Different Aproaches to Security Incidents and Proposal of Severity Assessment of Security Incident

Lukas Kralik, Roman Senkerik, Petr Stipek
Faculty of Applied Informatics
Tomas Bata University in Zlin
Zlin, Czech Republic
e-mail: kralik@fai.utb.cz

Abstract—**This paper presents comprehensive theoretical background for future work, which will be aimed on multi-criterial evaluation and assessment of security incidents and proposal of methodology focused on audits of security incident management. This paper describes and comments three different points of view on security incident according to international standards or law (Cyber Security law in Czech Republic). The paper is mainly intended for Czech companies since it is based on project about Cyber Security Level in Czech Companies. Some criteria for assessment and evaluation of severity of security incident are proposed at the end of this contribution.**

Keywords-cyber security; security; incident; assessment of severity; ISMS; information security; incident management.

I. INTRODUCTION

An issue of security incidents and their resolving is inseparably connected with the field of ICT. It is necessary to look for more and more effective ways to prevent security incidents due to the increasing heterogeneity, complexity and pressure of confidence, integrity, availability or non-repudiation. It does not matter what it is monitored, it is important to be always prepared to act appropriately. Each security incident is bound with time pressure, which requires automated and clearly defined steps. A severity assessment of a security incident is absolutely necessary since it strongly affects a readiness for next incident.

This paper is divided into 4 sections which deal with theoretical aspects on the field of security incident. Section 2 describes basic terms and elements for resolving the security incident. Also there is a brief explanation of a security incident resolving in few steps. The next section is devoted to the definition of a security incident. This paper will serve as theoretical background for project about cyber security level in Czech companies. For that reason, there are 3 different definitions on the basis of used standards in Czech companies. The last section is the shortest but it is the most important. This section shows a conceptual proposal of severity assessment of the security incident. An objective of future work is to extend this proposal for multi-criterial evaluation. On the basis of this evaluation, it will be possible to assess occurred security incidents.

II. SECURITY INCIDENT – BASIC TERMS

A security incident is an event in information system, which caused disruption of confidence, integrity, availability or non-repudiation of information due to the failure of security measures or violation of security policy [1]-[5].

A suspected violation of a security policy or an attempt to overcome security measures is very often regarded for a security incident. A security incident usually has the following course: Incident Detection - Analysis of the Incident - Response to the Incident. Detection may be either automatic based on the information from some monitoring system, or manual, i.e., the incident is reported by someone. The company, which wants to deal with the security incidents and effectively solve them, should have an appropriate security standard and also it must properly present such standard to employees. The next step is formation of a team, which will be responsible for receiving reports, evidence and solving of incidents, etc. In many cases, this team is called Information Security Incident Response Team (ISIRT). The amount of ISIRT members depends on the total number and frequency of security incidents and of course on the size of company. For a proper function, ISIRT must have an adequate equipment, means and mainly authority [5][8]-[11].

The question is than as to how to determine the severity of the incident. There are many possible ways and approaches. The severity of the incident can be determined based on a value of an impact. In other words, the incident had financial or non-financial impact to the company. Another solution is to determine the severity of the incident according to the number and expertise of people who have to deal with the incident (more details are given in Section 3). It can be assumed that different number of people or teams with diverse levels of knowledge will participate in solution of various incidents [7]-[9].

A. Security standard

Each security standard must contain three basic elements. The first one is a definition of the security incident. The security incident must be clearly and understandable described with appropriate examples. These examples should be placed in attachment.

The next is information about security incident report. Contact should involve address on the intranet, e-mail, phone and office or workplace address because it is necessary to take into account the simple fact that the network infrastructure may not work.

And the last one is a structure of a security incident report - form for reporting incidents [5][10].

B. Security incident log

Creation of security incident log is necessary for successful resolving of particular incident. Information listed in this log includes:

- When the incident has occurred - due to the fact that the incident may be related to other events, it is always advisable to ascertain the exact time.
- Where the incident has occurred - the exact place and its description will enable the investigative team to respond quickly.
- Who committed the incident - the identity of the intruder can sometimes be difficult to identify, but we should try to get about him as much relevant information as possible.
- How the incident has occurred - sometimes we do not have enough information, but we should try to build a probable scenario describing the incident.
- What was the target of an attack - we should also distinguish whether the system was directly attacked or used to preparation for another attack.
- Which security attribute was compromised - integrity, confidentiality, availability and/or non-repudiation.
- What was the nature of the incident - if the incident was intentional or unintentional. And if unintentional, thus if there was negligence or lack of knowledge of security policy.
- What measures have been overcome - whether the measures at the physical, logical, organizational, personnel or technical security.
- What asset has impaired - hardware, software (operating system, applications, databases), network, data, etc.
- What is a probability that the incident will be repeated again - rather low, medium, high or certain [5][10].

