Tomasz MULIŃSKI[1]

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

ICT security in tax administration - AV protection systems

DOI: 10.34739/si.2021.25.06

Abstract. The article discusses the topic of ICT security in tax administration. This paper presents a study of the security level of endpoints[8], servers using three antivirus protection systems. It discusses three independent solutions used to ensure the protection of ICT equipment in public administration.

Keywords. ICT security, malware, viruses, tax administration

1. Introduction

This article is the next in a series that addresses the issue of ICT security in tax administration in Poland. It will present three different solutions for comprehensive anti-virus protection, the related challenges, problems and differences in their functioning.

The specificity of public administration services is the obligation to act on the basis of law and within the framework of existing legal regulations. This implies the need to apply the Public Procurement Law [3], which forces a public procurement procedure before the end of AV system support. The bid selection result most often results in that particular antivirus protection system being replaced by another. This affects the need to plan how to remove the old solution

[8] This term should be understood as PCs, notebooks.

and implement the new one in the existing infrastructure, adapt the infrastructure to embed the new AV system, train IT staff. From 2017 to 2021, Trend Micro Office Scan, Symantec Endpoint Protection, and ESET Endpoint Security Suite were sequentially in place at Tax Administration. Each solution is characterized by different capabilities, method of threat detection, management of devices on which client software is installed.

The subject of the research of this publication is the production ICT system of the tax administration, which is exposed to cyberattacks that can lead to systems malfunction. The fundamental objectives of the research were:

- discussion of the most significant problems during the migration, the change of AV protection system having a significant impact on lowering the level of ICT security, and the solutions used to reduce threats during the change of protection system,
- a summary of various techniques for analyzing detected threats based on the available reporting tools in each AV protection system and responding to detected vulnerabilities,

The subject of the research is the evaluation of security threats, resulting from the change of AV protection system, detected threats. The specificity of the subject of research was that a variety of protection systems with different technical solutions giving different research material was analyzed, which to a significant extent the way of developing the article. The selected solutions are commercial products and it was not possible to extend to other products without deployment in a production network. An additional complication was the incomplete implementation of Symantec's system, which prevented it from obtaining extensive research material to develop threat analysis techniques and methods to respond to detected threats. The collected data and analysis seem to indicate that the best protection of the ICT system is provided by Eset's solutions, which have a threat detection rate comparable to Symantec, which has a higher system load during operation and less extensive endpoint management and threat reporting tools. The collected research material and the evaluation of the products show that the IT system of the tax administration was well protected in all solutions, but Eset's solutions allow to implement solutions which increase the security level.

When evaluating these types of solutions, the greatest weight is given to the algorithms used, the level of detection, the technological solutions (e.g., Sonar, threat sense, machine learning). However, it is also a requirement for tax administration when implementing or changing software to ensure the confidentiality, integrity, and availability of the ICT system in which the changes being examined are made. The article shows how important are the knowledge and experience of the IT team responsible for ICT security. The manufacturer's support for implementations was not satisfactory, resulting in the need to develop and implement custom solutions. Therefore, it was reasonable to present in the article the use of solutions (content filtering) that have had a measurable impact on reducing the accessibility problems of the system. The article aims to point out that the human factor is an essential part of an AV protection system, as algorithms implemented in software alone do not solve all threats that may occur in cyberspace.

2. Malware Protection Systems

2.1. Trend Micro Office Scan

Trend Micro Office Scan malware protection system is the first of the tools described in this article. Trend Micro OfficeScan is used to protect corporate networks from malware, network viruses, Internet threats, spyware. OfficeScan web server console manages all clients, as integrated solution resides on the all endpoints and servers in network. The program installed on the endpoints, servers protect the devices from threats and reports its security status to the server. The server, through a Web-based management console, facilitates setting coordinated security policies and deploying updates for each client [19]. OfficeScan is powered by threat information, malware signatures from Trend Micro's cloud-based Smart Protection Network, which provides faster and smarter updates to the program installed on endpoints. Smart Protection Network's cloud-based technology causes the software on the workstation to require fewer resources to operate, reducing the frequency and size of downloaded patterns, eliminating delays in the availability of information about new threats.

Users can access the latest signatures no matter where they connect - on the corporate network, at home or on the road. To do this, the client program must be in roaming mode which means that it will not send or receive information, commands from the regional OfficeScan server. Roaming mode allows the OfficeScan client to download updates directly from Trend Micro's ActiveUpdate (AU) server without connecting to the OfficeScan server. Enabling roaming mode allows mobile computers to download updates even when they are outside the corporate network [11]. Due to a number of consolidation processes, its distributed architecture was not compatible with the changes taking place in the tax administration. Fig. 1 schematically shows the functioning of antivirus protection in the resort.

Due to the need to implement a new version of Trend Micro's AV protection system, it was decided to abandon the local TM servers, switching all client stations to a regional server. Using local servers, a remote parameter change was performed on the client software, which streamlined the migration process to the new Trend Micro version. On the regional server, automatic client updates were disabled and the Trend Micro system version was upgraded, and then updates were enabled for connected workstations in parts. In some cases, it was necessary to uninstall old software directly on the client because the installer could not handle removing all services from the system. For this purpose, after the uninstallation process was completed, it was necessary to search for OfficeScanNT, RealTime Scan services with the `sc query` [13] command and stop them and then remove them with the `sc delete` [12] command from the system, which after a reboot enabled the installation of a new version of OfficeScan. Installation of a new version of the software was based on an installer package generated on the server, which contained the parameters necessary for communication with the server and proper functioning of the software on the client.

