Mirosław Ryba*, Józef Sulwiński**,
Aleksander Poniewierski***

THE METHODOLOGY FOR DETECTING AND MANAGING THE ABUSE OF IT SYSTEMS

This paper focuses on the processes of dealing with security breaches which are becoming one of the most pressing problems in every organization whose systems are connected to the global web. The study presents the most widely used methodologies which were designed in order to detect and react to security violations in a systematic and efficient way. Based on presented methodologies, announced and supported by such credible organizations as SANS, NIST, CERT® or ISO, authors present their own methodology. It takes into account selected aspects of these methodologies, with the purpose of creation a systematic and coherent approach to the process of detecting and reacting to abuses in IT systems.

Keywords: *Incident handling, security breach, SANS, NIST, CERT®, ISO*

MODEL PROCESU DETEKCJI I REAKCJI NA NADUŻYCIA W SYSTEMACH INFORMATYCZNYCH

Niniejsza praca prezentuje aspekty związane z procesem reakcji na incydenty bezpieczeństwa, które stają się jednym z najbardziej dotkliwych problemów każdej organizacji, której systemy informatyczne są połączone z siecią Internet. Autorzy przedstawiają najpopularniejsze metodyki wykrywania i reakcji na incydenty bezpieczeństwa, opracowane i wspierane przez takie uznane i poważane organizacje jak SANS, NIST, CERT® czy ISO. Następnie autorzy prezentują swoją własną metodykę, która integruje wybrane elementy przedstawionych rozwiązań w kompletne i spójne podejście do detekcji i reakcji na incydenty bezpieczeństwa.

Słowa kluczowe: *zarządzanie incydentami bezpieczeństwa, SANS, NIST, CERT®, ISO*

1. Introduction

The number of reported incidents concerning IT systems keeps rising each year. It is a result of IT technologies becoming increasingly common in nearly all areas of daily life, as well as of the imperfections of currently employed solutions. Hostile attempts to take control over an IT system have also become a means of fighting competition, thus effective security measures are necessary to maintain competitive advantage on

* Ernst & Young Business Advisory, Miroslaw.Ryba@pl.ey.com
** Ernst & Young Business Advisory, Jozef.Sulwinski@pl.ey.com
*** Ernst & Young Business Advisory, Aleksander.Poniewierski@pl.ey.com

the market (numbers of security incidents reported to CERT/CC since 1988 are shown in Figure 1 below[1]).

Organizations must take determined actions in order to minimize potential losses and to prevent the occurrence of incidents in the future. The lack of such actions may result in the increase of hostile activities in IT systems performed by intruders, as well as greater financial losses or external entities seizing the control over the systems.

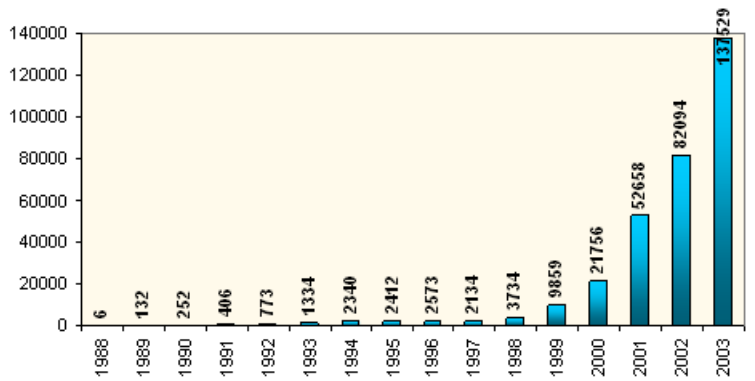

Fig. 1. Number of security incidents reported to CERT/CC since 1988, according to CERT/CC [1]

Conducting casual and uncoordinated steps towards detection and reaction to abuse (defined as security incidents resulting from misuse of granted privileges) is, in most cases, ineffective and inefficient. This is due to variety of reasons, the most frequent being:

- wrong approach, where making one incorrect decision (i.e. concerning the data seizure process) may ruin all activities carried out during the incident handling,
- lack of suitable tools, which may render the data seizure or data analysis impossible,
- lack of decision making process, resulting in the inability to make any decision or a considerable delay of undertaken actions,
- lack of funds or qualified personnel, which may prevent an effective reaction to abuse, or lead to delays and inefficiency,
- chronicity of conducted investigation, which may obstruct the process of identifying the perpetrator (the general relation between abuse detection probability and time is presented by the curve in the Figure 2 [8] – specific values depend on particular incidents), as the electronic traces of incidents are volatile.

