Вісник Тернопільського національного технічного університету
https://doi.org/10.33108/visnyk_tntu
Scientific Journal of the Ternopil National Technical University
2022, № 2 (106) https://doi.org/10.33108/visnyk_tntu2022.02
ISSN 2522-4433. Web: visnyk.tntu.edu.ua

UDC 1:316.4

ECONOMIC ASPECTS OF INFORMATION PROTECTION UNDER PRESENT LARGE-SCALE CYBER-ATTACKS CONDITIONS

Ruslana Prus; Svitlana Yatsyuk; Ludmila Hlynchuk; Vadim Mulyar

Lesya Ukrainka Volyn National University, Lutsk, Ukraine

Summary. *The main attacks that have caused irreparable damage to enterprises and organizations around the world in recent years and radically changed the attitude to cyber-attacks and the fight against them are analyzed; systematized scientific and technical prerequisites for the security of information technology; substantiated the tasks facing the developers of modern information systems; the consequences of attacks on information are investigated and the main factors influencing financial losses due to security breaches are identified.*

Key words: *attack, security, cyber attack, information, electronic information, malicious software.*

https://doi.org/10.33108/visnyk_tntu2022.02.063 *Received 22.03.2022*

Problem statement. The amount of information stored in electronic form is growing every passing day due to the mass introduction of computer technologies into all spheres of human activity. Nowadays, the process of access-restricted information copying and extraction is much easier than hundreds of papers rewriting. Moreover, computer networks' appearance resulting in wireless network access has not guaranteed information integrity. Thus, cyber-attacks spread on information systems has put forward new higher requirements to the study in the field of information security. They involve new approaches to information protection.

Analysis of well-known research results. Some criteria of information protection assessment in computer systems against unauthorized access are described in [1, 2]. The papers review and the analysis of the results obtained on the terminology in the field of information security in computer systems against unauthorized access are given in [3–9]. Besides, practical use of information technology security and system approach are highlighted in [6–10]. Analysis of safety principles of enterprises and banks' commercial activity is made in [11, 12]. A multi-stage system of information protection is described in [13]. The insurance against information security risks is simulated in [14].

Paper purpose. To analyze the main attacks which caused incredible damage to numerous enterprises and organizations all around the world in recent years, and they have changed the attitude toward cyber-attacks dramatically; to systematize scientific and technical prerequisites on information technology security assurance; to substantiate the tasks the developers of modern information systems are facing; to study the consequences of the attacks on information and to make focus on the main reasons making an impact on financial expenses due to security violation.

Task setting. Some messages about cyber-attacks, hackers, and computer violations taking place more and more often have been considered in the paper under discussion. Information, the electronic one, in particular, is represented by hundreds of different kinds: separate files, datasets, records, and software complexes. All these objects can be attacked by intruders. Thus, the study of information protection under present cyber-attack conditions is quite urgent.

Corresponding author: Svitlana Yatsyuk; e-mail: yatsyuk.svitlana@eenu.edu.ua ……

It is necessary to provide continuous activity for any enterprises and institutions, both state and private. While storing, supporting, and providing access to any information object, its owner or his/her representative specifies a set of rules to work with it. Their purposeful breaking can be classified as an attack against information.

According to the historic and international safety experience, the objects of security, taking into account their priorities, are as follows:

1) a person;
2) information;
3) material values.

Whereas the priority of personal safety is a natural phenomenon, the priority of information over material values requires more thorough consideration. It includes not only information that is a national or commercial secret, but open information as well.

Market relations with their integral component, i.e. competition, high demand to oppose the external and internal impacts. The objects of protection may more or less be affected by different attacks or threats to be in a dangerous situation, it depends on the purposes of an assaulter and on the specific conditions.

The concept of safety activity of an enterprise and institution involves:

1) physical safety, which means protection assurance against threats to human life;
2) economic safety;
3) cybersecurity;
4) material security, i.e. protection of material values against any kind of danger – from their stealing to fire danger and other catastrophes.

We must admit, that there is a close relationship between economic safety and cybersecurity. As experts consider, 20% leak of commercial information in 60 cases out of 100 results in the company's bankruptcy. We can also argue, that 93% of companies having no access to their information for more than 10 days have lost their business. Moreover, half of them claimed their inability to run a business [1]. Thus, economic safety and cybersecurity have been closely interrelated. Reducing threats to a company's economic activity means obtaining the required information about the competitors. So, it's quite natural, that the less growing threat for certain companies' economic activity the more growing it is for the others. It is possible due to the industrial, and economic one, in particular, espionage.

