Practical Issues of IT Security Incident Handling in Market Environment and in Public Administration

Gábor Sági[1]

Abstract:

Without the knowledge of events taking place in IT systems and their analysis from security's point of view, the organizations cannot ensure the business and legal expectations and adequacy. The author in this article introduces the criteria needed to realize efficient security event and incident handling, including technical, processual and legal aspects.

Keywords: incident handling, security operation center

Absztrakt:

Az informatikai rendszerekben zajló események ismerete, biztonsági szempontból történő elemzése nélkül a szervezetek nem tudják biztosítani az üzleti és jogszabályi elvárásokat, megfeleléseket. A szerző jelen cikkében bemutatja milyen feltételek szükségesek a hatékony biztonsági eseménykezelés megvalósítása érdekében, legyen szó az eseménykezelés technikai, folyamati vagy jogi aspektusáról.

Kulcsszavak: incidens kezelés, biztonsági felügyeleti központ

[1] *PhD student of NKE, e-mail: gabor.sagi@yahoo.com, ORCID identifying number: 0000-0002- 4473-0895*

Review

All the actors of the market and society, the state's institutions, educational institutions are forced to introduce newer and newer services as our age requires to serve their clients better and more efficiently. The more complex requirements, the shortening of development lifecycles and the lack of available financial sources are bound to carry possible failures caused by the inadequacy of planning or implementation. Because of the more complex structure of systems the number of visible or less visible failures are increasing. Contrary to the errors in business processes which are noticed in a short time, the errors in operation, security insufficiencies come to light in connection with an incident such as the slowing down or the shutting down of the system or - in case of security insufficiencies – the unauthorized modification or disclosure of data handled in the system. Failures in business processes usually can be avoided by thorough testing, those in operation can be avoided by deliberate planning and by the selection of an adequate configuration, but the avoidance of security insufficiencies can only be ensured limitedly because of the high number of system components, the errors within, and because of unknown vulnerabilities. It is especially important to the secure operation of the system that the improper functioning comes to light i.e. the alert of the loss of the system's and the stored data's integrity, confidentiality and availability reaches the assigned (IT security and/or operational) division. The loss of availability is usually easily noticeable, the loss of integrity and confidentiality is not so spectacular, in a lot of cases during the monitoring of the system's parameters they may stay invisible. To make these security events visible, it is essential to operate sufficient security systems and processes.

Mostly in such a large enterprise environment where numerous IT systems with different purposes operate, the effective information security can barely be realized without a security monitoring center which contains a central security system, the human resource operating it and the properly operating processes. In accordance with available resources and depending on the maturity of the organization, security operation can use different technological solutions, and depending on the organizational culture, can ensure the operation of the activity in frames of different organizational solutions. In general, the applied technological solutions, the legal options, the organizational frames and the organization's maturity define the quality and the quantity of the processes used during the security operation.

National Regulation

In case of critical information infrastructures important from the state's, the market's, the society's and defense's points of view Act No. CLXVI. of 2012. on the identification, designation and protection of critical infrastructures and facilities[2], and Act No. L. of 2013. on the electronic information security of the government and local governments (hereinafter: Ibtv.)[3] and their implementing regulations contain several rules in order to protect electronic information systems. The requirements and activity related to security events, or with international terminology: incident handling, are defined in the implementation regulations of Ibtv. [Regulation of the Ministry of Interior No. 41/2015 (VII. 15.) on the technological security, the secure informational devices, products and the requirements of classification to security category and security level defined in Act No. L. of 2013 on the electronic information security of the government and local governments (hereinafter: Reg. No. 41.)[4], as well as in Regulation of the Government No. 185/2015. (VII. 13.) on the governmental incident handling center and its functions and authority, and on the rules of security incident handling, the security incident's technical investigation and on the carrying out of the vulnerability testing process (hereinafter Reg. No. 185.)[5]]. While Reg. No. 185. contains the rules of notifying the incident handling center of security incidents and the investigation of said incidents, Reg. No. 41. contains requirements related to the security classification of the system for organizations operating (using and operating) electronic information systems themselves.

