https://www.proconference.org/index.php/usc/article/view/usc24-00-009
DOI: 10.30888/2709-2267.2024-20-00-009

УДК 004.056.5

REQUIREMENTS FOR SECURING COMPANY NETWORK INFRASTRUCTURE

ВИМОГИ ДО ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ КОМПАНІЇ

Korobeinikova T.I. / Коробейнікова Т.І.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0003-2487-8742
Kishchak M.M. / Кіщак М.М.
студентка / student
Luzhetska N.M. /Лужецька Н.М.
assistant / асистент
ORCID: 0000-0002-5449-5825
Lviv Polytechnik National University, S.Bandera St. 12, Lviv, 79013
Національний університет "Львівська політехніка", Львів, Бандери, 12. 79013.

Анотація. *В роботі розглядається процес управління ризиками та безпекою інформації в організації. Він включає ідентифікацію та класифікацію активів, оцінку потенційних загроз та вразливостей, оцінку наслідків та ймовірності ризиків, розробку стратегії мінімізації ризиків, моніторинг та аналіз, адаптацію та вдосконалення в мережевій безпеці, а також документування та написання звітів. Кожен етап детально розглядається, з акцентом на його значення для забезпечення безпеки інформації та стійкості бізнесу.*

Ключові слова: *ризики мережевої безпеки, загрози безпеці, вразливості, активи, інформаційна безпека.*

Abstract. *The paper examines a process for managing risks and information security in an organization. It includes the identification and classification of assets, assessment of potential threats and vulnerabilities, evaluation of the consequences and likelihood of risks, development of risk mitigation strategies, monitoring and analysis, adaptation and improvement in network security, as well as documentation and reporting. Each step is examined in detail, with an emphasis on its importance for ensuring information security and business resilience.*

Key words: *network security risks, security threats, vulnerabilities, assets, information security.*

Вступ.

У сучасному світі, де інформація стає все більш цінним активом, питання її захисту набуває особливої актуальності [1]. Компанії по всьому світу використовують різноманітні стратегії та методики для забезпечення безпеки своїх даних та ресурсів [2-4]. Одним з таких підходів є систематичний процес управління ризиками [4-6], який включає в себе ряд послідовних етапів. Цей текст розглядає дев’ять ключових етапів цього процесу, починаючи від ідентифікації активів і закінчуючи документуванням та звітністю. Кожен з цих етапів має свою важливість та специфіку, і разом вони створюють цілісну

систему управління ризиками, яка допомагає організаціям ефективно захищати свої інформаційні активи.

Таким чином, виникає потреба у формуванні конкретних етапів для вирішення задач захисту мережевої інфраструктури компанії.

Вимоги до етапів вирішення задачі захисту мережевої інфраструктури компанії.

Першим етапом пропонується ідентифікувати активи. Це усі матеріальні та нематеріальні ресурси, які має організація та які мають значення для її функціонування та досягнення цілей. Це можуть бути інформація, ПЗ, обладнання, інтелектуальна власність, фінансові ресурси, клієнтська БД тощо. Гарним тоном було б після ідентифікації активів – виконати їх класифікацію. Класифікація допомагає компанії визначити, які активи потребують найбільшого захисту, і які можуть бути менш критичними. Для цього активи можна класифікувати за критеріями, такими як їхня важливість для бізнесу, рівень конфіденційності, цілісності та доступності інформації, а також ступінь потенційного впливу в разі компрометації. Класифікація активів дозволяє раціонально розподілити ресурси для захисту, зосереджуючи увагу на найбільш критичних елементах інфраструктури та даних.

Другим етапом потрібно оцінити потенційні загрози. Цей етап допомагає зрозуміти, які ризики можуть вплинути на діяльність та як їх можна запобігти або пом'якшити. Потенційні загрози можуть бути різноманітними, включаючи кібератаки, витоки інформації, природні катастрофи, людський фактор, технічні вади тощо. Ці загрози можуть призвести до різних негативних наслідків, таких як втрата конфіденційності чи цілісності даних, збитки для репутації організації, фінансові втрати, перерви у роботі бізнесу та інші. Ідентифікація та оцінка цих загроз дозволяє підготуватися до можливих сценаріїв та розробити стратегії захисту, щоб зменшити можливі ризики та зберегти стійкість бізнесу.

Далі пропонується виявляти вразливості. Звісно що у кожній компанії вони можуть бути різні, проте цей підхід має бути комплексним та унікальним, і враховувати всі особливості компанії. Цей процес передбачає виявлення

слабких місць у захисті, які можуть бути використані для незаконного доступу, крадіжки даних або зупинки роботи систем. Виявлення вразливостей допомагає компаніям приймати вчасні заходи для виправлення проблем та запобігання можливим атакам або інцидентам.

Обов'язково необхідно оцінювати наслідки ризиків: чи приймаємо їх, чи уникаємо. Коли компанія приймає ризик, вона свідомо визнає і приймає можливі наслідки інциденту або події. Це може бути доцільно, якщо вартість управління ризиком перевищує можливі збитки від виникнення інциденту. З іншого боку, уникнення ризику передбачає вжиття заходів для зменшення або усунення можливості виникнення негативних наслідків. Це може включати припинення певних дій або встановлення заходів безпеки для запобігання ризикованим ситуаціям. Обидва підходи мають свої переваги та недоліки, і вибір між ними залежить від унікальних обставин та цілей організації.