Losses from the competitors' activity, when industrial espionage methods are used, are equal to 30% of total losses in the world, i.e. billions of dollars [1]. It is impossible to estimate the exact losses as neither offenders nor victims are eager to make information about the illegal methods of running a business public. This may explain a high level of offenses latency and the absence of announcements about them in mass media. Thus, only less than 10% of all cases of illegal activity of criminal nature have become public information that cannot be hidden.

So, the tasks concerning any kind of security must be solved at any time when various aspects of human activity are taken into consideration. But, as we can see, all these types of security are closely connected with information.

Information security (IS) is a state of information when the information properties saving specified by the security policy can be assured [1]. An information system (IS) is an organizational-technical system involving a computing system, physical environment, staff, and processed information. Information security in IS means the activity aimed at providing the security of information processed in the IS and the IS security in general and allows to prevent or make less possible the implementation of threats, as well as to reduce the number of possible losses caused by the threats implemented.

In fact, the sphere of information security is not information protection but protection of property rights on it. Historically, a traditional object of property rights is a material object, and that means that the property right was the right to a thing.

But information is not a material object, information is knowledge, i.e. the reality reflected in human consciousness. And only later information can be introduced into material objects. Despite not being a material object, information can't be separated from the material carrier: human memory or non-human material carriers like books, floppy disks, or other kinds of «memory» (memory devices).

As an analysis of historical facts and the latest experience have shown, new types and forms of information processing are constantly coming into existence, as well as new kinds and forms of its protection are being developed. Nevertheless, offenders have always been one step ahead, and security services must do their best and involve lots of effort and resources to avoid bad consequences of various violations impact.

We have tried to systematize the scientific and technical prerequisites of security support with information technologies [1].

1. Increased volume of information, collected, stored, and processed by means of IS and information technologies (IT). In this case, we can see that the range of methods, ways, and possibilities of its collection and storage is becoming greater and greater, for example, when information of various purposes and designation can be stored in the same databases [1]. In fact, by penetrating a database, one can obtain complete information about any company or state institution's activity.

2. The latest generations of computers have acquired enormous calculating capacity lately, whereas they have become much simpler in use. It means, that as it is much easier to use them, more and more new users are getting access to computers. Obviously, the average qualification of users is getting lower which makes the task of an offender much easier, as due to such personalization of IT most users have their own workstations and they carry out their administration by themselves [2]. Most of them can't take care of the safety of their systems at a high level, as it requires the proper knowledge, skills, large amount of time and money. The wide spread of network technologies has joined separate machines into local networks enabling them to use mutual resources, and the use of «clip-server» technology has transformed these networks into distributed calculating environments. Now, network safety starts to depend on the safety of all its components, so it will be enough for an offender to disrupt the operation of one of them to disable the network.

Modern telecommunication technologies have united local networks into global ones. In spite of all other advantages of use, the Internet provides wide possibilities to violate information processing systems security all around the world. If a computer is connected to the Internet, for an offender it does not matter where it is located – in the next room or in the other corner of the world.

The progress in the field of hardware is accompanied by the more rapid development of software. As practice has shown, the vast majority of the most popular software (first of all, operating systems), despite the huge efforts of their developers, do not meet even the minimum safety requirements [1]. When detected, lots of faults are eliminated by the versions restoring or some additional means, though the constancy when new and new defects occur cannot but cause apprehension. This can prove, that most systems provide the offenders with wide opportunities to commit violations.

The discrepancy between the data and programs has disappeared due to the introduction and wide use of virtual machines and different interpreters. Now, any application from a text processor to a browser can not only process the data but interpret the instructions of a special programming language integrated into them. It increases the opportunities of an offender considerably concerning the creation of devices for breaking into someone else's system, and simultaneously it complicates the security as it requires controlling the interaction on one more level, i.e. on virtual machines or interpreters' level [3].

3. There is a significant gap between theoretical models of security, operating some

abstract concepts like object, subject, etc., and current information technologies. It has resulted in some discrepancies between the security models and their implementation in information processing devices. Besides, lots of protection aids, for example, anti-virus tools or firewall systems, do not have any system scientific basis at all. This situation could happen because of the absence of the general theory of information protection, and complex security models of information processing describing the mechanisms of an offender's actions in real systems. Moreover, there aren't any systems enabling us to check the efficiency of decisions dealing with the security sphere properly. The result of this is that practically all security systems are based on the analysis of successful attack results, and this fact predetermines that they lag behind the real situation. As an example, we can mention the well-known practice of «suddenly» closing the detected defects in the security system.

