MILITARY UNIVERSITY OF LAND FORCES

Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2023, Volume 55, Number 3(209), Pages 182-205
DOI: 10.5604/01.3001.0053.8961

Resilience of public administration bodies to cyberattacks

Dominika Dudziak-Gajowiak[1], **Artur Szleszyński**[2]*

[1] Faculty of Management and Leadership,
General Tadeusz Kościuszko Military University of Land Forces, Wrocław, Poland,
e-mail: dominika.dudziak-gajowiak@awl.edu.pl

[2] IBM X-Force Centre, Wrocław, Poland,
e-mail: artszl@poczta.fm

INFORMATION

Article history:

Submited: 18 October 2022

Accepted: 18 August 2023

Published: 15 September 2023

ABSTRACT

Public administration bodies are responsible for the organization of crisis management in their allocated area of responsibility. Currently, the exchange of information between elements of crisis management is carried out using the telecommunications system. Thanks to the use of remote sensing, it is possible to exchange data, and build information about the crisis phenomenon on its basis. The responsibility for the protection of information resources is incumbent on heads of municipalities, mayors of cities or marshals of voivodeships (provinces) collecting and processing data in order to carry out the tasks of their subordinate offices. One of the elements of the crisis situation will be a cyberattack carried out against the IT infrastructure of the office in order to hinder or prevent it from performing its tasks. Such incidents have taken place in Poland. Of interest is the issue of managing an incident which directly affects a given office. The article presents an analysis of the cases of cyberattacks described in the media. The paper demonstrates passive reconnaissance methods used by cybercriminals.

KEYWORDS

cybersecurity, information security management in an organization

* Corresponding author

Introduction

Public administration and related organizations are targeted in the same way as commercial enterprises. Public administration, right from the lowest organizational level, has at its disposal information resources which are an attractive object for potential attackers. Many of the data resources used by public administration are classified as sensitive resources. These include, for example, personal data of residents of a municipality, district, province, etc. Municipalities and districts hold information qualified as classified information, e.g. dislocation of military facilities, state protection services, information on companies using hazardous materials for production, landfills of hazardous materials or storage of the reserves, e.g. of fuels, etc.

Since public administration units exist in an environment with which they interact, cyberattacks on cooperating entities, e.g. power plants, fuel suppliers, hospitals, etc. will have a direct impact on the functioning of public administration. Cyberattacks will be the cause of crisis situations, which will be an element of crisis response for the affected organization and the crisis management system of a given level of public administration.

Therefore, public administration bodies should be prepared to protect their information resources. Since many areas of public administration use ICT tools to provide services to the population, the study will focus on the protection of information resources obtained, processed and transmitted through the Internet.

Currently, it is difficult to find a municipality that does not have its own website or does not provide e-mail addresses in order to improve communication with citizens.

This work will present an example of reconnaissance based on commonly available data sources. Examples of cyberattacks against administrative units in Poland will be described.

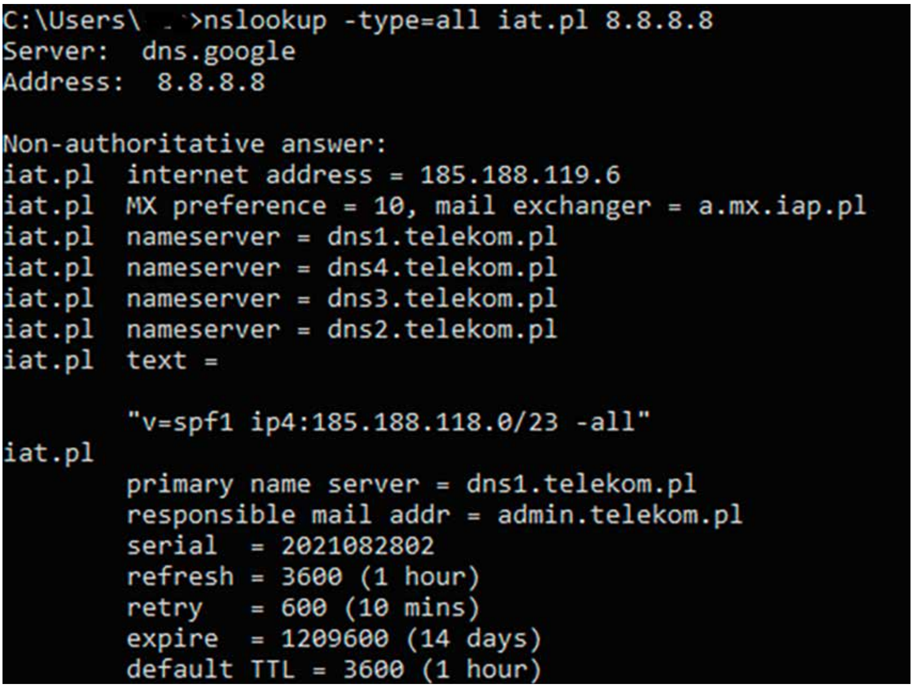
The aim of the study is to present selected examples of successful cyberattacks against local administration units of various levels. The description and analysis of successful cyberattacks is supposed to be used as indication of those areas of cybersecurity that have not been included in information security plans in local government units. The fact that similar methods of cyberattacks are effective means that in the offices of municipalities, districts or provincial marshals the awareness of cyber threats and their consequences is insufficient. The employed research method is a case study described in the available literature.

1. Public administration bodies as a target of cyberattacks

Each reconnaissance begins with obtaining data on the selected target of attack. The work is limited to the passive collection of information, which is allowed by the law in force in Poland. The Czernica municipality in Wrocław district was selected as an example object for data collection. The first step will be to identify the server of WWW webpages supporting the communication of the municipal office with the population. Figure 1 shows how to obtain data on the service operator. A querying tool was used, which is a DNS server (in the example shown, a server supported by Google Inc. company).

The information returned by the DNS server indicates that the municipal office uses the services of an external company maintaining the website. This is now a common practice, relieving an office of the necessity to maintain a server and ensure reliable and secure operation.

Figures 2 and 3 show an example website of Czernica municipality located in the Lower Silesia Province and contact details enabling communication by



```
C:\Users\[redacted]>nslookup -type=all iat.pl 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
iat.pl  internet address = 185.188.119.6
iat.pl  MX preference = 10, mail exchanger = a.mx.iap.pl
iat.pl  nameserver = dns1.telekom.pl
iat.pl  nameserver = dns4.telekom.pl
iat.pl  nameserver = dns3.telekom.pl
iat.pl  nameserver = dns2.telekom.pl
iat.pl  text =

        "v=spf1 ip4:185.188.118.0/23 -all"
iat.pl
        primary name server = dns1.telekom.pl
        responsible mail addr = admin.telekom.pl
        serial  = 2021082802
        refresh = 3600 (1 hour)
        retry   = 600 (10 mins)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
```

Fig. 1. The use of the nslookup command to obtain information about the ICT data of an organization which is a possible target of a cyberattack

Source: The authors' own study.

