CONTRIBUTIONS REGARDING THE IMPLEMENTATION OF COMPUTER INCIDENT MANAGEMENT IN A PUBLIC ORGANIZATION PROVIDING SERVICES TO CITIZENS

Aurel-Mihail ȚÎȚU [1,2], Constantin-Dorin OLTEANU[3], Petrică TERTEREANU[4], Radu-Costin MOISESCU[5]

Rezumat. *Lucrarea științifică prezintă o cercetare cu privire la modalitatea de a implementa în cadrul unei organizații publice prestatoare de servicii către cetățeni unui management al incidentelor informatice. Digitalizarea tot mai mult a activităților în sectorul public aduce foarte multe avantaje cum ar fi eficiența, creșterea calității serviciilor, scurtarea timpilor de lucru. Pe de altă parte, digitalizarea se poate realiza cu o tehnologizare amplă cu echipamente folosite în cadrul rețelei locale de informatică pentru desfășurarea activităților, pentru stocarea bazelor de date, pentru interconectare cu alte sisteme informatice. Toate aceste echipamente și sisteme informatice au un anumit grad de vulnerabilitate existând riscul apariției unor incidente informatice. Cercetarea propusă de autori vine cu propuneri în acest domeniu al managementului incidentelor informatice oferind soluții prin realizarea unei proceduri de rezolvare a unui incident informatic. În urma cercetării făcute sau implementat mai multe politici pe serverele din rețeaua locală la nivelul întregului domeniu local cât și implementarea unor politici la nivelul fiecărei stații de lucru din rețeaua locală a organizației pentru evitarea unor incidente informatice de tipul unor atacuri cibernetice. S-au implementat soluții de backup pe dispozitiv de tip NAS pentru eliminarea riscurilor privind incidentele informatice ce pot să apară în cazul defectării unui hard disk sau pierderea de date. De asemenea s-au implementat soluții pentru eliminarea în mare măsură a riscurilor de apariție a unor incidente informatice datorate de defectarea dispozitivelor informatice din cadrul rețelei locale în urma unor probleme ce pot apărea la rețeaua de alimentare cu energie electrică. Cercetarea făcută a identificat și găsit soluții pentru eliminarea unor vulnerabilități în rețeaua wireless, ce pot duce la incidente informatice. În finalul lucrării sunt prezentate concluzii ce reies în urma acestei cercetări.*

Abstract. *The scientific work presents research on implementing computer incident management within a public organization providing services to citizens. The increasing digitization of activities in the public sector brings many advantages, such as efficiency, increasing the quality of services, and shortening working times. On the other hand, digitization can be achieved with extensive technology with equipment used within the local IT network to carry out activities, store databases, and interconnect with other IT systems. All these equipment and computer systems have a certain degree of vulnerability, and there is a*

[1] Prof., dr. eng. and dr. ec. -mg., Dr. Habil. Dr. h. c., Lucian Blaga University of Sibiu, 10, Victoriei Street, Sibiu, România (mihail.titu@ulbsibiu.ro).
[2]The Academy of Romanian Scientists, 3 Ilfov Street, Bucharest, Romania.
[3]Sc.D Student, University Politehnica of Bucharest, Faculty of Industrial Engineering and Robotics, Splaiul Independenţei nr. 313, Bucharest, Romania, (ocosti@gmail.com).
[4]Sc.D Student, University Politehnica of Bucharest, Faculty of Industrial Engineering and Robotics, Splaiul Independenţei nr. 313, Bucharest, Romania, (tertereanupetrica@yahoo.com).
[5]Sc.D Student, University Politehnica of Bucharest, Faculty of Industrial Engineering and Robotics, Splaiul Independenţei nr. 313, Bucharest, Romania, (radu_moisescu@yahoo.com).

risk of computer incidents. The research proposed by the authors comes up with proposals in this field of computer incident management, offering solutions by carrying out a procedure for solving a computer incident. Following the research, several policies have been implemented on the servers in the local network at the level of the entire local domain and the implementation of policies at the level of each workstation in the organization's local network to avoid computer incidents such as cyber-attacks. Backup solutions have been implemented on a NAS-type device to eliminate the risks of computer incidents during a hard disk failure or data loss. Solutions have also been implemented to eliminate the risks of computer incidents due to the failure of computer devices within the local network following problems that may occur with the electricity supply network. The research identified and found solutions to eliminate some vulnerabilities in the wireless network, which can lead to computer incidents. At the paper's end, conclusions from this research are presented.

