BADM 590 MS1

Trustworthy Computing: Information Security and Management

FINAL PROJECT

VULNERABILITY MANAGEMENT AND ASSESSMENT

Submitted By: Syed Haider (Riz): shaider2@uiuc.edu

Submission Date: 05/05/2006

Submitted to: Professor Mike Shaw: mjshaw@uiuc.edu

MStech

MS in Technology Management

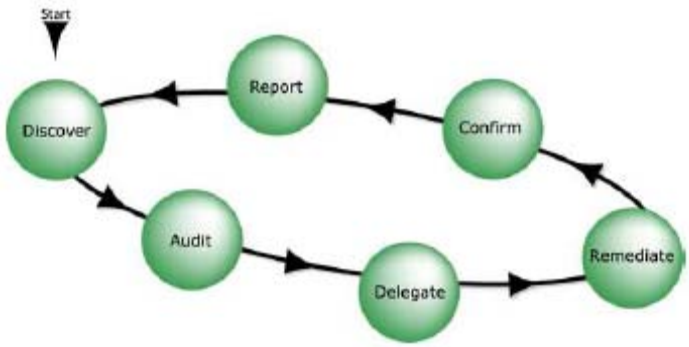
University of Illinois at Urbana-Champaign

Executive Summary

To prevent hackers or dissatisfied insiders from exploiting network weaknesses, every organization needs to perform timely identification and remediation of network. The process of identifying vulnerabilities, evaluating the risk, remediation and reporting is called vulnerability management. By using a formal vulnerability management process, an organization is able to more efficiently find and fix security vulnerabilities within their network.

Vulnerability management is a measurable and proactive process which enables organizations to understand the risk of certain vulnerabilities in its IT environment and ensure its network is not compromised. The process includes the following steps:

- Discover and categorize IT assets
- Scan for vulnerabilities
- Prioritize remediation effort based on risk
- Apply the patch, upgrade or workaround
- Re-scan and confirm the fix action
- Report risk assessment to upper management



In the past, vulnerability assessment was performed manually for auditing purposes. This process would take from one to several weeks and the reports produced were out of date by the time they were delivered. Today, high speed scanning software allows these steps to be formalized and automated. With the criminal threats facing IT infrastructure in this era, the process of vulnerability assessment, policy compliance and remediation has become part of the daily administrative process.

Identifying and managing risk relating to vulnerabilities requires that an organization understand the impact and cost of a successful attack on their environment. Automating the vulnerability

management process with software provides a cost effective way for organizations to quantify and qualify the security risks to business applications and apply resources to remediate those risks in the most efficient manner.

This formalization of the vulnerability management process satisfies regulatory and policy compliance issues and provides best practices for corporate governance of sensitive data.

This paper addresses the methodology required for successfully conducting, reviewing, and maintaining an effective Enterprise Vulnerability Management program.

TABLE OF CONENTS

INTRODUCTION

Most businesses take vulnerability management 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 condition 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.

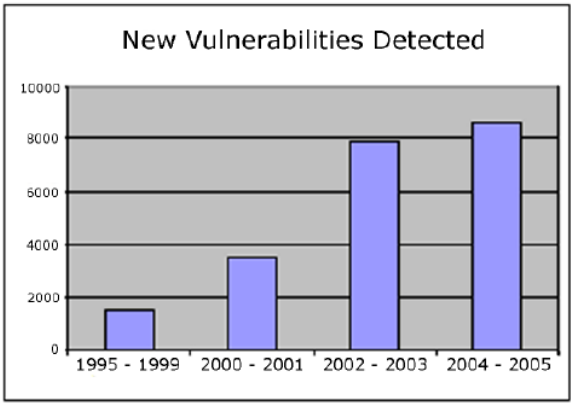
What is Vulnerability Management?

A process to determine whether to eliminate, mitigate or tolerate vulnerabilities based upon risk and the cost associated with fixing the vulnerability.

The Need for Vulnerability Management

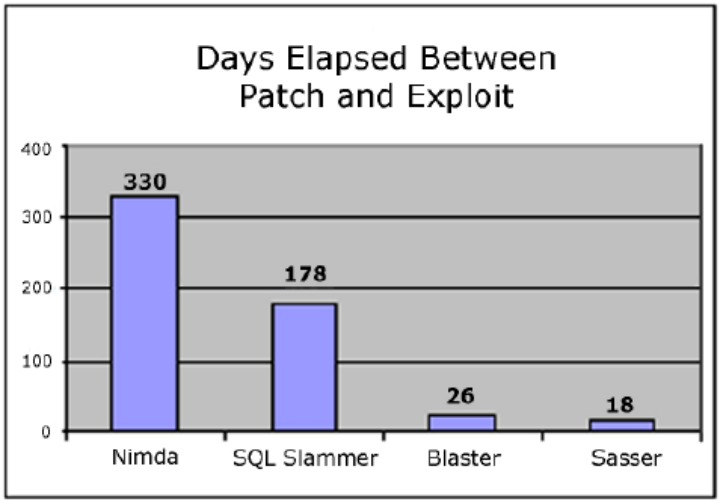
According to the Computer Security Institute (CSI/FBI) Computer Crime and Security Survey, in 2004 the average company lost over $822,000 as a result of computer crime perpetrated through insecure systems. Fraud, system downtime, lost productivity, repair time, and lost customers and revenues are intolerable business impediments created by these threats.

Cyber criminals are constantly scanning IP addresses looking for vulnerabilities that can be exploited. The Code Red virus, which was distributed in late 2001, infected over 250,000 web servers in the first nine hours and caused over $2.6 billion in damages. The patch to protect servers from this worm was released 6 weeks prior to the start of its spread. Unfortunately, most network administrators simply failed to patch their systems in a timely manner.



History has shown that as the complexity of IT systems increase, the likelihood of vulnerabilities existing within those systems also increases. Since CERT began tracking computer security data in 1995, the number of discovered vulnerabilities has grown exponentially. In 1999, the number of unique vulnerabilities reported in that year was around 500, but by 2004 that number had swelled to over 4,500. But it is not just the sheer number of vulnerabilities that is worrisome; it is also the speed at which the vulnerabilities are now being successfully exploited.

The Nimda worm, which started spreading in April 2001, exploited an Internet Explorer vulnerability for which Microsoft released a patch almost a year prior. The Sasser worm, which struck in May 2004, exploited a Windows vulnerability that had only been identified 18 days before Sasser began to spread.



