SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2020
ORGANIZATION AND MANAGEMENT SERIES NO. 149

ANALYSIS OF THE INTERNET ACTIVITY OF EMPLOYEES IN THE CONTEXT OF THREATS AND THEIR ACTIVITY IN THE NETWORK – A CASE STUDY

Grzegorz PODGÓRSKI

University of Lodz, Faculty of Management, Department of Computer Science; grzegorz.podgorski@uni.lodz.pl,
ORCID: 0000-0001-8695-5075

Purpose: The aim of the article is to analyse selected aspects of network threats and Internet activity of the organization's employees.
Design/methodology/approach: The article consists of two parts. The first one is theoretical. The second is a case study of an educational organization along with an analysis of selected aspects.
Findings: Some network applications used by employees carry a high risk for the organization. On the one hand, they can be a vector of malware in an organization, they can contain the latest security vulnerabilities, use significant network resources or can hide the activity of attackers. On the other hand, they are of little importance to business: they are not related to the work and the activities of the organization.
Practical implications: Analysis of user activity in the context of information security allows achieving tangible benefits, especially in increasing the level of information security. It also gives you the ability to tune and better match existing security solutions or implement new ones.
Originality/value: This article contains a case study of a university unit in terms of threats related to users' online activity. The article presents the actual data collected for a period of eighteen months related to the activity of users on the network, as well as threats that have been recorded in the organization.

Keywords: security of information, threats, users activity, case study.

Category of the paper: Case study.

1. Introduction

Nowadays, there is no organization which does not touch the problems related to information security. Due to the increasing use of the Internet, modern cloud solutions, network applications and progressing digitalization, each organization regardless of the industry is exposed to certain dangers related to its data. Organizations must face many of the threats associated with the digital world. These threats may be related to the loss of one of the three

http://dx.doi.org/10.29119/1641-3466.2020.149.42

main attributes of security: confidentiality, accessibility and integrity, but they may also be related to losses resulting from the decrease of employee efficiency. For the purposes of this article, the threats have been divided into three categories to which the case study will refer.

One of these hazard categories is associated with applications that are used every day by employees. These applications may contain vulnerabilities that allow organizations to "open" themselves to the selected network attack vector, or even may contain malware (ransomware/malware). Exploiting a potential vulnerability could cause a threat, and this can easily lead to a loss. This loss, as we know, may be directly related to financial losses but may also have a dimension related to moral losses. Malware may cause any effects programmed by the creator, which may result in data theft, modification or more often may be used for blackmail due to data encryption. Then, the process of collecting fees related to the recovery of encrypted data begins (Dobran, 2019). Statistics show that this is a particularly profitable business for attackers. Their victims are the largest organizations, public offices and even cities (like in the case of Atlanta city (Olenick, 2018) or Baltimore City (Cook, 2019)).

Another aspect is the use of applications that are not needed by employees to perform their work but they use them for private purposes. In this case, the drop in "productivity" translates directly into financial loss for the organization. It is an increasingly frequent case in many organizations around the world. Many sources indicate that employees can spend between one hour up to three hours on private Internet browsing during business hours (Heathfield, 2019).

There are Internet browsers and Internet browsing in one category and the other – confirmed by case analysis. This is particularly dangerous because for many employees of the organization it is the basic form of their activity on the Internet. The last category of threats are threats related to the use of sociotechnical methods and techniques such as phishing, which cause that the users themselves, unaware of their actions, pose a threat to the organization. This type of threat is very common – according to CERT (Polish division) statistics more than 44% of all incidents handled by the organization in 2018 concerned phishing (CERT, 2018). There are also a number of other threats resulting from the activity of employees on the Internet, but due to the extent of the subject matter, they are not the subject of this article.

2. Network threats in Poland and in the world

It is estimated that cybercrime damages will cost the world $ 6 trillion annually by 2021 (Morgan, 2018). According to Gartner, in 2019, information security related expenses will exceed USD 124 billion. The number of incidents related to information security is still very high, both in the world and in Poland (CERT, 2018) – Figure 1. It should also be emphasized that not all organizations report security incidents to relevant organizations or services. Such a policy results mainly from fear of losing reputation and market position.

The number of potential attack vectors in connection with the use of new technologies, the number of applications, the speed of the Internet and the possibilities of publicly available tools is enormous. The most commonly used threats are those related to ransomware, which is broadly understood malware and phishing. It is estimated that at the end of 2019, an attack on a company will occur every 14 seconds, and this time will be reduced to 11 seconds by 2021 (Morgan, 2018). Currently, about 4,000 such attacks are carried out every day. Among all network attacks, those that touched the trojan/malware category most often concerned the education industry (Malwarebytes, 2019). However, in the category of malware, education industry found itself in second place (Malwarebytes, 2019).