[2] *Act No. CLXVI. of 2012. on the identification, designation and protection of critical infrastructures and facilities* *http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV* *(downloaded: 2017.06.04)*

[3] *Act No. Act L. of 2013. on the electronic information security of the government and local governments* *http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV* *(downloaded: 2017.06.04)*

[4] *Regulation of the Ministry of Interior No. 41/2015 (VII. 15.) on the technological security, the secure informational devices, products and the requirements of classification to security category and security level defined in Act No. L. of 2013 on the electronic information security of the government and local governments* *http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV* *(downloaded: 2017.06.04)*

[5] *Regulation of the Government No. 185/2015. (VII. 13.) on the governmental incident handling center and its functions and authority, and on the rules of security incident handling, the security incident's technical investigation and on the carrying out of the vulnerability testing process* *https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm* *(downloaded: 2017.06.04)*

In Reg. No. 41. the expectations of logging activity at the lowest security level appear[6], but the requirement of security incident handling appear only in case of electronic information systems at least at security level 3, though the regulation gives few guidelines to what concrete technological content is enough to meet certain requirements.

Several national works are available on the possible processes of incident handling, on the participants, their activity and their responsibilities, but the technical literature is still in debt with works on the formation of supervisory competency, the technical competency necessary to operate processes.

International excursion

Incident handling on an international level has a greater past than the national, that is why the available literature is more extensive. From the available literature *„Computer Security Incident Handling Guide special Publication”*[7] published as No. 800-61 in 2012 by NIST which describes in detail the elements of incident handling, the process and the communication between the participants is outstanding. From the NIST's Publication No. 800-61's different point of view, partly expanding its content and complementing it with newer but nonetheless important details for the formation, operation and maintenance of a new security center MITRE published the *„Ten Strategies of a World-Class Cybersecurity Operations Center”*[8] and Cisco Press published the *„Building, Operating, and Maintaining Your SOC”*[9], and many other, shorter works can be read on particular subfields from which the works published by SANS, Ernst & Young, Paladion and Gartner are outstanding.

Competencies of the security operation center

To operate an effective security supervision, numerous competencies are necessary, but which these competencies are, appear differently in different works.

[6] *SÁGI, Gábor: Informatikai rendszerek naplózása (Nemzetbiztonsági Szemle MMXVII/I, http://uni-nke.hu/uploads/media_items/sagi-gabor-az-informatikai-rendszerek-naplozasa.original.pdf (downloaded: 2017.06.04)*

[7] *NIST 800-61 Computer Security Incident Handling Guide Special Publication Revision 2 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (downloaded: 2017.06.04)*

[8] *MITRE Carson Zimmerman: Ten Strategies of a World-Class Cybersecurity Operations Center https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf (downloaded: 2017.06.04)*

[9] *Joseph MUNIZ, Gary MCINTYRE, Nadhem ALFARDAN: Building, Operating, and Maintaining Your SOC CISCO Press 2016 ISBN-13: 978-0-13-405201-4*

However, different literature works agree that these activities can be divided into three categories[10]:

- Preventive: during prevention such activities shall be done that make it impossible for the dangerous event to occur. Preventive measure is for example the content filtering of e-mails, which prevents the infiltration of harmful codes through mailing.
- Detective: during detection, you try to notice the attack or damage in progress as soon as possible, then you try to eliminate it before any critical damage is done. For instance, the use of an IDS[11] system alerts you of suspicious packets. Based on the detection you can perform other activities.
- Corrective: corrective measures decrease or eliminate the damage done by an event. Corrective measure is for instance the restoration of the system from a save, as well as having an insurance that provides cover in case of damage.

However, countless competencies can appear in the three groups of activities which are – in my opinion – essential to the effective operation:

- real time detection: notifications on communication channels (telephone, e-mail) or the detection of alerts coming from business/supervision/monitoring systems
- analysis of incidents, response and mitigation: the collection, analysis of information related to real time detection, the giving of possible response and mitigation to the incident
- Threat intelligence information management: the collection and analysis of technical, tactical, strategic information coming from external sources and the forwarding of relevant information to the divisions concerned (e.g.: forwarding vulnerability information to the IT operation division, forwarding operative information related to new attack techniques to IT management, forwarding strategic information to senior management level). Sharing threat intelligence information (e. g. on new attack forms, on new IoCs[12]) revealed inside the organization with other organizations.
- handling artifacts: the collection of evidence emerged during an incident and their storages in an adequate way (such as making a bit-by-bit copy[13]) and the investigation of activity (e.g. the analysis of malware, analysis of network traffic, analysis of endpoint activity,

[10] *MUHA Lajos: Útmutató az informatikai biztonság megvalósítására önkormányzatok számára* *http://www.kormanyhivatal.hu/download/0/1a/00000/it_biztonsag_onkormanyzatoknak.doc (downloaded: 2017.06.01)*

