Interested in learning more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Using Proactive Depth in Defense to Ease Patch Management Problems

Information Security experts agree that "Depth in Defense" is a crucial concept in securing information assets for every organization. This concept is often overlooked when discussing a Patch Management strategy. The release of several damaging viruses over the last year continues to prove that being reliant on the reactive nature of patch implementation alone cannot prevent malicious code from impacting information assets. Depth in Defense is the process of adding a layered approach to protection. By choosing a layere...

Copyright SANS Institute

Author Retains Full Rights

AD

ForeScout

# Using Proactive Depth in Defense to Ease Patch Management Problems

By David J. Gadue
GSEC Practical Assignment V1.4b
Option 1 – Research on Topics in Information Security
Submitted June 13, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

**Abstract**

Information Security experts agree that “Depth in Defense” is a crucial concept in securing information assets for every organization. This concept is often overlooked when discussing a Patch Management strategy. The release of several damaging viruses over the last year continues to prove that being reliant on the reactive nature of patch implementation alone cannot prevent malicious code from impacting information assets. Depth in Defense is the process of adding a layered approach to protection. By choosing a layered approach, if one layer fails there are other layers in place that can provide protection. Even though a layered approach cannot guarantee complete protection, it can greatly limit the number and scope of compromises for any company. This paper will discuss the issues of patch implementation and reactive protection solutions. It will also show how some proactive solutions can add depth and help overcome the challenges created by the reactive nature of patch management. Different layers of proactive solutions will be discussed that will show how to add Depth in Defense. The goal is to help improve overall information protection and ease the critical burden of any patch implementation solution.

© SANS Institute 2004, Author retains full rights.

