DOI: https://doi.org/10.30837/csitic52021232206

Evaluation and Decision-Making System as Vulnerability Management Process in Information and Telecommunication Systems

Vadym Poddubnyi [1]
Roman Gvozdov[2]
Oleksandr Sievierinov[3]
Vitalii Martovytskyi[4]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, e-mail: vadym.poddubnyi@nure.ua
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, e-mail: roman.hvozdov@nure.ua
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, e-mail: oleksandr.sievierinov@nure.ua
[4]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, e-mail: vitalii.martovytskyi @nure.ua

Abstract. *This article proposes a system for risk assessment and management of software vulnerabilities. Such a system should function as part of the security policy of information security management systems.*

Keywords: *CVSS, risk management, ISMS, vulnerabilities, risks.*

I. Introduction

Protection of information in information and telecommunication systems (ITS) during their operation requires not only compliance with security policies, organizational measures or maintenance of security, but also effective management, monitoring, control and assessment of information security risks. One of the components of effective information security management in ITS is the correct response to vulnerabilities. The existing vulnerability does not cause harm in itself, as it is necessary to have a threat that will take advantage of it. A vulnerability that does not cause a relevant threat may not require the implementation of controls, but must be identified and monitored for measurements. This paper presents a system for assessing and making decisions that should improve vulnerability management processes.

II. Risk Management

Vulnerability management is an organizational process that exists as part of information security and the process of controlling information security incidents. Vulnerability management can be an integral part of the information security management system (ISMS) or complex information protection system (CIPS). Creating clear rules, instructions, actions for the processes of detection, response and elimination vulnerabilities is the main tasks of risk management [1].

III. Vulnerability Assessment and Decision-Making System. General Description

We propose the following model of the evaluation and decision-making system: a description of the criticality of resources in numerical representation comes to the input (such indicators are formed in advance during the creation of ITS security policy) and specific vulnerability assessments from vulnerability scanners. These data are overlaid on the description of the system to determine the impact of vulnerabilities on specific components, the relationships between components and the system as a whole [2]. After that, the obtained qualitative impact assessment provides an indicator for risk assessment and choice of specific actions. Different indicators will have different methods for correcting or accepting a vulnerability if it is not critical or does not affect the operation of the system.

To assess vulnerabilities, it is proposed to use CVSS, which provides a qualitative score and impact vector that can be used in the implementation of vulnerability management system [3]. This vector provides information about the impact on privacy, integrity, availability, attack vector, availability of fixes, availability of software implementation of the exploit, and so on. The security policy in this case will set only the actions that need to be performed for a specific value of risk.

Rules for responding to a specific assessment should be established in advance, agreed with management and administrators. From the set of rules, the best option for action is selected based on a qualitative impact assessment. The administrator then takes the necessary action to eliminate or accept the risk associated with the vulnerability.

In this system, the risk assessment stage is completely removed from the administrator, which means the ability to automate the process of controlling vulnerabilities, eliminating the subjectivity of the danger, the unambiguity of the results.

The main stages of this system:

1) Creating a description of ITS
2) Development of a security policy or its modernization
3) Combining the description of ITS with security policy;
4) Division of responsibilities and creation of instructions for action;
5) Commissioning and modernization

IV. Description of ITS According to the Risk Assessment and Decision-Making System

UML classes are used as ITS objects [4]. Software attributes (OS, browser, etc.) are used as attributes, and software name and version are used as attribute values.

Operations describe the processes that take place on the object, as parameters process flows (for example: Working with a browser (Search pages, Download files)).

That is, an object is a separate ITS module, an attribute is a characteristic of an object, an operation is a process that takes place on an object.

Degrees of interaction with other components are set for attributes and operations.

Different levels of ITS detail are allowed, the level of detail depends on the developer. However, the following requirements must be met and displayed:

– all system components;

– installed software, the functions of which are used in ITS (it is allowed to skip the standard OS software);

– hardware description;

– levels of virtualization;

– basic processes on objects;

– information flows between objects.

This scheme will provide a better understanding of the interrelationships of the processes and visually display the entry points of the vulnerabilities.

V. Security Policy

Before using the risk assessment and decision-making system in ITS, an information security policy must be established according to the law. In addition, as part of such a policy, a criticality assessment of each ITS asset should be performed.

