STUDIA INFORMATICA
Nr 1-2 (24) Systems and information technology 2020

Tomasz MULIŃSKI[1]

[1] Chamber of Tax Administration in Lublin
ul. Tadeusza Szeligowskiego 24, 20-883 Lublin, Poland

ICT security in tax administration - Rapid7 Nexpose vulnerability analysis

DOI: 10.34739/si.2020.24.03

Abstract. The article focuses on the subject of IT security in tax administration. This study presents the research on the security level of endpoints, servers, printing devices, network switches and other ICT devices using the Rapid Nexpose vulnerability scanner. We discuss the specifics of security research in public administration resulting from the laws in force in these institutions.

Keywords. ICT security, Vulnerability scanning tool, Tax Administration, Rapid7 Nexpose, Computer network, Vulnerability tests

1. Introduction

This article is the first in a series of articles discussing the issues of ICT security in the tax administration in Poland. The complexity of the protection of ICT systems in public administration in Poland results from the sources of threats, technical methods of system protection as well as from the provisions of EU and state law, as well as the rules and procedures established in public administration units [8]. Subsequent articles will discuss the various elements of building the ICT system protection system in the tax administration.

The specificity of the functioning of public administration services is the obligation to act on the basis of legal provisions and within the framework of existing regulations. This undoubtedly significantly facilitates the construction of the ICT security protection system. Based on regulations and procedures, it is possible to use solutions, standards and good practices developed for the administration, codified into legal provisions, created for public administrations [17]. There are a few of them that shape the security of ICT systems and the data processed in them:

- Act of 5 July 2018 on the national cybersecurity system [3],
- Act of 10 May 2018 on the protection of personal data [2],
- Act of 17 February 2005 on computerization of the activities of entities performing public tasks [1],
- Regulation of the Prime Minister of 20 July 2011 on the basic requirements of ICT security [13],
- The announcement of the Prime Minister of 9 November 2017 on the publication of the uniform text of the regulation of the Council of Ministers on the National Interoperability Framework [6],
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [14],

There is no definition of cybercrime in Polish criminal law [16], but there are penalized acts related to: illegal access to information (Article 267), destruction of information (Article 268), causing damage to IT data (Article 268a), sabotage computer (Article 287) or disrupting the operation of the ICT system (Article 269). Investigating the vulnerability of an ICT system requires the use of various methods in order to understand the security level. Article 269c of the Criminal Code allows for the legal use of various types of penetration tests, however, it is subject to a number of restrictions that must be met in order to avoid being subject to the above-mentioned provisions.

Preparing the test method and environment, taking into account the fact that they take place on the production network, was a big challenge. The encountered problems and the variety of tested devices made it difficult to find the appropriate settings of the scanned computers and servers so that the Nexpose scanner was fully authenticated, enabling accurate obtaining of information about vulnerabilities. How important this is was shown by the comparison of tests from December 2018 and March 2019, when the problems with full authentication reduced the number of detected vulnerabilities 22 times.

The use of the white box method to test vulnerabilities in the ICT system seems to be a good solution. The choice of the Rapid7 Nexpose tool for the test implementation allowed for the collection of a large amount of information on vulnerabilities on devices located in the analysed ICT subnets. In relation to the black box method, in which the main goal is to break security and achieve the set goal, the use of the Nexpose tool allows not only to automatically identify system vulnerabilities, but also allows you to obtain ready-made reports containing methods of removing the detected vulnerabilities. An additional functionality is the possibility of re-running the tests after fixing the detected gaps.

2. Penetration tests

The use of penetration tests is a form of practical verification of the security level of ICT systems [15]. In the scientific literature, it is postulated that such research should be carried out by external companies having appropriate human resources and software to verify the security level of ICT systems. There are three methods of conducting penetration testing [7, 11, 18]:

- black-box test,
- white-box test,
- grey-box test,

Black-box testing based on the assumption tester lack of knowledge about the system under study. Such a scenario may be, for example, the tester obtaining the website with the IP address that should be attacked in the same way as a malicious attacker does by breaking the encountered security. During the tests, the person conducting the tests does not know the technical and organizational solutions ensuring security in the organization. Therefore, using hacking tools, it carries out subsequent stages of tests aimed at learning about the weaknesses of system protection. Breaking security or using vulnerabilities enables the achievement of the set goal, including the development of conclusions, guidelines for the implementation of security measures that eliminate gaps in the security system. These methods are expensive and time-consuming in relation to the other two types of tests [7].

