An Executive's Guide to Vulnerability Management:

How to Save Time and Money by Using Managed Services to Find and Fix Critical Security Exposures

INTERNET | SECURITY | SYSTEMS®

Ahead of the threat.™

ABSTRACT

"Vulnerability Management and Remediation" sounds like a mouthful. It can also be difficult to swallow — if senior executives and security staff do not work together to develop a plan to find, prioritize and fix network security exposures in a timely and cost-effective manner. This paper gives executives insight into how to make remediation a more inclusive and successful process.

Many organizations view security vulnerabilities as holes to be located and repaired by technical staff. Without communication and guidance from senior managers and executives, however, technicians cannot test for weaknesses without interfering with normal business activities. If the remediation plan does not prioritize vulnerability testing, the organization will remain at risk for attack or misuse.

The absence of business drivers in test planning and post-test remediation does more than undermine network operations. Without acceptable risk modeling practices, prioritizing remediation efforts and proof of security best practices for regulatory compliance becomes greatly complicated.

A business-based approach that works across multiple internal constituencies is the only approach that goes beyond short-term fixes and truly removes the root causes that allow network security vulnerabilities to arise. And yet, such business-based IT expertise is rarely available on staff, and outside consultants are expensive and are not available on a 24/7 basis.

The answer for many companies is a managed solution, in which an outsourced or hybrid in-house/outsource security service couples vulnerability management with other security offerings. Companies that choose such a managed solution receive superior levels of network protection, but limit costs by outsourcing security operations that fall outside their core areas of business expertise.

INTRODUCTION

Most businesses take vulnerability remediation for granted. As a result, senior executives and IT staff have differing ideas on how to make this process successful. Vulnerability management is like a trip to the doctor for a physical. We assume that we are in good or near-good health and that the doctor will find nothing wrong. When high cholesterol or diabetes shows up on the test results, we prefer a quick, one-shot cure, and often convince ourselves that nothing more is needed — even when the doctor tells us what we really need is a significant change in diet or lifestyle.

Think of vulnerability management as this same syndrome operating at the corporate level. Network administrators may find vulnerabilities and fix them, but rarely does anyone dig a little deeper. The short-term, tactical fix does nothing to eliminate a deeper, much more serious underlying cause.

VULNERABILITY MANAGEMENT ESSENTIALS

When executives are unaware of the massive volume of security vulnerabilities that exist in any network, the potential for a significant security lapse becomes much more real. These security exposures cover a wide range of threats, including but not limited to:

- Misconfigured or unpatched servers, laptops and desktops
- Out-of-date or misaligned security policy
- Unauthorized hardware, software or applications
- Easily-guessed passwords
- Inadequate controls on traffic from trusted third-party networks

Networks change over time. Today's successful lockdown can be obsolete within hours. Each new application, upgrade or device introduces a new variable that must be tracked. Even seemingly innocent interactions between separately hardened network assets can introduce significant opportunities for attack or misuse.

It is an IT necessity to identify vulnerabilities, prioritize which ones need to be fixed first and verify that repairs are in place and working as intended. It is also a business necessity. Regulations such as Sarbanes-Oxley and HIPAA mandate that IT security controls be used as a key component of documenting compliance. Executives cannot truly verify that security controls are in place without tight coordination with IT.

Business concerns create the environment in which vulnerabilities arise in the first place. In a perfect world, there would always be ample time and budget to test and repair everything. In the real world, there is never enough time or money to track and repair all potential weaknesses in a network.

The only logical means to protect the most critical business operations and most valued online assets must be a structured, strategic plan that corrects risky business activities by applying a comprehensive risk management model. This model must include input from both senior business and IT managers as a central part of the vulnerability management process. Vulnerability management, therefore, must be considered to be as much a business activity as it is an IT activity.

HOW TO IMPROVE VULNERABILITY MANAGEMENT PROCESSES

The benefits of a business-based approach to vulnerability management are clear: reduced security exposure, simpler proof of regulatory compliance and a greater return on network security expenditures. A properly planned and managed vulnerability remediation effort will yield a significant and rapid return on investment (ROI), especially if all or part of the vulnerability management process is handled through a managed service (more on this option later). A poorly planned and/or managed remediation plan will not produce the required results, and is likely to add cost, complexity and reduced profitability.

