RESEARCH REZULTS OF A NETWORK SECURITY PERIMETER FOR ROMANIAN E-COMMERCE COMPANIES

Iustin Priescu
Associate Professor, Ph.D., Titu Maiorescu University, Bucharest, Romania
Rodica Neagu
MBA, Outpost24, Sweden
Sebastian Nicolaescu
Eng., Ph.D. Candidate, Verizon Business, New York, USA

ABSTRACT:

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the networks security.

In august 2010, a network perimeter security was conducted by Outpost24 together with Titu Maiorescu University for 22 Romanian e-commerce companies, as participants to the event E-Commerce Award 2010 - 5th edition 1. GPeC (http://www.gpec.ro) is an annual event dedicated to e-commerce companies where 80 criteria are used to different tests by users and specialts and the best in different domains are rewarded.

The study was facilitating by Link2commerce, organizer of the event, and results had been presented during the Award Gala, on September 02, 2010.

1. THE VULNERABILITY SCANNING METHODOLOGY

New security risks are discovered every day in commonly used applications, operating systems and network components. These are used by hackers and criminals to carry out attacks. With the increased dependency on information technology, the consequences of attacks are becoming increasingly severe. The victims are suffering from losses related to interruption in business, bad publicity and exposure of confidential information.

Vulnerabilities are defects, bugs or misconfigurations in software that can be exploited by an attacker to compromise the confidentiality, integrity or availability of information. Vulnerabilities in networked systems are a major source of today's information security risks, as they expose an organization and its assets to external threats like black-hat hackers, crackers or plain criminals.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

Outpost24 provides an easy to deploy and user friendly solution to continuously assess your risk exposure. Using our automated services is like having a highly skilled security team constantly probing your network to discover vulnerabilities.

Identified vulnerabilities are rated and reported together with recommended remedy. The process of correcting identified vulnerabilities is supported by workflow tools for delegating remediation tasks to appropriate administrators.

The results can also be compared over time, to monitor trends in risk exposure.

In contrast to manual penetration testing, automated vulnerability scanning is typically performed very frequently. This is important as new vulnerabilities are discovered in a high pace and your risk exposure increases in proportion to elapsed time since the last assessment of your network. Outpost24's extensive vulnerability database is updated on a daily basis. Other advantages of using our services include:

- *Proprietary technology* - All services delivered by Outpost24 are based upon our leading core vulnerability scanning technology.
- *24/7 technical support* - Unlimited phone and e-mail support provided by security experts.
- *Ease-of-use yet flexibility* - An easy-to-use web interface. By using the standard configuration you are quickly up and running, whereas more advanced features can be used on-demand.
- *Cross platform support* - All commonly used operating systems, applications and network types can be successfully assessed.
- *Maintains network availability* - Several mechanisms to minimize possible network interruptions are implemented and the user can schedule the scans with respect to individual requirements.
- *Alignment with standards* - Vulnerability information is aligned with the CVE (Common Vulnerability and Exposures) standard for Information Security Vulnerability Names.

Outpost24 offers two products within this field. OUTSCAN is an on-demand service for Perimeter Vulnerability Assessment and HIAB is a plug-and-play appliance for Internal Vulnerability Assessment. Both solutions can be used independently, but together will provide you with a complete assessment of network.

2. THE VULNERABILITY SCANNING TOOL - OUTSCAN

The study used the vulnerability scanning tool - OUTSCAN, a Software as a Service (SaaS) solution, with which only software security vulnerabilities that were exposed to the public internet were analyzed (Figure 1).