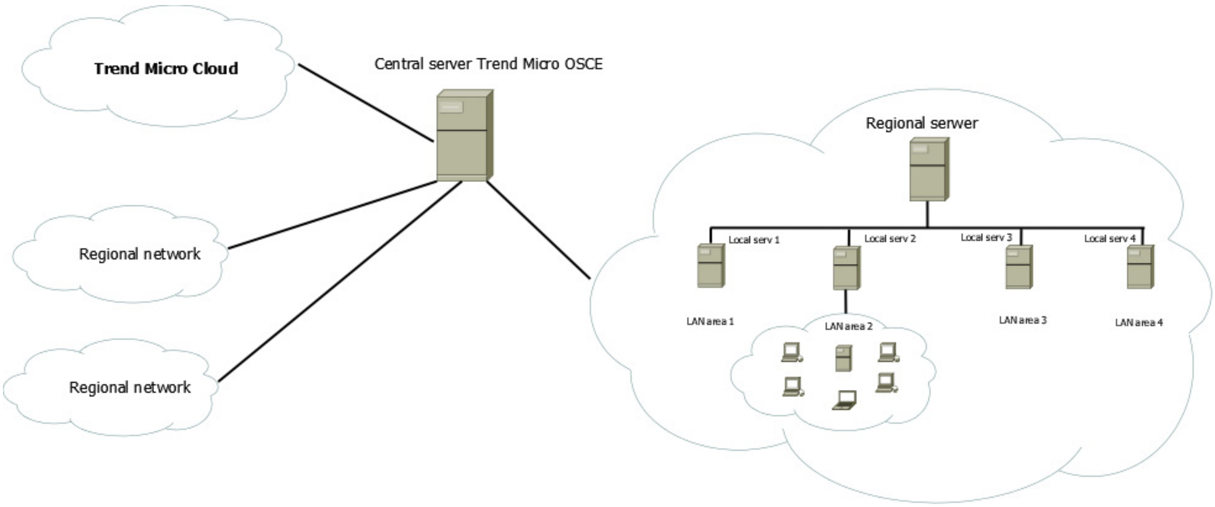

Figure 1. The architecture diagram of Trend Micro system in Tax Administration
Source: own study

Tab. 1 shows the distribution of installed Trend Micro client versions before the OfficeScan client version upgrade process began.

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

TM agent version	Number of TM agents
10.0	17
10.06.5162	118
10.06.5614	1349
10.06.5712	188
10.06.5900	630
11.0.6325	117
Total	2419

On the same time when Trend Micro's version 11 was deployment, discovered and reported by three teams vulnerability in Microsoft systems to attacks dubbed Meltdown Spectre, which exploit a flaw in processor architecture and allow user-level reading of kernel memory. Microsoft prepared the first patches to patch this bug for Windows 10 [14]. These patches required verification of their compatibility with antivirus software by their developers. Compatibility tests performed showed that OfficeScan version 11.0 and higher is compliant with the compliance requirements set by Microsoft [8]. The problem was that Microsoft prevented installation of the patch and required AV vendors to test and prepare an update that makes a registry entry confirming that the Meltdown Spectre bug fix would not cause antivirus software to malfunction. Since Trend Micro had not developed a patch at the time to changing registry entry, action was required to install Microsoft patches to block the vulnerabilities found. Accordingly, a Trend Micro-protected devices registry key with the following parameters was entered via Active Directory:

```
Key="HKEY_LOCAL_MACHINE"Subkey="SOFTWARE\Microsoft\Windows\Cur
rentVersion\QualityCompat"
Value Name="cadca5fe-87d3-4b96-b7fb-a231484277cc"
Type="REG_DWORD”
Data="0x00000000”
```

This enabled automated installation of patches to fix the vulnerability using a regional WSUS server distributing patches to workstations and servers. No exploitation of the Meltdown Spectre vulnerability was observed while using Trend Micro OfficeScan version 11, and no malfunctioning of operating systems or antivirus software was observed.

2.2. Symantec Endpoint Protection

The next antivirus protection system used in Tax Administration was Symantec Endpoint Protection, which replaced the solution discussed in the previous section.

Symantec Endpoint Protection is a client-server solution that proactively protects desktops, laptops, and servers from malware, security vulnerabilities, known and unknown threats to which we can include Trojans, viruses, worms, and adware. Symantec Endpoint also provides protection against the most sophisticated attacks such as rootkits, zero-day attacks and mutating spyware [18].

The implemented Symantec software was the first solution that was managed from a single location - Symantec Endpoint Protection Manager (SEPM). The ability to manage from a region was achieved by assigning subnet ranges in SEPM to administrator accounts from a given unit.

Fig. 2 shows the Symantec Endpoint Protection architecture encompassing three functional groups of components, with some components belonging to multiple groups because they perform many different functions.

Replacing the software with SEP was definitely more challenging than migrating the Trend Micro system. The management method was changed - one central SEMP console with accounts for regional administrators. It was necessary to uninstall the old and install new anty-virus protection software. The purchase order for AV protection services estimated that over 66,000 computers, notebooks, servers and at least 2,000 mobile devices would be covered [15]. In the analysed region, the estimated number of protected devices was over 3850.

The first step in implementing the new system was to uninstall Trend Micro agents from all workstations. The uninstallation order was executed from the Trend Micro regional server console. On most devices, there was no need for the manual uninstallation mentioned in the previous section.

