applied sciences

MDPI

Article

Introduction of the ARDS—Anti-Ransomware Defense System Model—Based on the Systematic Review of Worldwide Ransomware Attacks

Veronika Szücs *, Gábor Arányi and Ákos Dávid

Department of Electrical Engineering and Information Systems, University of Pannonia, Egyetem Street 10, H-8200 Veszprém, Hungary; aranyigabor@hardening.hu (G.A.); david.akos@uni-pannon.hu (Á.D.)

* Correspondence: szucs@virt.uni-pannon.hu

Abstract: We live in a world of digital information communication and digital data storage. Following the development of technology, demands from the user side also pose serious challenges for developers, both in the field of hardware and software development. However, the increasing penetration of the Internet, IoT and digital solutions that have become available in almost every segment of life, carries risks as well as benefits. In this study, the authors present the phenomenon of ransomware attacks that appear on a daily basis, which endangers the operation and security of the digital sphere of both small and large enterprises and individuals. An overview of ransomware attacks, the tendency and characteristics of the attacks, which have caused serious financial loss and other damages to the victims, are presented. This manuscript also provides a brief overview of protection against ransomware attacks and the software and hardware options that enhance general user security and their effectiveness as standalone applications. The authors present the results of the study, which aimed to explore how the available software and hardware devices can implement digital user security. Based on the results of the research, the authors propose a complex system that can be used to increase the efficiency of network protection and OS protection tools already available to improve network security, and to detect ransomware attacks early. As a result, the model of the proposed protection system is presented, and it can be stated that the complex system should be able to detect ransomware attacks from either the Internet or the internal network at an early stage, mitigate malicious processes and maintain data in recoverable state.

Keywords: cybersecurity; ransomware; autonomous ARDS model

check for updates

Citation: Szücs, V.; Arányi, G.; Dávid, Á. Introduction of the ARDS—Anti-Ransomware Defense System Model—Based on the Systematic Review of Worldwide Ransomware Attacks. *Appl. Sci.* **2021**, *11*, 6070. https://doi.org/10.3390/app11136070

Academic Editors: Andrea Bondavalli and Andrea Ceccarelli

Received: 26 May 2021
Accepted: 25 June 2021
Published: 30 June 2021

1. Introduction

Today's digital world affects everyday life so extensively that there are hardly any sectors of the economy where there are no IT systems, whether it is to control, schedule and regulate production and production processes, or even to store operational data in near-human areas. This huge development that characterized the last 2–3 decades has brought not only positive contributions. This development has also been accompanied by its negative effects and by the vulnerability of digital data. These can be results of accidental misuse, malfunction, or intentional 'digital' damage. Simultaneously, with the development of technology, a layer of cybercriminals with a high level of expertise has emerged and is evolving, taking advantage of digital vulnerabilities to exploit the opportunities arising from victims' ignorance, fear and low IT skills. Cybercrime has become a particular mode of treatment for unsuspecting or irresponsible users. The goal is different, as it can simply be a form of self-expression that can be called very specific, which involves the attacker breaking into the victim's system because they are able to do it. Often, the user does not even notice this, because there are no clear signs of the attack to be interpreted. In recent years, however, there has been an increase in attacks in which victims find a clear message on their computers and servers. The message usually informs the user about the fact that their computer or network has been attacked or compromised and that their files have been encrypted, while the original files stolen. In these cases, hackers ask for a ransom with a short deadline of 24–48 h in a virtual digital currency, usually Bitcoin.

The current research has been indicated by an increasing number of ransomware attacks, a significant increase in the extent of the damage caused. The fundamental question of the research was focused on small and medium-sized enterprises: how often these attacks occur in this entrepreneurial class, how successful they are, and what connections can be revealed between the elements of corporate IT culture and IT security, and whether these economic operators in the current situation are willing to adopt a new, complex, autonomous system of protection designed and modeled on the basis of emerging needs.

This manuscript contains the research questions that were formulated with the help of the answers obtained during interviews. Based on the evaluation of the survey, a definable goal has been to design a cost-effective protection model that can work with currently available network and virus protection solutions, enable the early detection of ransomware attacks, protect the data undertaken, and in all cases, allow recovery in the case of damage or incident.

The following subsection gives a brief overview of cyberattacks from the last 6 months that have affected different sectors and demanded ever higher ransoms from users.

2. Literature Review and Investigation of the Trends of Ransomware Threats

2.1. Brief Overview of Ransomware Attacks of the Last Six Months from the Worldwide News

Data assets and their associated software environments are currently the greatest technological assets. The developers of extortion viruses are taking advantage of this to try to attack almost any organization for which the above two are essential for their operation. Today, as a result of our growing IT vulnerability and profitability, this form of attack is responsible for nearly a third of security incidents.

The continued rise of cryptocurrencies and the steep increase in their exchange rate makes their inclusion (as ransom) very attractive to cybercriminals, and it does not help that many prominent players in the tech industry are also accepting them as a form of payment, legitimizing it. These tendencies can be seen in Figures 1 and 2 [1].

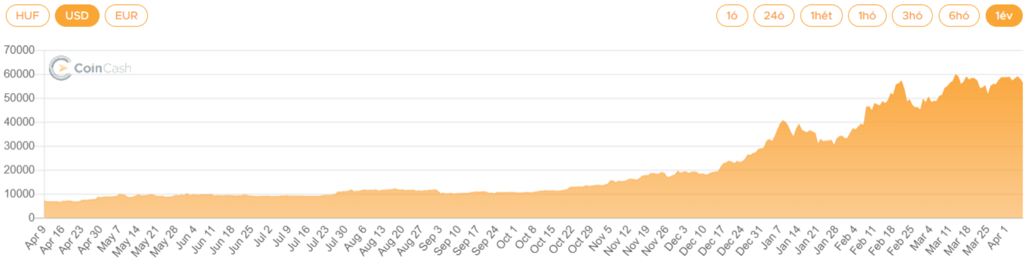

Figure 1. One-year Bitcoin rates in USD.

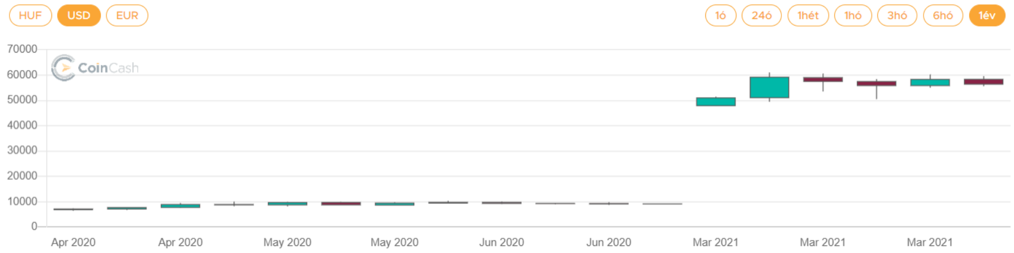

Figure 2. One-year Bitcoin rates in USD.

For the period under review, an increase in the number of ransomware-type attacks was observed, as well as a significant increase in the exchange rate of Bitcoin, the most commonly used cryptocurrency by attackers. On the one hand, the change in the exchange rate with the appreciation of Bitcoin has unfortunately intensified ransomware-type attacks, while at the same time, the consideration for the ransom demanded by the attackers in Bitcoin has multiplied. In the spring of 2020, BTC 1 was convertible at USD 7185, whilst the same in April 2021 represented USD 62,926. At the same time, this also means that although the amount set in Bitcoin during the extortion virus attacks did not change, companies and institutions still paid out orders of magnitude more to the extortionists to recover the data and prevent data leakage. There clearly seems to be a trend, but currently there are simply not enough data to prove this correlation.

In 2019, EUR 10.1 billion in ransoms were paid by victims within the EU, which is EUR 3.3 billion more than in 2018. The attacks detected showed an increase of 365% during the first 6 months of 2018 and 2019, while on average, victims paid ransoms in 45% of cases, while nearly half of them lost their data [2]. In 2018, the attackers still mainly targeted multinational companies, however, since 2019, the public sector and its cloud services which provide and manage education and healthcare have also gradually become targets. It is also a matter of concern that, according to 2019 reports, 66% of healthcare institutions in the EU have experienced such an attack [3].

The year 2020 estimates that extortion viruses caused a total of EUR 400 billion in damage within the EU. According to U.S. statistics, we see that in 2020, nearly 184 million attacks were detected [4].

Meanwhile, by 2020, attacks have become increasingly sophisticated. The length of the algorithms and keys used for encryption also make decryption difficult. The ransom is already often claimed in Bitcoin and the amount claimed also increases over time.

Attackers often put under pressure by not only taking data hostage, but also by threatening to publish or sell it.

In addition, the situation caused by the COVID-19 pandemic has led to a particular focus on healthcare institutions. The first registered death caused by an extortion virus occurred at a clinic in Düsseldorf on the 10 September 2020, while a widespread wave of attacks has swept across German healthcare facilities [5].

From an economic point of view, one of the most serious incidents in 2020 was the DoppelPaymer extortion virus attack on Foxconn, in which nearly 1200 servers were encrypted, 100 GB of data were stolen and 30 TB of backups were erased, while attackers demanded USD 34.7 million in Bitcoin [6].

To date, a REvil ransomware attack was the most critical in economic terms, targeting Acer in March 2021, where the actors were demanding the largest known ransom to date—USD 50,000,000 [7].

Further complicating the investigation of attacks and the quantification of the data is the fact that incidents such as these are often not reported by those involved. The reason is that the victims not only suffer material damage and their operation could become impossible, but the reputation of the organization may also be damaged. A further concern from their side could be a possible fine for violating the GDPR.

2.2. State-of-the-Art Research in Ransomware-Type Cyberthreats

There are several points of interest related to cybersecurity questions [8]. On the one hand, the detection of malicious servers is an important task, and on the other hand, the early detection of ransomware-type vulnerabilities is a key factor in the prevention of data loss.

