Zoran Davidovac
Mathematical Institute, Belgrade
zorandavidovac@mi.sanu.ac.rs

Vanja Korać
Mathematical Institute, Belgrade
vanja@mi.sanu.ac.rs

UDK 007:004.056.5
005.21:004.49
Original research article

Received: May 30, 2010
Accepted: August 02, 2010

VULNERABILITY MANAGEMENT AND PATCHING IT SYSTEMS

ABSTRACT

In this paper, problems are presented which occur most frequently in informative systems, as well as profile of people being interested in their abuse. An overview of attack types is also given and their different motives through examples of electronic warfare. In this paper, security managemet is suggested which prevents abuse of vulnerability of IS systems within an organisation, which again is being introduced through vulnerability management and patching IT systems. Proactive scanning of systems was conducted at the Mathematical Institute of the Serbian Academy of Science and Arts and an overview is given in this paper.

Key words: Information security, Vulnerabilty Management, Patch Management, Reducing Costs, botnet

1. INTRODUCTION

Introducing the practice of patch and vulnerability management – PVM system represents a precaution measure which prevents abuse of vulnerability of an IT system within an organisation.

The results include reduced costs concerning human resources (time), as well as reduction of costs caused by patching and abuse of system's vulnerability. On the other hand, information about potential new threats is increased.

With proactive management of system's vulnerability, potential abuse is reduced or eliminated, while duration and effort are much reduced in comparison to these activities when abuse already took place.

To whom is PVM intended? The use in predominantly intended for national institutions, banks and other public institutions possessing large information systems which, if endangered, could endanger security of vital institutions , which could further lead to severe consequences in relation to the security of the country and its citizens, no matter whether these systems posses internet access.

* The article results from the project: *Viminacium, Roman city and military legion camp – research of material and non material of inhabitants by using the modern technologies of remote detection, geophysics, GIS, digitalisation and 3D visualisation* (*no 47018*), funded by Ministry of Education and Science of the Republic of Serbia.

2. PROBLEMS RELATED TO INFORMATION SYSTEMS

A common thing for all the large information systems (further IS) is the presence of a large number of different software and servers with different purposes, but on the other hand, the IS is limited with costs of the Information System, through which human resources considering the number of employees is limited.

Budgets are usually limited and it is a common case that the number of people maintaining servers and working stations, updating software and offering support to local users is insufficient. A special problem includes low level of education, causing insufficient knowledge and the lack of people who are in charge of security. In case when there is someone in charge, which is rare, that person usually only possesses basic net knowledge, meaning that he/she never attended a security course abroad and cannot recognize any of the hacking technologies. In other words, patching management is completely neglected (one is leaning on automatics) and vulnerability of the system is not the main concern.

By using similar IS and software on other locations, a larger number of individuals automatically becomes acquainted with the same IS, and in the case of vulnerability there is a greater number of attack spots.

Certain enabling circumstances and bad trained employees, informational and security unawareness contribute to the magnitude of errors, so therefore even social engineering is possible. Examples are numerous: stickers with users data for logging usually taged onto a screen or housing, questions like „What was your password?“ etc. Cases are known that even when suggestions are given to improve the net, there is an answer that our net is secure enough, that there were no intrusions and even if the net was not secure, we would ot be interesting enough: „who would attack us, we have no confidential data and they would be of no use for anyone“. The question whether anyone would intrude is wrong, since one would actually have to know whether someone already broke in. Even if there are no interesting data on the existing net and that the user is of no interest for the intruders, the net itself as a source for attacking nets of other users is a very intriguing matter and that is exactly the most usual case.

Still, one has to admit that a great number of public institutions advanced their security by introducting serious logging systems, but in practice it is shown that this alone is not enough. As a result of all the named facts, it turns out that the bigger the IS, the greater the vulnerabiliy of the system from different directions.

In order to gain a better insight into this problem regarding the profile of abusers of Information systems, some examples of the IS abuse shall be presented further on in this paper.

3. INFORMATION SYSTEMS AND THEIR ABUSE

Who is an individual or a group being interested in using system's vulnerability and abusing it? And what is the purpose – information, material income or damage?

Individuals or groups with a similar or identical aim could be of different demographic structure from adolescents to students, amateurs and professionals, employees or former employees, to people who are curious about confidential information like criminals, terrorists working for profit only, up to informatically extremely well trained enemies who, by making public services inaccessible, wish to destabilize and paralize the state and make enormous economic damage.

The greatest degree of abuse is possible in the case of electronic warfare (Cyber War) which aims towards paralizing, destruction, disabling or deleting systems of public or military importance, like in cases of switching off the IS of electric suppliers, paralizing banks, the infrastructure of

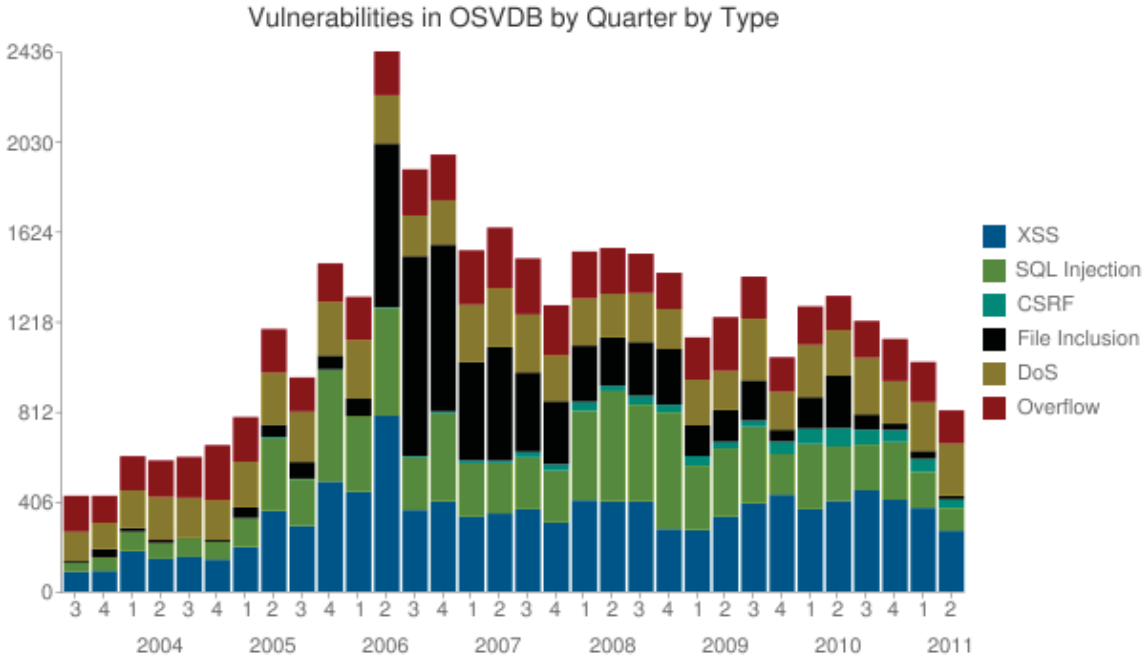


Figure 1 Quartal display of vulnerability

cellular or fixed telephones, traffic internet and disabling the IS for country's defence.