Keywords: computer incident, informatics vulnerabilities, management, local network, public organization

DOI https://doi.org/10.56082/annalsarscieco.2023.2.47

1. Introduction

According to law 362 of 2018, the term incident means any event that has a real negative impact on the security of networks and computer systems. [1] Thus, we can consider a computer incident, any unexpected event due to an action that changes the current state of a hardware device, IT software, or existing data within the network.

When we refer to computer incident management, we must consider the existing legislative environment and the standards in this field, which are currently in progress. According to Pfleeger, author of Security in Computing, computer incident management is critical to detecting, preventing, and correcting computer incidents. [2]

For organizations to limit the possibility of damage in the event of a cyber-attack, it is necessary to have the ability to respond to security incidents efficiently and methodically. Also important is the organization's ability to fix the effects of problems caused by such attacks. To achieve this effective response, private organizations and public institutions, through their policies and procedures, also add a response capability to IT incidents. [3]

For operators of essential services, the NIS directive 1148/2016 was adopted at the level of the European Union, which requires measures to ensure a standard high level of security of networks and IT systems. The studied organization is not among the operators of essential services. However, it is desired that the security policies, the measures taken, and the management of IT incidents be based on this directive and law 362/2018. Therefore, right from the beginning of the directive, the role and importance of IT networks and systems are highlighted: "Networks together with IT systems and services fulfill a vital role in society. Their reliability and security are

essential for economic and societal activities and, in particular, for the functioning of the internal market." [4]

Law 367/2018 defines the legal and institutional framework as well as the measures and mechanisms necessary to ensure a high level of security of computer networks and systems. This law wants to achieve the security of computer systems and networks by increasing training through requirements and measures. It also establishes ways to audit networks and IT systems. To achieve efficient IT incident management, all incidents that occur must notified. [1]

To implement information security management, the ISO 27001:2013 standard can be used as a tool for data security policy. This standard comes with control measures and recommendations that, through implementation, are intended to keep IT risks under control within the organization. Other standards that help implement IT risk management are ISO 270033:2015 – a standard dealing with network security, ISO 270032:2012 Cybersecurity standard, and ISO 27005:2018 Risk management standard

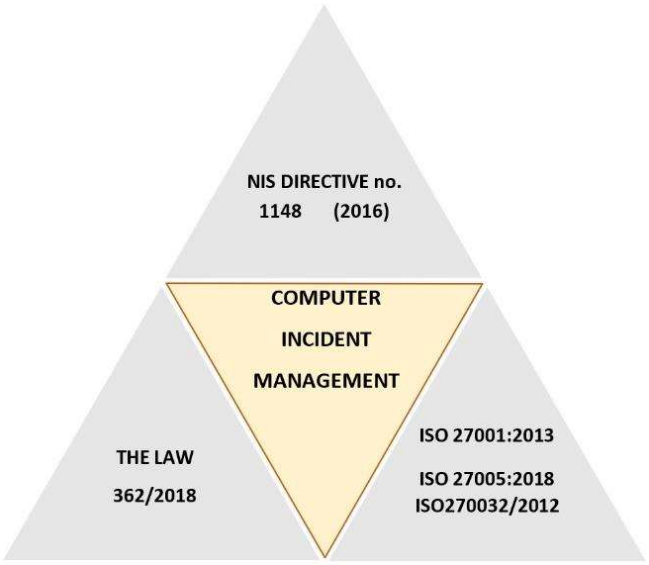

Fig. 1 Legislative environment

The broad legislative environment used indicatively to create computer incident management strategies is presented in Figure 1.

Computer incidents can occur in countless ways, and their nature can be diverse, so it is impossible to develop step-by-step procedures for handling every incident. Instead,

organizations must be prepared to handle any incident but should create procedures and strategies to handle incidents that may be more likely to occur.

2. Security of data and data networks in a public organization providing services to citizens

Due to the nature of the activities within the studied organization, sensitive, personal information is used. The standard, ISO 27701:2019, refers to implementing an information privacy management system that helps to protect personal information. This standard provides requirements and measures that can help the studied organization achieve the confidentiality and protection of personal data used in the activity, complying with the requirements and regulations of the GDPR. The GDPR establishes the rules for protecting natural persons about the processing of personal data and the rules for the free movement of personal data. Thus, it is desired to pay increased attention to the existence of personal data throughout their entire course from their acquisition, processing, circulation, storage, or destruction. Computer incident management aims to identify an incident, report it, classify it, assign a person to solve it and find a solution and remedial measures. If there are no solutions for local remediation, contacting a company specialized in solving the incident is necessary. The resolution of the computer incident involves recording the incident, analyzing and evaluating the incident, remediation measures, and subsequent prevention planning.