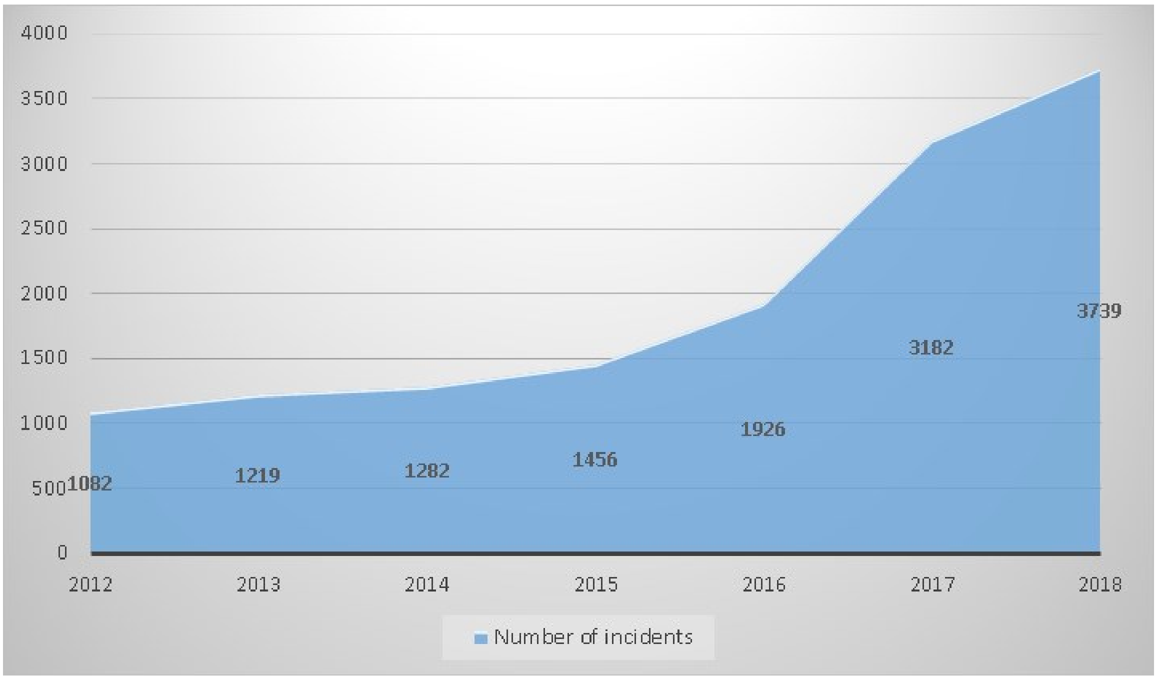


Figure 1. Number of incidents handled by CERT over the years. Adapted from: CERT Report 2018 (CERT, 2018).

Ransomware worked well for the last three years. Starting in 2017 and continuing to 2018 there has been a steady decline in ransomware campaigns. In 2018 and in 2019 cyber-criminals moved away from ransomware to cryptocurrency miners, largely for the same reasons that led to the rise of ransomware in the first place. At this point, cryptocurrency miners are more profitable than ransomware.

Additional danger arises from the fact that there are ample of hacking tool kits and software available on the dark web costing as little as literally $1. Of course, the costlier, the better the tools and services available. Especially when we can have new cyber-crime infrastructure on demand. New tools using cloud computing appeared on the market of cybercriminals. The first one is RaaS (Ransomware-as-a-Service) – it allows attackers to rent ransomware infrastructure rather than develop it themselves. The second is CaaS (Crime-as-a-Service) which allow cybercriminals to rent whole IT infrastructure and services needed to do cyber-attacks. An example are on-demand distributed denial-of-service attacks and bulletproof hosting to support malware attacks.

Symantec's ISTR 2019 report states that public administration organizations receive one malicious e-mail per 302 e-mails.

The greater part of security incidents is related to the activity of users/employees on the Internet in the context of performing their duties as well as in connection with their activities that are not related to their duties. It is particularly evident especially where the industry of the organization requires employees to use the Internet as a tool for everyday work. The educational centres are exposed to particular danger. Firstly, because they are perceived as less secured goals than large corporations. Secondly, because the main activity of the scientific staff (employees) is to look for information that is increasingly available to them in the form of electronic materials on the Internet. There are other reasons associated with the choice of educational centres as targets of attacks such as patents, scientific studies, research documentation, etc., which may translate into a specific financial value in the event of theft.

3. Case study

The research method used in the presented article is a case study. In this study, the subject is a unit of a university employing over 340 people. Most employees are academics, the rest is broadly understood administration staff. This unit is a highly computerized unit within the university on which it is located. It has its own IT department, which is responsible for help desk, IT network management (wired and wireless), supervision over ten IT laboratories and development and creation of dedicated IT solutions (systems) used by the unit. The number of physical workstations in the unit is more than 550 machines, not including the server facilities. The number of students is around 4,000.

The collected statistics show the period of one and a half year – from January 1, 2018 to June 30, 2019. These data were collected on various security devices, including systems that specifically investigated the vulnerability to external attacks, the so-called HoneyPot systems. All information provided below (unless stated otherwise in the source) comes from the author's own work based on data from various devices and information systems of the university unit under study. The number of public higher education institutions in Poland is 385, and the number of non-public higher education institutions is 247 (POLON, 2019). Thus this is a very large group that can be a potential target for attacks.

The number of attacks on the audited entity carried out in the period from January 2018 to June 2019 was 3,223, of which 1,520 (47.16%) were classified as significant and having a major impact on the organization's security. This means they targeted machines that were likely vulnerable to these attacks. Security systems identify high impact events automatically by correlating attacks with target risk, which is determined by passively profiling network devices and their vulnerabilities in real time. The following attacks are very important to investigate because they directly target machines that have been identified as potentially vulnerable in the organization. The target machine's operating system version, running services, and potential vulnerabilities all match what threat is designed to be attacked.

