https://www.sworldjournal.com/index.php/swj/article/view/swj25-00-021
DOI: 10.30888/2663-5712.2024-25-00-021

УДК 004.056.5

TECHNOLOGICAL CHAIN OF PROTECTION FOR THE COMPANY'S NETWORK INFRASTRUCTURE

ТЕХНОЛОГІЧНИЙ ЛАНЦЮЖОК 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 методи та засоби визначення ризиків мережевої безпеки, які є сукупністю різноманітних підходів та інструментів, що спрямовані на ідентифікацію потенційних загроз, вразливостей та можливих наслідків для інформаційних систем та мереж. Тут розглянуті основні поняття захисту мережевої інфраструктури, виклики у галузі захисту мережевої інфраструктури. Особливу увагу в розділі приділено формуванню технологічного ланцюжка для вирішення задачі захисту мережевої інфраструктури компанії.*

Ключові слова: *ризики мережевої безпеки, загрози безпеці, вразливості, активи, інформаційна безпека, технологічний ланцюжок захисту мережевої інфраструктури компанії.*

Вступ.

Мережева інфраструктура – це система обладнання, програмного забезпечення, протоколів і зв'язків, які дозволяють комп'ютерам та іншим пристроям зв'язуватися та обмінюватися даними між собою. Це може включати в себе локальні мережі (LAN), розширені корпоративні мережі (WAN), хмарні мережі та інші типи мереж [1-3], що забезпечують зв'язок між різними пристроями та системами. Мережева інфраструктура є основою для забезпечення комунікацій та обміну даними у сучасному світі [4-6].

Отже, існує є потреба у формуванні конкретних технологічних рішень для вирішення задач захисту мережевої інфраструктури компанії.

Об'єкти захисту мережевої інфраструктури.

Мережева інфраструктура складається з різних компонентів, які спільно забезпечують зв'язок між пристроями і обмін даними.

Основними складовими мережевої інфраструктури є: пристрої мережевого з'єднання, мережеві протоколи, кабельна і бездротова інфраструктура, мережеве ПЗ, хмарні сервіси, засоби безпеки мережі (шифрування, мережевих брандмауерів, ідентифікація та аутентифікація користувачів, аудит мережевої активності тощо).

Захист мережевої інфраструктури – це набір заходів та стратегій, спрямованих на забезпечення безпеки комп'ютерних мереж і всіх компонентів,

що в них використовуються [7]. Основні механізми захисту мережевої інфраструктури: аутентифікація; авторизація; конфіденційність; цілісність; доступність; захист від атак; моніторинг та аналіз безпеки; шифрування; резервне копіювання та відновлення.

Ці поняття складають основу для розробки та впровадження стратегій захисту мережевої інфраструктури, спрямованих на забезпечення безпеки та стабільності комп'ютерних мереж. В межах цієї роботи будемо цікавитися пристроями мережевого з'єднання (рис. 1), зокрема маршрутизаторами та мережевим ПЗ які дозволяють захищати мережеву інфраструктуру [8].

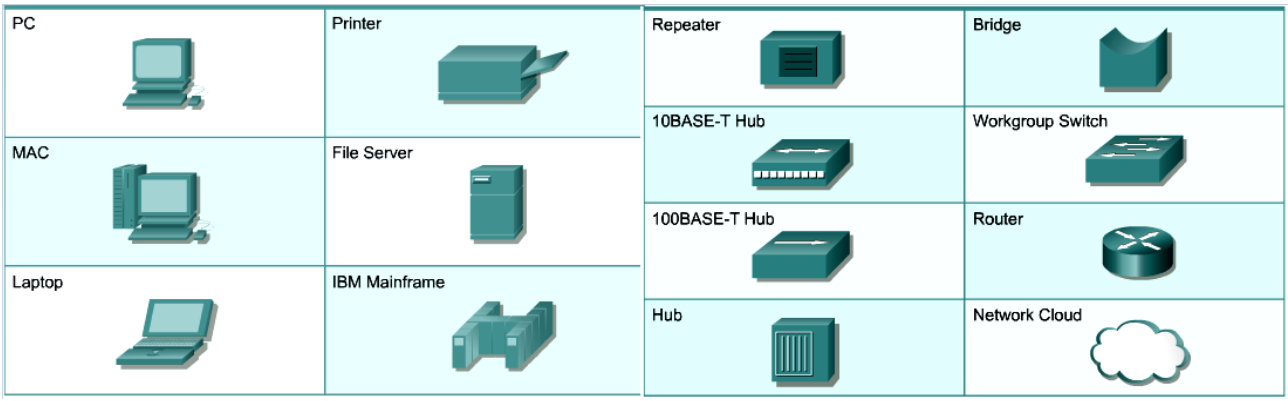

Рисунок 1 - Мережеві пристрої

Джерело [8]

Мережеве програмне забезпечення – це програмне забезпечення, що дозволяє організувати роботу користувача в мережі. Воно представлено загальним, системним і спеціальним програмним забезпеченням.

До системного програмного забезпечення належать: операційна система; сервісні програми; система технічного обслуговування.