We must identify possible vulnerabilities and threats to secure network and network data. Vulnerabilities are weaknesses that can allow an incident to occur. [2] By vulnerabilities, we mean the weak points through which attacks can occur from outside and inside the network. Threats are actions that, through their manifestation, can negatively influence the activity within the IT system. Network and data security requires finding and implementing the most effective decisions that will increase the protection of the data network and the data used in the network.

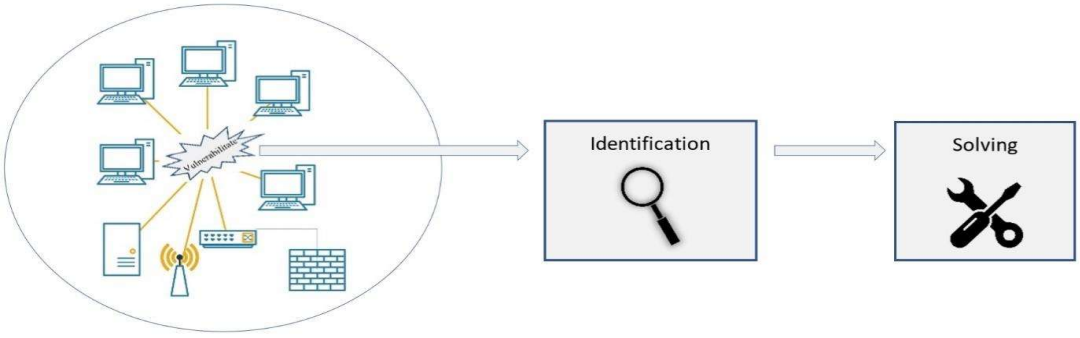

Fig. 2. Approach computer incidents

IT incident response is a coordinated and structured approach from incident detection to incident resolution. An incident response may include activities that:

of reference items of different categories are given below:

- Certifies the existence of the incident;
- Detects and isolates efficiently and quickly;
- Provides about the nature of an incident;
- Provides a quick and coherent response;
- Reduces the impact of activities in the organization;
- Reduce as much as possible the damages caused by the incident;
- Returning to normal activities;
- Educating the management team;
- Improving security to avoid future incidents. [5]

An essential aspect of achieving adequate security of the data network within the studied organization is to identify the threats that may appear. Starting from a classification according to Dumitru Oprea, we scored several types of threats:

- Work environment. Equipment can be seriously and irreversibly damaged due to elements such as extreme temperatures, high humidity, excess dust;
- Natural factors such as fires, strong earthquakes, floods, or other extreme weather phenomena can affect equipment and IT systems, but also the physical structure of the premises where the specific activities are carried out;
- Incidents of human nature, physical failure of computer equipment, errors in software applications, problems due to improper supply of electricity by non-compliance with technical parameters or unannounced interruption of supply;
- Unintentional accidental actions on the IT system:
  - intentional cyber-attacks on the existing IT system. These attacks can be:
  - computer viruses that can negatively affect both the software component and hardware components existing in the computer system;
  - worm-type software programs that will spread throughout the network;
  - trojan programs, or rootkits that want to control the host computer;
  - backdoor software programs that want to control the computer;
  - spyware-type software programs that want to collect personal data about the user's commercial options;
  - DDoS – Distributed Denial of Services – software programs that want to make a workstation or a website unavailable;
  - phishing-type software programs that clone a website, redirect access to obtain personal access data to the website or information about bank accounts by requesting data from cards;
  - malware-type software programs that want to corrupt, destroy, or stealing data from a computer system;

- ransomware-type software programs usually encrypt files of certain types on the computer with a private key. Decrypting the information on the computer is possible only after a monetary ransom.

- Attacks of a different nature than those presented, such as selling information (customer personal data, trade secrets, manufacturing recipes, etc.), industrial espionage; acts of vandalism; and certain activities of journalists. [6]

According to specialized literature, approximately 70% of cyber-attacks were carried out by disgruntled employees and not outsiders outside the organization. Thus, the security system must be designed taking these aspects into account. [7]

3. Implementation of a computer incident management system within the public organization providing services to the studied citizens

The responsibility for the security of the information system within a public organization is all the higher the more the data and information have a particular character, as they are often subject to the GDPR. The digitization of activities applied on an increasingly large scale comes with apparent facilities. However, digitization also exposes the information used, cyber-attacks being a threat that requires the management of computer incidents.