The following applications have been identified as associated with attacks – table 1 and table 2.

Table 1.
Applications associated with high impact events

Applications associated with high impact events	Count
Web browser	1,032
Telnet client	397
DNS client	50
ICMP client	10

Adapted from: Own study.

Table 2.
Applications associated with lower impact events

Applications associated with lower impact events	Count
Web browser	859
NetBIOS-ssn (SMB) client	213
Firefox	121
DNS client	35
Chrome	31

Adapted from: Own study.

As one can see, the majority of incidents, both those with high and low rates, relate to web browsers (Internet browsing), i.e. typical activities that users usually perform. Therefore, from the point of view of security, it is very important to provide employees with the latest versions of web browsers without known security vulnerabilities as well as fine-tuning network devices to filter network traffic at such an angle or to filter out pages and dangerous domains as much as possible. Not without significance is also the awareness of users using the Internet about threats as well as appropriate behaviour (knowledge of threats, security procedures, etc.).

The number of incidents related to ransomware in 2018 is shown in figure 2. It is easy to notice that the most incidental months were April, May and November. This is reflected in world statistics on the spread of malicious software, as well as finding gaps and exploits in various types of products used by users (Chebyshev, 2018). When searching through exploit databases, it is easy to discover that for example on 08/11/2018 there were many exploits related to Cisco products (Vuldb, 2019). This is even more evident because the university unit uses Cisco solutions. As you can see, the search tools in the Cisco product network quickly recognized such an element of infrastructure.

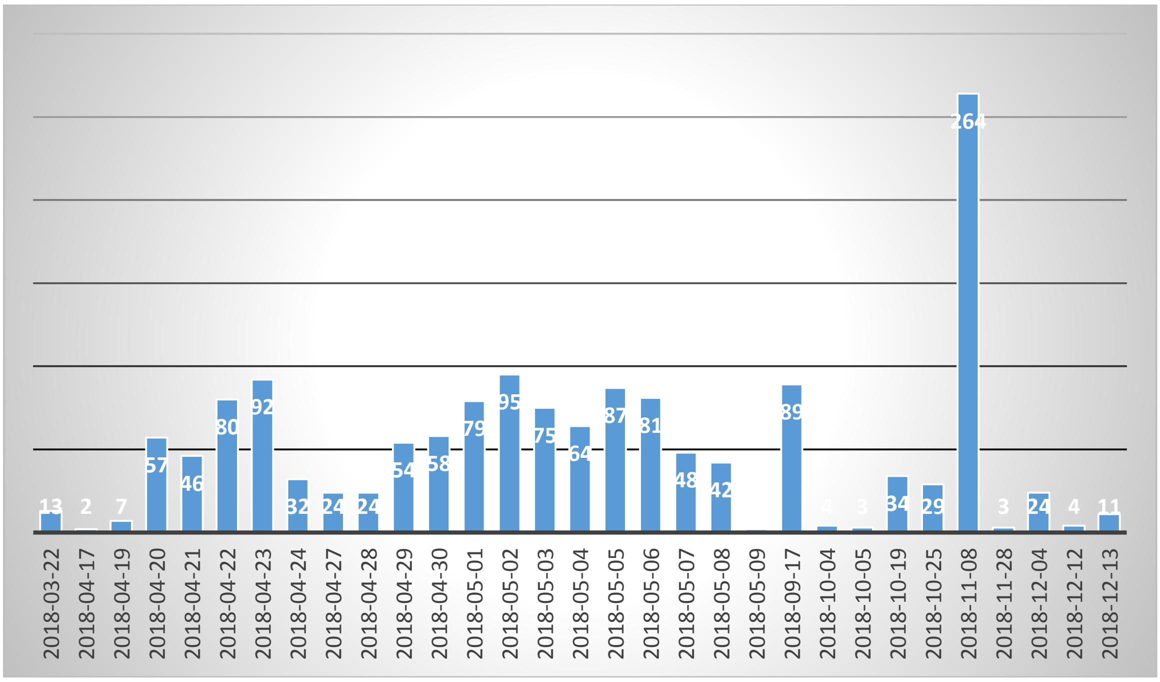


Figure 2. The number of malware incidents, broken down by dates in 2018. Adapted from: Own study.

As for days of the week in which incidents related to malware occurred, the distribution of incident data was fairly even – figure 3. A certain decrease in incidents can be noted in the case of Saturdays and Sundays. However, this is only related to two aspects. The first of these is the smaller occupancy of classes on these days for the majority of employees – a smaller number of extramural students than full-time students. The second aspect is the issue related to running classes just on the days when employees rarely run their computers doing any work other than conducting classes. During the week when classes are spread over the whole day for employees, they devote more time to scientific work and so the number of working computers increases. Less presence of employees in the network means fewer computers being launched, and thus fewer potential targets for attacks. Analysing this distribution, it can be easily adapted to other existing data, such as the number of connected computers and the number of transfers in the network, in other words the Internet activity of employees. These data confirm the thesis related to the activity of users and the amount of threats that are directed at them.