C. Equipment of ISIRT

The team should have developed procedures for dealing with specific types of incidents, and these procedures should be still updated with new types of incidents occurring. Also they should have prepared a communication plan to make it clear who has to inform whom, or who decide on further action etc.

A basic equipment of this team is a common room (war room), where it will be possible to meet and agree on the next steps in the event of an incident.

Last but not least, they need access to an adequate software and hardware resources - for example, the team will need to make a copy of configuration, logs or possibly an entire partition of the infected system.

D. Simplified procedure for investigation of incident

The whole procedure has 7 steps. The biggest problem in practice is in step 3. A top management usually requires immediate recovery of operations, thus there may be no time for ensuring clues and finding causes. However, ignoring this step makes environment/conditions for another step No. 6 more difficult. There should be proposed appropriate measures to prevent recurrence of incident. Choosing a suitable measure is so difficult, thus the company has no other option than hope that the incident will not occur again [3]

1. Identify where a security incident has occurred;
2. As quickly as possible prevent further damage;
3. Analyze cause of security incident and ensure clues for further analysis;
4. Remove a cause and restore functionality;
5. Assess damage;
6. Design and implement appropriate measures to prevent a recurrence of this incident;
7. Inform others (employees, top management...) with results of the investigation [2][8][9].

III. Definition of the security incident

Many companies deal with incidents, but what kind of incident? Is it a computer, cyber or information incident? The usage of this term without any “additional specifying word/phrase” is quite problematic. There are 3 main and different points of view on definition of the security incident [1][3]-[5].
The definition of a security incident according to**:**

1. Cyber Security Law
2. NIST 800-61 (Computer Security Incident Handling Guide)
3. ISO/IEC 27001 - part of the growing ISO/IEC 27000 family of standards; information security management system (ISMS)

In Czech Republic, a new law about cyber security came in 1.1.2015. The main objective of this new law is to increase an overall security of cyberspace and set up a mechanism for active collaboration between business sector and public authorities. This implies new duties for companies. On these facts it was prepared this paper, whose main goal is to provide basic overview about this field and mainly help with an implementation of an incident management in companies. In the implementation phase it is placed emphasis on a determining a severity of the security incident.

A. Security incident according to Cyber Security Law

In §8, section 2, the cyber security incident is defined: "*Cyber security incident is a cyber security event, which represents violation of information security in information systems or violation of security services and electronic communications networks*."[5]

For understanding of this definition it is necessary to look into section 1, as to how security event is defined. There is: "*Cyber security event is an event that can cause violation of information security in information systems or violation of security services and electronic communications networks.*" [5]

Information according to §2 d) means to ensure the confidentiality, integrity and availability of information. Cyberspace is defining as a digital environment enabling the creation, processing and exchange of information, consisting of information systems and services and electronic communications network. [5]

B. Security Incident according to NIST 800-61

A computer security incident is defined in NIST handbook 800-61 (Computer Security Incident Handling Guide, chapter 2.1) as: „A *computer security incident* is *a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.* " [1].

Even here, the term event appeared and it is specified as: "*An event is any observable occurrence in a system or network.*" and "*Adverse events are events with a negative consequence…*" [1].

