INFORMATION SECURITY INCIDENTS MANAGEMENT IN MARSHAL OFFICES AND VOIVODESHIP OFFICES IN POLAND

DOMINIKA LISIAK-FELICKA, MACIEJ SZMIT

Summary

The article presents the results of surveys concerning information security incidents managements, which were conducted in marshal offices between December 2012 and April 2013 and in voivodeship offices between December 2013 and March 2014. Survey questionnaires were sent to all sixteen marshal offices and all sixteen voivodeship offices in Poland.

The article is devoted to information security incidents management. The aim of the research was an analysis and evaluation of information security incidents management in marshal offices and voivodeship offices. It presents the numbers of incidents and ways of incident management.

Keywords: information security, information security management systems, information security incidents management

Introduction

An information security incident is defined in ISO/IEC 27000:2014-2.36 *[2]* as a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security". Whereas an information security event is understood in the same standard as an "identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant" ISO/IEC 27000:2014-2.36. The occurrence of an event does not have to equate to security breaches, in contrast to an incident, what usually means an occurrence of a security problem.

It should be noted that the information security incident relates to the information security (information confidentiality, integrity, availability and other properties like accountability or non-repudiation). An information security incident means not only confidentiality breaches but also unauthorized data modification of lack of information availability (e.g. Denial of Service). The NIST standard *[14]* also defines the term "computer security incident" as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices". Information security has a wider meaning, because, in addition to the processed information in ICT systems, the information in paper documents or microfilms are also taken into account *[1], [7]*.

The most popular group of standards devoted to information security incident management is the family of ISO/IEC standards marked ISO/IEC 27k. Especially, the ISO/IEC 27001:2013, ISO/IEC 27002:2013 and ISO/IEC 27035:2011 *[3], [4], [6]*. There are a set of controls devoted to

incident management in the ISO/IEC 27001:2013 (see Appendix A, Table A.1, point A.16 Information security incidents management):

- A.16.1.1 Responsibilities and procedures;
- A.16.1.2 Reporting information security events;
- A.16.1.3 Reporting information security weaknesses;
- A.16.1.4 Assessment of and decision on information security events;
- A.16.1.5 Response to information security incidents;
- A.16.1.6 Learning from information security incidents;
- A.16.1.7 Collection of evidence.

Appendix A from ISO/IEC 27001:2013 is directly related to the chapters of the ISO/IEC 27002:2013 standard. The ISO/IEC 27035:2011 standard provides guidance on information security incident management. It also provides a structured and planned approach to: detect, report and assess information security incidents, respond to and manage information security incidents, detect, assess and manage information security vulnerabilities and continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

There are many reasons why the issues of information security incidents management in public administration are interesting.

Firstly, there is a regulation of the Polish Council of Ministers regarding the National Interoperability Framework, containing the minimum requirements for public registry and information exchange in electronic form and the minimum requirements for ICT systems *[16]*. The regulation imposes on managers of public administration units some obligations relating to security management including the obligation to immediately report information security incidents in a defined and fixed way for quick corrective action.

Secondly, there are many information security incidents in public administration in Poland. The latest incidents, which were commented, were e.g.:

- police arrested a 28-year-old, who reported to the voivodeship office with information about a hole in one of the servers belonging to the office (Kielce, May 2013) *[15]*;
- website of Greater Poland Voivodeship Office was swapped (Poznan, November 2013) *[17]*;
- website of the City Office of Lodz was attacked by hackers. Office paid 43000 PLN for a company that "cleaned" the system after the hacker attack and restored the website (Lodz, June 2013) *[12]*.

What is more, information security in public administration has a direct relationship to the safety of citizens and the cyberspace security of Poland *[5], [8], [13]*.

1. Statistics

Information on the numbers of incidents in the public administration in Poland can be found in the cert.gov.pl reports *[17], [18], [19]*. The main task of The Governmental Computer Security Incident Response Team (cert.gov.pl) is ensuring and developing the capacity of organizational units of the Polish public administration to protect themselves against cyber threats. Every year, the Governmental Computer Security Incident Response Team prepares report on the status of cyberspace security in Poland. The numbers of notifications and incidents recorded by cert.gov.pl in 2011–2013 are shown in Figure 1.