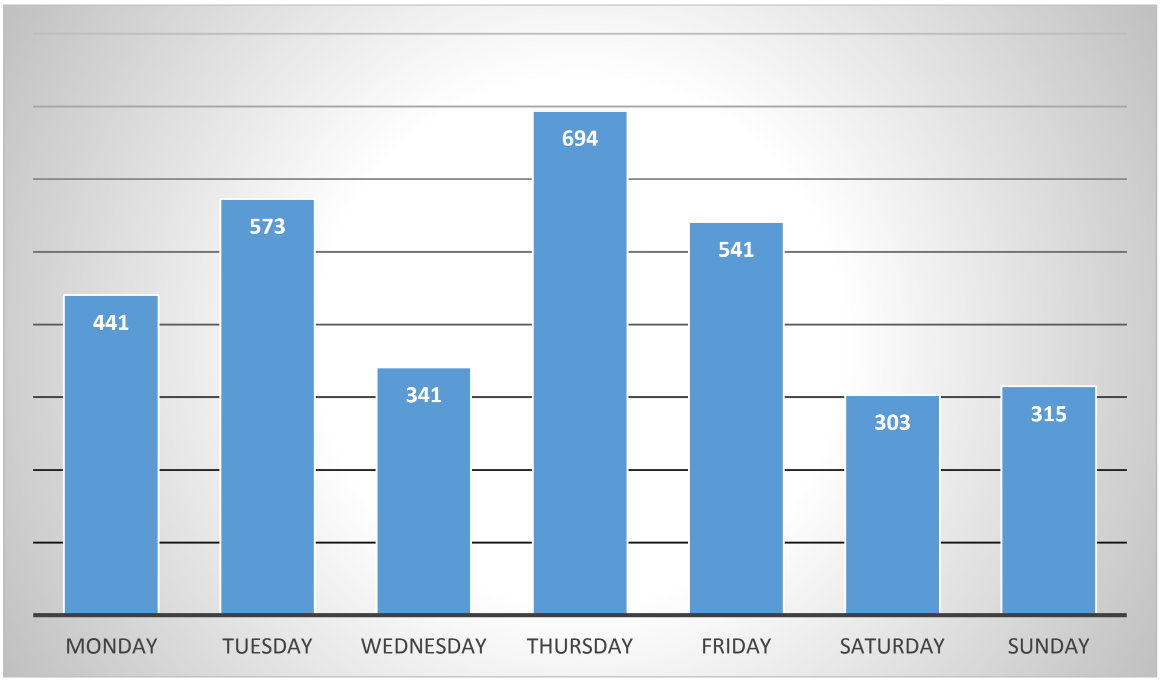


Figure 3. Days of the week and the number of malware-related incidents. Adapted from: Own study.

Typical working hours of employees of a scientific unit (hours between 8.00 and 16.00) are also reflected in the number of incidents recorded at particular hours of the day – Figure 4. However, it should not be forgotten that in the case of other times of a day, we mainly deal with incidents directed at the server infrastructure.

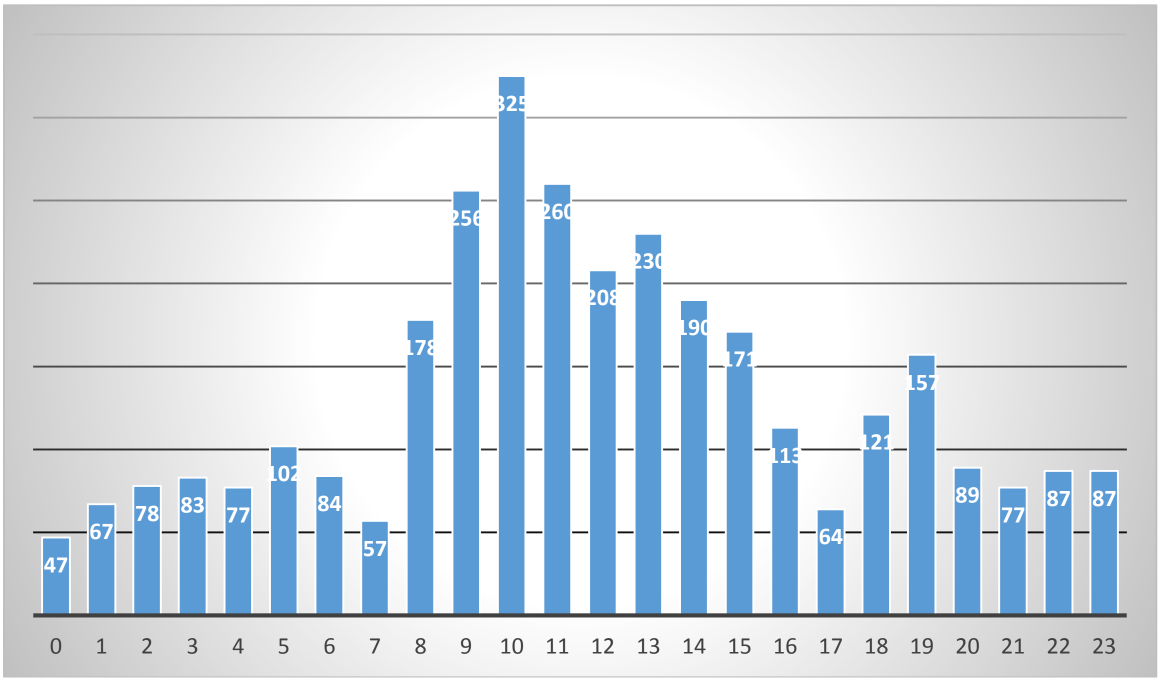


Figure 4. Number of security incidents per particular hour. Adapted from: Own study.