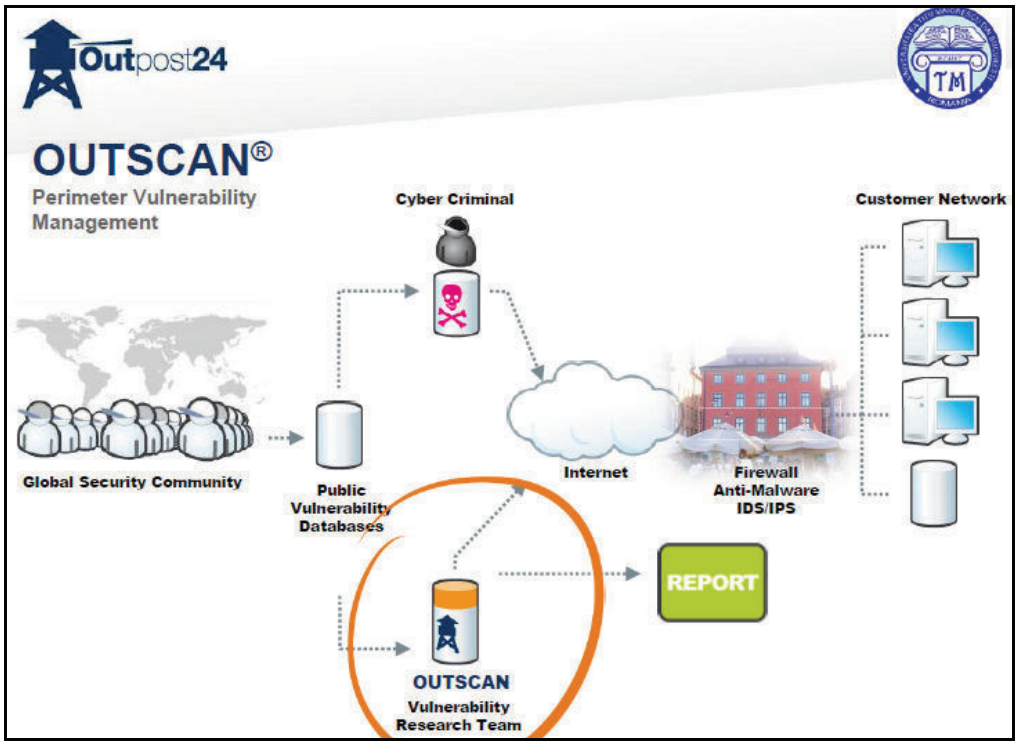


Figure 1. The OUTSCAN architecture and functionality

All participating organizations had given their consent for the conducted vulnerability scans and each company was afterwards confidentially informed about the identified weaknesses in their own network. Being a study dedicated to companies from one industry the study allowed also to the participants to compare their own results with general findings.

Since most of the e-commerce companies are using hosting services they were pleased to have an independent opinion, was one the conclusions of the survey done after the event.

3. THE RESULTS OF THE STUDY

The vulnerability analysis revealed a total of **2035 vulnerabilities on 30 hosts run by 22 different organizations**.

This study analyzed vulnerabilities in networked computer systems that were accessible from the internet, most being websites and email servers.

Vulnerabilities are defects, bugs or miss-configurations in software that can be exploit by an attacker to compromise the confidentiality, integrity and availability of information. New vulnerabilities are discovered every day, and in March 2010, the U.S. National Vulnerability Database (NVD) (http://nvd.nist.gov/) holds well over 41 000 known vulnerabilities.

The Common Vulnerability Scoring System (CVSS) measures the relative severity of a vulnerability on a scale from 0 (low) to 10 (high). CVSS is used by the National Vulnerability Database (NVD). Specification available online at http://www.first.org/cvss/.

Thus, organizations that rely on dependable information systems need to frequently assess their exposure to these vulnerabilities in order to be able to manage their risk. E-commerce companies are such organizations and the study could be looked as a pilot which could be in the future one of the criteria of GPeC for establishing the best in domain.

We present the results of a recent vulnerability exposure assessment conducted for 22 different organizations. During the study it was done a small survey regarding vulnerability management solutions. The results show the most vulnerable system types, service families and network ports. Limits of the survey were: no interview with IT responsible was done and indicators are only an image, for trends a new survey will be need it. Key findings:

- High-risk vulnerabilities make up **21.5%** of the total number of identified vulnerabilities;
- **14%** of hosts managed not to have high-risks, however all organizations suffered of risks;
- Most vulnerabilities related to the CVE1 belongs to 2009, and the oldest were from 1999-2002;
- **Average risk according to CVSS2 score was 5.6** .

3.1 Analysis

The following analysis is based on the assessment of 2035 vulnerabilities on 30 hosts in 22 different e-commerce organizations. To protect the identity of the participating organizations each has a hypothetic ID. The purpose of the analysis is not to provide statistical proof for particular claims but to learn from examples to help better protect all organizations assets.

The results are presented bellow:

a). Vulnerability services

HTTP, DNS and SSH are the most vulnerable services identified, followed by POP3, IMAP, SMTP (Figure2).