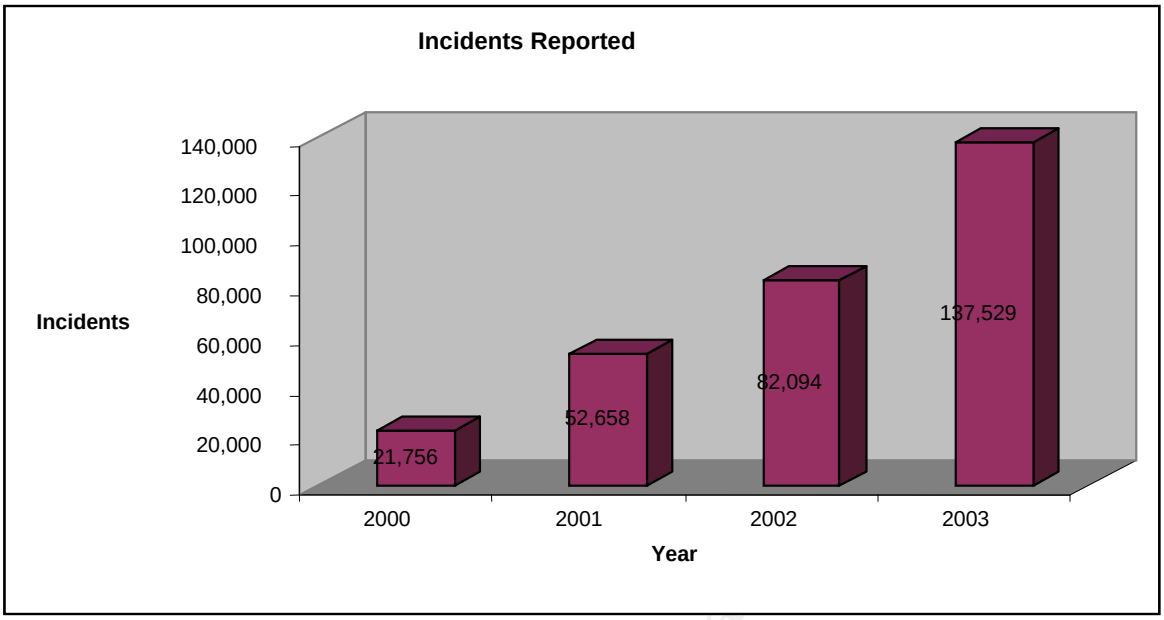
## Introduction to Patch Management

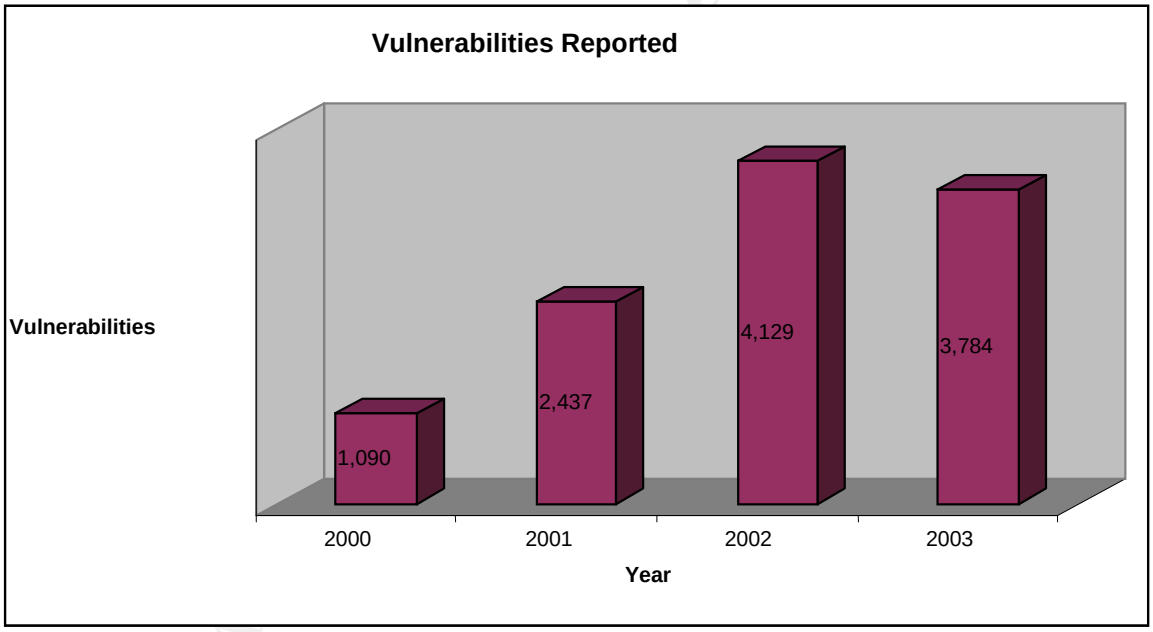
In the Information Technology (IT) industry, a “patch” is a small update that fixes a flaw in application code. “Roll-ups” and “service packs” are releases that typically contain a collection of patches. When discussing patches, the perception is that patches are fixes for security vulnerabilities or exploitable flaws. It is important to note that not all patch releases are to fix exploitable flaws in application code. Some patches provide functionality corrections within flawed software. Patch Management is the process of identifying and deploying these updates across a technical environment. This discussion will focus on patching as it relates to the correction of exploitable flaws in application code.

Ill-intended people continue to release malicious code in increasing numbers. This malicious code typically attempts to exploit flaws in application code in an attempt to compromise, damage, or disrupt the information flow and assets of others. This is why Patch Management has become one of the greatest challenges to every information security department and infrastructure support areas. Microsoft seems to take the brunt of the frustration from the IT industry when it comes to the patch management related costs and problems. This is somewhat due to the market reach of their product. However, to state that it is only Microsoft’s problem is completely incorrect. Red Hat has released 90 security advisories for Red Hat Linux version 9 over the year between March 2003 and March 2004 [1]. Over that same period of time, Microsoft released 51 security advisories [2]. Even the MAC OS X is becoming a target with the recent release of the AS.MW2004.Trojan. "A small number of virus writers are showing an increased interest in UNIX, and there have been Unix worms that have spread in the wild," said Graham Cluley, senior technology consultant at anti-virus company Sophos. "For this reason Mac OS X users should not think they have nothing to worry about moving into the future"[3] (Betteridge). While Microsoft’s products continue to be the target of most attacks, all operating systems and software vendors need to take a diligent approach to providing secure products.

Over the last few years, most organizations have dramatically increased the amount of time, resource, and budget being applied to Patch Management. “The market growth rate of enterprise patch management tools is expected to accelerate from 58 percent in 2002 to 68 percent in 2003, driven by marketing and sales investments by the pioneering vendors as well as by the entry of new, larger vendors. By 2007, the enterprise patch management tools market is expected to quadruple to over $40 million in new license revenue from its $10 million 2002 level.” [4] (Schroder, Colville, and Nicolett, p. 1) This increase can be directly correlated to the dramatic increase in vulnerabilities found over the last several years. The CERT Coordinate Center operated by Carnegie Mellon University provides support and trending for security activity reports the following trends in security incidents and vulnerabilities:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.






As companies scramble to react to vulnerabilities and incidents, industry experts have provided significant documentation on “best practices” and technical solutions for helping solve the patch management dilemma. Rutrell Yasin lists best practices in his December 2001 article “Patch management best practices” as:

- Get senior executive support.
- Establish standardized patch management policies, procedures and tools.
- Clearly assign responsibilities and provide dedicated resources.
- Create and maintain an inventory of all hardware, software, services and other technologies in use throughout the agency.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Identify vulnerabilities and appropriate patches.
- Conduct risk assessments.
- Test each patch.
- Distribute patches effectively.
- Continue monitoring the network for vulnerabilities. [5]

The problem is that even organizations using an effective solution and implementing these best practices will have patch management issues.

**Patch Management Issues**

*Proactive vs. Reactive*

Many industry experts and vendors flaunt that their "Proactive" approach to patch management will save money. CIO.com posted an article by Gordon Edall and David Senf called "Security Patch Management: 6 Step Proactive Process" [6]. The title of that article is very misleading. To deem a patch management process proactive could be one of the biggest misrepresentations in the IT industry today. Those who fall to this misconception will someday succumb to an exploit that will have a tremendous impact on their information assets.

