International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 1 (2018) pp. 534-538

Analysis of Security of Selected Crisis Management Information System

Katerina Vichova, Roman Jasek and Martin Hromada

Tomas Bata University in Zlín, nám. T. G. Masaryka 5555, 760 01 Zlín, Czech Republic.

Abstract

Information support for crisis management is quite diverse within each region in the Czech Republic. As a result of the failure of the national crisis management information system, some municipalities have developed their crisis management systems and, therefore, the security of individual systems is somewhat different. Information security is an extensive area today, and consequently, it must also take into account in the section of crisis management. In the event of leakage of sensitive information, the life, health, and property of citizens may endanger.

The thesis aims to analyze the security of the information system of crisis management of the selected city. Within the Crisis Management Information System, identification and evaluation of the assets of the information system will carry out, which will provide necessary information about the assets, which can then follow by an estimate of the probability of occurrence of threats. The last part of the analysis is the identification and evaluation of the information system's attractiveness. Also, SWOT analysis was used. At the end of the article, recommendations are suggested to increase the security of the information system.

Keywords: information system, crisis management, security, threat analysis, vulnerability.

SECURITY OF INFORMATION SYSTEM

Security of information systems is a process which protect the corresponding information systems and the information included in them. Part of this ordinarily understood protection of information technology is also communicative security (protection of data transferred between computers), physical security (protection against natural threats and physical attacks) and personal security (protection from internal invaders.) [1]

Security is a property of an element (e.g., an information system) which is at a certain level protected against losses, or also a state of protection (at a certain level) against losses. IT security covers protection of confidentiality, integrity and availability during processing, storage, distribution and presentation of information. [2]

An information system is a functional aggregate enabling the goal-oriented and systematic acquisition, processing, storage and access to information and data. Includes data and information sources, mediums, hardware, software and utilities, technologies and procedures, related standards and employees. [2]

Each information system is made up of individual assets. That includes the primary, supporting and technological assets.

Primary asset means information or service processed or provided by the information system. A technical asset, employees, suppliers involved in the operation, administration and security of the information system consider as supporting assets. The technological asset includes specialized equipment, means of communication and program equipment of the information system and the objects in which these systems locate. [3]

There are not many standards on the security of information systems. The most common are ISO / IEC 27001 - Information Security Management Systems (ISMS). These international standards have been prepared to provide support for setting up, implementing, managing, monitoring, maintaining and improving the information security management system.

Another is the British standard for information security BS 7799-2, which was developed as a useful tool for the evaluation of information security management systems (ISMS), which has rapidly spread around the world and is now available in more than 11 languages. In 1998, the standard was adapted to the requirements of new trends and in 2000 approved as an ISO standard. In 2005, the latest standard, incorporating the most up-to-date knowledge in the field of comprehensive information security - ISO 27001, was built by British Standard BS7799 / ISO 17799.

ISO 20000 is a new standard that addresses explicitly IT management and focuses on improving quality, improving efficiency, and reducing costs for IT processes. [1]

RISK ANALYSIS OF INFORMATION SYSTEM

When analyzing the security information system, the goal is to check the current state of safety, to detect weaknesses and to find the most appropriate measures to eliminate it. The protection and security of information include both the computer part and the social part. We include a human factor in the social sphere, which plays an essential role in ensuring the security of the system and the possible leakage of information (not only staff who work with the system, but also office support staff, external staff, security guards, and repairers).

Risk analysis is a necessary condition for risk decision making and is, therefore, a fundamental process in risk management. Risk analysis should answer the questions:

1. What threats are the system exposed?
2. How robust are the assets of the system vulnerable to threats?
3. How high is the likelihood that the risk abuses a specific vulnerability?
4. What impact will this have on the system?

The answer to these questions will bring us the key to ensuring the security of the information system.

We can divide the risk analysis into the following steps:

- Asset Analysis - Identify critical assets of the system and determine their value.
- Threat Analysis - Identification and quantification of threats.
- Vulnerability analysis - identification and quantification of all weaknesses at the level of physical, logical and administrative security.
- Determining the level of risk - expressing the level of risk, e.g., in monetary units.

Risk analysis shows us:

- What can happen?
- Why can this happen?
- How can this happen?
- Where can this happen?
- Who will it concern? [4]

Because of the risk analysis of the information system, we can identify and evaluate the assets, threats, and vulnerabilities of the information system.

CRISIS MANAGEMENT INFORMATION SYSTEM

The information systems, in general, are essential and indispensable part of planning, organizing, managing and controlling. These information systems applied to the crisis management information systems. The crisis management information system is a tool which can help the joint rescue service and the municipality offices to save a life, health, and property. The history and importance of the crisis management changed radically after the enormous flood in 1997 in the Czech Republic. Today, both the joint rescue service and the municipality offices are using the crisis management information systems. These systems contain the information about the situation, forces and resources, navigation, SMS communication, meteoradar and others. This system changed manner for the conversation and the decision making process in times of the crisis.