4. Thus, under present conditions, the substantiation of the safety requirements, and the creation of a regulatory basis that does not complicate the tasks of developers, but, on the contrary, defines the compulsory level of safety, is extremely important. Some new decisions in this field are really essential under the informatization and computerization of the most important spheres of economy and state apparatus conditions.

Due to the collective action of the above-mentioned factors, the developers of modern information systems for important information processing are facing assignments requiring their efficient solutions [1].

1) Providing the security of new types of information resources. As the present computer systems are directly integrated into the information structures of modern society, the protection aids must take into account the latest forms of information representation (hypertext, multi-media, and others). It means, that the security systems must provide security on the information resources level, but not on the level of separate documents, files, or messages [1].

2) Organization of trustful interaction of both sides (mutual identification/ authentication) in information space. Development of local networks and the Internet dictate the necessity to provide efficient protection under remote access to information conditions, as well as the interaction of users via public networks. Moreover, this problem should be solved globally, in spite of the fact that the sides involved may be located in different parts of the planet, and can function on different hardware platforms and in different operating systems.

3) Protection against automatic means of attack. The experience of existing systems running has proved, that completely new functions are required from the security systems, namely possible provision of security under their interaction with any similar means conditions, including inside the programs, which carry out destructive actions, i.e. computer viruses, automatic hacking tools, aggressive agents [1]. At the first sight, it looks like that this problem can be solved by means of access demarcation, though it is not quite so, that was proved by well-known cases of computer viruses spread in «protected» systems.

4) Information security integration into the process of information processing automation as a compulsory component. To be in demand by the modern market of information systems, security aids can't be in conflict with the conventional applications and the existing technologies of information processing, but, on the contrary, they should become an integral part of these facilities and technologies [1].

5) Development of modern, reliable, proper, and efficient mathematical models of security.

If these problems are not solved, then any further spread of information technologies in the sphere of critical systems processing important information will soon be in danger. Moreover, some possible consequences of the attacks on information may have a considerable impact on running a business:

1) Commercial information reveal can lead to serious direct losses on the market.

2) An announcement of a theft of a large volume of information may affect the

company's reputation dramatically and can result in losses of trade deals volume.

3) Companies-competitors can make use of the information theft if it was unwitnessed to make their opponent bankrupt by imposing some fictitious or unprofitable agreements.

4) Changing information either at the transfer stage or at the storage stage may result in considerable losses for the company.

5) Multiple successful attacks on the company providing any kind of information services result in reducing the level of customers' trust in the company and may influence the volume of income.

Fear of the security alert is based on financial losses caused by attacks, which is not a hypothetical number at all. The violations have resulted in enormous economic losses for the organizations, when it may take long months or years to compensate for them. According to the study by Ponemon Institute, by the respondents' estimates, more than half (53%) of all attacks lead to financial losses in the amount of more than 500 000 US dollars, including lost income, consumers, and opportunities (fig. 1).

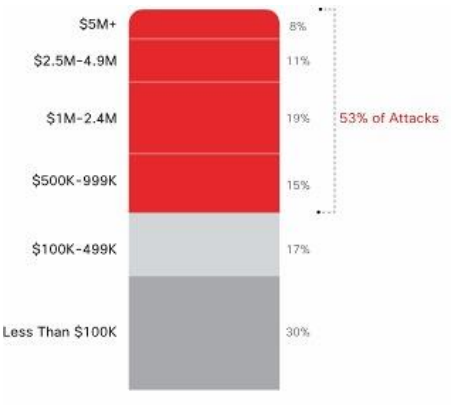

Figure 1. Financial consequences of IS attacks

Security services are facing lots of obstacles in their efforts aimed at the protection of their organizations. The most complicated areas and functions for protection are mobile devices, data in the public cloud, and the behavior of users (fig. 2) [4].

