Microsoft Patch Management:
A Comparison of St. Louis Companies

May 21, 2004

Brian Middendorf
Sarah Middendorf

Appendices:

Raw Data: http://mis.umsl.edu/bov/BOV04-1app.pdf
Presentation Slides: http://mis.umsl.edu/bov/BOV04-1app2.pdf

Table of Contents

Objective and Scope

The objective and scope of this white paper is to document and analyze methodologies and best practices in patch management for Microsoft systems, focusing on security patch management.

Executive Summary

This white paper will first provide background information on Microsoft patch management and list the St. Louis IT professionals who were interviewed for this paper. The security leadership within the organization is then discussed to identify how these companies prioritize the issue of security. The paper presents data on the size and proportion of patch management teams within the organizations. Patch management practices such as notification of new releases, determination of severity, testing, deployment schedules, and deployment methods are compared. Patch management challenges relating to people, processes, and technology are also discussed. The paper also discusses practices in areas of change control processes, incident response plans, quarantine technology, management of remote access users, and risk assessment. Finally, the conclusion will provide some observations of best practices and opportunities for improvement.

Patch Management - Background

Patch Management is one of the most critical and complex Windows security-related issues in today's business environment. Effective patch management has become an essential task for the network administrator of every corporation. Why do corporations need to worry about patching? According to International Network Services, software companies are frequently reporting defects in their software. These defects allow unauthorized users to access systems that are running the software. Once the software vendor announces the defect, hackers begin attempting to break into the systems; therefore, the software vendor is in a race against the hackers to create a patch to protect the software before the hacker can hack in (22).

Patching "consists of scanning machines on the network for missing patches and deploying these patches as soon as they are available (21)." Failure to deploy patches in an expedient and timely manner can make the network even more vulnerable, because once the vulnerability has been publicized; there is the increased risk that it will be exploited by hackers and virus writers (21).

IT professionals face enormous security challenges with more devices and mobile users accessing corporate networks than ever before. The Microsoft Patch Management white paper provides some statistics about remote users and internet devices: "According to industry analysts at Forrester Research (Forrester Research, 2003) there will be 35 million remote users by 2005 and 14 billion devices on the Internet by 2010."

CSI/FBI Computer Crime and Security Survey

The Computer Security Institute and the FBI conducted a Computer Crime and Security Survey in the spring of 2002. "Ninety percent of the CSI/FBI survey's respondents detected computer security breaches in 2002. Of these security breaches, 95 percent occurred because of poor system configuration. About 85 percent of the surveys participants detected viruses even though most had deployed firewalls (98 percent) and anti-virus technology (99 percent)." The attacks included "theft of proprietary information, financial fraud, worms, viruses, and net abuse by employees (23)."

What is most interesting is the fact that many of these security invasions could have been prevented. "According to CERT Coordination center, "most intrusions result from exploitation of known vulnerabilities, configuration errors, or virus attacks where counter measures were available, including most major Internet worm/virus alerts (23)."

According to Robert Lemos, "A recent trend in the computer security world is the recognition that vulnerabilities in common technologies can have widespread effects (26)." After the federal government, Microsoft is the second largest target for these threats (20).

Microsoft Trustworthy Computing Initiative

In January of 2002, Bill Gates introduced the Microsoft Trustworthy Computing Initiative as a long-term company strategy that focuses on four key areas: security, privacy, reliability, and business integrity (22). This security effort is striving to do the following:

- "Improve and simplify the patching experience to help customers keep all of their systems protected and up to date.
- Provide security guidance to help its customers deploy and operate Microsoft products as securely as possible.
- Innovate on safety technologies that will make Windows-based computers more resilient to attack, even when patches are not installed.
- Improve the quality of Microsoft software through the Trustworthy Computing Development Process, to reduce vulnerabilities before the software ships (23)."

Recently, Microsoft has rated more patches as "critical" because of the current security environment. In early 2003, Microsoft introduced the "important" category to the existing list of categories: critical, moderate, and low categories. The important category helped in reflecting the level of deployment urgency that should be used for some patches. The critical label is now used "only for vulnerabilities that could be exploited by allowing malicious Internet worms to spread without user action (25)."

Microsoft continues to rely heavily on customer feedback to improve the Patch management process. In particular, it created the Patch Management Taskforce in 2002 as an ongoing customer feedback process that ensures the constant refining of the software update and security patch management process. This Patch Management

Taskforce gathers feedback from all sizes of corporations around the world. From this feedback, the Taskforce focuses on these four key areas:

- "Provide clear and timely communication and guidance
- Provide consistency in standards and behavior
- Provide high quality patches reducing recalls, patch sizes, and system reboots
- Provide consolidated and cost conscious tools (23)."