[11] *IDS: intrusion detection system*

[12] *IoC: Indicator of Compromise, e.g. attacker IP addresses, suspicious file hash)*

[13] *bit-by-bit copy: create an exact, bit stream copy of the original storage medium*

- the maintenance, operation and development of the operation center: the performance of daily operational tasks, the fitting to the constantly changing IT environment, the incorporation of vulnerability information, and the incorporation of experiences collected during incident investigation that are essential to the effective supervision, which can be complemented even with the use of individually developed solutions
- the support of compliance tests and audits
- the support of inner fraud reconnaissance and investigation

In an organization, several competencies can be developed, although which are closely related to the organization's security operation system do not necessarily belong to the operation center, even though they are essential from the secure operation's point of view:

- discovery and management of vulnerabilities: the mapping of vulnerability of devices in the network infrastructure ad-hoc or periodically, the revelation of the real threat of vulnerabilities (e.g. if the system is not accessible from the outside according to the network map, the handling of the vulnerability can happen with a lower priority), the following of the vulnerabilities' reparations
- operation of border protection systems: the operation and configuration of the organization's border protection devices (firewall, router, proxy)
- penetration testing: putting systems operated by the organization into operation or the security testing of a system development before put into operation, and periodically in order to ensure that the system cannot be hacked even with special knowledge and devices
- security testing: the security testing of newly introduced functions and devices
- consultation: support in information security issues during the development systems
- awareness training: making materials for general and information security education related to security incidents, providing and organizing awareness trainings, and measuring the information security of employees (e.g. the willingness to open spams "created" by the security division, the handling of "accidentally" lost devices),
- media relations: communicating the daily course of business and security incidents

Depending on the information security involvement of the organization, the available resources and last but not least the organization's traditions, some competencies does not appear inside the organization, or if they do appear, it is not sure that they are under the operation of information security division. Based on my experience, in a lot of cases the network division is responsible for the operation of border protection devices, or for example security testing (involving penetration testing as well) is done by a dedicated testing group, the other listed competencies can usually be found at other departments of the organization.

The condition of the security operation center's operation

To perform the tasks assigned to the security operation center all necessary conditions for its operation should be provided together. The lack of these conditions or reduced performance can significantly influence the quality of the incident handling competence.

- data, information providing
    - Data created in IT systems (e.g. security devices, endpoints, servers, applications) that are relevant from security's point of view have to be sent to the operation center for processing. These data can be descriptions of activities carried out on a computer (logs) or alerts of security systems. The task of the systems supporting the operation center is to process these data and notify the incident handlers of the security event's detection if necessary.
    - The relevant data from security's point of view related to IT systems (e.g. functions of systems, their locations, risks of systems, information on their vulnerability, data of the users). These data can improve the classification of incidents detected, the definition of the incident handling's priority, fasten the response for a security event significantly and can make the analytical activity easier.
    - Vulnerability information from external sources (e.g. CERT[14], TI[15] providers). Information from others' analyses of events can help effectively to protect an organization's information systems and carrying out preventive activity.
- operating processes
    - With the help of processes related to preventing incidents (e.g. awareness trainings, setting IoCs) the organization can be capable of preventing or stopping attacks at an early stage, and thus ensuring the secure operation of the organization.
    - Processes related to the identification and analysis of incidents ensure that with the automatic or manual investigation of data generated in information systems, those events can be identified

[14] *CERT: Computer Emergency Response Team*

[15] *TI provider: threat intelligence provide (provide e.g. harmful IP's, domains, suspicious file hash)*

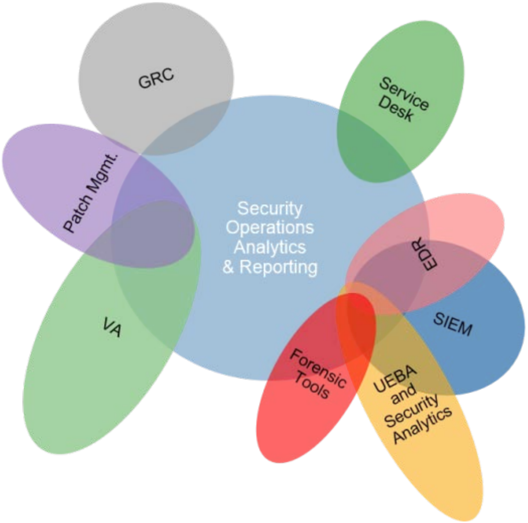
that have a malicious effect on the secure operation of an information system.