The sources of security incidents are mainly countries from which most threats of this type originate and in this case the statistics reflected the standard for the whole country and the world (Baig, 2017) – Figure 5.

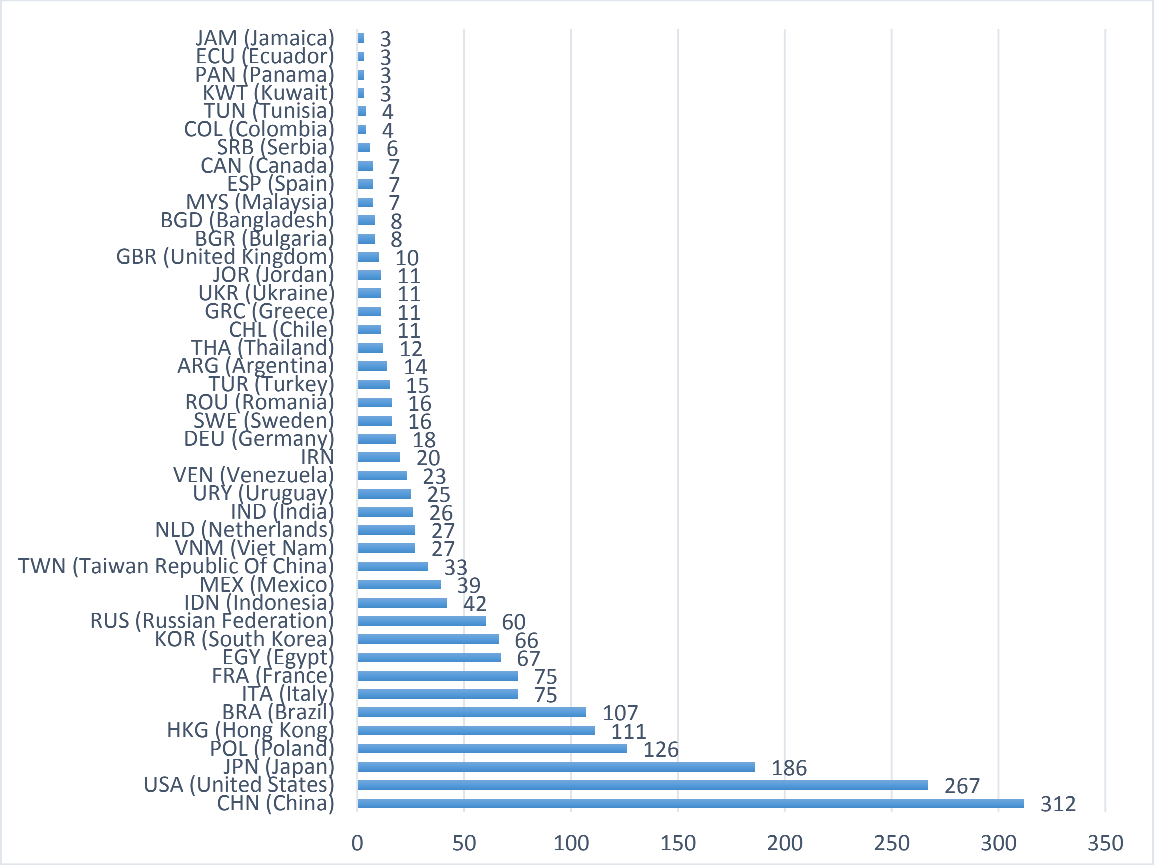


Figure 5. Countries as a source of security incidents. Adapted from: Own study.

The most frequently detected threats were all kinds of malware, attacks on web applications and attempts to gain administrative access (using vulnerabilities in software or operating systems) – Figure 6.