In the international literature and news, as already mentioned in the introduction, we read more and more often about ransomware-type cyberattacks. The range of targets is widening, and there are almost no areas in the economic and administrative sphere where there would be no affected victims of such an attack. Unfortunately, the attacks show several trends that encourage IT security professionals to make a serious effort. One of these is that their attacks are becoming more sophisticated, with more and more organizations perceived behind them. Another issue is the elaborated preparation regarding the economic potential for exploitation of the victims attacked: this is indicated by the determination of the value of the ransom, which is far from random. The third and most problematic dimension of the attacks is the change in the nature of the targets. Unfortunately, there has been a proliferation of attacks on public institutions, schools and educational institutions, but the most severe have been on hospitals that save lives and provide healthcare. Attacks on hospitals are already subject to a completely different assessment, a much more serious act than previous attacks, and their reward is a threat to mass human life. The efforts of colleagues in the field of information security have been strongly motivated by this factor, and various technological developments, innovations, new methods for the development and improvement of intrusion detection and prevention systems are appearing almost continuously.

Yousaf et al. [9] investigated the possibility of preventing client-side attacks. It was found that the increase in the number of client-side attacks can be attributed, on the one hand, to the fact that server protection systems are much more advanced, and better and centrally monitored. Using as few resources as possible and in the shortest amount of time that attackers want to achieve their goal, this is obvious. The combined result of these two factors is that they want to enter the network environment by attacking the clients and then continue their activities there. The variety of client-side attacks also makes this path easier for attackers to navigate. As the authors noted in the article, in many cases, currently available systems focus on identifying malicious servers, and isolating clients from these servers is only a secondary consideration. Their proposed solution for detecting and preventing malicious servers is already blocking the malicious link at the gateway.

Cyberattacks, particularly ransom-oriented attacks, most often target Windows clients and servers. Ransomware itself is a member of the malware family, a malware that has caused significant damage to users and server owners over the last 4 years. Ransomware is designed to block access to data on victims' computers in some cases, but as a general mechanism of operation, for most of them, it encrypts data, documents, backups and databases. Unfortunately, decrypting and decoding the data is almost the same if it is not done by a professional, but even then, there is no chance that the data can be recovered 100%. The perpetrators of the attacks offer a decryption key for a ransom, as well as a decoder application that can be used to decrypt the files. On the behavioral mechanisms of different types of ransomware, Lemmou et al. [10] have reviewed three years of experience with 20 ransomware families based on more than 200 different ransomware samples.

In recent years, the COVID-19 pandemic period which started in 2019 and continues to this day has brought new impetus to this branch of cybercrime, with the rise of work from home and distance learning. In their study of authentication protocols, Shemita and Dhas [11] found that the activity of cybercrime and advanced persistent threat (APT) teams has increased, exploiting the position of vulnerable systems and individuals as targets. The authors found that there is a strong correlation between the epidemic situation and the increase in the number of targeted cyberattacks. It is also sad to note their finding that during the pandemic, the main victims of the attacks were healthcare organizations. A similar conclusion was drawn from Croke [12] and his research when he found that healthcare organizations, which are unfortunately frequent and ideal targets for attacks, often have outdated cyberdefense systems and are unable to provide staff with such training. The article states that management teams of healthcare institutions have stated that at least 75% of health institutions have recently been involved in some kind of cyberattack. Healthcare institutions and healthcare as a sector are already a common target for cybercriminals, where there is a high chance of a successful attack, since the challenged institutions are more willing to pay ransom than other sectors due to the nature of the data they handle. The data processed are suitable for personality theft, can lead to medical fraud, but also endanger patient safety.

In addition to analysis and detection, defense against ransomware attacks is obviously a similar topic in the research of cybersecurity professionals. Ayesha et al. [13] also present an analysis of ransomware-type malware in their work published in 2020, focusing on different Windows operating systems. The study explains that although the first ransomware came into operation as early as 1989, the Internet and IT had few users. Since then, this number of users has increased by several orders of magnitude. In the manuscript, the authors summarize the characteristics of more than 40 Windows-based ransomware attacks, their detectable features, their methods of infection, and the types of encryption. The main purpose of their survey and investigations was to determine how important it is for users of Windows computers to consciously protect themselves and understand how a ransomware attack affects the availability of their data and the operation of their systems. Mohammad [14] suggests protecting your entire system through monitoring your Windows system files as a promising way to defend yourself on Windows systems, as described in their 2020 study.

Prior to these manuscripts, as early as 2018, Hampton et al. [15] also reported in their study that the number of ransomware attacks had skyrocketed and caused significant damage in several industries, including the government sector. Their research examined 14 different pieces of ransomware for the Windows platform and compared their operational processes with the standard Windows API (application programming interface) calls and API calls that appear during a ransomware attack. In the study, the behavioral characteristics of the examined ransomware that could be specified through API calls were identified and presented.

Bander et al. [16] also published their study on the new challenges facing ransomware research in 2018. In many ways, the survey raised a new ransomware taxonomy. The study detailed the factors that led to successful ransomware attacks, and discussed research issues in ransomware defense options, including the analysis, prevention, detection and prediction solutions. This study also includes a brief discussion of current open issues and possible research directions.

In many cases, the news in the media does not help the defense or reconnaissance. On the one hand, users' fears are well founded, but without expertise they cannot find effective information on how to defend themselves. Victims of an attack cannot always identify a phenomenon, and only realize that their system has fallen victim when it is already too late. Aaron et al. [17] also published a study as early as 2018 that presented a methodology for detecting the then reverberating WannaCry ransomware through network interactions using reverse engineering. The logic of detection serves as a basis for the dynamic analysis of malicious programs that appear later, and the behavioral mechanisms discovered help increase the effectiveness of protection against them. The development of a defense technique against WannaCry ransomware was also developed by Lee et al. [18] and published in 2019.

Vulnerabilities in cloud-based technologies were analyzed by Zimba et al. [19], and then a Bayesian network-based weighted modeling procedure was used to model attack paths. An optimized algorithm-based solution was proposed that finds the shortest attack path based on key nodes and key edges, resolves the connection between equal-weight paths, and then classifies potential attacks according to attack time. To evaluate the model, the WannaCry ransomware attack was used in the research.

The analysis of the mechanism of action of malware and ransomware helps developers of intrusion detection (IDS) and intrusion prevention (IPS) systems. Chaabouni et al. [20] completed their study in 2019, which was based on the examination of the Dyn attack in 2016, which highlighted that the huge increase in the number of IoT (Internet of Things) devices opened up another platform for attacks. They state in their study that this is not only an issue that affects the security of IoT, but also threatens the entire Internet ecosystem, and that smart devices can become botnets. An example of this is the malware called Mirai, which attacked video surveillance systems and security camera systems, and paralyzed the systems with a DDoS attack. They also state that, recently, the vectors of the attacks have evolved in terms of their complexity, but there has also been a great deal of change and development in terms of their diversity. The study classified IoT security threats and the associated security challenges by examining and evaluating existing security techniques. The main emphasis was placed on network intrusion detection systems (NIDS), the review of existing NIDS system tools, analysis algorithms, and free and open source tools. Due to the variety of attacks, one of the directions of defense system developments is to break ransomware attacks at different points in attack cycles. As it stands, as Castiglione et al. [21] state in their study, none of them eliminate the vulnerability of static nodes in dynamic networks. This has raised the idea that ransomware attacks themselves can be traced back to a lack of digital social balance, where processes are dynamic and non-local, with data storage in static and local positions in systems used for social functioning. One possible solution for this is the non-stationary, dynamic storage of data, which is associated with a local encryption, thus ensuring a high degree of security between the speed of encryption and the right balance.

Alomary [22] found in their 2020 study that, unfortunately, ransomware is currently the most effective form of a cyberattack. The biggest challenge that ransomware poses is that in addition to diversity and a high number of pests, newer and newer versions are constantly appearing in the digital space in a very short time. As a shortcoming of the infrastructures to be protected, the authors mention the fact that although intrusion detection systems automatically alert the administrator, any action against intrusion must be manually performed by the administrator. The aim of their study was to present an IDS system that is present in the institutional infrastructure in the form of a service agent and functions behind the standard firewall as the first line of defense behind the network boundary as the first entry point.

A similar study was conducted in 2019 in which Keong Ng et al. [23] presented a new IPS system produced as a result of their research. Their concept was based on the development of a new kind of honeypot, which has incorporated more voting points compared to previous systems, with the aim of improving the detection rate and accuracy. The framework they propose has achieved high accuracy in ransomware discovery using machine learning models.

Kim et al. [24] also published the results of their research on the subject in 2020. On the one hand, it also numerically describes that 70% of cyberattacks were committed by ransomware attacks as early as 2017, and that this rate has only drastically risen since then. Their study points out that although many anti-ransomware applications are available, a large proportion of them, similarly to traditional anti-malware solutions, identify pests from code signatures based on a special list called blacklist. However, these solutions are ineffective against new pests that are not blacklisted yet. Alternatively, one can constantly monitor the software running on users' computers, monitor abnormal software processes, unusual API calls, or name and protect secure folders. However, due to their resource requirements, these solutions can greatly slow down the operation of the user system, lead to degraded performance and cause inconvenience to users. In their study, they presented a new solution for ransomware detection, blocking their operation, which is based on a whitelist-based access control. The advantage of this is that the whitelist-based system does not need a blacklist database and can prevent future ransomware attacks as well.

Cabay et al. [25] presented a software-defined network-based (SDN) detection approach based on the communication characteristics of ransomware. Based on the analysis of the HTTP traffic characteristics of two crypto virus families, it was concluded that HTTP message sequences and their content size provide sufficient information to detect threats. The results of their experiments confirmed that this approach can bring feasible and effective results in developments against ransomware attacks.

3. Materials and Methods

In the course of the research, the authors conducted several studies.

The first part of the investigation focused on actual news in media about the ransomware attacks and the actual state of the research was investigated in the ransomware detection and protection field. In this early phase of the research, the available anti-malware techniques which are available in commercial products were examined. This overview was presented in the previous section, in the Introduction, because this provided the main motivation and direction of the authors' further R&D works. The whole research and development process is presented in Figure 3. The structure of this manuscript follows this visually presented process for easier transparency and comprehensibility.

