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 Independenței nr. 313, Bucharest, Romania, (ocosti@gmail.com).
[4]Sc.D Student, University Politehnica of Bucharest, Faculty of Industrial Engineering and Robotics, Splaiul Independenței nr. 313, Bucharest, Romania, (tertereanupetrica@yahoo.com).
[5]Sc.D Student, University Politehnica of Bucharest, Faculty of Industrial Engineering and Robotics, Splaiul Independenței 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