The website www.dictionary.com defines being "proactive" as "acting in advance to deal with an expected difficulty". Being "reactive" is defined as "to react to a stimulus".[15] By our definition of a patch (a small update that fixes a flaw in application code), it is very evident that a patching is reacting to fix flawed code. Therefore, the potential always exists that an exploit could occur prior to a patch being available. This is proven time and time again. For example, eEye Technologies (www.eeye.com) frequently discloses when flaws exist in software well before a vendor can reasonably develop, test, and make a patch available. While eEye and others typically release very limited detail about flaws, information like that in the wrong hands can create a race between the virus writers and end users patching devices. The best patch management solutions can never prevent these exploits from impacting their networks.

Even in the scenarios where patches are available before exploit code is in the wild, there is often a large gap in the ability to secure devices. One crucial component to a successful patch management process is testing. How long does adequate testing take? For large companies with several mission critical applications, this could be days or even weeks leaving a company in a race with the attackers.

When it comes to propagation of viruses, minutes could be the difference. "At 0600 hours (GMT) on January 25, 2003, a vicious Internet worm called SQL Slammer was launched onto the Internet. The number of computers it infected doubled every 8.5 seconds in the first minute of the attack. In less than 30 minutes over 75,000 computers were impacted worldwide, resulting in business losses estimated in the billions of dollars." [7] (Internet Security Systems) With the need for speedy patch deployment,

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

challenges such as low bandwidth, exposures related to connectivity to the public Internet, and communication gaps need to be overcome when attempting to manage mobile devices. These hurdles will always create lag time in deploying patches. Again, this becomes a timing race that even the best patch management process cannot guarantee to protect against.

The last important aspect of patch management that needs to be discussed would be non-company owned devices. These days patching every company owned device is nowhere near enough. For most companies, a patch management solution would include all company owned assets. Significant vulnerability can exist from a remote worker who VPN tunnels in from their home PC, a proprietary application that is served on a device owned and managed by a vendor such as a phone switch, a router that is owned and managed by your Internet Service Provider, or a laptop managed by the consultant you have hired to implement a patch management process. Just about every company will have devices connected to its infrastructure that will not be or cannot be managed by the company itself. So what if those devices are not maintained by stringent patch management policies? This can create a significant problem.

*Risk vs. Reward*

It would be inappropriate not to quickly talk about the “risk vs. reward” challenges when it comes to patching an environment. To the bottom line of a business, is there a difference between down time or damage to information assets due to an attack, or down time or damage due to installing an inadequately tested patch? The answer would definitely be there is no difference. When a patch is released, the questions senior management usually wants answered from their IT personnel are: Will implementing the patch cause system downtime and impact business? Will an exploit entered our network and impact business? Since the typical response to both questions would be “maybe”, the risk versus reward challenge has begun.

These days decisions are made based on a risk assessment of installing or not installing a patch. This decision will be made in part by business leaders which often have drivers other than just security. The reactive nature of patch management now becomes even more evident. Most business leaders will tend to make decisions without the specific technical details of the vulnerability in mind. The decision will weigh the possibility of being exploited and the potential impact of implementation of the fix. The one constant that can help reduce the risk of implementation is time. The longer a company has to setup and complete testing, pilots, and deployment, the less likely implementation will impact business. This results in a lower risk of implementation. This need for time increases the head-start hackers and virus writers have in the race to patch. This is where adding depth becomes so important because it can provide organizations added time to properly engage their patch management process.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## Adding Depth in Defense

There are two types of solutions that can be used to add depth to patch management solutions. There are those that are proactive, and those that are reactive. Being proactive when it comes to a patch management solution itself is not possible. However, what is possible is to add proactive measures to reduce the risks associated with your patch management solution.

Until recently, proactive depth in defense solutions have been one of the most overlooked solutions in security. "Companies can no longer afford to depend on reactive security techniques. The potential for huge business losses from sophisticated new Internet threats, new compliance pressures and the spiraling cost of managing outmoded security approaches are all wake-up calls for corporate management." [7] (Internet Security Systems) Reactive technologies and processes are still the most commonplace. While these solutions do play a significant role in overall security, being reliant on this type of solution is difficult.

Popular reactive solutions and processes most commonly found in use today include Anti-Virus products, Network Based Intrusion Detection Systems (NIDS), System Integrity Verifiers, and Vulnerability Assessment technologies. By no means is this to imply these solutions do not provide benefit to improving security and easing patch management risk. To have the best opportunity to reduce the risks associated with patch management proactive solutions should be implemented in conjunction with the more common reactive solutions used today.

## Proactive Depth Solutions

*Policy and Awareness*

Two of the most overlooked methods to help secure your environment are the implementation of a solid Information Security Policy and providing employees information and training on security awareness. These two practices go hand in hand and should be implemented in every organization. Creating a solid Information Security Policy is not an easy task. A great place to find templates, samples, and information is from the Network Security Library web site (http://secinf.net/info/policy/isptg.en/ISPTG-Contents.html). This policy should be the groundwork for all information security within your organization. It should address both acceptable usage policy as well as policy on implementation of technology. The Acceptable Use Policy should be read, understood, and available to all employees. A solid policy should be reviewed and updated periodically. Also, note that policy that is not strictly enforced will quickly become ineffective. There will need to be consequences for not abiding by set policies.

