Chemical Technology, Control and Management

Volume 2021 | Issue 3 Article 9

6-28-2021

IDENTIFICATION OF KEY PERSONS IN THE INFORMATION SECURITY INCIDENT MANAGEMENT PROCESS AND DISTRIBUTION OF ROLES BETWEEN THEM

Fayzullajon Bakhtiyorovich Botirov
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi Address: 108, Amir Temur st., 100068, Tashkent city, Republic of Uzbekistan E-mail: botirov_fz@mail.ru, Phone: +998-97-751-16-97;, botirov_fz@mail.ru

Sharifjon Rakhimovich Gafurov
Center of Cybersecurity State Unitary Enterprise, Address:10a, Kirk kiz st., Tashkent city, Republic of Uzbekistan E-mail: sh.gafurov@tace.uz, Phone: +998-71-203-55-11;, sh.gafurov@tace.uz

Azam Anvorovich Gafurov
Center of Cybersecurity State Unitary Enterprise, Address:10a, Kirk kiz st., Tashkent city, Republic of Uzbekistan E-mail: a .gafurov @ tace.uz, Phone: +998-71-203-00-23., a.gafurov@tace.uz

Recommended Citation

Botirov, Fayzullajon Bakhtiyorovich; Gafurov, Sharifjon Rakhimovich; and Gafurov, Azam Anvorovich (2021) "IDENTIFICATION OF KEY PERSONS IN THE INFORMATION SECURITY INCIDENT MANAGEMENT PROCESS AND DISTRIBUTION OF ROLES BETWEEN THEM," *Chemical Technology, Control and Management*: Vol. 2021 : Iss. 3 , Article 9.
DOI: https://doi.org/10.51346/tstu-02.21.3-77-0023
Available at: https://uzjournals.edu.uz/ijctcm/vol2021/iss3/9

IDENTIFICATION OF KEY PERSONS IN THE INFORMATION SECURITY INCIDENT MANAGEMENT PROCESS AND DISTRIBUTION OF ROLES BETWEEN THEM

Erratum

there was a small change

ISSN 1815-4840, E-ISSN 2181-1105
Himičeskaâ tehnologiâ. Kontrol′ i upravlenie
CHEMICAL TECHNOLOGY. CONTROL AND MANAGEMENT
2021, №3 (99) pp.72-77. https://doi.org/10.51346/tstu-02.21.3-77-0023
International scientific and technical journal
journal homepage: https://uzjournals.edu.uz/ijctcm/
Since 2005

UDC 004.056

IDENTIFICATION OF KEY PERSONS IN THE INFORMATION SECURITY INCIDENT MANAGEMENT PROCESS AND DISTRIBUTION OF ROLES BETWEEN THEM

Botirov Fayzullajon Bakhtiyorovich[1], Gafurov Sharifjon Rakhimovich[2], Gafurov Azam Anvorovich[3]

[1]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Address: 108, Amir Temur st., 100068, Tashkent city, Republic of Uzbekistan
E-mail: botirov_fz@mail.ru, Phone: +998-97-751-16-97;
[2]Center of Cybersecurity State Unitary Enterprise, Address:10a, Kirk kiz st., Tashkent city, Republic of Uzbekistan
E-mail: sh.gafurov@tace.uz, Phone: +998-71-203-55-11;
[3]Center of Cybersecurity State Unitary Enterprise, Address:10a, Kirk kiz st., Tashkent city, Republic of Uzbekistan
E-mail: a .gafurov @ tace.uz, Phone: +998-71-203-00-23.

Abstract: *This research paper is devoted to the process of information security incident management and the distribution of the roles of key persons in this process. The skills required for members of the information security incident response team are considered, positions and responsibilities are given - typical positions that exist in each organization, testing and improvement procedures are given, the role of the information security incident response team members and employee positions is shown. The quality of the group leader is reflected; responsible for personnel management, scoping and reporting on the state of the organization at a higher level of the hierarchy.*

Keywords*: information security incident response teams, information security, incident management, Incident Response Team.*

Аннотация: *Иш ахборот хавфсизлиги ҳодисаларини бошқариш жараёни ва ушбу жараёнда муҳим ролларрнинг тақсимотига бағишланган. Ахборот хавфсизлиги ҳодисаларига жавоб қайтариш гуруҳи аъзолари учун зарур бўлган кўникмалар, лавозим ва мажбуриятлар келтирилган – ҳар бир ташкилотда мавжуд бўлган лавозимлар, синаш ва такомиллаштириш процедуралари келтирилган бўлиб, ахборот хавфсизлиги ҳодисаларига жавоб қайтариш гуруҳи иштирокчиларининг роли ва ходимларнинг лавозимлари кўрсатилган. Ходимларни бошқаришга, соҳани аниқлаш ва иерархиянинг юқори даражадаги ташкилотга ҳисобот бериш учун масъул гуруҳ раҳбарининг сифатлари кўрсатилган.*