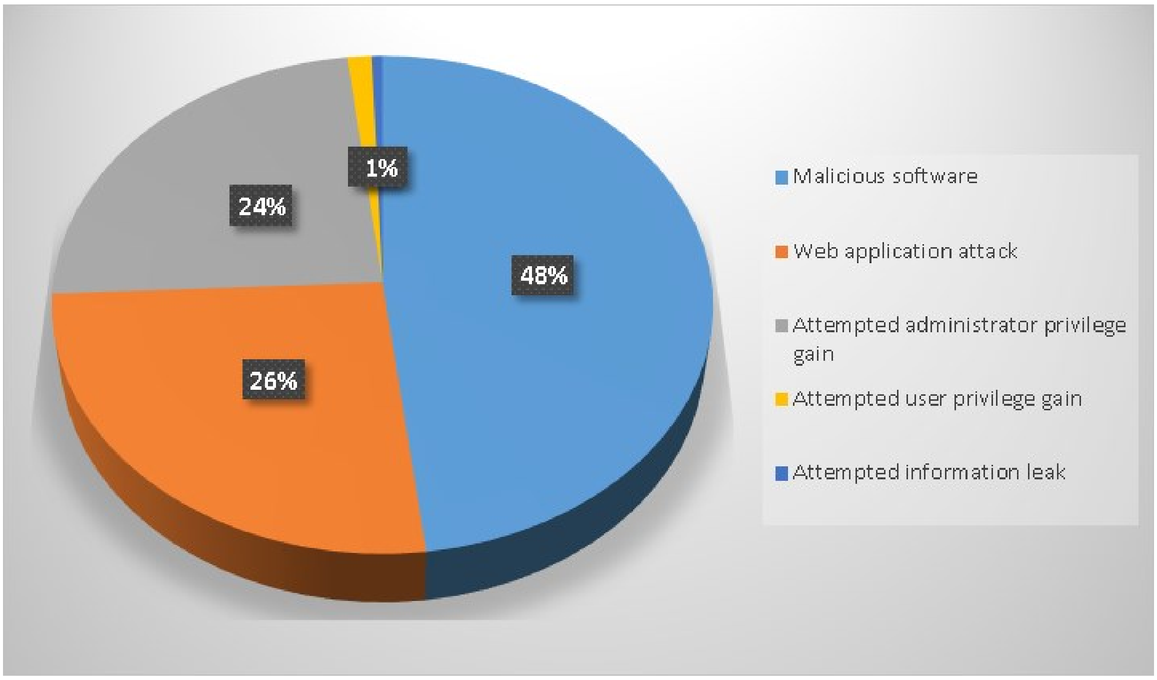


Figure 6. The percentage of each category of threats. Adapted from: Own study.

It should be noted that malicious software may also involve the user's activity on the Internet. This is the case when they consciously or not can download malware or software impersonating other usable one. It is also possible to infect the operating system due to vulnerability in the system, software or infection related to e-mail attachments.

Study has determined that the unit is at a high risk due to the use of applications that are potentially dangerous to the enterprise yet have low business relevance. These applications may leave the network vulnerable to attacks, carry malware, or waste bandwidth. Some applications carry high risk because they can be vectors for malware into the organization, possess recent vulnerabilities, use substantial network resources, or hide the activities of attackers. Other applications have low business relevance: they are not relevant to the activities of a typical organization. When an application has high risk and low business relevance, it is a good candidate for application control to reduce your application risk.

In addition to applications that are not related to work, there are also applications that are responsible for high network bandwidth load. In the case of this organization they are not that important, but for other reasons they may seem significant. This can happen for two reasons: because of the costs incurred due to them (transfer fee) or because they occupy bandwidth. This bandwidth usage can be costly to organization and can negatively impact overall network performance. It should also be noted that in the case of the university unit under examination, such cases were recorded mainly in the case of WiFi networks made available to students and it they mainly concerned applications such as: YouTube, Netflix Stream or BitTorrent.

Another potential source of threats may be applications that use cryptographic algorithms. On the one hand, they guarantee the security of communication between the parties of network communication (e.g. a user with a bank), but on the other hand, they can be a potential source of threats. These applications encrypt data they process, causing security administrators to be blind to attacks and usage patterns. With SSL decryption, administrators can look inside these applications and observe their use. An SSL decryption appliance, such as a Cisco SSL Appliance, can decrypt SSL inbound and outbound traffic: inbound by storing the certificates of private web servers, and outbound by acting as an intermediary in browsers' connections to the Internet. It is important to use SSL decryption to obtain insight into encrypted applications to help mitigate this potential attack vector.

Analysing the network activity of users in the studied unit, evasive applications were also observed. Evasive applications try to bypass security by tunnelling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications.

Also other applications were observed that may be of interest and possibly candidates for control. Users may use anonymizers and proxies to bypass network security or cloak their identities. Gaming applications may be distractions to productivity and use excessive bandwidth. Peer-to-peer applications are often malware vectors and remote administration applications may allow malicious users to control machines in organizational environment.

In this category of applications the following have been analysed:

- Anonymizers and Proxies;
- Games and Recreation (accesses): Facebook (2,302,140), Instagram (78,450), Facebook Messenger (36,621), Facebook Video (10,026), Messenger (4,344);
- Peer-to-Peer and Sharing (accesses): MSN (829,929), Skype Tunnelling (351,410), Windows Live (86,921), Instagram (78,450), Pinterest (57,428), MS Online (39,208);
- Remote Administration and Storage (accesses): Dropbox (324,129), iCloud (290,104), Wget (275,978), BITS (153,130).

Then, as a result of analysis and implementation of security rules, some of them were blocked. An example may be the lack of use of the Dropbox platform in the case of personal data and the lack of appropriate legal regulations.