Overview of IT Professionals and Companies Interviewed

Company	IT Professional	Title
Anheuser-Busch	Mark Hickey	Senior MIS Team Leader, Packaging Division
A.G. Edwards	Chris McCloud	Information Systems Analyst
Accenture	Mike E. VanVooren	Senior Manager
	Ian Russell	Security Lead for Internal Helpdesk
Boeing	Kyle Hatcher	SMS Site Manager
DMI (Supplies Network)	Mark Daugherty	Director of Information Services
EDS	Ken Rolland	Infrastructure Analyst
Edward Jones	Tim Spakowski	Head of Security Assurance Team
	Hugh Spaulding	Head of Security Infrastructure Team
MasterCard	Lowell Mattox	Vice President Global Internal Technology
	Paul Moran	Director of Software Engineering
The May Company	Sue Mitchell	Director of Software Application Development
	Gene Hall	Director of St. Louis Operations
Metro Bi-State Development Agency	Debbie Erickson	Vice President and Chief Information Officer
Microsoft	Austin Wilson	Director of Security
	Will McKnight	Group Manager for MS IT
Monsanto	Mark Williams	Manager of Systems Engineering Services
Nestle Purina	Christopher Vaughn	Manager, Information Assurance
SBC	Steve Farmer	Lead Database Administrator

Security Leadership within the Organization

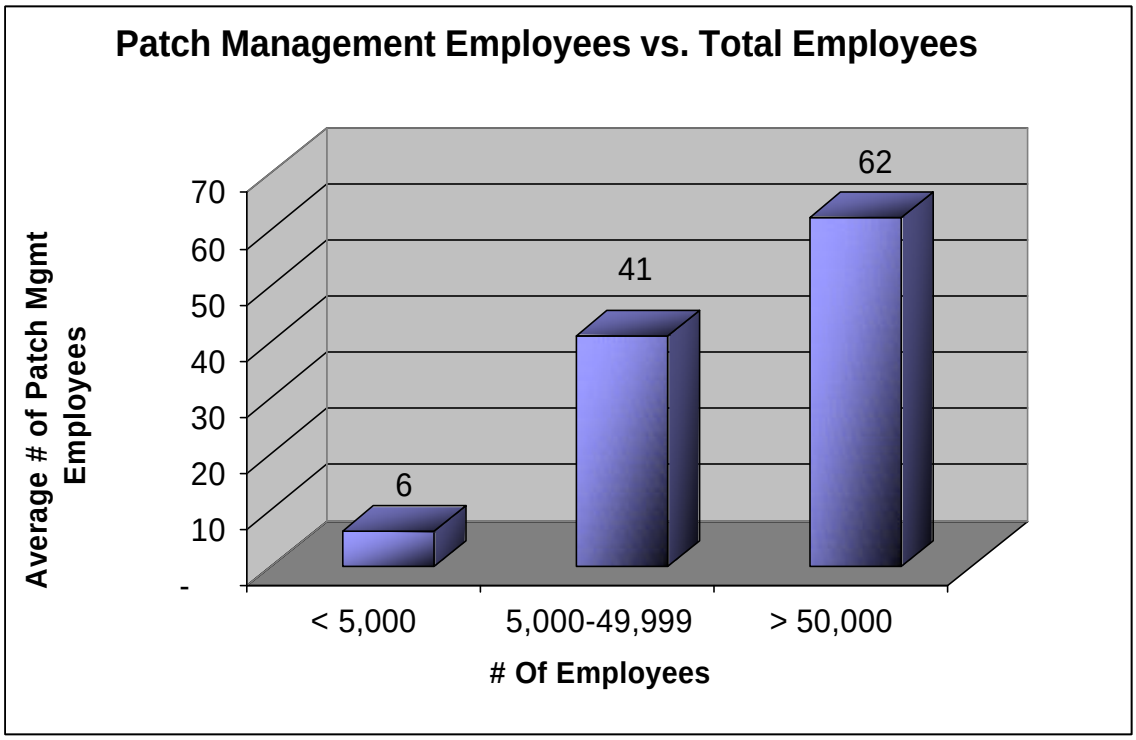
One important indicator of the importance that a company places on security is the relative rank of the person in charge of security within their organization. It is becoming more common to have a Chief Security Officer who is highly ranked within the organization. Only three companies that were interviewed report having someone with the title of Chief Security Officer. Other titles for individuals responsible for security include Chief Information Officer; Director of Security, Security Administration Group; Director of IS Security; and Director of Information Security Office.

May of the IT professionals commented that IT security is moving higher on the priority list of senior management. Especially because of recent security threats, senior management buy-in to the importance of IT security is no longer a problem.

Size of Patch Management Team

The companies that were interviewed have a broad range of infrastructure within the IT department. The number of employees with patch management responsibilities depends on the type of company and the security risks that are present. Each company assigns patch management responsibilities, including identifying, testing and deployment, in a different way.

Companies with less than 5000 employees have an average number of 6 employees who worked on Microsoft patch deployment. For companies with 5000 to 49,999 employees, the average is 41 employees. And for companies with 50,000 and more employees, the average number of employees involved with patch deployment is 62.



Reporting and Inventory Methods

The ability to produce an immediate report of an organization's current inventory of software and hardware is an important step towards maintaining a secure organization. Companies that have an organized method of identifying what kind of software and hardware they have in their organization will be better equipped to make knowledgeable decisions about what type of patching they need to perform and to how many users.

All of the companies interviewed have some ability to determine what kind of software and hardware they have in their environment. A few companies are still relying on hard copies of inventory records to keep track of their current inventory levels. However,

most companies have an electronic method of pulling together an inventory report. A few companies have developed internal auditing software that keeps track of the inventory of their computers and software. Most companies use Microsoft Systems Management Services (SMS) software for reporting.

