SECURITY DIMENSIONS
INTERNATIONAL & NATIONAL STUDIES
NO. 21; 2017 (44–59)
DOI 10.24356/SD/21/2

INFORMATION SECURITY MODEL FOR CRISIS MANAGEMENT SIMULATIONS

ASSOC. PROF. ING. KAROL FABIÁN, CSC.
Matej Bel University, Slovakia

PHDR. MICHAL DOBRÍK, PH.D.
Matej Bel University, Slovakia

MICHAELA MELKOVÁ, M.A.
Matej Bel University, Slovakia

ABSTRACT

Research activities of Crisis Management Center at Matej Bel University are focused at development and tuning of crisis scenarios for different critical events. Specialized tools are used for crisis management scenario workflow design and simulations. For complex analysis and information security crisis management, complex multilevel multisilo information security model was designed and described in the paper. Equipment and procedures used in current security measures defending organizations and states against advanced persistent threats and attacks from the cyberspace are attached to each level and silo of the model. This enables simulation of crisis management scenarios in case of cyberattack as precise as possible to real situations of critical architecture attacks, which can have dramatic consequences as outages or complete shutdown of energy grids, destroying factories, key data destructions and other catastrophic events.

ARTICLE INFO

Article history
Received: 03.03.2017 Accepted 29.03.2017

Key words
crisis management center of excellence, advanced persistent threats, simulation model, cyberspace,

Introduction: Crisis Management Center At Matej Bel University

Crisis Management Center, an academic center of excellence in crisis management research, was established with direct financial support of the EU structural funds at Matej Bel University in the city of Banská Bystrica, Slovak Republic. It has been involved in development and tuning of crisis scenarios for different critical events as cyberattacks, accidents with multiple casualties, floods, nuclear accidents and migration crisis, which are all very important events in current evolving geopolitical situation requiring specialized crisis management[1]. For complex analysis and simulation of information security crisis management scenarios, information security multilevel multisilo model has been designed. This model covers most used procedures and equipment including artificial intelligence used in current protection against advanced persistent cyber-attacks and threats. Today, outages or complete shutdown of energy grids, destroying factories, key data destructions and other catastrophic scenarios are several results of possible attacks of cyber units[2]. There is an ongoing struggle between absolute freedom of expression on the Internet and the level of serious constraints to ensure the safety of key government institutions. Compromise between these two policies shows that cyber-attacks targeting the institutions and individuals are everyday reality in the cyberspace. Crisis management simulation and planning system KRIMA (Emergency Enterprise Manager EEM), implemented in the above mentioned CMC enables construction and simulation of crisis management steps and systems in critical situations at institution after noticed cyberattack or known threat in place. Therefore, it is necessary to deal with consistent education and protection of individuals[3], institutions and states in the cyberspace. Crisis management planning after cyberattack is not well devel-

[1] I. Bremer, *The geopolitics of cybersecurity*, „Foreign Policy“, http://foreignpolicy.com/2011/01/12/the-geopolitics-of-cybersecurity/(accessed: 27.02.2017); P. Terem, P. Čajka, L. Rýsová, *Slovakia in geopolitical and geo-economic context*, Kamil Mařík – Professional Publishing, Praha 2015; J. Ušiak, *Security cooperation within V4*, [in:] *Central and Eastern European Political Systems*, Metropolitan University in Prague, Prague 2016.

[2] T.A. Johnson, *Cyber-security. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare,* CRC Press. 2015, p. 363.

[3] R. Kazanský, M. Melková, *Information Technologies and their Usage in Crisis Management as a Tool to Increase the Quality of Educational Process,* [in:] 15th International Multidisciplinary Scientific Geoconference SGEM 2015. Vol. 3. STEF92 Technology Ltd. Sofia, Bulgaria.

oped and described yet. KRIMA system, operated at the CMC enables users to create and simulate crisis scenarios dealing with situations right after cyberattack targeting the technical infrastructure of institution, state or personal computer networks as well. Emergency Enterprise Manager KRIMA is the basic software tool of the center[4]. It is a crisis management system supporting various types of users and their requirements concerning the prevention, solution and reconstruction.

