document all changes and additions in a readme file. Not all patches contain security fixes, and not all patches will fix the security issues listed. This is why just having a patch management tool will not make you secure.

Vulnerability management is a process that discovers assets on the network, categorizes the OS and applications on the assets and reports on security vulnerabilities on target systems. The vulnerability management product will scan the asset and report the known vulnerabilities found along with remediation advice.

The remediation of a security vulnerability usually involves patching the vulnerable system, but it could also consist of implementing configuration changes, turning off vulnerably services or even blocking exploitation attempts with an IPS device.

Watch Vulnerability Management: Myths, Misconceptions and Mitigating Risk – Part I

After a system is patched, the scan is repeated to verify that the vulnerability is no longer present. This is a crucial step because sometime the patches may not overwrite or remove the vulnerable components, the remediation may also require some manual steps, or you may need to apply multiple patches to completely remove the vulnerability.

Article 5: Vulnerability Management and Patch Management Are Not the Same (cont.)

Trying to use a single dedicated vulnerability/patch management product to play both roles is like trying to strap pontoons to your car. It's not very practical. More than that, you end up with an abomination like the Amphicar built in the 1960s. It seemed really cool, but it wasn't a good car or a good boat.

A vulnerability management tool is designed to detect vulnerabilities, and it is not designed to provide insight into what patches you have installed. Many times, administrators misinterpret even good patch guidance, or the organization fails as a whole to use the tool to implement patches for all vulnerable components.

This leads to false positive reports that are almost always incorrect. A good understanding by the organization of how the tools work and how they are different will help avoid confusion and wasted time.

Tripwire's IP360 is an excellent vulnerability management tool. Tripwire VERT writes all of the security content and tests it against vulnerable and non-vulnerable systems to ensure the accuracy. This delivers a low false positive rate (0.02% in 2018) that saves time tracking down potential or nonexistent vulnerabilities.

IP360 looks at the various system components like files, registry keys, firmware, etc. to determine the vulnerability state of an asset. When false positives do arise, they usually reflect the fact that the patch was not applied correctly or that not all vulnerable components were remediated.

Tripwire Dynamic Software Reconciliation (DSR) is a reconciliation tool for Tripwire Enterprise (TE) that helps the Change Manager or TE Admin better understand the origin of a given change as they relate to authorized OS or software patches or upgrades.

With this system, admins can easily track patches and automatically promote them via change management.

Article 6: Three Tips for Enterprise Patch Management

Lane Thames

A few weeks ago, I woke up one morning to discover that Android had 34 software updates waiting for me. This was followed by my laptop wanting to reboot after installing the latest patches from Microsoft; my tablet needing a reboot after its latest firmware update; and my server screaming for me to put "yum" into action to install the latest patches available from Red Hat – all before 10:00 am in the morning!

With all of the technology we have today, installing software updates has become a near-daily activity. That statement is true for all professionals in the technology industry, especially those who handle patch management for large-scale enterprise IT systems.

Understanding the Patch Management Process

Recently, Tripwire's Vulnerability and Exposure Research Team (VERT) wondered how organizations might be handling the influx of patches, so we decided to conduct some research on the topic. Not surprisingly, we found that many organizations are having trouble keeping up with the vast number of patches constantly being added to the work queue.

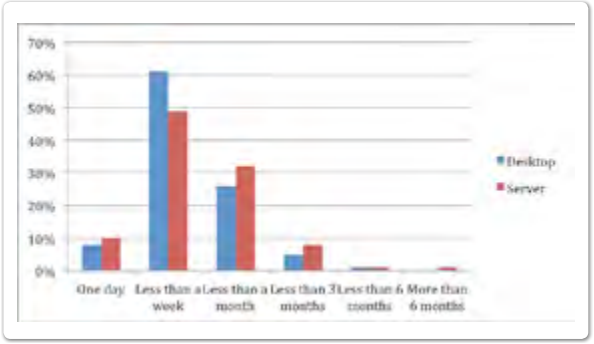
To many, installing a patch might sound easy. It's just the simple click of a button, right? Not really. Patch installation difficulty varies across platforms, ranging from the most trivial of installation methods (clicking a button) to complex scenarios involving delicate sequences of events.