[1] Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, CERT/CC stopped providing this statistic at the end of 2003. [1]

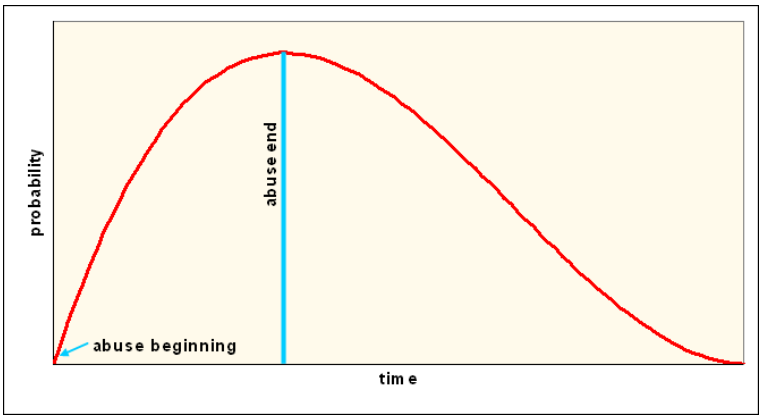

Fig. 2. Curve showing the general relation between abuse detection probability and time [8]

Moreover, in most cases handling of incidents takes place in tense atmosphere, which significantly increases the possibility of making mistakes by people engaged in the process.

A solution which effectively minimizes the influence of the aforementioned threats is the implementation of a systematic approach to detection and reaction to the abuse of IT systems. A properly designed and applied process, reinforced by procedures which explicitly appoint the responsibilities of individual employees, imposes the conduct of activities in accordance to thoroughly planned steps. It allows effective decision making and increases the possibility of successful incident handling, which leads to minimizing business risks.

2. Incident handling models

Currently, the most popular models of incident handling are:

- SANS model,
- NIST model,
- CERT® model,
- ISO model.

2.1. SANS model

The SANS model, described in detail in the publication titled "Computer Security Incident Handling Step by Step" [3], is based on the Navy Staff Office Publication 5239-19 [2]. This model defines a 6-stage process of incident handling illustrated in Figure 3.

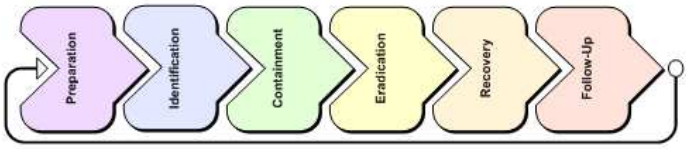

Fig. 3. SANS model schema

The stage schedule is as follows:

1. **Preparation** – during this phase the organizational and technical assumptions concerning the general process are prepared. The stage ends with the approval of the arranged plan by the Board of Directors.
2. **Identification** – this stage is focused on the analysis of available information and the identification of a potential abuse and it ends with determining the incident's nature.
3. **Containment** – during this stage the influence of the abuse on the organization is minimized.
4. **Eradication** – establishing the symptoms of the abuse, as well as its origins. The aim of this stage is to eliminate the reasons of the abuse.
5. **Recovery** – the goal of the activities performed during this phase is the recovery of the IT system and restoration of its operational status after eradicating the abuse.
6. **Follow-up** – preparing a report and analyzing the progress of detecting and reacting to abuse process in order to identify and implement potential enhancements of the process.

Due to the fact that this model was the first approach to systematic incident handling and is the oldest amongst the presented four, it is most commonly used in a variety of organizations. Within the model, the problem is eradicated as quickly as possible, so restoring normal business operations is possible in a short time. However, incidents are treated separately and without prioritization, comprehensive information about the incident is not gathered and analyzed; there is also no analysis of the incident's impact on the organization.

2.2. NIST model

The second methodology of detecting and reacting to abuse was published in January 2004 by the National Institute of Standards and Technology. The NIST 800-61 [4] model described in detail in the publication is illustrated in Figure 4.