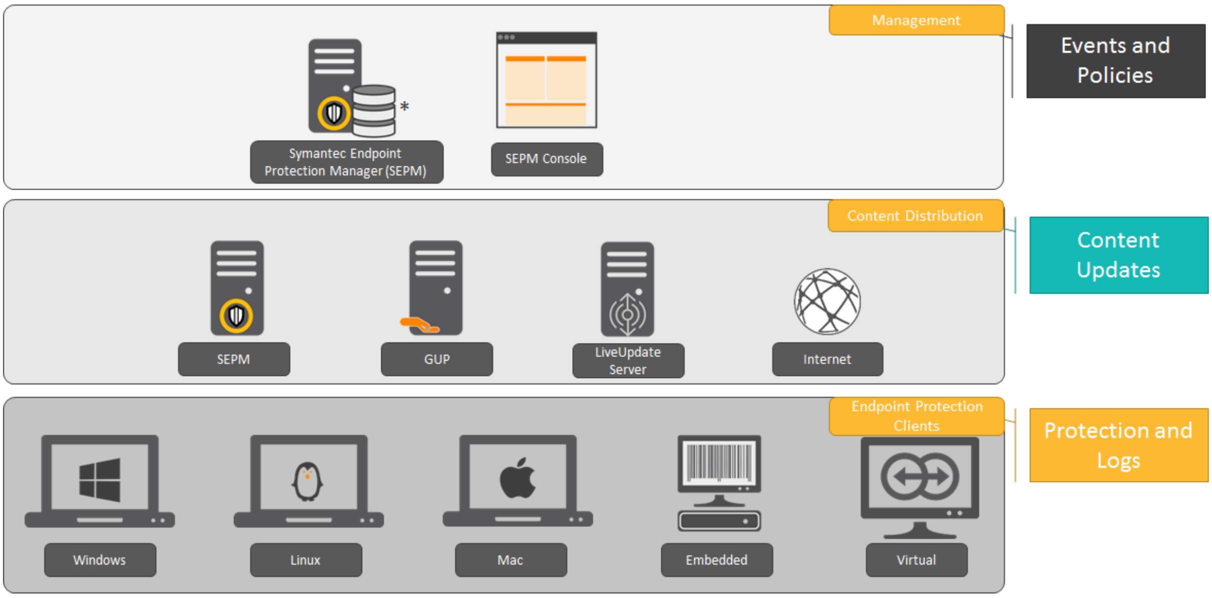

Figure 2. Symantec Endpoint Protection architecture diagram
Source: Symantec [18]

The next stage was to prepare distribution packages with the installer containing configuration information for SEP agents so that the agents could establish communication with the server and receive signature updates. Pre-implementation tests of the SEP system showed that the installation process may cause the computer to slow down, during which time the computer may not respond. It was also necessary to distribute the installer to the local drives of the endpoints using policies, as tests showed that only then there were no problems during the installation of Symantec software. In order to avoid problems with two antiviruses running on an endpoint, software uninstallation was monitored and verified, and SEP installations were ordered using domain policies. This solution required two restarts, the first one was related to the necessity of loading the policies and the second one was required after the installation in order to complete the installation processes during the system start-up. In order to improve the process of changing the AV system, tests were performed on the installer, in which an option to automatically uninstall anti-virus software was added, which improved the SEP implementation process.

The anti-virus protection implemented was based on centralised client management and provision of vaccine updates, which, with a significant number of devices, could lead to server overload and difficulties in the availability of updates. Symantec Endpoint Protection Manager server supports the implementation of randomness for simultaneous downloading of software components by clients from the default management server or group update provider. It also supports random downloads of components by clients from the LiveUpdate server. The enabling of this functionality during the deployment phase has reduced peak network traffic ensuring the availability of up-to-date software patches and vaccine definition packages.

Symantec Endpoint Protection was an interim solution, used for the time of selection of the target system of anti-virus protection of workstations and servers. During the implementation and operation there were no significant problems in the functioning of the system, which fulfilled its tasks correctly.

2.3. ESET Endpoint Security

The last of the antivirus protection solutions discussed is ESET Endpoint Security, whose implementation was slightly different from the previous solutions. ESET prepared a commercial solution consisting of two components:

- ESET Management Agent (EM Agent) - used for remote management of the computer, antivirus software, but also the firewall, enabling remote shutdown, restart and disconnection of endpoints from the network,
- ESET Endpoint Security - proper software for endpoint protection, collection of information on the security status, which enables generation of detailed reports on the state of security in the company's infrastructure.

ESET Endpoint Security (EES) provides integrated protection for computers against threats using dedicated ESET modules. There is a noticeably lower load on the system compared to the antivirus programs discussed above. EES uses AI-based solutions to detect and neutralise threats to the system caused by spyware, trojans, viruses, worms, adware and rootkits, avoiding performance degradation or disruption.

ESET Endpoint Security provides web access protection and monitors the communication between the web browser and the remote server, it also protects the e-mail client by checking incoming communication via POP3(S) and IMAP(S) protocols [5].

The second ESET solution implemented as part of the change in antivirus protection in the tax administration was ESET Server Security (ESS), which is an integrated solution designed for the Microsoft Windows Server environment. ESS uses two methods to protect servers: malware protection and anti-spyware protection.

ESET Server Security provides protection for virtualised environments by enabling scanning of virtual machine disks on a Microsoft Hyper-V server without the need to install an agent on a given virtual machine. Like ESET Endpoint Security, the server solution does not burden system resources and does not compromise the performance of server systems [6].

Fig. 3 shows a simplified architecture of ESET Endpoint Security.