Individuals within such a group permanently follow inovations of modern technologies and possess an high degree of knowledge, even higher than an average knowledge of an IT sector employee.

A group or an inidivdual motivated to abuse IS possess unlimited resources and time. Such an individual possesses main features which include: programming knowledge, knowledge about operative systems, excellent knowledge about nets, an average knowlegde of cryptography, as well as an excellent knowledge about data bases and web applications.

Still, there are huge differences between individuals and groups of indiviuals „working together". Cooperation does not necessarily mean that there was a joint action in order to use and/or abuse an error within an IS.

There is an assumption that such a group of people involved in hackering are actually some kind of software companies or even huge organisations which, instead of creating softwares for legal organisations do exactly the opposite.

Cooperation of groups and individuals can be simple exchange of experiences on a forum, sending exploita to public lists and groups, even on exclusive sites dealing only with security topics and existing only to inform the public about potential security abuses, latest threats and vulnerability. The titles of sites involved in this kind of informing are The Open Source Vulnerability Database[1], National Vulnerability Database[2], Common Vulnerabilities and Exposures *(*CVE*)*[3]. On figure 1 vulnerability is displayed in quartals, within the period from 2004 to 2011 on 22nd of September 2011 (source http://osvdb.org/).

1 http://osvdb.org/
2 http://nvd.nist.gov/
3 http://cve.mitre.org/

4. ELECTRONIC WARFARE

Security of the internet is getting more and more critical with the expanion of the internet. Lately, the cyber space is observed as one of the biggest security challenges of 21st century. We testify the always growing number of attack attempts on PCs, phishing attacks, hackernig, spreading of worms and viruses. All of these elements represent a sort of electronic warfare. Data from different strategic documents of leading countries like the USA and China show how huge a security challenge the cyber space is. In these military strategic documents as battlefields land, sea, air and the Universe are mentioned, but recently also the cyber space.

Some examples of the „Electronic warfare“ shall be listed below (Carr 2009; Clarke and Knake 2010; Kramer, Starr, S. and Wentz, L. 2009).

Great Britain

In 2007 the British Information Agency discovered that Chinese hackers had priviledges on servers of some of the British banks and companies.

In 2009 Gordon Brown became the first national “cyber-security” minister.

Germany

In 2007 the PCs of the German cancelor and three ministries were infected with the Troyan virus. This attack opened acces to the infected PCs and sensitive data to the hackers.

France

In 2007 hackers attacked French state sites, including the site of the Ministry of Defense with much success.

The official news connected to this case were that the hackers tested the security of the IS and were not interested in stealing sensitive data.

United States

In April 2009 the “Wall street Journal” informed the public that security around the Penthagon’s project „Joint strike fighter“, which is several million dolars worth, was compromized and that several terabytes of data were stolen by unknown hackers. A hypothesis remained that the hacker attack originated from China.

In May 2009 the Americal president Barack Obama announced that he shall introduce a cyber coordinator who shall develop cyber security strategy.

In July 2009 a DDos[4] attack occured of a rather small capacity against 25 sites of the American goverment. Some of them remained inaccesible for several days (among others there were the Federal Trade Commission[5] and the Department of transportation).

Kyrgyzstan

In January 2009 hackers attacked three out of four ISPs (Internet service providers) and 80% of the country was left without internet, e-mail and web for several days. The motif of the attack remained unknown, as well as who was responsible for it. One of theories was that the Russian goverment forced the president of Kyrgysztan to close his air-bases in Manas for the USA air-traffic. Another theory was that the president himself engaged Russian non-govment hackers to interrupt air-traffic to prevent the opposition to use the internet as fighting weapon against the leading party, since there were political tensions growing within the country.

4 A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

5 The Federal Trade Commission (FTC) is an independent agency of the United States government, established in 1914 by the Federal Trade Commission Act. Its principal mission is the promotion of consumer protection and the elimination and prevention of what regulators perceive to be harmfully anti-competitive business practices.

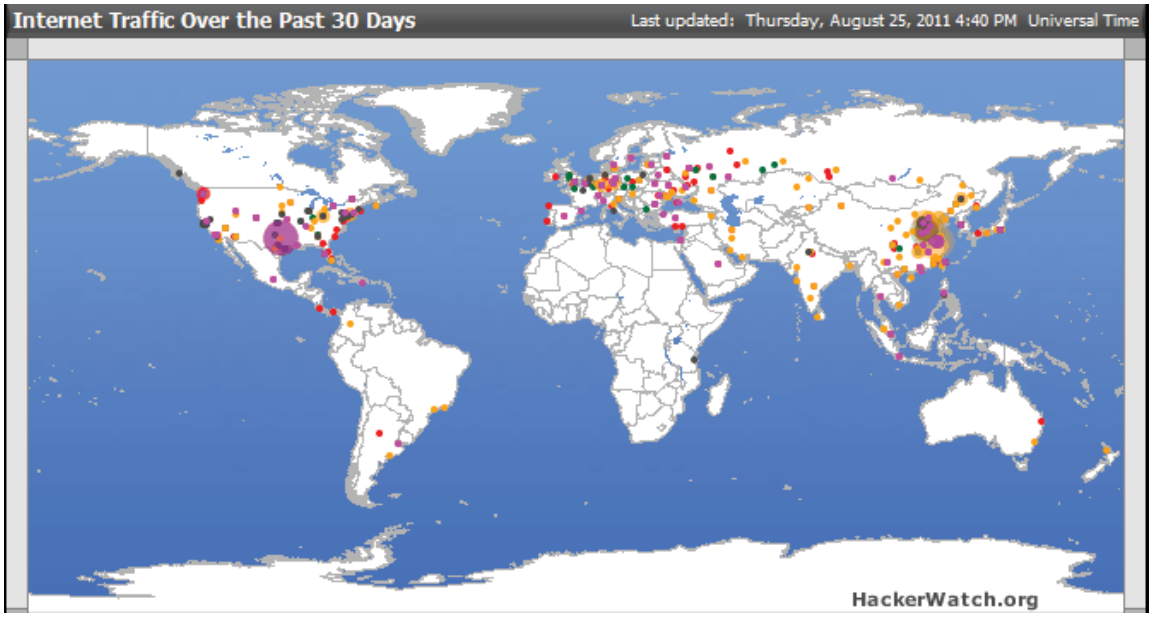


Figure 2: Hacking activities during the last 30 days

Estonia

In April 2007 hackers attacked the Estonian IS, ministries, political parties, means of public informing and banks. The Estonian minister of defence let NATO solve the problem. In literature, places can be found in which the Estonian case is described as the WWI – web war one.