Notification of Newly-Released Patches

Microsoft received a great deal of customer feedback on their Security Bulletin Notification Service. As a result, in the past year, they made many improvements to the service, including sending it once a month (or immediately when a known exploit exists). Microsoft also responded to customers' needs by making more general and less technical Consumer Bulletins (the original is still available). In the past, customers had to search four different Web sites to locate security updates and patches. With the new Security Bulletin Web search tool, customers can only need to view one site the get the information they need (23).

The Microsoft Security Response Center sends a monthly bulletin on the second Tuesday of each month (23). Most of the surveyed companies subscribe to this service and receive the bulletin in an email. In addition, some subscribers are set up to receive a page from Microsoft for unscheduled emergency notifications. One IT professional in St. Louis mentioned the frequency of these emergency pages on several Sundays this Spring 2004 because of the increased number of exploited code.

Many companies reported that they still perform a good amount of research on the patch and security threat beyond what is initially sent to them from Microsoft. Some companies prefer to have this notification service outsourced to another IT vendor, which will analyze the patch for them. One company uses an outside vendor, NCR, which identifies their internal patch rating and the location from which to receive the patch. News groups such as Bugtraq are becoming more popular as IT professionals seek to widen their radar screens to be aware of as much as they can.

Determination of Patch Severity Rating

Recently, many Microsoft customers complained that Microsoft's security level ratings were unclear and inconsistent. As a result, Microsoft revised the definitions for security ratings to make it easier for IT departments to determine the vulnerability levels. See the ratings at the left (27) and the Severity Rating Definitions Table from the Microsoft Patch Management white paper.

Severity Rating Definitions

Rating	Definition
Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm/virus without user action.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

Almost all companies create their own internal patch rating system based upon their IT infrastructure and business-critical needs. Only three companies reported that they automatically accept Microsoft's rating and do not perform much additional analysis to confirm the rating level. The first step in determining a patch's severity involves analyzing the company's inventory of software and hardware. As stated above, most companies rely on SMS for this inventory function. Obviously, if the critical patch is for a piece of software that a company does not use, such as Outlook, or a different version than they currently have, then they will not deploy the patch.

Most companies then analyze what the patch has been released for and then determine where that software vulnerability fits in with their security priorities. For instance, financial firms have different sets of security priorities than retail and distribution firms. IT departments also analyze the number of applications the patch will affect and the number of workstations that will need to be patched.

One company divides critical patches into two categories. Critical patches are labeled "immediate" when active code exists or exploits are already present. Patches are internally labeled "critical" when Microsoft has deemed them critical but there are no known exploits. Companies also examine their firewall to determine if it provides sufficient protection.

Many larger companies also have Microsoft representatives that work with their IT departments directly. The Microsoft representatives help the company determine their rating. It is interesting to note that many of the IT professionals interviewed stated that rarely are the patches that Microsoft deems critical actually determined to be critical to that company by their Microsoft representatives.

In the same way, some companies work with their IT vendor company (Microsoft partner) to determine their patch rating. One company also looks at the Homeland Security Office's recommendations for their industry as they review patches.

Patch Testing Prior to Deployment

The amount of time spent testing patches prior to deployment varies according to a company's internal patch severity rating. As previously discussed, the internal rating takes into account the company's industry, business-critical needs, and IT infrastructure. According to Hewitt P. Wright of Microsoft, the industries that will increasingly be targeted by security threats are the financial industry, energy industry, and public utilities (6). These companies will most likely focus on more sufficient patch deployment.

Most companies go through a testing procedure that involves testing their essential software programs. When testing critical patches, few companies interviewed test software beyond the more common and essential programs for the sake of time. Some companies strive to test as many applications as possible within the allotted time before they must deploy. Also, many companies are making testing simpler by moving towards more uniform software configurations.

Testing is important because a patch can cause problems with the current software that is running. For example, the patch to protect against the recent Sasser virus originally had a problem with Windows 2000. Some companies ran into problems when testing this patch, and Microsoft had to create a fix for it.

In the case of an emergency, some companies will abandon their scheduled patch testing times and will send the patch out immediately. One company said that they would put a patch into production immediately as long as back-out plans are in place, in case there was a problem. Another company said that they would deploy within thirty minutes if necessary. Most of the other companies would rarely consider deploying a patch this quickly.

One international company has 24 test machines across different regions. It will test the patches on these different machines before allowing deployment. One of the reasons that certain companies had longer testing times is because they have a larger number of software configurations at employee workstations. Companies that have less variation in configurations can effectively test in a shorter amount of time.