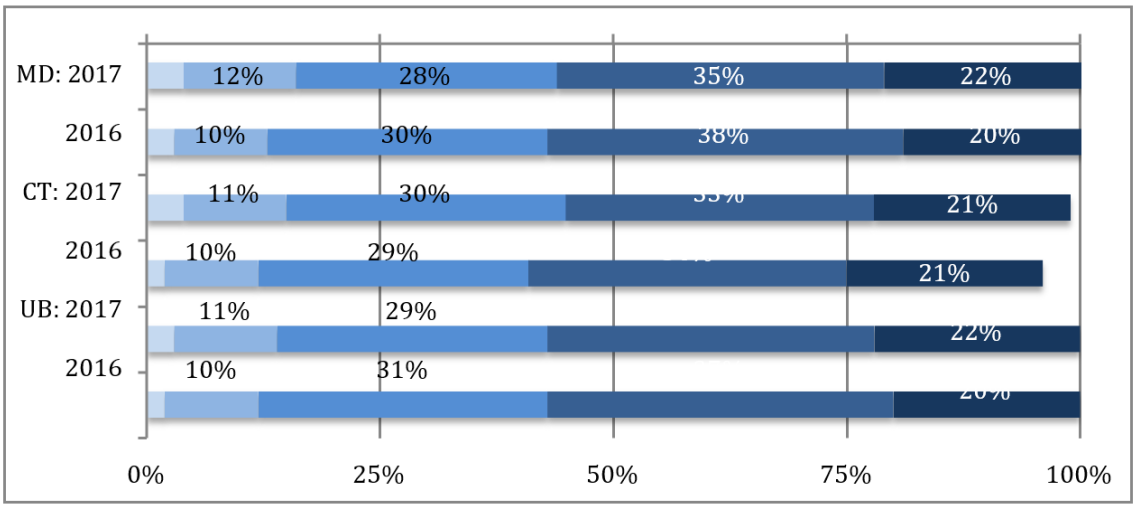

Figure 2. The most difficult attacks to be solved in 2017: from easy to the most complex: MD – mobile devices, CT – cloud technology, UB – user behavior

Let's analyze some main attacks, that caused irreparable damage to numerous enterprises and organizations all over the world in the last years, and have changed the attitude towards cyber-attacks and fight against them dramatically.

1) Petya/NotPetya – a devastating cyber-attack on Ukraine. It was one of the biggest and the most devastating cyber-attacks, which took place at the end of June 2017, deleting data on thousands of computers and disrupting the work of many companies in Ukraine, as well as in the countries which run business with Ukraine.

Up to December 2017, it was the most expensive cyber-attack of 2017. Taking into account all damaged companies, the total sum of losses was approximately equal to 1,2 billion US dollars [1].

This harmful software was used to destroy and damage, but not to receive some money as a ransom. It means that offenders did not want to have some financial profits, but tried to eliminate or damage the hard disc of the infected computer to cause as much harm as possible. Harmful programs code the system files and then damage the hard disc, removing the main loading record (MBR – Master Boot Record). As a result, even if the hard disc can be restored, the files won't.

Malicious software was used against companies and organizations in Ukraine. In total, the violations were recorded at about 2000 companies and organizations; among them are state institutions, banks, corporations as well as small and medium businesses. Besides, lots of international companies working with Ukraine and also using MeDoc were damaged considerably. One of them was Maersk (the biggest shipping company), and another was TNT, which had to restore their work for a long time. One more accident happened when an American security company announced that about 5000 computers of the company cooperating with Ukraine were destroyed on the territory of the USA.

2) WannaCry has been a global destructive cyber-attack since 2017. The attack WannaCry provoked an unprecedented global accident when 230000 computers in 150 countries were infected and damaged in one single day.

The time interval between the event identification and its classification as a difficult one by different organizations (security companies, CERT, and others), and the report on that matter was a few hours. Nevertheless, lots of warnings and instructions on attack mitigation were not helpful at all. A large organization can't update all its systems as soon as possible, i.e. within a few days. The fundamental problem restraining large organizations is their inability in making serious adjustments in their systems quickly, for example, locking networks, and servers, and suspending the company.

At present, any security company can't stop the accident completely within the period necessary to provide the required assistance for these organizations in real time. The process of investigation, analysis, and detection of cyber-attacks is frequently long and restricted. In recent years, the most noticeable vector of invasion concerning organizations has been based on malicious email and fishing. The readiness of the organizations and companies to adapt to new vectors is quite limited and requires reconsideration of the situation.