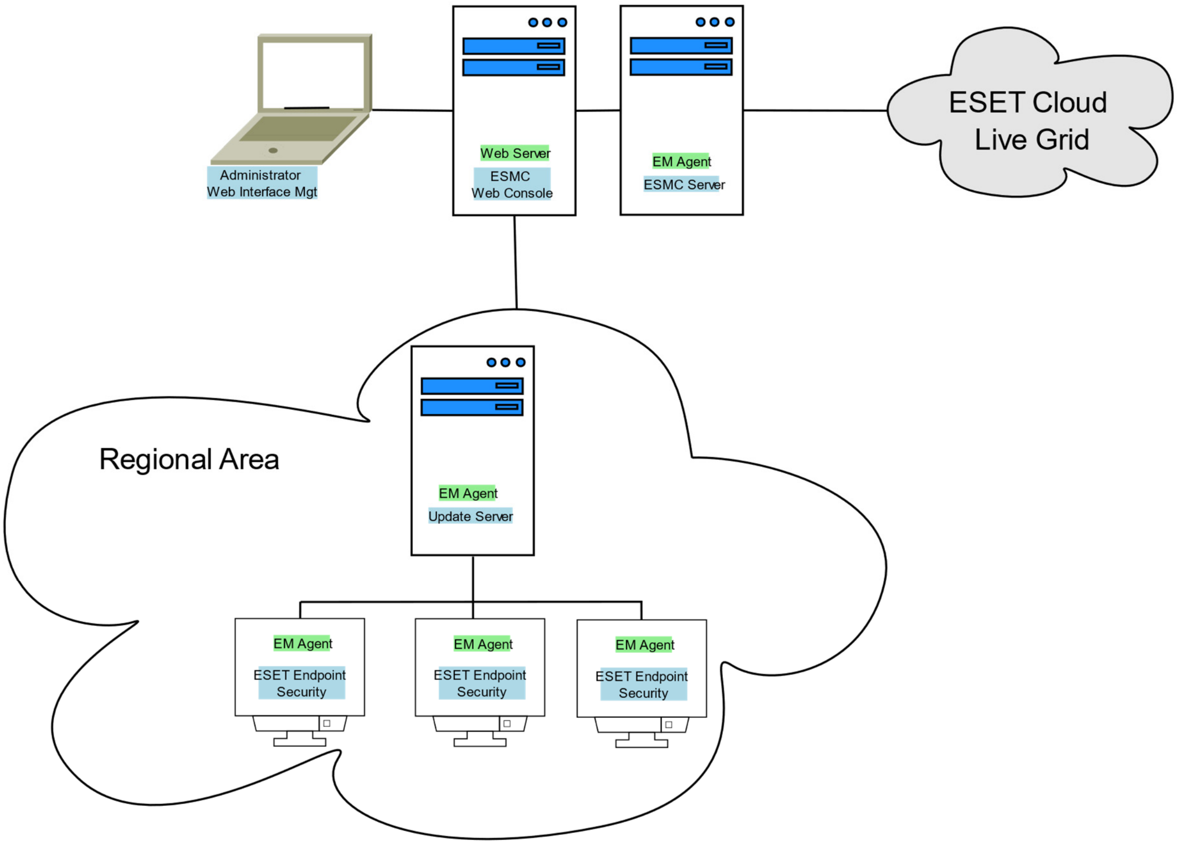

Figure 3. Simplified architecture diagram of ESET Endpoint Security in Tax Administration
Source: own study

The Management Agent solution has simplified the deployment process, as installing this software via domain policies enables remote uninstallation of programs on endpoints and mandated deployment of ESET Endpoint Security. The management console enables monitoring of the process of uninstallation, installation, and selection of the group of devices on which the tasks of implementing new antivirus protection software will be performed. It should be noted that the process could largely be performed by a limited number of administrators without the need to involve local IT teams, but a certain percentage of endpoints required manual uninstallation and installation (about 3-5%). For reasons of ensuring the continuity of operation of server systems, the anti-virus software was changed by local IT staff. As in previous implementations, attention needed to focus on off-line computers, which were not used during the implementation periods due to employee absence or departure. Using the ESMC web console, it was possible to efficiently deploy ESET software on endpoints, monitor system health, and quickly respond to problems and threats occurring on remote computers.

3. Anti-virus protection systems - threats to security of ICT systems

It may seem that anti-virus protection only covers the area of detection, prevention, protection against threats to ICT systems. It is often claimed [1, 4, 7] that the built-in Microsoft Windows Defender is sufficient for protection. The authors do not pay attention to the needs of remote system management and monitoring in organisations with a large number of computers and servers, extensive distributed infrastructure. The following considerations and analyses show what challenges ICT system administrators and anti-virus system administrators have to confront.

3.1. Trend Micro

The Trend Micro system is the oldest of the antivirus protection systems discussed in this article, which certainly does not allow for a comparison of protection effectiveness, capabilities with other antiviruses [7], however, it shows that changes in AV systems require a different approach to analysing the level of ICT security.

The antivirus system in question did not have many reports showing the status of antivirus protection, it was only possible to obtain a detailed report containing 60 columns with relevant information on the status of individual endpoints.

For the purposes of monitoring migration, Trend Micro used OCS Inventory [2], which allows for monitoring the validity of signatures, software versions. Tab. 2 shows the status of migration of the antivirus system on endpoints and servers to version 11.

Table 2. List of version Trend Micro before and during migration.
Source: own study

Data before TM version change version
Trend Micro console 29.06.2017

Trend Micro version	Number of Endpoints
10.0	17
11.0.6325	117
10.06.5162	118
10.06.5614	1349
10.06.5712	188
10.06.5900	630
Total	2419

Data during TM migration to version 11.0
OCS system 22.11.2017

Trend Micro version	Number of Endpoints
10.0	181
11.0	2076
10.6	559
Unknown version	81
Total	2897

The differences in the tables are due to a number of reasons, the AV software versions on the console are more accurate, while the OCS allows the retrieval of two parts of the installed version number. Also, on the TM console all computers were not attached at the time the information was downloaded.

Other numbers of Trend Micro instances result not only from the above-mentioned reasons, but also from the fact that the OCS system contained archival data on computers withdrawn from use and maintained in the database for the needs of the conducted inventory of withdrawn equipment and inventory of equipment intended for decommissioning.

The use of the dual-source method of device information streamlined the migration process by providing accurate identification of resources that were experiencing AV upgrade issues. In the Trend Micro console there is also the possibility to remove endpoints that have been withdrawn which was implemented in some sub sites.

The differences in Tab. 2 and Tab. 3 are due to several reasons:

- The OCS shows the status after 5 months,
- Re-introduction of computer equipment,
- Verifying and correcting the reasons for missing signature updates.

Table 3. Trend Micro signature update status over 5 months.
Source: own study

Number of days since last signature update	Trend Micro console 29.06.2017	System OCS 22.11.2017
more than 365 days	270	220
more than 14 days, less than 366	797	719
less than 15 days	1830	1958
Total	2897	2897

In the course of determining the reasons for the lack of updates, it emerged that this was most often caused by the lack of implemented patches for the operating system, as Microsoft had implemented a mandatory reboot after installing the patches. Users very often switched off the computer after installation and switched it on the next day. As a result, the operating system patches were not fully implemented and the antivirus system could not update the signatures. Microsoft has made changes in later updates that allow patches to install themselves when the computer is rebooted and any reboots are performed during system start up without user interaction.