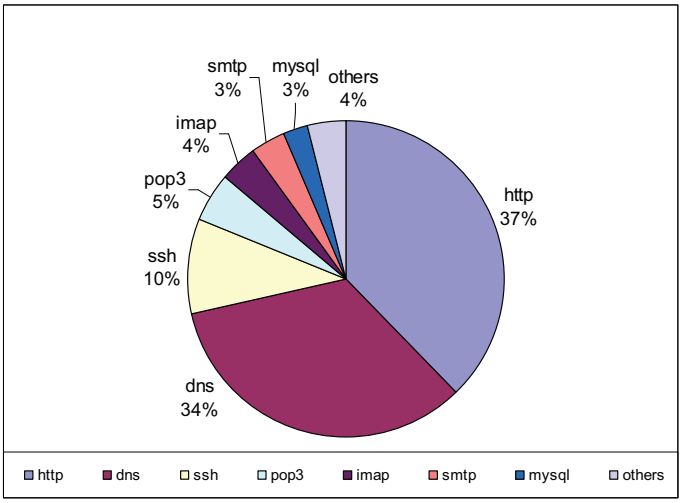


Figure 2. The most vulnerable services identified in study

b). Vulnerability families

PHP vulnerabilities were overall the most common, followed by those related to SSH and SSL. Also for CVSS score >7 PHP is in top (Vulnerabilities with a CVSS score of 7 or more are considered „high-risk“. Below 7 is medium, below 4 is low).

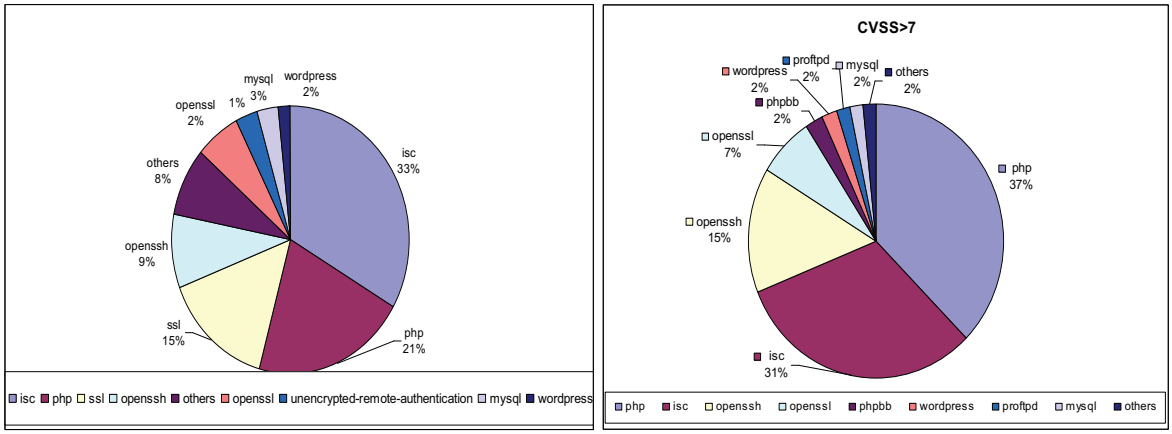
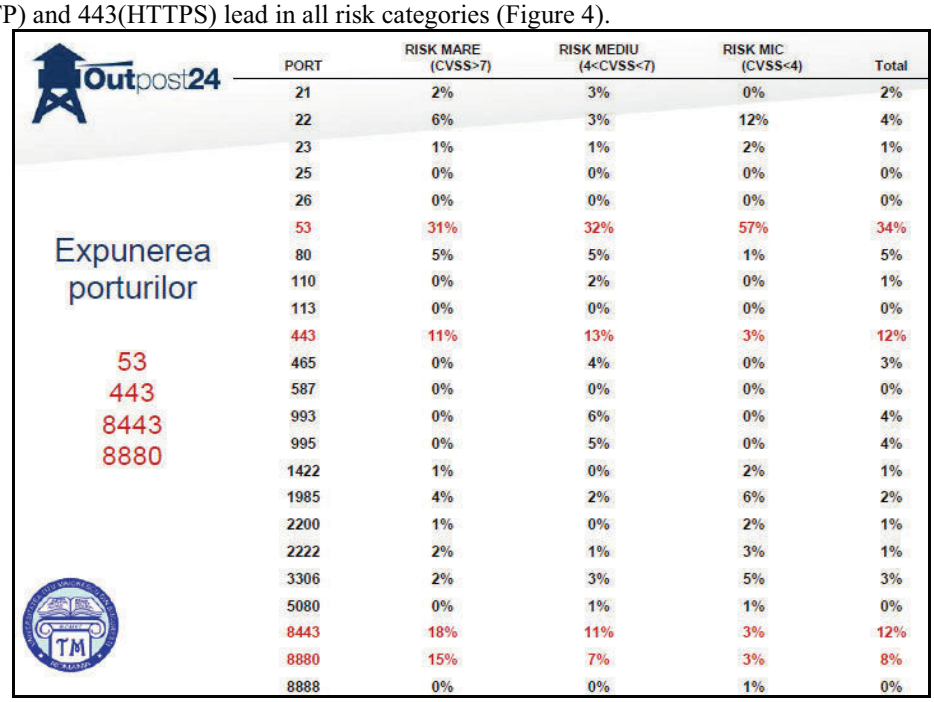