The opposite of black box testing is the white box method. The tester has full knowledge of the ICT system, network structure and topology, and the application operating systems used. This solution has some disadvantages related to the fact that it does not reflect a real hacker attack in which knowledge about the structure and security is obtained by using appropriate techniques. The advantage of this method is the high accuracy of the results and the results achieved present the possibility of the most malicious attack materializing. The tests enable not only a complete diagnosis of the system security, but also a significant increase in the level of security with relatively little effort [15].

The last method used is the grey box test, which uses partial assumptions from the two previously discussed methods. The tester receives some information about the analysed system (names of test accounts, IP backend servers, etc.), but does not have full knowledge of the operating services, network topology. It is also allowed to conduct tests from within the network, simulating cases of employee attack from within the organization. Like the black box method, it is quite time consuming in the case of a fairly well secured system. However, it allows you to reflect a real hacker attack.

There are many divisions of test methodologies, some are based on differentiation according to the elements of the ICT system [7], others focus on the organizations creating test methodologies [15]. Due to the complexity of the problem and the limited volume of the article, it will not be discussed in more detail.

Finally, the ethical side of conducting penetration testing should be mentioned. The authors in their publications, presenting methodologies and detailed techniques, draw attention to the fact that the use of knowledge should be used to detect and protect ICT systems. Tests must take place with the knowledge and consent of the system owners in order not to be exposed to criminal charges in a given country.

To meet the expectations of the International Council of Electronic Commerce Consultants (EC-Council), for ten years she has been conducting training and certification of skills described as Certified Ethical Hacker. The training is guided by the idea of educating "ethical hackers" who will have the skills to identify weak elements of the ICT system and find effective methods of defence against cyber-attacks [9, 10].

3. Rapid7 Nexpose vulnerability scan

3.1. Tool description

Vulnerability management is a key element of the organization's IT systems security. ICT infrastructure that does not have tools to identify vulnerabilities is more exposed to security breaches. The Rapid7 company was founded in 2000 in New York and from the very beginning has been creating ICT security systems. The company is recognized as the most technologically advanced manufacturer offering solutions for the analysis and detection of vulnerabilities in ICT systems. The company's products enable the automation of the entire vulnerability management cycle [5].

The Rapid7 Nexpose product is used to search for and manage vulnerabilities, and reduce the likelihood of successful cyber-attacks on the organization's ICT systems. Detailed audit reports, it enables the assessment and response to detected system vulnerabilities. The Rapid7

Nexpose has a number of functionalities ensuring vulnerability lifecycle management, including:

- dynamic discovery of resources in the network using the Discovery and Connection Discovery functions,
- possibility of static and dynamic grouping of detected resources using system-defined tags or user-defined tags,
- performing a vulnerability assessment based on CVSS v2 and intelligent risk assessment based on real risk and context-driven mechanisms,
- extensive functionality to remove vulnerabilities,
- extensive reporting on detected vulnerabilities and how to remove them,