System logs important events automatically in order to make revision of objects and crisis situations in later stages. Ways to log in can be set in configuration setting of database server. System supports simulation mode. This mode is very similar to a real one. Simulation mode is configured to send notifications to created simulation accounts, not to responsible persons or management of organization.

Crisis situation reporting uses templates to categorize the incident. Reported incident can be supported either by existing workflow or by creation of new one, if necessary. According to severity of the situation the risk factor is being calculated. In case of advanced persistent threat or attack from the cyberspace we must create complex general model, which includes all possible security levels and corresponding tools for defending targeted organization most effectively in order to include all aspects of information security in simulation.

1. General Model of Information Security

In this chapter we will show options for protecting company, organization and individuals against advanced threats from the cyberspace divided into two levels and four silos model of information security[5].

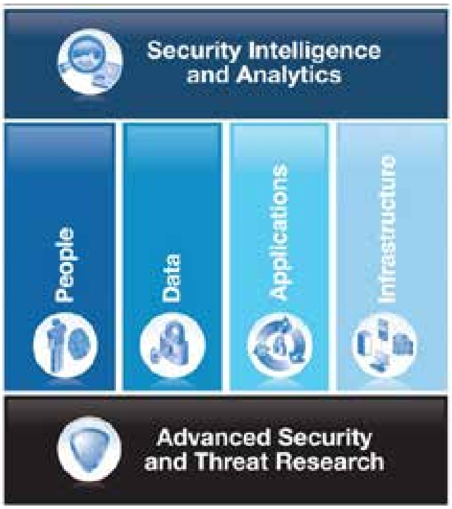
We will describe the architecture and functions of the technology, technical programming or combined dedicated equipment with the application of advanced artificial intelligence continuously adaptable to changing security environment in the cyberspace. In fact, it is a never ending process. These specialized technologies, complemented by sophisticated software protection at the application level now represents complete pro-

[4] K. Fabián, *Crisis Management Training System For Advanced Security Threats In Cyberspace*, Proceedings of IMSCI, Orlando, Florida USA 2014.

[5] K. Fabián, M. Melková, *Vybrané otázky kybernetickej bezpečnosti*, Belianum -Vydavateľstvo Univerzity Mateja Bela v Banskej Bystrici, Fakulta politických vied a medzinárodných vzťahov, 2016.

tection against unwanted penetration and threats. Security of all connected equipment into Internet is tested immediately by robotic explorers and cyber criminals. In the era of Internet of things (IoT), penetration is possible trough equipment of everyday life. Ports, which are input gates into connected PC´s and running web pages are targets of hundreds of attacks every hour.

Picture No. 1: Model of information security for crisis management simulations


Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

Credibility of documents, important business communications, access to state administration web portals and its services, tax authorities, etc. are secured by electronic signature. It is now an integral and mostly obligatory part of a secure cyberspace. Only by use and combination of more technologies in described two levels and four silo model later will help to achieve organisation desired information security.

Model of information security which will serve for complex crisis management simulation in case of advanced attack from the cyberspace has four basic vertical silos:

1. People and identity
2. Data and information
3. Application security
4. Infrastructure

All silos of the model covers layer of security intelligence, analytics monitoring and analysis and separate layer of advanced security and threat research.

2. People and Identity Silo

Every organization must be sure that authorized users within the organization and beyond it, will have access to data and tools they need, at a time where it is needed. Unauthorized access must be blocked. Large organizations employ a large number of diverse users, so it means that access control is very important and complicated. An important part of access control and identity check is to monitor privileged users, such as administrators. This silo includes the management of directory services.

2.1. Identity and Access Rights Policy

The information security management of identities and access rights (Identity and Access Management IAM) is the decision factor. It has a major impact on the organization's information security and its protection against attacks from within the organization. It allows authorized persons to access the resources and data available to them at the required time. Conversely, unauthorized persons are not able to access the data, their access to data is blocked. Systems that provide identity management and access policies are composed of specialized combination of hardware and software. It carries out activities such as obtaining identity, identity protection and technological means for its security. They are specialized network protocols, digital certificates, keys, passwords etc. Access management includes authorization, authentication, access rights and audit. Authorization is a set of rules that determines who is entitled to do certain specific tasks. For example, someone may delete records in the database and another user performs only reads. Authentication is the process by which the system assures that someone really is who he says he is. Today, the usual two-phase authentication is standard in Internet banking, where in addition to login and password, user is forced to confirm the actual code by text message, biometric sensors or electronic keys.