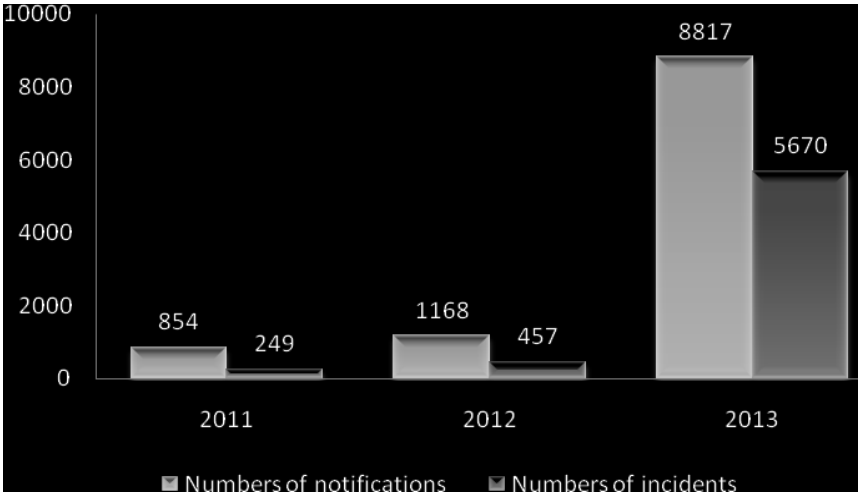

Fig. 1. Numbers of notifications and incidents recorded by cert.gov.pl

Source: own preparation on the basis of the cert.gov.pl.

Statistics of incidents in 2011–2013 by category are listed in Table 1.

Table 1. Statistics of incidents by category.

	Year		
Category	2011	2012	2013
Botnets	1	49	4270
Other	30	42	866
Scanning	40	117	146
Unauthorized modification of information	19	16	124
Spam	27	27	47
WEB Application Errors	31	36	45
Incorrect configuration of the device	10	8	36
Trojan	4	17	25
Social engineering	6	9	22
Virus	13	19	20
Unauthorized access to information	3	13	19
Identity theft, impersonate, phishing	7	9	12
Distributed denial of service (DDos)	3	23	8
Login attempts	6	6	6
Application compromise	13	26	4

Category	Year		
	2011	2012	2013
Administrators activities	7	5	4
Discrediting, insulting	3	5	4
Exploiting of known vulnerabilities	2	-	2
Spyware	5	-	2
Unauthorized use of resources	5	-	2
Denial of service (DoS)	4	8	2
Privileged account compromise	-	-	1
Worm	9	-	1
Sniffing	-	-	1
Copyright infringement	-	-	1
No classification	1	-	-

Source: own preparation on the basis of the cert.gov.pl.

Cert.gov.pl allows reporting of the incident by sending the completed form, which can be downloaded from its website. To correctly complete the form, the knowledge of incidents classification is required. Cert.gov.pl uses The European Computer Security Incident Response Team Network classification *[20]*, which distinguishes classes and types of security incidents:

- Abusive content (Spam, Harassment, Child/Sexual/Violence/...);
- Malicious code (Virus, Worm, Trojan, Spyware, Dialer);
- Information gathering (Scanning, Sniffing, Social engineering);
- Intrusion attempts (Exploiting of known vulnerabilities, Login attempts, New attack signature);
- Intrusions (Privileged Account Compromise, Unprivileged Account Compromise, Application Compromise);
- Availability (DoS, DDoS, Sabotage);
- Information security (Unauthorized access to information, Unauthorized modification of information);
- Fraud (Unauthorized use of resources, Copyright, Masquerade);
- Other (Incidents, which do not fit into listed types).

This classification is very popular and used i.e. by the cert.pl and Computer Emergency Response Team Orange Polska (CERT OPL).

2. The aim and the method of the research

The aim of the research was an analysis and evaluation of information security incidents management in marshal offices and voivodeship offices in Poland, especially to find the answer to the following questions:

- whether information security incidents have occurred;
- whether information security incidents are registered;
- how many incidents have occurred and are registered;
- the methods of information security incidents management.

The survey is a part of our investigations concerning selected aspects of cyber security in government organizations in Poland *[11], [9], [10]*.

The research was conducted using a survey questionnaire. For all marshal and voivodeship offices, a letter asking for help in the scientific study by completing a questionnaire was sent. The content of the letter posted a link to the questionnaire in electronic form, which is located on the server google.com. During the research, many telephone and e-mail contacts with officials were conducted.