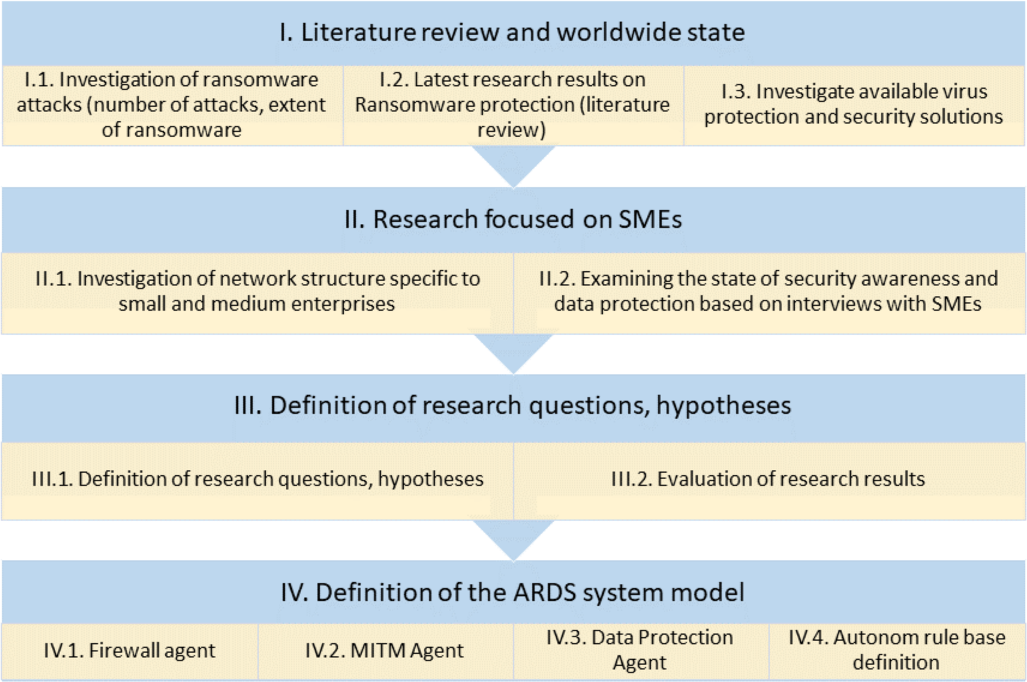
I. Literature review and worldwide state
I.1. Investigation of ransomware attacks (number of attacks, extent of ransomware
I.2. Latest research results on Ransomware protection (literature review)
I.3. Investigate available virus protection and security solutions
II. Research focused on SMEs
II.1. Investigation of network structure specific to small and medium enterprises
II.2. Examining the state of security awareness and data protection based on interviews with SMEs
III. Definition of research questions, hypotheses
III.1. Definition of research questions, hypotheses
III.2. Evaluation of research results
IV. Definition of the ARDS system model
IV.1. Firewall agent
IV.2. MITM Agent
IV.3. Data Protection Agent
IV.4. Autonom rule base definition

Figure 3. Visualization of research process.

The research aspects included the operational mechanism of the available systems: based on which the network and operating system events, the behavior of the systems are monitored, the type of database on which the malware is identified, as are the system memory, email traffic and network connection requests. The authors examined the existence, availability, and out-of-app accessibility of the log files. The complexity of the currently available systems and the possibility of their modular operation were also examined.

In the next phase of the research, possible network structures were analyzed. At this stage of the research, the structures of small office and home office (SOHO) systems, enterprise IT systems were measured and modeled by the authors. The structures were specifically identified on the basis of data collection in the form of questionnaire research and personal interviews among small and medium-sized enterprises. In the next phase of the investigations, based on the previously mapped network structures, devices and services available, the entry points that are present as a specific source of danger in these networks were determined.

In the fourth phase of this study, among the interviewees and respondents to the ransomware attack, the authors conducted a survey of what damage occurred after the attack and what steps they took to prevent a possible next attack.

One of the last steps was to perform the evaluation of the investigations.

Based on the results of the research, the authors proposed a network protection system model in which the behavior of identified access points, attack vectors, vulnerable service layers are constantly monitored. The proposed system appears as a monitoring and intervention layer on the network, and the intervention is controlled by an improved MITM Agent.

4. Research on Anti-Malware Techniques Available in Commercial Products

Today's advanced antivirus systems have been able to fend off increasingly complex attacks as malware evolve. It is critical for the security of IT systems that we can effectively protect end-user devices (workstations, mobile devices), regardless of the platform, as a significant part of serious security incidents stem from a user device (patient zero). If we take a look at the antivirus solutions from the largest manufacturers, we find that in addition to classic features such as pattern-based scanning or heuristic scanning, the following innovative solutions can also be found:

- Real-time download and email (anti-spam and anti-phishing) control module,
- Multi-layered ransomware protection with behavior-based learning ability,
- Sandboxing,
- WEB content and URL filtering,
- Proprietory software firewall,
- Proprietory VPN service,
- Secure DNS service,
- Webcam protection,
- Custom file and directory access layer,
- Network vulnerability analysis,
- Secure file deletion,
- Software update manager (installs security updates for the installed operating system and third-party applications),
- Powershell and malicious script blocking,
- Device management module (management of external storage, Bluetooth connections, Firewire devices),
- Anti-theft (device tracking),
- Screen lock-breaker,
- System backup,
- Privacy cleaner,
- Browser configuration review,
- Check and automatically restore system configuration (task scheduler, register entries, policy changes, etc.),
- Identity protection (browser session, keylogger, screen grabber, clipboard snooping protection),
- Secure browser (for banking, online shopping). [26]

In addition to the protection running on the above client devices, effective action against extortion viruses requires lateral movement in the network, the monitoring of operations on centralized storage, efficient logging, and the establishment of appropriate automatic backup systems.

5. Reseach Focused on SMEs

5.1. Questionnaire-Based Data Gathering about Network Structures and Security Awareness

The survey questionnaire is structured around several groups of questions. Some of these questions relate to the organizational structure of the company (activity, location, size), and others to the IT infrastructure of the organization (servers, network, endpoints, operating systems, cloud services, network security solutions), with a separate group of questions on security maturity (physical protection, IT security policies, data loss prevention) and IT operations security practices. In addition, a separate set of questions lists the security incidents to date and their consequences, as well as the current level of security awareness.

5.2. The Target Group of the Study

The primary target group for cybersecurity investigations was micro-, small- and medium-sized enterprises, where the total number of employees does not exceed 250. In terms of their number, this category of enterprises is currently present in the largest number in the Hungarian economic sphere, which also means that although their annual income does not approach that of large companies, they form a significant part of their annual GDP production. This study involved the managers, owners or IT managers of 46 small- and medium-sized companies. Due to the low number of items in the sample, the study cannot be characterized as significant, but they provide a comprehensive picture of the situation of small- and medium-sized companies with a general, non-IT security profile. The companies operate in various sectors, such as agro-food production, industrial production, health services, catering, beauty services (the full list of sectors is presented in the results section). The criteria for selecting small and medium-sized enterprises were as follows:

- The total number of employees of the company involved in the investigation does not exceed 250 people,
- The company is not headquartered or domiciled in the capital,
- It has a period of operation of at least 2 years,
- Willingness to participate in an anonymous survey,
- Undertaken to take part in a telephone interview.

5.3. Examination Method

The guided interview technique was used by the authors during the survey. With the help of this, a survey was conducted in the framework of individual, personal interviews in connection with the companies' IT tools and activities requiring IT support. During the interview, each interviewee answered 86 questions, which were received in the form of direct and indirect questions.

5.4. The Purpose of the Examination

The purpose of the study was to determine how much attention companies pay to the protection of their data, what internal regulations they have to ensure this, and how the current pandemic has affected their attitude towards remote work and home office conditions. The authors also examined the personnel composition of the companies in terms of suitability for the IT task, IT degree, qualification level, and the competencies of the person making decisions on IT issues within the companies.

A separate group of questions was aimed at mapping the daily administrative tasks that can be performed via the Internet, such as Internet banking and online invoicing.

During the interview, the authors asked questions about company executives or IT managers about the company's internal network architecture, the servers available on the network, and the network access policy.

The most important group of questions was about the experience of virus and ransomware attacks on the corporate network, how to handle the incidents. The question was whether there had been a virus attack on the company's network (either on the server side or on the workstation side) in the past year that had noticeable signs and consequences. In this regard, the authors examined the reactions of incident-stricken businesses to attacks, the success of recovery, the time lost from business continuity, the duration of full recovery, the degree of ransom required by attackers and the willingness to pay. With additional questions, the authors assessed the amount spent by companies on post-attack changes to improve network infrastructure security.

The questions also included control questions that have already been asked in order to eliminate the bias in the results caused by uncertain answers.

In the order of questions, in several cases, there are topic changes that were intentional. In doing so, the authors wanted to avoid the phenomenon of interviewees presenting themselves during a question process to show themselves under their best light, rather than bringing real information to the surface.

6. Interview Results and Defined Research Questions

During the evaluation of the results of the interviews, the authors came to the following conclusions:

1. Small and medium-sized enterprises shall, without exception, use services in the performance of their day-to-day administrative and administrative tasks which can only be performed via an online Internet connection. Such services include, for

example, electronic banking, the fulfillment of data provision obligations in electronic form, online invoicing, and online shopping.

2. When choosing network devices, the low purchase price and the possibility of installation that does not require expertise are important factors, therefore their networks do not have network devices that provide adequate protection and can be configured according to individual needs.
3. Based on the examined sample, it can be stated that the examined enterprises do not operate in the field of IT, but represent a wide range of economic production and service sectors (retail, industry, service, animal husbandry, crop production, food production, private and public health services, security hardware installation, hairdresser, beautician, tattoo studio, manicurist, pet food trade, education, administration services, etc.).

6.1. Correlation between the IT Qualification of Decision Maker and the IT Security Solution Presented

During the processing of the interview results, the authors sought answers to the following questions (research question, RQ):

- RQ1: Is there a significant correlation between the IT decision makers of the companies in the field of IT, their level of education and what IT security solutions are present in the network?

The company-specific data include the number of servers, endpoints and workstations (which later in the article is "number of computers", NoC) in the IT infrastructure and the level (shown in Figure 4), presence or absence of IT skills of the IT decision maker.