Таянч сўзлар: *ахборот хавфсизлиги ҳодисаларига жавоб қайтариш гуруҳи, ахборот хавфсизлиги, ҳодисаларни бошқариш, Incident Response Team.*

Аннотация: *Работа посвящена процессу управления инцидентами информационной безопасности и распределения ролей ключевых лиц этого процесса. Рассмотрены навыки, необходимые для членов группы реагирования на инциденты информационной безопасности, приведены должности и обязанности – типичные должности, существующие в каждой организации, приведены процедуры тестирования и улучшения, показана роль участников группы реагирования на инциденты информационной безопасности и должности сотрудников. Отражена качество лидера группы; отвечающего за управление персоналом, определение области и отчетности о состоянии организации более высокого уровня иерархии.*

Ключевые слова: *группы реагирования на инциденты информационной безопасности, информационная безопасность, управление инцидентами, Incident Response Team.*

Introduction

Effective incident response depends on the capabilities and reliability of the Information Security Incident Response Team (ISIRT) staff. ISIRT staff and their capabilities become even more important when their activities include developing information security (IS) incident management

policies, auditing, coordinating with other departments, and advancing technical activities. Skills required for members of the ISIRT may include the following.

1) Personal skills: communication, problem solving, teamwork, time and project management.

2) Technical skills: security principles, risk analysis, threat modeling, vulnerability analysis, log analysis[1-2].

3) Incident Response Skills: Team Policy / Procedure, Communication, Incident Analysis, Recording and Tracking Incident Information.

4) Specialized skills: presentation, leadership, subject matter expertise, programming.

To respond to different types of incidents, ISIRT members must have technical knowledge and skills such as the following:

– current network security issues, including attacks, threats, malware and vulnerabilities;

– security techniques for system administration such as patch management, secure configuration, backup, and disaster recovery;

– cryptography (encryption and hashing algorithms), digital signatures, modern protocols such as SSL / TLS;

– common network protocols such as Ethernet (IEEE 802.3), WiFi (IEEE 802.11), IPv4, IPv6, ICMP, UDP, TCP;

– common network application protocols such as DNS, SMTP, HTTP (S);

– collection of digital evidence, reverse engineering;

– computer science and programming concepts such as entropy, secure development, functional and object-oriented programming, system architecture, and memory structure.

Other specific knowledge and skills should be determined by the responsibilities of the ISIRT and the technology used by the organization. ISIRT members must maintain current knowledge and skills[3-4-5].

After receiving management support, and management realized the need and importance of incident management, it was the turn of identifying key persons in the incident management process and assigning roles to the process participants. Table 1 - Positions and Responsibilities - lists the typical positions that exist in each organization, identifying their roles and responsibilities within the incident management process.

Table 1.

Positions and Responsibilities

№	Position	Role	Responsibilities
1.	Information Security Center	The structure vested with the maximum authority in the field of information security	1. Responsibility for the incident management strategy. 2. Approval of the incident management plan. 3. Reconciliation of exceptions and deviations. 4. Making final decisions.
2.	Information Security Manager	Incident Management Team Leader and Information Security Committee Liaison	1. Development, implementation of incident management plans. 2. Effective risk and incident management. 3. Carries out proactive and proactive measures to control the level of information risk.
3.	Incident response manager (often an information security manager)	Incident Response Team Leader	1. Incident Response Leadership. 2. Coordination of personnel for effective incident response 3. Responsible for the successful implementation of incident response plans. 4. Presentation of the incident response report to the information security committee.
4.	Member of the provision of the information security incident response team (ISIRT)	Participation in the work of the group	1. Performs tasks to minimize damage from the incident. 2. Documents the steps taken in the incident response process. 3. Maintains the chain of evidence and oversees the incident handling process in the event of litigation. 4. Incident response report writing.