3. Results of the research

We obtained 13 positive responses from marshal offices and 11 positive responses from voivodeship offices. Among the 13 marshal offices, only in 7 the information security incident had occurred and was registered. Among the 11 voivodeship offices, only in 5 the information security incident had occurred and was registered (see Figure 2).

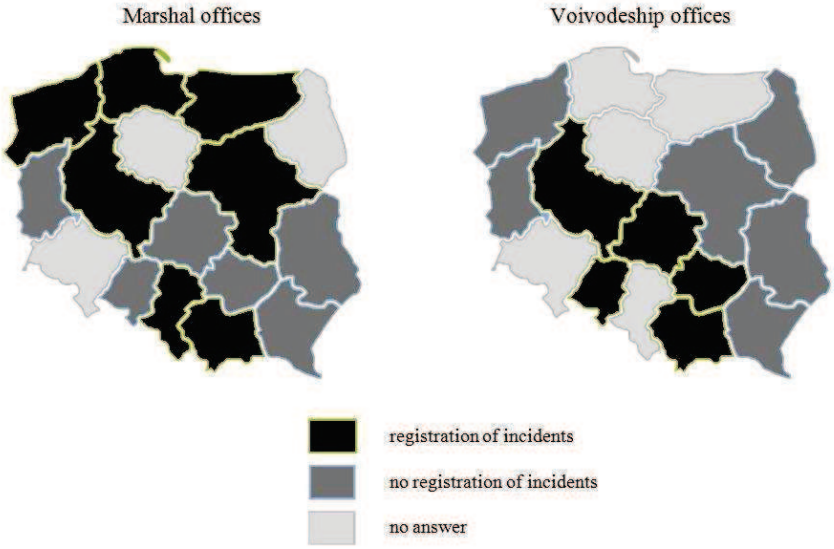

Fig. 2. Information security incidents registration in marshal offices and voivodeship offices

Source: own preparation on the basis of the research.

The numbers of incidents registered by marshal offices are listed in Table 2.

Table 2. Numbers of security incidents in marshal offices

Voivodeship, in which is the marshal office	2011	2012
Lesser Poland Voivodeship	15	7
Masovian Voivodeship	5	6
Pomeranian Voivodeship	1	0
Silesian Voivodeship	2	4
Warmian-Masurian Voivodeship	0	0
Greater Poland Voivodeship	a few	6
West Pomeranian Voivodeship	Office does not want to disclose the information.	

Source: Own preparation on the basis of the research.

The numbers of incidents registered by voivodeship offices are listed in Table 3.

Table 3. Numbers of security incidents in voivodeship offices

Voivodeship, in which is the voivodeship office	2012	2013
Łódź Voivodeship	0	0
Lesser Poland Voivodeship	1	6
Opole Voivodeship	2	4
Świętokrzyskie Voivodeship	0	1
Greater Poland Voivodeship	0	3

Source: Own preparation on the basis of the research.

Officials were asked to describe the security incidents management. Descriptions provided by particular offices are listed in Table 4 and Table 5.

Table 4. Security incidents management in marshal offices

Voivodeship, in which is the marshal office	Description of security incidents management
Lesser Poland Voivodeship	Office performs a quarterly review of information security incidents. And each incident takes corrective and repair actions.
Masovian Voivodeship	All the issues related to the management of incidents are described in the integrated management system.
Pomeranian Voivodeship	1. Analysis of the incident; 2. Settlement of the responsible persons; 3. Implementation information security policy procedures.
Silesian Voivodeship	1. Confirmation / incident report; 2. Take procedural action by persons responsible for the required decisions and the persons responsible for the execution of technical activities; 3. Perform repairs and corrective actions and, if required, at the same time documenting the description of the event and the action taken;

Voivodeship, in which is the marshal office	Description of security incidents management
	4. Discussion of the incident and, if necessary, formulate proposals with the proposed modifications or new solutions implementation.
Warmian-Masurian Voivodeship	1. Determine the nature of the incident; 2. As soon as possible, take action in order to minimize the effects of incident; 3. Notification to the authorities.
Greater Poland Voivodeship	Incidents are reported to the helpdesk and the information security administrator. Next, they are registered. In cases where the helpdesk finds a violation of information, security policy is reported to information security administrator. Then, during the team meetings, incidents are discussed and a decision to implement the necessary organizational and technical solutions is taken.
West Pomeranian Voivodeship	1. Identification of the incident; 2. An investigation; 3. Conduct of inquiries; 4. Determine the need to inform the relevant departments; 5. Corrective action and preventive action (implementation); 6. Control; 7. Termination of proceedings.