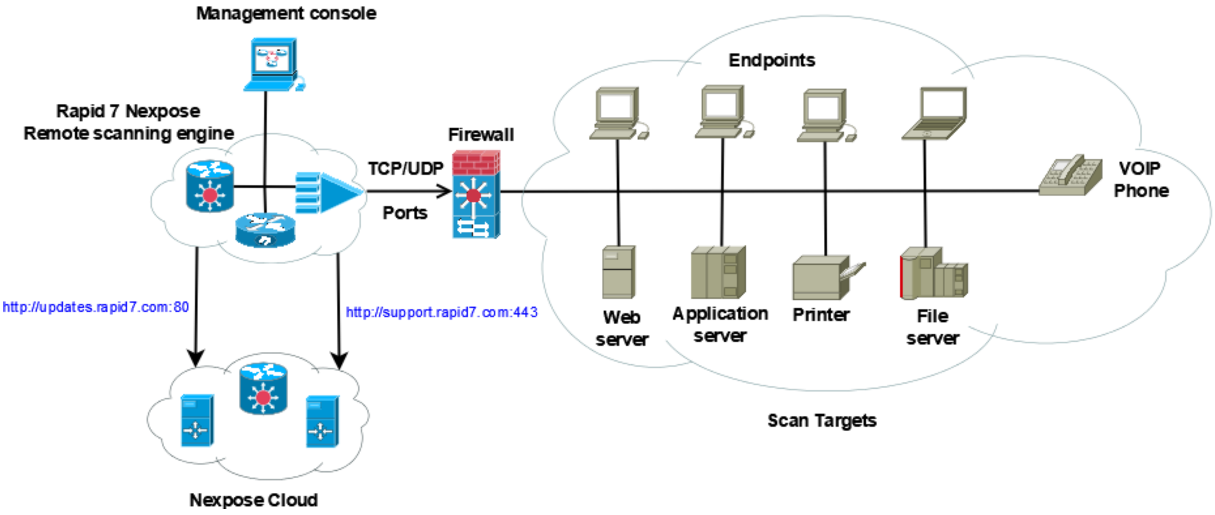

Figure 1. Rapid7 Nexpose architecture used in research
Source: own study

Due to the extensive structure in the analysed organization, the Rapid7 Nexpose Enterprise scanner used four remote scanning engines managed from a remote web console. The Figure 1 shows schematically the Rapid7 Nexpose architecture used in the study.

3.2. Preparation of research methodology using Rapid7 Nexpose

In preparation for the research, two paths of vulnerability testing using Rapid7 Nexpose were developed. In the first approach, it was assumed that Nexpose will access scanned resources using local service accounts for selected systems. By default, service accounts were assigned the privileges of a regular user, but in a few cases, for the purposes of testing, the privileges were raised to the administrator level. After the on-demand scan of the account authentication service resources have been removed. As part of the selection of scanned resources, 22 resources were selected from the proposed 74 computers and servers, on which

18 accounts with ordinary user rights were created and on 4 resources the rights to the administrator level were raised. Various operating systems used in the organization were selected to obtain a complete overview of the security status. The Table 1 presents the list of tested operating systems.

The first method of Nexpose vulnerability scanning showed numerous problems while scanning with resource authentication. The access problem also occurred on the assets on which administrative accounts were created, which indicated problems on the side of devices filtering network traffic. Vulnerability management with the use of service accounts was abandoned due to the need to maintain the rules for changing passwords, the possibility of moving equipment. The focus was on looking for configuration solutions for scanned assets in order to obtain Nexpose authentication on end points allowing for vulnerability testing. The tests took place from July to October 2017.

Table 1. List of tested operating systems. Source: own study

The name and version of the operating system	Number of scanned assets
Microsoft Windows 7 Professional	8
Microsoft Windows 8 Professional	2
Microsoft Windows 8.1 Professional	6
Microsoft Windows XP Home Edition	1
Windows Server 2008 R2	2
Windows Server 2012 R2 Standard	2
Windows Server 2016	1

The second method focuses on finding the optimal network traffic settings to achieve full endpoint authentication without the need to create service accounts. This solution allows for safer and easier testing with the Nexpose scanner. During the tests, a larger number of tested devices was used, adopting a different scanning method i.e., selecting entire networks with all devices instead of selected endpoints. The adoption of this method made it possible to scan almost 500 devices during one scan, which significantly contributed to obtaining more complete results and to understanding the security status of the computer network. The tests were conducted from October 2018 to May 2019.

3.3. Configuration of scanned endpoints

The information on endpoint settings obtained from generally available sources for the vulnerability scanning with Rapid Nexpose indicated:

- the need to unblock traffic on ports 135, 139, 445 in the system firewall (or other e.g., AV, routers) for traffic coming from Nexpose scanners,
- create a registry entry for the DWORD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy key with a value of 1,
- starting the Remote Registry service on endpoints,