This process comprises 4 stages:

1. **Preparation** – during this phase the process, organization and technology layers are adjusted to the general process of handling security incidents. Once this phase is completed, the organization is fully capable of detecting and reacting to abuse.

2. **Detection and analysis** – the stage covers all actions concerning collection of information on the way the system operates, concerning the detection of abuse and analysis of its occurrence and its impact on the organization.
3. **Containment, eradication and recovery** – the scope of activities performed in order to minimize the negative impact of abuse and to restore normal operational status of the IT system.
4. **Post-incident activity** – preparing improvements to the general process based on the observations made during the handling of an incident. The goal of these activities is to protect IT environment from the reoccurrence of similar abuse events in the future and to adjust the process of detecting and reacting to security incidents to fluctuating conditions (due to the constant development of technology).

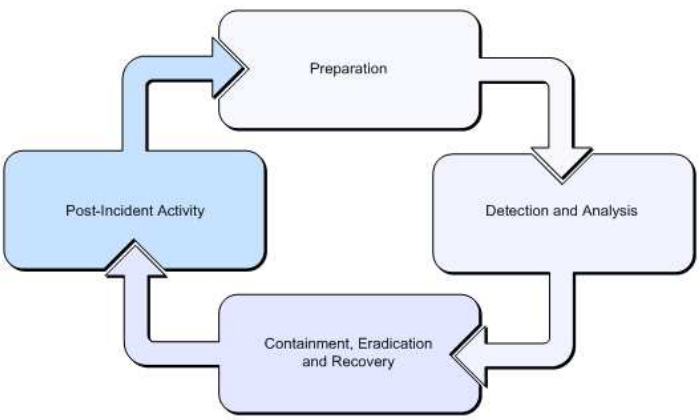

Fig. 4. NIST model schema

Comparing to the SANS model, using NIST approach comprehensive information about the incident is gathered and analyzed. Also, an analysis of the incident's impact on the organization is performed, which sets higher requirements for technical skill and planning. Moreover, incidents are still analyzed, managed and handled in isolation from each other, which implies lack of categorization and prioritization.

2.3. CERT® model

Another approach to incident handling was presented in a publication by Carnegie Mellon University Software Engineering Institute, named "Defining Incident Management Processes for CSIRTs: A Work in Progress" [6]. It was originally created specifically for handling incidents related to the Internet, but shortly after has been adopted by many organizations for their needs.

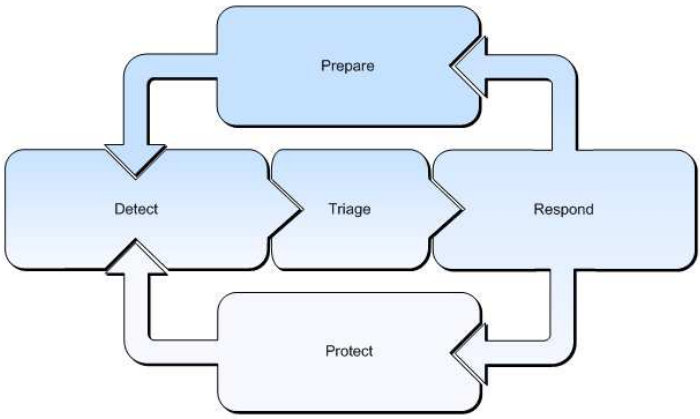

Fig. 5. CERT® model schema

The main 5 stages in the CERT®, model (Fig. 5) are as follows:

1. **Prepare** – During this stage incident management capability and the appropriate process are established in order to effectively handle detected incidents, which includes security awareness trainings, preparation of incident reporting guidelines forms and notification lists, creation of incident handling tools, incident tracking system and response policies and procedures etc.
2. **Detect** – In the Detect stage constituency reports are analyzed in order to detect incidents. For this purpose also public and private mailing lists are scanned, while assigned employees monitor the network and detect potential intrusions.
3. **Triage** – In this stage the incidents detected in the previous phase are categorized in order to standardize their further management. After that they are associated and compared with other incidents to identify any dependencies between them. During this stage the incidents are also prioritized and a team of competent employees is assigned to handle the incidents.
4. **Respond** (**management, technical and legal**) – The Respond stage consists of the following sub-stages, which, performed subsequently, ensure a proper incident handling. The sub-stages are as follows:

    - verification – verifying whether the evidence used to make decisions in the triage stage were correct, documentation – documenting all gathered information concerning the detected incident,
    - containment – minimizing possible influence of an incident on the organization,
    - notification – notifying people on the notification lists created in the Prepare stage,

- analysis & research – collecting information on the way system operates and performing analysis concerning the root causes of the detected incident,
- eradication and mitigation – establishing signs of an incident and its derivation, as well as eliminating the reasons of the incident,
- recovery – restoring the regular operational status of the affected IT system,
- follow-up – writing a report and performing an analysis of the progress of detecting and reacting to the incident, connected with the identification of possible enhancements to the incident management process in a current stage.

5. **Protect** – During this stage internal and external controls are updated and adjusted based on the current threats that have been detected. If necessary, all operational management and information systems are patched, modified and reconfigured accordingly. Moreover, infrastructure evaluations are performed and, based on threat and probability analysis, risks are determined and assessed. This, in turn, is connected with vulnerability scanning.

It is worth to point out that among the authors of publications on this model there are active members of CERT/CC – the main organization dealing with the detection of abuse on the Internet. As a result this model may be treated as a reference methodology of handling abuse incidents on the Internet or originating from it.

Comparing to previously described models, the CERT® model puts emphasis on triaging incidents – detected incidents are categorized and prioritized, so that their further management can be standardized and resources having appropriate competencies can be assigned to handle them. There is also a comparison made between the incidents in order to identify dependencies between them.

On the other hand, the main problem connected with the model is the fact that – due to multiple sources of information regarding each incident – more work is required.

2.4. ISO model

Concurrently with the publication of the NIST model, the International Organization of Standardization (ISO) introduced its own methodology, presented on the graph (Fig. 6).

ISO model is fully compatible with the Deming cycle concept – PDCA (Plan-Do-Check-Act), constituting the basis for ISO 9000 and ISO 14000 standards. The ISO model proposes 4 stages:

1. **Plan & Preparation** – this stage covers all activities resulting in a development of a new process of detecting and reacting to abuse, which offers effective control and all necessary safety mechanisms.
2. **Use** – actions focusing on detection and reaction to abuse, conducted in accordance to a plan arranged and approved in the previous stage.

3. **Review** – a number of measures taken after the reaction to the incident is finished, in order to determine the background of the event in detail.
4. **Improvements** – enhancing the general process of handling security incidents, based on observations made under way and gained experience.

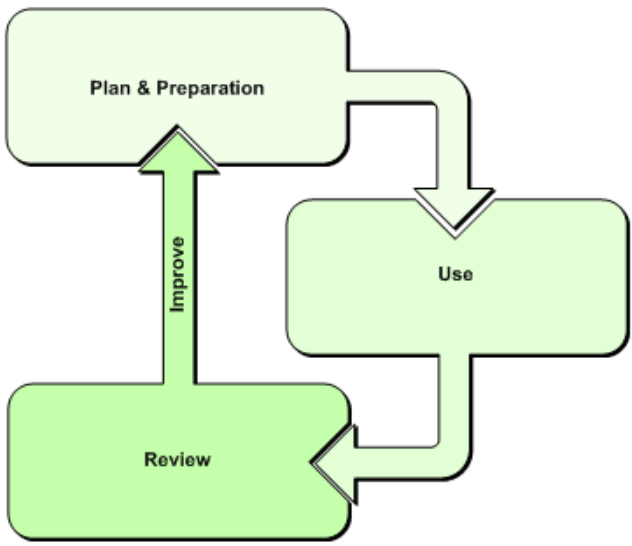

Fig. 6. ISO model schema

The main advantage of the ISO model is its integrity and compliance with other ISO standards, thus, the systematic approach to detection and reaction to IT systems abuse presented below is based on it as well. The disadvantage, though, is the fact that ISO is the most generic model (a framework, actually) amongst the others, not providing any "cookbook recipes".