To increase efficiency and reduce the response time in dealing with a computer incident within the studied public organization, a basic procedure was created to resolve that incident. This procedure is highlighted in Figure 3.

To control computer incidents, the studied public organization must be prepared for such situations with the help of computer incident management. The main component of this management system is specialized staff with training and capabilities in informatics. In addition, this staff has specific duties in computer incident management.

Also, the studied public organization must have means and ways to identify computer incidents, namely management and monitoring programs for the local computer network, antivirus protection programs with an administration console, and management and protection hardware devices. Furthermore, for the protection of data and databases in the local network, the studied public organization has several ways of action to avoid the occurrence of computer incidents, such as the existence of an antivirus program at the level of the entire network, the existence of solutions for daily backups of data on devices such as NAS and protections against problems that may

occur at the level of the electricity supply network.

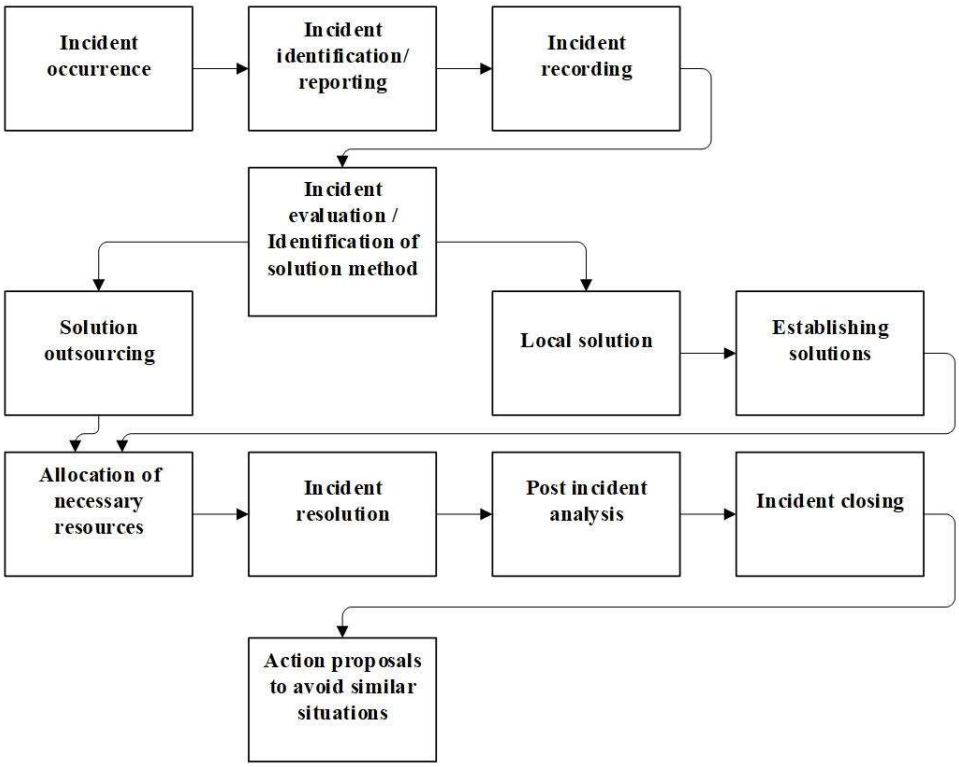

Fig. 3. General incident management procedure

An essential aspect of preventing computer incidents is reducing risks in the face of cyber-attacks. A vulnerability used very often is the fact that the operating systems and applications used are not updated to the latest version made available by their manufacturers. In the studied public organization, efforts are made to install the latest versions of this software. Getting to the latest version and making the latest updates are priorities for the existing antivirus system. Also, to the extent possible and as much as the financial situation allows, purchasing the latest versions of the used applications, operating systems, and antivirus systems is desired.

One way to detect IT events in the studied public organization is by analyzing the reports obtained from the management software installed for managing the network. However, only network administrators in the IT department have access to this software.

Another way to detect non-compliant situations on workstations is to conduct periodic internal audits on all equipment in the network. Of course, as well as outside of these audits, any observation regarding non-compliant operations will lead to measures to resolve this observed event.

4. Policies implemented at the level of the local computer network within the studied public organization, providing services to citizens

Proactive actions are essential to computer incident management in the studied public organization. Using a network domain is one of the critical tools in preventing such incidents. In addition, the policies implemented within the domain eliminate some of the risks and vulnerabilities that may arise.