ROOT CAUSES AND EFFECTS

The key to improving vulnerability management processes is to realize that vulnerability management is a superb tool for discovering the root effects that result from inefficient security practices. It is these root effects that provide valuable insight into the business drivers and behavioral issues that are the root causes of these effects — and the elimination of root causes is the ultimate goal. Over time, root causes can be controlled by modified policy, standards, practices and procedures. Each change must be clear, concise, enforced and based on business needs as defined by the corporate business risk model.

Proper vulnerability management begins with detailed assessments that provide a snapshot of the actual state of information asset protection at a given point in time. If a company conducts an assessment to establish a baseline, then subsequent assessments can determine the net change, good or bad, from that baseline. If a business does not assess its business or network environment, then it has no indication of how well or poorly it is performing compared to plan.

Any business that stores regulated information or information considered proprietary to the company's customers is likely to be required to conduct a risk assessment to prove compliance with relevant regulations. Without the benefit of assessments, it is highly unlikely that the company can prove compliance. Just because an organization has policies, standards, practices and procedures, it does not mean that those internal standards are useful, followed or enforced.

INCOMPLETE PROCESSES LEAD TO INCOMPLETE RESULTS

Many companies stop after the assessment step. The assessment finds holes. The IT department is ordered to plug them. The IT department will usually take one of two approaches. Either it will plug the easiest holes first, to show that it is being proactive and productive, or it will guess at the most important systems, and do what it can to protect them.

In both cases, the IT department works from what it knows best — network infrastructure. However, the IT department is considerably less knowledgeable about the business drivers that may have led to the root causes behind the vulnerabilities. For example, a major expansion within a business unit may have led to a number of PCs being deployed before they can be made fully compliant with security policy.

The assessment process uncovered the root effects of a significant security exposure. And yet, the exact same problem will occur over and over again until the business drivers that created the rush to deploy unsecured PCs are modified to prevent it from happening again.

It is this final step — the balance between business behavior and the limits inherent in technology, budget and staffing — that most often eludes businesses. Nevertheless, this final step is becoming increasingly important.

The due diligence effort required to prove regulatory compliance almost always mandates using assessments within a formal business risk model to review and evaluate all applicable regulations, standards, guidelines and best practices. A court generally will find that the business is negligent if the business is below this level of due diligence, which in turn can lead to liability at the corporate and senior management levels. The need to prove that vulnerability management resulted in the elimination of the business-driven root causes of security exposures is a powerful incentive to establish proper risk modeling as part of normal daily business operations.

FIX IT - AND KEEP IT FIXED

Properly applied, vulnerability management helps businesses identify the root causes of behaviors that introduce network security vulnerabilities. The trick is to avoid a number of common traps that keep businesses from implementing vulnerability management practices that continue to be effective over time. The following scenarios illustrate these common traps.

Trap One - "Just fix the vulnerabilities that were discovered."

The normal, logical tactic taken by many IT departments is to fix the parts of the network that are found to be the easiest to attack — and not necessarily the segments that carry the most sensitive information. This approach is invalid because most enterprise environments have far too many potential security exposures for the organization to catch them all. Even worse, the dynamic nature of networks means that new vulnerabilities arise all the time. Without determining the root causes that lead to the introduction of these weaknesses, a business will never find or fix the business drivers that allowed the vulnerabilities to develop, and never properly prioritize the order in which vulnerabilities need to be fixed.

Trap Two - "IT can fix the problems and does not need to work as an integrated team with management."

Vulnerability management is not an IT-only process. IT is the service supplier that supports the entire organization. In other words, IT must directly support normal business operations. That is its mission. At the same time, IT must apply the correct protection model without interfering with those day-to-day activities. These conflicting needs are, by definition, intertwined. It is not productive to ask the IT staff to make changes to underlying infrastructure without giving them the tools to understand how each change will impact the rest of the organization.

Trap Three - "Remediation can be a part-time activity."

Vulnerability management helps businesses address the root causes that impact the efficiency of business operations. As a result, it is best to think of vulnerability management as an ongoing cycle that repeats over time, not as a series of discrete events that only take place when convenient. Remediation also is very time-consuming. It can have an achievable ROI in as little as six months, but that requires a full-time team, fully backed by senior management. Organizations with part-time vulnerability management efforts generally put themselves at unnecessary risk. Even worse, an on-again/off-again approach makes it difficult to prove regulatory compliance — even if all systems have been properly secured.