Source: Own preparation on the basis of the research.

The voivodeship offices (Świętokrzyskie Voivodeship, Greater Poland Voivodeship, Lódź Voivodeship, Opole Voivodeship, Subcarpatian Voivodeship and Lublin Voivodeship) have reported security incidents to cert.pl, cert.gov.pl, police, the Internal Security Agency (ABW).

Five offices declared that they could count on support from other authorities in the incidents management in the range of:

- Recommendation in the form of guidelines of the Internal Security Agency;
- Current cooperation with cert.gov.pl;
- Review the logs, web security control, guidelines for improving security provider side;
- Notifications of incidents in other institutions and suggest solutions to prevent;
- cert.gov.pl helps in the investigation.

Only in the Marshal Office of Mazovian Voivodeship and the Marshal Office of Warmian-Masurian Voivodeship were security incidents reported to the police. The Marshal Office of the Greater Poland Voivodeship reported only one incident to this institution and also explained that "not all incidents were qualified for registration in the cert.gov.pl or the prosecution. Only the Marshal Office of Pomeranian Voivodeship mentioned that could be counted on for a substantive support from other public administration units in the field of incident management.

Table 5. Security incidents management in voivodeship offices

Voivodeship, in which is the voivodeship office	Description of security incidents management
Lublin Voivodeship	Detection => neutralization => notification => analysis => implement changes to prevent a recurrence of the incident
Lesser Poland Voivodeship	1. Identification of the incident; 2. Assess and improve security; 3. Estimation of the risk of incident occurrence; 4. Training of staff.
Opole Voivodeship	Incident management aims to: 1. Identify the cause of the incident; 2. Reduce the size of the incident; 3. Rapid restoration of normal operation of the service; 4. Minimize the resulting losses; 5. Draw conclusions; 6. Improve the state of security.
Świętokrzyskie Voivodeship	Disclosed incident is reported to cert.gov.pl and, if necessary, the police.
Greater Poland Voivodeship	Detailed procedure is based on the procedure given in the Security Policy.

Source: Own preparation on the basis of the research.

4. Conclusion

Information security incidents have occurred and were registered in only 7 marshal offices and 5 voivodeship offices. The offices, in which the information security incidents have not been registered, should implement an information security incident management as soon as possible because a lot of security incidents in public administration could happen.

The numbers of information security incidents have grown rapidly. This is confirmed by reports cert.gov.pl.: 1168 notifications were registered in 2012, of which 457 were classified as security incidents. In 2013, the number of registered notifications were 8817 and 5670 were classified as security incidents. Unfortunately, the data obtained from the officials did not confirm this situation. However, there has been an increase in the number of incidents, the number of incidents recorded in voivodeship offices and marshal offices is not impressive. A small number of incidents may indicate that officials are reporting only the most serious of them. The absence of a detected incident does not in itself constitute a high risk (unless of course, appropriate corrective and recovery action has been taken), but – on the other hand – this makes it difficult for institutions like cert.gov.pl to provide correct statistical analysis of the incident occurrence.

Not all offices have the correct way of information security incidents management. In some units, this process is reduced only to notifying the relevant departments of the fact that the incident occurred. Some of the offices have implemented comprehensive incident management.

A good practice is to prepare a list of events that can be classified as an information security incident. It is important to register information security incidents. The register should containing data of incident that occurred along with information about the person notifying, the operator of the incident and actions in handling the security incident.

It can be argued that the number of reported incidents in the future will grow. Evaluate the effectiveness of implemented "Cyberspace security policy of Poland" *[13]* will be effected through the following measures, such as: the number of responses on reported incidents and the number of handled incidents. In order to prove the effectiveness of this policy, the government will want to show the largest number of handled information security incidents.

To summarize this article, it must be concluded, that:

- many marshal and voivodeship offices do not collect nor report information about information security incidents. It is impossible that in these offices the incidents do not occur. Most likely, the officials do not register incidents intentionally out of fear or they do not know how to manage the information security incidents. Officials of these units should be trained in the field of information security. A known maxim says that risk is not something to fear, but something to manage and a similar rule applies to incident management: you can fear incidents but you have to manage them (and when you manage them your fear may even be less);
- information security training should be performed also in the units, where the process of information security incidents management is reduced only to notify the relevant departments of the fact of the incident occurrence;
- it is necessary to conduct research concerning information security incidents in other government and local government units in order to verify ways of an information security incidents management and to raise awareness about the issues of information security among the officials.