Israel

In 2009, due to the Hamas conflict in Gaza, the sites of Israel were attacked with DOS (denial-of-service) and damaged with the power of 15 million hits per second from half a million PCs from the whole world (botnet[6]). Both government and civil sites were under attack. One of the features of this cyber event is participation of the state (Israeli Defense Forces and Hamas), which does not occur often.

South Korea

On 4th of July 2009, a DDOS attack brought down both state and commercial sites in South Korea, while American sites were attacked simultaneously. Although South Korea held North Korea responsible for the attack, the identity remained unknown. In 2009, the defense minister of South Korea stated in public that in 2004, North Korea started a five-year education of 600 hackers, which ended in 2009. Their goal was conduction cyber wars mostly against the United States, South Korea and Japan.[7]

Iran

During the controversal presidential elections held on 14th of June 2009, over 100.000 of citizens protested against the results of the elections, stating that they were fraud. One of the means of protest was the usage of DDOS attacks aimed against the Iran govement. The social web Twitter was used as a platform for the organization of this DDOS attack.

6 In information technology, a botnet is a collection of compromised computers connected to the Internet, termed bots, that are used for malicious purposes. When a computer becomes compromised, it becomes a part of a botnet. Botnets are usually controlled via standards based network protocols such as IRC and http.

7 http://www.docstoc.com/docs/3878208/Biznis-and-Finansije-1

Zimbabwe

In December 2008, the African scientists published a paper entitled „Glass Fortress: Zimbabwe's Cyber Guerilla Warfare". It was stated in the paper that Mugabe's goverment silenced the opposition by using obstruction techniques of the internet and controlling all of the e-mails. For at least five years, the techniques of DDOS attacke were used as well.

Serbia

Between 1999 and 2011 similar attacks also occured in Serbia, like hackering state sites and sites with Serbian character. Such stations were usually defaced. In March 2011, the site of the Media research Centre (Medijski istraživački centar - MIC) from Niš was attacked by Albanian and Kosowo hackers.[8] In September 2011, the Kosowo hackers brought down the site of the Studenica monastery and of the ombudsman of Vojvodina.[9] Hackering activities during the last 30 days can be seen on Fig. 2.

White parts unfortunately do not mark spots in which there were no activities, but about which there are no data.

Another important fact, especially ever since the event in Estonia in 2007, is that the NATO activity engaged because of cyber threats dramatically increased. In 2008, a NATO document entitled "Cyber Defence Policy", and another one entitled "Cyber Defence Concept" were formed, in which threats, vulnerability risks and precaution measurments are estimated. In all of these NATO documents it is mostly stated that the NATO states are responsible for protecting their cyber space, but NATO is there to help and coordinate these activities, as well as educate staff. In 2008, an Expert centre was established in Estonia out of seven members for Cyber Defense (Clarke R. and Knake R. 2010). It is interesting to notice that this centre is never mentioned as a part of the NATO, but as an international organisation supported by NATO. For Serbia as a participant of the Partnership for Peace it is important that in 2009 a frame was formed for cooperation between the NATO and partners.

5. BOTNET FEATURES

On the Israeli example one can notice that half a million of PCs worked as one and generated 15 million hits per seconds, attacked by the "denial-of-service" (DOS) .

The group of PCs having the same goal and preforming the same command are called botnet.[10]

The action of creating a botnet is shown below, used in order to send spam mail[11] as one of the means of attack:

1. Botnet operator (the conductor of botnet) sends viruses or worms containing malicious applications – the bot, aiming to infect users' PCs.

2. On an infected PC, the bot becomes controlled by C&C servers (command and control). It is usually either the IRC server or the Web server.

3. Spamer buys access to the botnet from the botnet operator.

4. Spamer sends instructions to the infected PCs over the IRC server, ordering them to send spam mails to mail servers.

When PCs are concerned, most of people have their PCs turned on for 24 hours and each of the PCs or servers being directly or indirectly on the internet can potentially be a art of such a botnet and might already perform scanning or attacking a system without user's knowledge!

One immediately asks whether "Antiviruses keep us safe?". The answer is that an antivirus program reduces the possibility of a PC to become a part of a botnet, but that it is still possible that a virus is within a PC and that it is a part

8 http://www.blic.rs/Vesti/Hronika/240918/Albanski-hakeri-napali-srpski-sajt

9 http://www.vesti.rs/Svet/Gr%C4%8Dka/Hakovani-Studenica-i-ombudsman-3.html

10 Bot is an abbrevation of RoBot, while net is an abbrevation of Network.

11 http://en.wikipedia.org/wiki/Botnet

Figure 3: From Troyan to botnet.

of botnet even when the latest antivirus program is installed.

The problem is serious, but it is not treated seriously enough. In order to become aware of how much such a problem is complex, we shall state some types of botnet attacks:[12]

Spam e-mail – messages masked in such a way that the addressee thinks that they come from a familiar person, but are actually either advertisments or of malicious content or both.

Denial-of-service attacks[13]

Adware[14] – its purpose it to advertise a commercial entity without knowledge or aprovement of the user, by changing banners of the advertisment on web pages with some other advertisment content.

Spyware[15] – is a program which sends data to its createor about activities of the user. Usually, information about passwords, credit-cards and other useful information are gathered, which could be sold at the black market. Compromising machines situated within huge corporations are even more worth (in the botnet sense), because they contain huge numbers of confidential information.

Click fraud – is created when user's PC visits a web site without the knowledge of the user himself, creating false „web" traffic for personal or commercial purposes.