A proactive approach was achieved by implementing security policies configured in the Windows Server operating system, which will act on the entire local domain.

All users must log in with a username and password to use the workstation and access the network and network resources. The local domain is managed with a Windows Server system, and this policy is implemented domain-wide. The implemented policy stipulates that the password used by the user expires periodically, requiring its change. The password format is complex; in its composition, there must be letters, numbers, special characters, and lower and uppercase characters. Furthermore, the password must not be identical to the last passwords used as an additional measure. Also, an account will be locked if a wrong password is used; unlocking them can only be done by a network administrator.

At the local domain level, a directory service (Active Directory) is used, which offers full-scale integrated authentication and authorization services. Thus, users' access to the network is limited according to the department they belong to and the function they hold within the studied public organization. Therefore, users are grouped into groups that correspond to existing departments. With the help of Active Directory, policies have been implemented with different permissions to the directory system on the server, depending on the department or service.

Ordinary users have limited rights; they cannot install and uninstall programs, and they do not have access to the administration level of the operating system. The only ones with unlimited rights in the domain are administrators; they can install or uninstall programs and unlock or block accounts on the network.

Accounts are blocked and subsequently deleted for people who, for various reasons, are no longer active due to medical or other interruptions. All these aspects are highlighted in Figure 4.

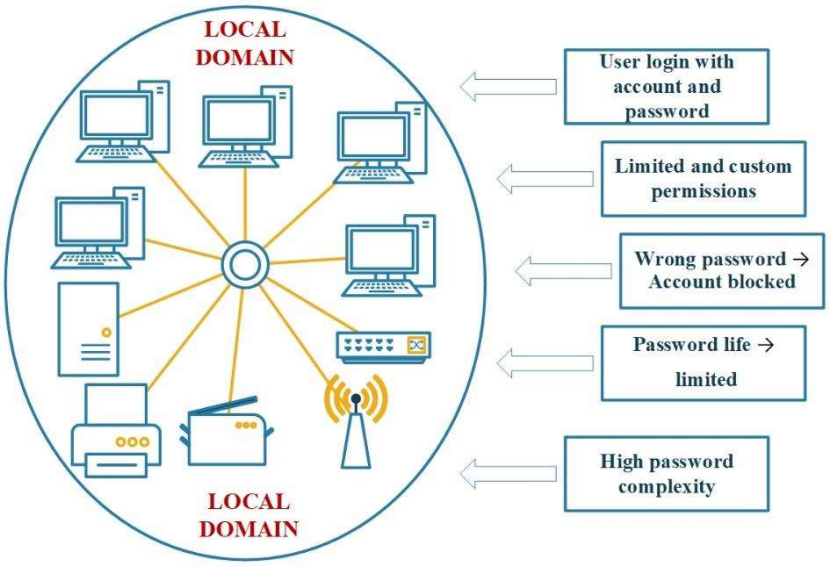

Fig. 4. Policies implemented at the local domain level

A large part of the security policies implemented are at the user account level, and they were implemented on the Windows Server system at the level of the entire domain. In addition, another part of the implemented policies was carried out at the workstation level. These policies are presented in Figure 5.

USB port blocking has been implemented at the station level. By using some storage devices, the risks that can occur are apparent. These storage devices may be from outside the institution, and the risk of bringing viruses or other dangerous elements is relatively high. It is also possible to copy data from the network using these devices. Therefore, to block the USB ports, the way to edit the registers at the USB STOR level was chosen.

CD-ROM blocking has been implemented to eliminate the risks that may arise from using the CD-ROM. There is a risk of infecting the local station and the entire network with viruses from outside the network. Moreover, in this case, there is a risk of copying data from inside the network, just like with USB ports. This security policy was chosen to be implemented on each workstation by locking the CD-ROM through registry editing.

Another locally implemented policy is *Print Screen blocking*. Moreover, this policy was implemented by editing registries. This policy eliminates the risk of making copies of the workstation desktop. Again, this policy was implemented on each workstation by editing the registries.

Using a user account for local access on the workstation. This security policy is implemented at the domain level and eliminates the risk of unauthorized access to the

workstation. This security policy is strengthened because the access password has imposed a high degree of complexity, namely the minimum length of the password and the obligation to use letters, numbers, and special characters. Also, the lifetime of the password is limited, and the new password must be different from the last password used. Using the wrong password results in the account being locked out and requiring the intervention of a network administrator to unlock it.