Trap Four - "Security policy applies to everyone but me."

The management team itself must be fully responsible for working with the IT department to determine which root causes of security vulnerabilities require a change in employee behavior. Otherwise, the IT department will be perceived unfairly as interfering with daily operations, and the overall security posture of the organization will continue to suffer. More to the point, executive managers must follow these guidelines themselves. Behavior changes require consistent compliance and accountability. If leadership and accountability is removed from a policy, standard, practice or procedure, it is useless advice given to a non-listening audience.

Fortunately, each successful vulnerability management effort makes the next one easier to implement, at least until diminishing returns become evident. One measure to determine when continuing remediation is no longer supportable is when the next steps show no additional ROI for these activities. This feedback is critical to make sure that time and money are not wasted on programs that deliver no reasonable benefit.

Of course, vulnerability management is not as simple as avoiding the pitfalls laid out above. If it were, there would never be such a thing as a network security failure. The following list details the areas where senior managers need to pay particularly close attention in order to ensure success:

- Allocate sufficient time to develop, gain approval, train and roll out policy, standards, practices and procedures, including the acquisition of subject matter experts to participate in the vulnerability assessment and remediation process.
- Focus on finding root causes rather than quick fixes, with clear communication across the organization so that senior management understands what is at risk, and IT understands how each projected change will affect normal daily operations.
- Introduce proper socialization of policies, standards, practices and procedures across the organization, including opportunities for feedback prior to finalization, to create buy-in from as broad a sample of employees as possible.
- Establish accurate performance metrics and accountability requirements that hold the remediation team accountable and sponsors responsible for errors, misses and failures.
- Allow long-term follow-through on the remediation plan itself, to ensure that the results of each individual remediation effort work as intended.

COST-EFFECTIVE VULNERABILITY MANAGEMENT VIA MANAGED SECURITY SERVICES

Successful remediation clearly demands a wide range of very specific skills, plus the experience to apply those skills in a timely, cost-efficient manner. Although they are absolutely essential, vulnerability management and remediation are rarely part of an organization's existing core competence. Each business must make difficult decisions with respect to how it deals with three inescapable facts concerning vulnerability assessment and remediation:

- If done improperly, it is time-consuming and disruptive
- It requires a long-term perspective to implement successfully
- It usually requires resources not already at hand inside the organization

Until recently there were only two ways to work around these challenges. The first was to add staff and training, even if those resources did not reflect the central mission of the company. The second was to retain outside consultants on an intermittent basis, hoping that changes in the business environment or network infrastructure would not leave the organization open to attack or misuse between those often-costly engagements.

Today, there is a third option: managed security services. Managed security services allow businesses to offload much of the burden of network security to a trusted third-party provider. The business receives guaranteed levels of protection utilizing best-of-breed firewalls, virtual private networks (VPNs), intrusion detection and prevention and other related services — without having to invest in expensive staff training or maintaining a 24/7 in-house security presence.

In effect, using managed security services is comparable to leasing a car. The business only pays for the part of the service provider's security infrastructure that the business actually needs. Intuitive customer portals give the business full and immediate insight into what is happening on its networks, and what the service provider is doing to monitor and respond to security alerts.

This same high-value, lower-cost approach to security directly benefits vulnerability management and remediation. In addition to protection services, top-tier managed service providers have the ability to assess networks for vulnerabilities. These tests can originate either inside or outside their client's networks. In other words, each customer can choose when and what to test using the provider's customer portal.