Fast flux – represents a DNS technique of botnet, with the intention to hide sites delivering „malware" and phish by hiding behind compromizing machines presented as proxy server.

12 http://en.wikipedia.org/wiki/Botnet
13 http://en.wikipedia.org/wiki/Denial-of-service_attack
14 http://en.wikipedia.org/wiki/Adware
15 http://en.wikipedia.org/wiki/Spyware

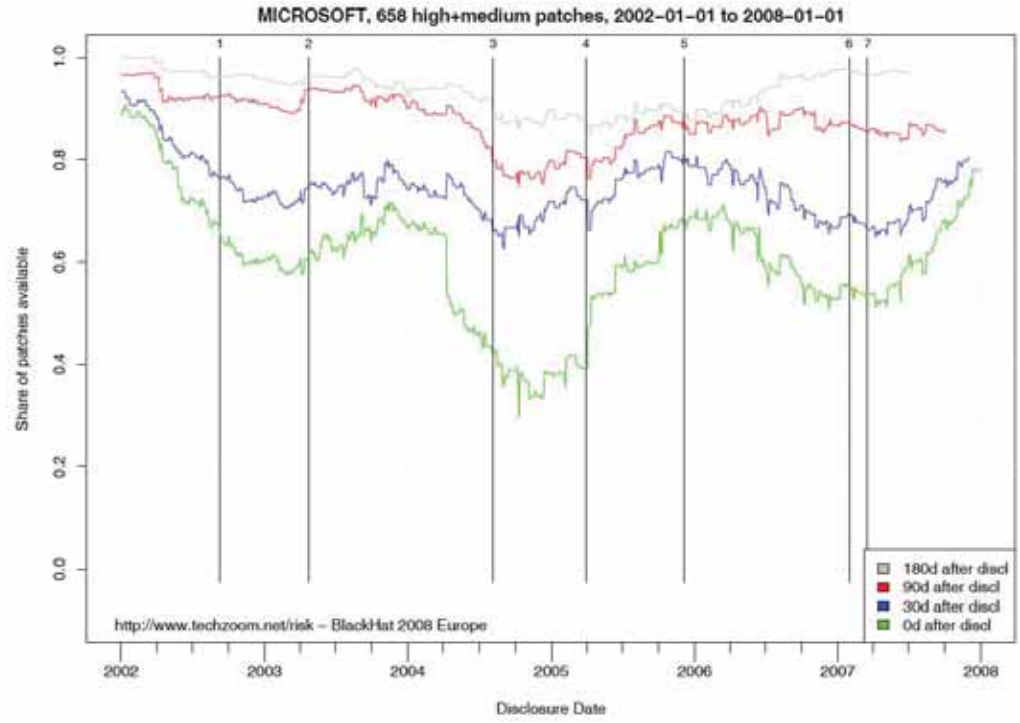


Figure 4: Graph of announcing a patch compared to announcing vulnerability.[16]

Brute-forcing – organizing bots in such a manner that, by coordinated action, they break in (by a brute-force attack) services like FTP, SMTP and SSH.

Scareware – making useres buy a false antivirus in order to clean the PC from a suspected infection. The scareware itself could install a virus an vice versa. They could possess „worm" features, i.e. the botnets could be created in such a manner to infect other PCs automatically.

This is a list of some of the most famous botnets spread throughout the cyber space:

BredoLab – 30 million bots
Mariposa – 12 million bots
Conficker – over 10.5 million bots
Kraken – half a million bots
Srizbi – half a million bots
Bobax – 185.000 bots
Rustock – 150.000 bots
Cutwail – 1.5 million bots
Storm – 160.000 bots
Grum – half a million bots
Onewordsub – 40.000 bots
Mega-D – half a million bots
Spamthru – 12.000 bots

On the Israeli example one was able to see what the number of half a million (500.000) PCs could cause, which took part in the attack. This directly pionts out to the potential hackers have at their disposal. The question arises whether hackers are leaders in technology.

The answer would be that not all of them are, but what they have in common is to abuse system's vulnerability while it is vulnerable and in such a manner sell PC by PC or server by server to their resources.

For instance, after discovering and announcing security ommissions, pathces are not available for a while, until they are announced by software producers.

The example at Fig. 4 shows how fast MS reacts and how fast a patch for OS is delivered.

Actually, the time in which there is no patch

16 Izvor: http://www.techzoom.net/publications/0-day-patch/index.en 2008

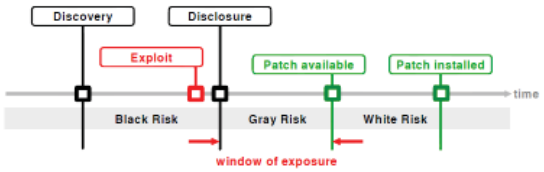


Figure 5: An overview of window of exposure and announcing a patch compared to announcing vulnerability.[17]

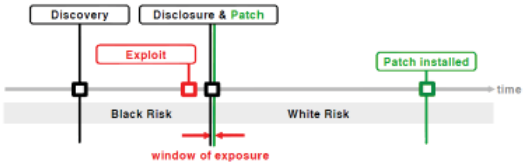


Figure 6: Depiction of a „zero-day window of exposure“, when vulnerability is announced simoultaneously with announcing a patch.[18]

(window of exposure) is the time during which system's vulnerability is abused, Troyans are posted and one's PC and server become parts of botnet or a hackers' target (Frei and Tellenbach and Plattner 2008). This time approximately includes 20 days, while practically this time measures between 0 and 180 days. This gives a completely different awareness about automatic patching and system's updating which is provided by system's producer.

Still, in some cases patches are quickly announced, which is called Zero Day Exploit. It is usually system's vulnerability discovered and admitted by software producer himself, when along with the announcement of vulnerability a system's patch is also announced, thus making window of exposure zero (Frei and Tellenbach and Plattner 2008).

6. VULNERABILITY MANAGEMENT

After the definition security ommission is an error in a software system which can lead towards working against its documented design and could be compromized in documented security policy (Organization for Internet Safety 2004). Security ommissions represent permanent threat for PC users and even the internet itself. All the ommissions of this kind represent vulnerability of a system.

From all the stated facts it turns out that it is necessary to track vulnerabilities which occur and if IS possesses a vulnerability which could be abused, it is in such a case necessary to close it or to do everything to prevent abuse until a patch is announced.