We have to include to this silo encryption, electronic signature and guaranteed electronic signature. Unlike most other described elements of protection against attacks from cyberspace that are installed and maintained by institutions, this category is fully within the competence of the individual Internet users[6].

3. Data and Information Silo

Organizations and individuals must protect unstructured and structured data to be within its scope. Each organization must determine the level of confidentiality, the value of data and information. It must define management and control of the risk. An effective plan for the protection of data and information includes the catalogue, respectively inventory of these files with attributes, policies and services that manage access, transfer and data transformation and information included in data archives. Privacy is for many organizations the most important thing for safety features. Encryption and protection of encryption keys is critical for ensuring data protection and is crucial for compliance with new incoming EU legislation[7].

Data encryption on mobile devices and secure sharing of encryption keys between the organization and the user or provider of cloud services is often overlooked. Transmission of sensitive data over the Internet must be encrypted. Analysis of data to and from network institutions is now monitored by a new generation of firewalls with elements of artificial intelligence.

3.1. Firewalls

Firewall is an essential component of network security technology that monitors and controls the incoming and outgoing data flow according to pre-established safety rules. Usually forms a barrier between a trusted, secure internal network and open cyberspace such as the Internet, which is considered unreliable. Generally it separates environments with different levels of security. Firewalls are often categorized as a network firewall or firewall software application, according to the level at which the device examines passing data.

Network firewalls are software applications that run on a standard or specialized computer and filter traffic between two or more networks.

[6] ISO, ISO/IEC 27032:2012 *Information technology — Security techniques — Guidelines for cybersecurity*, International Organization for Standardization, 2012, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375 (accessed: 27.02.2017).

[7] EU International Cyberspace Policy. 2014. *European Union External Action*, 2014, http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm (accessed: 27.02.2017).

Application firewalls are software applications developed for monitoring of incoming and outgoing traffic at specific application level.

The first type of firewalls called "packet filters" oversee the network addresses of passing messages and packets and decide if the packet is to be released into the system or must be blocked. This filter has a list of rules, which are used either to cancel or to reject message or packet. It sends an error message to the sender automatically. On the other hand, if the packet conforms to the programmed filter rules, it is transmitted to the other side of the firewall. This type of packet filtering takes no account of whether the packet is part of an existing data stream or not. It checks only basic information from a data stream contained in the examined packet, e.g. the sender and recipients type, communication protocol and if they are the most common types of protocols, checks TCP and UDP ports, finding the port number, which is the gate on the side of the recipient. So it is than clear what type of transmission is going on. TCP and UDP protocols are used to a certain type of transmission on defined port numbers and so packet filtering detects whether it is probably a surfing on Internet sites, remote printing, e-mail transmissions, file transfers etc. However, hackers are able to cover under the headings of standard network traffic to transfer sensitive data to or from the organizations, which are protected. Therefore the need for elimination of this danger brought next generation firewalls[8].

The second generation firewalls works similarly to previous generations, but retains the transmitted packets and identifies their connections. The test criterion here is the link packet or if it is a start packet of the connection, part of already closed connection, or a packet without any connection.

The main advantage of the third generation firewalls is that it examines the network traffic passing through the monitored levels of application. That means it understands and recognizes certain applications and corresponding network protocols. It is often useful because if unsolicited application or service attempts to bypass firewall rules and shapes itself as it is a protocol for e.g. web browsing http protocol, firewalls will block it immediately and evaluate how likely it is an illegal access or malicious communications. Greatest theft of personal data and access passwords have been made through improperly configured firewalls with theft covered by http web browsing protocol. A new generation firewall examines

[8] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.), Elsevier Science, 2014.

in greater detail the contents of transmitted packets and is usually complemented by specialized systems for preventing penetration. Elements of artificial intelligence are used for pattern recognition of hacker attempts.