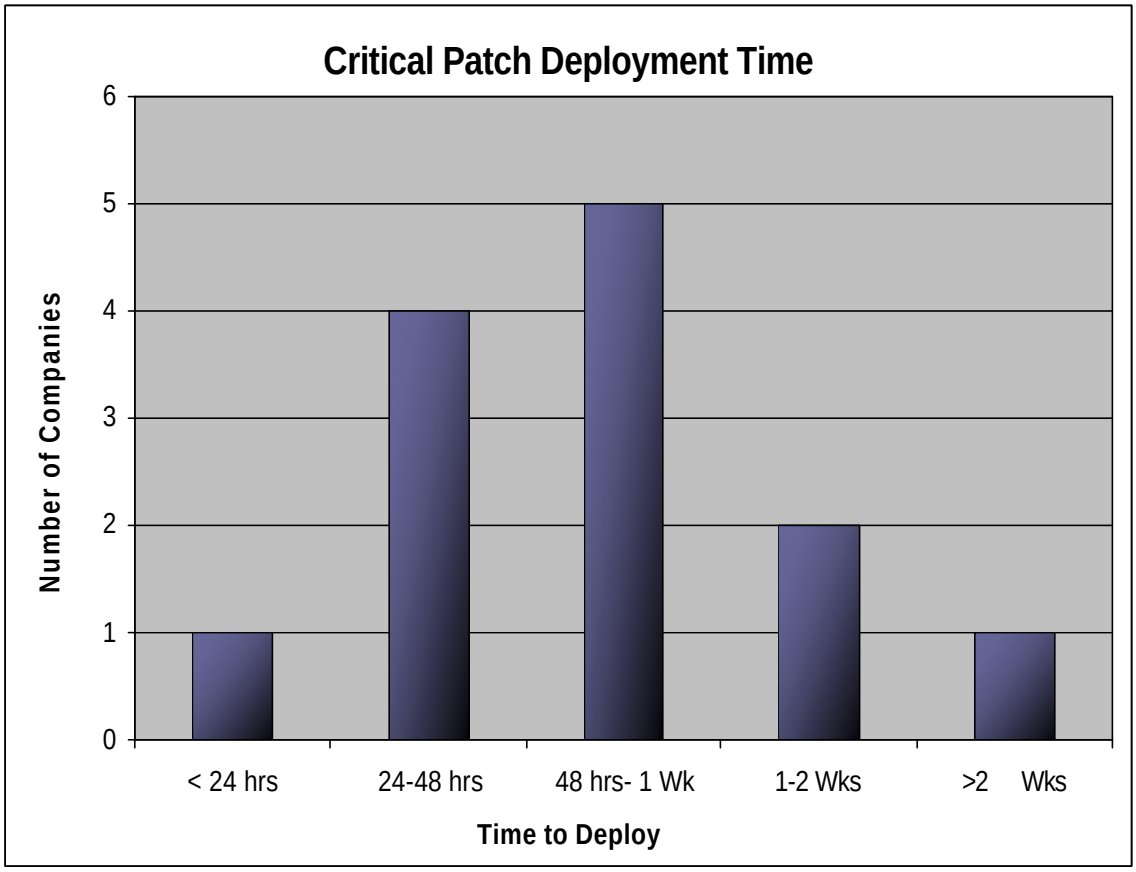
Patch Deployment Schedules

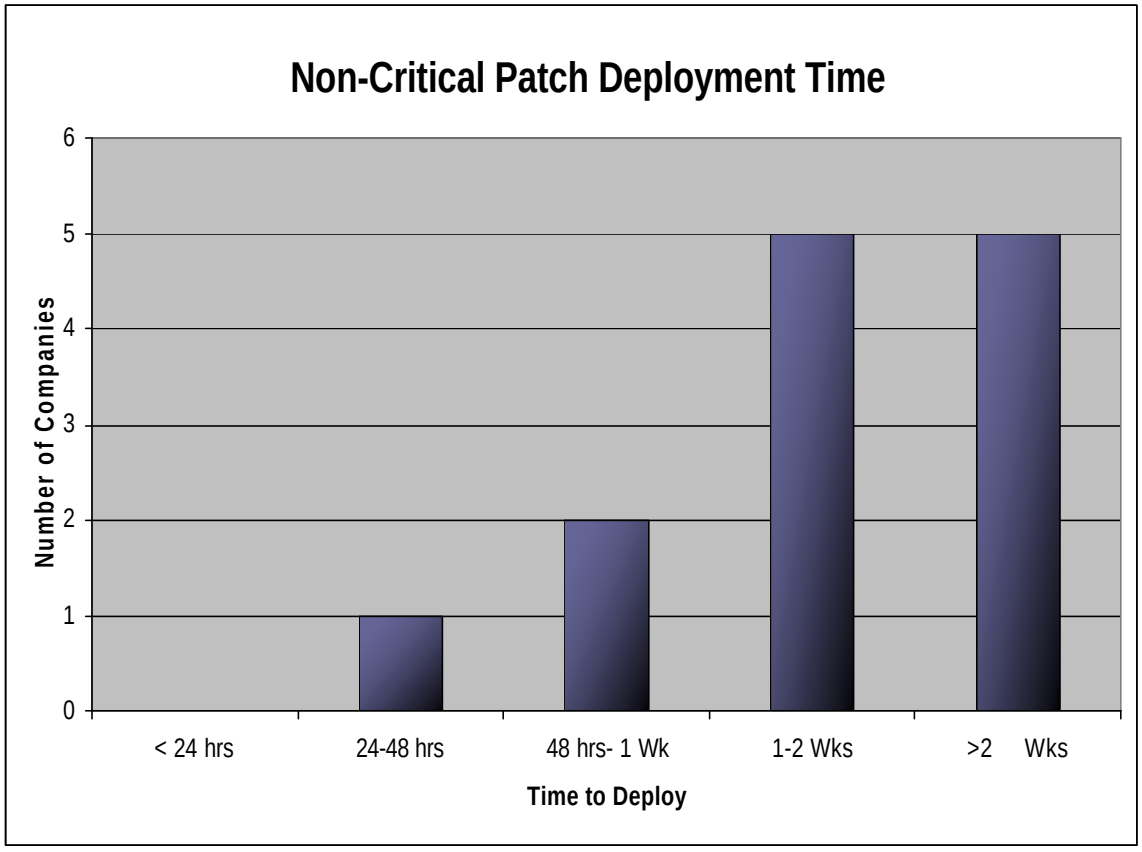
A company typically deploys a patch immediately after testing is complete. Some companies that were interviewed followed strict deployment schedules. Other companies have a less-structured schedule that they followed. There were not clear patterns of time to deployment within certain industries, such as IT or financial companies maintaining a faster time to deployment than retail, manufacturing, and distribution companies. This is probably attributed to the fact that companies are still fine-tuning their processes. It can

be concluded that a company's policy on length of time to deployment is attributed to how a company weighs the risks of patching or not patching. This will be discussed further later in this paper.