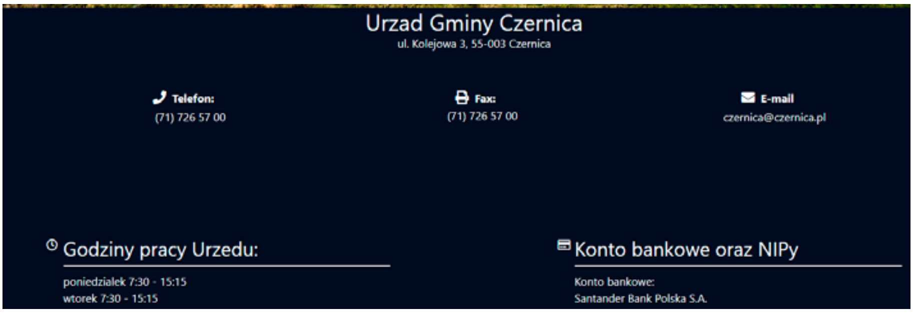
telephone or e-mail. The presented data allows a potential assailant to obtain information about the company maintaining the municipality's website.

In the case of a selected municipality, the company responsible for maintaining the municipality's website is Telekom sp. z o.o. with its registered office in Stary Sącz at Św. Jana Pawła II Street 35. The presented information is an introduction to acquiring knowledge of a potential target of attack, which could be Czernica municipality. The appearance of the website together with contact details is shown in Figures 2 and 3.

An interesting question is the answer to the question about the motivation for launching a cyberattack. It can be assumed that Czernica municipality is connected to the ICT network of Wrocław district, of which it is an element. Thus, an effectively conducted and concealed cyberattack gives a chance to access

Fig. 2. Website of Czernica municipality, Lower Silesia Province

Source: [1].



Urzad Gminy Czernica
ul. Kolejowa 3, 55-003 Czernica

Telefon:
(71) 726 57 00

Fax:
(71) 726 57 00

E-mail
czernica@czernica.pl

Godziny pracy Urzedu:

poniedzialek 7:30 - 15:15
wtorek 7:30 - 15:15

Konto bankowe oraz NIPy

Konto bankowe:
Santander Bank Polska S.A.

Fig. 3. Example of telecommunications data of Czernica municipality

Source: [1].

the ICT network of Wrocław district. And from the ICT network of the district, one can access the ICT network of the Lower Silesia Province. One of the motivations of the attackers will be to gain access to information resources of the offices at other levels than the originally attacked office. Access to computers in these offices allows for infiltrating the ICT infrastructure. What constitutes the greatest value for attackers is the data collected and processed on the computers or other devices seized. What the attacker does with the information obtained will indicate their real intentions. It will also identify the type of attacker. The concept of the type of attacker should be understood as individuals or hacker groups motivated ideologically: propagandist operations, e.g. out of opposition to the policy of local authorities. Financially motivated hacking groups: criminal operations (data theft and sharing, extortion of ransom, anti-state or industrial espionage, etc.). Both types of groups include state-sponsored hacker groups, such as APT28 group or Lazarus. The first of these groups belongs to the Main Intelligence Directorate of the Ministry of Defence of Russia. The other one was created in North Korea and is used to finance North Korea. In 2017, the Lazarus group deleted data from the disks of an online casino in Central America [2]. The Lazarus Group is credited with attacks on e-banking websites in Poland and Mexico [3]. Financing is carried out through the transfer of funds, from electronic banking accounts, in the seized computers.

2. Selected method of attacking a public administration unit

Launching an attack against the selected administrative unit requires preparation. These preparations are a project carried out by the attacker. These projects can be carried out using methodologies such as the "death chain" developed by Lockheed Martin (Fig. 4).

The project begins with collecting information about the selected object of attack. This phase is called reconnaissance. In this phase, the attacker tries to collect as much useful information as possible about the target of the attack. The attacker collects the following data:

- range of IP addresses used by the attack target,
- operating systems and software used by the public administration unit, e.g. e-mail servers, web servers, database servers,
- access points to the ICT network,
- the structure of the network under attack,
- network equipment and security devices used such as routers, firewalls, UTMs (Unified Threat Monitoring – a group of devices combining firewall

functions with an intermediary in the establishment of encrypted connections executed with the use of SSL/TLS protocols and protection against malicious software), NGF (New Generation Firewall – a group of devices the feature of which is the control of transmitted information at the application level. This allows for, e.g., effective reduction of threats related to the operation of malware, e.g. host-server connections, etc.

As the weakest link in the security system is the human being, collecting as much information as possible about the employees of a given public administration unit is one of the most important tasks.

Social media such as Facebook, Linkedin, or the Public Information Bulletin are a very good source of information. The information collected in social media will be included in the data set describing the infrastructure of the attacked object.

Much of the information presented can be collected in an overt and passive way. A passive way of collecting information about an attack target means that there are no direct connections between the attacker and the attack target. This type of reconnaissance uses external sources, made available independently of the object of attack. Thus, passive reconnaissance gives the attacker an advantage, as they do not have to actively scan the object of a future attack. The disadvantage of passive reconnaissance is the lack of significant information items about the target of the attack: e.g. the organization of a computer network, the names of computers, and other resources of the ICT environment. It does not provide information about the vulnerabilities present in the ICT system. This information will be collected during active reconnaissance. In the case of the attack target under consideration, Telkom is responsible for maintaining the website of the office. This company provides an e-mail service based on the Postfix server with the Roundcube communication interface (Fig. 5). Information about the email server in use is obtained directly from the website of the office.

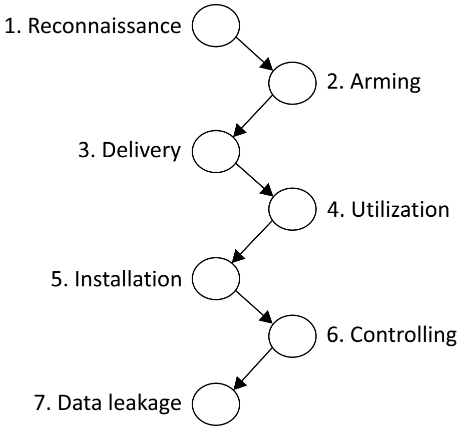


Fig. 4. The process of preparing for and launching a cyberattack – referred to as the “death chain”

Source: [4].