The purpose of the chosen system is to support crisis and emergency. It can not say positively that the system is only used in crisis situations such as floods. However, it is also used for less dangerous events, such as interruption of drinking water supply.

The purpose of this system is to have a system that will support the preparation of extraordinary events and, at the same time, to provide support to Prague's management in the process of managing the situation.

This system has many functions. Therefore, this system divides into individual modules - GIS, risk analysis, catalogues, CCTV control, implementation event of crisis measures in the map, GPS tracking, alert and warning system, displaying online information from the traffic situation, routes.

As is clear from the above-mentioned modules, the information system is not only a system that directly addresses the crisis but complemented by modules such as CCTV control.

ANALYSIS OF CRISIS MANAGEMENT INFORMATION SYSTEM

The purpose of the next chapter is to examine the current state of security of the information system and to detect the weaknesses of the tested system.

Identification and asset valuation

As already mentioned in the introductory chapter, the information system consists of individual assets. The identification and evaluation of the Assets of the Crisis Management Information System will be carried out in the following analysis. Asset valuation will be evaluated based on availability, confidentiality, and confidence.

The value of the asset will be valued as follows: 1 - low - low impact, 2 - medium - medium impact, 3 - high - high impact, 4 - very high - very high impact.

The asset categories divided into: I - information, SW - software, P - physical, H - human resources, O - others.

Table 1: Identification and evaluation of assets of the information system

Asset name	Category	Availability	Intimacy	Integrity
Warning and information messages	I	3	1	3
SSL certificates	I	3	4	3
Signature certificate	I	2	3	2
Email server	O	3	1	3
Thin client, web browser	SW	3	1	3
Thick client, operator station	SW	4	1	4
LAN MHMP	O	4	1	4
WAN	O	4	1	4
Proxy servers HW	P	4	1	4
GIS servers HW	P	4	1	4
GIS servers operating system	SW	4	1	4
GIS servers, ArcGIS server	SW	4	1	4
Computer room	O	4	x	x
Users	H	4	x	x
Directory of subjects	O	4	2	3
Object catalog	O	4	2	3
Registers and records	O	4	2	3

Codes	O	2	1	3
Agendas	O	2	1	2
Recovery plan	O	1	2	1
Type plans	O	1	2	1
Forms for data collection	O	1	2	3
Solved events	O	4	3	4
Monitoring information	O	4	2	2
Web publishing information	O	2	1	3

Table 1 presents the results of analysis of selected crisis management information system and identification and evaluation of assets. As can be seen in the table 1, the highest value and hence the impact has the "Solved Events" asset. This asset has a very high impact regarding availability, a high impact from a confidentiality point of view and a very high impact on integrity. Altogether, this asset reached 11 points. The second most highly rated asset with 10 points is "SSL certificates" that have a significant impact regarding availability, a substantial incidence from a confidentiality point of view and a considerable effect on integrity.

Estimation of probability of occurrence of threats

At the same time, an analysis of the likelihood of the event of threats performed on this information system.

The probability score was divided into: 1 - very unlikely occurrence, historically nothing happened, no more than 1 x, 2 - the possible occurrence of the threat, occasionally happens, 3 - very likely occurrence.

Table 2: Estimation of probability of occurrence of threats of the information system

Threat	**Evaluation**	**Defense**
Damage to water (flood, rainwater flooding).	2	There was rainwater in the roof.
Fire.	1	There has never been a fire.
Damage to the building (static disruption).	1	There were no problems with statics.
SW failure (error messages and SW failures).	2	Occasionally, the application will terminate unintentionally.
HW failure (due to wear).	2	At times, the computer restarts spontaneously.
Introduction of malicious SW (virus infection).	2	In the past, viruses have removed.
Unauthorized access to control and software by third parties.	1	There was an unauthorized manipulation of the printer by a stranger.
Unauthorized access to management and software equipment by employees.	1	An attempt was made to run the program by an unauthorized employee.
Use of information in an illegal way (misuse of data).	1	In the past, personal information about employees placed on the site.
Tracking communications (eavesdropping, eavesdropping).	2	Employees made official calls in the presence of clients.
Traffic overload (slow internet connection).	2	The central application starts very long.
Lack of employees.	3	The department has only one specialist in the field.
Intentional damage by strangers.	1	Repeated checks at clients' initiative.
Intentional damage to employees.	1	The redundant employee deleted the information on the network drive.
Thefts did by employees.	1	They did not record.
Theft by strangers.	1	They did not record.
Report error.	1	The IT claim has claimed because it has resolved in violation of the specification.
User error.	2	Agenda information had to repair due to an employee error.
Breach of legislation.	1	Failure to comply with the statutory time limit for performing administrative activities.
Overvoltage in the network.	1	They did not record.
Power supply failure.	3	Once a month there is a one-minute breakdown.