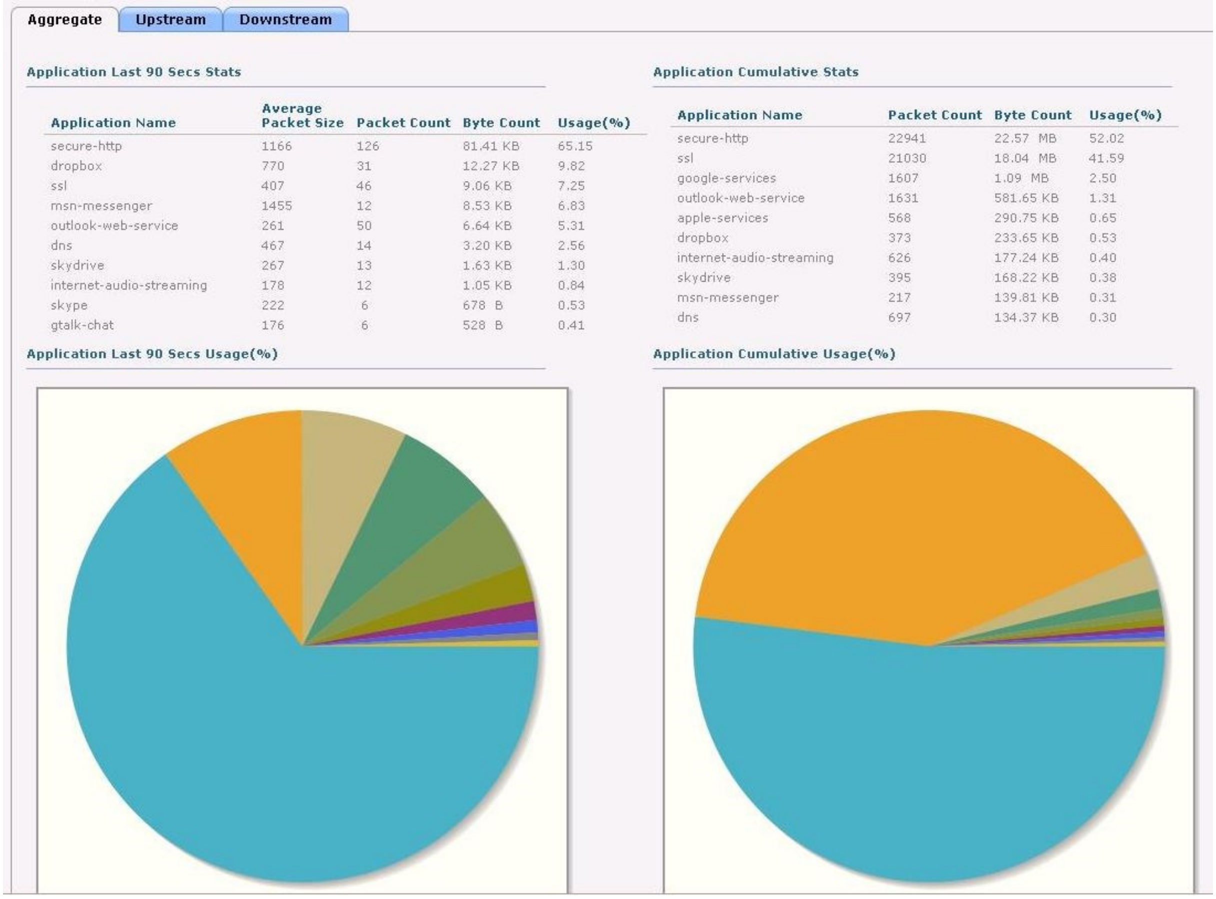
The following web communications that correspond to risky activity were identified. Malware sites, open proxies and anonymizers, keyloggers, phishing sites, and spam sources are all Web activities that can put organization networks at risk. It is wise to evaluate the use of URL filtering technologies to detect and control communications to risky sites – table 3.

Table 3.
Risky web browsing URL category connections

URL Category	Connections
Social Network	2,684,489
Proxy Avoid and Anonymizers	21,820
Malware Sites	7,220
Phishing and Other Frauds	3,562
Spyware and Adware	1,968
Peer to Peer	151
SPAM URLs	12

Adapted from: Own study.

The activity of the organization's users was also analysed in more detail in terms of their network traffic. An example set of information (at a very general level) for a selected user is shown in Figure 7. In addition to aggregate analyses at the level of each or a selected user, it also allowed to determine the characteristics of network traffic at the level of selected sub-networks occupied by specific groups of users including students. This analysis allowed to determine firstly what typical network traffic looks like in given network segments and on this basis follow any anomalies appearing in this traffic. Secondly, the analysis allows you to collect statistics on the effectiveness of users' work.



Application Last 90 Secs Stats

Application Name	Average Packet Size	Packet Count	Byte Count	Usage(%)
secure-http	1166	126	81.41 KB	65.15
dropbox	770	31	12.27 KB	9.82
ssl	407	46	9.06 KB	7.25
msn-messenger	1455	12	8.53 KB	6.83
outlook-web-service	261	50	6.64 KB	5.31
dns	467	14	3.20 KB	2.56
skydrive	267	13	1.63 KB	1.30
internet-audio-streaming	178	12	1.05 KB	0.84
skype	222	6	678 B	0.53
gtalk-chat	176	6	528 B	0.41

Application Cumulative Stats

Application Name	Packet Count	Byte Count	Usage(%)
secure-http	22941	22.57 MB	52.02
ssl	21030	18.04 MB	41.59
google-services	1607	1.09 MB	2.50
outlook-web-service	1631	581.65 KB	1.31
apple-services	568	290.75 KB	0.65
dropbox	373	233.65 KB	0.53
internet-audio-streaming	626	177.24 KB	0.40
skydrive	395	168.22 KB	0.38
msn-messenger	217	139.81 KB	0.31
dns	697	134.37 KB	0.30

Application Last 90 Secs Usage(%)
Application Cumulative Usage(%)

Figure 7. Sample of collected information about user activity. Adapted from: Own study.