From the results of this survey, the shortest time to deploy a critical patch is within 24 hours, and the longest is two weeks. The company that allows two weeks for deployment has a change management process that requires a board approval for the patch deployment. The patch cannot be deployed until the board has given their signatures. Another company's policy on critical patch deployment states that 80% of the machines must receive the patch within two to three days. About 95% of the machines will receive the patch within one week.

The following charts show the distribution of deployment times for the companies interviewed for critical and non-critical patches.



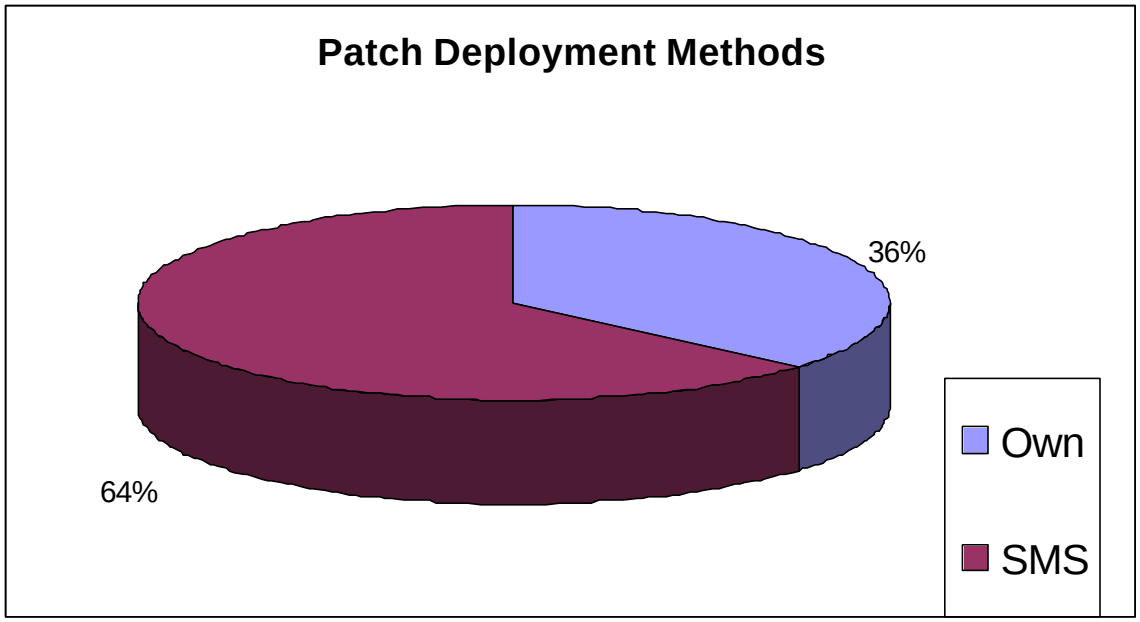


Patch Deployment Methods

One of the goals of IT department is to automate processes that can be automated to save time and money. Most of the companies interviewed have some part of their patch deployment process automated, but to many different degrees.

One company reported that they manually apply patches to servers, but they have developed software to automatically deploy the patches to the workstations overnight. Another company said that they have the ability to automatically deploy smaller patches. But for larger patches, they use a logon script for desktop users or send out a CD to remote users.

Most companies use SMS to automate patch deployment. A few companies have developed internal software programs for patch deployment. Here is a graph that shows the percentage of companies using SMS versus their own software.



Patch Management Challenges within the Organization

People

"Managing people" was the most common response when asked what the main challenge is within patch management. The number of remote access users is increasing, and this presents the challenge of having users that are not protected by the company's firewall.

At the same time, managing the people in an organization has become less challenging and necessary as more IT functions have become automated. However, even when a system is patched, there is always a security risk when users have access to email. To minimize this risk, many companies are focusing on educating their employees about security risks. From including security in the employee orientation to keeping employees informed via mass email when there is a security threat, IT departments are ensuring that employees are informed and well-trained.

A few companies mentioned the demanding schedules of overworked IT staff as the main people challenge. The IT department has high standards to serve their company, and it puts a strain on the quality of life of their staff. They need more staff but cannot afford to hire at this time. Another company explained the emphasis on asset utilization that is increasingly common in Fortune 500 companies today. A few years ago, the goal was to increase revenue by growth and hiring. Today, increased revenue must be accomplished by increasing the efficiency of the current employees, or utilizing their assets.

Process

Process challenges were mentioned less often than people and technology challenges, but there are still many process issues that need to be improved. Process challenges include

finding the best time to deploy a patch to minimize business disturbances but to not risk security. It was mentioned that processes put a strain on resources. How to best allocate resources is a constant learning process.