The problem was the analysis of the threats detected by the TM, as the collected data were not collected for their further study. Due to the interesting results and the one-year interval between the analysed data it was reasonable to use them in this study, as presented in Tab. 4.

Table 4. Number of threats detected by Trend Micro.
Source: own study

Date	Number of Devices	Number of devices with Virus/ Malware	Virus/ Malware detections	Max Virus/ Malware detections per device	Number of devices with Spyware/ Grayware	Spyware/ Grayware detections	Max Spyware/ Grayware detections per device
20.06.2017	2421	146	5490	2324	45	970	342
20.06.2017	16	16	4568	2324	16	921	342
29.11.2018	16	16	4167	2324	7	572	327

The analysis compared both 2017 data and the information we have on the 16 devices on which the most malware was detected in 2018. For the purpose of the analysis, a summary of 16 devices from 2017 was also prepared which allowed the identical number of devices to be compared and taking into account that the vast majority of incidents in the network studied occurred on 20-30 endpoints and considering that the TM system reports the number of incidents cumulatively.

Of the 16 endpoints reported in 2018, eleven occurred in the 2017 report with the highest number of malware, an increase of 339 detected incidents. In the area of grayware, the number of devices from 2017 was seven, with no new threats detected on these devices. Due to space limitations, it should be noted that most threats were reported on application servers and largely originated from websites or downloads. Workstations made a negligible contribution to incident generation.

When using Trend Micro and Symantec Endpoint Protection systems, false alarms were generated for programs created to configure utility applications and update database tables. Trend Micro, after several years of use as a result of signature updates, began identifying threats in these applications by deleting them from disks. These programs were developed in Visual Basic and it is difficult to determine what piece of code caused the false-positive alerts. The removal of these programs was not threatening to the functioning of the application, as these tools were mostly one-time in duration and stored as application archives.

3.2. Symantec Endpoint Protection

The anti-virus protection system being implemented was of a transitional nature, so the focus was on ensuring full migration of the AV protection system on all computers and servers. This required monitoring of the implementation of the new solution. The management console did not have tools to record the status of protection including detected incidents. During the five-month exploitation, the analysis of detected threats was based on the information available in the administration console, but due to other safeguards implemented (which will be discussed in other articles), there were no significant numbers of incidents not detected or blocked by SEP requiring additional action by local ICT system administrators.

As already mentioned, the implementation process was work-intensive due to the heavy load on the system during the installation of the SEP, resulting in up to half an hour of endpoints being out of service. This required spreading the software replacement over time and analysing the status of the implementation and the functioning of the protection. Tab. 5 shows how, based on the OCS system, the state of ICT security looked in one region with about 4,000 workstations and servers.

Different days covered different numbers of devices on which SEP was deployed, while analysing the problems encountered with Microsoft patch updates. The noticeably higher number of SEP installation issues on 17/06/2019 was a result of the inclusion of 24/7 devices in the analysis, which caused more problems with the implementation of the new antivirus protection. All identified problems were forwarded to local administrators for correcting. It is noticeable that a large proportion of endpoints with problems installing or updating signatures also had an outdated operating system.

We should mention the problem of removing tool applications created in Visual Basic, which was signalled in the article. Closer analysis of the problem indicated that Symantec detected two threats reported as Trojn.Gen.2 and Heur.Adv.ML.C in executable files with .exe extension. The first threat was qualified as a virus, while the second was reported by SEP as heuristically detected. Another misidentified threat in PrivacyProtector was the detection of the malware PUA.Superfluss. As these incidents were detected at the deployment test level, deletion of these files by SEP was blocked, MD5 checksums were generated from them and entered into the AV system to exclude them from analysis for vulnerabilities.

Table 5. Monitoring the implementation of Symantec Endpoint Security.
Source: own study

Date	Number of endpoints	Number of endpoints without SEP installed		Number of endpoints with definitions older than 30 days	
		Total	of which no current updates from WSUS	Total	of which no current updates from WSUS
21.05.2019	237	5	3	21	17
31.05.2019	65	4	4	3	3
13.06.2019	204	1	0	7	6
17.06.2019	373	31	12	8	8

3.3. ESET Endpoint Security

The last antivirus protection system discussed is ESET's solution, which consists of two applications to monitor and provide antivirus protection. Extensive possibilities of reporting the status of AV protection and security updates, it will be possible to focus on detected threats.

In order to show the complexity of monitoring the update and proper functioning of the antivirus protection system, it should be mentioned that during the change of the software version it is necessary to monitor the versions of three different programs, two of them are agents for remote computer management and two AV protection solutions for PCs - ESET Endpoint Security and servers - ESET File Security. Tab. 6 shows the status of implementation of new versions of ESET programmes.

Table 6. Monitoring of ESET software module updates.
Source: own study

Application	ESET Endpoint Security		ESET File Security			ESET Management Agent x32		ESET Management Agent x64	
Version	7.1.2053.0	7.2.2055.0	6.5.12018.0	7.1.12006.0	7.1.12008.0	7.0.577.0	7.1.717.0	7.0.577.0	7.1.717.0
Number of installations	926	2113	2	41	47	767	2424	21	1
Total	3039		90			3191		22	

🟨 - outdated version 🟩 - current version

The results show that version changes force the monitoring of double the number of programs, as each protected device has two ESET solutions installed necessary to ensure communication with the server and antivirus protection. Before presenting the results of the research on detected security incidents, the results of the analysis of blocking audio, video content with the use of the built-in ESET filter will be presented. In order to limit unfavourable streaming media traffic for the organisation, ESET's built-in streaming media blocking filter was test enabled for 1.5 hours. It turned out that Endpoint Security detected and blocked more than 3,750 connections during that time, while normally around 100-200 events are detected per day and responded to by anti-virus software. Due to the rather restrictive blocking, it was decided to create a custom filter that did not exclude certain sites, such as YouTube, used by the organisation. Tab. 7 lists the most frequently blocked domains during the testing period.