However, patch installation difficulty is not the only variable in this equation. Patch testing is another critical piece of the puzzle and, along with scale, is one of the more challenging aspects of patch management in the modern world of enterprise IT.

1. REFINE YOUR PRE-DEPLOYMENT PATCH MANAGEMENT PROCEDURES

Enterprises cannot go about installing patches blindly without understanding potential impacts of the change brought by a patch. Patches have a history of breaking things, and when things break in the enterprise, chaos ensues.

In a recent survey, we asked 483 IT professionals their thoughts on patch management topics. We found that roughly half of those involved with patch management will always test patches before deployment, with approximately 30 percent saying



Source https://www.tripwire.com/misc/combating-patch-fatigue-register/

it depends on the patch. Fewer than 20 percent never test their patches.

Another set of questions was related to the amount of time spent testing patches for desktops and servers. As you can see in Figure 1, most organizations spend approximately one week or less testing patches in their environment before deployment.

2. BE WARY OF PATCH FATIGUE

A while back, I was interviewed by "Padre" over at TWiT for an episode on the TWiET channel. The topic was "Enterprise Patch Fatigue," and one

Article 6: Three Tips for Enterprise Patch Management (cont.)

of the questions Padre asked was related to the feasibility of thoroughly testing patches before enterprise rollout.

An organization's ability to thoroughly test patches depends on scale and resources. Virtualization and orchestration technologies, coupled with good patch management and vulnerability management software, can help organizations create environments that enable extensive patch testing.

Still, testing every possible configuration is hard for any organization. As you scale, it becomes impossible. More nodes mean an increase in the number of scenarios that need to be tested. Those considerations can quickly spiral out of control.

This leads us to the following conclusion: Patch testing is currently done on a best-effort basis, and as with most software-based testing, it only covers a small portion of the overall "state space" of test cases. An important question to ask is, "Will this scenario work in the future as more and more systems become highly interconnected?"

3. EXPLORE PATCH MANAGEMENT BEST PRACTICES FOR EMERGING IT

Current trends, such as the Internet of Things, the Industrial Internet and cyber-physical systems, are pushing the envelope of scale with an exponential explosion of devices coming online in the near future.

Will the failure of a patch installation in some data-center in Australia cause my infotainment center to malfunction, possibly causing my navigation to go wacky? What other questions need to be asked? Technologists should be considering these types of questions.

Obviously, new techniques and innovations will surface to help alleviate some of our patch testing problems. I believe automation will play a huge role, and advanced research in automated testing processes will surely help us in this domain. It will be interesting to see what developments tomorrow will bring us into the realm of patching.

What are your thoughts on the state of patching and patch testing? Let us know in the comments!

To learn more about how our patch management solutions can benefit your business, click here.

How can you keep up with thousands of new vulnerabilities reported each year?

BUILD A MATURE VULNERABILITY MANAGEMENT PROGRAM WITH TRIPWIRE IP360.

Get Complete Asset Discovery

You can't protect what you don't know about. Asset discovery and inventory are the foundations for any successful security program. Tripwire IP360 covers on-premises, cloud and hybrid environments, including container technologies such as Docker. It discovers and profiles all your assets and the applications they're running. In addition to agentless scanning, Tripwire IP360 uses agent-based vulnerability management (ABVM). Combining agent-based and agentless scanning means you can expect faster scanning results while consuming less network bandwidth.