Microsoft began using the term "dogfood" for the practice of testing their own software in their own production environment before sending it out to their clients. This has enabled them to catch errors before their clients could. This demonstrates the increased care that companies are taking with patch testing before deploying.

One company mentioned that their decision-making processes were not as rigorous as they needed to be. For companies that are international, their IT security process is one of the later processes to be standardized company-wide. Often, different parts of the world are using different software to manage and install patches.

Technology

Technology challenges are decreasing as processes are improving and becoming more automated. Companies that have more manual patch deployment processes ranked technology challenges higher than other challenges. Most of these companies are in the process of updating their systems and have plans to start using SMS or another software program to have an automated process for patch deployment.

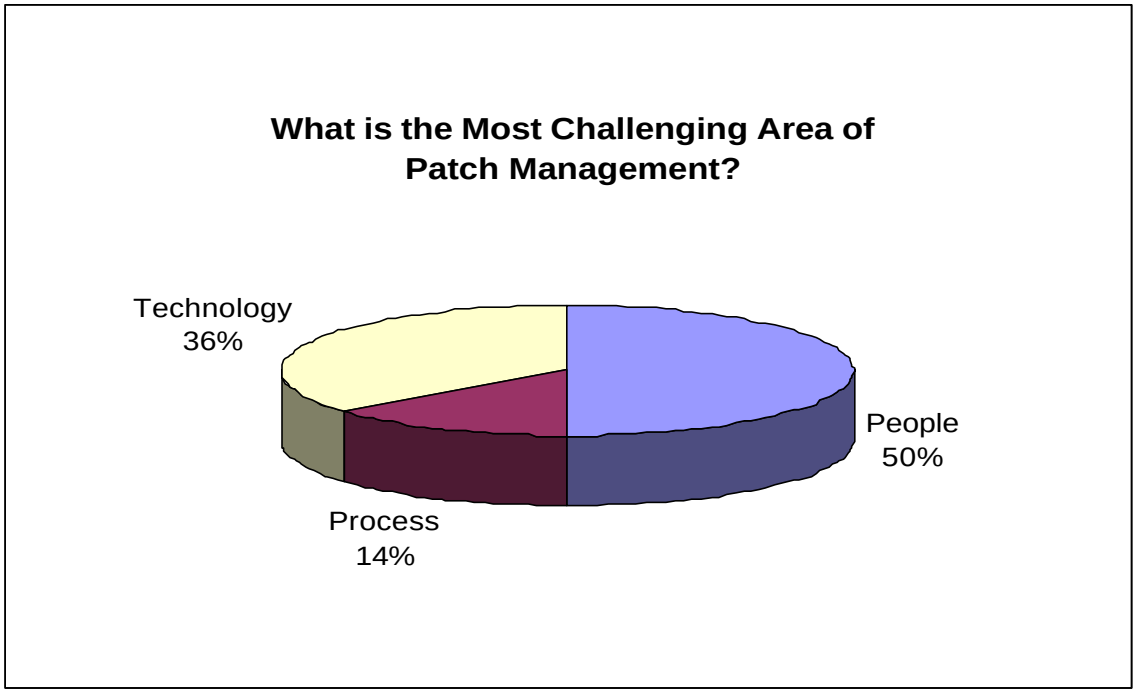
One technology challenge mentioned is the difficulty of testing patches in a realistic set-up and environment. Also, most companies do not have time to test the patches for all of the software that they use. Most test only the most common or necessary software. Determining what software to test is a learning process.

Even though most of the companies interviewed are satisfied with SMS, there are some limitations to SMS that Microsoft is aware of and needs to improve. For example, one company mentioned that most of their infections occur when an outside vendor comes to visit their office and connects to the network. Because SMS only reports on its clients, it does not prevent the unpatched vendor from connecting to the network and introducing an infection. The Active Directory and SMS do not match up, and Microsoft admits this is something that needs to be worked on.

A new technology has been recently introduced that could amend this situation. Network Authentication and Discovery will identify authorized users so that unauthorized users can not connect to a company's network when they are on site.

Financially, the short shelf life of software can be difficult when budgeting and allocating resources. One company has a more conservative approach to purchasing software updates. However, they have had instances when they had to purchase a new version of software to complete a patch because a patch did not exist for their current version.

Most of the companies interviewed discussed challenges in all three of the above areas. However, when asked which area presented the most challenges, each company mentioned one category that has been more challenging.



Change Control Process and Incident Response Plan

According to the Microsoft Patch Management white paper, effective change control processes are an important part of managing security risks. "Increasingly, improving security means improving systems management. Consistent, repeatable processes, reliable auditing and reporting against policy, and effective change control can drastically reduce the level of uncertainty and risk throughout the IT infrastructure (23)."

About 78% of the companies interviewed have the same change control processes for all of the different platforms within their organization. One company stated that it is an important part of their culture to maintain the same processes. For the companies that do not have the same change control processes, the reasons varied but included geographical challenges, software differences, and age of the equipment.

Almost all companies have an official incident response plan. One company has a Security Incident Response Team called SIRT that has its own governance and is called into action when they are under attack. SIRT was called into action three times in the last eighteen months. Most of the incident response plans depend on the scope or type of problem, such as a worm. Because of recent worm threats, many of the incident response plans are recently created or revised.

Managing Remote Access Users

Many companies view remote access users as their greatest risk in security patch management. It is becoming increasingly difficult to manage remote users as more business professionals work with laptops and dial-in to non-secure networks. Most companies have developed or are in the process of developing a solid system for managing patches that adequately balance their business and security needs. However, most companies are not confident in their current procedures for patching their remote users.

Managing security patches for remote users presents challenges because the remote users are not connected to the company network all the time like desktop users are, so they might not receive all the patches that are sent out. And when remote users do connect to the network, it is often by dial-up, which makes it difficult for them to download large patches. Remote users are also more of a security problem because they might connect to the Internet without the protection of the company firewall.

Remote access users tend to be employees that are generally highly ranked in the company, such as managers and officers. IT staff have a more difficult time setting standards that these remote users most follow. When these remote access users want access to their networks, they can demand it and override the standard screening process.

One company is working towards converting more remote users to VPN (virtual private network). This would allow them to use SMS to patch the remote users. For their remote users that are not on the VPN, their dial-up service is manually shut down, the user is mailed a CD containing the patch, and the dial-up service is turned on only after they have reported that they have patched their computer.

Most of the companies that felt somewhat confident in how they were managing these users were using SMS, which has support for remote access clients. When a mobile client attempts to logon to the network, SMS determines what upgrades or patches they need and then advertises to them.

One company allows only a very small amount of laptop users (about 5%) to dial-up to a network besides their own.

Risk Assessment

One of the IT department's most important tasks in today's business environment is weighing the risks of patching versus not patching. Each company must analyze whether or not their actions are in line with their priorities to effectively carry out the mission of the company. The risk assessment of patch management is a key part of this analysis. Even within the IT department of an organization, different IT professionals have their own sets of priorities, such as maintaining the fastest online service to their customers or ensuring that no vulnerabilities are exposed.

The IT professionals mentioned risk assessment throughout the interviews before the question of risk assessment was mentioned. This is an underlying element to every decision made in the IT departments concerning patching, from the amount of software tested, as earlier discussed, to the regulations for remote access users.

Some companies are being proactive in finding out whether or not they are being attacked specifically. Services such as Intrusion Detection Services, or IDS, will show what the risk of attack is.

Many of the companies have different functional departments within the IT department that serve as checks and balances for risk assessment purposes. However, for critical processes, there is typically not any type of risk analysis performed. The risk analysis has essentially already been performed when the patch is rated.

According to the companies that were interviewed, the task of analyzing the risk of patching is performed solely in the IT departments. The other segments of the organizations seem to assume that the IT department is basing their decisions on the best interests of the organizations as a whole. As in any business decision, the choice of whether to patch or not comes down to a financial decision. The IT department knows the priority of the business is to be profitable. Therefore, the IT department must manage patching within their budget.

Quarantine Technology

Windows Server 2003 has a new feature, Network Access Quarantine Control, which "delays normal remote access to a private network until the configuration of the remote access computer has been examined and validated by an administrator-provided script." It is important to note that Microsoft states that this tool is not a security solution. It is not intended to be a private network's protection against malicious users who falsely appear to have a valid set of credentials. Its purpose is to prevent a remote user from connecting to a private network without having updated configurations (24).

One company mentioned a limitation of Microsoft's Network Access Quarantine Control that prevents them from being able to use it. The software is proprietary; therefore, if a company's IT infrastructure is not solely Microsoft then they can not use it. This company uses Nortel for their VPN. The VPN is relatively new, so they are not anxious to replace it soon. Microsoft does have some native quarantine technologies within the firewall that this company can use.

Most of the companies that were interviewed are only using a simple type of quarantine process for questionable emails. Many companies use an Anti-Virus software that strips any suspicious email attachments so they can further review the attachments or dispose of them. One company does not have any quarantine software, but they have manually isolated regions from the network because of security concerns. Of course, if a machine is infected, it will be manually disconnected from the network.

According to one IT professional, quarantine technology is not on their "radar screen yet." Also, a few IT professionals that were interviewed had not yet heard of quarantine technology.

Conclusion

During the research process of this paper, it became evident that many companies were managing certain aspects of patching consistently well. There were also several areas of patch management that were inconsistent and needed improvement to adequately protect the organization against security threats. This conclusion will outline some of the best practices that were observed by many of the companies interviewed. It will also give some suggestions for improvement.

Best Practices of Companies Interviewed

Most of the companies interviewed are well-informed about new security threats against Microsoft software and when new patches are released from Microsoft to protect against these threats. This shows that most St. Louis-area companies have a reliable means of communicating with Microsoft and are aware that they need to have a good system of patch management in place.

Many companies have a system in place for automated patch deployment. SMS is currently being used by most of the companies. Some companies have developed their own software for patch deployment, or they are using a combination of SMS and their own software. Of the companies that are not yet using SMS or comparable software, most have a twelve-month plan to start using SMS or another software that would automate the patch deployment.

Most of the companies have a formal process in place to address security threats and vulnerabilities. Even though there is a wide range of testing and deployment schedules, most companies maintain a reasonable schedule for their industry and are currently comfortable with the schedule that they maintain.

Most of the companies appear to have a healthy risk assessment process in place. Most of the IT professionals have a clear sense of the mission of their organization, and they are executing IT practices that are in line with their mission. IT departments are trusted by their organizations to make critical decisions about patch management that can drastically affect the profitability of the entire organization. Most of the IT professionals understand this responsibility and take it seriously.

Opportunities for Improvement

This paper will only provide general suggestions for improvement because each company is unique and has its own set of priorities.

Most of the organizations that were interviewed are international organizations. For most international organizations, it is difficult to maintain consistency in patch management processes across all geographical segments of the organization. For example, if the St. Louis office is regularly applying security patches to keep their software updated and protected, but another location of the organization is not, then the St. Louis office could be in danger because another employee has allowed a possible security threat onto the company network. Many companies do not yet have a global process in place for patch management, but uniform processes are needed.

Most companies could benefit from having a tighter control of their inventory of software and hardware. While most companies have some sort of reporting capabilities, sometimes this reporting is limited to known computers. Some employees have more than one desktop or laptop computer, and the IT department has not kept track of this. It does not help the organization to get the recognized computer patched when there is a chance that an employee could log onto the network with an unknown, and possibly infected, computer. Companies need to have better inventory systems in place to protect against a possible infection.

Managing remote access users is a growing issue for most of the companies interviewed. Some of the companies have strict policies for remote users, such as restricting dial-up access to their secured network. This is a good idea if it makes sense in the business context and allows the company to run as it should to be profitable. Many laptop users act as if their laptops are for their personal use when they are out of the office. Maintaining stricter policies would add another level of protection to these companies.

As companies evolve their infrastructure and leadership in the future, IT security will get more attention. Some companies have recently added the position of Chief Security Officer. This demonstrates that security is a main priority for these companies. More companies should analyze whether or not their organization could benefit from a Chief Security Officer.

In the next year, many companies will look into Microsoft's Network Access Quarantine Control technology. More people are doing business outside of the home offices and laptop use is increasing. Quarantine technology brings a solution to many of the problems that companies are experiencing with unpatched clients.

Bibliography

1. Austin Wilson, Director of Security, Central Region for Microsoft, interviewed by telephone by Brian Middendorf and Sarah Middendorf, March 12, 2004.

2. Chris McCloud, Security Manager for A.G. Edwards, interviewed in person by Brian Middendorf, April 22, 2004.

3. Christopher Vaughn, Manager, Information Assurance for Nestle Purina North America, completed survey by email, May 17, 2004.

4. Debbie Erickson, Vice President and Chief Information Officer of Bi-State Development Agency, interviewed by telephone by Sarah Middendorf, April 26, 2004.

5. Gene Hall, Director of St. Louis Operations for the May Company, interviewed by telephone by Sarah Middendorf, May 20, 2004.

6. Hewitt P. Wright, Management Technology Specialist for Microsoft, presentation at Microsoft/Oakwood Systems seminar, March 12, 2004.

7. Hugh Spalding, Head of Security Infrastructure Team for Edward Jones, interviewed in person by Sarah Middendorf, April 26, 2004.

8. Ian Russell, Security Lead for Internal Helpdesk of Accenture, interviewed by telephone by Sarah Middendorf, March 25, 2004.

9. Ken Rolland, Infrastructure Analyst for EDS, completed survey by email, March 30, 2004.

10. Kyle Hatcher, SMS Site Manager for Boeing, interviewed by telephone by Sarah Middendorf, April 23, 2004.

11. Lowell Mattox, VP Global Internal Technology of MasterCard International, interviewed in person by Brian Middendorf and Sarah Middendorf, April 12, 2004.

12. Mark Dougherty, Director of Information Services for DMI (Supplies Network), interviewed in person by Sarah Middendorf, March 12, 2004.

13. Mark Hickey, Senior MIS Team Leader for Anheuser Busch Packaging Division, interviewed by telephone by Sarah Middendorf, May 18, 2004.

14. Mark Williams, Manager of Systems Engineering Services for Monsanto, interviewed in person by Sarah Middendorf, April 26, 2004.

15. Mike E. VanVooren, Senior Manager for Accenture, interviewed on the telephone by Sarah Middendorf, March 25, 2004.

16. Paul Moran, Director of Software Engineering for MasterCard International, interviewed in person by Brian Middendorf and Sarah Middendorf, April 12, 2004.

17. Sue Mitchell, Director of Software Application Development for The May Company, interviewed in person by Sarah Middendorf, March 25, 2004.

18. Steve Farmer, Lead Database Administrator of SBC, completed survey by email, April 7, 2004.

19. Tim Spakowski, Head of Security Assurance Team for Edward Jones, interviewed in person by Sarah Middendorf, April 26, 2004.

20. Will McKnight, Group Manager for MS IT for Microsoft, interviewed by telephone by Sarah Middendorf, May 19, 2004.

21. http://www.gfi.com/whitepapers/patch-management.com, viewed May 1, 2004.

22.http://www.ins.com/downloads/whitepapers/ins_white_paper_security_patch_mgmt_0303.pdf, viewed April 30, 2004.

23. http://www.microsoft.com/security/whitepapers/patch_management.asp, viewed May 2, 2004.

24. http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspx, viewed May 1, 2004.

25. http://www.serverwatch.com/tutorials/article.php/3299831, viewed May 1, 2004.

26. http://www.zdnet.co.uk, viewed February 11, 2004.

27. http://www.microsoft.com/security/security_bulletins/200405_windows.asp, viewed May 7, 2004.