In the context of further research, a study of information security incident management in other government and local government units is planned.

Bibliography

[1] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwo WNT, 2007.
[2] ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary.
[3] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.
[4] ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.
[5] ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cyber security.
[6] ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management.
[7] Korzeniowski L. F., *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa 2012.

[8] Lisiak-Felicka D., Szmit M., "*Tango Down" – Some Comments to the Security of Cyberspace of Republic of Poland*, Biały W. Kaźmierczak J. (ed. ed.), *Systems supporting production engineering*, pp. 133–145, PKJS, Gliwice 2012.
[9] Lisiak-Felicka D., Szmit M., *Information Security Management Systems In Marshal Offices In Poland*, „Information Systems In Management", vol. 3(2)/2014, pp. 134–144.
[10] Lisiak-Felicka D., Szmit M., *Selected Aspects of Information Security Management in Voivodeship Office in Poland*, "Securitologia" (in print).
[11] Lisiak-Felicka D., Szmit M., W*ybrane aspekty zarządzania bezpieczeństwem informacji w urzędach marszałkowskich*, Securitologia 2/2013, pp. 39–53.
[12] Łódź, Nasze Miasto, *Atak hakerski kosztował UMŁ 43 tys. zł*, http://lodz.naszemiasto.pl/artykul/atak-hakerski-kosztowal-uml-43-tys-zl,1950650,t,id.html [2014-06-16].
[13] Ministerstwo Administracji i Cyfryzacji, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013.
[14] National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, NIST Special Publication 800-61 Revision 2, 2012.
[15] Niebezpiecznik, *Zatrzymała go policja, bo zgłosił dziurę urzędnikowi* http://niebezpiecznik.pl/post/zatrzymala-go-policja-bo-zglosil-blad-na-stronie-urzedu-wojewodzkiego/ [2014-06-16].
[16] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U. 2012 nr 0 poz. 526.
[17] Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 r.*, Warszawa 2014, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/686,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2013-roku.html [2014-06-16].
[18] Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 r.*, Warszawa 2013, http://www.cert.gov.pl/portal/cer/57/605/Raport_o_stanie_bezpieczenstwa_cyberprzestrzeni_RP_w_2012_roku.html [2014-06-16].
[19] Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 r.*, Warszawa 2012, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/549,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2011-roku.html [2014-06-16].
[20] The European Computer Security Incident Response Team Network, *WP4 Clearinghouse*, http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html [2014-06-16].

Studies & Proceedings of Polish Association for Knowledge Management
No. 72, 2014

ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI W URZĘDACH MARSZAŁKOWSKICH I WOJEWÓDZKICH W POLSCE

Streszczenie

Artykuł prezentuje wyniki badań dotyczących incydentów związanych z bezpieczeństwem informacji, które były prowadzone w urzędach marszałkowskich w okresie grudzień 2012–kwiecień 2013 i urzędach wojewódzkich w okresie grudzień 2013–marzec 2014. Kwestionariusze ankiety zostały wysłane do wszystkich szesnastu urzędów marszałkowskich i szesnastu urzędów wojewódzkich w Polsce.

Artykuł poświęcony jest zarządzaniu incydentami związanymi z bezpieczeństwem informacji. Celem badania była analiza i ocena sposobów zarządzania incydentami związanymi z bezpieczeństwem informacji w urzędach marszałkowskich i urzędach wojewódzkich. Zaprezentowano liczby incydentów oraz sposoby zarządzania tymi incydentami.

Słowa kluczowe: bezpieczeństwo informacji, systemy zarządzania bezpieczeństwem informacji, zarządzanie incydentami związanymi z bezpieczeństwem informacji

Dominika Lisiak-Felicka
Department of Computer Science in Economics
Faculty of Economics and Sociology
University of Łódź
ul. Polskiej Organizacji Wojskowej 3/5, 90-214 Łódź
e-mail: dominika.lisiak@gmail.com

Maciej Szmit
Corporate IT Security Agency
Orange Labs Poland
ul. Obrzeżna 7, 02-691 Warszawa
e-mail: maciej.szmit@gmail.com