3. Our systematic approach

There are different varieties of abuse concerning IT systems, therefore, incident detection and handling require carrying out numerous activities. Among these activities we can point out certain distinctive stages adjusted to the needs of the organization and its environment. These stages constitute the model of the process of detecting and reacting to IT systems abuse.

The model of the process presented herein is a development of the ISO model, with various steps taken from different models (SANS, NIST, CERT®) included. Moreover, as it is based on the Deming Plan-Do-Check-Act cycle, it is possible to

dynamically enhance it in order to adjust it to constantly fluctuating needs of the organization in regard to security.

The scheme of the systematic approach presented in this paper is shown in the Figure 7.

Table 1 shows an overview of elements common between the model presented and other models described in Section 2.

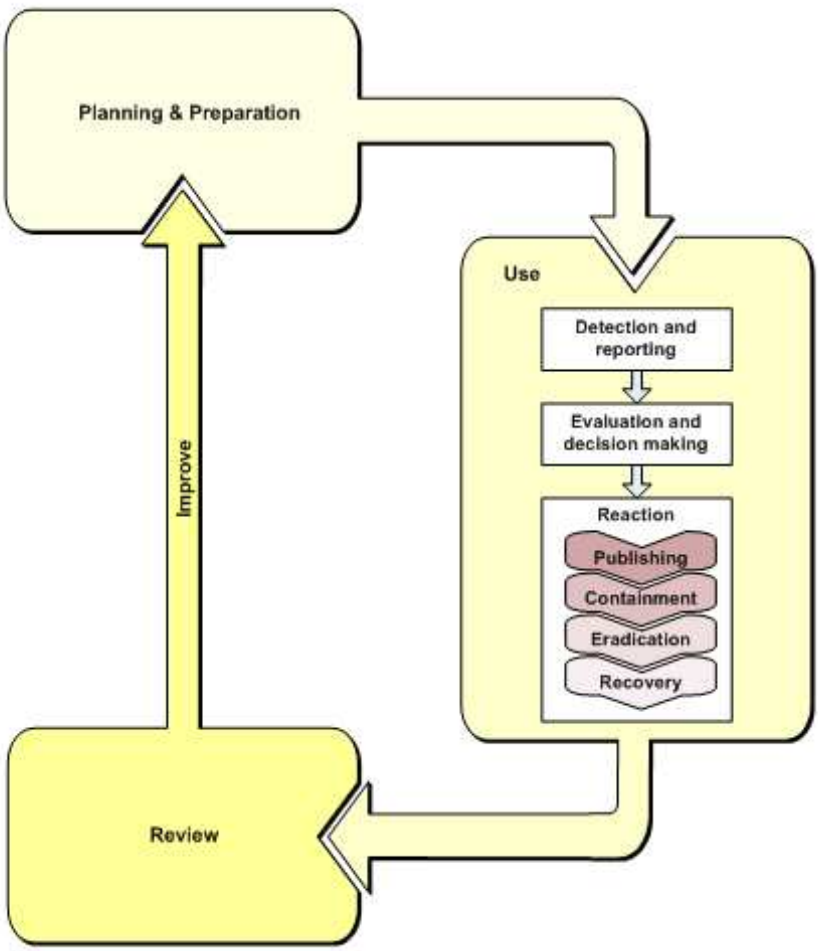

Fig. 7. A systematic approach to the process of detecting and reacting to IT systems abuse [9]

The following stages of proposed process of detection and reaction to IT systems abuse are described below.

Table 1
Comparision of incident handling models

	SANS	NIST	CERT	ISO	Our approach
Eradicating the problem as quickly as possible, so restoring normal business operations is possible in a short time	✓				
Cyclic improvements introduced to the process		✓	✓	✓	✓
Gathering and analyzing comprehensive information about the incident		✓	✓		✓
Performing analysis of the incident's impact on the organization		✓	✓		✓
Categorization and prioritization of detected incidents, so that their further management can be standardized and resources having appropriate competencies can be assigned to handle them			✓		✓
A comparison being made between the incidents in order to identify dependencies between them			✓		✓
Using multiple sources of information on the incidents			✓		✓
Integrity and compliance with other ISO standards				✓	✓
Bi-directional exchange of information on the incident (Publishing sub-phase)					✓