Table 7. Tests of ESET's built-in filter for blocking domains with streaming media.
Source: own study

Domain name	**Number of blockades**
static-global-s-msn-com.akamaized.net	736
onet.pl	694
youtube.com	494
googlevideo.com	386
rmfon.pl	318
eskago.pl	153
gazetaprawna.pl	108
polskieradio.pl	101
constellation.mixer.com	82
tvn.pl	61

The number of total blocked connections from the 10 domains was 3133 which accounted for over 83% of all incidents. The first domain in the ranking came about because Microsoft configured its browsers to open the MSN news page by default, which contained content blocked by ESET. In addition, each time a new empty tab was opened, MSN messages were loaded, resulting in further incidents noted by ESET. The high positions of YouTube and Google are due to the practice of embedding streaming media in websites, quite often automatically playing when the page loads. The popular portal Onet.pl is also overloaded with many streaming media. It would seem that the second position and the number of recorded events indicate a considerable interest of employees in this information portal.

However, when analysing other cases involving a large number of events detected on a single endpoint, it was found that adding favourite sites to the bookmarks bar in Firefox is a common practice. While determining the reason for such a high number of generated events, it turned out that the browser is querying the site in order to quickly display the content to the user after selecting the site from the bookmarks bar.

Tab. 8 shows how the number of blocked connections to domains looked before and after the ESET filter was switched on and after it was switched off, and the application of a custom filter developed based on knowledge of sites providing access to streaming media services excluding YouTube.

The obtained results do not show how many domains are blocked per day, while the example of tuba.fm indicates similar problems as in the case of akamaized.net and onet.pl domains, therefore some alerts were disabled in order to limit the size of reports, limiting them to relevant and important information. It was taken into considerations that the blocking information is only informative and does not bring relevant news about the level of risks.

Table 8. Domain locks before and after testing.
Source: own study

Domain name	Number of blockades 17.05.2020 - 19.05.2020	Domain name	Number of blockades 21.05.2020 - 10.07.2020
remarketingpixel.com	35	fm.tuba.pl	2466
onlineradio.pl	21	sluchaj.fm	246
sluchaj.fm	18	polskieradio.pl	154
d18mpbo349nky5.cloudfront.net	16	stat777.com	49
rmfon.pl	16	rmfon.pl	47
radiofm-online.com	8	remarketingpixel.com	42
mobile-app-market-here2.life	5	cloudfront.net	35
player.radiozet.pl	5	radiofm-online.com	22
postlnk.com	5	rmfon.pl	18
wypr.pl	4	wypr.pl	18

Definitely fewer threats were detected and removed from files on computer disks and removable media. The number for the four-month period was 717 incidents. A significant part of them was related to web browsers, extensions installed for them and html, java files downloaded while browsing websites. A small proportion of threats (53) originate from removable media. Some of the detected undesirable applications are the result of long-term storage of programs that were not detected by previous antivirus software or a full scan of the media was never performed. Tab. 9 lists the detected threats with a brief description.

An analysis of detected threats in email and web browsers over a period of one week was carried out, looking at where it occurred. The following results show the greater variety of threats that can be encountered when using the Internet. In the case of the threats detected by the ESET plug-in to the e-mail programme, there was one type of threat MSIL/Kryptik.ZIG identified by antivirus programmes as a Trojan. It seems that the small number of detected e-mails is due to the fact that only some employees use Outlook software to receive mail, the majority receives mail via a web browser, and that spam was not directed to all employees in the region, which number over 4200.

Table 9. Threats detected by ESET during the period 20.01.2020 - 30.05.2020. Source: own study

Name of risk	Number of occurrences	File type	Description of risk
ML/Augur	119	dll file	inf Firefox profile widevinecdm.dll
Win32/Adware.SpeedingUpMyPC.AM	116	7z file	Executable in 7zip - DeviceDoctor.exe
Win32/Toolbar.Widgi	91	cab files	Data1.cab in pdfforgeToolbar.msi
Win32/RemoteAdmin.RemoteExec.AA	79	exe file	Hirens tool - tool siw.exe
JS/Adware.AppNexus.A	68	html file	In web pages on cache html file
Win32/HackTool.WinActivator.I	56	exe file	Windows Loader.exe
Win32/TFTPD32.B	25	exe file	tftpd32.exe
Java/Riskware.DirBuster.A	22	jar file	In web pages in browser cache DirBuster-1.0-RC1.jar
JS/Lightning.B	22	zip file	content.zip
Win32/UwS.SlimDrivers.A	22	msi file	Packages instaler app.cab
PHP/Obfuscated.F	14	php file	Blueblog/index.php
Win32/Keygen.EV	14	exe file	Classic Menu for Office 2007 - key35.exe
Win32/PSWTool.KonBoot.A	11	gz file	Hirens tool - konboot.gz
Win32/MagicalJellyBean.B	10	zip file	Ekeyfinder archive
Win32/NetTool.Ncat.A	9	exe file	Nmap - ncat.exe
Win32/SecurityXploded.A	7	exe file	Setup_MailPasswordDecryptor.exe
BAT/HackTool.WinActivator.B	4	cmd file	Install.cmd
Win32/Bundled.Toolbar.Google.D	4	no data	in Avast setup
Win32/PSWTool.ProductKey	4	exe file	Nirsoft produkey.zip -ProduKey.exe
Win32/Avast.Cleanup	3	dll file	Avast library TuneupSmartScan.dll
Win64/PSWTool.ProductKey.A	3	exe file	ProduKey.exe
JS/Adware.Agent.AF	2	html file	In web pages in browser cache html file
MSIL/Toshiba3rdParty.A	2	exe file	Toshiba wireless util
Win32/Bundled.Toolbar.Ask.P	2	js file	Firefox extention background.js
Win32/TFTPD32.A	2	exe file	tftpd32.exe
Win32/Toolbar.Conduit.AU	2	exe file	unknown Setup.exe
Win64/Pokki.B	2	exe file	hostappserviceupdater.exe
EFI/CompuTrace.A	1	no data	Absolute Computrace Installer
Win32/Hidcon.B	1	exe file	Aktywator office 1.3 2010.exe

In order to provide a holistic overview of the threats, the time distribution of detected threats was analysed by assuming a weekly period. It should be noted that the days of 16 and 17 January were a Saturday and Sunday which was reflected in the low number of incidents detected during this period. The specificity of tax administration is that some offices work on a 24/7 schedule, also on days off, hence incidents detected by the antivirus protection system occurred. The analysis of the data shows two increases in the number of incidents on working days, which occur most frequently around 8 a.m. and 2 p.m., with the afternoon increase being significantly higher. The number of incidents during a single day is relatively low in relation to the approximately 2,000 computer devices operating on weekdays. In addition, the number of incidents is reduced by protection systems at the intranet/Internet interface and user awareness of threats they may be exposed to while using the Internet and mail (see Tab. 10 and Fig. 4).