Також пропонується оцінювати ймовірності ризику. Цей процес відбувається через комплексний аналіз, який передбачає ідентифікацію загроз та оцінку вразливостей. Після ідентифікації потенційних загроз аналізується, наскільки вразливі організаційні ресурси перед цими загрозами. Оцінка проводиться з урахуванням різних факторів, таких як ступінь захищеності систем, сильні та слабкі сторони захисту, історія попередніх інцидентів та інші контекстуальні аспекти. На основі цієї інформації приймаються рішення про те, які ризики є найбільш ймовірними та як їм краще керувати. Це допомагає приймати обґрунтовані рішення щодо призначення пріоритетів у впровадженні заходів з мінімізації ризиків, а також у розробці ефективних стратегій управління цими ризиками.

Наступним етапом пропонується розробити стратегію мінімізації ризиків. Він дозволяє компанії ефективно управляти і зменшувати ризики, які виникають внаслідок потенційних загроз. Шляхом розробки ефективних стратегій мінімізації ризику організація може зменшити вплив потенційних загроз на свою діяльність, забезпечити безпеку своїх даних та ресурсів, а також зберегти довіру клієнтів та партнерів. Такий підхід сприяє стійкому розвитку

організації та забезпечує її успішну діяльність в умовах постійно змінюючогося інформаційного середовища.

Після цього варто було б провести моніторинг та аналіз. Цей процес забезпечує постійний контроль за станом безпеки інформації та інфраструктури, дозволяючи оперативно виявляти потенційні загрози та вразливості. Моніторинг дозволяє перевіряти ефективність заходів з мінімізації ризиків, вчасно реагувати на нові загрози та зміни у середовищі. Аналіз даних, зібраних під час моніторингу, допомагає розуміти тенденції та патерни ризиків, що дозволяє вдосконалювати стратегії безпеки та управління ризиками. Правильно налаштований процес моніторингу та аналізу дозволяє організації оперативно реагувати на загрози, зменшує ризик виникнення інцидентів та сприяє збереженню стабільності та довіри до діяльності організації.

Передостаннім етапом пропонується адаптація та вдосконалення в мережевій безпеці. Цей процес важливий, оскільки дозволяє компаніям підтримувати адекватний рівень захисту, враховуючи нові тенденції в кіберзлочинності, вразливості програмного забезпечення та зміни внутрішніх потреб інфраструктури. Реалізація цього процесу може включати в себе такі кроки, як постійне оновлення політик безпеки, впровадження нових технологій та застосування сучасних методів виявлення та аналізу загроз. Також важливим аспектом є постійне навчання та підвищення кваліфікації персоналу, щоб вони були в курсі останніх тенденцій та кращих практик у сфері кібербезпеки. Регулярні аудити та тестування безпеки також допомагають виявляти слабкі місця та вдосконалювати заходи захисту.

І на останньому етапі необхідно задокументувати все та написати звіти. Їх важливість полягає в тому, що вони забезпечують прозорість у внутрішніх процесах безпеки, дозволяючи відстежувати та аналізувати діяльність зі збереження безпеки, виявлення і реагування на інциденти, а також впровадження та вдосконалення заходів безпеки. Реалізація цих аспектів містить створення та підтримку системи документування, яка включає політики, процедури, інструкції та інші документи, що регулюють безпеку

інформації. Це допомагає керівництву та зацікавленим сторонам розуміти стан безпеки та приймати обґрунтовані рішення щодо подальших кроків у забезпеченні безпеки інформації.

Висновки.

Отже, пропонуються такі етапи для формування технологічного ланцюжка визначення ризиків мережевої безпеки:

1. Ідентифікація активів: визначення важливих ресурсів організації.
2. Класифікація активів: розуміння цінності та ризику кожного активу.
3. Оцінка потенційних загроз: визначення можливих загроз для діяльності.
4. Виявлення вразливостей: виявлення слабких місць у захисті.
5. Оцінка наслідків ризиків: рішення про прийняття/уникнення ризиків.
6. Оцінка ймовірності ризику: комплексний аналіз загроз та вразливостей.
7. Стратегія мінімізації ризиків: управління та зменшення ризиків.
8. Моніторинг та аналіз: постійний контроль за станом безпеки.
9. Адаптація та вдосконалення: підтримка адекватного рівня захисту.
10. Документування та звітування: прозорість внутрішніх процесів безпеки.

Література:

1. Трояновська Т. І. Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.

2. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

3. Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2021. – 188 с.

4. Комп'ютерні мережі: навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2022. – 228 с.

5. Таченко І. А. Огляд сучасного стану питання в галузі оцінювання ризиків мережевої безпеки / І. А. Таченко, Т. І. Коробейнікова, С. М. Захаченко // Scientific Collection «InterConf», (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021. 478 p. – С. 417-432.

6. T. Korobeinikova, I. Tachenko, R. Chekhmestruk, P. Mykhaylov, O. Romanyuk and S. Romanyuk, "A General Method of Risk Estimation," 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023, pp. 410-413, doi: 10.1109/ACIT58437.2023.10275626.

Науковий керівник: к.т.н., доц. Коробейнікова Т.І.

Стаття надіслана: 16.05.2024 р.