Writing an Information Security Policy is only half the battle. It must be communicated to employees through education and security awareness programs. Recent viruses such as Beagle (Bagle), MyDoom, and Netsky continue to have an impact on companies world-wide. These are all mass-mailing viruses that get launched from an

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

email attachment. Educating end-users on the signs of a potentially harmful email is just one example of how you can proactively help prevent virus propagation well before detection and prevention is in place.

Other methods where security awareness will help reduce the risks associated with patch management would be in the enforcement of policies when it comes to non-company owned devices. Those organizations that do not have a technical method to block non-companies controlled assets from connecting to their network now must rely on the manual enforcement of policy to be successful. Most companies who do let non-company owned or supported assets connect to their network usually have written policies that must be adhered to. These policies usually require that the device be up to current patch levels and have updated virus definitions, etc. It will take an educated employee to convey and enforce these policies for non-company personnel and assets.

*OS Hardening on ALL devices*

Until recently, one in many vendor methodologies of operating system installation is in the default configuration of installation. Until just recently, few tended to do a good job of applying security by default. This would include installing and starting only those services and processes that are required. For example, in previous Windows versions, by default almost every bell and whistle was installed and started requiring the system administrator to lock down the device afterwards. In any scenario, it is important for a company to take the time to lock down or harden every device. This hardening measure should be a proactive attempt to completely secure a system. This would not only include servers, workstations, and laptops, but also network infrastructure devices, network printers, PDA's, etc. By taking this proactive measure to shutoff, isolate, or remove unneeded services, listening ports, or processes, many vulnerabilities could be avoided. Over the last year Microsoft has released critical patches for the Messenger and DCOM services. If these services are disabled on all devices, the vulnerability cannot be exploited and the update can be deployed as part of a regularly scheduled service pack update providing organizations time to properly test.

To aide in the operating system hardening effort, vendors publish white papers on best practices to secure devices. Also, many will provide support when hardening efforts impact business application functionality. Another valuable resource is the Center for Internet Security (CIS). CIS works with industry experts to generate best practice security templates for many operating systems. CIS also provides a benchmark scoring tool to help compare systems to best practice and indicate where further security can be implemented. Information on CIS benchmarking can be found at http://www.cisecurity.org/benchmarks.htm.

*Network Infrastructure Devices*

When discussing security of information assets the first thing many people think of is firewalls. Network firewalls are great tools to help protect your environment. There is a tremendous amount of details that can be discussed for the implementation of network

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

firewalls. For the purpose of providing an additional layer of protection to aide in the patch management process, a few key ideas should be thought out and implemented. Firewall best practices include only allowing required services access into your network. In addition, access should be limited to a Demilitarized Zone (DMZ) or site of increased security that usually exists between a trusted internal network and the public Internet. By using firewalls to limit access between the Internet and a DMZ as well as between a DMZ and the trusted network, risk of exploitation of a vulnerability will be lessened.

When speaking of firewalls, the first thought would be limiting access to ingress traffic (what is allowed into your network). Configuration of egress traffic (flow out of the trusted network) can be equally important to help mitigate risks. Your organization may not reap the benefits of controlling egress traffic on a perimeter firewall, however, everyone else's will! For example, mass-mailing viruses often create their own SMTP (Simple Mail Transfer Protocol) engine to deliver the virus to other hosts. By preventing devices other than your email servers to communicate via SMTP at your firewall, you can control the spread of a virus to others. These types of controls can also be put in place on firewalls internally or even on network routers or even layer 3 switches. Preventing unnecessary network communication can greatly help prevent the exploitation of vulnerability or the spread of an infection throughout your organization or to others.

*Host Based Protection*

A Zero-Day exploit is defined by as "any vulnerability that's exploited immediately after its discovery" [8] (Joshi). These exploits are becoming a more realistic threat on a daily basis. Abhay Joshi, Top Layer Networks Inc. outlines this in his March 2004 Computerworld article:

> "Hackers are getting better at exploiting vulnerabilities soon after discovery. It would typically take months for vulnerabilities to be exploited. In January 2003, the SQL Slammer worm exploit appeared eight months after the vulnerability was disclosed. More recently, the time between discovery and exploitation has been reduced to days. Just two days after Cisco Systems Inc. disclosed a vulnerability in its Internetworking Operating System software, exploits were seen; MS Blast was exploited less than 25 days after the vulnerability was disclosed, and Nachi (a variant of MS Blast) struck a week later". [8]

With zero-day threats becoming increasingly more likely, many vendors are developing zero-day host based protection solutions. These solutions are a proactive attempt to take the lead in the patch management race. Products such as Wholesecurity's Confidence Online and Cisco's Client Security Agent (CSA) tout that their products can protect against exploits until patches and updates are applied. These products are considered behavioral based technologies and do not require signatures or reactive updating. Confidence Online's product literature notes that "During testing performed by TrueSecure's ISCA Lab, Confidence Online detected 100% of the unrecognized Trojans. ANTI-VIRUS Products only detected 35% after being updated with the latest

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

signatures." [9] The Cisco CSA technology looks for changes in the operating systems that would represent the behavior of a virus or worm allowing protection against known or unknown vulnerablilities. An article published by Jason Deign on Cisco's website indicates:

> "Nine out of 10 threats against operating systems are covered by CSA," says Klaus Lenssen, Cisco business development manager for Security and Government Affairs. "Because it protects against the unknown, it means you do not have to fix vulnerabilities as soon as they are discovered - you can afford to wait until a cumulative patch comes along." [10]

The one drawback to behavior based products is that while they seem to replace anti-virus protection, they typically do not. This is mostly because they will not remove an infection and clean the infected device.