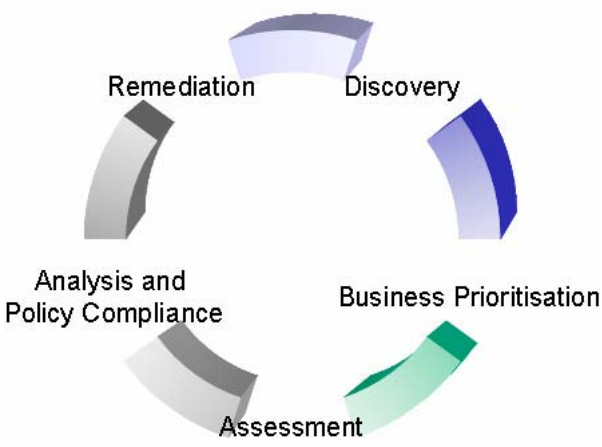
The delay between vulnerability detection and exploitation is shrinking

Without a systematic process to detect, prioritize, delegate and effectively remediate vulnerabilities, enterprises will suffer from successful attacks. In addition, most criminal exploits usually don't advertise their stealth as overtly as public nuisance worms such as Sasser, and thereby are less likely to be detected. Firewalls, antivirus software, intrusion detection systems (IDS) and other security products can give IT administrators a false sense of security of believing that they are shielded from intrusion. Web based attacks that target web and database servers can bypass firewalls and virus scanners using techniques such as SQL injection and buffer overflow opportunities.

Laptops that employees move from network to network are especially vulnerable to exploits that can enter the corporate environment, as well as be the catalyst for exploits entering the corporate network.

Intrusion Detection Systems are installed at the network perimeter but don't usually detect internally generated threats. Those that can are often unable to stop the offending machine from infecting other

Vulnerability Management Business Model:



Model 1

Model 2

Source: Security-Assessment.com

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

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.

Vulnerability Management Process:

There are several steps required to perform regular vulnerability assessment tests in any environment, particularly in an enterprise where other variables, such as centralized management, efficient bandwidth utilization, and non-intrusiveness, must be considered. By consistently executing a sound vulnerability management process, an enterprise can ensure their environment is secure from those who are looking for entrance into a corporate network.

The remainder of this document describes each step in the vulnerability management process.

1. **Discover:**

   Discover and categorize IT asset

   The first step for an organization to assess their network for security vulnerabilities is to understand the assets that make up the network. This step, known as discovery, involves identifying all of the servers, workstations, devices, services, and applications running on the network.

2. **Audit:**

   Scan for vulnerabilities

   The vulnerability audit is the most important step in the vulnerability management process. It entails checking all operating systems, hardware vulnerabilities, application vulnerabilities, system misconfigurations, and policy infractions. In the past, manual network audits, usually performed by an external consultant, could take days or even weeks for large networks. The time can be reduced by automating the process by using some security software.

3. **Delegate:**

   Prioritize remediation effort based on risk

   Once the vulnerability audit is complete, the next step is to prioritize the remediation effort and assign remediation tasks to individuals or teams. Most IT staffs have limited personnel and a limited budget, making it important to prioritize discovered vulnerabilities such that resources are pointed in the optimum direction to maximize efficiency. Remediation priority should be based on the criticality of the vulnerability, which takes into account the likelihood and difficulty of exploitation and the business use and importance of the IT asset.

4. **Remediate:**

   Apply the patch, upgrade or workaround

   The task of remediation the vulnerabilities is usually the most time consuming part of the vulnerability management process. Even with automated patch management tools, push failures, incompatibilities, and false positives can cause a network administrator to spend

most of their day on the remediation effort. Without a clear and efficient remediation plan in place, security managers will waste time and money when patches are applied in the wrong order or critical legacy systems fail.

5. **Confirm:**

   Re-scan and confirm the fix action

   After a patch or fix has been applied, it is important to perform a follow-up scan to verify that the vulnerability has been properly mitigated. Human or machine error during the remediation phase is very common and proper verification can ensure that a false sense of security does not exist, whereby the network remains vulnerable to an issue that was thought to be fixed. Additionally, verification, with the resulting documentation, is an important step for compliance with many laws and regulations such as Sarbanes-Oxley, Gramm-Leach Bliley, and HIPAA.

6. **Report:**

   Report risk assessment

   Proper reporting is a critical step in the vulnerability management process. Reporting can convey lower level tactical information to security administrators on vulnerability information, affected systems, external references, and remediation steps.

   Proper reporting is also an important tool for managers and executives to allow them to gain a strategic understanding of the overall risk of a system. Business leaders rely on concise and relevant reports in order to have the information to make correct business decisions. Executives can be presented with a very high level map of the overall risk across the entire enterprise.

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.

CONCLUSION

Vulnerability Management provides the some 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 interprets test results and prioritizes 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.

Appendix A — Acronyms

Selected acronyms used in *Creating a Patch and Vulnerability Management Program* are defined below.

CVE	Common Vulnerabilities and Exposures
DMZ	Demilitarized Zone
DoS	Denial of Service
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
IP	Internet Protocol
IT	Information Technology
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OMB	Office of Management and Budget
OVAL	Open Vulnerability Assessment Language
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PVG	Patch and Vulnerability Group
RPC	Remote Procedure Call
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
XML	Extensible Markup Language

Appendix B—Glossary

Selected terms used in *Creating a Patch and Vulnerability Management Program* are defined below.

Application: Any data entry, update, query, or report program that processes data for the user.

Accreditation: The process by which certification is reviewed, and formal declaration made that a system is approved to operate and interconnect at an acceptable level of risk.

Administrative Access: An advanced level of access to a computer or application that includes the ability to perform significant configuration changes to the computer's operating system. Also referred to as "privileged access" or "root access".

Availability: Assurance that IT resources remain readily accessible to authorized users.

Backup: A copy of a system's data or applications that can be used if data is lost or corrupted.

Certification: The comprehensive evaluation of the technical and non-technical security features of a system, made in support of the accreditation process that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Adjustment: The act of changing an application's setup. Common configuration adjustments include disabling services, modifying privileges, and changing firewall rules.

Configuration Modification: See "Configuration adjustment".

Exploit Code: A program that allows attackers to automatically break into a system.

Firewall: A program that protects a computer or network from other networks by limiting and monitoring network communication.

Host: A computer or IT device (e.g., router, switch, gateway, firewall). Host is synonymous with the less formal definition of system.

Hotfix: Microsoft's term for a security patch.

Integrity: Assurance that information retains its intended level of accuracy.

Misconfiguration: A configuration error that may result in a security weakness in a system.

Operating System: The master control program that runs a computer.

Patch: An additional piece of code developed to address a problem in an existing piece of software.

Remediation: The act of correcting vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application.

Remediation Plan: A plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation.

Risk: The probability that a particular threat will exploit a particular vulnerability.

Security Plan: Document that details the security controls (management, technical, and operational) established and planned for a particular formally defined system.

System: A set of IT assets, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs; and reside in the same general operating environment. When not used in this formal sense, the term is synonymous with the term "host". The context surrounding this word should make the definition clear or else should specify which definition is being used.

System Administrator: A person who manages the technical aspects of a system.

System Owner: Individual with managerial, operational, technical, and often budgetary responsibility for all aspects of an information technology system.

Threat: Any circumstance or event, deliberate or unintentional, with the potential for causing harm to a system.

Virus: A program designed with malicious intent that has the ability to spread to multiple computers or programs. Most viruses have a trigger mechanism that defines the conditions under which it will spread and deliver a malicious payload of some type.

Vulnerability: A flaw in the design or configuration of software that has security implications. A variety of organizations maintain publicly accessible databases of vulnerabilities.