Lots of defected organizations needed to have some time to return to normal functioning. The process of restoring after a big cyber-attack is rather slow and «painful». It can be explained by numerous reasons, mostly dealing with the necessity to continue providing services to their customers during the attack, as well as during the restoration period. The requirements to the IT subdivisions on the simultaneous restoration of defected systems and returning to normal operation within their cleaning are almost impossible assignments.

3) Penetrating to EquiFax: at the beginning of September, the consumer credit-rating agency Equifax Inc. announced that it was a victim of a large-scale cyber-attack and as a result, more than 143 million records of individuals and legal entities were compromised [1]. The majority of stolen data deals with the citizens of the USA, Great Britain, and Canada.

Equifax is one of three of the largest American credit agencies running their business all over the world. It aggregates and manages sensitive databases, including credit ratings of about 800 million persons and companies.

4) Leak of national state tools of attacks and documents: CIA documents leak combined with vulnerabilities and attack tools have contributed to accelerated development of new and more complex vectors of attack.

Numerous actors from all over cyberspace were involved (hacktivists, criminals, and terrorist organizations).

5) Russia's interference in the elections of the USA and other countries, and in democratic processes, including Brexit. Some claims were made of the sensitive and/or fake information spreading by Russian public figures to make an impact on the democratic process and damage it in different countries [2]. Within these events, malicious use of different social platforms like Facebook and Twitter was marked as an attempt to undermine the political status quo of western and pro-western countries. In the second half of 2017 Microsoft Office was the second in the software attacks from 22,80% of all attacks (an increase from 10,26% in the first half of 2017); leaving behind OS Android which is now equal to 22,71% of the systems attacked (Table 1). This change can be partially explained by the increasing tendency of attacks DDE based on the contactless execution of a harmful code using the function of their own service Office [4].

Table 1

The systems that suffered from attacks most of all in 2017

Software	Percentage of the attacks
Browsers	35.00
Microsoft Office	22.80
Android OS	2271
Java	7.62
Adobe Flash	5.48
PDF Software	1.39

In 2017 ransomware (a harmful program that racketeers a ransom) was one of the most expensive threats that could influence an organization. Modern encryption programs used by offenders can make any coded file invalid unless the decryption key is obtained. If the infected organization does not have any extra copies, there will not be any other choice except to pay the ransom to cybercriminals so that not to lose the important data (though it is impossible to guarantee that hackers will keep their promise and will pass the required decryption key).

Nevertheless, potential expenses do not stop at that moment. The attacks of ransomware, especially if they aim at several computers in the network, may cause considerable losses resulting in efficiency loss, overdue, and expenses on the elimination of the consequences. It may cause reputation damage, especially, if the reason for disruption becomes public, resulting in loss of business. In some cases, organizations have confessed that the attacks of ransomware have made a considerable impact on their financial abilities.

When 500 dollars are demanded as a ransom it does not look like a big sum of money even for a small company, but the organizations should remember that this is the average ransom for one infected computer. The attack, when dozens or even hundreds of computers are infected, will cause much more cumulative loss on the ransom [6].

Figure 3. The average ransom amount in US dollars per year

For example, as the result of Ransomware Erebus Linux-version (Ransom.Erebus) attack on the southern Korean web-hosting company Nayana more than 153 servers Linux were infected and encrypted. Thus, more than 3400 websites of the customers were offline. Having announced about the attack, Nayana recognized, that the criminals demanded a ransom of 550 bitcoin (approximately 1,62 million dollars at that moment). In a few days, Nayana announced that the ransom amount was agreed with the blackmailers, and they agreed to pay 397 bitcoins (approximately 1 million dollars). Up to now, this ransom amount has been considered to be the largest one officially recognized.

The delivery giant corporation FedEx announced in July, that Petya attack would influence the annual financial results. The company shares fell for more than 3 percent immediately after the announcement. The company FedEx has claimed that when the incident took place it had no insurance to cover the losses from the cyber-attack.

Danish shipping giant AP Moller-Maersk has claimed, that Petya attack will cost them 300 million US dollars of the lost income.

According to the data of the study carried out by the team Norton Cyber Security Insight, 34% of victims pay a ransom. This share is increasing in the USA up to 64% of victims [3].

Apparently, the fact that people are ready to pay a ransom is explained by the attack increase and persistence. The ransomware attack is also simple in controlling.

Separate security measures reduce or increase the costs of the data breach. The list of factors increasing or reducing expenditures on data protection or restoration under security violation conditions is given in Table 2 [3]. For example, an incident response team, encryption use, training of staff, the management involved, and the use of an analytical security system can reduce the damage done by the violation significantly [6].