Table 10. Locations of the incident during the period 13.01.2021 – 20.01.2021.
Source: own study

	Location of the incident				
Name of risk	Internet Explorer	Firefox	Opera	Outlook	Summary
HTML/Hoax.Agent.P		1			1
HTML/ScrInject.B		2			2
JS/Adware.Subprop.U	4	1			5
JS/Adware.Subspromo.A	5	5			10
JS/Agent.OLF		1			1
JS/ExAds.A		1	1		2
JS/PopunderJS.E		2			2
JS/Redirector.NDS	1	1			2
MSIL/Kryptik.ZIG				18	18
Total	10	14	1	18	43

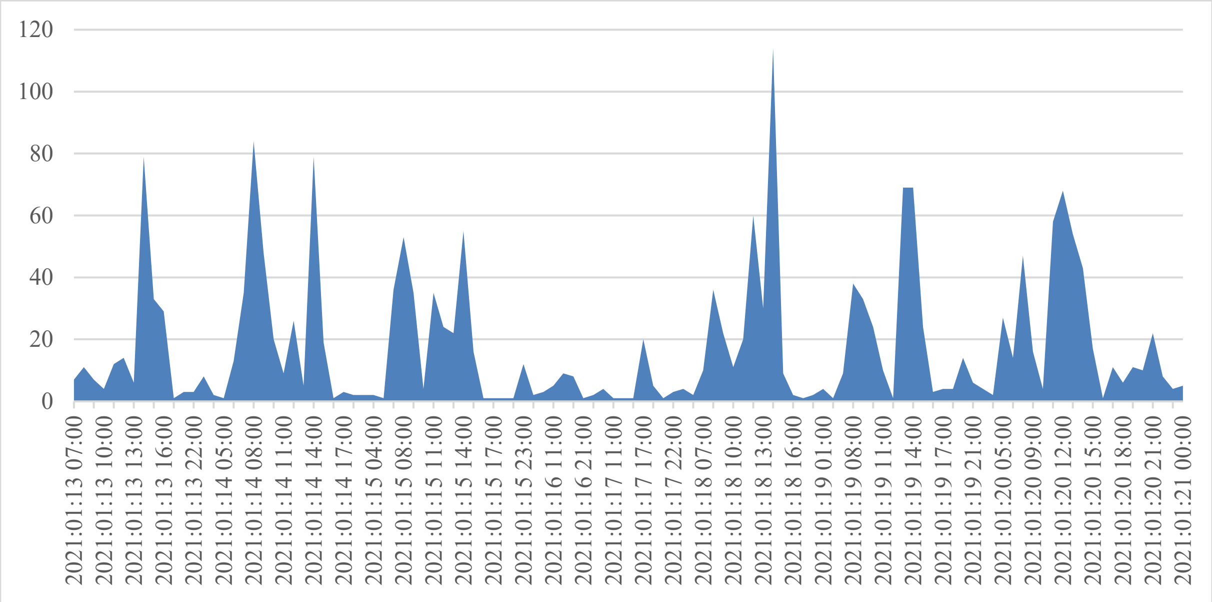

Figure 4. Distribution of threats detected by ESET in the period 13.01.2021 - 21.01.2021
Source: own study

Finally, when considering security threats, it is worth presenting the results of an analysis of several ESET reports from a year of its use. When using websites, users usually use bookmarks containing shortcuts to the most visited sites. It happens, however, that domain names are maintained manually and this can be the cause of threats, as hackers take advantage of the fact that they have redirections or domains with names similar to the most popular ones, placing malicious software on them. The analysed case concerned the google.pl domain, for which 58 errors and attempts to redirect to malware sites were observed. The most common wrong domain name was googe.pl with 34 occurrences. The remaining occurrences were much less frequent, with the following domain name errors detected, which were blocked by ESET: fgoogle.pl, gppgle.pl, goodle.pl, googel.pl, googfle.pl, googlle.pl, googlwe.pl, googole.pl, goolge.pl. This shows that even a mistake in the name of a website can have serious consequences, resulting in a threat which, if there is no antivirus protection, can infect the computer. Hackers use various types of vulnerabilities, holes, and human errors to break through defences against cyber-attacks.

4. Summary

Administration of AV protection systems is not only about monitoring incidents, reacting to them and implementing new versions of software. It is necessary to analyse and draw conclusions from detected incidents, use built-in tools in AV systems to improve security, monitor the status of implementation of security patches for operating systems.

Providing an anti-virus protection system is a complex task in which not only threat alerts and signature updates must be analysed and monitored, but also the status of operating system updates, emerging challenges due to hacker activity, new versions of AV software, which must be implemented on an ongoing basis to raise or sustain a high level of protection for endpoints and servers.

The antivirus protection solutions presented in this article show the diversity of solutions and their specific use, which translates into the need to develop different methods of AV system administration and device protection management. Migrations of anti-virus protection systems are also a great challenge due to the different ways in which they function and the need to ensure continuity of IT security.