Table 2 summarizes the estimation of the probability of occurrence of threats of the crisis management information system. As can be seen in table 2, only two risks evaluated. The first is a power failure when a month-long power failure occurs. The second threat with a very likely occurrence is the shortage of employees. There is only one person in the field who knows the entire know-how of the system and has knowledge in the relevant field. If the employee had to stay out of work on a long-term basis, it would pose a very high threat to the information system.

Identification and evaluation of vulnerability

Subsequently, a third analysis carried out, namely identification and assessment of the weakness of the information system.

The vulnerability was determined: 1 - small, 2 - medium, 3 - high, 4 - very high, 5 - critical.

Table 3: Identification and evaluation of vulnerability of information system

Vulnerability description	Evaluation
List of servers and technology rooms is not up to date.	4
There is no central access database for external entities.	4

Table 3 contains identification and evaluation of the vulnerability of crisis management information systém. As can be seen in table 3, the assessment of the fragility of the crisis management information system was identified only at two points where the weakness set as very high.

SWOT ANALYSIS OF INFORMATION SYSTEM

SWOT analysis serves to gain, unify and evaluate the knowledge we can achieve on a given issue - the information system. It aims to identify strengths and weaknesses of the system and opportunities and threats. Based on this analysis, there may be additional strains from the information system operator.

Table 4: SWOT analysis of information system

Strengths	Weaknesses
• The state of the technical device • Financial resources The effort to develop the information system by the city	• Service • Updates • User interface
Opportunities	**Threats**
• Improving and speeding communication in an emergency or crisis • New information system • Improving the user environment of the system • Use of modern technologies - Dynamic Situational Impressions	• Peopleware • Insufficient updating can lead to faulty decisions at an emergency

Table 4 demonstrates analysis of strengths, weaknesses, opportunities, and threats. As can be seen in table 4, among the weaknesses include service and system upgrades, which are currently very low. On the contrary, the state of the technical equipment and the efforts of the information system operator to boost and develop a new crisis management information system can be considered a strong side.

Furthermore, the opportunities and threats of the tested information system evaluated. Opportunities include the development of a new information system that will have a more user-friendly environment that makes it comfortable for crisis management staff to make better decisions in the emergency. Another possibility is the use of the dynamic situational display in the crisis management information system. That would provide a more efficient overview of the situation and more quick decision-making by crisis managers.

VERIFICATION AND RECOMENDATION

Within the selected crisis management information system, we conducted security analysis. It involved identifying and evaluating assets, estimating the likelihood of threats, and identifying and assessing vulnerabilities. Also, the SWOT analysis of the information system carried out, which highlights the strengths and weaknesses of the system and its opportunities and threats.

The identification and valuation of assets have shown that the most significant impact on the security of the information system has the "Solved Events" asset. This asset has a very high effect regarding availability, a high impact from a confidentiality point of view and a very high incidence of integrity. Overall, this asset received 11 points out of 12 possible.

From the estimation of the probability of occurrence of threats to the information system, two risks evaluated with the same number of points obtained. The first is a power failure when a month-long power failure occurs. The second most likely threat is the shortage of workers.

Based on vulnerability identification and assessment, only two vulnerable boats were selected. That is an out-of-date list of server rooms and technology rooms, and there is no central database of access permissions for external entities.

The aim of the Prague City Hall should be to eliminate possible threats, particularly in the field of information technology human resources. The only one responsible for the crisis management system throughout the system is entirely unsatisfactory. The second most dangerous threat is the failure of electricity. This risk should eliminate by deploying a backup resource at least for those who are in crisis management. Also, a list of server rooms and technology rooms should be created, which is currently out of date. The ultimate overarching goal should be to create a central database of external authority access permissions so that an outside person who does not have the appropriate privileges cannot attack by the crisis management system.

The SWOT analysis revealed the strengths and weaknesses of the information system. The weaknesses include service and

system upgrades, which are currently very low. On the contrary, the state of the technical equipment and the efforts of the information system operator to improve and develop a new crisis management information system can be considered a reliable side.

CONCLUSION

The work aimed to evaluate the current state of security of selected crisis management information system. Based on the analyses we conducted, we highlighted attention to the threats and the viable way to explain them.

Overall, the whole system is quite sophisticated, but as with any system, there have been weak sections. Therefore, it is essential for the municipality to update, develop and modernize the system. If there is a vulnerability in the system that is vulnerable, there is a high chance of leaking sensitive information from the system. It is consistently essential to reiterate the need for the system to have the data up-to-date and to ensure system security.

REFERENCES

[1] "ISMS, Security in cube." 2017 [online]. Available: http://www.chrantesidata.cz/cs/art/1147-dil-1/ Acessed: Nov. 17, 2017.
[2] Jirásek, P., Novák, L., Požár, J. “Cyber Security Glossary.” Praha, 2013.
[3] Czech Republic. Act No. 181/2014 Sb., on cyber security.
[4] Šefčík V., 2009, Risk analysis, 2009. ISBN 978-80-7318-696-8.