Other companies have implemented proactive protection in the development of application controls. Smart application controlling is essentially what the behavioral based products are doing. Companies such as F-Secure have integrated a lower level application control in their recent Anti-Virus Client Security (AVCS). This technology allows administrators to configure what executables can and cannot access the network, essentially disabling the ability for worms to spread. The drawback to this type of implementation is that it takes quite a bit of administration and configuration testing.

The Wholesecurity, Cisco, and F-Secure solutions are not the only type of proactive Host Based Protection solutions being developed. Others include a Host Based Intrusion Prevention Systems (IPS) that looks for network activity that would be suspicious and takes action as an administrator configures. Companies such as Symantec, Network Associates, and many others have integrated this type of proactive protection into their recently released client security products. This protection in some cases integrates with a host based firewall product. One important note on IPS technology is that it is different from Intrusion Detection Systems (IDS) and has a separate place in the security administrator's toolkit. An IPS is a proactive solution that can monitor and react to traffic inline and real time. Traditional IDSs monitor traffic passively by "sniffing" traffic from a network port. IDSs typically have very limited response mechanisms.[11]

Host based firewalls can be considered another proactive solution to protect against vulnerabilities whether known or unknown. By implementing a host based firewall solution, the spread of a virus or worm could easily be prevented or contained. In the recent outbreak of the Sasser worm, the exploit spread via setting up an FTP service on port 5554. If a host based firewall were implemented to block unwanted communications on unknown ports such as port 5554, the spread of this virus would have been prevented. There are many free and fee based host firewalls available. One of the most popular free products is ZoneAlarm made by Zone Labs. These days, almost all the major vendors providing host based protection are integrating firewalls into their products.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Several things must be considered when making a selection for a proactive host based protection solution. All the “bell and whistles” may be best for the company Security Administrator, however may not be best for the overall Total Cost of Ownership (TCO) for the company itself. With so many choices available the pro-’s and con-’s must be carefully weighed. This does not just include functionality. Things such as cost, performance, administrative requirements, and maintenance are just some of the considerations when making a decision to implement a solution. Thorough testing and analysis of these type host based products will be critical. The risk vs. reward of implementation can then be accurately assessed.

*Plan of Action*

Another important proactive measure that should be integrated into every organizations security implementation would be the definition of response and action plans for security events. Security events could be a vendor patch release, a virus outbreak, system compromise, or even the termination an employee. When a security event occurs it either has or could damage the information assets to your organization. While engaging such processes is a reactive measure, being proactive about defining and communicating an action plan will have a dramatic impact on the result of the event.

One critical step to defining any process or plan would be to gain full knowledge of the environment and your organization. In some instances this could be considered very difficult. Very large organizations with over 100,000 employees will tend to be more decentralized making it very difficult to identify simple things such as key contact information, critical business requirements, and understanding the technical infrastructure. A piece of this knowledge that is becoming increasingly more difficult to outline would be defining an organization’s network perimeter. Products such as Lumeta’s IPSonar are solutions designed to help network administrators map their environment and perimeter, as well as potential exposures.

Other important information should be understood and documented prior to responding to a security event. What is the communication strategy in the case of a Security Event? What are the testing and deployment processes, schedules, and protocol? What are the critical systems and applications and how are they protected? Does your response team have the required administrative access to infected or compromised devices? This topic alone can be discussed at great length. In this paper we have only scratched the surface. What will be important to remember is that understanding your environment, creating a plan of action, and communicating this information will be a crucial proactive process that will help diminish the risk when a vulnerability is discovered within your infrastructure.

*Email (SMTP) Policies*

Email has become probably the most important technical advancement for any company over the last 20 years. A Network Administrator has a better chance of taking away the CEO’s desk than he does trying to take away access to email, even for a short period of time. With the world today being so reliant on email communications, it has become a favorite vehicle for hackers to spread viruses, worms, and trojans. Quite

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

often, mass mailing viruses spread so quickly that virus protection vendor cannot get signatures created and distributed quickly enough. This creates a significant exposure to any organization reliant solely on patching and virus protection. To proactively help mitigate some of this risk, policies should be implemented on Simple Mail Transfer Protocol (SMTP) communications (email).