Internet Security Systems' (ISS) Managed Security Services provides a powerful example of how this process works. ISS maintains a full range of managed security services, with global monitoring across multiple security operations centers operating on five continents. In addition, Internet Security Systems' X-Force® security research and development organization is one of the world's leading resources for vulnerability identification and remediation advice. X-Force research informs ISS' Managed Security Services, allowing businesses to:

- Significantly lower the cost of ownership for a security solution, while meeting or surpassing industry-specific certification and regulatory compliance requirements
- Gain 24/7 access to service scheduling and results as well as certified security professionals
- Minimize the risk of attack or misuse through rapid identification of security exposures and automatic application of dynamic virtual patching
- Reduce system downtime through expert management and monitoring of security technology
- Track the productivity of staff responsible for security planning, execution and support

SIX STEPS TO BUILDING AN EFFECTIVE VULNERABILITY MANAGEMENT SOLUTION

Internet Security Systems' managed services customers receive vulnerability testing as part of their managed services agreements. Firewall customers scan for vulnerabilities related to potential security issues surrounding the firewall. Intrusion detection/protection customers scan for vulnerabilities associated with attacks identified and deflected by the service. Or customers can subscribe to the separate Vulnerability Management Service, which offers a broader set of capabilities.

Effective vulnerability management is complex, and the team charged with implementing it must be fully supported and held accountable for its successes and failures. The following sections outline how to build a truly effective remediation strategy using Internet Security System's Vulnerability Management Service (VMS). The Vulnerability Management Service focuses on six key steps:

Step One - Vulnerability Discovery

Description - Internet Security Systems' VMS customers schedule and launch internal and external scans of their network assets via a secure, easy-to-use Web-based customer portal.

Result - Customers receive detailed descriptions of potential security exposures. The flexible nature of the tests gives administrators both an outside-in and an inside-out perspective, so that scenarios can be identified that indicate both external attack and internal misuse. Since the time that elapses between assessments and remediation efforts is critical to addressing root causes, the customer can choose to trigger scans as often as necessary. Regularly scheduled and ad hoc tests become much simpler to integrate into normal business operations because the testing infrastructure and expertise is provided by Internet Security Systems.

Step Two - Prioritization of Assets

Description - VMS identifies network assets, then allows customers to assign ownership to each asset. Customers can then rate how critical each asset, or the information contained on that asset, is to the business. The VMS customer portal streamlines this process through a simple, easy-to-use prioritization format.

Result - The prioritization process enables businesses to notify asset owners when vulnerabilities are discovered and to rank the severity of those exposures. Individual managers also receive a personalized view into how areas under each person's control may impact the overall security posture. This information helps foster the cross-departmental and management-IT communications necessary to implement a truly effective vulnerability remediation effort.

In short, prioritization makes it possible for businesses to understand and define an acceptable level of risk and how each risk affects the technology and business activities of the company. This model can then be communicated to staff in business, technical and behavioral terms, so that all employees understand what will be expected of them when vulnerabilities are fixed.

Step Three - Delegation of Remediation Tasks

Description - The VMS solution enables customers to assign specific vulnerabilities to designated asset owners for review and remediation. Detailed workflow with visual queues and notifications helps asset owners through the remediation process for each vulnerability.

Result - VMS gives customers the insight needed to ensure that the most critical vulnerabilities are fixed first, and that proper responsibility for each task has been properly assigned. Clear delegation of remediation tasks and ongoing tracking of progress gives businesses the ability to enforce accountability and intervene early if remediation efforts begin to slip off schedule.

Step Four - Dynamic Protection

Description - VMS integrates with other managed services from Internet Security Systems to request automatic, dynamic updates of server and network intrusion prevention system policies. The results of each vulnerability assessment give VMS the information necessary to update blocking responses using ISS' Virtual Patch™ technology, so that network assets are fully protected against attack or misuse, even in advance of system upgrades or patch deployment.

Result - Customers who use more than one Internet Security Systems managed service gain measurable improvement to their security posture immediately upon completion of a vulnerability assessment. The results of each scan generate automatic updates to security policies to enable blocking of malicious activity until systems can be upgraded or patched. In effect, the dynamic protection process and Virtual Patch™ technology allows administrators to focus remediation efforts on the most urgent situations first, with other systems able to operate safely until a normal update cycle corrects their security faults.

Step Five - Verification

Description - VMS' workflow capabilities help customers verify that all remediation efforts work as intended once each remediation task is complete. Each task remains active until the fix itself can be tested to show that all attack vectors for a given vulnerability have been successfully eliminated.

Result - Tracking, tracing and quality control for all remediation tasks help organizations recognize root causes that lead to network security vulnerabilities. This aggregate information helps businesses determine if specific behaviors or operational decisions indicate the need for updated security best practices and regulations. Once a business combines root effects from technical vulnerability assessments with root effects evident through policy, standards, practices and procedures, it should become easily apparent how to improve security operations, and which areas of practice need attention first.

