Scientific and Practical Cyber Security Journal (SPCSJ) 1(1):23-26

Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

IMPROVEMENT OF THE EFFECTIVENESS OF INFORMATION SECURITY MANAGEMENT USING INTELLIGENT TECHNOLOGIES

K. Alieksieiev V. Dmytruk

Taras Shevchenko National University of Kyiv

ABSTRACT

The new types of threats to information introduce new approaches to building protection systems, the protection against threats in real-time. The arising number of security issues in the information environment makes you look for new methods and approaches to the management of information security incidents. The incidents management is a critical process that provides organizations with the ability to, firstly, identify an incident, and then using properly selected support tools as soon as possible to resolve it. Intelligent systems have recently become a common commercial product that finds wide demand from users-specialists in various fields of engineering-technical and scientific spheres of activity.

Key words: incident, decision support, incident management, information system, security.

None of the most advanced measure to reduce information security risk, whether it is thoroughly worked out policy or modern firewall can guarantee appearance of events that potentially threaten the business activities of the organization in the information environment. The complexity and diversity of the business environment of modern business determine the presence of residual risk regardless of the quality of preparation and implementation of countermeasures. Also there is always the possibility of new, unknown threats for information security. Also there is always the possibility of new, unknown threats to information security. The unwillingness of the organization to process such situations can significantly hinder the recovery of the business processes and potentially increase damages.

The number of potential channels of information leakage is sufficiently large. The most common ones belong to the category of unintentional disclosures by the employees of the organization for reasons of ignorance or lack of discipline. Lack of understanding of the rules of working with confidential documents, the inability to determine what documents are confidential, and ordinary negligence in the handling of information – all these can lead to the occurrence of an accident or incident of information security.

Analysis of existing systems of management of modern information and telecommunication networks have shown that their level does not fully meet the modern requirements to the management of next generation networks, does not allow to obtain information of the right quality for making decisions on property management, exchange of information between the management

system and also makes it impossible to quickly manage situations on networks in an automated mode.

Incidents of information security (IS) is a separate subclass of crisis and emergency situations that can happen in the info-socio-technical infrastructure of the country, and, as a special case, in organizational-technical systems (OTS) and communication networks (CN), affecting the status of state information resources and national security.

The main objective of incident management is to restore normal services and minimize the negative impact of the incident on the organization to maintain the quality and availability of services at the highest of the possible level. It's considered normal, that is not beyond the scope of the agreement about level of service.

Specific issues of the management of information security incidents are described in the following documents:

- ISO/IEC 27001:2005 Information security management system. Requirements;
- ISO/IEC TR 18044 Information security incident management [1];
- CMU/SEI-2004-TR-015 Defining incident management processes for CISRT.

The first step in making decisions related to the management of incidents should be the systematization and inclusion the incident classes definitions to the Service Level Agreements (SLA).

The process of managing events and incidents can be carried out with solutions of Security information and event management (SIEM) class and well-designed organizational process [2].

Before selecting a SIEM system, you must define the criteria by which to make comparison. First and foremost, is the ability to collect events. The most significant in system of events and incidents management are the opportunities for intelligent analysis of events and their correlations. The important point is the number of basic sets of rules correlated with the possibility of adjustment.

After the discovery of the incident the task of what to do with it sharply raises. The solution is organization and documentation of identification, processing, closing, saving, and deleting the incident. Providing tools for investigation and analysis of incidents is one of the priority tasks implemented with SIEM solutions [3].

Intelligent systems have recently become a common commercial product that finds wide demand from users-specialists in various fields of engineering-technical and scientific spheres of activity.

It is also important to note that SIEM systems provide the ability to create reports on the state of information security, incident investigation reports to middle and senior management levels, as well as owners of information resources and business processes in general.

In your organization the notification system of incidents must be developed and implemented. The creation of a chain of alert is necessary to maintain the proper level of management of the organization during the processing of the incident. Team alert and the notification method are developed with consideration of peculiarities of the functioning and structure of the organization;

Analyzing the number of incidents during 2004-2015, we can trace their noticeable increase from year to year. Every day it becomes increasingly difficult to maintain a monopoly on information. The attacker always has the advantage, therefore, for organizations it is very important to be able to successfully establish an IS management system for the early detection and rapid response to incidents of any kind to minimize costs and to eliminate negative consequences.

The using of intelligent technologies in the management of incidents should give a boost to the effectiveness of the management of this process [4].

For the first time the concept of "intelligent machine" or "intellectual system" appeared in at least two decades ago. The concept of "intelligent system" and "system-oriented processing and use of knowledge" are synonymous. Intelligent systems have recently become a common commercial

product that finds wide demand from users-specialists in various fields of engineering-technical and scientific spheres of activity [5].