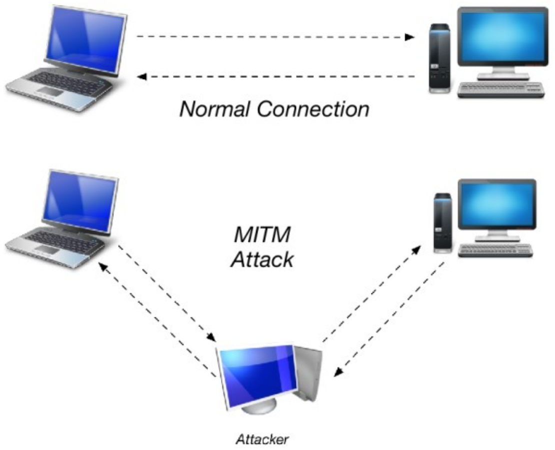

Figure 1. Principle of MITM attack

In the aforementioned handbook, it is possible to find attack vectors, which are removable media and e-mail (this way the malicious code can spread); Distributed Denial of Service (DDoS) attacks (Figure. 1), password guessing, finding vulnerabilities on web sites, **impersonation, spoofing**, Man-in-the-middle (MITM) attack (See Figure. 2), fake access points, violation organization's security policy, loss or stolen devices or media etc. [7][10][12].

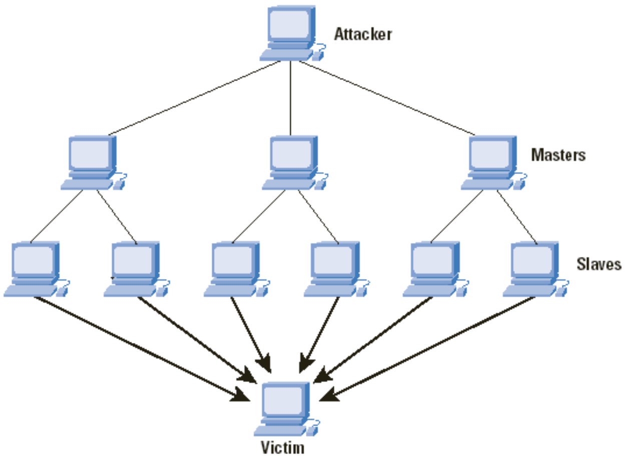

Figure 2. Principle of DDoS attack [6]

C. Security Incident according to ISO/IEC 27001

In chapter 3.6 of this standard, the security incident has following description: "One or more unwanted or unexpected security events for which there is a high probability of compromise of the organization's activities and threats to information security." Security event is defined in previous chapter 3.5. Security event is identifiable state of the system, service or network, pointing to a possible violation of security policy or failure of security measures. It may also be a different situation had not occurred before, which may be important in issue of information security [2]-[4].

D. Comparison of definitions

Each security incident should be caused by force majeure or violation of security policies. For the purpose of the project there were used 3 different definitions. Comparison between these definitions is described in following table (table 1) where:
"**?**" – the source of security incident is not clear if the definition is including it;
"**0**" – the source of security incident is not included in the definition;
"**1**" – the source of security incident is included in the definition.

TABLE I. SOURCES OF SECURITY INCIDENTS INCLUDED IN DEFINITION

	Force Majeure	Violation of Security Policies	
		intentionally	*unintentional*
Cyber security law	?	?	?
NIST 800-61	0	1	1
ISO/IEC 27001	1	1	1

The main standard for Czech companies is the cyber security law. The definition according to this law is quite wide, but it is not completely clear if cyber security incident represents also the violation of security by force majeure. Into this category it is classified for example interrupting of critical network infrastructure or servers due to flooding. Further, there should be a violation of security policy and standards that operator of critical infrastructure certainly published and it is mandatory for operator's employees.

The definition according to NIST 800-61 strictly claims that there has been a violation of security policies. Simultaneously there are no references to force majeure and the definition is clearly distanced from security violation due to natural disasters, blackout, etc.

Probably the best definition of security incident is presented in ISO/IEC 27001. It possible to notice that failure of security measures is also mentioned in addition to violation of security policies. Failure may be an unexpected event that could significantly compromise the security of information. However, it is questionable whether to be considered as a security incident, virus detected at the workstation (PC) and removed by antivirus, unplanned downtime of the system, utilization of an employer's mean for private purpose or retention and disposal of confidential documents on the table.

IV. ASSESSMENT OF SEVERITY OF INCIDENT

To correctly determine the severity of the incident it is very often a problem. In addition, the severity may vary throughout the life cycle of the incident. For example, at the beginning of the investigation of the incident, it may seem that this is a security incident with a negligible impact on the company and later on during the investigation it may prove that the original assumption was wrong.

If companies already have established a process that could be used with some exaggeration as an incident management and the severity of each incident is determined in this process, then their approach is very different. It is understandable that different companies use various number of degrees to reflect the severity of the incident and also individual levels have other names. However, it is striking that for determining the degree of severity, the companies do not have defined clear rules.