3.1. Planning & Preparation

The Planning & Preparation stage constitutes the key phase of defining the process of detection and reaction to abuse in IT systems. The actions carried out are focused on the development of organizational infrastructure for IT incident handling in three following layers:

1. process layer – creating a strategy, policy and detailed procedures for detection and reacting to incidents,
2. organization layer – assigning human resources necessary for incident handling, deciding on organizational structure (distributed or centralized), appointing a team responsible for reaction to security incidents, creating a training program for team members and employees, etc.,
3. technology layer – the development and implementation of mechanisms for gathering information on events concerning security of all IT systems used in the organization and of tools supporting the process of detecting and reacting to abuse.

The strategy of detecting and reacting to abuse is the reflection of the will of the Board to maintain security within the organization. The creation of the strategy as a reference point for people engaged in the process is a means of gaining support for the actions taken in the future.

The strategy of detecting and reacting to abuse should answer the following questions:

- What is the purpose of incident handling?
- For whom is this process conducted? Who is the constituency?
- Who benefits from the team's incident handling effort?
- Who is responsible for maintaining the process (funding and resources)?
- What kind of services will be provided? – (The answer to this question requires a decision of the Board, whether incidents will only be registered or additional analysis and investigation will be performed.)
- Who is responsible for the process of detecting and reacting to abuse in IT systems?

Based on the strategy, a policy of detecting and reacting to abuse is defined. In order to achieve this, the Board needs to specify in detail how the organization intends to detect and react to incidents. Additionally, the Board should indicate the relation between reaction to incidents and the performance of business processes, the requirements in regard to incident handling and the assumptions concerning work of the team responsible for reaction to information security incidents. Finally, what also should be considered are the regulatory requirements that need addressing during the general process.

A key element of creating the strategy and the policy of security incident management is management buy-in (it is easier when the created policy is based on the strategy defined by the Board). An unambiguous message to all employees (in the form of an internal regulation) is equally important, informing them of the new policy and imposing its applications.

The next step within the scope of the process layer is to design an abuse management model, including detailed procedures, forms and tools for detection, classification and handling of incidents, as well as generating reports. During this phase it is vital to pay special attention to the availability of necessary components like Change Management processes or, above all, Patch Management processes.

The specified policy and security incident management model should comply with the general information security policy of the organization. Moreover, it is crucial to assure that the activities carried out during the reaction to security incidents are in line with the current regulations.

For the purpose of effective information security incident handling, a special ISIRT (Information Security Incident Response Team) team should be appointed and adequately placed within the organizational structure. On creating the team, aspects such as the character of the team (whether it should operate in a distributed or centralized manner), the number of members and their competencies need to be taken into consideration. Individual roles and responsibilities within the group also need to be specified. Practice shows that ISIRT in most organizations is not a standalone unit, but a virtual entity (gathering as need arises). It is directed by a senior manager and supported by specialists from various fields connected with security

incidents (data analysis, seizure of evidence, etc.). The team is appointed according to the security incident management model whenever a crisis occurs, and dismantled after the incident has been handled.

The element of the technology layer of the process of detecting and reacting to abuse in IT systems are the tools (both hardware and software). They are to assure the completeness of the registration of incidents and to support the data analysis and incident handling, as well as to provide non-repudiation of data which may potentially become evidence in court.

On defining the technology layer it is important to consider the implementation of security monitoring systems, the vulnerability of assessment systems and the installation of antivirus applications. These activities are not directly connected with the process of detection and reaction to abuse, but they may have a great positive influence on its effectiveness. They are useful in gathering additional information on events occurring within the systems or in minimizing the number of incidents and abuses.

The last element of the process of detection and reaction during Planning & Preparation stage is conducting trainings which are adequate to the needs and competencies of people involved in the general process, directly or indirectly. It is also crucial to carry out so called Security awareness program on abuse of IT systems and related security oriented activities. These need to be undertaken in case of suspected abuse and conducted by the organization with regard to detection and reaction to the abuse.

The approved methodology of detecting and reacting to security incidents should be thoroughly tested. This can be performed as a general test or tests of individual procedures (e.g. the procedure of informing about a detected abuse). Any potential deficiencies observed during the process of detecting and reacting to abuse events should be corrected during the testing phase, and the process should become the subject of a next test.