1	*2*	*3*	*4*
5.	Investigator	Member of ISIRT	1. Investigates the incident. 2. Finds the cause of the incident. 3. Prepares an investigation report.
6.	IT Security Specialist	ISIRT member, independent information security expert	1. Performs a comprehensive analysis of an incident from an IT security perspective 2. Performs auditing and self-assessment as a proactive measure and part of the vulnerability management process.
7.	Heads of business units	Owners of business processes, assets, information systems	1. Make decisions regarding processes / resources / systems in the event of an incident based on the recommendations of the ISIRT 2. They conduct an initial assessment of the impact of threats on business processes and determine the priority of restoring their assets.
8.	IT-specialist	IT employee	1. Provides assistance to the ISIRT in the process of resolving the incident. 2. Maintains company information systems in accordance with accepted policies and regulations.
9.	Lawyer	Legal Officer	Provides assistance with incident management / response / investigation as required.
10.	Employee personnel service	HR Specialist	1. Provides assistance in managing / responding / investigating an incident when an employee is suspected of implementing it. 2. Incorporates into the personnel management policy aspects related to incident management (sanctions for employees suspected of violating policies or involved in an incident).
11.	Press secretary	Specialist in working with the media (media) and the public	Provides prepared and necessary information about the incident to shareholders, the media and others in order to preserve the company's reputation and preserve the brand.
12.	Risk Analyst	An employee of the information security service, internal control or risk management	1. Works closely with business leaders and organizational leaders to identify and manage risks. 2. Provides baseline data, risk management strategy.

After we have identified all the key roles, their functions, the order of escalation and interaction, it is time to formalize and document the incident management process[6-7-8].

Like any process, incident management should be cyclical, constantly improving (Figure 1).

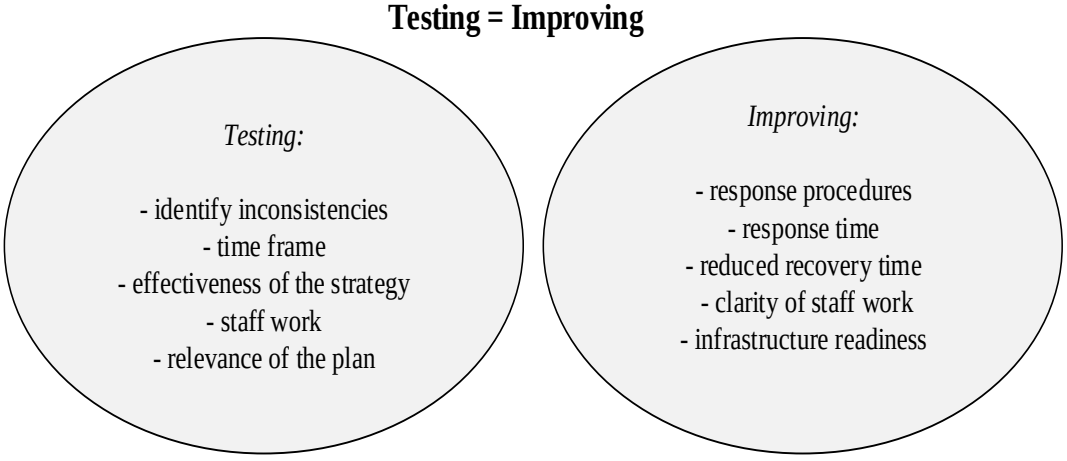

Fig.1. ***Testing and improving.***

For the organization of the ISIRT, the roles of the participants can be defined as shown in Table 1. Some of these tasks may be shared or performed by other organizational units outside the ISIRT. The ISIRT can provide information, but not have final authority. An example of the roles and tasks of ISIRT employees:

IRTM (Incident Response Team - manager) - the role of the group leader; responsible for personnel management, scoping and status reporting in the higher-level organization.

Planning- Responsible for managing the ISIRT. It sets or plans various security policies, communicates them to higher-level authorities, collaborates with third parties, and registers and approves vulnerability reports. His roles are as follows:

- creation and planning of security policies;
- implementation of security processes;
- adjustment of risk priorities;
- communication with parent organizations and other third parties;
- administration support;
- discussion / registration / approval of vulnerability reports in target organizations;
- performing other activities under the direction of the IRTM.

Monitoring employee (Monitoring)- responsible for real-time monitoring and actual operations such as monitoring / detecting / identifying security events, incident logging and prevention. It performs real-time security monitoring and does the following:

- monitoring and operation 24 x 365 h;
- intrusion detection, incident logging and first responses;
- performing security patches and updates;
- security policy implementation and backup management;
- help desk;
- facility management;
- performing other activities under the direction of the IRTM.

Responder *(Response)* - Manages the case from monitoring agents for intrusion incidents, intrusion, theft, deletion or disclosure incidents, performs additional secondary analysis and actions, including investigation, performs recovery actions, and establishes an adequate strategy. Services such as live responses, technical support, and the following are also provided:

- dissemination and reporting of incidents;
- correlation analysis between monitoring systems;
- support the investigation and recovery of the incident;
- analysis of the vulnerability of the target organization and the ISIRT;
- performing other activities under the direction of the IRTM[9].

Incident Analysis Officer *(Analysis)* - In collaboration with the response team, it conducts in-depth analysis, including incident correlation analysis. Analysis of incidents and the following are also provided:

- planning a vulnerability analysis for the target organization and the ISIRT;
- improving security analysis tools and checklist;
- improvement of monitoring rules;
- publication of a newsletter;
- performing other activities under the direction of the IRTM.