Superior Vulnerability Scoring and Prioritization

Classify and rank assets based on their true risk to your organization, and identify owners for each system. Establish a scan frequency that allows asset owners to track the progress of remediation efforts and identify emerging risks based on new intelligence. Tripwire IP360 uses a unique fingerprinting methodology that provides vulnerability signatures specific to the operating system and installed applications for high accuracy results. Scans are also faster and more accurate, as they're limited to relevant assets only. Vulnerability rules are visible and customizable, and the detailed instance data that is returned by executing the rule is available for deep inspection.

Easy System Remediation

Customers with the most successful vulnerability management programs start by taking an overall baseline average of all the Tripwire IP360 risk scores across their organization. They set a target of 10 percent to 25 percent risk reduction per year to systematically strengthen their security posture. They are guided by Tripwire IP360 reports that outline the most vulnerable hosts, the highest scoring vulnerabilities and the most vulnerable applications.

GET TRIPWIRE IP360, THE INDUSTRY-LEADING VM SOLUTION

Schedule a call with one of our experts to learn how Tripwire can help you create a more mature vulnerability management program at your organization.

About the Authors

Tim Erlin

Tim Erlin is VP of Product Management & Strategy at Tripwire. He previously managed Tripwire's Vulnerability Management product line, including IP360 and PureCloud. Erlin's background as a Sales Engineer has provided a solid grounding in the realities of the market, allowing him to be an effective leader and product manager across a variety of products. His career in information technology began with project management, customer service, as well as systems and network administration. Erlin is actively involved in the information security community. His contributions include blogging, podcasts, press, speaking and television.

Irfahn Khimji

Irfahn brings a wide range of expertise in the field of Information Security specializing in Vulnerability Management, Compliance, Risk Identification and Scoring, as well as Social Engineering. He is a recognized leader in building Information Security Solutions and Customer Satisfaction. He has experience providing technical security leadership and guidance to Fortune 500 accounts, as well as smaller companies, in several verticals including financial, energy/commercial, healthcare, and retail. See what he's thinking on Twitter @ TheRealKhimji

David Bisson

David Bisson is an infosec news junkie and security journalist. He works as Contributing Editor for IBM's Security Intelligence, Associate Editor for Tripwire's "The State of Security" blog, and Contributing Writer for Gemalto, Venafi, Zix Corp, Bora Design and others.

About the Authors

Anthony Israel-Davis

Anthony 'Ant' Israel-Davis has been with Tripwire for over 18 years and is a Sr. Manager leading the team delivering Tripwire's from-the-cloud solutions. During his tenure he's worked as a web developer, managed the Business Applications team, helped develop the security awareness program, and led IT compliance initiatives including SOX, PCI DSS, and SOC2. He is currently earning his Master's in Information Security Management and when his head isn't in the cloud, you'll find him playing his fiddle, socializing around a board game, or rooting for the local soccer teams.

Lamar Bailey

Lamar Bailey is responsible for leading Tripwire's Vulnerability and Exposures Research Team (VERT), which is comprised of world-renowned security engineers and researchers who scour the globe looking for the latest public and private vulnerabilities, then write detection algorithms based on a propriety OS, Application, and threat fingerprinting techniques for inclusion in Tripwire's commercial Vulnerability Management products.

The Tripwire Vulnerability Assessment engine is part of IP360 and it is the brains for detecting network assets and evaluating these assets using the VERT algorithms. This team is comprised of world class software developers/engineers with low level understanding system and network programming.

Lane Thames

Lane Thames is a senior security researcher with Tripwire's Vulnerability and Exposure Research Team (VERT). As a member of VERT, Lane develops software that detects applications, devices, and operating systems along with vulnerability detection and management software. He also spends time looking for new vulnerabilities, contributing to the Tripwire State of Security blog, and understanding emerging cybersecurity threats. Lane received his PhD in Electrical and Computer Engineering from the Georgia Institute of Technology and has spent over 15 years working in information technology and software/hardware development.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at** tripwire.com

***The State of Security*: News, trends and insights at tripwire.com/blog Connect with us on LinkedIn, Twitter and Facebook**

BRVMAAv3a 1909