Vulnerability mangement is serious work for huge teams and requires a long time and resources even with a smaller IS. The bigger the IS is, the more hetherogenous and complex the problems are involved. Problems are so complex that companies like Master Card and Visa required that if they do business or process payment cards, their parnters need to possess "Vulnerability Management". In such a way, „Vulnerability Management" became part of security standard for payment cards PCI DSS (Payment Card Industry Data Security Standard).

Since huge resources are needed for vulnerability tracking, it was logical that firms were established dealing with this matter exclusively and offering tools which automaticaly search for vulnerabilities within the IS, report, give risk estimations and abusement possibilities of such a system. The risk caused with security errors can be reduced if they are identified, examined and solved early enough. With support of scientific-research unit, quality of software products is improved by detecting security threats, methods to avoid them and conditions under which threats appear, which is an additional benefit.

As far as commercial leaders in the "Vulnerability Management" field are concearned, there are Rapid7 and Saint companies. Their soft-

17 Izvor: http://www.techzoom.net/publications/0-day-patch/index.en 2008

18 Source: http://www.techzoom.net/publications/0-day-patch/index.en 2008

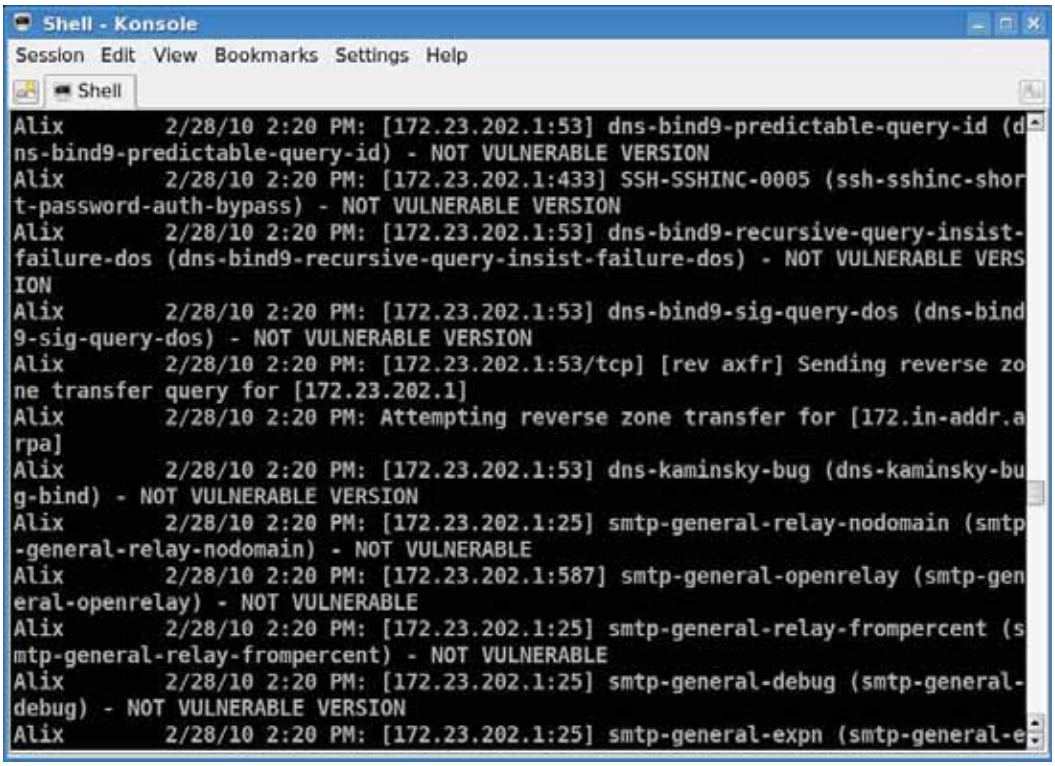


Figure 7: Rapid7 NeXpose[19] searching for system's vulnerability.

19 Rapid7 NeXpose Unified Vulnerability Management (http://www.rapid7.com/)

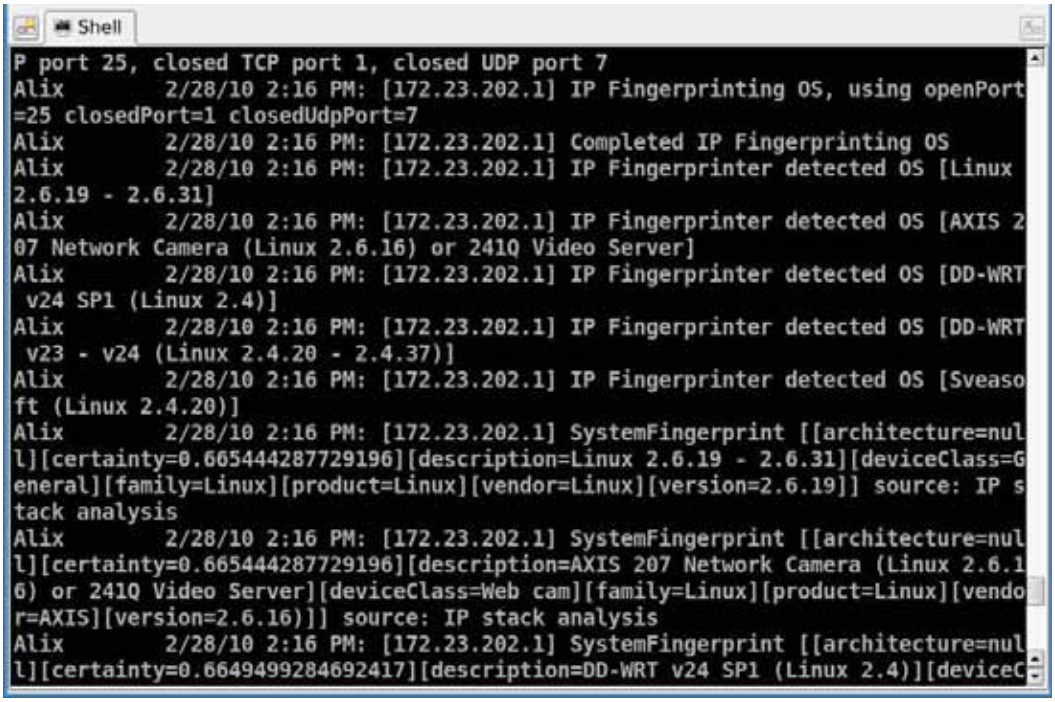
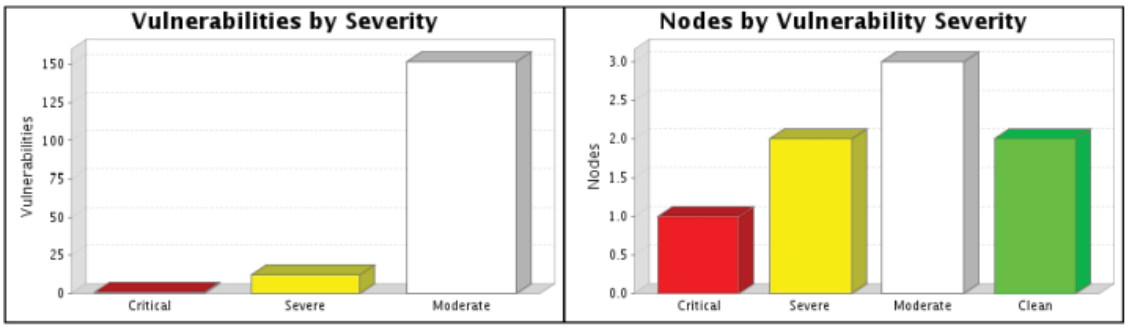