Workaround: A configuration change to a software package or other information technology resource that mitigates the threat posed by a particular vulnerability. The workaround usually does not fix the underlying problem (unlike a patch) and often limits functionality within the IT resource.

Worm: A type of malicious code particular to networked computers. It is a self-replicating program that works its way through a computer network exploiting vulnerable hosts, replicating and causing whatever damage it was programmed to do.

Appendix C—Patch and Vulnerability Resource Types

This appendix discusses the advantages and disadvantages of the various types of resources that provide information on patches and vulnerabilities. The following resources are discussed:

+ Vendor Web sites and mailing lists

+ Third-party Web sites

+ Third-party mailing lists and newsgroups

+ Vulnerability scanners

+ Vulnerability databases

+ Enterprise patch management tools

+ Other notification tools.

C.1 Vendor Web Sites and Mailing Lists

Vendor Web sites are probably the most popular resource for information about new patches. These sites offer significant amounts of information and are the primary sources for downloading patches. Vendor Web sites offer several advantages:

+ Patches are released by the application vendors who developed and are most familiar with the product.

+ Patches downloaded from vendor Web sites are most likely free of malicious code.

+ Vendors often provide an array of information about vulnerabilities associated with their applications, including methods of mitigation and instructions for installing and using patches.

+ Vendors have unique expertise concerning their products.

Vendor Web sites do have some limitations:

+ Active notification may not be provided, so the site must be visited and reviewed frequently.

+ Numerous vendor Web sites may need to be monitored to encompass all supported products.

+ New vulnerabilities may not be listed in a timely manner, because many vendors will not report the vulnerability until the patch is available. The vulnerability and even exploit information may already have been posted on a third-party Web site or mailing list.

Many large vendors maintain mailing lists that enable them to send e-mail messages and notifications of vulnerabilities, patches, and updates to product users. These lists inform users of new vulnerabilities in a particular vendor's product line without having to regularly visit the vendor's security Web site. A drawback to these lists is that the PVG and system administrators may have to subscribe to numerous vendor lists to manage multiple operating systems or a large number of applications. In addition, vendors may use their mailing lists for marketing purposes, resulting in system administrators ignoring or filtering all messages from the list. Vendors do not generally distribute actual patches within e-mails since e-mail is not a secure delivery mechanism. If patches are distributed in e-mail, they should be digitally signed and the signature checked before being trusted.

C.2 Third-Party Web Sites

A third-party patch or vulnerability Web site is one that is not affiliated with an application vendor, and it may offer more detailed information than a vendor site. These Web sites may cover a large number of vendors and products or may specialize in a specific vendor or product. The Web sites often report new vulnerabilities before the vendor reports them because vendors often delay notification until they have confirmed the vulnerability and created a patch or other mitigation technique. Third-party Web sites offer several advantages:

+ Timely release of information on new vulnerabilities

+ Depending on the site:

– Coverage of more than one vendor or product, allowing the system administrator to visit fewer Web sites to gather information (i.e., "one-stop shopping")

– Specialization in a particular product or platform (saving the system administrators time because they do not have to navigate through unrelated data)

+ For sites that allow site users to post:

– Similar benefits as the third-party mailing lists and newsgroups (see Section C.3)

– A filtering or rating mechanism that allows user to read only "high value" postings

+ Potentially more acceptable alternatives to the official mitigation techniques provided by the vendor

+ Information that the vendor chooses not to provide.

Third-party Web sites have some disadvantages:

+ More likely for third-party patches to have unintended consequences or contain malicious code

+ No comprehensive information on patching the vulnerability, requiring the research of multiple resources.

C.3 Third-Party Mailing Lists and Newsgroups

Mailing lists and newsgroups are threaded discussion groups that rely on e-mail. They are a way for users with similar interests to communicate with each other. The primary advantage of third-party mailing lists and newsgroups is that they allow system administrators and other users to interact in two-way communications, whereas vendor mailing lists support only one-way (vendor to user) communications. This allows system administrators to share their experiences and to ask questions. The principal difference between a newsgroup and mailing list is that a newsgroup is an "officially" recognized Internet forum and, as such, can only be established by following certain procedures. In contrast, anybody with a mail server and Internet access can set up a mailing list. Mailing lists may be moderated and participation controlled.

The advantages of third-party mailing lists and newsgroups are as follows:

+ Allow interaction between system administrators

+ Reduce the number of sites that a system administrator is required to search actively

+ Allow a system administrator to learn directly from the experiences of others (e.g., are there problems associated with a particular patch, does it really correct the problem)

+ May provide a workaround to be used until a patch is released.

The disadvantages of third-party mailing list and newsgroups are as follows:

+ Generate a large number of e-mails that may not be useful to system administrators

+ Potentially release sensitive information to unauthorized entities (a system administrator who asks questions relating to a system can inadvertently invite an attacker to try to exploit that vulnerability)

+ Potentially increase exposure to malicious code because third-party fixes and workarounds are often created by unaccountable parties

+ Expose an organization to unsolicited advertising (spam)

+ Possibly provide inaccurate information

+ May provide links to self-testing sites that automatically launch an exploit against hosts that visit the site (this may cause problems if an unpatched system visits the site).

C.4 Vulnerability Scanners

Vulnerability scanners are commonly used in many organizations to identify vulnerabilities on their hosts and networks. Vulnerability scanners employ large databases of vulnerabilities to identify vulnerabilities associated with commonly used operating systems and applications. There are two types of vulnerability scanners: network scanners and host scanners. Network scanners are used for identifying open ports, vulnerable software, and misconfigured services. Host scanners are used for identifying specific operating system and application

misconfigurations and vulnerabilities. Refer to Section 2.9.1 for more information about vulnerability scanners.

Vulnerability scanners can:

+ Proactively identify vulnerabilities

+ Provide a fast and easy way to measure exposure

+ Automatically fix discovered vulnerabilities

+ Identify out-of-date software versions

+ Validate compliance with an organizational security policy

+ Generate alerts and reports about identified vulnerabilities.

However, vulnerability scanners do have some weaknesses. Scanners:

+ Depend on regular updating of the vulnerability database

+ Tend to have a high false positive error rate

+ May generate significant amounts of network traffic

+ May cause a denial of service (DoS) of hosts, because scanner probing may cause a system to crash inadvertently.

C.5 Vulnerability Databases

Vulnerability databases are collections of searchable information on vulnerabilities that affect information systems. Many of these databases are publicly accessible via the Web. These Web sites are generally run by third parties not affiliated with software vendors, and can provide a wealth of information to system administrators and security professionals. They strive to cover most operating systems and software applications. Because they are not affiliated with software vendors, they often provide information that the vendor, or other organizations affiliated with the vendor, does not provide.

Vulnerability databases tend to be the quickest to report new vulnerabilities, which is both a benefit and a disadvantage. The provision of timely information on vulnerabilities can be critical to the success of a system administrator in securing a network.