Analysis of users' activity, devices and network traffic has led to modification and better tuning of many security mechanisms that have already been implemented in the organization. It also showed areas related to broadly understood security, which require refinement or implementation of new solutions. The scientific unit also carries out work related to the creation of a user activity profile that will allow to quickly and automatically pick up anomalies related to traffic that do not match the given standard user profile.

In matters related to phishing, the examined unit did not report wider attempts to use this method. All attempts were made by means of electronic mail. Thanks to the good awareness of users and the wide campaign on this issue, the unit did not suffer any dangerous effects. It should also be noted that the high awareness of users often resulted in reporting such incidents to relevant services and a quick response in the form of appropriate messages to all employees sent by the IT department.

In the near future, work related to improving the security of the organization will be carried out in several independent but coherent directions.

Firstly, security systems with App Control and URL Filtering will be deployed to:

- Reduce application attack surface;
- Granularly control applications, bandwidth, URL access and acceptable use policies;
- Get insight into network risks and usage, including mobile devices and BYOD risk.

These changes are aimed at improving the security of IT infrastructure in which data and information are stored. A big challenge will also be to increase the ability to control the mobile work environment of users, especially those who use their own devices to work in the BYOD (Bring Your Own Device) system. Control over such an environment is particularly difficult due to many technical and organizational, as well as legal aspects.

However, it should not be forgotten that the process of achieving an appropriate level of security and its maintenance is a continuous process subject to continuous validation and modification together with new threats and technologies used.

4. Conclusion

As this paper shows, the analysis of user activity in the context of information security allows to achieve measurable benefits especially in information security perspective. It also gives the possibility of tuning and better matching existing security solutions or implementing new ones. This is especially important when a large part of the threats is associated with the typical activity of each user, which is browsing the Internet for information, and especially in the context of research centres where one of the basic activities of academic staff is searching for information, downloading materials from various sources, wide correspondence in electronic form, etc. Noteworthy is the fact that in these centres there are huge amounts of sensitive electronic information: patents, research results, analyses, research papers, dissertations, etc. As we have seen, particularly high risk is associated with malware, which is directly related to the user's awareness. Therefore, organizational security is an important aspect in addition to physical and software security. They are associated with trainings of employees, introduction of regulations, rules of conduct and identifying best practices. Only thanks to the high awareness and responsibility of employees, together with the use of the latest security measures, organizations are able to achieve and maintain an adequate level of information security.

References

1. AV Test. *The Independent IT-Security Institute.* Retrieved from https://www.av-test.org/en/statistics/malware/, 23.07.2019.
2. Baig, A. *Top 5 Countries Where Cyber Attacks Originate.* Retrieved from *https://securitytoday.com/Articles/2017/03/03/Top-5-Countries-Where-Cyber-Attacks-Originate.aspx?m=1&Page=1,* 23.07.2019.

3. CERT Polska (2019). *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2018.* Retrieved from https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf, 23.07.2019.
4. Chebyshev, V., Sinitsyn, F., Parinov, D., Liskin, A., Kupreev, O. (2018). *IT threat evolution Q2 2018. Statistics.* Retrieved from https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/, 23.07.2019.
5. Cofense Annaul Phishing Report 2019. *Phishing Threat & Malware Review 2019.* Retrieved from https://cofense.com/phishing-threat-malware-review-2019/, 23.07.2019.
6. Cook, S. *2017-2019 Ransomware statistics and facts.* Retrieved from https://www.comparitech.com/antivirus/ransomware-statistics/, 23.07.2019.
7. Dobran, B. *27 Terrifying Rasomware Statistics & Facts You Need To Read.* Retrieved from https://phoenixnap.com/blog/ransomware-statistics-facts, 23.07.2019.
8. G Data. *Malware figures for the first half of 2018. The danger is on the web.* Retrieved from https://www.gdatasoftware.com/blog/2018/09/31037-malware-figures-first-half-2018-danger-web, 23.07.2019.
9. Heathfield, S. *Surfing the Web at Work.* Retrieved from https://www.thebalancecareers.com/surfing-the-web-at-work-1919261, 23.07.2019.
10. Kujawa, A., Zamora, W., Umawing, J., Segura, J., Tsing, W., Arntz, P., Boyd, C., Malwarebytes Labs (2019). *2019 State of Malware.* Retrieved from https://resources.malwarebytes.com/resource/2019-state-malware-malwarebytes-labs-report/?utm_source=blog&utm_medium=post&utm_campaign=0119_ws_stateofmalwarereportq119_mb, 23.07.2019.
11. Morgan, S. *Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021.* Retrieved from https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/, 23.07.2019.
12. Olenick, D. *Atlanta ransomware recovery cost now at $17 milliond, reports say.* Retrieved from https://www.scmagazine.com/home/security-news/ransomware/atlanta-ransomware-recovery-cost-now-at-17-million-reports-say/, 23.07.2019.
13. POLON *Rejestry publiczne.* Retrieved from https://polon.nauka.gov.pl/opi/aa/rejestry/szkolnictwo?execution=e2s1, 23.07.2019.
14. Vulnerability Database. Retrieved from https://vuldb.com/?exploits.20181108, 23.07.2019.