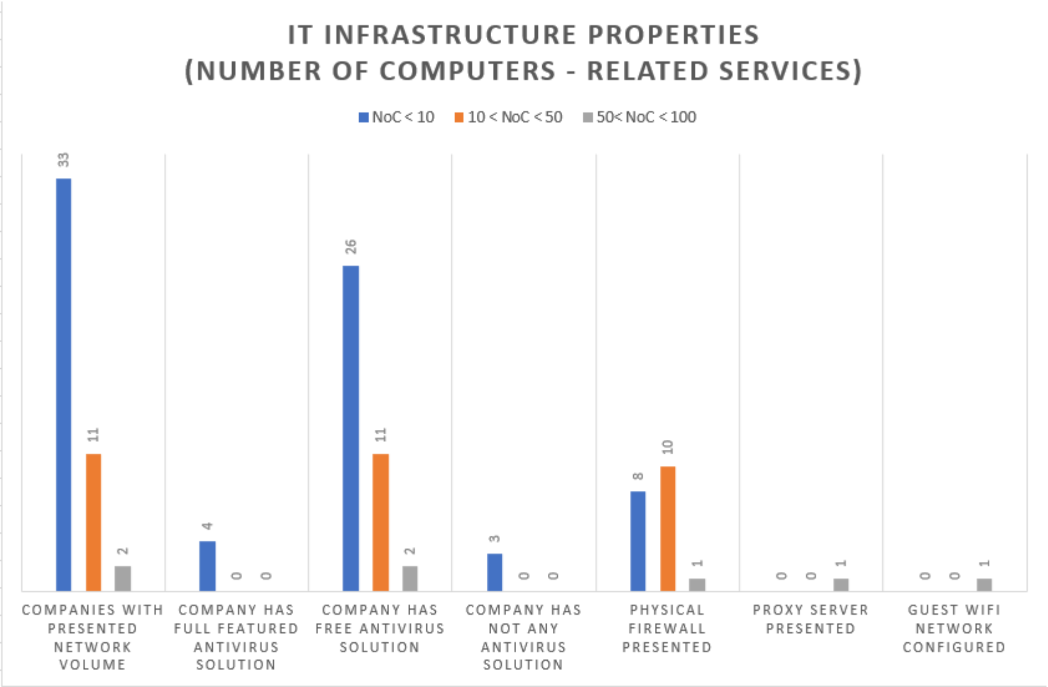

Figure 4. IT infrastructure properties for examined companies.

As it can be seen in Figure 5, the examined companies have different levels of protection.

Table 1 presents information on the companies' physical intrusion detection and presence of the physical firewalls on their networks. The results show that 67% of them have physical protection over their locations, but only 41% of the companies have a firewall on their computer network. A higher proportion of companies on the network have firewalls installed where the decision maker does not have an IT degree. This statement proves that the hardware protection of networks and IT infrastructures is not closely related to the IT skills of the decision maker.

Table 1. Relation between IT grade of decision maker and presented protection level of the company.

Resp. IT Grade/Basic Protection Level	No Physical Intrusion Protection	Physical Intrusion Protection Presented	Physical Firewall Not Presented	Physical Firewall Presented
Higher grade, specialized	2	5	4	3
Higher grade, not specialized	4	13	8	9
Secondary grade, specialized	1	1	1	1
Secondary grade, not specialized	8	12	14	6
Number of companies	15	31	27	19
Percent(%) of 46	33%	67%	59%	41%

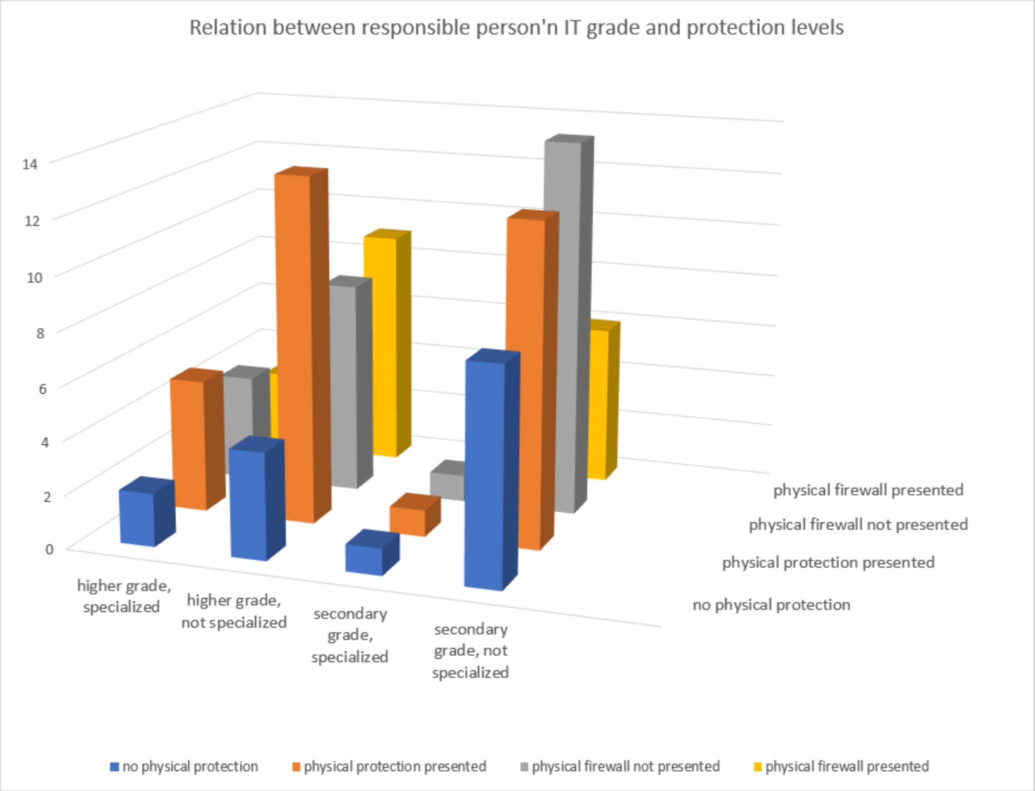

Figure 5. Correlation between the companies' decision makers' IT skills and the presented security state.

The next issue is concerned with the overall headcount of the company and the number of people working with sensitive data within the firm. Figure 6 presents the number of employees at the examined companies, and especially the number of employees working with sensitive data (e.g., employees' personal data, contracts, salary data). With the use of quick classification, the companies were divided into four clusters, based on their manpower. This classification is equal to the classification based on the number of computers at the company.

The examined companies include companies with 2–250 employees, which is typical among small- and medium-sized companies. The number of companies with a similar number of employees in Hungary today (micro-sized enterprises that employ up to nine people make up the majority of SMEs in Hungary) is approximately 549,000, and the estimated number of small and medium-sized enterprises (SMEs) in the European Union was approximately 25.1 million in 2018 [27,28].

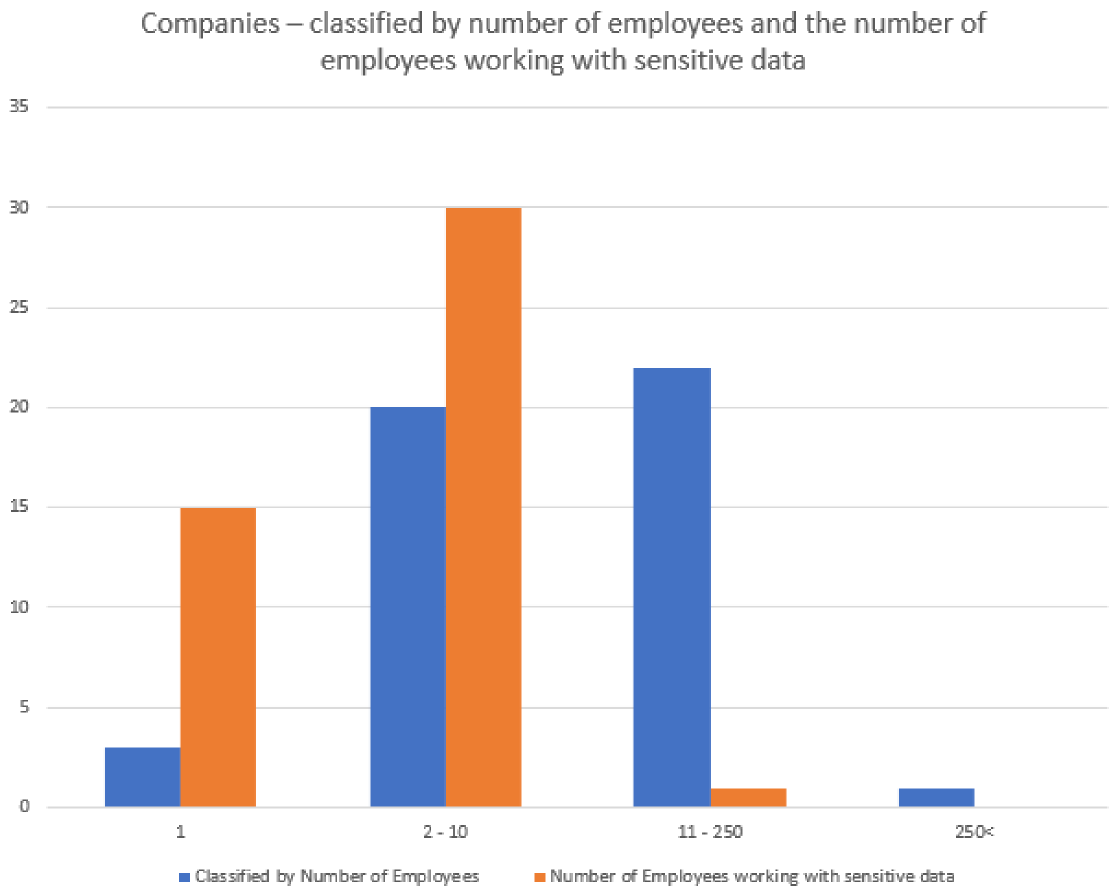

Figure 6. Number of employees at the examined companies.