Although the quantity and quality of information vary to some degree from site to site, vulnerability databases typically include the following types of information:

+ **Vulnerability Overview**—An introduction to the vulnerability that includes the CVE name; type of vulnerability; date the vulnerability was first publicly identified; date the vulnerability or patch information was last updated; and the operating system, application, or hardware affected by the vulnerability.

+ **Discussion or Analysis**—Detailed information on the vulnerability, from one paragraph to several pages, depending on the complexity of the vulnerability. This discussion may be highly technical.

+ **Solution**—A detailed discussion on mitigating or eliminating the vulnerability. Generally contains hyperlinks to the pertinent vendor's Web site for patches and updates. If available, other remediation techniques will typically be included.

+ **Exploit**—Information on exploiting the vulnerability and any applicable code, or links to other sites that have more information and exploit code. This information can be useful to the system administrator in determining whether a system is susceptible to exploitation (before or after the patch is applied). However, great care should be exercised in using these techniques so as not to cause unintended harm to systems.

Overall, vulnerability databases are one of the most powerful resources available. Even if other sources are principally relied upon for vulnerability information, the general news and discussions provided on the vulnerability database sites can prove invaluable.

C.6 Enterprise Patch Management Tools

The number of vulnerabilities and corresponding patches continues to grow, making manual patching of computers more difficult and less effective. Therefore, the majority of an organization's systems should participate in an enterprise patch management program. Enterprise

patch management tools scan for vulnerabilities on computers participating in this patching solution, provide information regarding needed patches and other software updates on those computers, and allow an administrator to decide on the patching process.

There are two primary categories of enterprise patch management tools, those with agents and those that are agent-less. Both approaches typically involve a central computer that stores the patches that should or could be installed, as well as a console for the patching administrator to control the process. Each approach has advantages and disadvantages that should be considered. The primary advantage of agent-less patch management tools is that there is no need to install software agents on the computers involved in the patching solution. However, agent-less tools can consume significant amounts of network bandwidth and may take a greater amount of time to scan larger networks. Agent-based solutions scan larger networks more quickly and use a minimal amount of network bandwidth, but require the installation and management of software agents on each participating system. Section 4.1 provides detailed information about enterprise patching solutions.

Automated patch management tools and utilities are available from various vendors to assist in the identification of known vulnerabilities and automate the patch and vulnerability management process. The guidance provided in this document is an adjunct, not a substitute, for the documentation and recommendations of the product vendors.

C.7 Other Notification Tools

Because the task of keeping up with reports of vulnerabilities, releases of patches, and publishing of exploits has become more burdensome, various tools and applications have been created to provide the PVG and system administrators with automated and customized notifications for the systems they support. These tools are provided by vendors and third parties. Some products are free, while others require a one-time fee or subscription.

The advantages of these notification tools are as follows:

+ Customized notification limited to those applications and operating systems of interest

+ Real-time alerts to the system administrator (e.g., not requiring them to visit a Web page).

The disadvantages of these notification tools are as follows:

+ Cost (for fee-based services)

+ Information quality (these sources are only as good as the underlying information database)

+ Lag time inherent in certain services

+ Somewhat invasive, since an administrator must tell a third party which operating systems and applications are in use.

Appendix D—Patch and Vulnerability Resources

The lists below provide examples of resources such as software and Web sites that may be helpful in identifying known vulnerabilities and locating, acquiring, and applying patches for common operating systems and applications.

Common Patch Management Software

Software Name	Vendor	URL
Altiris Patch Management Solution	Altiris	http://www.altiris.com/products/patchmanagement/
ANSA	Autonomic Software, Inc.	http://www.autonomic-software.com/patch.html
BigFix Patch Manager	BigFix, Inc.	http://www.bigfix.com/products/products_patch.html
BindView Patch Management	Bindview Corporation	http://www.bindview.com/Solutions/VulnMgmt/ManagePatches.cfm
C5 Enterprise Vulnerability Management Suite	Secure Elements	http://www.secure-elements.com/products/
Ecora Patch Manager	Ecora Software	http://www.ecora.com/ecora/products/patchmanager.asp
eTrust Vulnerability Manager	Computer Associates International, Inc.	http://www3.ca.com/Solutions/Product.asp?ID=4707
GFI LANguard Network Security Scanner	GFI Software Ltd.	http://www.gfi.com/lannetscan/
Hercules	Citadel Security Software	http://www.citadel.com/hercules.asp
HFNetChkPro	Shavlik Technologies, LLC	http://www.shavlik.com/
HP OpenView Patch Manager using Radia	Hewlett-Packard Development Company	http://www.managementsoftware.hp.com/products/radia_patm/index.html
Kaseya Patch Management	Kaseya, Inc.	http://www.kaseya.com/prod1/pl/patch_management.phtml
LANDesk Patch Manager	LANDesk Software	http://www.landesk.com/Products/Patch/Index.aspx
LiveState Patch Manager	Symantec Corporation	http://sea.symantec.com/content/product.cfm?productid=30
ManageSoft Security Patch Management	ManageSoft Corporation Ltd.	http://www.managesoft.com/product/patchmanagement/index.xml
Marimba Patch Management	BMC Software, Inc.	http://www.marimba.com/products/solutions/patch-mgmt.html
NetIQ Vulnerability Manager	NetIQ Corporation	http://www.netiq.com/products/vsm/default.asp
Opsware Server Automation System	Opsware, Inc.	http://www.opsware.com/products/serverautomation/patchmgmt/
PatchLink Update	PatchLink Corporation	http://www.patchlink.com/products_services/patchlink_update.html
PolicyMaker Software Update	DesktopStandard Corporation	http://www.desktopstandard.com/PolicyMakerSoftwareUpdate.aspx
Prism Patch Manager	New Boundary Technologies	http://www.newboundary.com/products/prismpatch/prismpatch_info.htm
SecureCentral PatchQuest	AdventNet, Inc.	http://www.securecentral.com/products/patchquest/
Security Update Manager	ConfigureSoft	http://www.configuresoft.com/SUMMain.aspx

Software Name	Vendor	URL
Service Pack Manager	Gravity Storm Software	http://www.securitybastion.com/
Sitekeeper (Patchkeeper module)	Executive Software	http://www.execsoft.com/sitekeeper/sitekeeper.asp
Software Update Services	Microsoft Corporation	http://www.microsoft.com/windowsserversystem/updateservices/evaluation/previous/default.mspx
Systems Management Server	Microsoft Corporation	http://www.microsoft.com/smserver/default.asp
SysUpdate	SecurityProfiling Inc.	http://www.securityprofiling.com/eng/products/sysupdate.shtml
UpdateEXPERT	St. Bernard Software	http://www.patches-management.stbernard.com/
Windows Server Update Services	Microsoft Corporation	http://www.microsoft.com/windowsserversystem/updateservices/default.mspx
ZENworks Patch Management	Novell, Inc.	http://www.novell.com/products/zenworks/patchmanagement/index.html