Table 2 provides an example of the types of staff, range of positions, and tasks for the various positions that may be required for an ISIRT [10].

Table 2.

Approximate positions of IRT employees

Employee's position	Tasks
Team Leader or Leader	– provides strategic direction – allows and facilitates the work of team members – leads the team – presents ISIRT to management and others – interviews and hires new team members
Assistant managers, supervisors or group leaders	– supports the strategic direction of the assigned functional area – supports team leadership as needed – provides guidance and mentoring for team members – assigns tasks and responsibilities – participates in interviews with new team members
Help desk or sorting staff	– handle the main numbers of the ISIRT for reporting incidents or security – provide initial assistance, depending on skills – conduct initial data entry and sort and prioritize incoming information
Incident Handlers	– analyze incidents, track, record and respond – coordinate responsive and proactive guidance to constituencies (develop materials such as documentation, checklists, best practices and guidelines) – disseminate information – liaise with ISIRT, external experts and others (such as websites, media, law enforcement or legal personnel), as appropriate, on behalf of the team leader or other management personnel. – carry out technology surveillance activities, if assigned – develop appropriate training materials (for ISIRT staff and / or voters) – mentor new ISIRT staff as appointed – monitor intrusion detection systems, if this service is part of the IRIB's activities – perform penetration testing if this service is part of the ISIRT's activities – participate in interviews with new hires as directed
Vulnerability handlers	– analyze, test, track and record vulnerability reports and vulnerability artifacts – research or develop patches and fixes as part of a vulnerability response effort – interact with constituencies, ISIRT, application developers, external experts (other ISIRT, researchers, suppliers) and others (media, law enforcement or legal entities), as needed – distribute information about vulnerabilities and related fixes, patches or workarounds – carry out technology surveillance activities, if assigned – mentor new ISIRT staff as appointed – participate in interviews with new employees of ISIRT
Technical Writers	– provide assistance and assistance to ISIRT in the development of publications such as guidelines, best practices or technical advice

Conclusion

In conclusion, an effective response to incidents depends on the capabilities and reliability of the employees of the information security incident response team. when the activity involves developing an information security incident management (IS) policy, auditing, coordinating with other departments, and promoting technical activities, then the information security incident response team members should have high-level skills. The knowledge of information security personnel is the key to a successful analysis and conclusion of the causes of the incident.

References:

1. T.F.Bekmuratov, “Konsepsiya i zadachi postroyeniya intellektualnix sistem informatsionnoy bezopasnosti” [The concept and tasks of building an intelligent information security system], *Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari: Respublika miqyosidagi ilmiy-texnik konferensiya*, Toshkent, 2018, pp. 4-8. (in Russian).
2. ISO/IEC 27001 Information security management system. Requirements.
3. S.A.Konovalenko, I.D.Korolev, “Identification of vulnerabilities of information systems”, *Innovations in Science*, no. 9 (58), pp. 12–20, 2016.

4. T.F.Bekmuratov, F.B.Botirov, “Axborotni himoyalash tizimini boshqarish masalasi”, *Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi muammolari Respublika ilmiy-texnik konferensiyasi*, Toshkent, 2019, pp. 151-155.
5. A.A.Kizdermishov, S.X.Kizdermishova, “K voprosu o vvode v ekspluatatsiyu DLP-sistem” [On the question of the method of operation of the DLP system], *Vestnik Adigeyskogo gosudarstvennogo universiteta*, *Seriya 4: Yestestvenno-matematicheskiye i texnicheskiye nauki*, no. 3 (206), pp. 128–133, 2017. (in Russian).
6. T.F.Bekmuratov, F.B.Botirov, “Development of structures of intellectual information protection system”, *Chemical technology. control and management*, no. 6(90), pp. 63-71, 2019.
7. K.V.Petuxov, Y.V.Strigunov, S.Ye.Denisenko, *Metodi otsenki nadejnosti lokalnix vichislitelnix setey. Razrabotka proyekta lokalnoy vichislitelnoy seti [A method for evaluating the reliability of local computer networks. Development of a local computer network project]*. Temryuk, 2017, 86 p. (in Russian).
8. S.Herbert, “Why IIoT should make businesses rethink security”, *Network Security*, vol. 2019, Issue 7, July 2019, pp. 9-11.
9. NIST SP 800-61 Computer security incident handling guide.
10. V.I.Popov, I.D.Korolev, V.A.Larionov, “Analysis of the problems of information management and security events in information systems”, *Innovations in Science*, no. 12 (88), pp. 19–26, 2018.