Figure 7.1: Rapid7 NeXpose precise system detecting.

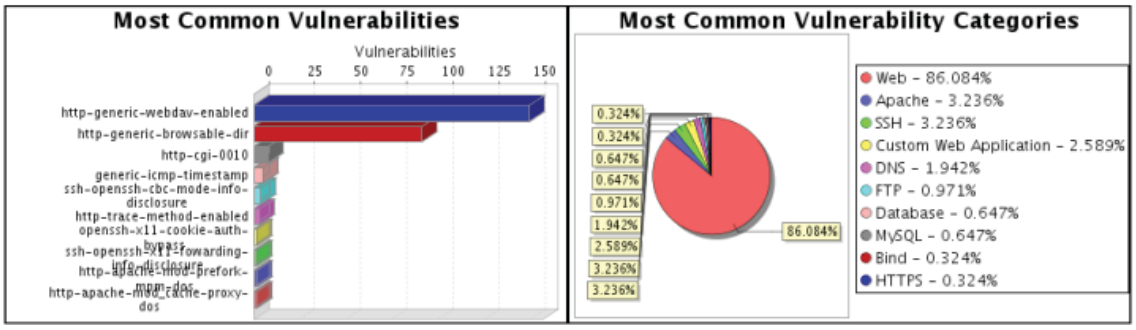
Site Name	Start Time	End Time	Total Time	Status
	November 17, 2009 14:17, CET	N/A	N/A	Unknown

The audit was performed on 5 systems, 5 of which were found to be active and were scanned.



There were 165 vulnerabilities found during this scan. One critical vulnerability was found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 12 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 152 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 1 of the systems, making them most susceptible to attack. 2 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 3 systems. No vulnerabilities were found on the remaining 2 systems.

Figure 8: Report of the Rapid7 NeXpose-a: Vulnerability compared to the level of risk.



There were 149 occurrences of the http-generic-webdav-enabled vulnerability, making it the most common vulnerability. There were 266 vulnerabilities in the Web category, making it the most common vulnerability category.

Figure 8a: Report of the Rapid7 NeXpose-a: The most common vulnerabilities.

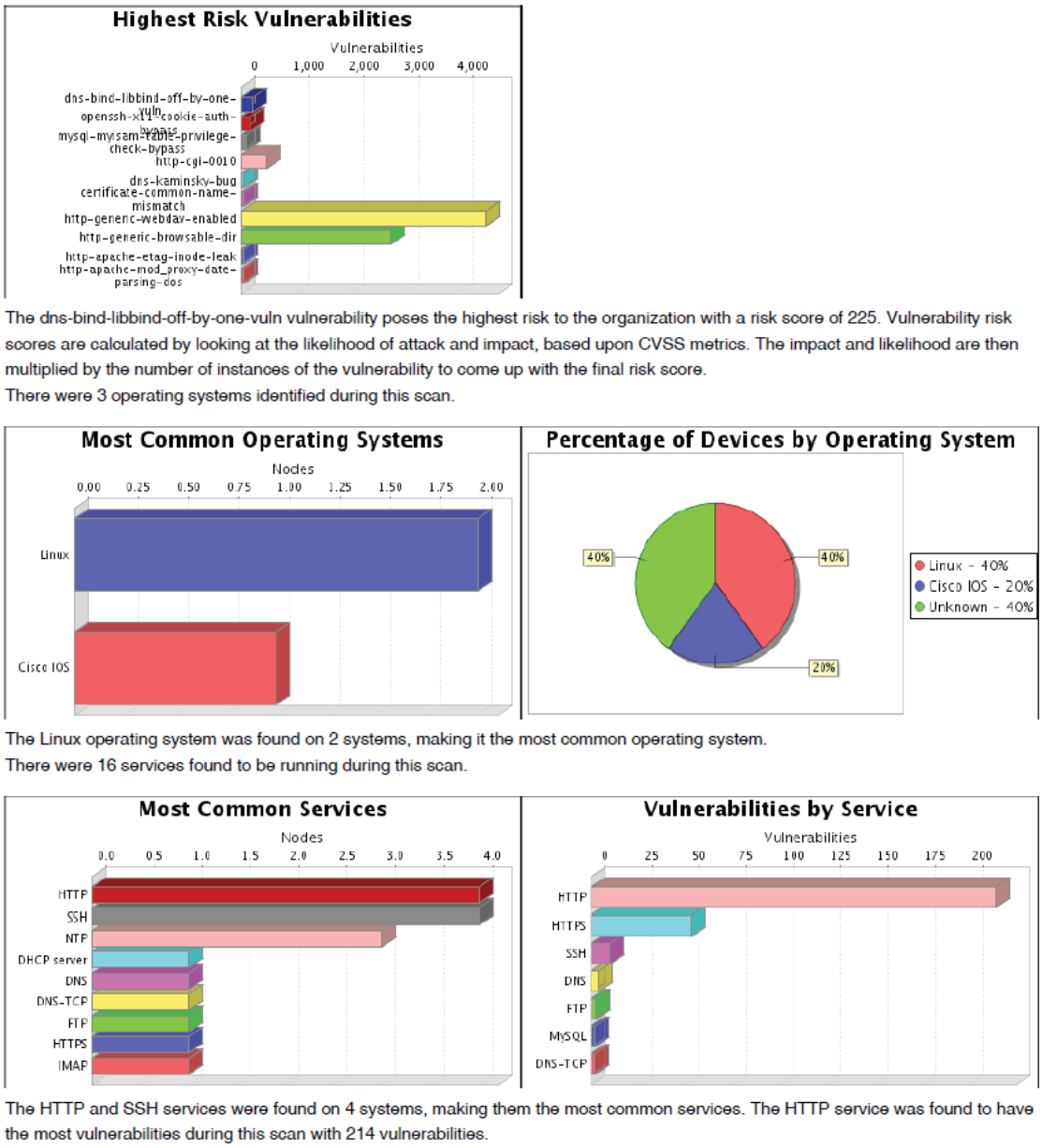
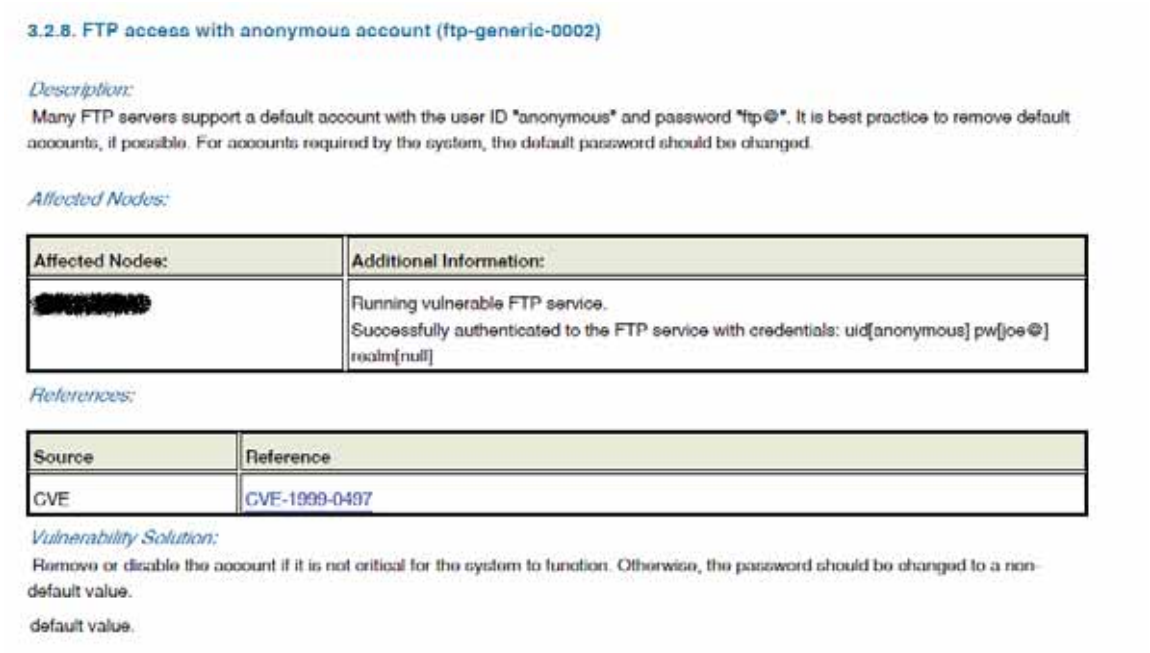