Common Operating Systems

Web Site or Page Name	URL
Apple	
Apple Support	http://www.apple.com/support/
Apple Downloads	http://www.apple.com/support/downloads/
BSD	
FreeBSD Security Information	http://www.freebsd.org/security/index.html
Getting FreeBSD	http://www.freebsd.org/where.html
OpenBSD Security	http://www.openbsd.org/security.html
Getting OpenBSD	http://www.openbsd.org/ftp.html
Cisco	
Cisco Product Security Incident Response	http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
Improving Security on Cisco Routers	http://www.cisco.com/warp/public/707/21.html
Products & Services Security Advisories	http://www.cisco.com/en/US/products/products_security_advisories_listing.html
Technical Support & Documentation	http://www.cisco.com/en/US/support/index.html
Linux[40]	
Debian GNU/Linux Security Information	http://www.debian.org/security/
Getting Debian	http://www.debian.org/distrib/
Fedora Download	http://fedora.redhat.com/download/
How to Download [Fedora] Updates	http://fedora.redhat.com/download/updates.html
Mandriva Linux Download	http://www.mandrivalinux.com/en/ftp.php3
Mandriva Security Advisories	http://www.mandriva.com/security/
Ubuntu Linux Download	http://www.ubuntulinux.org/download/
Ubuntu Support	http://www.ubuntulinux.org/support/
Microsoft	

[40] This table lists some of the most popular Linux distributions of the hundreds available. For information on other distributions, see DistroWatch.com (http://distrowatch.com/).

Web Site or Page Name	URL
Microsoft Download Center	http://www.microsoft.com/downloads/search.aspx?displaylang=en
Microsoft Help and Support	http://support.microsoft.com/default.aspx
Microsoft Security Home Page	http://www.microsoft.com/security/default.mspx
Microsoft Security Notification Service	http://www.microsoft.com/technet/security/bulletin/notify.mspx
Microsoft Windows Update	http://windowsupdate.microsoft.com/
Security Bulletins	http://www.microsoft.com/security/bulletins/alerts.mspx
Novell	
Novell Security	http://www.novell.com/products/security.html
Novell Support	http://support.novell.com/
Sun	
Solaris Download	http://www.sun.com/software/solaris/get.jsp
Solaris Live Upgrade	http://www.sun.com/software/solaris/liveupgrade/
Sun Update Connection--Patches and Updates	http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage
SunSolve Online	http://sunsolve.sun.com/

Common Client Applications

Product Line	Vendor	URL
Compression Utilities		
7-Zip	7-Zip/Igor Pavlov	http://www.7-zip.org/download.html
ArchiveXpert	Concepts for Future	http://archivexpert.com/download/
PicoZip	Acubix	http://www.picozip.com/downloads.html
PKZip	PKWare	http://www.pkware.com/business_and_developers/support/updates/
PowerArchiver	ConeXware, Inc.	http://www.powerarchiver.com/download/
PowerZip	Trident Software Pty Ltd	http://www.powerzip.biz/download.aspx
SecureZip	PKWare	http://www.pkware.com/business_and_developers/support/updates/
StuffIt	Allume Systems Inc.	http://www.stuffit.com/
WinZip	WinZip Computing	http://www.winzip.com/downwzeval.htm
ZipMagic	Allume Systems Inc.	http://www.stuffit.com/win/zipmagic/
E-mail Clients		
Balsa	GNOME Project	http://balsa.gnome.org/download.html
Barca	Poco Systems, Inc.	http://www.pocosystems.com/home/index.php?option=content&task=category&sectionid=2&id=21&Itemid=38
Eudora	Qualcomm	http://www.eudora.com/download/
Eureka Email	Eureka Email	http://www.eureka-email.com/Download.html
GNUMail.app	Collaboration-world.com	http://www.collaboration-world.com/cgi-bin/project/release.cgi?pid=2
GyazMail	GyazSquare	http://www.gyazsquare.com/gyazmail/download.php
i.Scribe	Memecode Software	http://www.memecode.com/scribe.php
InScribe	Memecode Software	http://www.memecode.com/inscribe.php

Product Line	Vendor	URL
KMail	Kmail	http://kmail.kde.org/download.html
Mac OS X Mail	Apple	http://www.apple.com/support/panther/mail/
Mailsmith	Bare Bones Software	http://www.barebones.com/support/mailsmith/updates.shtml
Mercury Mail Transport System	David Harris	http://www.pmail.com/patches.htm
Mozilla	Mozilla	http://www.mozilla.org/security/
Mutt	Mutt	http://www.mutt.org/download.html
Nisus Email	Nisus Software	http://www.nisus.com/NisusEmail/FAQ.php?PHPSESSID=0ba9f9639672d1fdf836a97f3ad29383#HowUpgradeOS9
Outlook	Microsoft	http://office.microsoft.com/en-us/officeupdate/default.aspx
Outlook Express	Microsoft	http://www.microsoft.com/downloads/search.aspx?displaylang=en&categoryid=7
Pegasus Mail	David Harris	http://www.pmail.com/patches.htm
Pine	University of Washington	http://www.washington.edu/pine/getpine/
PocoMail	Poco Systems, Inc.	http://www.pocosystems.com/home/
Sylpheed	Sylpheed	http://sylpheed.good-day.net/
Thunderbird	Mozilla	http://www.mozilla.org/products/thunderbird/
VM	VM	http://www.wonderworks.com/vm/download.html
FTP Clients		
BulletProof FTP Client	BulletProof Software	http://www.bpftp.com/download.php
CuteFTP Professional	GlobalSCAPE	http://www.cuteftp.com/downloads/cuteftppro.asp
FileZilla	FileZilla	http://sourceforge.net/projects/filezilla/
FlashFXP	IniCom Networks	http://www.flashfxp.com/download.php
FTP Voyager	Rhino Software	http://www.ftpvoyager.com/dn.asp
gFTP	Brian Masney	http://gftp.seul.org/
NcFTP	NcFTP Software	http://www.ncftp.com/download/
SmartFTP	SmartFTP	http://www.smartftp.com/download/
Transmit 3	Panic, Inc.	http://www.panic.com/transmit/index.html
WS_FTP Professional	Ipswitch	http://www.ipswitch.com/support/WS_FTP/patch-upgrades.html
Instant Messaging Clients		
AOL Instant Messenger	AOL	http://www.aim.com/download.adp?aolp=1
GAIM	GAIM	http://gaim.sourceforge.net/downloads.php
Jabber	Jabber, Inc.	http://www.jabber.com/index.cgi?CONTENT_ID=503
Lumen Instant Messenger	Novell	http://www.novell.com/partnerguide/product/200671.html
Miranda	Miranda	http://sourceforge.net/project/showfiles.php?group_id=94142
MSN Messenger	Microsoft	http://messenger.msn.com/Download/
Trillian	Cerulean Studios	http://www.download.com/Trillian/3000-2150-10047473.html
Vypress Messenger	Vypress	http://www.vypress.com/products/messenger/