The concept of "intelligent system" and "system-oriented processing and use of knowledge" are synonymous. Intelligent systems have recently become a common commercial product that finds wide demand from users-specialists in various fields of engineering-technical and scientific spheres of activity.

There is a classical model for continuous improvement of management processes, called the cycle of the Shewhart–Deming PDCA (plan, Plan — Do, Do — Check, Check, Act).

Advantageously, the algorithm of intellectual management system of incidents of IS also can be fit into the cycle of the PDCA model. Information system of decision support is proposed as informational system, which can operate in the following algorithms:

1. Operational data of security sensors should be analyzed and evaluated for the presence of signatures of known incidents using knowledge base of information system of decision support (ISDS).

2. ISDS, on the basis of the analysis should provide the instruction on elimination of the causes and consequences of the incident, if the signature is in the knowledge base.

3. If there was an incident of the signature which is not in the knowledge base, ISDS gives several hypotheses regarding further actions the administrator of IS.

4. It is advisable to perform actions to prevent a recurrence of the incident. In order to have the procedure performed correctly and efficiently, all these steps must be constantly and consistently repeated.

One of the stages of incidents management is to investigate them. The investigation process can be divided into two phases: data collection and forensic analysis.

Analysis of the data collected includes analysis of files, logs, configuration files, Internet history-conductors (including cookies), email messages and attached files of installed applications, graphic files and other things. It is necessary to analyze, keyword search, check the date and time of the incident.

Forensic analysis may also include a search for deleted files and areas lost clusters, free space, and analyzing the recovered data from destroyed media (for example, residual magnetization).

The information gathered during the first phase of the investigation, is then used to develop response strategies to the incident. At the analysis stage, in fact, who, what, how, when, where and why the incident was involved can be determined.

During the investigation, incident data collection can be performed using the software "Duplicate Disk". It allows you to make exact copies of hard disk ("sector") of workstations of users (company employees) and servers. For the analysis of the obtained data VMware Virtual Machine" can be used for special emulation of working machines. Analysis of spaces of hard disks can be performed using specialized software "Encase Enterprise Edition" or the expert of Vogon International company funds. These two products are key in the world of the incidents investigation [6].

In some cases, all sorts of hardware and software packages can be used to detect traces of computer incidents, listening for the local network of the company (the commonly used product is a network sniffer Ettercap).

At the stage of investigation an important role is put on: the keeping of logs, a clear separation of user rights, responsibility for the taken actions — is an important proof of who was involved in the incident and what actions he performed.

Typical practice is logging the investigation of the incident, which has no standard form and is being developed by the response team.

Properly organized incident management process in information security is:

• a clear definition of the key roles and responsibilities for quality and current incident response;

• operational information for monitoring the effectiveness of applied measures;

• transparency of performance control of staff;

• improving the quality of interaction between experts in related it and business units.

The system of automation of the incident management process in addition allows to:

• process and store information about events and incidents of information security, and all actions on their elimination;

• make decisions on how to resolve the incident, which is based on the analysis of information about previous incidents;

• conduct analysis of the accumulated data.

To sum up, the attacker always has the advantage, therefore, for organizations it is very important to be able to successfully establish an IS management system for the early detection and rapid response to incidents of any kind to minimize costs and to eliminate negative consequences. During this task we identified the main factors, criteria and indicators of automated procedures of decision-support for managing incidents.

Thus, the proposed functional diagram of ISDS for managing incidents in the OTS can be implemented for the improvement of the effectiveness of information security management. This scheme fits into the PDCA model and process approach, defined in the relevant international standards ISO/IEC.

Also the problem of decision support during incidents in the OTS, which can be seen as part of a more general problem of support of managerial decision-making in crisis situations was described. During this task we identified the main factors, criteria and indicators of automated procedures of decision-support for managing incidents.

REFERENCES:

1.Standart ISO/IEC TR 18044:2004 "Management of information security incidents"

2.David R. Miller. Security Information and Event Management (SI-EM) implementation. / David R. Miller, Shon Harris, Allen A. Har-per, Stephen VanDyke, Chris Blask - 25.10.2010 – 430 p.

3.Information security is a big data issue [Electronic resource]. – Available with http://www.computerweekly.com/feature/Information-security-is-a-big-data-issue

4. Toliupa S. V. Design of the decision support system in the recovery process and ensure comprehensive protection in information systems. // Scientific-technical journal “Modern information security”.– 2012. - №4. – p. 69-74”

5. Gladysh S. V. “Support decision-making for managing information security incidents to the organizational and technical systems. Expert systems and decision support.” p. 116-124.

6. Software solutions [Electronic resource]. – Available with http://www8.hp.com/us/en/software-solutions/siem-arcsight/