Table 2

Factors influencing the level of damage caused by the threat execution

Factors	**Percentage of companies applying appropriate measures**
1	2
Staff training	51%
Use of management tools of business continuity	50%
Incident response team	48%
Appointment of the head of the IT-security department	45%
Wide use of encryption	44%

The end of the table 2

1	2
Participation of the third side	36%
Advisors involving	35%
Restoration of lost or stolen devices	33%
Insurance	32%
Management involving	31%
Speed of response	29%

Advisors' involvement, data transfer to the cloud, mobile platforms use, restoration of lost or stolen information carriers, as well as an increase in speed of response pile up the expenses to eliminate the consequences of security incidents.

Some typical measures to detect and immediately respond to the incidents include the following: conducting the investigation, the forensic examination, finding probable victims of violations, organizing a team of incident response, organization of communication and expansion of public relations, writing documents for notification of the data leakage victims and the proper structures about the case of violation, implementation of procedures on call-center organizing and special training.

The expenditures of Cisco Systems respondents on different means and measures to prevent violations, reduce and eliminate their consequences, as well as to improve the system are given in Table 3 [4].

Some typical activities conducted within the period after the violation detection include audit and consulting, legal services on security, free or discount services for victims of crimes, measures on personal security, restoring the customer business on the basis of customer churn calculation, expenditures on the customer base broadening and loyalty programs.

Table 3

Classification of information protection mechanisms and their cost

<table>
<tr><th colspan="2">Tools</th><th colspan="2">Measures</th></tr>
<tr><td>Perimeter protection</td><td>$11,9 bil.</td><td>Consulting</td><td>$21 bil.</td></tr>
<tr><td>Personal data protection</td><td>$4,6 bil.</td><td>Integration</td><td>$20 bil.</td></tr>
<tr><td>Endpoints protection (computers, mobile phones, tablets)</td><td>$3,8 bil.</td><td rowspan="3">Incident management:
- warning
- detection
- reaction</td><td rowspan="3">$20 bil.</td></tr>
<tr><td>Web-protection</td><td>$2,6 bil.</td></tr>
<tr><td>Others</td><td>$11 bil.</td></tr>
</table>

Due to the increase in data security violations costs and volume, IT-security is considered by business leaders not only as a completely technological problem but as a large business risk. Such change has stimulated the increased interest in cyber resources insurance [1], the creation of special security departments at an enterprise, and staff training.

Thus, we can list the main reasons influencing the financial expenses caused by the security violation and the main tendencies of the last three years [1], [2], [3], related to the security violation:

1. Losses caused by security violations are the highest in the USA and Canada, and the lowest ones are in Brasil and India.

2. Losses caused by security violations vary depending on the industry. Health care institutions ranked first for the last seven years, they are followed by the financial services sector, mass media, research organizations, and the public sector ranked last.

3. 47% of violations are caused by hackers and criminals-insiders activities.

4. Malicious or criminal attacks vary significantly depending on the country.

5. The cost of elimination depends on the time interval necessary to detect and block the violation. The analysis demonstrates the relation between the speed of incident detection and blocking, and the financial consequences of the elimination of the violation.

6. Creation of incident response groups and wide use of data encryption have reduced the losses caused by security violations.

7. Four new factors whose influence on the expenditures dealing with the security violation is growing: non-compliance with the requirements and instructions, wide use of mobile platforms, the appointment of the privacy service manager, and security analytics use.

8. Security violation results in customers' loss and makes an impact on the company's profits.

9. Security violations involving third persons (providers of cloud technologies and software for CRM systems, etc.) have become the main factor, that caused an increase in damage done.

10. Business continuity management plays an important role in reducing the losses caused by security violations.

The conducted analysis has proved that the majority of damaged organizations could not meet the requirements concerning information protection necessary to reduce the number of such cyber-attacks. These are three main directories that are critical to mitigate such attacks:

1) Security update installation: all computer systems of the organization (workstations, servers, routers, commutators, software, etc.) and/or computer systems have the latest security patches. Nevertheless, this predicate is followed by an almost impossible challenge. As it is practically impossible for big organizations to guarantee that each of its servers is constantly being updated with security patches. Taking into consideration workstations, the situation is much better, as most organizations update their workstations within their validity of up to two months. In comparison with their servers updating schedule – from two months to a year, and even a few years for the systems that are not the Microsoft company. The systems which cannot be updated by means of security patches should be removed from the network and divided into segments.