Due to the variety of assets found in most organizations, it is likely that some assets with known monetary value will be valued in local currency units, while others have a higher value that can be assigned a value that varies, for example, in ranges from "very low" to "very high". Deciding which scale to use, quantitative or qualitative, is in fact a matter of the organisation's advantage, but it should be relevant to the assets being valued..

Both types of valuation can be used for the same asset.

The decision on what to consider minor or serious consequences depends entirely on the organization. The consequences, catastrophic for a small organization, can be insignificant or even negligible for a very large organization [5] [6].

It is necessary to rank each component according to its criticality.

I. COMBINING ITS DESCRIPTION WITH SECURITY POLICY AND SCORE CALCULATION

After valuing the assets, each system object must have a confidentiality / integrity / availability assessment (hereinafter - C / I / A), which must be included in the UML chart.

After adding each estimate for each object, it is necessary to calculate each vulnerability according to rule (1):

$$Inf_g = S_{cvss} * R_c * V_c + S_{cvss} * R_i * V_i + S_{cvss} * R_a * V_a , \quad (1)$$

where Inf_g – overall impact score; S_{cvss} – vulnerability assessment according to CVSS; R_c – resource confidentiality score; V_c – the impact of vulnerability on confidentiality; R_i – resource integrity score; V_i – the coefficient of the impact of vulnerability on integrity; R_a – resource availability score; V_a – the coefficient of the impact of vulnerability to availability.

The impact coefficient of the vulnerability V_c, V_i, V_a is determined from the vulnerability vector and is 0 for the value of None, 0.5 for Low, 1 for High.

If the confidentiality or availability of the vulnerability is high (High), the C / I scores are increased to half the maximum value (rounding goes to the larger side). That is, if C / I / A is 1/1/5, then for vulnerabilities with a high impact on privacy, the parameters of C / I / A are calculated as 3/1/5.

However, this assessment will be the impact of the ITS component on the system as a whole.

To understand the situation for a particular object, for each object it is necessary to figure out a relative estimate of the resource by formula (2):

$$Inf_r = Inf_g * \ (10 / (10 \ * R_c \ * V_c + \ 10 \ * R_i \ * V_i + 10 \ * R_a \ * V_a)) \ (2)$$

This rating is in the range of 0 to 10.

The division into general and relative evaluation is necessary for better ranking of priorities. It gives a better understanding of criticality of the vulnerability on particular component or system, which component needs to be prioritized, and so on. First of all, you should perform actions on the component that has a higher score. If the vulnerabilities have the same score, you should choose the vulnerability of the object that has more dependencies and relationships.

Thus, the absolute score is used to determine the order of correction of components, and the relative score for actions to correct an individual object.

VI. Division of Responsibilities and Creation of Instructions for Action

Before using the system, the organization must share responsibilities for control, action and response. It is recommended to create such roles as: Security Administrator - the person responsible for the implementation of security policies and vulnerability management. System administrator - a person who is responsible for setting up vulnerability scanners and scheduling scans, making fixes.

VII. Commissioning and Modernization

After performing all the actions, the system can be put into operation. It is recommended to use the NVD vulnerability database during operation. During system operation, it is forbidden to change the vulnerability database to another due to CVSS vulnerability scores may differ.

The system should be reviewed once a year or in the following cases:

- when changing the structure of ITS;
- when revaluation of assets;
- after incidents as a learning process;
- at the request of the security administrator;
- at the request of management.

Management of the organization must re-agree the upgraded system.

VIII. Conclusion

This paper proposed a system for assessing and making decisions that should improve the process of managing vulnerabilities in ITS. Structure, use of formalized description, assessment of information properties and vulnerabilities, prioritization of actions in ITS and in a separate component of ITS are key features of such system.

Such a system of assessment and decision-making should regulate and establish the procedure for vulnerability management, actions in the system should be performed in stages.

REFERENCES

[1] Поддубний В. О., Сєвєрінов О. В., Менеджмент вразливостей як складова частина системи управління інформаційної безпеки : НТУ «ХПІ», 2020.

[2] Поддубний В.О., Сєвєрінов О.В., Менеджмент вразливостей з використанням формалізованого опису// Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Vol. 203. pp. 72 – 77.

[3] Common Vulnerabilities and Exposures https://cve.mitre.org

[4] Р.Ю. Гвоздьов, Р.В. Олійников, Метод і методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах// Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Vol. 203. pp. 91-96

[5] ISO/IEC 27005 Information technology — Security techniques — Information security risk management, 2018.

[6] ISO/IEC 27035 Information technology — Security techniques — Information security incident management.