Step Six - Customized Reporting

Description - Internet Security Systems' VMS delivers detailed assessment and remediation reporting through its customer portal. These easy-to-understand reports deliver critical insights into service performance and security posture. Each report is available either as a stand-alone presentation or in a combined format with data from other ISS-managed offerings. These reports have the flexibility to reflect both technical- or business-oriented perspectives, depending on the audience. VMS customers also receive secure, real-time access to service controls, issue status and information on emerging security events.

Result - Network security has matured from a technical specialty to a must-have for both senior executives and line-level staff. Increasing amounts of governmental and industry regulation require that proper security practices be quickly and easily documented to prove that security best practices have been followed, and that businesses are in compliance with any particular regulation. Internet Security Systems' VMS greatly accelerates and simplifies this critical process for all levels of an organization.

CONCLUSION

Internet Security Systems' Vulnerability Management Service delivers the following key advantages for businesses seeking a smarter, more cost-effective means to find, prioritize and remedy security exposures:

- Comprehensive internal and external vulnerability testing in a high-value, lower-cost managed services model that does not require an extensive investment in expensive, highly specialized staff
- In-depth security knowledge that helps customers interpret test results and prioritize remediation efforts
- Consulting services to assist clients in building effective, long-term risk models, improving security policies and procedures and developing cost-effective vulnerability remediation plans with rapid ROI
- A complete family of managed security services that establish due diligence and simplify reporting for proof of regulatory compliance

This turnkey program delivers superior vulnerability discovery, prioritization, remediation, dynamic protection between discovery and remediation, verification of remediation and reporting. Internet Security Systems' Vulnerability Management Service is a high-value solution that helps businesses meet industry-specific certification and regulatory guidelines while improving security posture and simultaneously reducing the overall cost of protecting critical online assets.

Internet Security Services' VMS is a cost-effective vulnerability management program that delivers the following key attributes:

- Integrated workflow, case management and remediation, so that assessment and remediation can be directed through a single easy-to-use portal interface
- A vendor-neutral framework that protects existing investments in network security infrastructure while adding additional capabilities when needed
- Deep security knowledge that helps customers preempt security challenges rather than reacting after the fact

Each Vulnerability Management Services customer uses information collected and organized by Internet Security Systems' extensive managed services infrastructure to determine the root effects of each potential security exposure. This information then becomes the base of the root cause discovery effort. The resources of Internet Security Systems' X-Force greatly accelerate the process of understanding the technological implications of each discovered vulnerability.

Internet Security Systems' Professional Security Services organization can be brought in to help clients focus and prioritize their remediation plans. Internet Security Systems consultants integrate this information with extensive, real-world business experience to build meaningful, acceptable risk models and fine-tune policies and procedures so that root causes can be eliminated over time.

These combined offerings help relieve some of the due diligence burden from managed services customers. Since Internet Security Systems assumes responsibility for securing its customers' online assets, it has had to establish a long, proven track record of best-practices and proper due diligence procedures for businesses of all sizes and markets. Extensive and easy-to-use reporting tools greatly simplify the process of documenting regulatory compliance.

Finally, Internet Security Systems' Vulnerability Management Service has the ability to provide Virtual Patch protection for systems or services at risk of attack. Network traffic can be routed around the affected system, or dangerous TCP/IP packets can be automatically quarantined before a potential malicious attack reaches its target. This on-the-fly capability protects online assets from attack or misuse until a proper patch or upgrade cycle can take place.

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS

Australia and New Zealand
Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838-1555
Fax: +61 (0)7 3832-4756
e-mail: aus-info@iss.net

Asia Pacific
Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: jp-sales@iss.net

Europe, Middle East and Africa
Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America
6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (509) 756-5406
e-mail: isslatam@iss.net

ABOUT INTERNET SECURITY SYSTEMS

Internet Security Systems is the trusted expert to global enterprises and world governments providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. ISS products and services are based on the proactive security intelligence conducted by ISS' X-Force® research and development team - the unequivocal world authority in vulnerability and threat research. With headquarters in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 800-776-2362.

Distribution: General
SM-VMSWP-0905

INTERNET | SECURITY | SYSTEMS®
Ahead of the threat.™