Using the tool for website security analysis, it is possible to determine

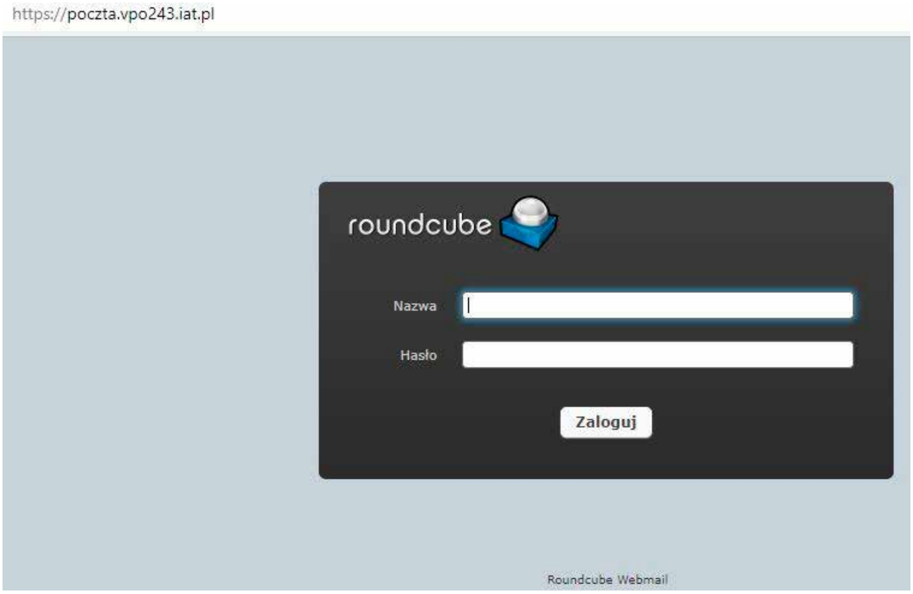


Fig. 5. The login window of the e-mail server of Czernica Municipality Office

Source: The authors' own elaboration.

which services are offered by the server serving Czernica municipality (Fig. 6). Tools such as Shodan periodically send queries to various servers collecting, processing, and presenting information.

Another source of information is the passive DNS. Using passive DNS, it is possible to find other websites supported by the server, as shown in Figure 7.

Based on the collected data, the following information may be obtained:

– the website and webmail of the municipality are supported by a single server owned by the company Telekom,

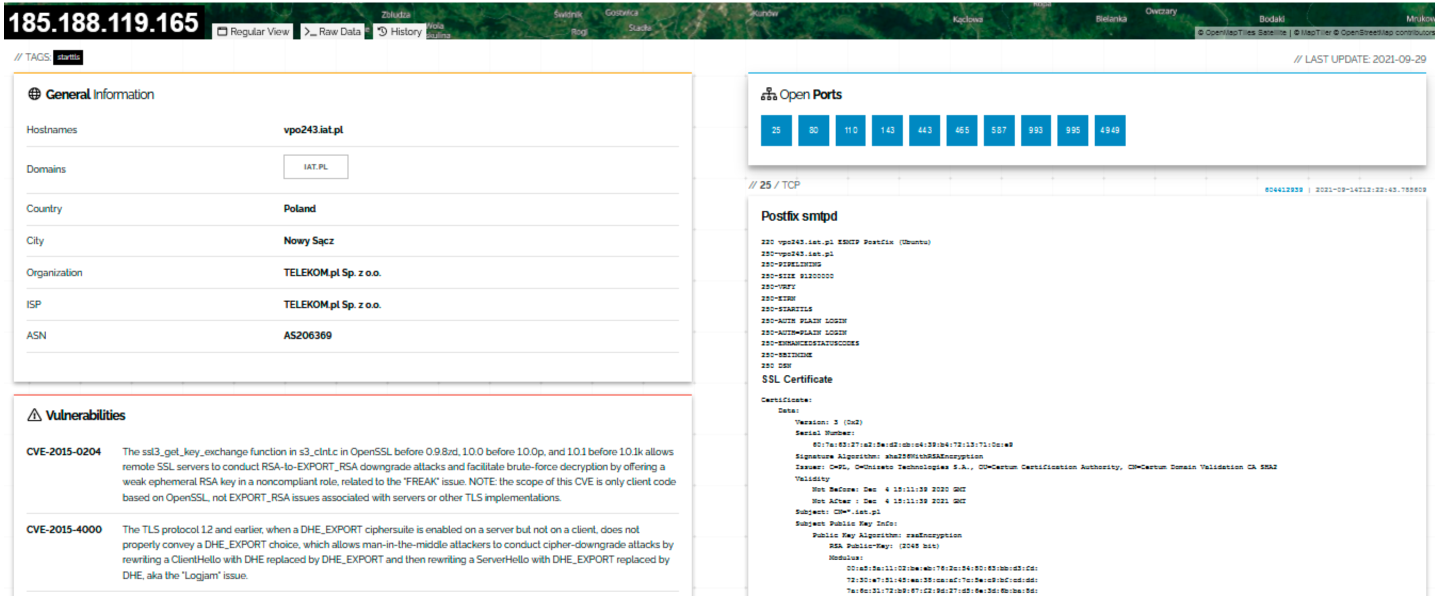
– e-mail uses a Postfix server with the Roundcube graphic interface,

– the server may be susceptible to the threats described in the CVE (Common Vulnerability and Exposers) database: CVE-2015-0204 and CVE-2015-4000,

– the server functions under the control of the Ubuntu operating system.

Since the server stores the website and email of the office, an attack against it will allow an intruder to gain access to the municipality's computers. This will allow for the enumeration of computers as well as network and peripheral devices installed in the municipal office.

As a possible means of attack, spearphishing based on sending emails with attachments containing malicious code is proposed for consideration. Activating the attachment on the user's computer will cause the malicious code



Hostnames	vpo243.iat.pl
Domains	IAT.PL
Country	Poland
City	Nowy Sącz
Organization	TELEKOM.pl Sp. z o.o.
ISP	TELEKOM.pl Sp. z o.o.
ASN	AS206369

CVE-2015-0204 The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.

CVE-2015-4000 The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

Postfix smtpd

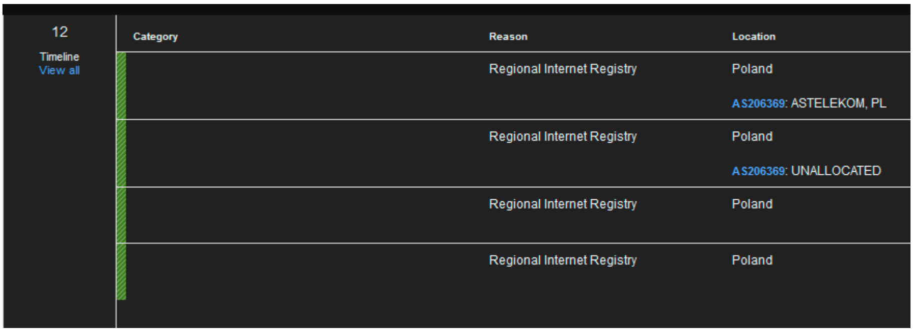
```
220 vpo243.iat.pl ESMTP Postfix (Ubuntu)
250-vpo243.iat.pl
250-PIPELINING
250-SIZE 91200000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            60:7a:63:27:a2:5e:d2:cb:c4:39:b4:72:13:71:0c:e9
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=PL, O=Unizeto Technologies S.A., OU=Certum Certification Authority, CN=Certum Domain Validation CA SHA2
        Validity
            Not Before: Dec  4 15:11:39 2020 GMT
            Not After : Dec  4 15:11:39 2021 GMT
        Subject: CN=*.iat.pl
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a5:5a:11:02:be:eb:76:2c:54:50:63:bb:d3:fd:
                    72:30:e7:51:45:ea:35:ca:af:7c:5e:c9:bf:cd:dd:
                    7a:6c:31:72:b9:67:f2:9d:27:d5:6e:3d:6b:ba:5d:
```

Fig. 6. Services offered by the server of Telekom Sp. z o.o. supporting the website and e-mail of Czernica municipality

Source: [5].