Rapid Nexpose tests carried out on selected computers showed the occurrence of problems with determining the correct settings on the endpoints, which would enable full authentication of the scanner on the analysed computer. Computers used for tests belonged to the single domain, the first tested group of computers belonged to one subnet, which facilitated the management of settings during the research. As part of the tests, inconsistent results were obtained, which manifested in the fact that the scanner was properly authenticating on the computer in the initial tests, but not authenticating after two days. The causes of this condition have been tested on two computers. It turned out that the problem is caused by the existence of more than one network interface - in the first case, Wi-Fi was enabled (Win 10), in the second case, the network interface with Virtual Box (Win 7) was enabled. After disabling these interfaces, full authentication took place, but due to the need to determine whether the firewall was also the cause, it was reset in the tested Windows 10 system. This action caused the scanner could not authenticate the computer with Windows 10. The tests focused on finding the cause. It turned out that after resetting the firewall settings, ICMPv4 traffic was disabled by default, after enabling the ICMP protocol Nexpose began to authenticate on endpoints. In addition, the Wi-Fi and VirtualBox interfaces were enabled, which did not contribute to the deterioration of the conditions for the scanner, which was partially authentic on the Windows 7 Professional system and the authentication error occurred in Windows 10 Professional. The search focused on other protocols. Only unblocking the firewall traffic on ports 500-60000 allowed for full authentications on Windows 7 and Windows 10. Using the method of half-division of the tested pool, an additional port number 50192 was found, the unblocking of which allows for full authentication of the computers that were used in the tests. The Table 2 shows the cumulative results of research tests.

Table 2. List of tested TCP ports. Result: X - Credential Failure, V - Credential Success, O - No Credential Used. Restrictions: T - Nexpose ports only, N - All remote ports. Remote Registry Service: T – On, N – Off. Source: own study.

Protocol	Ports	Restrictions	Remote Registry	Result
Any	Any	N	T	V
TCP, UPD, IPV6	Any	N	T	O
TCP, UPD, ICMPv4	Any	N	T	V
TCP ICMPv4	135,139,455 Any	N	T	X

TCP ICMPv4	135,139,455, 500-60000 Any	N	T	V
TCP ICMPv4	135,139,455,500-60000 Any	T N	T	V
TCP ICMPv4	135,139,455,500-60000 Any	T T	T	V
TCP ICMPv4	135,139,455,500-10000 Any	T T	T	X
TCP ICMPv4	135,139,455,500-40000 Any	T T	T	X
TCP ICMPv4	135,139,455, 500-600, 40000-60000 Any	T T	T	O
TCP ICMPv4	135,139,455, 500-600, 50000-60000 Any	T T	T	O
TCP ICMPv4	135,139,455, 593, 50000-60000 Any	T T	T	O
TCP ICMPv4	135,139,455, 593, 50000-60000 Any	T T	N	O
TCP ICMPv4	135,139,455, 50000-60000 Any	T T	N	O
TCP ICMPv4	135,139,455, 55000-60000 Any	T T	N	X
TCP ICMPv4	135,139,455, 52000-60000 Any	T T	N	X
TCP ICMPv4	135,139,455, 50000-55000 Any	T T	N	O
TCP ICMPv4	135,139,455, 50000-52000 Any	T T	N	O
TCP ICMPv4	135,139,455, 51000-52000 Any	T T	N	X
TCP ICMPv4	135,139,455, 50000-51000 Any	T T	N	O
TCP ICMPv4	135,139,455, 50000-50500 Any	T T	N	O
TCP ICMPv4	135,139,455, 50000-50200 Any	T T	N	O
TCP ICMPv4	135,139,455, 50000-50100 Any	T T	N	X
TCP ICMPv4	135,139,455, 50100-50200 Any	T T	N	O
TCP ICMPv4	135,139,455, 50150-50200 Any	T T	N	O
TCP ICMPv4	135,139,455, 50170-50200 Any	T T	N	O
TCP ICMPv4	135,139,455, 50190-50200 Any	T T	N	O
TCP ICMPv4	135,139,455, 50196-50200 Any	T T	N	X
TCP ICMPv4	135,139,455, 50192-50195 Any	T T	N	O
TCP ICMPv4	135,139,455, 50192-50193 Any	T T	N	O
TCP ICMPv4	135,139,455, 50192 Any	T T	N	O
TCP ICMPv4	135,139,455, 50193 Any	T T	N	X

The tested devices were configured using domain policies. Detailed studies on the effects of these settings were first tested on a desktop computer and a notebook on which manually configuring a firewall operating system. In further research, tests were also carried out on a larger group of workstations and servers from a different subnetwork. Entries unlocking TCP protocols on selected ports and ICMPv4 were set with domain policies on computers and servers, which allowed the scanner only for partial authentication on the tested devices. Due to the previously identified unpredictable behaviour of Nexpose, a never-scanned workstation was tested. The test performed for the first time was successful, full authentication was performed and the vulnerability was detected. Subsequent scans were then performed during which the scanner did not recognize this station. The tests took about 8 minutes and there were no configuration changes on the scanned station (switching on the firewall, traffic blocking programs). The station received a policy which ensured opening ports 135, 139, 445 and 50192. The same scanning method was used in all scans, Full audit without Web Spider. The Table 3 shows the subsequent scans and that they were performed by the same scanner engine number 873 and the exact time of the scans performed.