An analysis of publicly available AV software rankings indicates that black-box methods are used [16], in which the observation of antivirus software's response to particular threats, task and system scanning times, and software price determines the ranking position. In contrast to this approach, the evaluation of the three systems presented was based on a grey-box approach [16] in which the system architecture was known, both reports and additional customer management tools were used. It should be emphasized that the results were collected on a real IT system consisting of several thousand endpoints and servers, as opposed to rankings that involve several devices subjected to a specific number of threats. Undoubtedly, it is easier to make an assessment using a homogeneous research environment, but the complexity and unpredictability of threats in a large research group allows for results that can be compared to a kind of behavioral research in which machine learning plays an important role. Unfortunately, the producers do not disclose detailed information on the applied artificial intelligence solutions and machine learning algorithms, which undoubtedly makes it difficult to assess their quality and performance.

When assessing the presented AV solutions, it should be noted that the scope of protection of ICT systems was increasing and the subsequent implemented systems had more and more additional solutions, such as:

- Artificial intelligence and machine learning algorithms (Eset has used since 1997 [9], Symantec has Sonar [17], Trend Micro has used for 15 years [10]),
- remote endpoint management (Eset, Symantec),
- The ability to protect virtual machines (Eset, Symantec),
- Extensive reports on the security status of individual devices as well as the entire IT system (Eset),
- High performance and low system load during online scanning and protection (Eset).

Eset's solution is not only characterized by very good results in both detection and removal of threats, unlike other used antivirus protection solutions it did not slow down the system - no reports from users indicating that AV protection caused delays in interaction when using endpoints. Symantec noticeably overloaded endpoint systems during normal operation, however, in various antivirus rankings it takes leading positions, but in the area of customer management, performance, monitoring it is inferior to Eset's products. The weakest performer is Trend Micro's OfficeScan, which lacks a number of innovative solutions that provide heuristics-based, advanced monitoring and management of ICT system security.

A very important element of security is raising the awareness of users, whose actions, conscious or unconscious, can lead to weakening ICT security. The collected incidents and conclusions drawn from them are good didactic material for raising the level of awareness of users, whose actions have a decisive influence on the level of ICT system security in the tax administration.

References

1. 5 free security tools from Microsoft , Niebezpiecznik, https://niebezpiecznik.pl/post/5-darmowych-narzedzi-bezpieczenstwa-od-microsoftu/, Accessed 20 Dec. 2020,

2. About OCS inventory, OCS Inventory NG, https://ocsinventory-ng.org/?lang=en, Accessed 20 Jul. 2020,

3. Act of 11 September 2019. - Public Procurement Law, Journal of Laws 2019, item 2019 with changes,

4. Data security on Windows 10 (Surface devices), Niebezpiecznik, https://niebezpiecznik.pl/post/bezpieczenstwo-danych-na-windows-10-urzadzenia-surface/, Accessed 20 Jul. 2020,

5. ESET online help - ESET Endpoint Security 8, ESET, https://help.eset.com/ees/8/pl-PL/, Accessed 20 Jul. 2020,

6. ESET online help - ESET Server Security 8, ESET, https://help.eset.com/efsw/8.0/pl-PL/overview.html, Accessed 20 Jul. 2020,

7. Good antivirus? That's Windows Defender. You don't need anything else , Jakub Szczęsny, https://antyweb.pl/windows-defender-av-test, Accessed 20 Jul. 2020,

8. Important Information for Trend Micro Solutions and Microsoft January 2018 Security Updates (Meltdown and Spectre), Trend Micro, https://success.trendmicro.com/solution/1119183, Accessed 20 Jul. 2020,

9. Leading ESET Technologies, Eset, https://www.eset.com/pl/about/technology/, Accessed 17 Dec. 2021,

10. Machine learning, Trend Micro, https://www.trendmicro.com/pl_pl/business/technologies/machine-learning.html, Accessed 17 Dec. 2021,

11. Manually enabling roaming mode and allowing updates from ActiveUpdate for OfficeScan (OSCE), Trend Micro, Inc., https://success.trendmicro.com/solution/0121893-manually-enabling-roaming-mode-and-allowing-updates-from-activeupdate-for-officescan-osce , Accessed 20 Jul. 2020,

12. Microsoft Docs - Windows Server Windows Commands by Server Role - sc delete, Microsoft, https://docs.microsoft.com/pl-pl/windows-server/administration/windows-commands/sc-delete, Accessed 20 Jul. 2020,

13. Microsoft Docs - Windows Server Windows Commands by Server Role - sc query, Microsoft, https://docs.microsoft.com/pl-pl/windows-server/administration/windows-commands/sc-query, Accessed 20 Jul. 2020,

14. Microsoft Knowlege Base - January 3, 2018—KB4056892 (OS Build 16299.192), Microsoft, https://support.microsoft.com/en-us/topic/january-3-2018-kb4056892-os-build-16299-192-c0ce8445-3adc-7a71-2fbd-9e93ed00b04e, Accessed 20 Jul. 2020,

15. Ministry of Finance, Terms of Reference - Proceedings conducted as an open tender for the provision of a service providing functionality of antivirus protection and Web Cache, Ministry of Finance, Warsaw, 2017,

16. Muliński T., ICT security in tax administration - Rapid7 Nexpose vulnerability analysis, Studia Informatica. Systems and Information Technology 2020, nr 1-2, pp. 37-51,

17. Program release notes Symantec ™ Endpoint Protection 14.3 RU1, Symantec, https://techdocs.broadcom.com/content/dam/symantec/techdocs/us/pl/dita/symantec-security-software/endpoint-security-and-management/endpoint-protection/14-3/14-3-ru1-mp1/Release_Notes_SEP14.3.1.pdf, Accessed 17 Dec. 2021,

18. Symantec Corporation, Installation Guide and Program Administration Guide Symantec™ Endpoint Protection 14.2., Symantec Corporation, Mountain View, 2018,

19. Trend Micro OfficeScan Server Version 10 Service Pack, Trend Micro, Inc., https://docs.trendmicro.com/all/ent/officescan/v10.0SP1/en-us/osce_10.0_sp1_server_readme.htm, Accessed 20 Jul. 2020.