As mentioned earlier, the survey cannot be considered as a representative sample due to the small number of participants, however, it covers a wide range of SMEs, as participants have similar characteristics, so the results show a realistic picture.

Since all the companies surveyed carry out online activities in the performance of their administrative tasks, the next research question focuses on virus protection solutions.

6.2. Proportion of Free and Full-Featured Protection Solutions

- RQ2: Do all companies have a software security solution, and if so, is this a free version with limited features, or have commercially installed subscription-based, full-featured solutions on their devices?

All of the surveyed companies carry out online activities: advertising their own activities, operating a webshop, online banking, online invoicing, among other electronic administration tasks. Nevertheless, 79% do not have a firewall, 91% use a software antivirus solution, and 80% have installed free antivirus software on their IT system. Among the respondents, 91% had previously been victim of a virus attack and 48% had also been the victim of a ransomware attack. Following the attacks, 39% of companies did not change their previous hardware or software protection, however, 76% said they would be willing to implement a cost-effective, complex IT security system at their company. Figure 7 illustrates the comparison of the aforementioned data.

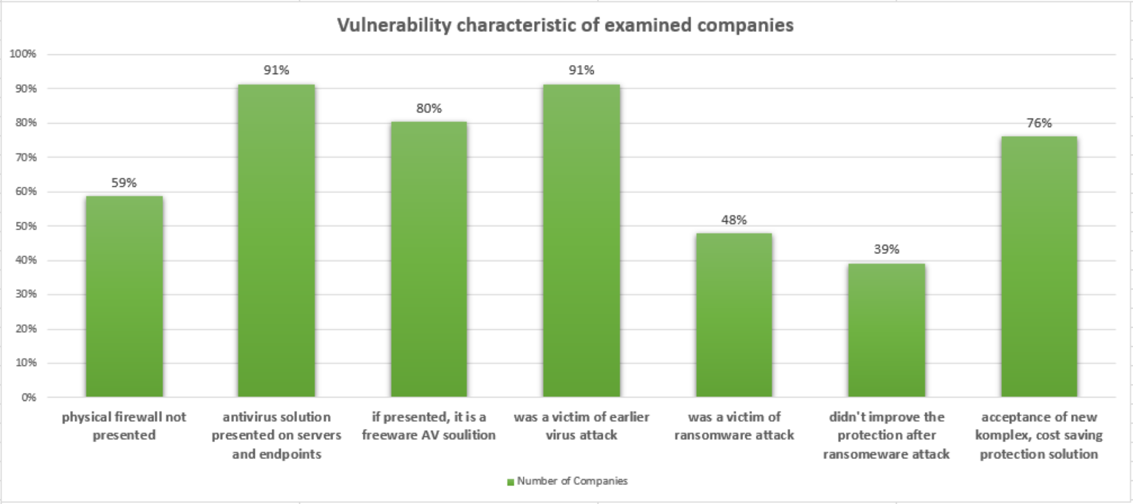

Figure 7. Vulnerability characteristics of examined companies.

Closely related to question RQ2 is the following research question.

- RQ3: What is the role of the IT decision maker in the selection of the virus protection solution and what relation does this have with their level of existing professional qualification in the field of IT?

In examining the IT skills of decision makers, the authors sought answers to the contexts that, in the presence or absence of IT skills, appear as an impact through decision making with the presence or absence of applied security solutions.

The results obtained by examining the relationship in question are also illustrated in Figure 8. The next study was the number of virus attacks suffered and the virus protection solution available in the year preceding the interview. The result of this is shown in Figure 9.

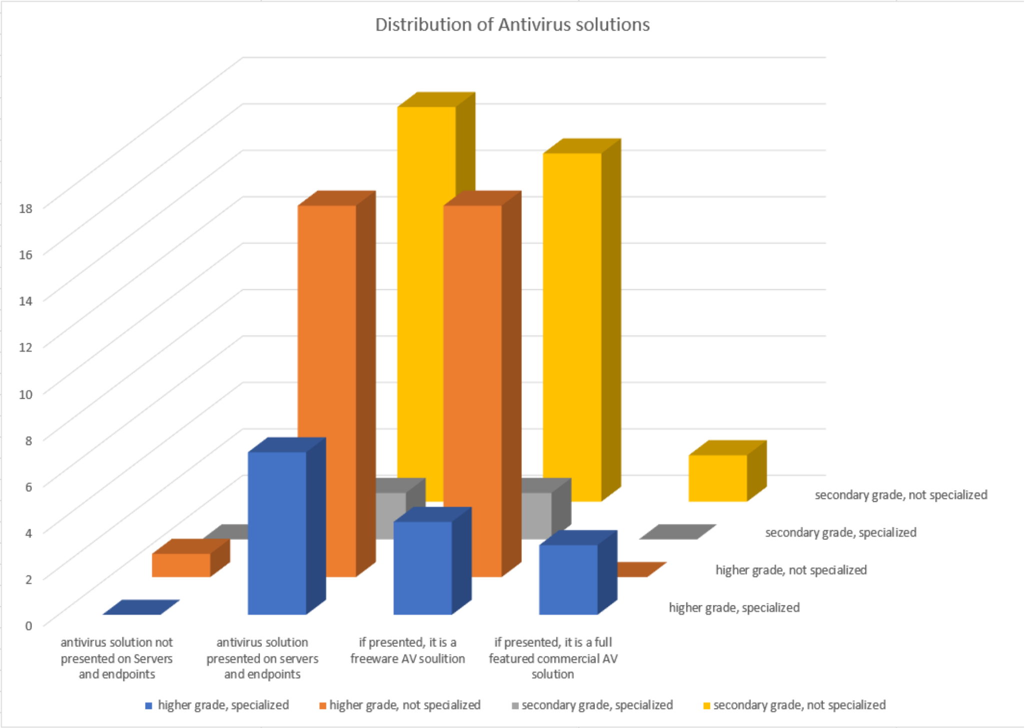

Figure 8. Present AV solutions in companies related to the decision makers IT grade.

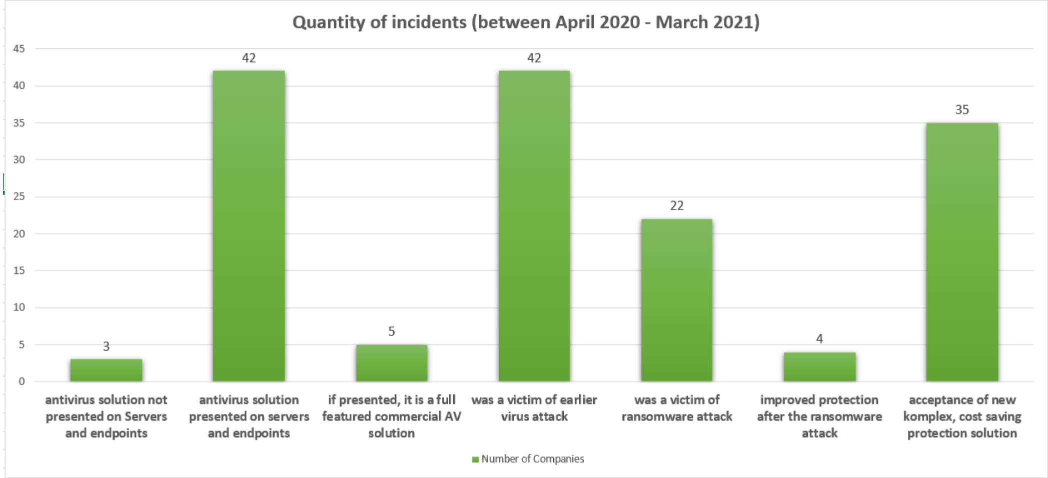

Figure 9. Virus and ransomware attacks in the year preceding the interview.

Only five of the companies surveyed had a professional, commercial virus protection solution installed on the system, and although a large number, 42 out of 46, were already victims of a virus attack, only four companies made changes to the IT system to increase security.

A large amount of data was gathered during the interviews, and of course, the evaluation is not limited to the above questions.

The main purpose of this manuscript was to present an improved, model-based ransomware protection system; therefore, from the results of the interviews, only the closely related criteria supporting the development and justifying the general need are discussed below.

6.3. Willingness to Accept a Cost-Effective IT Security Solution for the Small- and Medium-Sized Enterprises Surveyed

The primary purpose of a ransomware protection system is to thwart a ransomware attack. In addition to the available protection solutions, the questions of the interviews focused on whether the interviewed companies had fallen victim to any virus attack, ransomware attack, and if so, how this was handled, and how it affected the company's business and operations. Based on these, the following research question was formulated:

- RQ4: What is the willingness of micro-, small- and medium-sized enterprises to adopt a solution that greatly automates and elevates the protection of IT infrastructure in the company's system, even without special expertise?

Among the companies surveyed, 91% were already victims of a virus attack, and the rate was very high, 48%, for those who were already victims of a ransomware attack.

Barely 20% of companies that have suffered a ransomware attack have taken steps to ensure a higher level of security for their IT system after the attack.

In the case of the interviewed companies, it was observed that in many cases they were not aware of the significance of an attack and the extent of the damage, and in many cases, the company does not have a colleague with IT skills, or a system administrator, or system operator that could also conduct a proper procedure.

The survey also found that a significant proportion of companies would be willing to invest in a low-budget, automated, hardware and software-enabled, complex solution, in addition to existing widely available antivirus and other IT security solutions, and working with them would increase the security of the corporate network, servers and workstations.

In the next subsection, an examination of the IT security of networks is presented, which was aimed at detecting the most typical attackable elements.

7. Attack Vectors, Identified Entry Points on Networks

Interviews revealed that the companies surveyed are either peer-to-peer machines and have simple small office/home office (SOHO) networking tools, which in many cases are not properly configured due to a lack of appropriate expertise.

Another typical network topology is when a broadband inbound connection is available to access the Internet. The machines on the internal network access Internet resources through a network router and some non-configurable Layer2 switches, and the internal network has contiguous machines, one or some of which provide access to files and databases through simple sharing.

The following is a typical topology where a dedicated server machine with a server operating system that serves the workstations on the network is located on the internal network. The mentioned topology sample is presented in Figure 10.