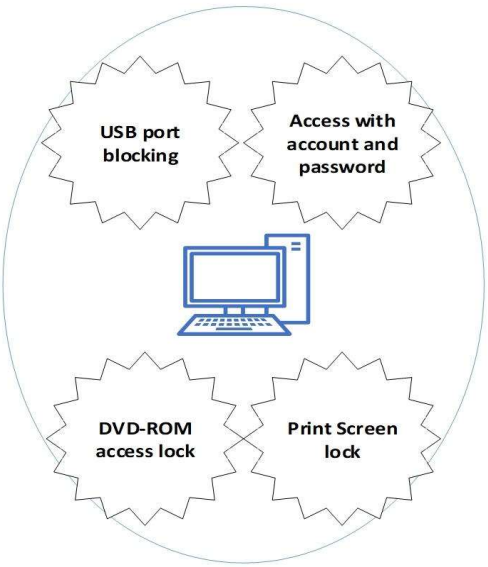

Fig. 5 Policies implemented at the local level

Also, within the framework of proactive measures using an antivirus program implemented at the entire network level within the studied public organization, respectively, on each server and station separately. Calder summarizes some rules for the effective use of an antivirus program [8]:

- An antivirus program must be installed on each computer within a local network;
- Free antivirus software solutions are not recommended because, most of the time, they protect only partially;
- Avoiding the installation of several antivirus programs because compatibility problems may occur, which leads to functionality with low computer performance;
- Correct configuration of the antivirus program;
- Automatic and permanent update of the antivirus program;
- Periodic and automatic scanning of the entire system.

Feinstein believes that the main functions of an antivirus are: real-time scans, scheduled scans, scans on a specific partition or the entire system, scanning e-mail

messages, checking scripts, checking archives, monitoring suspicious activities, and removing identified threats. [9]

An antivirus console-type program is also used for more efficient management. Using the antivirus console allows several facilities that come to the aid of the network administrator, such as (Figure 6):

From the antivirus console, the version of the antivirus software located on each workstation located in the local domain is updated;

- Update to the latest antivirus database for all modules included in the antivirus software;
- Effective global management of security solutions in the local computer network;
- Interface with an efficient overview of the entire local area network;
- Realization of customized configurations of the antivirus application for clients in the network;
- Statistics and reports.

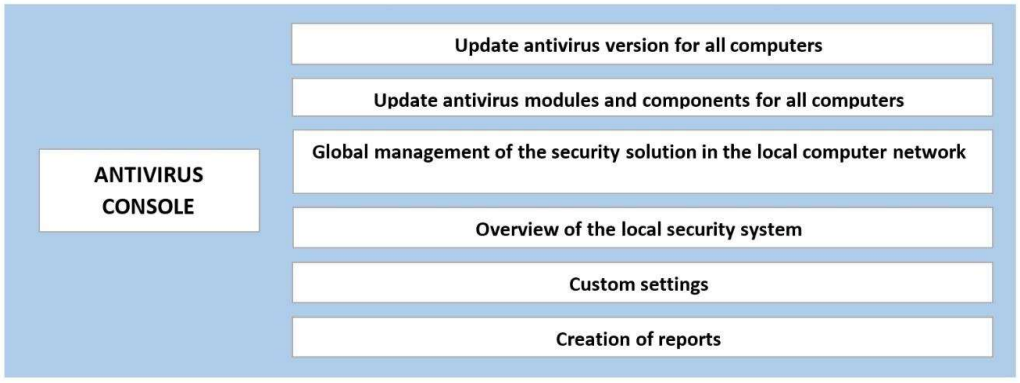

Fig. 6 Antivirus console benefits

The scanning function must be permanently active for the protection provided by the antivirus application to work in real-time. Therefore, maximum efficiency can achieved when the antivirus application is updated to the latest version, and the modules included in the application must updated to the latest version. Only in this way, the risk of access and damage to data in the local network decreases considerably.

Another proactive measure is anticipating a situation where specific data is lost, or even an entire hard drive fails, affecting all its information. All data is saved on a NAS storage device to avoid these situations. Data backups are done automatically daily using an application provided by the NAS device manufacturer. Also, this application provides the ability to recover deleted or compromised data. Moreover, in case of a computer incident that involves the irreparable failure of the hard disk on the

workstation, the data recovery application offers the possibility of restoring the old hard disk to a new one with the data saved on the NAS. The hard disk restoration is complete, with all partitions of the old hard disk with the complete operating system with all settings and all data.