3.2. Honeypot, Honeynet – Traps For Capturing Cyber Attackers

Honeypot is fictitious vulnerable IT system used to attract attackers and then breaking their protection. Generally, honeypots are created as a repository of data to appear as a legitimate part of the target infrastructure, but in reality they are just a trap data, which are separated from the actual data and monitored. They seem to contain information that could be of interest to attackers. According to the use of their functions, there are two types of honeypots, production and research honeypots.

Production honeypots are easy to use, allowing only limited possibilities to identify the attacker. They are located within the production network with other production servers and thus increase the overall information security of the organization.

Research honeypots collect information about the motives and tactics of the attackers. Thus enabling the organization to detect cyber threats it faces and to improve the protection of the institution. They are very complex devices and applied mainly in military and government institutions. Honeypots for malicious software (or malware honeypots) represent another type of traps for cyber attackers. They are used to collect malicious software and uses familiar and recurring characters which is searched by attacker software. Mostly used at open repositories of virtual money (e.g. Bitcoin). Another growing Internet problem is spam, which now constitutes the majority of Internet traffic. Identification of sources, e.g. server addresses generating spam is also possible through the dedicated honeypots, also called spam traps. In recent years, usage of such devices reduced amount of spam across the Internet significantly. To protect large-scale architectures whole networks of dedicated traps are used to form dedicated honeynets.

4. Application Silo

Access to IT security in layers and silos, as described in our model is necessary especially because of the fact that most attacks are happening in the application layer of the ISO standard communication model. The most effective anti-penetration precaution is organization's approach, which requires users to use applications that have been proposed and implemented with security in mind. Organizations and individuals must proactively protect their critical applications against external and internal threats throughout their life cycle, i.e. from design, development, testing and production. Automatic inspections of the application source code and test of operating systems enables the identification of vulnerabilities which could be exploited by attackers. To keep attackers out of internal protected area of the institutions and simultaneously also provide services for the users from non-secured Internet, specialized demilitarized zone must be used[9].

4.1. Demilitarized Zone DMZ

Architecture called demilitarized zone (DMZ) is used to address safety of current computer systems, which is basically physical or logical computer subnet separated by specialized firewalls from the Internet and protected infrastructure of the organization. It is run by organizations that need to make their services and data available to authorized Internet users. Its purpose is to add another layer to enhance the security of protected local area network of the organization. External users will only have access to devices, servers, and databases in the DMZ area.

Services, which are usually in the demilitarized zone are e-mail, web site servers with information for the public and DNS servers. Since these servers are at increased risk of attacks, they are located in a specific subnet, so that the remaining part of the infrastructure of the organization has been effectively protected. Servers in the DMZ have only limited ability to communicate with servers on the internal network of the organization. Also communication rights for servers in the DMZ to the Internet is controlled and limited in order to improve the safety of these facilities and to allow trouble-free operation for these services. This DMZ configuration creates increased protection against external attacks, but has no protective efficiency against internal security incidents.

4.2. Services at DMZ

In principle, all services which are provided on the Internet can be placed in the DMZ. Most often these are web servers that for example provide

[9] D.Shindler, *SolutionBase: Strengthen network defenses by using a DMZ*, TechRepublic, 2005, http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/(accessed: 27.02.2017).

basic information about the institution, internet shops, mail servers, FTP servers for downloading large files, VoIP servers, which offer digital telephony services over the Internet etc. These servers typically need access to the database servers which can also contain sensitive information that must be more protected against attackers than is a standard protection in the DMZ. Therefore, these are placed behind application firewall. Similarly e-mail messages and user databases must be more protected against direct access from the Internet but must be directly accessible for e-mail servers that are available on the Internet. Mail server inside the DMZ transmits incoming mail to secure internal mail server.

4.3. Proxy and Reverse Proxy Servers

In order to increase security, many institutions install specialized proxy servers (proxies) within DMZ. Employees are forced to use proxy server in order to access to the Internet. This can have also advantage for frequently asked pages, which will be stored at proxy and so some bandwidth with Internet is saved. In addition, proxy allows to monitor activity of employees on the Internet and enables to filter access regarding content and policy of the institution.