It is characteristic of all network topologies in the examined cases that in most cases, the client machines are connected to the network peripherals, such as network printers, copiers, scanners and shared folders without authentication. The next observation is that even if there is a server on the network, the server usually acts as a simple database and file server, there is no domain control service, no lightweight directory access provider (LDAP) server installed.

In addition to all these shortcomings, workstations and servers often do not have adequate virus protection.

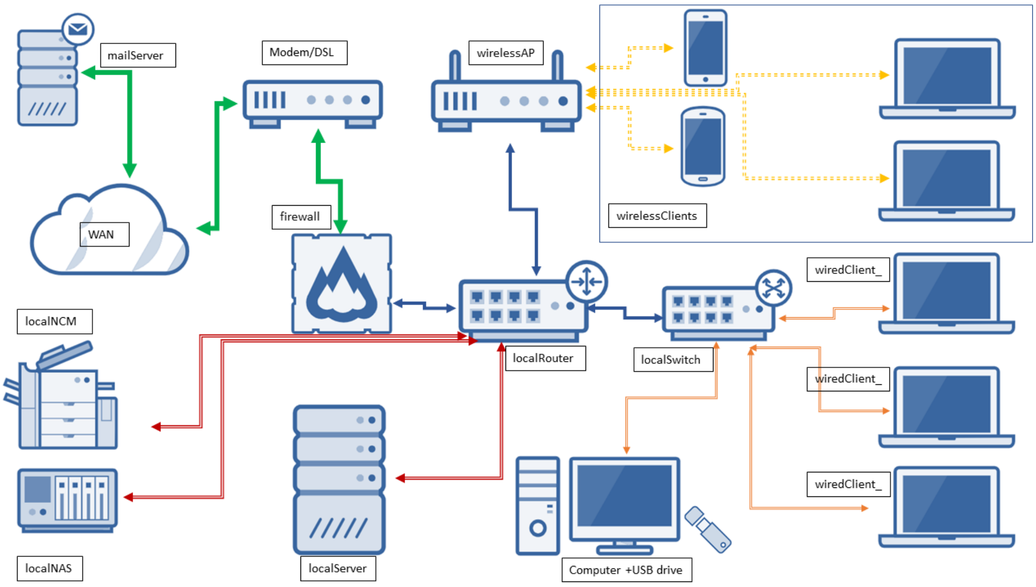

Figure 10. Typical network topology used by micro- and small-sized companies.

By reviewing the attack vectors, it can be stated that while in 2019 the attacks were mostly carried out through infected files (application installers, documents, patches), by 2020, the threat landscape had changed dramatically. Ransomware were mostly spread using phishing emails. A good example of this approach is the Zeppelin ransomware, in which beside a seemingly harmless invoice embedded in an MS Word document as an image, VBA macros will be running in the background. These types of attacks can be effectively prevented by using an appropriate antivirus solution, spam filter, macro security and by educating users on information security awareness. Another common form of ransomware attacks is when the infrastructure is compromised through exposed RDP services. This typically occurs when the system is outdated/unpatched or poorly configured. In many cases, access is gained with login credentials purchased on the Darkweb (approximately 15 billion RDP credentials available, priced at 20 USD/account) or obtained during brute force attacks. Publishing the RDP service on the default port increases the likelihood of an attack by 37 percent, however, two-factor authentication and enforcing a strict password policy can drastically reduce this risk. A further widely used technique is when the attacker obtains access through vulnerable VPN services (e.g., earlier versions of Pulse Secure and Fortinet). In these cases, regularly updating one's services and changing one's previous login credentials may be a solution.

8. The Defense Model

In order to obtain valuable data by using ransomware, the attackers either have to infect one of the clients in the network (e.g., phishing emails, malware infection) and from there, move forward to obtain access to sensitive data, or they need to directly compromise the exposed server (e.g., exploiting the vulnerabilities of the protocols and security flaws of RDP, VPN).

Remote access to and control over the infected environment occurs via the connection established with the attacker's command and control (C2) infrastructure. This communication process, in the case of infected clients, either starts with a DNS query or with direct IP (hardcoded IP) access, so it is possible to continuously monitor any suspicious DNS queries, direct IP accesses, unusual inbound traffic and large volumes of outbound data movement on the primary DNS server and on the perimeter firewall. During lateral movement in the local network—assuming a centralized data storage architecture, in addition to reconnaissance and compromising further vulnerable devices—the attacker (a bot or human) also scans available network drives. Modification, encryption, deletion and transmission of data to remote locations results in significant data traffic and a large number of file operations (it is loud), which may be clear indicators of an incident (IoC).

The advanced antivirus solutions available on the market mainly focus on fending off infections and on preventing the execution of malicious code. The aim of the present research was to determine how active malware already infiltrated into the network can be detected on client-independent points (honeypotting, integration checking, log analysis, packet inspection, etc.), while ensuring safe data storage (snapshotting techniques using, i.e., ZFS) and automated backup (e.g., iSCSI, rsync). Advanced malware tend to use a "living off the land" (LotL) technique and access data stored on file servers via commonly used protocols.

By means of monitoring the communication using the man-in-the-middle (MITM) technique between clients and file servers, it is possible to look for anomalies, suspicious patterns of action or data transfer peaks in order to generate alert triggers.

The schematic model of the proposed method and system can be seen in Figure 11.

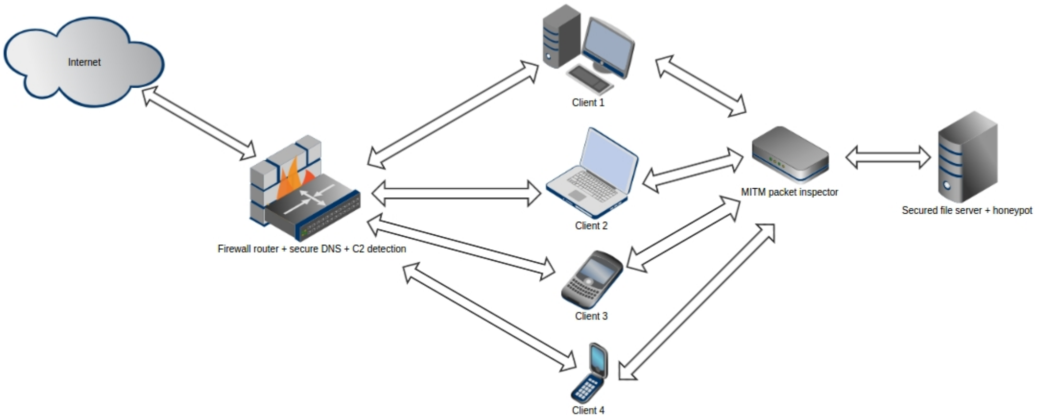
Internet
Client 1
Firewall router + secure DNS + C2 detection
Client 2
MITM packet inspector
Secured file server + honeypot
Client 3
Client 4

Figure 11. Network topology of the ARDS model.

A significant proportion of ransomware running on Windows platforms accesses network drives in alphabetical order. Based on this, honeypot network shares (with drive letters chosen from the beginning or end of the alphabet) can be created, which seemingly contain valid, freshly generated data that fit into the profile of the given organization.

However, their content is fake and their sole purpose is to enable daemons monitoring the drives to log/report any file operation (access, read, write, rename, delete). Obviously, users should be informed in advance that they should not use the "fake network drives" in any way. Another opportunity offered by this method is that by limiting the speed of file operations in various ways (e.g., IO limit, old IDE drives, large amounts of small files), the progress of malware can be delayed, thus additional time can by gained for incident response.

The outlined operating mechanism is directly independent of the user, and it is suitable for the early detection of dangerous processes at many points in the network at service layers. Of course, the diversity of the protection system also includes the preliminary examination and classification of heterogeneous systems. Unlike the systems classifying network infrastructures from the current IT security point of view, the protection system model is based on a weighted assessment in which the vulnerability of the systems is calculated in a system-adaptive way. In the next subsection, the classification, system protection rating, and a model of the complex system providing protection are presented.

ARDS—The Proposed IDS/IPS Model

The operation model of the proposed ransomware protection system is shown in Figure 12. An essential feature of the system design is that it performs multi-step filtering, classification, and analysis in real time. Incoming requests from the Internet go through a pre-qualification, as a result of which they are placed in event sets. These event sets are classified based on the inbound port, source IP address, and network delimiter device (usually router and/or firewall) rules based on the probability of the threat.

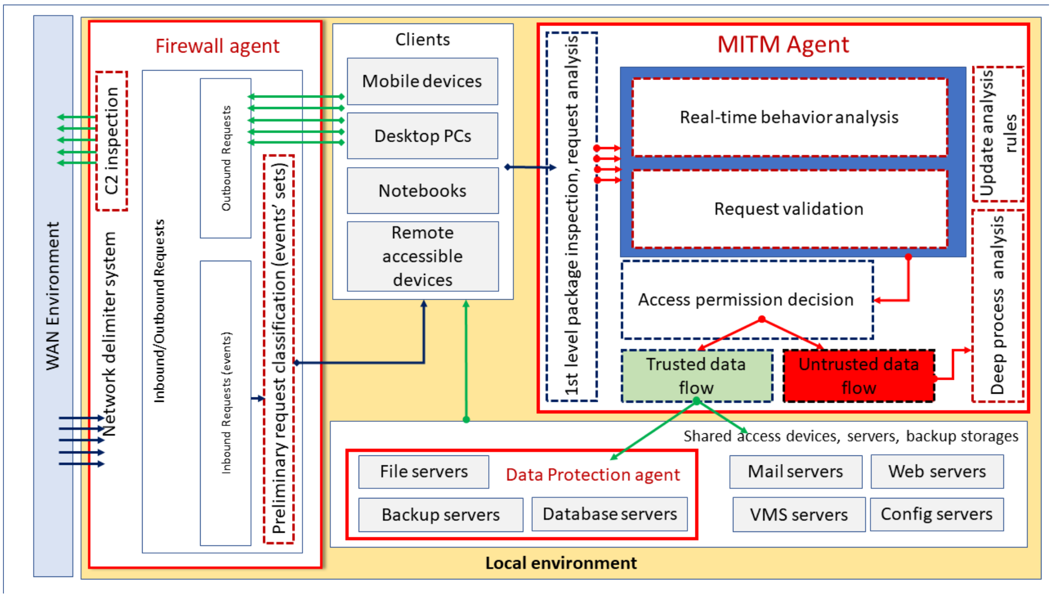

Figure 12. Operation model of autonomous ARDS.