As outlined earlier, education and awareness can help users themselves prevent exploitation. Also, putting thought into a corporate SMTP communication strategy will greatly reduce this risk. Providing a single point of entry to and from your company for external communications is a critical first step. By limiting email communication through just one or two controlled gateways allows better control on what is coming and going from your network. Often time security intelligence sources provided notification of email borne viruses in the wild prior to the creation of signature files being available. In an environment with controlled communication to external sources, holds or blocks can easily be put on the gateways to prevent the infections from reaching your end users. This is another example on how a proactive approach can provide a better solution when reactive measures are required.

Preventing the ability to access external email including web based email should be included in this strategy. Hotmail, Yahoo Mail, AOL, and other web based email providers typically provide little, if any, virus protection or detection services at the server level. What should also be considered when setting policies on web based email, would be Internet based Chat or Instant Messaging services. These are also communication vehicles that can be used to transmit infected files and exploit code. Use of these types of accounts and services open the door for exploitation of company assets.

Another method of helping take a proactive approach to protection with email policies would be how companies act on potentially dangerous email attachments. A dangerous email attachment can be defined as a file attached to an email message that could have an undesired impact to a system, multiple systems, or the network. Typically, unwanted processes or actions are initiated through the single execution of an infected email attachment. In the Windows environment, these type attachments would include files with extensions such as .exe, .bat, .cmd, .com, .cpl, .vbs, etc. Industry best practices indicate that these extensions should be prevented from entering the mail system. “Dangerous attachments have no business entering your system at all. Even if they aren't blocked by your antivirus software, you should filter these types of dangerous attachments from all incoming and outbound mail.” [12] (Reynolds) To aide in this type of effort, best practices for configuration of an email infrastructure would include an SMTP gateway that would relay SMTP traffic to and from your email system. This would be the ideal location to filter unwanted email. It also would provide an additional place to scan for viruses. Many larger companies utilize different anti-virus vendors on the gateways and mail systems to increase the odds that their mail infrastructure will have virus definitions in place at the earliest possible time.

Quite often when we think of providing a more secure environment we think strictly of what lies within our own perimeter. In the case of email, every company does have the

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

ability to make a tremendous proactive impact on others. Your SMTP communication strategy should take into account email egress from your network. By scanning outbound mail, you are protecting the "next guy". Also, by preventing the egress of rogue SMTP communications from your firewall will also help others from becoming infected. As outlined earlier, the recent rash of mass mailing viruses all created their own SMTP engines on infected devices. By preventing the egress of SMTP communication from your network from non-authorized devices, you will proactively save someone else. Information Security is a responsibility we all must share. Help your neighbors!

*Secure Remote Access*

With the advancements of wireless technology, increased connection speeds provided through DSL and cable modems, and functionality of portable devices, remote access requirements are expanding rapidly. Business users are beginning to find what technical staff has known for a long time. The ability to work remotely can be essential to performing job functions. "By the end of 2003, 27 percent of US workers telecommuted at least one day per week. Many more work occasionally from home at nights and on weekends." [13] (Phifer)

Remote devices are very difficult, if not impossible to manage. Corporate security administrators have no control over a person's personal computer, or even a corporate device while a user is traveling. These are the type of systems that are greatly exposed during a vulnerability patching cycle. Having controls in place for a remote access solution will help provide protection until the patching process is complete.

Securing remote access connectivity is yet another topic that should be its own discussion. To help in the discussion on adding proactive depth in defense to a patch management process, a few items should be noted. A remote access solution should have a couple of key components. Many consider access control is limiting who has access. Access control should go way beyond that. By limiting what remote users have access to also provides a great proactive step in securing your environment. Most companies take great care in configuring firewalls for their network to protect their assets utilizing a DMZ, however, they allow their remote access solutions to completely bypass this security. Most remote access technology has the ability to limit access much like a router or firewall. These features should be utilized to help prevent the possibility of an infected device from impacting other devices and performance on the corporate LAN.

Technology from companies like Nortel Network and InfoExpress provides additional means for remote access security by providing quarantine and scanning capabilities. The ability to quarantine and scan a device for required processes or services as it connects to the corporate network provides tremendous controls for the security administrator. Products on the market can check that a host based firewall is running, look for anti-virus software and the latest signature files, or even quarantine the device while it is scanned for things such as patch compliance through a script. If a device

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

fails, actions can be taken such as launching scripts, notifying the user with instructions, or limiting access until compliant. This type of solution can greatly help in managing and controlling a remote population especially in the case when the administrator is not certain on the system being used to connect to recourses.

Secure Socket Layer Virtual Private Networks (SSL VPN's) are another emerging technology that proactively mitigates problems with patch management requirements. SSL VPN's allow remote users to securely access company resources through a web browser. With this technology, users only have direct access to the company resources in a browser window eliminating the ability of most worms and Trojans to propagate to company resources. F5's Firepass (www.f5.com/f5products/FirePass/), Aventail's EX-1500 (www.aventail.com/products_services/appliances.asp ), and AEP System's Sureware A-Gate (www.aepsystems.com/products/agate) are just a few products available. Also, companies such as Citrix Systems (www.citrix.com) integrate SSL remote capabilities with their thin client technology to allow remote applications to work within a web browser.