On the opposite, reverse proxy server is used as an intermediary server for indirect access from the external network, the Internet to the resources in the protected network. For example, providing access to e-mail users who are outside the institution, but prevents direct access to internal protected e-mail server. Only the reverse proxy server has access to the internal server behind the DMZ. Typically, such a mechanism is applied as part of the firewall. There are two basic ways to implement DMZ, the demilitarized zone with one or two firewalls. The advantage of single-DMZ firewall is a lower price, the disadvantages are the high load and critical dependence on one element of the architecture.

5. Infrastructure Silo

Infrastructure of organizations and individuals, which consists of network, servers, routers, storage media, power appliances and other components must be physically and electronically designed and implemented secure in order to prevent physical and electronic intrusions. Physical penetration can be eliminated by adequate monitoring of access and biometric systems. Electronic intrusions are eliminated by firewalls and antivirus programs with mostly daily updates and with new virus signatures and malicious software recognition. Zero day virus and malicious software occurrence must be first examined in dedicated sandboxes and only after that is allowed to pass to critical infrastructure of the organization.

5.1 Antivirus and Protection Against Malicious Software

Antivirus and malware protection software is a program or set of programs intended for the prevention, search, detection and removal of viruses and other malicious code, such as worms, Trojans, adware, ransomware, keyloggers etc.[10] These tools must be constantly updated, because the computers without the latest virus and malware protection are infected within minutes after connecting to the Internet. Companies developing antivirus and malware protection products must renew its products on a daily basis, because there are created more than 60,000 new viral mutations every day and number of attacks is continuously increasing. Basic functions of antivirus and malware protection products are as follows:

– Scan specific files and directories and identify known malware and viruses;
– Allow to plan and execute automatically run anti-virus programs;
– Initialize at any time to scan suspicious files or the entire computer;
– Remove all revealed malicious code, informs the user of this fact, eventually only isolate suspicious files;
– Database of known malware and viruses signatures is periodically updated as necessary.

Antivirus software can be installed on an individual computer, access gateway servers, or specialized network device. In today's cloud-based time and the Internet of things it can be also rented as a service in the cloud, or can be integrated as part of the computing device in the car.

5.2 Penetration Testing, Ethical Hacking

Penetration testing is a method of testing the resistance of organization against cyberattacks[11]. Ethical hackers use the same methods of testing possible penetration for protected institutions as their less scrupulous op-

[10] CISCO, *What Is the Difference: Viruses, Worms, Trojans, and Bots?,* Security Center. 2016, http://www.cisco.com/c/en/us/about/security-center/virus-differences.html (accessed: 27.02.2017).

[11] C.C. Palmer, *Ethical hacking*, „IBM SYSTEMS JOURNAL", 2001, Vol 40, No 3, http://pdf.textfiles.com/security/palmer.pdf (accessed: 27.02.2017).

ponents. But unlike them, ethical hackers do not use detected holes in the institution defense to their advantage, but after a detailed documentation they provide effective guidance on how to increase information security for examined institutions.

The aim of ethical hacking is to evaluate the security of the network or infrastructure of the organization. The goal is to find and test all possible weaknesses in protection in order to identify all unauthorized penetration or other harmful activities. Vulnerabilities are usually found in incorrect or minimum configuration of the system, known or less known bugs in software and hardware, operating system defects or lack of technical countermeasures. Ethical hacking has become very important segment in the field of information security and is also used to investigate the possibility of human error in the complex measures in the security protection of the institution. The successful test does not automatically mean that the institution security is 100% guaranteed. It means only that the institution should be resistant to the robotic attacks and penetration attempts performed by less experienced attackers. In principle, every organization and IoT equipment connected to the Internet or providing online services should strengthen its information security by penetration tests. Different and stricter standards apply e.g. for internet payment portals, requiring operators to provide regular penetration tests after each change in the infrastructure or application. Ethical hacking is offered by many commercial companies and is sold as a service. To qualify for a penetration test to be considered as ethical, it must be done with the consent of the organization or individual whose infrastructure is subject of the test. Information as the results of the test is confidential and its disclosure without permission of the institution is considered a criminal offense. Known is a case in Slovakia, the theft of e-mails from the demilitarized zone of National Security Office through weak password of server administrator, as a warning of the weak protection of government institutions.