A very high risk of computer incidents can occur by accessing the Wireless network. The wireless connection method has become a necessity due to the multiple devices that can connect to it. On these devices, the level of security is lower than the security of an operating system used on workstations, which leads to an increase in the vulnerability of the entire network. To reduce these risks, take several measures:

- The router used in the wireless network is configured with the WPA2 (WI-FI Protected Access) security protocol, a safer and less vulnerable protocol than the old WEP and WPA protocols;
- A security measure taken is the use of a network that is not normally visible;
- Passwords required to access the wireless network are complex using different characters. Therefore, an additional security measure used for devices that connect to the wireless network is to perform a filter on the wireless router based on the MAC addresses of the connected devices.

These aspects, with the measures taken to avoid the risks of computer incidents in the wireless network, are highlighted in Figure 7.

The wireless network is one of the most exposed and vulnerable elements within the computer system in the studied organization. One measure proposed to reduce these risks is physically separating the wireless network from the internal one. A second Internet service provided by an Internet access provider is needed to separate the two networks. With the implementation of the proposed solution, in this way, in the event of a cyber-attack on the wireless network, the possibility of computer incidents occurring inside the internal cable network is eliminated.

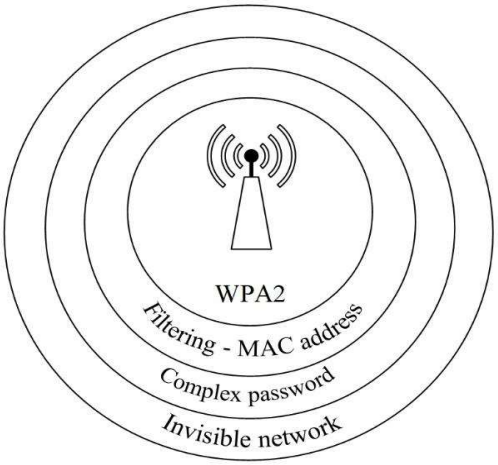

Fig. 7 Wireless network security

Many computer incidents are due to failures of physical devices on the network. The repeated interruption of the electric current or the change of the parameters of the electricity in the supply network can seriously damage these working devices. To avoid these situations, UPS (Uninterruptible Power Supply) devices are used to power all the devices that need to be protected. UPSs protect devices during voltage fluctuations in the power supply network. In a power outage, they can keep the connected devices powered, which they protect for a sufficient time to save the work session and close the applications.

An essential role in IT incidents is due to the human factor. Mainly the lack of training and knowledge in use leads to computer events. To improve this fact, the employees of the IT department provide technical support and train the staff of the studied public organization as often as necessary. Furthermore, most cyber threats come through the e-mail box, so if a risk arises, the IT department notifies the employed staff about the threat as soon as possible.

Continuous education and training of each employee lead to the awareness and responsibility of each employee. Continuous improvement of the products and services offered by the organization is possible only through continuous improvement of the organization's processes. [10]

Conclusions

Digitization of activities in a public organization providing services to citizens is the current new orientation of society. [11] In addition to the obvious advantages it brings, such as reducing the time for certain activities, increasing the quality of services, reducing errors, and increasing efficiency, it also comes with an increase in the degree

of vulnerability that can lead to the occurrence of computer incidents. To reduce these risks, implementing computer incident management is the optimal solution. However, when implementing such a management system, all aspects related to the possible nature of the incidents, the probability of occurrence, the possibility of solving the incident locally or solving it requires outsourcing, and taking proactive measures must be considered.

Implementing a computer incident management system was done in compliance with the legislative framework in force, considering law number 362 of 2018, which establishes the legal and institutional framework, measures, and mechanisms for ensuring a standard high level of network security and computer systems. Another essential tool used is the ISO 27001:2013 standard. This standard helps protect information systems by implementing an information security management system.

The research offers solutions for managing computer incidents in the public organization providing services to citizens studied by carrying out a procedure for solving a computer incident, which tries to provide measures for most possible computer incidents. However, the procedure cannot measure all possible computer incidents, as they are undefined.

To reduce the risks regarding the occurrence of computer incidents, several policies were implemented on the servers in the local network, but some policies were also implemented at the level of each workstation in the local network to avoid computer incidents such as cyber-attacks. Thus, the possibility of connecting in the local domain, on the workstation only, with an individual user account and password was achieved. The password must be changed periodically, and its format is subject to certain imposed conditions. USB port blocking policies have also been implemented, eliminating the possibility of connecting external storage devices, CD-ROM blocking, and Print Screen blocking.