The system hosts the MITM Agent, which is responsible for protecting the shared resources available on the network. The first step is a packet scan on the agent, followed by a real-time behavior scan and request/event validation. The reliability decision is then made. Events and requests classified as trusted by the agent are forwarded to the server corresponding to the original request. Requests that are marked as untrusted are further analyzed using the additional parser components of the agent. As a result of the analysis, the rules system of the autonomous agent is updated.

Protecting backup servers, file and database servers is a key task for the proposed ARDS. In the server layer, the data protection agent represents another line of defense using a ZFS file system, which is able to recover data from time-stamped snapshots.

The next element of the protection strategy of the proposed ARDS system is the inspection of the outbound data flow from the internal network to the Internet. With the help of the Firewall agent, the C2 activity can be detected based on the analysis of the outgoing network traffic.

In this way, ARDS is a complex system that can implement autonomous defense in several steps, at special intervention and access points, in the application and service layers, and it complements other protection technologies already available in the network.

In addition to the formal description based on the planned ARDS model the validation of the operation takes place in the next phase of the research, followed by the physical implementation and testing in a live environment. The designed and modeled system is able to work with already available software solutions, hardware solutions, and as a standalone, autonomous device, physically installed on the internal network, can automatically provide protection for servers storing and providing critical business data.

9. Results

As detailed in Section 6, the survey of SMEs provided important information on their current IT security situation. In the course of the survey, we mainly answered questions that show the existing information protection strategy in the companies, and in comparison with this, we focused on the events of the virus attacks and extortion virus attacks that have already taken place.

The number of employees in the enterprises was one of the analyzed data. Among the examined SMEs, on the one hand, the number of employees was limited in terms of the SME classification of a company, and on the other hand, we received information on the proportion of employees who handled the company's data to be protected in terms of IT security (data ensuring the business continuity of the enterprise, data forming the basis of data provision related to business activities, personal data). The headcount data were categorized into four groups, which are characteristic of the size of the SMEs studied.

Table 2 also shows numerically summarized data on how many of the responding companies belong to each size category. The second row of the table shows the number of cases in which the majority of employees have access to the data to be protected by companies during their daily work. The vast majority of the surveyed companies employ 2–10 employees, which was typical of 30 companies. The number of companies with one employee is also low in proportion, which means three companies out of the respondents.

Table 2. Number of companies/employees with access to sensitive data.

	One Person Business	Number of Employees between 2 and 10 People	Number of Employees between 11 and 250 People	Number of Employees over 250 People
Number of companies	3	20	22	1
Employees working with sensitive data	15	30	1	NA

In comparison, in one-third of the enterprises, a maximum of one employee has access to the company data to be protected, whilst in the case of 30 companies, 2–10 people, and in one case, more than 10 employees have access to the data to be protected.

A characteristic issue for the activities of enterprises in the survey was to examine how many of the companies have foreign business partners and how many enterprises have foreign sites.

According to Table 3, only three of the 46 surveyed companies have a foreign location, but 21 of the surveyed companies have foreign business partners, as it can be seen in Figure 13. This issue is an interesting achievement in terms of communication on the Internet, electronic administration, and the remote availability of the company's data to be protected.

Table 3. International business interest, business contacts.

	Yes	No
Company has foreign partners	21	25
Company has foreign office	3	43

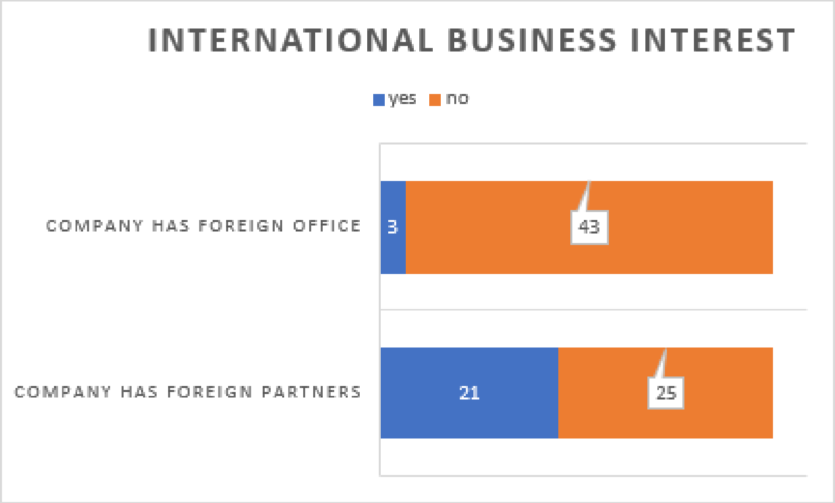

Figure 13. International business contacts.

The next result that the studies show is that 35 of the businesses allow home office work (Case A in Table 4). In 16 of these 35 companies, the use of a corporate email account is not regulated, and private use is also allowed (Case B in Table 4). Of the 35 companies mentioned, 17 have been victims of a recent ransomware attack (Case C in Table 4). Among the victimized businesses, there were 11 businesses where the use of a corporate email for private purposes was allowed along with the home office option (Case D in Table 4). These discovered relationships are illustrated in Table 4 and in Figure 14.

The cases examined:

- Case A: Home office enabled for employees,
- Case B: If home office is enabled, corporate email can be used for private purposes,
- Case C: In case home office is enabled, the company is a victim of ransomware attack,
- Case D: In the case where home office is enabled AND corporate email can be used for private purposes, the company is a victim of ransomware attack.

Table 4. Relation between enabled home office, private use of corporate email and ransomware attacks.

Home Office/Private Use of Corporate Email	Case A	Case B	Case C	Case D
Number of companies	46	35	35	16
Number of matched cases	35	16	17	11

Examining the above correlations and the results of the interviews presented in Section 6, it became clear that currently, there is no conceptual solution on the market, and that by compensating for regulatory errors and effectively preventing their negative effects, it is able to provide existing protection. In addition to necessity, the results of the interviews clearly show that there is a need for an autonomous but cost-effective solution. In the course of the research, we identified the critical points of the networks used in the daily business and work of SMEs, where the presence of viruses can be indicated and damage can be prevented independently of potentially infected clients and compromised servers.

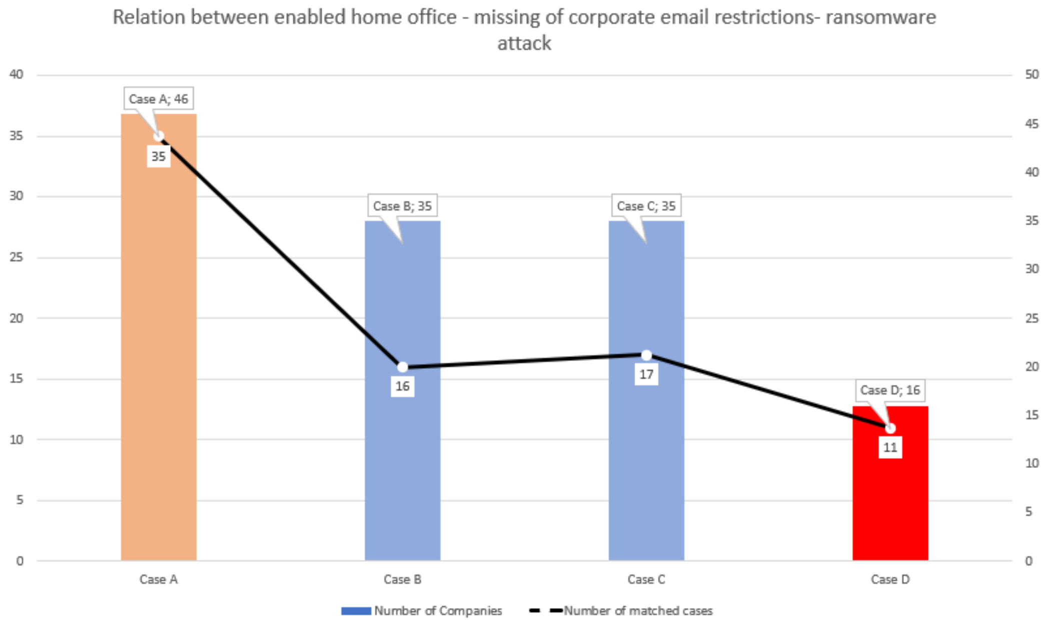

Figure 14. Correlation between the corporate policy for home office, corporate email use and ransomware attacks.

10. Discussion

Examining the specifics of companies and analyzing the nature and frequency of ransomware attacks, it has become clear that while there are advanced, high-performance antivirus solutions, user carelessness still leaves room for extortion virus attacks. For this reason, it is necessary to develop and implement a protection model with a similar functionality, but operating differently from the traditional strategy. The protection solution must take into account that user behavior is inherently a potential source of danger, which can be caused by (but not limited to) the following:

- A vulnerable external device can be accessed by an employee during daily work in the corporate network,
- The AV software is turned off intentionally or through carelessness (including ignorance),
- The use of weak passwords for convenience or other personal reasons,
- Security updates are not installed by the user due to time and Internet data usage problems,
- Legacy systems based on outdated technologies are used in some companies,
- The user does not recognize the presence of malware on the computer in time,
- The company does not have an IT specialist.

In addition to the dangers arising from user presence and intrusion, we should not lose sight of the aspects that become critical when a virus attack has already occurred and the company's operation and social image may be jeopardized by the damage, data loss or data corruption.

The key issues here include the theft of data, as is typical of ransomware attacks, and then preventing its sale on the Darkweb. In line with this requirement, the proposed ARDS system must be able to react to changes in data traffic from the internal network to the Internet. This is the responsibility of the firewall agent in the ARDS model, as this is the point where outbound traffic or C2 activities can be effectively monitored. In the case of early detection, stopping an ongoing data leakage can also be a good result, if it mitigates unauthorized access to the data by attackers.