5.3 Sandbox

In computer security terminology, the term "sandbox" means a security mechanism for the test of running programs in physical separated architecture. It is used frequently to verify untested programs or code, usually from an untrusted source. Thus preventing damage or infection to the production computers and operating systems. It usually consists of separate technical devices such as CPU, disk and memory. Network access and the possibility of intervention in the structure of the host computer are mostly limited. Programs in sandboxes are verified before entering the real operation, as they may contain viruses or malware. Sandbox can be configured as a virtual server with limited penetration possibility to interact with production infrastructure and thus prevent the spread of infection, especially with zero-day infections, whose signatures are not already in the database of known viruses, worms or malicious code.

6. Security Intelligence and Analytics Level

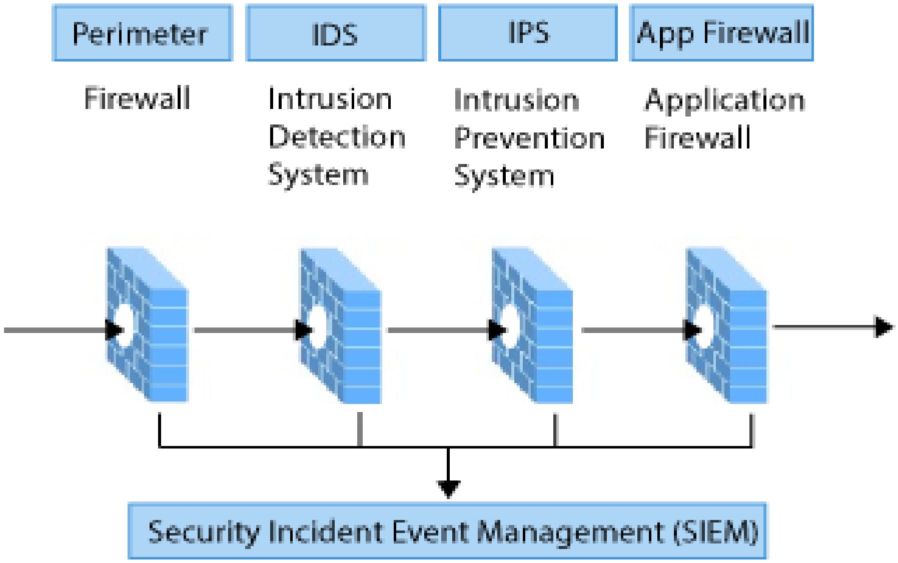
6.1 Security Information and Event Management, SIEM

System for information and event management is a combination of products and services by which institution obtains security information management and logs of security events in real time. Network hardware and software generates alarms and messages to the administrators of protected infrastructure. System monitors data from various sources and users behaviour. It monitors user and service authorizations, directory services accesses, and any changes in system configurations. Simultaneously it records all relevant information for audit and monitors all actions after the occurrence of a security incident. The system records obtained data in the correlation, seeks common event properties and combines them into meaningful ties. Data are stored for a long period of time to allow forensic analysis of connected or standalone incidents.

Intrusion Detection Systems (IDS) are devices or software applications that monitor malicious activity of network and computer systems, respectively an activity that is not in accordance with the policies of the institution. Each detected suspicious activity is reported to the administrator or recorded centrally in a specialized security system for information and events management, referred to as Security Information and Event Management. SIEM systems combine outputs from multiple sources and use filtering techniques to reduce false alarms. It is a very wide range of systems that can be implemented in SIEM, starting from anti-virus programs to hierarchical systems that monitor the operation of the entire network of the institutions.

Important IDS classification is based on the method of intrusion and event detection. Most are based on detection of signatures, i.e. known groups of code characters that are malware and anomaly detection that captures deviations from the standard model, normal operation. Such detection is based on a gradual learning IDS system, which recognizes usual normal operation and any unusual deviation raises an alarm in a suitable response system.