Product Line	Vendor	URL
Windows Messenger	Microsoft	http://www.microsoft.com/downloads/search.aspx?displaylang=en
Yahoo Messenger	Yahoo	http://messenger.yahoo.com/messenger/security/
Multimedia Utilities		
Flash	Macromedia	http://www.macromedia.com/downloads/
iTunes	Apple	http://www.apple.com/itunes/download/
QuickTime	Apple	http://www.apple.com/support/
Real Player	Real	http://service.real.com/realplayer/security/
Shockwave	Macromedia	http://www.macromedia.com/downloads/
Winamp	Winamp	http://www.winamp.com/player/free.php
Windows Media Player	Microsoft	http://www.microsoft.com/windows/windowsmedia/player/download/download.aspx
Office Productivity Tools		
Acrobat	Adobe	http://www.adobe.com/support/downloads/main.html
AppleWorks	Apple	http://www.apple.com/support/appleworks/
Microsoft Office	Microsoft	http://office.microsoft.com/en-us/officeupdate/default.aspx?displaylang=EN
Microsoft Works	Microsoft	http://www.microsoft.com/products/works/downloads.mspx
NeoOffice	NeoOffice	http://www.planamesa.com/neojava/en/download.php
OpenOffice	OpenOffice.org	http://www.openoffice.org/
StarOffice	Sun	http://www.sun.com/download/index.jsp?cat=Patches%20%26%20Updates&tab=3
WordPerfect Office	Corel	http://www.corel.com/servlet/Satellite?pagename=Corel3/Downloads/SupportDownloads
SSH Clients		
OpenSSH	OpenBSD Project	http://www.openssh.com/
PuTTY	Simon Tatham	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
Reflection for Secure IT	AttachmateWRQ	http://download.wrq.com/
SecureCRT	VanDyke Software	http://www.vandyke.com/support/index.html
SSH Tectia	SSH Communications Security	http://www.ssh.com/support/downloads/
Web Browsers		
Camino	Mozilla	http://www.caminobrowser.org/
Firefox	Mozilla	http://www.mozilla.org/security/
Internet Explorer	Microsoft	http://www.microsoft.com/windows/ie/downloads/default.mspx
Konqueror	KDE	http://www.kde.org/download/
Mozilla Suite	Mozilla	http://www.mozilla.org/security/
Netscape	Netscape Communications	http://channels.netscape.com/ns/browsers/default.jsp
Opera	Opera Software	http://www.opera.com/download/
Safari	Apple	http://www.apple.com/support/downloads/safari.html

Common Server Applications

Product Name	Vendor	URL
Application Servers		
Apache Tomcat	Apache Foundation	http://jakarta.apache.org/site/downloads/downloads_tomcat.html
BEA Web Logic Server	BEA Systems	http://commerce.bea.com/index.jsp
Borland Enterprise Server	Borland	http://www.borland.com/downloads/download_bes.html
Flash Communication Server	Macromedia	http://www.macromedia.com/support/flashcom/downloads_updaters.html
HAHTsite	HAHT Commerce	http://www.haht.com/HAHTsite/
IBM WebSphere Application Server	IBM	http://www.ibm.com/products/finder/us/finders?pg=ddfinder
Interbase	Borland	http://www.borland.com/downloads/download_interbase.html
JBoss	JBoss	http://www.jboss.org/downloads/index
JRun Application Server	Macromedia	http://www.macromedia.com/support/jrun/updaters.html
Oracle Application Server	Oracle	http://www.oracle.com/technology/software/products/ias/index.html
Orion Application Server	Orion	http://www.orionserver.com/
Pramati Server	Pramati Technologies	http://www.pramati.com/index.jsp?id=downloads_archive&product=psv
Sun Java System Application Server	Sun	http://www.sun.com/download/index.jsp?cat=Patches%20%26%20Updates&tab=3
Zope	Zope Community	http://www.zope.org/Products/
Collaboration Servers		
GroupWise	Novell	http://support.novell.com/support_options.html
Lotus Domino	IBM	http://www-132.ibm.com/content/home/store_IBMPublicUSA/en_US/Upgrades.html
Novell Evolution	Novell	http://support.novell.com/support_options.html
SUSE Linux OpenExchange Server	Novell	http://www.novell.com/products/openexchange/download.html
TeamWare Office	TeamWare Group	http://www.teamware.net/Resource.phx/download/index.htx
WebBoard	Akiva	http://www.akiva.com/downloads/index.cfm?id=webboard
Windows SharePoint Services	Microsoft	http://www.microsoft.com/windowsserver2003/technologies/sharepoint/default.mspx
Database Servers		
DB2	IBM	https://www-927.ibm.com/search/SupportSearchWeb/SupportSearch?pageCode=SBD&brand=db2
Informix	IBM	http://www-306.ibm.com/software/data/informix/support/
Microsoft SQL Server	Microsoft	http://www.microsoft.com/sql/downloads/default.asp
MySQL	MySQL	http://dev.mysql.com/downloads/

Product Name	Vendor	URL
Oracle	Oracle	http://www.oracle.com/technology/software/index.html
Pervasive PSQL	Pervasive Software	http://www.pervasive.com/support/updates/?product=psql
PostgreSQL	PostgreSQL Global Development Group	http://www.postgresql.org/ftp/source/
DNS Servers		
BIND	Internet Systems Consortium	http://www.isc.org/index.pl?/sw/bind/
djbdns	D. J. Bernstein	http://cr.yp.to/djbdns/install.html
Microsoft DNS	Microsoft	http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/dns/default.mspx
Nominum Foundation	Nominum	http://www.nominum.com/open_source_support.php?stype=2&sind=2
NSD	NLnet Labs	http://www.nlnetlabs.nl/nsd/index.html
PowerDNS	PowerDNS	http://www.powerdns.com/en/downloads.aspx
E-mail Servers		
602LAN Suite	Software602	http://support.software602.com/updates/
ArGoSoft Mail Server	ArGoSoft	http://www.argosoft.com/mailserver/download.aspx
CommuniGate Pro	Stalker Software	http://www.stalker.com/CommuniGatePro/
Eudora Internet Mail Server (EIMS)	Glenn Anderson	http://www.eudora.co.nz/updates.html
Eudora WorldMail Server	Qualcomm	http://www.eudora.com/download/worldmail/
Exim	Exim	http://www.exim.org/
IMail Server	Ipswitch	http://www.ipswitch.com/support/imail/releases/imail_professional/index.asp
inFusion Mail Server	CoolFusion	http://www.coolfusion.com/downloads/
Kaspersky SMTP Gateway for UNIX	Kaspersky	http://www.kaspersky.com/productupdates/
Kerio MailServer	Kerio Technologies	http://www.kerio.com/subscription.html
Lotus Domino	IBM	http://www-132.ibm.com/content/home/store_IBMPublicUSA/en_US/Upgrades.html
MailEnable	MailEnable	http://www.mailenable.com/hotfix/default.asp
MailMax	Smartmax Software	http://www.smartmax.com/mmupgradecenter.aspx
MailSite	Rockliffe	http://www.rockliffe.com/userroom/download.asp
MDaemon	alt-n Technologies	http://www.altn.com/download/default.asp?product_id=MDaemon
Merak Mail Server	Merak	http://www.merakmailserver.com/Download/
Microsoft Exchange	Microsoft	http://www.microsoft.com/exchange/downloads/2003/default.mspx
Postfix	Wietse Venema	http://www.postfix.org/download.html
Sendmail (commercial version)	Sendmail, Inc.	http://www.sendmail.com/support/download/patch_page.shtml
sendmail (freeware version)	Sendmail Consortium	http://www.sendmail.org/
Xmail	Davide Libenzi	http://www.xmailserver.org/