Table 3. Information about single station scanning with Rapid7 Nexpose. Source: own study

Address	Name	Operating System	Site	Vulnerabilities	Total Elapsed Scan Time	Scan Engine	Date	Type
10...224	b…1.mf.gov.pl	Linksys Linux 1.28	LB,Workstations,Auth	1	1 minute	SAP-WIN-873	15.11.2018, 2:24 PM	SCAN
10...224	b…1.mf.gov.pl	Linksys Linux 1.28	LB,Workstations,Auth	1	1 minute	SAP-WIN-873	15.11.2018, 2:22 PM	SCAN
10…224	b…1.mf.gov.pl	Microsoft Windows 10 Professional Edition	LB,Workstations,Auth	1086	9 minutes	SAP-WIN-873	15.11.2018, 2:16PM	SCAN

The purpose of finding the minimum requirements for passing network traffic through the firewall was to ensure the security of assets during the scan by limiting the number of open ports. During the study, the degree of workload of the stations was also verified during the scan using the Task Manager, there was no visible load on the workstations manifested by a significant increase in the load on the processor, memory, disk and network card. Subsequent tests were carried out on the notebook on which the vulnerability was previously searched for. This solution made it possible to discover the need to unblock a port other than 50192. During the tests, Nexpose stopped authenticating even though the firewall settings did not change. At that time, only updates to Office 2016 were installed, after which a preventive restart was performed before testing. Once again, the high port search method was used to unlock authentication. During the tests, it turned out that opening port 50216 allowed for full authentication of the Nexpose scanner. Thus, it seems that it was reasonable to open up traffic to a larger range of ports, which would enable authentication on a "floating TCP port" in the range of 50000-59999.

3.4. Endpoint vulnerability testing

Vulnerability tests were conducted from October 2018 to May 2019. During the tests, the number of scanned assets was increased. In December tests, it was possible to scan the largest number of endpoints with the highest number of vulnerabilities. After the implementation of the new antivirus system, the system firewall was integrated with the newly introduced solution. Due to this situation, Nexpose did not achieve full authentication on any device during the next tests, which resulted in almost twenty-two times lower vulnerability detection. The list of tests performed, the number of scanned devices and detected vulnerabilities is shown in the Table 4. The highlights the lines with tests that have been subjected to a more detailed analysis.

A detailed analysis of the vulnerability distribution of the scans carried out showed that the installation of a new antivirus system on Microsoft operating systems resulted in the fact that the Nexpose scanner was not authenticated on any of the endpoints. Logs on the AV console confirmed the blocking of network traffic and contained alerts about the attempts to scan. The Table 5 compares the results of assets scans from the same subnetwork at two dates. However, it should be noted that the scans were carried out in the production network, therefore there are noticeable differences in the number of scanned devices.

Table 4. The list of tests scanner Rapid Nexpose.Source: own study.

Started	Assets	Vulnerabilities	Total Elapsed Scan Time	Scan Engine
17.10.2018	93	504	31 minutes 41 seconds	4 Scan Engines
19.10.2018	82	438	35 minutes 12 seconds	4 Scan Engines
22.10.2018	101	550	46 minutes 26 seconds	4 Scan Engines
30.10.2018	95	1 287	40 minutes 10 seconds	4 Scan Engines
05.11.2018	93	566	46 minutes 24 seconds	4 Scan Engines
22.11.2018	357	7 418	2 hours 6 minutes 8 seconds	4 Scan Engines
29.11.2018	322	49 425	1 hour 44 minutes 46 seconds	4 Scan Engines
04.12.2018	390	155 445	2 hours 57 minutes 38 seconds	4 Scan Engines
10.12.2018	387	151 969	3 hours 9 seconds	4 Scan Engines
19.12.2018	372	149 736	2 hours 33 minutes 24 seconds	4 Scan Engines
28.03.2019	421	6 859	2 hours 11 minutes 43 seconds	4 Scan Engines
09.05.2019	179	2 051	1 hour 3 minutes 26 seconds	4 Scan Engines

The number of full authentications affects the detection of vulnerabilities occurring on the tested devices, which allows taking actions to correct the system configuration or eliminate the detected threats. Due to the fact that many utility programs are installed on the workstations, hence a much greater number of detected vulnerabilities than on servers. The Table 6 shows the breakdown of vulnerabilities by operating systems and devices.