  - Processes related to incident handling help the activity of incident handlers by ensuring workflow-based incident handling depending on the system's competencies even with automatic carrying out of activities (e.g. automatic sending of suspicious files to a behavior-based analysis system), sending the specifics of a harmful activity to the protection systems depending on the result of a given investigation (e.g. sending to the firewall and blocking automatically the IP address related to harmful traffic), and providing reporting competency.
  - With processes after closing the incident investigation (e.g. implementing experience, targeted awareness-raising) ensuring that the experience gained during security events are built in the daily work, those involved get information on preventing, noticing and handling attacks with similar specifics.
- technical conditions
  - The security operation center must be evolved in a way that it would be suitable for continuous work and in case of a more serious security incident, it would be suitable for supporting more people's (usually leaders') effective work, for ensuring a warroom kind of operation. It is advisable to build the office in a way that complies with the highest ergonomic requirements (because of the continuous and in case of an incident, work under stress).
  - A complete IT environment – possibly independent from the company's infrastructure - has to be provided to the data sent to the operation center and to ensure the operation of processes for data analysis. It is advisable for the whole infrastructure to be independent (e.g. individually operated network segment, serves, communication channels).
- providing personnel
  - For incident handling the personnel with adequate knowledge shall be provided. While for the detection and initial basic analyses of a security event an operator with a lower level of knowledge but with higher tolerance of monotony is suitable enough, for operating the analytical, engineering and hunter activities creative experts with a higher level of knowledge are needed. In a well put-together analytical team, an expert on every IT system can be found (e.g. Windows, Linux, network and database expert, malware analyst).

- The employees operating the devices (hardware, software, network) which ensure the operation of the incident handling center must have experience with the operation and configuration of the devices used.

The structure and connections of the security operation system

In the previous chapters it was introduced what kind of competencies a security operation center can have and which conditions are needed to ensure these competencies. However, the existence of these competencies is not enough on its own to sustain the operation function, and to make the activity operable, these parts should be integrated with one another. This integrated approach is presented by the model published by Gartner[16]. (Figure 1.)


GRC
Service Desk
Patch Mgmt.
Security Operations Analytics & Reporting
EDR
SIEM
VA
Forensic Tools
UEBA and Security Analytics

1. Figure - Gartner „Innovation Tech Insight for Security Operations, Analytics and Reporting", 2015

The support of the incident handling process

[16] *Oliver Rochford, Paul E. Proctor: Innovation Tech Insight for Security Operations, Analytics and Reporting* https://www.gartner.com/doc/3166239/innovation-tech-insight-security-operations *(letöltve: 2017.06.02)*

The most important part of the security operation center is the Security Operations Analytics & Reporting (SOAR) system, where the information generated in the relating systems appear to find out whether an event is indeed a security event and if so, to make its scope, effect, priority and the circle of those who should be involved in the incident handling definable, support the incident handling processes and, during the closing of an incident, to ensure the reporting of data gathered during the incident according to uniform principles and the sending of the report to the concerned parties.

The operators can get alerts from source systems in the SOAR, they can start the incident handling processes from here, the analysts can start the incident analysis from here or in case of suspicion, the hunting activity.

The visibility of a security event – data sources

The data generated in IT systems can arrive from multiple sources and in multiple ways. One of the most important element from the effectiveness of the security operation's point of view is the processing and analysis of logs and alerts of events occurred in different source systems (servers, work stations, network and other security devices), which are usually done by a central security information and event management system (SIEM). The log collection can be complemented with netflow and packet collections as well. It is the task of the SIEM system to receive and analyze technical threat intelligence information from external sources. Usually built in the SIEM systems, above the log collection and analysis function these systems are able to the correlation and statistical based analysis of data gathered, which ensures that the visibly not connected events are revealed.

One of the possible methods of recognition, primarily of security events with unidentified IoCs is the surveillance and analysis of endpoints' activity. Depending on the capability of the endpoint detection and response (EDR), above the-recognition of signature-based attacks they are able to recognize unknown patterns of behavior, to evaluate the security risks of different activities and to find connection between events so as to alert to suspicious activities. The EDR systems beyond the surveillance of activity on computers provide the opportunity to download important objects to the analysis of running files, data in memory etc. from the device. The modern EDR systems are able to take automatic actions as well as manual ones to prevent from harmful activities on the devices connected to the network, with the containment of running applications, processes and disconnecting the device from the network.