2) Division and segmentation of the organization network to minimize the possibility of malicious programs spreading in the organization system. Besides, the network segmentation and division into different environments and components must keep to the principles of the least privileged (PoLP; the so-called principle of the least authority), i.e. to grant minimal privileges to the user profile on the systems based on the requirements to the work of users.

3) To provide that the system has backup copies and is configured in a way enabling its quick restoration. Creation of a reliable backup copy, which, on the one hand, can survive without cyber-attack harm, but, on the other hand, it will allow restoring the process quickly after an exhausting attack that switches off most computer systems of the organization.

The analysis of incidents' consequences and their development has enabled us to highlight the following proposals and conclusions.

Conclusions. At present, the organizations do not have any reliable method to check, and if necessary, to block the updating from legal sources containing malicious software. Accordingly, similar attacks on other objects can cause considerable damage. As a result, it is necessary to take into consideration the methods of monitoring the software updating.

It is very important to preserve the basic level of organizational security, where the main focus is made on segmentation, implementation of the strict mechanism of authorization, and supporting autonomous and comprehensive backup copying.

Information about the attack is reported sporadically, some messages are difficult to understand and they often contain some mistakes. As a result, the organizations have to struggle

against the attacks and make quick decisions on their future activity possessing only fragmented and inaccurate information. Due to the communicative channel improvement, an organization can receive more reliable and accurate information, and in this way, it may implement the best plans in case of emergency situations to reduce the attack's damage (there are services Cyber Security for this purpose, antivirus announcements, and CERT).

The companies having representative agencies in other countries of the world must be ready to switch off their infected branches immediately from the organization network during the attack. Although it should be mentioned, that if the attack vector contains a component of "time bombs", the disconnection of offices after the attack identification can be too late, as we can see in the case with Maersk and TNT.

Tools and vectors of attacks are constantly developing and creating new threats. The main vector of attacks for the last four years has been via email, and many organizations managed to develop quite efficient mechanisms of protection. Nevertheless, these recent attacks have used new vulnerable places requiring the organizations' protection reassessment and the development of new safety measures.

References

1. Information technology. Security techniques. Information security management systems – Requirements: ISO/IEC 27001:2017.
2. Kryterii otsinky zakhyshchenosti informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu: ND TZI 2.5-004-99. [Chynnyi vid 28.04.1999]. K.: DSTSZI SBU, 1999. No. 22. URL: https://tzi.ua/assets/files/ND-TZI-2.5-004-99.pdf.
3. Terminolohiia v haluzi zakhystu informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu: ND TZI 1.1-003-99. [Chynnyi vid 28.04.1999]. K.: DSTSZI SBU, 1999. No. 22. URL: https://tzi.com.ua/downloads/1.1-003-99.pdf.
4. Cisco 2018, Annual Cybersecurity Report, Cisco Systems, February 2018.
5. FBI/IC3: 2016 Internet Crime Report.
6. Ponemon Institute, 2017 Cost of Data Breach Study: Global Overview – Research Report, June 2017.
7. Ponemon Institute, 2018 Cost of Data Breach Study: Impact of Business Continuity Management – Research Report, 2018.
8. Ponemon Institute, Cost of a Data Breach Report 2019 – Research Report, 2019. DOI: https://doi.org/10.1016/S1361-3723(19)30081-8
9. Ponemon Institute, Key findings from the 2017 Cost of Data Breach Study: Global Overview – Research Report, June 2017.
10. Domarev V. V. Bezopasnost ynformatsyonnыkh tekhnolohyi. Systemny podhod. K.: TYD DS, 2004. P. 655.
11. Zubok M. I. Osnovy bezpeky komertsiinoi diialnosti pidpryiemstv ta bankiv. K.: KNTEU, 2005. P. 135.
12. Kopytin Yu. V. Model strakhuvannia ryzykiv informatsiinoi bezpeky. "Tsyfrovi tekhnolohii|. 2010. No. 8. P. 99.
13. Levchenko Ye. H., Prus R. B., Rabchun D. I. Pokaznyky bahatostupinchastykh system zakhystu informatsii. Visnyk Inzhenernoi akademii Ukrainy. 2009. No. 1. P. 128–133.
14. Odarchenko R/ S., Lukin S. Yu. Ekonomichna efektyvnist vprovadzhennia system zakhystu stilnykovykh merezh 4G. "Systemy obrobky informatsii". 2012. Vypusk 4 (102). Tom 2. P. 52.