As a result of completing this stage, in accordance to the steps described, the organization should be fully prepared to correctly detect and react to abuse of IT systems.

3.2. Use

The Use stage constitutes the central part of the presented process of detection and reaction to IT systems abuse. In this phase we can define the following steps:

1. Detection and reporting,
2. Evaluation and decision making,
3. Reaction.

Detection and reporting focuses on collecting events connected with IT environment security and reporting them to all people who may be involved. During this step, all events that take place in the IT infrastructure are taken into consideration. These may be those which alone seem to be an abuse incidents as well as those connected

with individual, independent events whose further analysis and comparison to detected abuse incidents may provide information on the background of the happening (user ID, computer name, network card address, etc.).

The process of collecting information can be based on the automatic acquisition of data concerning the IT system activities (e.g. through the analysis of system logs or IDS reports), or on the analysis of events coming from the users or the personnel maintaining the systems.

In the next step, i.e. the Evaluation and decision making, the classification of abuse is conducted along with the assessment of its impact on the IT environment. Depending on the decision made, the course of action regarding the abuse event is indicated. During this step the decisions concerning the seizure of evidence material and its analysis are made.

It is important to remember that any measures taken in this step should be carried out in a way that will enable securing the evidence material which is understood as source data enabling the identification of abuse, (and the perpetrator), as well as defining deficiencies which made the abuse possible. It is also vital to examine the current status of IT system that has been affected by the abuse.

After the available data has been analyzed in compliance with the scheme of detection and reaction to abuse, and after the abuse has been properly classified, the following actions can be conducted:

1. Publishing – contacts with environment with the purpose of acquiring or passing information on the detected abuse (informing the Board, internal and external communication department, cooperating CSIRTs, etc.),
2. Containment – all actions undertaken in order to minimize the negative influence of the abuse on the IT environment in the organization,
3. Eradication – measures connected with the elimination of factors which made the abuse possible,
4. Recovery – activities carried out in order to restore normal operational status of the IT system.

When no effective ways to prevent or eliminate threats concerning abuse in the IT environment are available [7], a crisis committee (capable of launching Business Continuity Plan) should be appointed.

It is worth to point out at this stage that the efficiency of actions will depend directly on the results of analysis of available evidence material and on the effectiveness of conduct of the forensic process – that is on the effectiveness of the approved security incident management model.

3.3. Review

After the analysis of security incident connected with the identified abuse, the following steps are conducted during the Review phase:

1. analysis of evidence material located outside the IT system the abuse concerned,

2. preparation of enhancements for the IT environment connected with the identified abuse,
3. preparation of potential improvements to the process of detecting and reacting to abuse in case when deficiencies are discovered,
4. preparation of final report.

The focus of the Review stage is a detailed investigation analysis conducted without any reference to the system directly associated with the abuse. It is due to the fact that not all signs of the activities concerning abuse are registered in the IT system. Thus, in most cases, it is necessary to secure and analyze the information recorded by different components of IT infrastructure which were directly connected to any abuse (e.g. network devices logs).

Towards the end of activities concerning abuse, handling an overall assessment should be conducted. The facts to be considered are measures undertaken by ISIRT within the layers of process, organization and technology. Such assessment should answer the following questions:

- What (specific) event took place?
- How well did the team and management handle the incidents?
- Were the procedures followed during the handling of abuse?
- Were the procedures adequate to the analyzed situation?
- What should be done differently by the team and management next time a similar situation occurs?
- What action could prevent similar incidents from reoccurring?
- What additional tools and resources are necessary to detect, analyze and handle abuse events in the future?

An evaluation of conducted activities provides the team with lessons learned and enables to enhance the process of detecting and reacting to abuse. Furthermore, it is very helpful when preparing the final report, covering all actions taken previously (in Use and Reaction stages).

The final report should describe in detail:

- information about the abuse (including the specific IT systems associated with the abuse, users connected with the abuse, etc.),
- measures taken by ISIRT,
- seized evidence material,
- conclusions and recommendations.

The last step of this stage is archiving all information gathered, as well as all the evidence materials seized during individual steps of Use and Review stages. This should be done in a manner which makes it impossible for unauthorized personnel to access the data.