12

Timeline
View all

Category	Reason	Location
	Regional Internet Registry	Poland AS206369: ASTELEKOM, PL
	Regional Internet Registry	Poland AS206369: UNALLOCATED
	Regional Internet Registry	Poland
	Regional Internet Registry	Poland

Fig. 7. Domains hosted on the server 185.188.119.165

Source: [6].

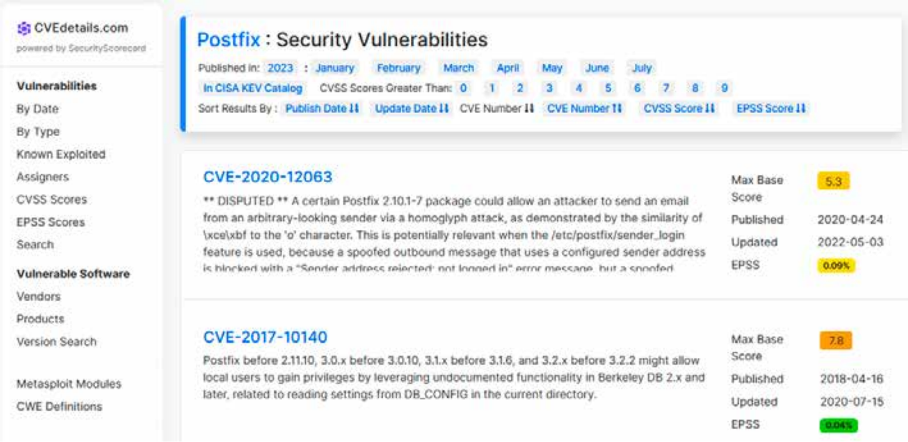
to be downloaded and then executed. The fact of correct loading and executing the malicious code will be confirmed by sending a message to an email address e.g. hotmail. A free email accounts service will allow the intruder to hide their identity. The best choice is to locate the email server in a country whose law does not oblige the institution that maintains the server to disclose its users' data.

The next task will be an active scan of the selected public administration unit. An effective way to test the security measures would be to send an enquiry about the tender organised by said unit. The feedback may include information on, for example, the anti-virus software used or spam protection software. Shown in Figure 6, the information includes data about the operating system and e-mail server used. This information allows the hacker to search for vulnerabilities in both of these products.

Examples of vulnerabilities for the Postfix e-mail server are shown in Figure 8. On the day the vulnerability database was checked, 57 different vulnerabilities were found. The knowledge of vulnerabilities allows for finding or developing a program that exploits a particular vulnerability, enabling the hacker to gain access to the program.

The described activities contained 3 elements of the "death chain": reconnaissance, arming and delivery.

The presented description of the preparation and partial preparation of the attack will serve to illustrate how cybercriminals can successfully attack public administration units.


CVEdetails.com
powered by SecurityScorecard
Vulnerabilities
By Date
By Type
Known Exploited
Assigners
CVSS Scores
EPSS Scores
Search
Vulnerable Software
Vendors
Products
Version Search
Metasploit Modules
CWE Definitions
Published in: 2023 : January February March April May June July
In CISA KEV Catalog CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : Publish Date ⇅ Update Date ⇅ CVE Number ⇅ CVE Number ⇅ CVSS Score ⇅ EPSS Score ⇅

Postfix : Security Vulnerabilities

CVE-2020-12063

** DISPUTED ** A certain Postfix 2.10.1-7 package could allow an attacker to send an email from an arbitrary-looking sender via a homoglyph attack, as demonstrated by the similarity of \xce\xbf to the 'o' character. This is potentially relevant when the /etc/postfix/sender_login feature is used, because a spoofed outbound message that uses a configured sender address is blocked with a "Sender address rejected: not logged in" error message, but a spoofed

Max Base Score 5.3
Published 2020-04-24
Updated 2022-05-03
EPSS 0.09%

CVE-2017-10140

Postfix before 2.11.10, 3.0.x before 3.0.10, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 might allow local users to gain privileges by leveraging undocumented functionality in Berkeley DB 2.x and later, related to reading settings from DB_CONFIG in the current directory.

Max Base Score 7.8
Published 2018-04-16
Updated 2020-07-15
EPSS 0.04%

Fig. 8. List of detected vulnerabilities in the CVE database for the Postfix email server

Source: [7].

3. Cyberattacks on public administration units in the Republic of Poland

The recording of attacks against public administration units became the responsibility of CERT (Computer Emergency Response Team) Poland. CERT Polska was established at NASK (Naukowa Akademicka Sieć Komputerowa – Academic Scientific Computer Network). The reports on the state of cyberspace security in Poland contain information about cyberattacks on administrative offices in Poland. In 2014, a CERT report claimed that the website of the Office of the President of the Republic of Poland had been attacked. The perpetrator of the attack was a Russian hacking group called “Cyber Berkut” [8]. The reason for the attack was the support, expressed by the Polish authorities for Ukraine in its conflict with Russia. In 2014, Russia occupied the Crimea peninsula, where the Russian Navy base is located. The second one of the institutions under attack was the Warsaw Stock Exchange. In the same year, a data leak from the Stock Exchange server was reported. A file containing hash functions was stolen. The file containing hash functions stores users’ passwords and, more specifically, their hash functions. A hash function is cryptographically irreversible, which means that it is not possible to obtain a user password by performing mathematical transformations, e.g. in reverse order. However, by using “rainbow tables”, the process of guessing a user’s password can be sped up by creating pre-determined strings of hash functions [9]. This method is more effective in comparison to the "brute-force attack" method, where an attempt is made to guess the user's password by means of successive attempts. Time reduction is 87% shorter compared to the "brute-force attack" method.

The method of both attacks is unknown. In the case of the Stock Exchange data leak, it is likely that software classified as APT was used, where APT is a program which may have resided in an infected system for several months.

In 2019, in the CERT Polska report, there is information about 7 successful cyber-attacks against municipal or district offices. The most widely described one was the successful cyberattack against Kościerzyna municipality [10]. As a result of using a ransomware program, the data on the computer disks of the municipal office becomes encrypted. The attempt to recover data from the backup failed because the disks on which the backups were stored had also been encrypted. Thanks to the partnership with the company Kaspersky[1], it was possible to develop a program decrypting the data. In the incident, the Mapo ransomware was used. The computers of the office were probably infected as a result of opening an attachment file arriving with an email. The use of the word "probably" stems from the fact that not much data was provided on the incident, such as: how did the infection occur? Was the e-mail the access point to the office's computer network? If so, which of the messages contained malware? Did the office have antivirus software and why did it fail to detect a malicious attachment? Were the computers belonging to the Kościerzyn District Office infected as a result of the incident?

This data forms the basis for the following tasks in the process of managing information security within an administrative office, such as:

- risk analysis – modification of the analysis,
- modification of operation continuity plans in the area of ensuring the continuity of IT/ICT systems operation,
- modification of training plans for the office personnel on information security in ICT systems,
- incident conclusions – modification of rules for storage and creating data security copies.

To sum up the incident described – the municipality was very fortunate, as the encrypted data was recovered. The office downtime was not long. Why was the term "fortune" used? As a result of an error in the encryption program code [11], it was possible to recover the keys to decrypt the data, which protected the office from paying the ransom and violating financial discipline.