Figure 8b: Report of the Rapid7 NeXpose-a: Vulnerability of OS and service.

wares do not offer only vulnerability management, but also the test itself represents a proof whether the system is ajusted to security standards (PCI DSS, NIST, SCAP, NERC-CIP , SCADA ...). Pen-test (penetration test)[20] is also performed, focused on intelligence. Actually, testing of the whole IS system is performed in such a way that it is not endangered.

By introducing one of the Rapid7 NeXpose or Saint solutions, the IS of a complete organisation is covered, i.e. network security, web applica-

20 Pentest or penetration test is a method for estimating security of PC's system or net by simulating a malicious insider (persons with legal access to the sysytem on some level) and outsider attack (persons with no legal access to organisation's system) Source: http://en.wikipedia.org/wiki/Penetration_test



3.2.8. FTP access with anonymous account (ftp-generic-0002)

Description:

Many FTP servers support a default account with the user ID "anonymous" and password "ftp@". It is best practice to remove default accounts, if possible. For accounts required by the system, the default password should be changed.

Affected Nodes:

Affected Nodes:	Additional Information:
[redacted]	Running vulnerable FTP service. Successfully authenticated to the FTP service with credentials: uid[anonymous] pw[joe@] realm[null]

References:

Source	Reference
CVE	CVE-1999-0497

Vulnerability Solution:

Remove or disable the account if it is not critical for the system to function. Otherwise, the password should be changed to a non-default value.

default value.

Figure 9: Unwanted anonimous FTP access.

Source	Reference
URL	http://httpd.apache.org/security/vulnerabilities_13.html
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 1.0 and < 2.0

Upgrade to Apache version 1.3.39

Download and apply the upgrade from: http://www.apache.org/dist/httpd/apache_1.3.39.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.0 and < 2.1

Upgrade to Apache version 2.0.61

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz

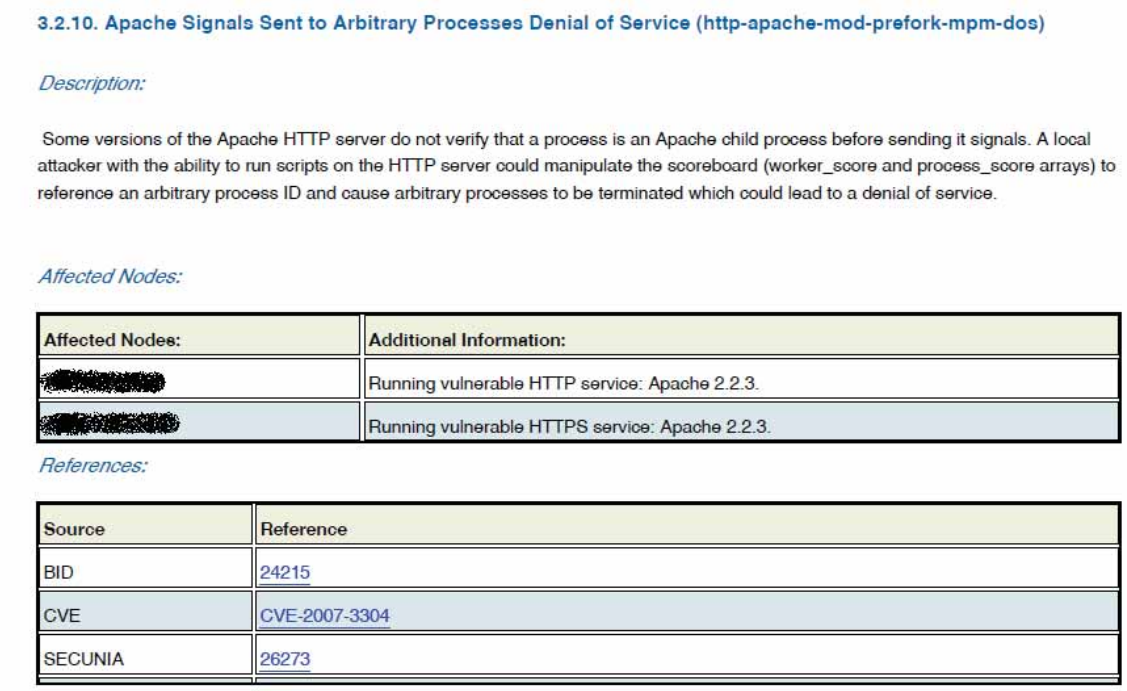
Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.1 and < 2.3