As web based solutions such as SSL VPN's, web portals, web based thin client technology get more and more popular, technology is also emerging to use browser capabilities to provide exploit scanning upon connection to a web page. WholeSecurity Confident Online product also comes in an "On-Demand" product. This product will allow you to embed a browser plugin to a web page to scan and terminate viral processes before the user proceeds to connect to company assets, login to a portal, or take other actions. Since this is the same technology used with their host based product, it is like having a behavioral based solution integrated into every device that connects to your web portal. Since it is not a signature based product and is proactive, this type of technology provides a tremendous benefit to patch management headaches.[9] Implementing both an SSL VPN's and embedded behavioral based scanning the security administrator can provide a more secure solution for connectivity of non-company owned devices.

**Building Your Strategy**

So far we have been able to outline where the problems exist with patch management and discussed many methods to add proactive depth to mitigate the risk of these problems. Now the question would be; how do I build a strategy? First, every strategy has "must's", "should's", and "would be nice". The "must's" are typically easy to identify and sell during budget time. The "should's" and "would be nice's" are not that simple. They must be carefully weighed in an effort to ensure adequate depth is achieved. This analysis goes well beyond the functionality or licensing cost for technology. Things such as administrative and maintenance cost, ease of implementation, impact to business flow, and other corporate initiatives all play a part in the decision. What should be considered critical in building this strategy should be implementing a good mix of proactive solutions with the typical reactive solutions found in use today.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The following tables are an example of how a medium sized company may prioritize, organize, and build their strategy:

### Proactive Defense

| Solution | Priority | Status | Comments |
|---|---|---|---|
| Policy and Awareness | Critical | Needs improvement | Polices in place, need to work on an awareness program. Need resource. |
| OS Hardening | Critical | Needs improvement | Only basic hardening in place. Can implement with service pack deployment project. |
| Plan of Action | Critical | Needs improvement | Nothing is formal or documented. Need resource. |
| Host Firewall | Moderate | None | Need further evaluation |
| Behavioral Based – Host (Zero-Day) | Critical | None | Need further evaluation |
| Host Based IDS/IPS | Moderate | None | Need further evaluation |
| SMTP Infrastructure | Moderate | Needs improvement | Technology in place, policies and configuration need review. Should be a project. |
| Remote Access Solution | Low | Needs improvement | Solution in place. A remote access policy is in place, however it will need to be upgraded to provide addition protection. |

### Reactive Defense

| Solution | Priority | Status | Comments |
|---|---|---|---|
| Perimeter Firewall | Critical | In Place | N/A |
| Network Based IDS | Low | None | Need further evaluation |
| Anti-Virus | Critical | In Place | N/A |
| Patch Management Technology | Critical | In Place | N/A |
| Security Intelligence | Low | Needs improvement | No formal process for gathering intelligence. No need for third party vendor, however a more formal strategy is needed. |
| Security Log Monitoring | Low | Needs improvement | Resource or technology needed to provided additional monitoring |
| Vulnerability Assessment/Audit | Low | Needs improvement | As needed for Patch management solution |

From the previous example, it is very easy to see that this company, like many, is heavily reliant on reactive depth. From this point it would be easy to then prioritize what needs to be done and a strategy that can be outlined and communicated to senior management. In some cases, proactive depth can be added at little cost. Other solutions will need to be more carefully considered.

One final note on building a strategy, with budgets tight it is very difficult for any security organization to implement every security measure they feel the corporation requires. This is where the Risk vs. Reward challenge becomes more difficult to assess. The

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

question now becomes Risk vs. Reward vs. Cost and again the decision typically is not made by the security professional, but rather senior management. One suggestion to help add light to the subject would be to make the effort to accurately account for time and resources required to react to a virus outbreak, or the drop everything approach to patch management. When resource time, business downtime, damage to information assets, etc. are all added up and presented, business leaders are typical shocked at the impact. Quite often this cost would have paid for that technical solution you have been requesting for a long time.

**Conclusion**

Proactive Depth in Defenses will benefit any patch management solution by reducing the risks associated to vulnerabilities allowing more time to evaluate, test, and deploy patches. Proactive defense will also better prepare an organization to respond during a security incident. It has been outlined that proactive solutions can add the biggest benefit to any patch management problem, yet are typically not found as often in organizations today. Reactive solutions such as anti-virus, network intrusion detection and a patch management technology itself play an important role in the overall security to any organization. However, proactive solutions will significantly enhance these capabilities and reduce the overall risk for a company to known and unknown exposures. Information Security is a dynamic industry. Technologies, best practices and philosophies change as threats change. This discussion outlines examples of some solutions and technologies that can add depth in defense to alleviate the problems created by the reactive nature of any patch management process. There are other solutions in existence today as there will be new solutions available tomorrow. What is critical when developing any strategy is to assess and ensure proactive solutions are identified and implemented to reduce the overall risk to your organization.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## References


[1] Red Hat, Inc. "Red Hat Linux 9 Security Advisories"
URL: https://rhn.redhat.com/errata/rh9-errata-security.html