Product Name	Vendor	URL
FTP Servers		
ArGoSoft FTP Server	ArGoSoft	http://www.argosoft.com/ftpserver/upgrade.aspx
BulletProof FTP Server	BulletProof Software	http://www.bpftpserver.com/download.php
CrushFTP Server	CrushFTP	http://www.crushftp.com/download.html
GuildFTPd FTP Server Daemon	GuildFTPd	http://www.guildftpd.com/
RaidenFTPD	Raiden	http://www.raidenftpd.com/en/download.html
Rumpus FTP	Maxum Development Corporation	http://www.maxum.com/Rumpus/Upgrades.html
Secure FTP Server	GlobalSCAPE	http://www.cuteftp.com/gsftps/upgrade.asp
Serv-U FTP Server	Serv-U	https://rhinosoft.com/custsupport/index.asp?prod=rs
SurgeFTP	NetWin	http://netwinsite.com/cgi-bin/keycgi.exe?cmd=download&product=surgeftp
Titan FTP Server	South River Technologies	http://www.southrivertech.com/index.php?pg=./download/index&pgr=./purchase/index
Vermillion FTP Daemon	Arcane Software, Inc.	http://www.arcanesoft.com/
WS_FTP Server	Ipswitch	http://www.ipswitch.com/support/ws_ftp-server/patch-upgrades.asp
Web Servers		
4D WebSTAR	4D	http://www.4d.com/products/downloads_4dws.html
AOLserver	AOLserver	http://aolserver.sourceforge.net/
Apache HTTP Server	Apache Foundation	http://www.apache.org/dist/httpd/
Commerce Server/400	iNet	http://www.inetmi.com/iseries/commerce/ptf.html
Jigsaw	W3C	http://www.w3.org/Jigsaw/
Microsoft Internet Information Services	Microsoft	http://www.microsoft.com/technet/security/prodtech/IIS.mspx
RaidenHTTPD	Raiden	http://www.raidenhttpd.com/en/download.html
Roxen WebServer	Roxen Internet Software	http://download.roxen.com/4.0/
Sambar Server	Sambar Technologies	http://www.sambar.com/download.htm
SimpleServer:WWW	AnalogX	http://www.analogx.com/contents/download/network/sswww.htm
Sun Java System Web Server	Sun	http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage
Tcl Web Server	Tcl Developer Exchange	http://www.tcl.tk/software/tclhttpd/
Zeus Web Server	Zeus Technology	http://support.zeus.com/doc/zws/v4/supported_versions.html

Common Enterprise Firewalls

Product Line	Vendor	URL
BorderWare Firewall Server	BorderWare Technologies	http://www.borderware.com/support/
Cisco PIX	Cisco Systems	http://www.cisco.com/en/US/support/index.html
CyberGuard	CyberGuard Corporation	http://www.cyberguard.com/support/index.html?lang=de_EN
DX	Resilience Corporation	http://www.resilience.com/support/support.html
Firebox	WatchGuard Technologies, Inc.	http://www.watchguard.com/archive/service.asp
FireWall-1	Check Point Software Technologies	http://www.checkpoint.com/downloads/index.jsp
FortiGate	Fortinet	http://support.fortinet.com/
GB	Global Technology Associates	http://www.gta.com/support/upgrade/
Kerio Server Firewall	Kerio Technologies, Inc.	http://www.kerio.com/ksf_download.html
NetScreen	Juniper Networks, Inc.	http://www.juniper.net/customers/support/
Sidewinder	Secure Computing Corporation	http://www.securecomputing.com/index.cfm?skey=246
SonicWALL	SonicWALL	http://www.sonicwall.com/products/gav_ips_spyware.html
Sun Cobalt	Sun	http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/index&nav=patchpage
Symantec Enterprise Firewall	Symantec Corporation	http://www.symantec.com/downloads/

Common Enterprise Network Intrusion Detection and Prevention Systems

Product Line	Vendor	URL
Attack Mitigator	Top Layer Networks	http://www.toplayer.com/content/support/index.jsp
Bro	Vern Paxson	http://bro-ids.org/download.html_
Captus	Captus Networks	http://www.captusnetworks.com/info/support/index.html
Cisco IPS	Cisco Systems	http://www.cisco.com/en/US/support/index.html
Cyclops	e-Cop.net	http://www.e-cop.net/_
DefensePro	Radware, Ltd.	http://www.radware.com/content/security/serviceinfo/default.asp_
Dragon	Enterasys Networks, Inc.	https://dragon.enterasys.com/
eTrust Intrusion Detection	Computer Associates	http://www.my-etrust.com/Support/TechSupport.aspx
IntruShield	Network Associates	http://www.mcafee.com/us/downloads/default.asp
iPEnforcer	iPolicy Networks	http://www.ipolicynetworks.com/support/index.html
ManHunt	Symantec Corporation	http://www.symantec.com/techsupp/enterprise/select_product_updates_nojs.html
Mazu Enforcer	Mazu Networks, Inc.	https://supportcenteronline.com/ics/support/default.asp?deptID=735
NetDetector	Niksun	http://www.niksun.com/Support_Technical_Support.htm
Netscreen	Netscreen Technologies	http://www.juniper.net/customers/csc/software/

Product Line	Vendor	URL
Proventia	Internet Security Systems	http://www.iss.net/support/
SecureNet	Intrusion Inc.	https://serviceweb.intrusion.com/
Sentivist	NFR Security	http://www.nfr.com/solutions/support.php
Snort	Sourcefire	http://www.snort.org/dl/
Sourcefire	Sourcefire	http://www.sourcefire.com/services/support.html
StealthWatch	Lancope	http://www.lancope.com/customers/
StoneGate	StoneSoft Corporation	http://www.stonesoft.com/support/
Strata Guard	StillSecure	http://www.stillsecure.com/strataguard/support/updates.php
UnityOne	TippingPoint Technologies	http://www.tippingpoint.com/support.html
V-Secure	V-Secure Technologies, Inc.	http://www.v-secure.com/support/packages_bundles.asp

Common Enterprise Antivirus and Antispyware Software[41]