Backup solutions have been implemented on a NAS-type device to eliminate the risks of computer incidents during a hard disk failure or data loss. A proposal is to make a copy of this data in another location to eliminate the risk of computer incidents or data loss in the event of a natural disaster. The existence of images on a NAS device makes it possible to recover information lost during the set time in the NAS device.

The possibility of computer incidents due to the physical breakdown of computer devices within the local network following problems that may occur with the electricity supply network has determined the installation of UPS-type devices to reduce these risks. Our proposal for the next step is to find a solution also for the situation where power outages occur for long periods that exceed the autonomy of current UPS.

The research identified and found solutions to eliminate some vulnerabilities in the wireless network, which can lead to computer incidents, by applying procedures that

make the local wireless network invisible, applying WPA2 protocols, and using complex and strong passwords. To eliminate all risks that may lead to computer incidents, we propose that the studied public organization purchase a separate Internet service from an Internet service provider who is not in the same network as the local computer network.

Another implemented measure is the periodic realization of internal audits on the line of IT activity. At the moment, this type of audit is done only internally. We propose to periodically do an audit by a team of specialists from outside the studied public organization.

Updating and bringing to the latest versions of anti-virus programs and permanent updating of operating systems and applications used in the specialized activity of the employees of the studied public organization is also an effort on the same line of avoiding IT incidents.

An essential aspect is the organization's quality policy. Achieving a high standard of quality by which it is desired to be concise, applied by any employee, and global, referring to all fundamental aspects of quality. [12] The risk of specific computer incidents can be reduced by orienting employees towards increasing quality.

The scientific work presents research on implementing computer incident management within a public organization providing services to citizens. The increasing digitization of activities in the public sector also brings many advantages, such as efficiency, increasing the quality of services, and shortening working times. On the other hand, digitization can be achieved with extensive technology with equipment used within the local IT network to carry out activities, store databases, and interconnect with other IT systems. However, all these equipment and computer systems have a certain degree of vulnerability, and there is a risk of computer incidents.

Through computer incident management, the aim is to identify an incident, report the incident, classify it, assign a person to solve it, and find a solution and remedial measures; if no solutions are found for remediation at the local level - contact the company specialized in solving the incident, solving the incident, incident registration (digital register), incident analysis and evaluation, measures and subsequent planning for prevention.

We must identify possible vulnerabilities and threats to achieve network and network data security. By vulnerabilities, we mean the weak points through which attacks can occur from outside and inside the network. Threats are actions that, through their manifestation, can negatively influence the activity within the IT system. Network and data security involves finding and implementing the most effective decisions that will protect the network and the data existing on the network.

Today, the risk of computer incidents in the form of cyber-attacks is real and present. The success of such attacks is mainly due to the human factor. Therefore, continuous training, information as often as needed, and awareness of the staff employed within the public organization providing services to citizens under study is and must remain a priority.

R E F E R E N C E S

[1] Legea 362, d. 2. (2018). Monitorul Oficial nr. 21/9 ian. 2019.

[2] Pfleeger, P. C. (2015). *Security in Computing - fifth edition.* Pearson Education, Inc.

[3] Johansen, G. (2022). *Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response, 3rd Edition.* Birmingham: Packt Publishing Ltd.

[4] (UE), D. (2016 - 6 iulie). *2016/1148 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL. Official Journal of the European Union.*

[5] Jason, L. K. (2014). *Incident Response & Computer Forensics, Third Edition.* McGraw-Hill Education.

[6] Oprea, D. (2007). *Protecția și securitatea informațiilor, Ediția a II-a.* Iași: Editura Polirom.

[7] Tanenbaum, A. S. (2003). *Reţele de calculatoare - ediţia a patra.* BYBLOS.

[8] Calder, A. (2005). *A business guide to information security.* London: Kogan Page.

[9] Feinstein, K. (2006). *Anti Spam, Viruși, Pop-up, Spyware.* București: Editura Rosetti Educațional.

[10] Oprean, C., Țîțu, M., & Bucur, V. (2011). *Managementul global al organizației bazată pe cunoștințe.* București: Editura AGIR, ISBN 978-973-720-363-2.

[11] Laura Carroll, E. F. (2011). A Comprehensive Approach to Born-Digital Archives. *Archivaria 72*, 61-92.

[12] Țîțu, M. O. (2011). *Cercetarea experimentală aplicată în creșterea calității produselor și serviciilor.* București: Agir.