3.4. Improvements

The Improvements stage, similarly to the ISO model, focuses on the implementation of prevention, detection and correction mechanisms in the IT environment of the organization. It also concentrates on implementing enhancements to the general process of detection and reaction to IT systems abuse in all layers (process layer, organization layer and technology layer).

These actions aim at both minimizing the possibility of reoccurrence of similar incidents in the future and providing the most effective reaction to a detected abuse. Conducting an update of the existing risk analysis concerning IT systems, in accordance with the approved methodology, should be a support measure for such actions.

4. From theoretical model to practical implementation

Shortly after development of the original version of the described approach, authors of this paper started to assist large Polish financial institution[2] in implementing this incident handling model into the organization. The project's goals were to systematize activities included in the incident handling process, define and assign responsibilities related to it, allow for appropriate control over the activities and provide means of measurement and accountability of the process. Implementation of the model took 9 months and has been completed over one year ago, since when the approach is effectively and efficiently supporting the financial institution in the incident handling activities. The project included assistance in defining the organizational units realizing the process, activities related to it together with their frequencies and minimal inaccessibility time, development of internal procedures and guidelines, assessment of risks, setting the process's controls and measures, assigning support systems to the process and defining its relation to other processes.

Original form of the approach was a result of in-depth analysis of both strengths and weaknesses of the existing incident handling models (described in Section 2) and organizations needs regarding incident handling. Initially, however, it did not put that much emphasis on the publishing sub-phase, treating it only as one-directional source of information – from the process, to its stakeholders – similarly to the CERT® model's notification sub-phase.

During the model's practical implementation in an actual business organization, it appeared that benefits could be taken if the exchange was bi-directional, parallel acquiring and passing information on the detected abuse from and to the stakeholders. Thus, the model was appropriately modified into its present form, described in this paper.

[2] For the reasons of information classification, the financial institutionss name cannot be publicly disclosed.

5. Summary

The main goal of every approach to the process of detecting and reacting to IT systems abuse is to constitute guidelines which may help properly manage potential security breaches. The economic justification of all undertaken activities is also an important aspect of such processes for every organization. It is also necessary to remember that incident handling models are only a part of enterprise security architecture and – as such – cannot be considered in isolation from other security elements.

As presented in this paper, there are several ways to achieve this goal, and each subsequently developed incident handling model attempts to provide more complex approach. However, it is crucial to choose the one which suits the organization's needs best and to ensure its proper implementation and application.

References

[1] CERT/CC, *CERT/CC: Statistics*. `http://www.cert.org/stats/cert_stats.html`

[2] Department of The Navy, *Computer Incident Response Guidebook, Module 19 – Information Systems Security (Infosec) Program Guidelines*. NAVSO P-5239-19, August 1996

[3] Mukund B.: *Computer Security Incident Handling Step by Step*. Version 1.5, May 1998

[4] NIST National Institute of Standards and Technology. *Special Publication 800-61, Computer Security Incident Handling Guide – Recommendations of the National Institute of Standards and Technology*, January 2004

[5] Killcrece G., Kossakowski K.P., Ruefle R., Zajicek M.: *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon University Software Engineering Institute, Pittsburgh, PA 15213-3890, December 2003

[6] Alberts C., Dorofee A., Killcrece G., Ruefle R., Zajicek M.: *Defining Incident Management Processes for CSIRTs: A Work in Progress*. Carnegie Mellon University Software Engineering Institute, Pittsburgh, PA 15213-3890, October 2004

[7] Rezmierski V., Carroll A., Hine J.: *Incident Cost Analysis and Modeling Project*. The University of Michigan, 2000

[8] Ryba M: *Oparta na koncepcji rywalizacji metoda analizy ryzyka systemów informatycznych*. Computer Science, UWND AGH, Kraków, 2004

[9] Ryba M., Sulwiński J.: *A systematic approach to the process of detecting and reacting to IT systems abuse*. IV Międzynarodowy Kongres Audytu, Kontroli Wewnętrznej i Procedur Wykrywania oraz Zapobiegania Oszustwom Gospodarczym – conference papers, Kraków, 16–17 June 2005