Список використаних джерел

1. Information technology. Security techniques. Information security management systems – Requirements: ISO/IEC 27001:2017
2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. Чинний від 28.04.1999. К.: ДСТСЗІ СБУ, 1999. No. 22. URL: https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf/
3. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. Чинний від 28.04.1999. К.: ДСТСЗІ СБУ, 1999. No. 22. URL: https://tzi.com.ua/downloads/1.1-003-99.pdf.
4. Cisco 2018, Annual Cybersecurity Report, Cisco Systems, February 2018.
5. FBI/IC3: 2016 Internet Crime Report.
6. Ponemon Institute, 2017 Cost of Data Breach Study: Global Overview – Research Report, June 2017.

7. Ponemon Institute, 2018 Cost of Data Breach Study: Impact of Business Continuity Management – Research Report, 2018.
8. Ponemon Institute, Cost of a Data Breach Report 2019 – Research Report, 2019. DOI: https://doi.org/10.1016/S1361-3723(19)30081-8
9. Ponemon Institute, Key findings from the 2017 Cost of Data Breach Study: Global Overview – Research Report, June 2017.
10. Домарев В. В. Безопасность информационных технологий. Системный подход. К.: ТИД ДС, 2004. С. 655.
11. Зубок М. І. Основи безпеки комерційної діяльності підприємств та банків. К.: КНТЕУ, 2005. С. 135.
12. Копитін Ю. В. Модель страхування ризиків інформаційної безпеки, «Цифрові технології». 2010. № 8. С. 99.
13. Левченко Є. Г., Прус Р. Б., Рабчун Д. І. Показники багатоступінчастих систем захисту інформації. Вісник Інженерної академії України. 2009. № 1. С. 128–133.
14. Одарченко Р. С., Лукін С. Ю. Економічна ефективність впровадження систем захисту стільникових мереж 4G. «Системи обробки інформації». 2012. Випуск 4 (102). Том 2. С. 52.

УДК 1:316.4

ЕКОНОМІЧНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ СУЧАСНИХ МАСШТАБНИХ КІБЕРАТАК

Руслана Прус; Світлана Яцюк; Людмила Глинчук; Вадим Муляр

Волинський національний університет імені Лесі Українки, Луцьк, Україна

Резюме. *Проаналізовано основні атаки, які завдали невиправної шкоди підприємствам та організаціям у всьому світі за останні роки та кардинально змінили ставлення до кібератак і боротьби з ними. Систематизовано наукові й технічні передумови ситуації із забезпеченням безпеки інформаційних технологій. Обґрунтовано завдання, які стоять перед розробниками сучасних інформаційних систем. Досліджено наслідки атак на інформацію та виділено основні чинники, які впливають на фінансові втрати унаслідок порушення безпеки. Досліджено інциденти кібератаки, про зловмисників та комп'ютерні злочини, що деструктивно впливають та завдають фінансових збитків корпораціям. Зокрема досліджено втрати унаслідок порушень безпеки найвищі у США та Канаді, а найнижчі – в Бразилії та Індії. Проаналізовано, який показує, що більшість постраждалих організацій не змогла виконати базові вимоги до захисту інформації, необхідні для обмеження обсягу таких кібератак. Три основні постулати є критичними для пом'якшення таких нападів: встановлення оновлень безпеки: всі комп'ютерні системи організації (робочі станції, сервери, маршрутизатори, комутатори, програмне забезпечення тощо) та/або комп'ютерні системи мають найновіші патчі безпеки; розподіл та сегментація мережі організації, щоб звести до мінімуму можливість поширення шкідливих програм у системі організації; забезпечення в системі автоматизованого процесу створення резервних копій.*

На основі проведеного аналізу кіберінцидентів у роботі виділено такі пропозиції: проведення сегментації, впровадження суворого механізму авторизації, підтримки автономного та всеосяжного резервного копіювання; удосконалення комунікативних каналів, організації для отримання достовірної інформації про загрози; своєчасне відключення уражених філій від організаційної мережі під час нападу.

Ключові слова: *атака, безпека, кібератака, інформація, електронна інформація, зловмисне програмне забезпечення.*

https://doi.org/10.33108/visnyk_tntu2022.02.063 *Отримано 22.03.2022*