Table 5. The number of credentials scanner Rapid Nexpose. Source: own study.

	Credential Success		**Partial Credential Success**		**No Credential Supplied**		**Credential Failure**		**Unknown**	
Date of scan **Operating system/ Asset name**	19.12. 2018	28.03. 2019	19.12. 2018	28.03. 2019	19.12. 2018	28.03. 2019	19.12. 2018	28.03. 2019	19.12. 2018	28.03. 2019
Microsoft Windows - unidentified version	0	0	0	0	0	0	2	3	2	3
Microsoft Windows 7	17	0	12	0	0	0	0	55	0	0
Microsoft Windows 8	0	0	6	0	0	0	0	36	0	0
Microsoft Windows 8.1	52	0	67	0	0	0	0	7	0	0
Microsoft Windows 10	45	0	24	0	0	0	0	133	0	0
Microsoft Windows Server 2003 SE SP2	0	0	1	0	0	0	6	7	0	0
Microsoft Windows Server 2008 SE SP2	0	0	4	0	0	0	1	4	0	0
Microsoft Windows Server 2012 R2 SE	0	0	10	0	0	0	0	11	0	0
Microsoft Windows Storage Server 2012 R2	1	0	1	0	0	0	0	0	0	0
Linux/Other systems	0	0	2	2	14	13	1	2	1	2
Printers	0	0	2	0	73	71	0	0	8	8
Other devices	0	0	1	27	9	9	2	1	1	4

The Nexpose scanner classifies vulnerabilities into three types, determining their impact on security weakness: Critical, Moderate, Severe. The most common vulnerabilities were identified: Critical, Severe at around 3300, while Moderate vulnerabilities are eight times less - 400. The Table 7 presents a list of the detected vulnerabilities due to their type and number of occurrences of the analysed assets.

Vulnerability analysis shows that the largest number of identified vulnerabilities concerns operating systems of Microsoft, which is understandable, as the largest number of endpoints are computers and servers equipped with this manufacturer's system. Other vulnerabilities are those related to Adobe products, which is understandable due to a number of publications on the huge number of vulnerabilities and resulting in the retirement of Adobe Flash at the end of 2020 [4]. Adobe products are also often used in public administration, which resulted in a huge number of detected vulnerabilities. A similar situation occurs with Java, which has been characterized by a large number of vulnerabilities for many years, which also resulted in a large number of detected vulnerabilities, amounting to over 10000. The Table 8 lists the vulnerabilities that occurred in the greatest number during the tests.

Table 6. The number of vulnerabilities identified by scanner Rapid Nexpose. Source: own study.

	Number vulnerabilities on operating systems		**Number scanned operating systems /devices**		**Number Vulnerabilities per operating system/device**	
Date of scan **Operating system/ Asset name**	19.12.2018	28.03.2019	19.12.2018	28.03.2019	19.12.2018	28.03.2019
Microsoft Windows - unidentified version	19	42	4	6	4	7
Microsoft Windows 7	23 688	486	29	36	816	13
Microsoft Windows 8	4 503	118	6	7	750	16
Microsoft Windows 8.1	84 748	2 203	119	133	712	16
Microsoft Windows 10	30 117	761	69	55	436	13
Microsoft Windows Server 2003, SE SP2	650	389	7	7	92	55
Microsoft Windows Server 2008 SE SP2	78	59	5	4	15	14
Microsoft Windows Server 2012 R2 SE	1 012	304	10	11	101	27
Microsoft Windows Storage Server 2012 R2	2 755	0	2	0	1 377	0
Linux/Other systems	836	864	17	17	49	50
Printers	1 252	1 177	83	81	15	14
Other devices	78	456	15	40	5	11

Table 7. Types vulnerabilities classified by scanner Rapid Nexpose. Source: own study

Vulnerability type	**Number of occurrences**	
	per vulnerability type	**on devices**
Critical	3 297	53 590
Moderate	402	9 349
Severe	3 384	47 112

The Nexpose scanner, in addition to detecting known vulnerabilities, verifies for example whether there are accounts in the systems that do not have a set password or use standard passwords, whether access from the guest account is enabled, etc. Individual cases caught during tests were forwarded to system administrators for their elimination. During the tests, there were also vulnerabilities related to encryption and the configuration of encryption protocols, but their number was not significant, therefore they were not included in the above list.