[2] "Security Updates." URL: http://www.microsoft.com/security/security_bulletins/

[3] Betteridge, Ian. "Mac Trojan Set Loose-More To Come?" (13 May 2004)
URL:http://www.eweek.com/article2/0,1759,1591850,00.asp?kc=ewnws051304dtx1k0000599

[4] Schroder, Norma; Colville, Ronni; and Nicolett, Mark. "Patch Management is a Fast Growing Market." Gartner Market Research (30 may 2003)

[5] Yasin, Rutrell. "Patch management best practices" Federal Computer Week (01 Dec. 2003)
URL: http://www.fcw.com/fcw/articles/2003/1201/cov-patch2-12-01-03.asp

[6] Edall, Gordon and Senf, David. Security Patch Management: 6 Step Proactive Process Analyst Corner (08 Mar. 2004)
URL: http://www2.cio.com/analyst/report2315.html

[7] Internet Security Systems. "PREEMPTIVE PROTECTION: CHANGING THE RULES OF INTERNET SECURITY" ISS EXECUTIVE BRIEFING
URL: http://documents.iss.net/whitepapers/ISS_Executive_Brief.pdf

[8] Abhay Joshi, Top Layer Networks Inc. "How to protect your company from 'zero-day' exploits" ComputerWorld March 2004 (01 March 2004)

[9] Confidence Online Enterprise Edition
URL:http://www.wholesecurity.com/news/media_kit_resources/ConfidenceOnline_Always-On.pdf

[10] Deign, Jason "Security: Cisco Systems Gives Networks Intelligence" (18 Mar. 2004)
URL: http://newsroom.cisco.com/dlls/2004/ts_031804.html

[11] Conry-Murray, Andrew "Emerging Technology: Detection vs. Prevention - Evolution or Revolution?" Network Magazine (05 May 2003)
URL:http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=9400017&classroom=

[12] Reynolds, Greg "Anti-Virus Best Practices: A Net Sense White Paper" URL: http://www.netsense.info/Antivirus_Best_Practices.pdf


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[13] Phifer, Lisa "Can Remote Access Costs Be Cut While Increasing Productivity?" (March 2004)
URL: http://www.thinplanet.com/opinion/racosts.asp

[14] CERT Coordination Center URL: http://www.cert.org/stats/cert_stats.html

[15] Dictionary.com URL: http://www.dictionary.com

© SANS Institute 2004, Author retains full rights.

Last Updated: September 1st, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Crystal City 2015 | Crystal City, VAUS | Sep 08, 2015 - Sep 13, 2015 | Live Event |
| SANS Network Security 2015 | Las Vegas, NVUS | Sep 12, 2015 - Sep 21, 2015 | Live Event |
| SANS Seoul 2015 | Seoul, KR | Sep 14, 2015 - Sep 19, 2015 | Live Event |
| Data Breach Investigation Summit & Training | Dallas, TXUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Baltimore 2015 | Baltimore, MDUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Perth 2015 | Perth, AU | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Tallinn 2015 | Tallinn, EE | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS ICS Amsterdam 2015 | Amsterdam, NL | Sep 22, 2015 - Sep 28, 2015 | Live Event |
| SANS Bangalore 2015 | Bangalore, IN | Sep 28, 2015 - Oct 17, 2015 | Live Event |
| SANS DFIR Prague 2015 | Prague, CZ | Oct 05, 2015 - Oct 17, 2015 | Live Event |
| SANS Seattle 2015 | Seattle, WAUS | Oct 05, 2015 - Oct 10, 2015 | Live Event |
| SANS Tysons Corner 2015 | Tysons Corner, VAUS | Oct 12, 2015 - Oct 17, 2015 | Live Event |
| SOS: SANS October Singapore 2015 | Singapore, SG | Oct 12, 2015 - Oct 24, 2015 | Live Event |
| SANS Gulf Region 2015 | Dubai, AE | Oct 17, 2015 - Oct 29, 2015 | Live Event |
| SANS Cyber Defense San Diego 2015 | San Diego, CAUS | Oct 19, 2015 - Oct 24, 2015 | Live Event |
| SANS Tokyo Autumn 2015 | Tokyo, JP | Oct 19, 2015 - Oct 31, 2015 | Live Event |
| SANS South Florida 2015 | Fort Lauderdale, FLUS | Nov 09, 2015 - Nov 14, 2015 | Live Event |
| SANS Sydney 2015 | Sydney, AU | Nov 09, 2015 - Nov 21, 2015 | Live Event |
| SANS London 2015 | London, GB | Nov 14, 2015 - Nov 23, 2015 | Live Event |
| Pen Test Hackfest Summit & Training | Alexandria, VAUS | Nov 16, 2015 - Nov 23, 2015 | Live Event |
| SANS Hyderabad 2015 | Hyderabad, IN | Nov 24, 2015 - Dec 04, 2015 | Live Event |
| SANS Cape Town 2015 | Cape Town, ZA | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS San Francisco 2015 | San Francisco, CAUS | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS Milan 2015 | OnlineIT | Sep 07, 2015 - Sep 12, 2015 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |