Latest News and Developments in Vulnerability Management

Min Soo Choi
University of Illinois Urbana Champaign
BADM 559
Professor Shaw
May 1, 2008

Table of Contents

Page

What is Vulnerability Management? *3*

Vulnerability Assessment *4*

Ethical Hacking *7*

Patch Management *10*

Vulnerabilities on the Rise *12*

A Solution *14*

Executive Summary *15*

Bibliography *16*

What is Vulnerability Management?

Vulnerability management is the overall responsibility of managing risks that are associated with the vulnerabilities of an organization. It involves identifying possible threats and making decisions based upon the costs of each threat. When companies uncover these threats, they attempt to eliminate, mitigate, or tolerate each problem depending on the risks and costs of implementing a solution.

There are three primary ways in assessing vulnerability management, which are vulnerability assessment, patch management, and ethical hacking. Out of these three methods, companies use vulnerability assessment the most to handle their IT securities. Nonetheless, the two remaining approaches are important sectors to vulnerability management and should not be neglected. Ignoring these two areas can compromise an organization's security.

Vulnerability Assessment

Vulnerability assessment acts as a discovery function under vulnerability management. It searches for security holes in a computer, network, or communications infrastructure by using scanning programs that inspect for already known vulnerabilities. Scanning programs also have the capacity to check for open ports, and running programs within protocols, applications, and operating systems. Figure 4.9 and 4.10 from Network Security: A Practical Approach provides an example of a vulnerability assessment at work. The two figures, created from a port scanning program, show which ports are open and vulnerable. Users can use this tool to check if any of their ports are open and vulnerable to any attacks.

```
Port Scanning host: 192.168.1.100

      open Port:                  21          ftp
      open Port:                  22          ssh
      open Port:                  80          http
      open Port:                  139         netbis-ssn
      open Port:                  427         svrlc
      open Port:                  515         printer
      open Port:                  548         afpvertcp
      open Port:                  631         ipp
      open Port:                  3031        eppc
Port Scan has cmpleted ...
```

Figure 4.9 A port scan of a wide open host

```
Port Scanning host: 192.168.1.1

      open Port:                  80          http
      open Port:                  2468        qip-msgd
      open Port:                  5678        rrac
      open Port:                  6688
Port Scan has cmpleted ...
```

Figure 4.10 The result of a port scan on an edge router

An ideal vulnerability scanner maintains the latest database of known vulnerabilities, detect genuine vulnerabilities with a low percentage of false positives, conduct multiple scans simultaneously, provide clear reports, and recommend solutions in eliminating the discovered vulnerabilities. In order to achieve these goals, it takes these steps:

- Classify network or system resources
- Categorize the degree of importance to the resources
- Search for potential threats within each resource
- Recommend solutions to problems that are considered to be the most dangerous
- Strategize ways to prevent another attack

With the importance of IT security on the rise, vulnerability assessment applications are a growing market. International Data Corporation (IDC), a global provider of market intelligence on the latest information technology, expects the application vulnerability market to increase by $287 million in the year 2010, doubling 2006 year's projection of $143 million. Their predictions are supported from the fact that at the end of 2005, vulnerability application companies such as Watchfire and SPI Dynamics, held 50% market share, which estimated up to $35 million. Watchfire's and SPI Dynamic's growth in the market made these companies popular acquisition targets. In June IBM aimed to acquire Watchfire and implement its technology into IBM's Rational development platform. Hewlett-Packckard Co. followed the same tactics and aimed to acquire SPI Dynamics to use the vendor's software under HP's Technology Solutions Group.

Vulnerability Assessment is an important process because it allows security groups to make preparations for the problem. The management team can then look over these preparations and makes decisions based on the risks and costs in fixing the problem. As much as they want to eliminate the root cause of the majority of exploits, reduce any other possible attacks and keep security incidents to a minimum, they still have to weigh the costs and risks. Some of the solutions may not be plausible, unless they factor in the budgetary constraints and financial risks.

Ethical Hacking

Ethical hacking, also know as penetration testing, intrusion testing, or red teaming, is the process of purposely breaking into a security system for the sake of testing vulnerabilities within the security system. Ethical hackers are computer and network experts, who attempt to breach a security system with the consent of the owners. However, instead of taking advantages of the security weaknesses, they report the vulnerabilities so that the companies can fix the problems.

The origin of ethical hackers can be traced back from the 1970's, when the United States government implemented a team of experts called red teams to breach into its computer systems. Since then, ethical hacking has evolved, becoming a common use within technology and government sectors. Large companies such as IBM hold a team of ethical hackers to continually test current and newly developed systems.

Besides working for large corporations, hackers compete against one another by using their skills through public held contests. Companies, who hold these events, look, not only for flaws within their systems, but for potential employees. During last year's CanSecWest conference, Dino Dai Zovi, a New York-based security researcher, hacked into Mac's operating system, which was once thought to be impenetrable. He discovered flaws within Apple's Safari and Quick Time applications and used these vulnerabilities to break into the system configurations. In an interview with Macworld magazine, he describes his experience in breaking the code.

> " I had found other vulnerabilities in Mac OS X and even QuickTime in the past, so I had some familiarity with the code, but I only discovered this vulnerability that night. There were reports of other vulnerabilities in QuickTime, and even

> Java-related vulnerabilities in QuickTime over the last few years. In my experience, if a certain software package has had vulnerabilities in the past, it is more likely to contain other undiscovered vulnerabilities.

Although the CanSecWest conference aimed for the Mac OS, it raised threat awareness for all types of operating systems. This contest warned Apple users about the security vulnerabilities within the Mac system and proved that Apple's operating system is not a secure alternative to Microsoft Windows. Since the contests, software analysts concluded that the exploited vulnerabilities within Quick Time threaten both Mac and Windows operating systems. Any Java-enabled browsers, such as Safari, Mozilla Firefox, or Internet Explorer under these systems are susceptible to the same type of attacks.

However, although ethical hacking provides a variety of benefits, it can be a dangerous practice that poses many risks. In the case with the CanSecWest conference, Apple is at a high risk for a potential breach, since the contest released the exploit details into the public. Analysts Rich Mogull and Greg Young from Gartner research firm claimed in an online analysis that the exposition of the QuickTime flaw dangers vulnerability research conducted in public. They claimed:

> "The sheer breadth of systems and browsers that potentially could be affected means that this could be a serious browser vulnerability. No single safeguard can guarantee complete protection."

They claimed that ethical hacking, especially those done in public, are "risky endeavors" that defy the good intentions behind them. Ethical hackers may avoid the responsible action of disclosing data to vendors, who use the newly acquired information to develop

patches for the flawed software. The practice could ultimately assist outside hackers to take advantage of the new information for their own selfish gains.

Patch Management

Patch management involves developing, testing, and installing multiple patches to an administered computer system. Patch management tasks include: maintaining current knowledge of available patches, deciding the appropriate patches for specific systems, properly installing the patches, testing systems after installation, and documenting all of these step to step procedures. Large corporations use products, such as RingMaster's Automated Patch Management, PatchLink Update, and Gibraltar's Everguard, to automate patch management tasks.

When it comes to patch management, the most common problem that companies face is the mismatch of configurations. Unmatched patch applications open new holes within the security network, making it an open invitation for outside hackers. Security specialists sometimes carelessly configure company's software with its hardware, allowing unwanted guests to enter without attracting immediate attention. Security teams can avoid such problems by updating and maintaining the right patches into their systems.

> "'One of the problems I've come across is the way IT infrastructure is patched together,' said Lee Benjamin, principal at ExchangeGuy Consulting in Waltham, Mass. 'Look at Wi-Fi access points in a hotel as one example. There are often five or six access points going all the time. Pull into a parking lot and you can find access points.'"

Companies, such as Core Competence Inc., agree that in the IT community, mismatched configuration and missing patches are the most significant vulnerabilities that an enterprise could face. Lisa Phifer, vice president of Core Competence Inc. and an

expert of network security over the last 20 years, noted that the infamous CodeRed worm infected servers at the end of 2007, even though server patches to neutralize it were available since 2001. She claims,

> "If you're a Web server admin and you haven't remediated this most notorious virus yet, that certainly counts as gross misconfiguration,"

She predicts that errors within patch management will account for 70% of successful WLAN attacks by the year 2009.

Due to insecure stored transactions and the lack of patch management, data breaches have been making headlines. TJX took the worst attacks in history in 2006, when an attacker exploited a flaw in TJX's computer network that overlooked information on credit cards, checks and return orders. The hacker stole over $45 million worth of credit card information and penetrated stores within the U.S., Puerto Rico, and Canada. Analysts believe that the intrusion could have possibly extended to the U.K. as well.

Other than TJX alone, other organizations currently face or have at least dealt with similar security issues. In December 2006, a hacker breached into the University of California, Los Angeles and stole private information on 800,000 students. Boring Co. lost one of its company-owned laptops that contained personally identifiable information on 400,000 of its employees. In August, a hacker cracked one of AT&T's computer system and gained access to credit card and personal information on 19,000 of its customers. Major incidents such as these show how businesses have struggled with data protection and the notification of breaches.

Vulnerabilities on the rise

IT security is growing in importance, as it provides value in all aspects of business. Enterprise Management Associates' Montecillo, who once served as a vulnerability management coordinator for the government, agrees that vulnerability management a key part to corporate governance and crucial to “operationalizing” security. He claims:

> “IT risk is emerging as a significant component of total business risk as IT assumes a more prominent role in organizations, and can account for more than 50 percent of total capital expenditure at some companies.”

After the TJX exposure, companies now know the risks and costs of not implementing the latest IT securities. Outside security firms have even released new products that help companies see their vulnerabilities and understand their IT risk.

Although companies have started to invest more into vulnerability management, the science behind it is still new and still growing. Since late as 1999, MITRE, a nonprofit research company, has searched for a standard gauging risk system in the context of network vulnerabilities. Over the last nine years, the company found 28,000 different types of vulnerabilities, making it difficult for the organization to establish a set standard. From last year alone, MITRE found 7,000 unique vulnerabilities.

Although a concrete standard does not exist, the U.S. government supports a standard called, the Common Vulnerability Scoring System (CVSS), which is an open framework that rates the vulnerabilities into different degrees. The Forum of Incident Response and Security (FIRST) released CVSS Version 2.0, which rates the severity of

weaknesses on a scale of 0 to 10, earlier this year. The standards from CVSS consider three factors:

- the base score measures the constant characteristics of the vulnerability
- the temporal score measures the possibility that the bug could change over time
- the environmental score measures characteristics in a user's environment.

A Solution

Due to the different types of vulnerabilities and the variety of standards that each company holds for these vulnerability, there isn't a definite solution when it comes to vulnerability management. Companies also have to factor in costs and risks, when implementing vulnerability solutions and have their own approaches in doing so. Outside sources are even figuring ways to minimize risk in relations to vulnerabilities, as an attempt to do business with these companies. The government does its part to lower risks for organizations by creating a common standard, such as the CVSS, so that tool vendors can develop similar software products.

Executive Summary

Due to the increase use and value in Information Technology, there is a high need for IT security. The lack of security leaves organizations susceptible to attacks that eventually lead them to heavy financial costs. Management teams often think that using scanning programs will be sufficient enough to keep their companies safe from hackers and fraudulent activities. However, recent headlines and disturbances in relations to IT security have proven that companies need more than vulnerability assessment programs to keep their data safe. Companies need to update their IT defenses with the latest technology, which requires them to use the latest patches, and be aware of the newest hacking activities. By implementing all three methods, companies can avoid becoming targets or at least be prepared for another attack.

Bibliography

Keizer, Gregg. "Contest Winner: Vista More Secure Than Mac OS." MacWorld 30 Apr. 2007. 3 Apr. 2008 <http://www.macworld.com/article/57616/2007/04/daizovi.html>.

Harrington, Jan. Network Security: a Practical Approach. 5 Apr. 2008 <http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1178844,00.html>.

Harrington, Jan. Network Security: a Practical Approach. 5 Apr. 2008 <http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1178844,00.html>.

Kaplan, Dan. "Vulnerability Management: Weathering the Storm." SC Magazine Feb. 2008. 5 Apr. 2008 http://www.scmagazineus.com/Vulnerability-management-weathering-the-storm/article/105009/.