In addition, after the end of the tests on the group of assets, the Rapid Nexpose functionality was used, which enables the determination of risks for the tested devices with an unchanged number of vulnerabilities detected in the last scanning in 2019. The risk assessment presented in the Figure 2 below shows that the degree of risk to the security of a computer system increases over time.

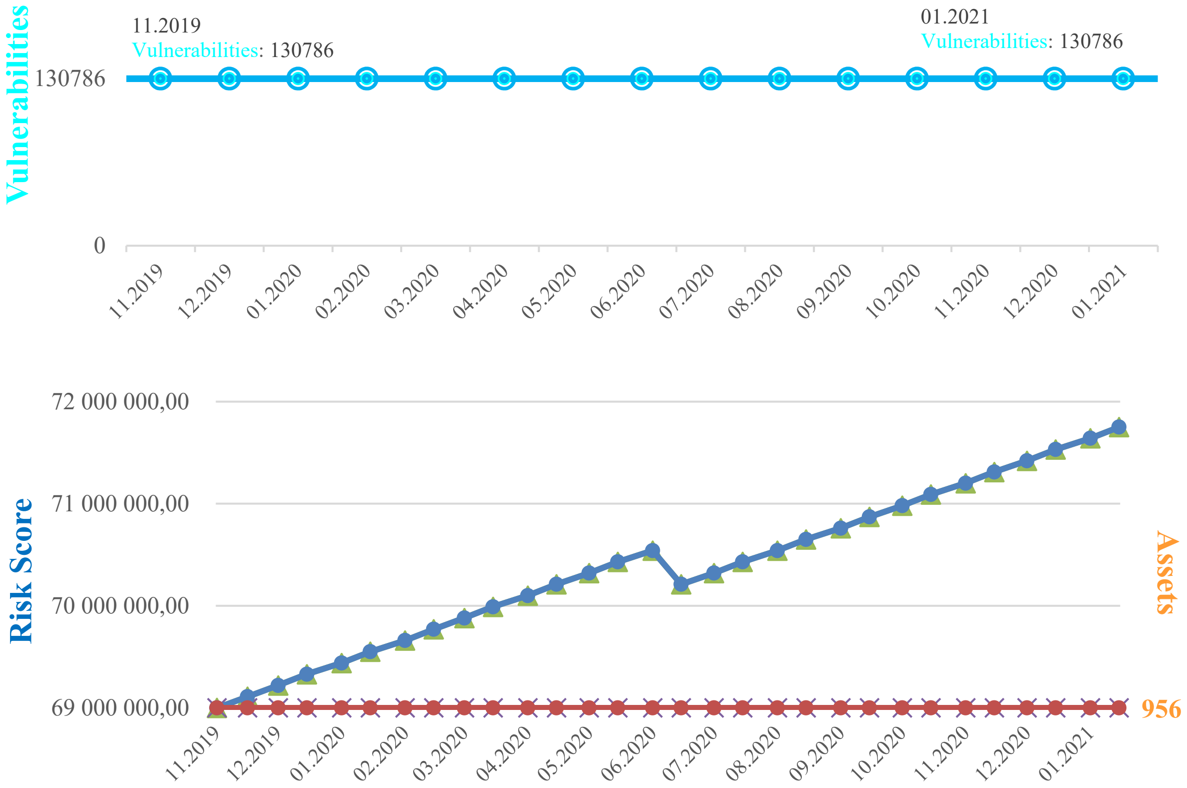

Figure 2. Change in the degree of threats to computer systems within one year. Source: own study.

Table 8. Types vulnerabilities classified by scanner Rapid Nexpose. Source: own study.