In addition, the ARDS system should be able to recover corrupted data in all cases if early detection failed or the operation of the ransomware could not be prevented for any other reasons. In the ARDS model, the data protection agent serves this purpose. Its task is to use the backups stored on the ZFS file system to restore the contents of the disk to any earlier point in time, taking advantage of the operational features of the file system. However, this requires that the Data Protection Agent backup system uses this ZFS, and this cannot be replaced by another file system, such as Ext, Raiser Fs, or NTFS.

Snapshot, cloning, and replica creation are the strongest features of ZFS. Snapshots are used to create copies of entire file systems or selected volumes at a given time, as cloning is simply used to create a duplicate data set, and replication can be used to copy data either from one repository to another repository on the same machine or to another repository. Ext, NTFS, HFS+, or FATx file systems do not provide the ability to take a time-stamped disk image snapshot, which is the basis for recoverability.

The proposed ARDS system should also have an additional line of defense against malicious activities, also resulting from user interaction. This is represented in the model by the MITM Agent, whose highlighted task is to protect the servers on the network. The interviews also revealed that a malware enters the internal network directly through privately used business email accounts or on a corporate laptop used in one's own home environment, and the process is currently not handled with due care in the corporate environments studied.

The task of the MITM Agent implementing server protection is to analyze the requests sent to the servers, to analyze the real-time behavior, to validate the requests, and to decide on the serviceability of the requests. The MITM Agent can divide requests into two categories. On the one hand, MITM Agent can mark a process as trusted, which can then communicate with the server designated as the target of the request in the usual way, but it can also mark the process as untrusted. If a process receives an untrusted flag, the MITM Agent must perform additional analyses, a deep process analysis, and then, as a result, update its own set of rules for efficient operation. In this way, the system also becomes suitable for filtering out and identifying malicious processes that were not previously known, and the Agent can add behavioral characteristics to its rule system that will later describe the identified process characteristics as malware-specific behavior. For detailed information, see the supplementary data.

11. Conclusions

Summarizing the results achieved in the research phase and the position expressed in the discussion part, it can be stated that the current trend is that there is a great need for a tool that can fill the gaps left by the financial difficulties of complex security systems, and that can work with and complement existing security solutions to avoid situations where, for whatever reason—but mostly the human factor—we find ourselves in the crosshairs of a ransomware attack (e.g., antivirus turned off, unknown hardware connected to the network, RDP).

The aim was to plan and develop an infrastructure that can protect data even in the event of ransomware attack, that can signal/warn about any potential attacks and can be built and maintained in a cost-effective manner. As the attack strategies of ransomware are constantly changing and becoming more and more sophisticated, it will be a challenging task to objectively assess the effectiveness of the system. Testing will take place on an infrastructure consisting of physical workstations, virtual machines and containerized services, by using clients infected with the most common types of ransomware. In order to achieve proper efficiency, the system must be able to recover encrypted or deleted data, or data made unusable without any arising problems in a smooth way, and must indicate the presence of malicious code with high accuracy (C2 server, file operations, outbound data flow, data traffic leaving the network).

Based on the survey of small and medium-sized companies, it can be clearly stated that there is a need for an improved, cost-effective anti-ransomware solution that specifically addresses the interests of this group of users. Implementing the solution is an increasingly urgent task, as cybercrime poses more and more challenges to users on a daily basis—all this compared to the fact that data protection has become a primary task in business and private communication and in the day-to-day operation of online space. The first step in the defense against sophisticated ransomware-type attacks is the implementation of the presented automated solution, which is able to detect and analyze rapidly changing attacks with special automation and protect the vulnerable infrastructure.

Supplementary Materials: The following are available online at https://www.mdpi.com/article/10.3390/app11136070/s1.

Author Contributions: Conceptualization, V.S., G.A. and Á.D.; formal analysis, V.S., G.A. and Á.D.; investigation, V.S. and Á.D.; methodology, V.S., G.A. and Á.D.; project administration, V.S. and Á.D.; resources, V.S. and G.A.; supervision, V.S.; validation, G.A.; writing—original draft, V.S., G.A. and Á.D.; writing—review and editing, V.S., G.A. and Á.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article or supplementary material.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

COTS	Component/commercial off-the-shelf
IDS	Intrusion detection system
IPS	Intrusion prevention system
APT	Advanced persistent threat
MITM	Man in the middle
C2	Control and command
GDPR	General Data Protection Regulation
ZFS	Zettabyte file system
LotL	Living off the land
IoT	Internet of Things
IoC	Indicators of an incident
RDP	Remote desktop protocol
DNS	Domain name system
iSCSI	Internet small computer systems interface

References

1. CoincashEU. Bitcoin Yearly Rate. Available online: https://hu.coincash.eu/arfolyam/btc/usd/1y (accessed on 25 April 2021).
2. Lemnitzer, J. Ransomware Gangs Are Running Riot—Paying Them Off Does Not Help. Available online: https://theconversation.com/ransomware-gangs-are-running-riot-paying-them-off-doesnt-help-155254 (accessed on 25 April 2021).
3. Vumetric. More than 66 Attack in 2019. Available online: https://www.vumetric.com/statistics/more-than-66-of-healthcare-organizations-experienced-a-ransomware-attack-in-2019 (accessed on 25 April 2021).
4. Groot, J.D. A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time. Available online: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time (accessed on 25 April 2021).
5. Ruckwied, D. Cyber-Angriff Mit Todesfolge an der Uniklinik Düsseldorf. Available online: https://www.dsin-blog.de/2020/10/14/cyber-angriff-mit-todesfolge-an-der-uniklinik-duesseldorf/ (accessed on 25 April 2021).
6. Haworth, J. Hackers Demand $34.7 Million in Bitcoin after Ransomware Attack on Foxconn. Available online: https://portswigger.net/daily-swig/hackers-demand-34-7-million-in-bitcoin-after-ransomware-attack-on-foxconn (accessed on 25 April 2021).
7. Abrams, L. Computer Giant Acer Hit by $50 Million Ransomware Attack. Available online: https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/ (accessed on 25 April 2021).
8. Sunde, N.; Dror, I.E. Cognitive and Human Factors in Digital Forensics: Problems, Challenges, and the Way Forward. *Digit. Investig.* **2019**, *29*, 101–108. [CrossRef]

9. Yousaf, B.K.; Yousaf, M.; Jalbani, A.H.; Batool, K. Detection of Malicious Servers for Preventing Client-Side Attacks. *Mehran Univ. Res. J. Eng. Technol.* **2021**, *40*, 230–240. [CrossRef]
10. Lemmou, Y.; Lanet, J.L.; Souidi, E.M. A behavioural in-depth analysis of ransomware infection. *IET Inf. Secur.* **2021**, *15*, 38–58. [CrossRef]
11. Pranggono, B.; Arabo, A. COVID-19 pandemic cybersecurity issues. *Internet Technol. Lett.* **2020**, 6. [CrossRef]
12. Croke, L. Protecting your organization from e-mail phishing and ransomware attacks. *Aorn J.* **2020**, *112*, 10–12. [CrossRef] [PubMed]
13. Naseer, A.; Mir, R.; Mir, A.; Aleem, M. Windows-based Ransomware: A Survey. *J. Inf. Assur. Secur.* **2020**, *15*, 107–125.
14. Mohammad, A.H. Analysis of Ransomware on Windows platform. *Int. J. Comput. Sci. Netw. Secur.* **2020**, *20*, 21–27.
15. Hampton, N.; Baig, Z.; Zeadally, S. Ransomware behavioural analysis on windows platforms. *J. Inf. Secur. Appl.* **2018**, *40*, 44–51. [CrossRef]
16. Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Comput. Secur.* **2018**, *74*, 144–166. [CrossRef]
17. Zimba, A.; Mulenga, M. A Dive Into the Deep: Demystifying Wannacry Crypto Ransomware Network Attacks via Digital Forensics. *Int. J. Inf. Technol. Secur.* **2018**, *10*, 57–68. [CrossRef]
18. Lee, S.; Kim, H.K.; Kim, K. Ransomware protection using the moving target defense perspective. *Comput. Electr. Eng.* **2019**, *78*, 288–299. [CrossRef]
19. Zirnba, A.; Chen, H.; Wang, Z. Bayesian network based weighted APT attack paths modeling in cloud computing. *Future Gener. Comput. Syst. Int. J. Esci.* **2019**, *96*, 525–537. [CrossRef]
20. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2671–2701. [CrossRef]
21. Castiglione, J.; Pavlovic, D. Dynamic Distributed Secure Storage Against Ransomware. *IEEE Trans. Comput. Soc. Syst.* **2020**, *7*, 1469–1475. [CrossRef]
22. Alomary, F.O. Defend Against Ransomware Detection Using Intrusion Detection System (IDS). *Int. J. Comput. Sci. Netw. Secur.* **2020**, *20*, 11–16.
23. Keong Ng, C.; Rajasegarar, S.; Pan, L.; Jiang, F.; Zhang, L.Y. VoterChoice: A ransomware detection honeypot with multiple voting framework. *Concurr. Comput. Pract. Exp.* **2019**, *32*, 29. [CrossRef]
24. Kim, D.; Lee, J. Blacklist vs. Whitelist-Based Ransomware Solutions. *IEEE Consum. Electron. Mag.* **2020**, *20*, 22–28. [CrossRef]
25. Cabaj, K.; Gregorczyk, M.; Mazurczyk, W. Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. *Comput. Electr. Eng.* **2018**, *66*, 353–368. [CrossRef]
26. Ellis, C.; Turner, B.; Williams, M. Best Ransomware Protection of 2021: Free and Paid Decryption Tools. Available online: https://www.techradar.com/best/best-ransomware-protection (accessed on 25 April 2021).
27. Official Website of the European Union. Internal Market, Industry, Entrepreneurship and SMEs. Available online: https://ec.europa.eu/growth/smes/sme-definition_en (accessed on 25 April 2021).
28. Clark, D. Number of Small and Medium-Sized Enterprises (SMEs) the European Union in 2018. Available online: https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/ (accessed on 25 April 2021).