Figure 3. The most vulnerable families identified in study

Most vulnerable ports by share of found vulnerabilities with high, medium or low risk. The common web ports 80 (HTTP) and 443(HTTPS) lead in all risk categories (Figure 4).



PORT	RISK MARE (CVSS>7)	RISK MEDIU (4<CVSS<7)	RISK MIC (CVSS<4)	Total
21	2%	3%	0%	2%
22	6%	3%	12%	4%
23	1%	1%	2%	1%
25	0%	0%	0%	0%
26	0%	0%	0%	0%
53	31%	32%	57%	34%
80	5%	5%	1%	5%
110	0%	2%	0%	1%
113	0%	0%	0%	0%
443	11%	13%	3%	12%
465	0%	4%	0%	3%
587	0%	0%	0%	0%
993	0%	6%	0%	4%
995	0%	5%	0%	4%
1422	1%	0%	2%	1%
1985	4%	2%	6%	2%
2200	1%	0%	2%	1%
2222	2%	1%	3%	1%
3306	2%	3%	5%	3%
5080	0%	1%	1%	0%
8443	18%	11%	3%	12%
8880	15%	7%	3%	8%
8888	0%	0%	1%	0%

Figure 4. Example of port exposure detected

c). Risk level of organizations

All analyzed organizations suffered of vulnerabilities (Figure 5).

However 14% managed not to have high risk vulnerabilities. 20% of the organizations are using a vulnerability management solution and 47% took in consideration implementation of ISO 27001 standard - ISMS (Information Security Management System) in the next period. The average severity score across all identified vulnerabilities was 5.6.