Over the last few years the user and/or entry behavior analytics (UEBA) has been widely spreading, which identifies which activities differ from the "usual" activity from the activities in a system and/or from network traffic that may as well imply harmful activity. While a few years ago these products were introduced to the market as independent products, nowadays – thanks to the acquisitions – this function has become an integral part of SIEM and other defense systems.

In order to collect and analyze traces of an occurred security incident, forensics equipment is used, which collects the traces of a security event from source systems such as data on hard drives, logs, network traffic and package data. The purpose of collecting is partly to support investigation and partly to support an occasional official or inner investigation with evidence.

Other information sources related to event handling

An organization – depending on its maturity – usually operates an Information Security Management System (hereinafter: ISMS), whose IT support can use a so-called GRC (Governance, Risk, Compliance) system, which may provide data from resources (e.g. services, systems, infrastructure's elements, human etc.) in the enterprise for the operation center and the risk data related to the resources to make it possible to set a priority during security event handling and for the analyzer to gain information important from the analysis' point of view as soon as possible.

In the information system operated by an organization, the existing and known vulnerabilities have a special importance because these points can easy be targets to an attack. At the same time, not all of these vulnerabilities mean an exploitable point of attack, though to define the possible involvement, the knowledge of network information is absolutely necessary beside vulnerability information. The important information for an incident handler are for example: in case of an alert coming from an IDS system, whether the initialization of an incident handling procedure is necessary, as the attack is against a system which is not vulnerable, or the target of the attack is inaccessible from the attacked network segment.

Information on change coming from the IT systems' patch management system partly helps the preparation of the SIEM, the central operation system for the change with configuring correlations, alerts and event handling procedures, and partly the false alerts caused by the different operation as a result of the system's change can be avoided.

The relations system of incident handling

Related to incident investigations and alerts, the incident handlers may initialize such changes that they cannot implement because of the lack of accessibility to the IT systems. These requests are advised to be initialized through ticketing (e.g ServiceDesk) operated by the organization, where the incident handler can receive feedback on the status of the request from.

Even though the figure of Gartner does not include the sharing of threat intelligence, in my opinion it is an important part of the incident handling procedure. In case of larger organizations, the disclosure of non-classified information can be regarded as a social engagement, because in this way this organization may contribute to the formation of a more secure information society.

Security operation as a service

Mostly small and medium sized organizations – because of the lack of resources – cannot operate an individual information security event handling division, cannot evolve an effective and continuously working incident reaction competency. The situation is similar to those organizations that are legally obliged to use a central IT and electronic provider as they do not have independent information security event handling competency – except those organizations which the central infrastructure operator provides only a part of the service for (e.g. infrastructure (IaaS) or platform (PaaS). At the same time, these organizations have to protect their information systems which they can use as a service from a provider with adequate competency, who can be a market participant, but in case of administrative bodies, the central infrastructure provider.

Independently from the type of the provider, the functions, the responsibility, the limits, and the technical conditions for providing service have to be defined in detail.

If the laws allow it, security operation can be imagined in several types of operation models:

- The whole event and incident handling is done by the service provider in possession of a certain authorization, either by directly controlling the IT operational divisions or by configuring other service provider-operated system components.
- The service provider only alerts the organization to the security event, the whole investigation and responding is done by the organization with the help of data sent by the service provider or stored in its own systems.
- Differed in contract, any transitional solutions can be imagined between the two models, depending on the quality and quantity of resources the organization has. In case of cloud computing "Defined Categories of Service 2011" published by the Security as a Service Working Group of Cloud Security Alliance helps[17].

[17] *Kovács Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai Doktori Értekezés* http://uni-nke.hu/feltoltes/uni-nke.hu/konyvtar/digitgy/phd/2015/kovacs_zoltan_2015.pdf *(downloaded: 2017.06.01)*

In case of a significant security event the organization can evolve in an ad hoc way or by law an external incident investigating organization (in case of public administrative bodies the GovCERT, in case of business organizations the service provider whose activity field is incident handling).

The incident handler operating in either model may have access to legally protected data (mostly personal, sensitive data and business secrets). In case of business secrets, data handling and accessibility can be regulated freely in a contract. In case of personal and sensitive data handling Act No. CXII. of 2011 on the right of informational self-determination and on the freedom of information (hereinafter: Privacy Act)[18] imposes strict rules, including that all the conditions of personal data handling have to be regulated in a contract with the responsibility, functions and informing obligation of the parties.