Upgrade to Apache version 2.2.6

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.



3.2.10. Apache Signals Sent to Arbitrary Processes Denial of Service (http-apache-mod-prefork-mpm-dos)

Description:

Some versions of the Apache HTTP server do not verify that a process is an Apache child process before sending it signals. A local attacker with the ability to run scripts on the HTTP server could manipulate the scoreboard (worker_score and process_score arrays) to reference an arbitrary process ID and cause arbitrary processes to be terminated which could lead to a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
[redacted]	Running vulnerable HTTP service: Apache 2.2.3.
[redacted]	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	24215
CVE	CVE-2007-3304
SECUNIA	26273

Figure 10: Vulnerability of Web Server to DOS attack.

tion security and database security. When vulnerability management of an IS is concearned, this represents an adequate solution.

7. APPLICATION OF SCANNING SYSTEMS WITH THE RAPID7 NEXPOSE

Software for vulnerability management at the mathematical institute of the serbian academy of sciences and arts

This aprticular system scanning was performed at the Mathematical Institute, agreed by the same Institute.

The complete report has 154 pages, while here only parts as examples are given (Davidovac, Z. 2010: 71-76).

Remark: Due to professional and security reasons, the IP addresses and names were left out or erased.

In one case, it was discovered that on one of the systems, there is an active FTP server, making anonimous access to the server possible, which is shown within the report in Fig. 9.

It can also be seen when and where the error and security recommendation were published, as well as what to do in order to eliminate the problem.

From the examples given (Fig. 9, 10) can be seen that there is always a vulnerability within an IS which was not noticed at all.

Obviously, an update of the web server was needed in order to solve problems on systems and provide security from a potential DOS attack.

Figures 8, 8a and 8b are graphs showing system's vulnerability, give direct answers that a system is maintained but not unvulnerable. According to present knowledge, it was possible to intrude into the system and abuse it.

One needs to stress that scanning with a Rapid7 Nexpose tool could be performed both internally and externally, but for the most precise data it is necesarry to remove the firewall and remove IDS/IPS durign scanning, in order to gain exact information, since firewall and IDS/IPS devices can give a false security image of the IS.

8. RESUME

Security practice preventing abuse of vulnerability of an IT system within an organisation represents introducing vulnerability management and patching T systems. It results in saving money in human resources (time) and reducing costs arising from patching and abuse of system's weaknesses, as well as increase of information about potential new threats. Proactive management of system's vulnerability reduces or elliminates potential compromising of an IT system and with that, time and effort are reduced, according to time and effort spent when abuse already took place. In this paper, attack types are shown to which information systems could be exposed and how much harm can they cause.

Resutls of a Rapid7 NeXpose scanning of servers directly shows where the problems are and what to do in order to solve them. It also shows to the IT personell where to focus and where the most critical problems are which should be solved immediately.

By intoroducing such a proactive approach into an information system, the complete information system of an organisation is covered, actually network security, web application security and database security. This represents an adequate solution when vulnerability management of an information system is concearned.

As a result, it appears that certain parts of an information system are thoroughly and detailed scanned in order to find out whether the system was abused, after which the system becomes updated.

After updating the system, it is necesarry to re-check the system againg, because of human factor which can cause some errors, which could again lead to system's compromizing.

Finally, as a result of vulnerability management of an IS, security is increased and stability in the work of the complete system is secured, while finances and human resources are reduced.

BIBLIOGRAPHY

Clarke, R. and Knake, R.
Cyber War: The Next Threat to National Security and What to Do About It, New York : Harper Collins, 2010

Kramer, F. and Starr, S. and Wentz, L.
Cyberpower and National Security (National Defense University), Virginia : Potomak books, 2009

Carr, J. 2009.
Inside Cyber Warfare, Sebastopol CA,O'Reilly Media, Inc., 2009

Davidovac, Z. 2010
Podizanje nivoa bezbednosti upravljanjem ranjivosti u informacionim sistemima, M. Mihaljević (ur.), Beograd: Metropolitan univerzitet, 2010

Organization for Internet Safety,
Guidelines for security vulnerability reporting and response, [e-book], 2004. Available through http://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf pristupljeno 3. juna. 2011

Frei, S. and Tellenbach, B. and Plattner, B.
0-Day Patch Exposing Vendors (In)security Performance, [e-book], Zurich :Computer Engineering and Networks Laboratory (TIK) Swiss Federal Institute of Technology, 2008. Available through http://www.techzoom.net/publications/0-day-patch/index.en , pristupljeno 11. septembra 2011

REZIME
UPRAVLJANJE RANJIVOŠĆU I ZAKRPAMA IT SISTEMA

Ključne reči: Informaciona bezbednost, upravljanje ranjivošću, upravljanje zakrpama, smanjenje troškova,botnet

U radu su prikazani problemi koji se najčešće događaju u Informacionim sistemima kao i ko je sve zainteresovan za njihovu zloupotrebu. Takođe dat je i prikaz tipova napada kao i njihovi različiti motivi kroz primere elektronskog ratovanja. U radu se predlaže bezbednosna praksa koja sprečava zloupotrebu ranjivosti IS sistema unutar organizacije, koja se ostvaruje kroz uvođenje upravljanja ranjivosti i zakrpa IT sistema. Proaktivno skeniranje sistema izvedeno je u Matematičkom institutu SANU i u radu je dat prikaz.