If company conducted a risk analysis then it can be relatively easy to determine the severity of incident based on the value of the asset whose confidentiality, integrity or availability has been or may be compromised. However, as already mentioned in section II, there are more possibilities. A proposal of criteria for determining the severity of the incident follows:

The severity should be defined by 4 levels:

- low
- middle
- high
- critical

Depending on the amount of affected users:

- one or few users
- whole department
- whole branch
- whole company

According to a level that will deal with the incident:

- technical (IT) support
- lower management
- middle management
- top management

Who should be familiar with the incident:

- one or a few employees of the company
- all employees
- own employees and persons outside the company
- own employees and the public

By level of expertise:

- first level of support
- system administrator
- security expert
- security company

Regardless of the size and scope of company, these four levels for assessment of the severity of the incident should be enough for most companies.

V. CONCLUSION

Security incidents and their solutions are an essential part of life of IS/ICT manager as well as of ordinary users. Absolute security of an information system is not guaranteed by implementation of any security policy. Although the implementation of various security functions and measures are part of ensuring security, vulnerabilities remain in the information system and these vulnerabilities represent risks. The existence of these vulnerabilities is the possibility of the security incident with direct or indirect impact on everyday operations of companies. Therefore, it is essential that each company pay attention to the definition and the implementation of security management system, its control and audit. At the same time companies should also deal with efficient and professional management of security incidents. Incidents can be controlled intuitively or in structured way - professionally. Only a professional approach allows gaining benefits from security incidents - experience, skills and knowledge from solutions of previous security incidents.

ACKNOWLEDGMENT

This work was supported by grant No. IGA/FAI/2015/039 and IGA/CebiaTech/2015/036 from Internal Grant Agency of Thomas Bata University in Zlin; further by financial support of research project NPU I No. MSMT-7778/2014 by the Ministry of Education of the Czech Republic and also by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

REFERENCES

[1] NIST, “Special Publication 800-61 – Computer Security Incident Handling Guide, Revision 2: 800-861“, 2012.

[2] International Organization for Standardization ISO/IEC 27000-Information technology-Security techniques-Information security management systems-Overview and vocabulary.

[3] International Organization for Standardization ISO/IEC TR 18044:2004- Information technology - Security techniques - Information security incident management.

[4] International Organization for Standardization ISO/IEC 27001 - Technology-Security Techniques - Information Security Management Systems-Requirements.

[5] Czech. Law nr. 181/2014 sb. Cyber Security Law. 2014.

[6] P. Doucek “IS/ICT Security Incidents and theire Solutions,” System Integration vol. 3, Prague 2005, pp. 77-85.

[7] C. Patrikakis, M. Masikos, and O. Zouraraki, “Distributed Denial of Service Attacks,” In: Internet Protocol Journal [online]. Volume 7, Number 4, San Jose, USA: Cisco Systems, Inc, 2004, ISSN 1944-1134, online: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html, [retrieved: July, 2015].

[8] L. Lukas, M. Cahlik, and L. Kralik, “Protection of Data Centers – Physical Protection, ”Recent Advances in Information Science, Proceedings of the 3rd European Conference of Computer Science (ECCS '12). Paris, France WSEAS Press, 2012, 171-176. ISBN 978-1-61804-140-1, ISSN 1790-5109

[9] L. Wan-Soo and J. Sang-Soo, “A Study on Information Management Model for Small and Medium Enterprises,” Recent Advances in E-Activities, Information Security and Privacy, Spain, WSEAS Press, 2009, ISSN: 1790-5117. ISBN: 978-960-474-143-4

[10] K. Prislan and I. Bernik, “Risk Management with ISO 27000 Standards in Information Security,” In Advances in E-Activities, Information Security and Privacy, Venezuela WSEAS Press 2010, ISBN: 978-960-474-258-5

[11] L. Kralik and R. Senkerik, “Proposal for Security Management System,” Recent Advances in Electrical Engineering and Educational Technologies. Proceedings of the 2nd International Conference on Systems, Control and Informatics (SCI 2014), Athens, 2014. p. 77-80. ISBN 978-1-61804-254-5

[12] S. Fenz and A. Ekelhart. “Formalizing Information Security Knowledge" Book Formalizing Information Security Knowledge' (ACM, 2009, Edn.): 183-194