[1] See: https://cert.pl/posts/2019/12/free-decryption-tool-for-mapo-ransomware/.

Data decryption is not always an option especially if the hacker uses a Viper-type program designed to destroy it.

A month later, a different public office is attacked in the same fashion as the Municipality Office in Kościerzyna [10]. This fact necessitates taking into consideration what the level of protection for collected and processed data in the offices of municipalities and counties is. A valid question, since about one and a half months after the incident in Kostrzyn, another public office faces a similar attack. A period of 1.5 months is sufficiently long for a data leak. Being a valuable source of information for criminal groups, this data could become a commodity in the "DarkNet".

Based on the cases described, it can be mistakenly assumed that incidents in the security of information kept in ICT systems, occur in municipal offices. In October 2020, Oświęcim District Office became the target of a cyberattack. The targets of the cyberattack were: the Department of Surveying, Cartography, Real Estate Management as well as the Department of Investment, Development and Roads [12]. CERT Polska, the Police and the Office for Personal Data Protection were informed about the incident. The data was encrypted, and the District Office decided to pay a ransom in the amount of PLN 602,000 [13] for decrypting said data. The ransom was not paid in directly. There was speculation that the tender conducted by the district authorities was a disguised form of paying the ransom. The company that won the tender was supposed to pay the ransom on behalf of the district administration [14]. There is no supporting evidence for the presented thesis, but the fact that the selected company did not have information on successful attempts to recover encrypted data allows for the conclusions presented [14].

Which local government units are targeted by cybercriminals? The comparison of the three local government units subject to cyberattack is presented in Table 1.

Table 1. Summary of statistical data of local government offices targeted by cyberattack

Public office name	Area [km^2]	Population
Municipal Office in Kościerzyna, Pomerania Province	310	13295
District Governor's Office of Oświęcim District in Lesser Poland Province	406	154292
Lesser Poland Marshal's Office	15183	3400000

Source: The authors' own elaboration.

The local government units shown in Table 1 fell victim to cyberattacks over the years 2019-2021. There are three known cases (listed in Table 1) of successful cyberattacks. As a result of them, the operations of the public offices were reduced to a greater or lesser extent. The case of the Marshal's Office of Lesser Poland Province is an interesting one. In February 2021, the aforementioned office becomes the target of a cyberattack [15]. The target of the attack was an e-mail server belonging to the office. The hacker paralyzed the operation of the mail server. It remains unknown how they had it done. The case was reported to the Police, no information was found regarding the notification to CERT Polska or to the Personal Data Protection Office. The attack resulted in the shutdown of some of the IT systems used by the office. According to the information of the "Kraków Nasze Miasto" portal, the data of the office was encrypted. Cybercriminals demanded a ransom paid in bitcoins. Allegedly, the amount of the ransom was several million zlotys. After four months of investigation, the prosecutor's office was unable to identify who had carried out the cyberattack. This is yet another case of a successful use of a ransomware program. If the attack was not carried out from inside the office, it should be assumed that the ransomware was delivered from outside. The probable channel of distribution was via e-mail. In many campaigns, email is used to spread malware. This happens because for the attacker e-mail is the only point of access to the computer devices of a public office. The e-mail server belonging to the office is maintained by S-Net Sp. z o.o. On the website of the company managing the service, there is information that, in addition to the Marshal's Office, the Kraków City Hall and the US Consulate are also the customers of the company. Thus, the acquisition and exploitation of data in the form of electronic correspondence will be a valuable resource for attackers.

In March 2021, an amount of PLN 1.5 million [16] is transferred from the accounts of Rewitalizacja Company, which is controlled by the Radom City Hall, to the accounts of fraudsters. The accountant receives a call from a "Police Officer", who informs her that the company's money deposited in the bank is at risk of being seized by hackers. At the same time, the "police officer" suggests transferring money to the indicated bank account in order to protect it from being taken over by the hacker(s).

Transfers are sent and the criminals gain access to the company's money. The attack described is an example of a vishing variation of a phishing attack, with the difference that email or text messages are replaced by a phone call. The described type of cyberattacks is based on "social engineering", the purpose of which is to deliberately mislead the interlocutor and persuade them to perform certain activities, e.g. transfer money or provide personal data.

4. Attacks on conjoined facilities not belonging to local government units

In Poland, such attacks have not yet occurred or have not been described by the media or CERT teams. Attacks on power plants and oil processing companies have already taken place around the world. Similar attacks targeted hospitals, pharmaceutical companies, and universities. The most spectacular incident against conjoined facilities was a cyberattack on 23 December 2015 in which Kyivoblenergo, a company supplying electricity to the city of Kyiv, was attacked. The detection of the incident was due to the occurrence of a major grid failure. Several transmission substations were switched off, which deprived consumers of electricity. The power outage resulted from unauthorized access to the company's computer controlling the SCADA system. Initially, it was predicted that about 80,000 electricity consumers would be affected by the attack. However, it turned out that three other sub-suppliers had also been attacked. As a result, there occurred a power outage cutting off 225,000 customers from electricity. Shortly after the described incident, Ukrainian authorities accused hackers affiliated with Russia's security service of causing the incident. Investigation of the cause of the failure was entrusted to institutions responsible for cybersecurity from Ukraine and the United States. One of the institutions participating in the post-intrusion analysis was the SANS Institute from the United States.

In connection with the incident, the US Department of Homeland Security issued an official report entitled IR-ALERT-H-16-056-01. According to the report, three regional energy companies became the target of a coordinated cyberattack. The attack on each supplier lasted approx. 30 minutes. As a result of the described cyberattack, 225,000 customers were left without electricity supply. Power companies were forced to manually control the transmission network. The power outage lasted for several hours. At that time, energy companies operated to a limited extent, trying to restore normal functioning.

The described event was the first publicly confirmed attack on an energy transmission grid. The targets of the attack were electricity supply companies. The incident itself can be treated as insignificant as the number of affected consumers in relation to all electricity consumers in Ukraine was not large. The incident had a local scope and concerned the city of Kyiv. The small significance of the incident is related to the number of recipients aggrieved as a result of the incident. The number of people living in Kyiv is 2,967,360. Thus, 225,000 recipients account for 7.6% of the city's population. In addition, the duration of the incident was limited (a few hours). Yet, for the companies that suffered damage as a result of the incident described above, this was an event classified as critical. Critical events affect the reliability of the services that these companies provide.

The analyses did not refer to interconnected networks such as water, gas or telecommunications networks. Most control devices are electrically powered. In the event of a power shortage, they are disconnected, depriving the population in the crisis area of the media supply. As a result of the impact of the incident on the interconnected networks, losses increase very quickly.

5. Preparing and conducting a cyberattack on the power grid in Kyiv

Carrying out a cyberattack on the power grid infrastructure required planning and preparation. These are elements that occur in project management. The project was divided into stages. In the first stage, the attackers collected information about the power grid, the entities supporting it and the interdependencies between them. It is not known how much data was available to the public. This stage of the project is called reconnaissance. According to the publication of the SANS Institute, they were not found to be the subject of reconnaissance conducted by a potential attacker. What was explored by the attacker was the automation systems used in controlling the operation of the power grid. The coordination of the attack indicates that only selected elements of the transmission system were explores. Such elements that, in the opinion of the attackers, gave a chance for a successful attack.