Picture No. 2: Security Incident Event Management


Perimeter
IDS
IPS
App Firewall
Firewall
Intrusion Detection System
Intrusion Prevention System
Application Firewall
Security Incident Event Management (SIEM)

Although intrusion detection systems IDS as a part of SIEM and firewalls both provide increased security to protected computer networks, the difference is mainly that firewall oversees intrusions into the protected network and tries to prevent them. Firewall usually does not report alarm in response to attacks occurring inside the protected network. IDS evaluates suspected intrusions declared by the respective alarms according to the type of incident. IDS also see the incidents that arise in the protected system so that examines the communication in the protected network and identifies known signatures, identification marks of cyber-attacks or unauthorized access and reports them to the operator. If the system is also in a position to terminate suspicious communication, this is an intrusion prevention system (IPS). Typical examples of the deployment of such systems with which we can all meet is the input protection to online banking to recognize typical behaviour of the account holder by unusual methods of potential thieves.

7. Advanced Security and Threat Research Level

Security threats from cyberspace are continuously evolving and changing. The number of attacks is still growing in number and complexity followed by corresponding increase in the losses caused by these attacks. For each institution and the individual it is therefore critical to deploy system for preventing and anticipating attacks. Such system must be permanently updated to contain effective security solutions. This layer of advanced security architecture and research monitors threats at all silos of the described security model. Organizations are facing an enormous increase of data that must be incorporated in this research. Also complexity of threats used in advanced persistent threats is evolving rapidly. Scope of relevant security data continues to broaden dramatically in social media and global event data. Advance in predictive analytic continue to advance. As it is nearly impossible for typical organization to perform even a small portion of this complex research, it is done by specialized companies, which monitor threat trends and develop security content for use in security products. If such research should be effective, access to live customer data by live monitoring of managed security services traffic is necessary. Global event monitoring and global reach is an important aspect.

References:

1. Andress J., *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.). Elsevier Science, 2014.
2. Bremer I., *The geopolitics of cybersecurity*, "Foreign Policy", http://foreignpolicy.com/2011/01/12/the-geopolitics-of-cybersecurity/(accessed: 27.02.2017).
3. CISCO, *What Is the Difference: Viruses, Worms, Trojans, and Bots?* Security Center. 2016, http://www.cisco.com/c/en/us/about/security-center/virus-differences.html (accessed: 27.02.2017).
4. Fabian K., *Crisis Management Training System For Advanced Security Threats In Cyberspace*, Proceedings of IMSCI, Orlando, Florida USA 2014.
5. Fabián K., Melková M., *Vybrané otázky kybernetickej bezpečnosti*, Belianum -Vydavateľstvo Univerzity Mateja Bela v Banskej Bystrici, Fakulta politických vied a medzinárodných vzťahov, 2016.

6. ISO, ISO/IEC 27032:2012 *Information technology — Security techniques — Guidelines for cybersecurity*, International Organization for Standardization. 2012, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375 (accessed: 27.02.2017).
7. Johnson T. A., *Cyber-security. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare.* CRC Press, 2015.
8. Kazanský R., Melková M., *Information Technologies and their Usage in Crisis Management as a Tool to Increase the Quality of Educational Process,* [in:] 15th International Multidisciplinary Scientific Geoconference SGEM 2015. Vol. 3. STEF92 Technology Ltd. Sofia, Bulgaria.
9. EU International Cyberspace Policy, *European Union External Action*, 2014, http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm (accessed: 27.02.2017).
10. Palmer C.C., Ethical hacking. [in:] *IBM SYSTEMS JOURNAL*, Vol 40, No 3, 2001, http://pdf.textfiles.com/security/palmer.pdf (accessed: 27.02.2017).
11. Shindler D., *SolutionBase: Strengthen network defenses by using a DMZ*, TechRepublic,2005,http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/(accessed: 27.02.2017).
12. Terem P., Čajka P., Rýsová L., *Slovakia in geopolitical and geo-economic context.* 1. vyd. – Praha: Kamil Mařík – Professional Publishing, 2015.
13. Ušiak J., *Security cooperation within V4*, [in:] Central and Eastern European Political Systems. Metropolitan University in Prague, Prague 2016.

Cite this article as:

K. Fabián, M. Dobrík, M. Melková, *Information Security Model for Crisis Management Simulations*, “Security Dimensions. International and National Studies”, 2017, no 21, p. 44-59, DOI 10.24356/SD/21/2.