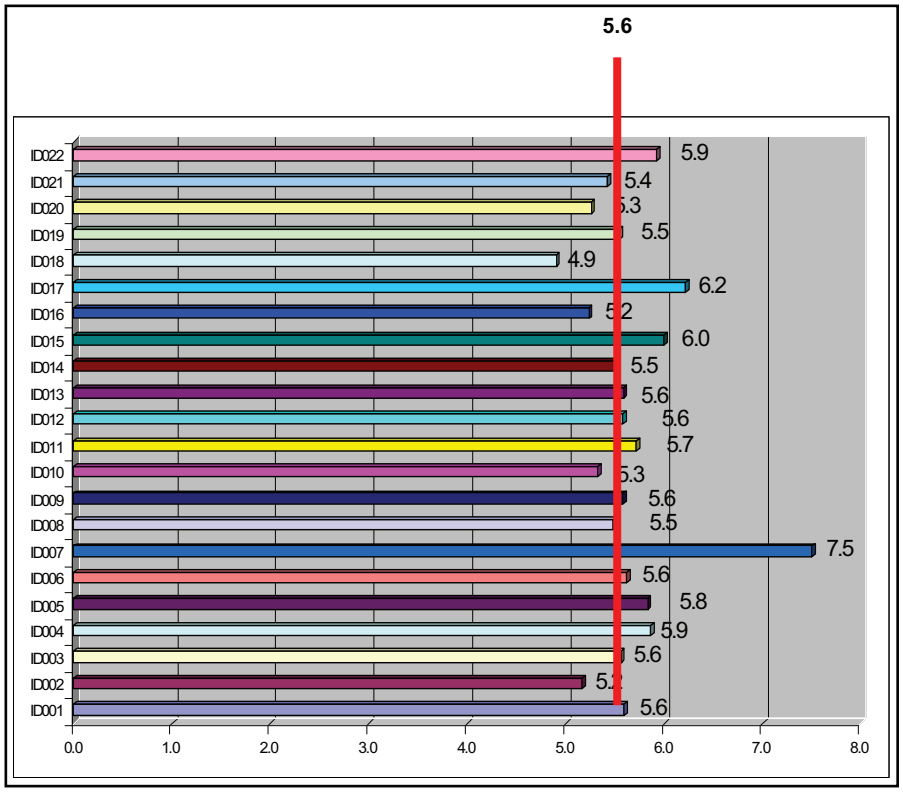


Figure 5. The risk level of organizations

3.2 Recommandation

Among the participating Romanian e-commerce companies in this study, many showed a low level of vulnerability exposure and demonstrated that high-risk vulnerabilities are not inevitable. Based on their success, we suggest the following actions to be taken by organization managers and network administrators:

- Many of the found vulnerabilities had been publicly known for a long time. Establish an organizational process to find and react on new vulnerabilities in a timely manner;
- All of the vulnerabilities identified in this study were found using automated vulnerability scanning tools that are publicly available. Administrators should make increasing use of the automated tools in order to be able to reduce their workload and conduct evaluations more frequently;
- As organizations change so do their IT systems and their exposure to vulnerabilities. The more dynamic a network or a system becomes, the more frequent vulnerability exposure assessments should be carried out.

4. CONCLUSIONS

E-commerce companies are forced to continuously maintain the protection of their networks. Traditionally, this has been accomplished by creating barriers against attacks by investing in reactive security tools such as firewalls, anti-virus tools and intrusion detection systems. In today's environment these reactive mechanisms simply are not enough.

Instead of waiting for attacks to occur, there is a need to take a proactive approach. Only by using proactive security tools that continuously identify security risks, it is possible to effectively manage and reduce the risk exposure. Outpost24 offers leading solutions within the following fields:

- Vulnerability Management - Proactively identify, manage and eliminate the security risks that make attacks against networks possible
- PCI Compliance - Verify and prove that the handling of credit card data is in compliance with the PCI Data Security Standard.

Conclusions of the survey done by Outpost24 Romania together with Titu Maiorescu University are:

- E-commerce companies in Romania should put a greater emphasis on information security issues;
- Increase the security culture in the e-commerce companies in Romania could make a difference in results;
- Vulnerability, security, risks and incidents are management problems, not only for the IT specialists.

All of the vulnerabilities identified in this study were found using automated vulnerability scanning tools (OUTSCAN) that are publicly available. Administrators should make increasing use of the automated tools in order to be able to reduce their workload and conduct evaluations more frequently.

REFERENCES:

[1] GPeC, http://www.gpec.ro/ro/conferintele-gpec-2010, 2010
[2] OUTPOST24, Vulnerability Management, O24_TKK_Network_Study, www.outpost24.com, 2010
[3] Peter Mell, Karen Scarfone, Sasha Romanosky, A Complete Guide to the Common Vulnerability Scoring System Version 2.0, http://www.first.org/cvss/cvss-guide.html, 2008
[4] Peter Mell, Tiffany Bergeron, David Henning, Creating a Patch and Vulnerability Management Program, Special Publication 800-40 v.2.0, NIST, 2005
[5] Priescu Iustin, Patriciu Victor-Valeriu, Sebastian Nicolaescu – The Viewpoint of E-Commerce Security in the Digital Economy, International Conference on Future Computer and Communication Kuala Lumpur, Malaysia, IEEE Computer Society, ISBN 978-1-4244-3754-2, 2009.
[6] Priescu Iustin, Patriciu Victor-Valeriu, Nicolaescu Sebastian, Ionescu Razvan, Current Perspectives on Information Security Management Systems, Communication'08, Vol II, IEEE Conference, Bucharest, 2008.
[7] SANS.org, Critical Controls as Applied to HTTP Server Threats, http://www.sans.org/top-cyber-security-risks, 2009