The next action was to find vulnerabilities in the used control systems. After finding vulnerabilities, another element was the development of software allowing the attackers to seize control of the control devices. The last element was finding entry points to the control system, installing malware and running it. Finding an entry point to the control system is difficult because systems of this class are not connected directly to external networks (e.g. the Internet). Therefore, it cannot be ruled out that people employed by the attacked electricity suppliers were used to obtain information about a possible entry point into the automation network controlling the transmission network. Such actions save the time needed to recognize vulnerabilities occurring in network monitoring and control computers.

6. Reasons for the success of cyberattacks against public administration units

The first of the reasons that led to the effective attacks on the offices of: municipality, district and provincial marshal's office was the low awareness of cyber threats among the employees of such offices. If the entry point to the computer network was electronic mail, and such an assumption can be made based on the available data, then the users should be informed how to handle attachments in messages. Probably each of these offices receives dozens or hundreds of messages with attachments every day. With such a number of attachments, "manual browsing" of each of them is a pointless task. Authorities should purchase or lease software that verifies attachments containing malicious code. Such attachments are part of a phishing attack which is dangerous for both desktop and mobile devices. Users should be educated about the rules for handling attachments received by electronic mail. In the case of Word text editor or Excel spreadsheet files, a macro embedded in the file must not be allowed to run if the file does not come from a trusted sender. And even in this case, caution is advised because malicious code may be attached to the file. Electronic mail is used to proliferate malicious code. Electronic mail very often constitutes the only entry point into the ICT system of the object of attack. Returning to the presented object of attack, hacking into the server of a public office's website may bring reputational damage. However, the separation of the website server from the office infrastructure will not affect the operation of the ICT infrastructure. In the case of electronic mail, the message can be downloaded to the hard drive of the computer in the office. Running the malicious code in the macro attached to the document will directly affect the devices in the office. Its spread in the environment is aimed at infecting more computers. Since the attempts to establish connections come from within the ICT network, they are not checked in such detail as in the case of traffic coming from the Internet.

The caution in the case of macros attached to document results from the fact that this program may contain instructions responsible for downloading a file with malicious code to a computer or other device , e.g. one encrypting files on a computer. In order to bypass detection by malware detection software, encryption software is used. They are responsible for encrypting the malicious file so as to prevent it from being detected on the basis of a digital signature. After downloading a file to the disk, software is launched to decrypt the malware, which proceeds, e.g. to establish a connection to the control computer or encrypt the files in the folder. These programs will try to get inside the network in order to infect more computers. In order for the transfer process between computers to be effective, the malware checks whether there is a copy of the program on the target computer. At the end of their operation, the programs are removed from the disks of the infected computer concealing their malicious activity.

No configuration or improper configuration of malware detection and neutralization software. Antivirus software may delete or quarantine a suspicious file when it is detected. The system administrator is informed about the fact that a suspicious file has been detected and blocked. The described activities include the organizational and technical aspect of data security in the ICT system.

The lack of software and hardware protecting public offices, e.g. antivirus software, anti-spam/anti-phishing systems or NGF devices can be understood. This lack is the result of the high cost of purchasing the listed elements, which is an expense exceeding the financial capabilities of a municipality/district. However, the lack of staff training in a public office is something incomprehensible. The costs of such training can be covered by a municipality or district. Such training can be carried out in the form of remote training or e-learning. The second form is more convenient, as it allows for the distribution of the number of trainees over time, minimizing disruptions in the functioning of the public office.

There is probably no current inventory of ICT equipment and software installed on it in public offices.

When cybersecurity incidents occur, employees should know how to proceed, what actions should be taken to minimize the negative effects of the incident and who should be informed about the occurrence of the incident. Without such knowledge and skills, incident response will be ineffective.

This is where the problem of personnel assigned to act in response to a cybersecurity incident arises. Most of municipalities are small or medium-sized organizations in which 1 or 2 people are employed in the IT department. In many municipalities, there is a problem with finding staff with knowledge and experience in the protection of information resources. Based on the research conducted by the authors using the pracuj.pl portal, the number of job offers for people dealing with cybersecurity in the Wrocław region amounted to: 18. The research was performed on 25.07.2021. The number of returned results for the query “IT security” & “Wroclaw up to 15km” amounted to 37. Of which 18 were relevant to the query. The number of job offers from the government or local government administration – 0.

The lack of a competent specialist means that controlling and responding to ICT security incidents is not feasible [17]. Supporting users of IT systems is an absorbing activity and fills the working time of the person(s) from the IT department. Tasks related to cybersecurity and information infrastructure management should be separated [17]. Such separation cannot be afforded by municipal or district authorities due to the lack of personnel. One possible solution is to entrust the tasks of cybersecurity incident detection to an external company. The outsourcing of security services is used in many organizations. Leasing ICT security management services enables organizations to reduce costs. There is no need to hire personnel, purchase, install and configure specialized software. This makes the project related to monitoring the security of the ICT infrastructure more likely to be successful. In the opinion of the authors, the merger of municipalities within the district will reduce the costs associated with the implementation of security services. Because the ordering party will be several organizations and not one and the number of purchased services will be greater, which translates into the price for the service.

In the event that municipalities and the district do not reach an agreement on the purchase of a safety management service, will they not be able to effectively protect their resources? The answer to the question posed is not clear. It will require the performance of many tasks related to: planning, implementation, control and improvement within the system of protection of information resources. IT departments must prepare and implement the following elements of the information security system:

1) preparation and maintenance of inventory: computer hardware, software, network and peripheral devices,
2) updating the system and business software as part of the licenses held in order to reduce the likelihood of effective use of the detected vulnerabilities,
3) purchase and update of EDR-class software (Endpoint Detection and Response) in the office along with periodic scanning of computers connected to the public office’s computer network,
4) separation of the computer network between the organizational units of the office in order to reduce the likelihood of malware transmission,
5) defining and enforcing rules for managing user accounts, e.g., full-time employees, temporary employees, external employees working in co-operation with the office,
6) preparation of rules for the cooperation of the public office ICT system with external entities, e.g., higher and lower levels of public administration, external companies (rules for granting access to data, scope of data exchanged, methods of verifying external users, etc.),