If an organization outsources the security operation function, then the organization is advised to act in accordance with the recommendation published by the Hungarian National Authority for Data Protection and Freedom of Information in 2013.

The law in effect imposes rules on the central IT and electronic service provider appointed by law how to operate its systems securely, though does not give additional authorization for the service provider and does not define what the service provider can do and what data it can handle in interest of this. As long as the service provider provides security services, in the current legal environment it has to agree on the terms of data processing/data handling with all the parties and regulate it in contracts. Regarding the circle and number or organizations concerned and the interest of protecting the handled data, it would be expedient to regulate the issue of data handling by laws, creating the bases of unified data handling during incident handling.

In interest of the requirements defined in Ibtv. and in the Privacy Act, it would be important to draw up recommendations for the professionals on – among others, in interest of the mass protection of personal data – what data the incident handler can handle, with what conditions the incident handler can look into that letter or netflow, with the help of which data leakage may be occurring, or other security event happens that concerns data handling or processing.

Summary

[18] *Act No. CXII. of 2011 on the right of informational self-determination and on the freedom of information* https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV *(downloaded: 2017.06.01)*

To protect information systems effectively – beside the traditional solutions – it should be ensured that logs of events in information systems are made, these logs are sent to the analyzing systems and the recognition and handling of security events occur. Beside the information generated during incident prevention and handling, indicators of harmful activity coming from external sources are very important. In many cases, the inclusion of co-areas is needed as well as in the practical realization of responding to incidents.

Above the technological and processual conditions there is a special importance to legal adequacy, mostly to Privacy Act, because the incident handler has to handle personal data (IP addresses, e-mail addresses, login names etc) inevitably during an incident. Even though the practice has been changing lately, it could not be said that it is uniform and – as far as I know – it has not been audited yet by the data protection authority.

References

- Act No. Act L. of 2013. on the electronic information security of the government and local governments http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (downloaded: 2017.06.04)
- Act No. CLXVI. of 2012. on the identification, designation and protection of critical infrastructures and facilities http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (downloaded: 2017.06.04)
- Act No. CXII. of 2011 on the right of informational self-determination and on the freedom of information https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV (downloaded: 2017.06.01)
- Joseph MUNIZ, Gary MCINTYRE, Nadhem ALFARDAN: Building, Operating, and Maintaining Your SOC CISCO Press 2016 ISBN-13: 978-0-13-405201-4
- KOVÁCS Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai Doktori Értekezés http://uni-nke.hu/feltoltes/uni-nke.hu/konyvtar/digitgy/phd/2015/kovacs_zoltan_2015.pdf (downloaded: 2017.06.01)
- MITRE Carson Zimmerman: Ten Strategies of a World-Class Cybersecurity Operations Center https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf (downloaded: 2017.06.04)
- MUHA Lajos: Útmutató az informatikai biztonság megvalósítására önkormányzatok számára http://www.kormanyhivatal.hu/download/0/1a/00000/it_biztonsag_on kormanyzatoknak.doc (downloaded: 2017.06.01)
- NIST 800-61 Computer Security Incident Handling Guide Special Publication Revision 2 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (downloaded: 2017.06.04)
- Oliver Rochford, Paul E. Proctor: Innovation Tech Insight for Security Operations, Analytics and Reporting https://www.gartner.com/doc/3166239/innovation-tech-insight-security-operations (downloaded: 2017.06.02)
- Regulation of the Government No. 185/2015. (VII. 13.) on the governmental incident handling center and its functions and authority, and on the rules of security incident handling, the security incident's

technical investigation and on the carrying out of the vulnerability testing process
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm
(downloaded: 2017.06.04)

- Regulation of the Ministry of Interior No. 41/2015 (VII. 15.) on the technological security, the secure informational devices, products and the requirements of classification to security category and security level defined in Act No. L. of 2013 on the electronic information security of the government and local governments
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV
(downloaded: 2017.06.04)
- SÁGI Gábor: Informatikai rendszerek naplózása (Nemzetbiztonsági Szemle MMXVII/I)
http://uni-nke.hu/uploads/media_items/sagi-gabor-az-informatikai-rendszerek-naplozasa.original.pdf (downloaded: 2017.06.04)