Software Manufacturer	Number of Vulnerabilities	Number Vulnerabilities on devices			
		Critical	Moderate	Severe	Total
Adobe Reader	923	14 536	0	5 191	19 727
Adobe Flash Player	917	21 434	0	1 416	22 850
CISCO	32	76	6	24	106
Debian	542	95	39	424	558
Java	239	789	993	8 735	10 517
Thunderbird	366	737	13	701	1451
Firefox	292	1 606	69	3 195	4 870
Microsoft	1 251	5 293	2 312	5 395	13 000
Oracle	447	76	99	997	1 172
PHP	498	2 302	100	3 098	5 500
VMware	100	248	96	1276	1 620

4. Summary

About 1000 devices were scanned in the tests: computers, servers, printers, network switches, UTM. The variety of devices and their number have shown that computers with Microsoft operating systems intended for personal computers are most at risk. Half of the detected vulnerabilities were of a critical nature, which may raise concerns about the security of ICT systems. These problems are partially mitigated by the security structure, as the devices are located in an intranet network protected at the interface with the internet by an extensive security system. Detected threats in popular applications used in office work also constitute a significant percentage of detected vulnerabilities.

The tests were also of a practical nature, based on the results obtained, a number of corrective actions were introduced, which contributed to the reduction of the number of vulnerabilities by updating operating systems and software. The specificity of some tasks performed by the tax administration requires leaving some solutions and applications despite their vulnerabilities. Therefore, the protection of assets was based on a new antivirus system, which limited the risk of using vulnerabilities for programs that could not be removed due to business needs.

How important the elimination of vulnerabilities is shown in the risk assessment presented in Figure 2. Over time, unremoved vulnerabilities from the system are becoming more and more dangerous due to the fact that newer versions of malware are able to use an increasing number of vulnerabilities in the software. Therefore, it is important to remove the identified threats or use software or hardware solutions that minimize the use of vulnerabilities.

References

1. Act of 17 February 2005 on computerization of the activities of entities performing public tasks, Journal of Laws 2005, no. 64, item 565, with changes.
2. Act of 10 May 2018 on the protection of personal data, Journal of Laws 2018, item 1000, with changes.
3. Act of 5 July 2018 on the national cybersecurity system, Journal of Laws 2018, item 1560, with changes.
4. Adobe Flash Player EOL General Information Page, Adobe, https://www.adobe.com /pl/products/flashplayer/end-of-life.html, Accessed 20 Dec. 2020.
5. Advance Security With Us, Rapid7, https://www.rapid7.com/, Accessed 20 Dec. 2020.
6. Announcement of the Prime Minister of 9 November 2017 on the announcement of the consolidated text of the Regulation of the Council of Ministers on the National Interoperability Framework, minimum requirements for public registers and electronic

information exchange, and minimum requirements for ICT systems, Journal of Laws 2017, Item 2247.

7. Baloch R., Ethical Hacking and Penetration Testing Guide. CRC Press, Boca Raton, 2015.

8. Barczak A., Sydoruk T, Barrier to computerization of management systems - Myths or reality?, Studia Informatica Systems and information technology, no 1-2(15) , UPH, Siedlce, 2011.

9. Certified Ethical Hacker, Altkom Akademia, https://www.altkomakademia.pl /szkolenia/certified-ethical-hacker-11/, Accessed 20 Dec. 2020.

10. Certified Ethical Hacker CEH, EC-Council, https://www.eccouncil.org /programs/certified-ethical-hacker-ceh/. Accessed 20 Dec. 2020.

11. Graves K., CEH – Certified Ethical Hacker – Study Guide. Wiley Publishing Inc, Indianapolis, 2010.

12. Rapid7 Nexpose Product brief, Rapid7, https://www.rapid7.com/globalassets/_pdfs /product-and-service-briefs/rapid7-nexpose-product-brief.pdf, Accessed 20 Dec. 2020.

13. Regulation of the Prime Minister of 20 July 2011 on the basic requirements for ICT security, Journal of Laws 2011, no. 159, item 948.

14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1.

15. Suski Z., Reconnaissance passive in penetration tests, Teleinformatics Review vol. 3, 2017.

16. The Act of June 6, 1997, Penal Code, Journal of Laws 1997, no. 88, item 553, with changes.

17. Warmiński A., Aspects of functioning of public administration, Doctrina. Socio-political Studies, vol. 8, no 8 (2011), UPH, Siedlce, 2011.

18. Whitaker A., Newman D.P., Penetration Testing and Network Defense, Cisco Press, Indianapolis, 2006.