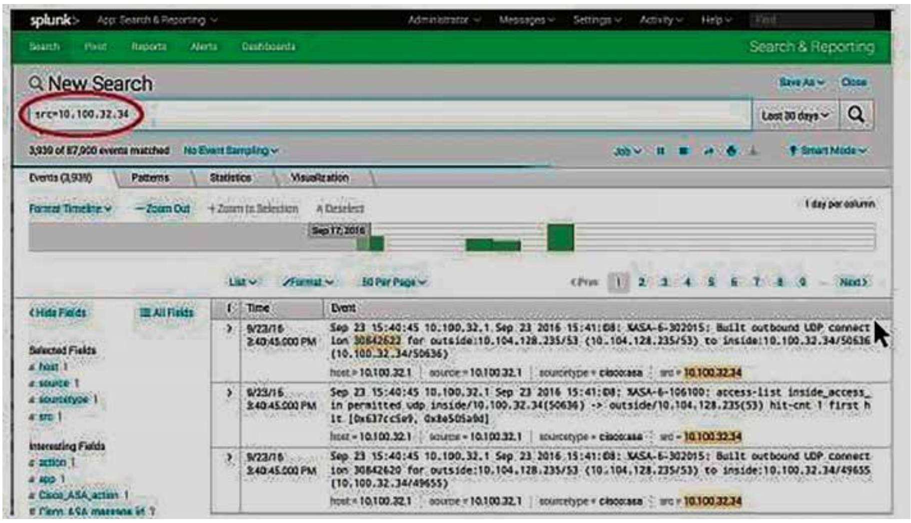
7) part of the backup copy transferred to the cloud (you can copy those groups of data for which there are no restrictions on their transfer, for example, outside the borders of the Republic of Poland),
8) verifying and testing backup copies,
9) encryption of data constituting highly sensitive resources, e.g. financial data, human resources data, data on economic turnover, etc.,
10) regular review of event logs of computers, peripherals, network devices,
11) establishment and training of an ICT security incident response team,
12) development of plans for restoration after a potential failure or disaster, along with the identification of technical parameters such as: the time required to restore the operation of selected elements of the ICT system, etc.,
13) theoretical and practical training of the office staff,
14) cooperation with CERT Polska and/or commercial entities in the area of susceptibility scanning in the ICT system of the public office.

The measures listed determine the effectiveness of the information security system. It is important to remember when creating an information security management system that the data to be secured is not limited to personal data. The effective operation of an information security management system depends on the understanding of its resources. An inventory is a document of major importance for the protection of the information resources. Activities such as asset inventory can be entrusted to specialized software that will relieve the IT staff from the routine and time-consuming task of performing inventory activities and verifying the results.

A similar kind of improvement can be provided by EDR-class programs and automatic distribution of operational system updates. In the case of the second class of ICT systems, this option is found in the operating system, which also reduces the workload of the IT department.

Task 10 is difficult to complete without specialized software such as a SIEM (System Information and Evidence Management) class system. This system collects data from selected infrastructure points, processes it, groups it and then filters it based on predefined filtering rules. An example of a filtering rule is shown in Figure 9 in the “New Search” section.

SIEM-type solutions relieve a data analyst of the necessity to “manually” read data from selected devices and then to standardize and subject it to analysis. An analyst can focus on evaluating the detected incident and on ways to mitigate its destructive impact. The result of the analysis will be a faster response to the incident which will give the attacker less time to act.



```
src=10.100.32.34
```

3,939 of 87,900 events matched

```
9/23/16            Sep 23 15:40:45 10.100.32.1 Sep 23 2016 15:41:08: %ASA-6-302015: Built outbound UDP connect
2:40:45.000 PM     ion 30842622 for outside:10.104.128.235/53 (10.104.128.235/53) to inside:10.100.32.34/50636
                   (10.100.32.34/50636)
                   host = 10.100.32.1 | source = 10.100.32.1 | sourcetype = ciscoasa | src = 10.100.32.34
9/23/16            Sep 23 15:40:45 10.100.32.1 Sep 23 2016 15:41:08: %ASA-6-106100: access-list inside_access_
2:40:45.000 PM     in permitted udp inside/10.100.32.34(50636) -> outside/10.104.128.235(53) hit-cnt 1 first h
                   it [0x637cc5e9, 0x8e505a9d]
                   host = 10.100.32.1 | source = 10.100.32.1 | sourcetype = ciscoasa | src = 10.100.32.34
9/23/16            Sep 23 15:40:45 10.100.32.1 Sep 23 2016 15:41:08: %ASA-6-302015: Built outbound UDP connect
2:40:45.000 PM     ion 30842620 for outside:10.104.128.235/53 (10.104.128.235/53) to inside:10.100.32.34/49655
                   (10.100.32.34/49655)
                   host = 10.100.32.1 | source = 10.100.32.1 | sourcetype = ciscoasa | src = 10.100.32.34
```

Fig. 9. Example of data search in a SIEM system on the example of Splunk Enterprise
Source: [18].

When creating a COB, the roles should be separated, which means that the COB and the Information Technology Centre are separate organizational units. This requirement must be observed, as the analyst cannot simultaneously be the person responsible for making sure that the ICT system is being monitored. That kind of situation constitutes a conflict of interest.

The data collected by the SIEM system can be used by law enforcement authorities as well as by the court during the trial of the attacker. It must be properly secured so that it can serve as evidence in legal proceedings. What is being discussed here is the chain of custody, which requires adequate and documented handling of acquired digital evidence. The chain of custody organization is designed to protect digital evidence from intentional or accidental damage, destruction or modification. In legal proceedings, the above-mentioned actions discredit the collected evidence.

Another important element is to carry out vulnerability scanning. It allows for detecting vulnerabilities in the investigated system and removing them before attackers do so. Such a measure reduces the chances of a successful cyberattack. Vulnerability scanning should be outsourced to an external organization. Prior to scanning, a framework for testing (what elements of the system will be tested and when) should be established. Moreover, a request for confidentiality of the entity performing such scanning should be made.

A vulnerability scan report should serve to rectify the identified defects, thus increasing the level of cybersecurity in the institution. This is an example of the verification of the introduced security measures in the elements of the organization's ICT system in accordance with the PN-ISO/IEC 27000 standard and the Deming model contained therein. According to the standard, the ICT security management process is based on 4 tasks: planning, implementation, verifying and actions aimed at improving the information security management system [19]. A system that operates according to the described process has a chance of surviving a cyberattack and incurring less damage.

Several conclusions can be drawn from the presented description. Organizing a COB is a costly and time-consuming project. Obtaining technical components is a more or less complicated task, but one that can be accomplished. The element associated with employing and retaining personnel is more complicated. Public administration entities will be forced to compete with commercial entities. This, in turn, may lead to a situation where it is not possible to collect sufficient COB staff. The staff shortage will delay the launch of the COB, and if the COB is launched with incomplete staffing, it may cause it to function incorrectly. The solution to such a problem is to hire (outsource) COB services from specialized companies, which relieves government administration entities of the need to create and maintain their own COB. The described solution is commonly used by commercial entities and public administration. On a large scale, outsourcing of security monitoring services by public administration takes place in the Kingdom of Denmark. This solution reduces the costs of running COB taking the burden of equipment purchases and hiring cyber security specialists off of the entity purchasing the monitoring service.

Conclusions

The described cyberattacks show that the awareness of cybersecurity threats is not common in public administration. The fact that a similar type of threat effectively uses the same vulnerabilities several times in different locations and at different times confirms the presented thesis.

They have not yet occurred, or information about them has not been made public – cyberattacks against conjoined facilities, such as: power plants, gas or water supply plants. If government entities have not been able to deal with a point cyberattack then they will not be able to cope with a distributed cyberattack. This is due to the limited quantity of resources at the disposal of public offices. The size of the office is irrelevant, as municipal offices, district offices or province level offices have fallen victim to cyberattacks. The example of the Marshal's Office of the Lesser Poland confirms the formulated thesis.