Web Site	URL
Central Command Vexira AntiVirus	
Downloads	http://www.centralcommand.com/downloads.html
Latest Version Numbers	http://www.centralcommand.com/versions.html
Support	http://www.centralcommand.com/support.html
Computer Associates eTrust Antivirus	
Computer Associates Security Advisory	http://www3.ca.com/securityadvisor/
Computer Associates Support	http://www3.ca.com/support/
Computer Associates Virus Information Center	http://www3.ca.com/securityadvisor/virusinfo/default.aspx
F-Secure Anti-Virus	
F-Secure Radar	http://www.f-secure.com/products/radar/
F-Secure Security Information Center	http://www.f-secure.com/virus-info/
F-Secure Support	http://support.f-secure.com/enu/home/
Lavasoft Ad-Aware	
Download, Support, Upgrade Center	http://www.lavasoftusa.com/
Microsoft Windows AntiSpyware (Beta)	
Using Microsoft Windows AntiSpyware (Beta)	http://www.microsoft.com/athome/security/spyware/software/howto/default.mspx
Network Associates McAfee VirusScan	
Downloads	http://www.mcafee.com/us/downloads/default.asp
McAfee AVERT Alerts	http://vil.nai.com/vil/content/alert.htm
McAfee AVERT Virus Information Library	http://vil.nai.com/vil/default.asp
Sophos Anti-Virus	
Download Latest Virus Identity Files	http://www.sophos.com/downloads/ide/
Sophos Email Notification	http://www.sophos.com/virusinfo/notifications/
Sophos Virus Analyses	http://www.sophos.com/virusinfo/analyses/
Spybot-Search & Destroy	

[41] This table lists some of the most popular antivirus and antispyware products. For information on other products, see the listing at the Virus Bulletin Web site located at http://www.virusbtn.com/resources/links/index.xml?ven.

Web Site	URL
Downloads	http://www.safer-networking.org/en/download/index.html
Support	http://www.safer-networking.org/en/support/index.html
Symantec AntiVirus	
Symantec Downloads	http://www.symantec.com/downloads/
Symantec Support	http://www.symantec.com/techsupp/
Symantec Security Response—Search and Latest Virus Threats Page	http://securityresponse.symantec.com/avcenter/vinfodb.html
Symantec Security Response—Alerting Offerings	http://securityresponse.symantec.com/avcenter/alerting_offerings.html
Trend Micro Anti-Spyware and VirusWall	
Support	http://kb.trendmicro.com/solutions/search/default.asp
Trend Micro Virus Encyclopedia Search	http://www.trendmicro.com/vinfo/virusencyclo/
Trend Micro Newsletters	http://www.trendmicro.com/subscriptions/default.asp

Other Common Security Applications

Product Line	Vendor	URL
Anti-Spam Servers		
Anti-Spam SMTP Proxy (ASSP) Server	ASSP Server Project	http://sourceforge.net/project/showfiles.php?group_id=69172
BitDefender AntiSpam for Mail Servers	Softwin	http://www.bitdefender.com/site/Main/view/Server-Products-Updates.html
GFiMailEssentials	GFI Software	http://support.gfi.com/
Kaspersky Anti-Spam	Kaspersky	http://www.kaspersky.com/productupdates/
MailShield Server	Lyris Technologies	http://www.lyris.com/store/mailshield/server/upgrade.html?s=sdbr
McAfee SPAMkiller	Network Associates	http://www.mcafee.com/us/downloads/default.asp
Merak Instant Anti Spam	Merak	http://www.merakmailserver.com/Download/
MIMEsweeper	Clearswift	http://www.clearswift.com/support/msw/patch.aspx
NetIQ MailMarshal	NetIQ	http://www.netiq.com/support/default.asp
SPAMfighter	SPAMfighter	http://www.spamfighter.com/Tutorial_Update.asp
Personal Firewalls and Suites		
BlackIce	Internet Security Systems	http://blackice.iss.net/update_center/
F-Secure Internet Security 2005	F-Secure	http://support.f-secure.com/enu/home/
Kaspersky Anti-Hacker	Kaspersky Labs	http://www.kaspersky.com/productupdates
Kerio Personal Firewall	Kerio Technologies	http://www.kerio.com/kpf_download.html
McAfee Personal Firewall Plus	Networks Associates Technology, Inc.	http://download.mcafee.com/us/upgradeCenter/?cid=11536

Product Line	Vendor	URL
Norton Personal Firewall	Symantec	http://www.symantec.com/downloads/
Panda Platinum Internet Security	Panda Software	http://www.pandasoftware.com/download/
PC-cillin Internet Security	Trend Micro	http://www.trendmicro.com/download/product.asp?productid=32
Sygate Personal Firewall	Sygate	http://smb.sygate.com/download_buy.htm
Tiny Firewall	Tiny Software	http://www.tinysoftware.com/home/tiny2?s=5375286922906826215A1&&pg=content05&an=tf6_download&cat=cat_tf6
ZoneAlarm	Zone Labs	http://download.zonelabs.com/bin/free/information/zap/releaseHistory.html
VPN Clients		
Cisco VPN Client	Cisco	http://www.cisco.com/public/sw-center/
NetScreen-Remote	Juniper	http://www.juniper.net/customers/support/
Nortel VPN Client	Nortel	http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=software&tranProduct=10621
ProSafe VPN Client	Netgear	http://kbserver.netgear.com/downloads_support.asp
SafeNet SoftRemote	CyberGuard	http://www.cyberguard.com/support/
VPN-1 SecuRemote, SecureClient	CheckPoint	http://www.checkpoint.com/downloads/index.html
Wireless IDS/IPS		
AirDefense	AirDefense	http://www.airdefense.net/support/
AirMagnet	AirMagnet	http://www.airmagnet.com/support/index.htm
AiroPeek	WildPackets	http://www.wildpackets.com/support/downloads
AirPatrol	Cirond	http://www.cirond.com/support.php
BlueSecure	BlueSocket	http://www.bluesocket.com/products/intrusionprotection.html
Highwall	Highwall Technologies	http://www.highwalltech.com/support.cfm
Red-Detect	Red-M	http://www.red-m.com/Support/
RFprotect	Network Chemistry	http://www.networkchemistry.com/support/
SpectraGuard	AirTight Networks	http://www.airtightnetworks.net/support/support_overview.html

General Vulnerability Management Resources

Resource Name	URL
US-CERT National Cyber Alert System	http://www.us-cert.gov/cas/
US-CERT National Vulnerability Database	http://nvd.nist.gov/
US-CERT Vulnerability Notes Database	http://www.kb.cert.org/vuls/
Open Source Vulnerability Database	http://www.osvdb.org/
SecurityFocus Vulnerability Database	http://www.securityfocus.com/vulnerabilities

CITATIONS

1. http://www.protiviti.com
2. http://nvd.nist.gov
3. **Vulnerability Management & External Penetration**, January 2006 Presentation in Trustworthy Computing, Andrew Retrum, CISSP – Manager
4. **An Executive's Guide to Vulnerability Management**: How to Save Time and Money by Using Managed Services to Find and Fix Critical Security Exposures, ISS 2005
5. **Enterprise Vulnerability Management**, Rapid7 Security, March 2006
6. **The Value of Vulnerability Management**, Robert Buchheit (Director), PwC
7. Jason Weile, Manager, Systems and Process Assurance, PWC "**Risk Assessment and IT**".
8. Security Risk Management **Case Study: AT&T, Global Communication Leader Deploys Vulnerability Management Solution That Scales to Size**, July 2004, CRA Reports
9. http://www.qualys.com
10. http://www.Security-Assessment.com