The remedy for the current situation is to combine the efforts of the public offices in order to obtain external resources that provide better protection against cybercrime. In addition, training office employees is also required. The training should include awareness of threats and procedures for handling the detection of an ICT security incident. Most of the incidents described could have been avoided if employees had been trained and knew how to behave when the incident was detected.

References

1. [online]. Available at: https://czernica.pl/ [Accessed: 10 October 2021].
2. *Przetarg w urzędzie na odszyfrowanie danych po ransomware? Zapłata w PLN nie BTC ;-) Bohater? System geodezyjno-kartograficzny w Oświęcimiu*, [online]. Available at: https://sekurak.pl/przetarg-w-urzedzie-na-odszyfrowanie-danych-po-ransomware-zaplata-w-pln-nie-btc-bohater-system-geodezyjno-kartograficzny-w-oswiecimiu/ [Accessed: 9 October 2021].
3. Kálani P, Cherepanov A. *Lazarus KillDisks Central American casino*, [online]. Available at: https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/ [Accessed: 8 October 2021].
4. *LockheedMartin*, [online]. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Accessed: 10 October 2021].
5. [online]. Available at: https://www.shodan.io/host/185.188.119.165 [Accessed: 10 October 2021].
6. [online]. Available at: https://exchange.xforce.ibmcloud.com/ip/185.188.119.165 [Accessed: 10 October 2021].
7. [online]. Available at: https://www.cvedetails.com/ [Accessed: 30 July 2023].
8. *CERT Polska Raport 2014*, [online]. Available at: https://cert.pl/uploads/docs/Raport_CP_2014.pdf [Accessed: 8 October 2021].
9. Oechslin P. *Making a Faster Cryptanalytic Time-Memory Trade-Off*. The 23rd Annual International Cryptology Conference, CRYPTO '03. Lecture Notes in Computer Science. 2003;2729:617-30.
10. *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2019 z działalności CERT Polska*, [online]. Available at: https://cert.pl/uploads/docs/Raport_CP_2019.pdf [Accessed: 8 October 2021].
11. *TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. March 18, 2016*. Washington: SANS Industrial Control System, Electricity Information Sharing And Analysis Center, [online]. Available at: https://pdf4pro.com/amp/view/tlp-white-analysis-of-the-cyber-attack-on-the-ukrainian-57c2eb.html [Accessed: 4 January 2021].
12. *Komunikat ws. awarii systemu teleinformatycznego w Starostwie Powiatowym w Oświęcimiu*, [online]. Available at: https://www.powiat.oswiecim.pl/aktualnosci/

komunikat-ws-awarii-systemu-teleinformatycznego-w-starostwie-powiatowym-w--oswiecimiu/ [Accessed: 10 October 2021].

13. *Opis grup hakerskich oraz stosowanych przez nie taktyk i technik. Mitre Att&ck*, [online]. Available at: https://attack.mitre.org/groups/ [Accessed: 30 September 2021].
14. *Ransomware – zapiski z placu boju*, [online]. Available at: https://sekurak.pl/ransomware-zapiski-z-placu-boju/ [Accessed: 10 October 2021].
15. *Małopolski Urząd Marszałkowski zaatakowany przez hakerów*, [online]. Available at: https://samorzad.pap.pl/kategoria/aktualnosci/malopolski-urzad-marszalkowski-zaatakowany-przez-hakerow [Accessed: 8 October 2021].
16. *Księgowa przelała ponad 1,5 miliona złotych oszustom. „Pieniądze są zagrożone atakiem hackerskim" – ostrzegali policjanci. Policjanci fałszywi*, [online]. Available at: https://sekurak.pl/ksiegowa-przelala-ponad-15-miliona-zlotych-oszustom-pieniadze--sa-zagrozone-atakiem-hackerskim-ostrzegali-policjanci-policjanci-falszywi/ [Accessed: 30 September 2021].
17. Nutting R. *CompTIA PenTest+ Certification. Exam PT0-001*. New York: McGraw Hill Education; 2019.
18. [online]. Available at: mediarecovery.pl/analiza-pakietow-jako-rozszerzenie-funkcjonalnosci-siem-splunk/ [Accessed: 12 October 2021].
19. Łuczak J, Tyburski M. *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*. Poznań: Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu; 2010.

Odporność organów administracji publicznej na cyberataki

STRESZCZENIE

Organa administracji publicznej odpowiadają za organizację zarządzania kryzysowego na podległym im obszarze. Aktualnie wymiana informacji pomiędzy elementami zarządzania kryzysowego realizowana jest z wykorzystaniem systemu telekomunikacyjnego. Dzięki zastosowaniu teledacji możliwa jest wymiana danych, a na ich podstawie budowanie informacji o zjawisku kryzysowym. Odpowiedzialność za ochronę zasobów informacyjnych spoczywa na wójtach, prezydentach miast czy marszałkach województw gromadzących i przetwarzających dane w celu realizacji zadań podległych im urzędów. Jednym z elementów sytuacji kryzysowej może być cyberatak wykonany na infrastrukturę informatyczną urzędu w celu utrudnienia lub uniemożliwienia wykonywania przez niego zadań. Takie incydenty miały już miejsce na terenie Polski. Interesujące jest zagadnienie zarządzania incydentem, który oddziałuje bezpośrednio na urząd. Artykuł przedstawia analizę przypadków cyberataków opisanych w mediach. W pracy pokazano pasywne metody rekonesansu wykorzystywane przez cyberprzestępców.

SŁOWA KLUCZOWE

cyberbezpieczeństwo, zarządzanie bezpieczeństwem informacji w organizacji

Biographical note

Dominika Dudziak-Gajowiak – Master of Science and Engineer in Computer Science, graduate of the Faculty of Computer Science and Management of the Wrocław University of Technology (field of study: Computer Science). Academic teacher at the General Tadeusz Kościuszko Military University of Land Forces since 2014, member of the Polish Information Processing Society since 2010. She has been dealing with practical aspects of the security of systems and IT networks for many years. Author or co-author of publications in the field of IT systems and networks as well as risk management.

Artur Szleszyński – Master of Science in Electronics Engineering. Former academic lecturer. Author and co-author of publications in the field of cybersecurity. Since 2019, he has been an employee of the IBM X-Force Centre in Wrocław. Holder of the certificates: CompTIA Network+, CompTIA Security+, Microsoft Certified Professional, ATTACK IQ Foundation and Operationalizing MITRE ATT@CK, Think like a Hacker, Splunk 7.x Fundamentals. Completed training: Certificated Ethical Hacker v. 11.0. Scientific and technical interests: Detection and identification of incidents in cybersecurity, artificial intelligence methods in detecting cyber threats.

ORCID

Dominika Dudziak-Gajowiak https://orcid.org/0000-0001-6898-7241

Artur Szleszyński https://orcid.org/0000-0003-4563-9329

Acknowledgement

No acknowledgement and potential funding was reported by the authors.

Conflict of interests

All authors declared no conflict of interests.

Author contributions

All authors contributed to the interpretation of results and writing of the paper. All authors read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.