Проблеми в галузі захисту мережевої інфраструктури.

Важливість проблематики інформаційної безпеки (ІБ) пояснюється:

– цінністю накопичених інформаційних ресурсів;
– критичною залежністю від інформаційних технологій.

Руйнування важливої інформації, крадіжка конфіденційних даних, перерва в роботі внаслідок відмови – стають великими матеріальними втратами, що завдає збитку в т.ч. і репутації організації. Проблеми з системами управління або медичними системами загрожують здоров'ю і життю людей [9].

Підтвердженням складності проблематики ІБ є рівнобіжний швидкий ріст витрат на захисні заходи і кількості порушень ІБ у поєднанні з ростом середнього збитку від кожного порушення.

Проблема ІБ – не лише є технічна; без законодавчої бази, без постійної уваги керівництва організації і виділення необхідних ресурсів, без заходів управління персоналом і фізичного захисту вирішити її неможливо. Комплексність також ускладнює проблематику ІБ; потрібна взаємодія фахівців з різних областей.

Проблеми в галузі захисту мережевої інфраструктури становлять серйозний виклик для організацій у всіх сферах діяльності, включно з урядовими установами, бізнесами та приватними користувачами. Ось деякі з основних проблем:

– Кібератаки;
– Недостатня обізнаність користувачі;
– Вразливості програмного забезпечення і обладнання;
– Недостатня захист мережевих пристроїв;
– Недостатня захист периметра мережі;
– Недостатнє оновлення систем безпеки;
– Недостатня реакція на інциденти безпеки;
– Недостатня захист від внутрішніх загроз.

Для боротьби з цими проблемами необхідно вживати комплексних заходів, які містять навчання персоналу з кібербезпеки, використання сучасних методів захисту, регулярне оновлення ПЗ та обладнання, а також реалізацію ефективних процедур реагування на інциденти безпеки.

Щоб організувати надійний захист мережі компанії, потрібно правильно визначити її активи.

Активи – це все, що має цінність для організації, наприклад дані та інша інтелектуальна власність, сервери, комп'ютери, смартфони, планшети тощо.

Вразливість – це слабке місце або недолік у системі, програмному забезпеченні або процесі, яке може бути використане зловмисниками для отримання несанкціонованого доступу, завдання шкоди або порушення нормального функціонування системи.

Вразливості можуть бути різного характеру і походити як від технічних проблем у програмному забезпеченні, так і від неправильної конфігурації, недоліків в безпеці мережі чи людських помилок.

У компанії можуть бути різноманітні вразливості, наприклад:

- Вразливості програмного забезпечення;
- Вразливості мережі;
- Вразливості людського фактору;
- Фізичні вразливості.

Компанії можуть мати справу із різними загрозами кібербезпеки, які можуть масштабуватися від простих до складних. Ось кілька основних загроз: віруси, хробаки та троянські програми; фішинг та соціальна інженерія; атаки з використанням відмови в обслуговуванні (DDOS); витік даних; недостатня безпека мережі та систем.

Антропогенні загрози – це загрози, які виникають в результаті дій або неуважності людини. У сфері кібербезпеки антропогенні загрози можуть такими: недбале використання паролів; несанкціоновані дії персоналу; соціальна інженерія; неправильна настройка програм та систем; використання нелицензійного або неофіційного програмного забезпечення.

Вразливість – це слабке місце в системі, яке може бути використано загрозою.

В контексті захисту мережевої інфраструктури компанії, вразливість визначається як потенційна слабкість або недолік у системі, програмному забезпеченні або конфігурації, яка може бути використана для нанесення шкоди або злому безпеки мережі. Це може включати в себе вразливості в програмному забезпеченні, які дозволяють зловмисникам отримувати несанкціонований

доступ до системи або отримувати конфіденційну інформацію, а також слабкі точки в мережевій інфраструктурі, які можуть бути використані для проведення атак на доступ або перешкоджання нормальному функціонуванню мережі. Виявлення, оцінка та виправлення вразливостей є важливими кроками у забезпеченні безпеки мережі компанії [10-11].

Технологічний ланцюжок визначення ризиків мережевої безпеки

Технологічний ланцюжок визначення ризиків мережевої безпеки (рис. 2) – це систематичний процес оцінки та ідентифікації потенційних загроз і вразливостей в інформаційних системах та мережах.

Процес ідентифікації активів.

Активи містять елементи, які можуть бути використані або потенційно загрожувати мережі. Це можуть бути фізичні пристрої (сервери, маршрутизатори, комутатори, комп'ютери), або цифрові активи (ПЗ, дані, логіни та паролі. Після ідентифікації активів важливо класифікувати їх за рівнем важливості та чутливістю. Наприклад, критичні дані, такі як особиста інформація клієнтів або фінансові звіти, можуть бути віднесені до вищого рівня важливості. Крім класифікації за важливістю, активи також можна оцінити за іншими атрибутами, такими як рівень доступності, конфіденційності та цілісності. Наприклад, деякі дані можуть бути доступні лише обмеженій кількості співробітників або можуть потребувати додаткового рівня шифрування.

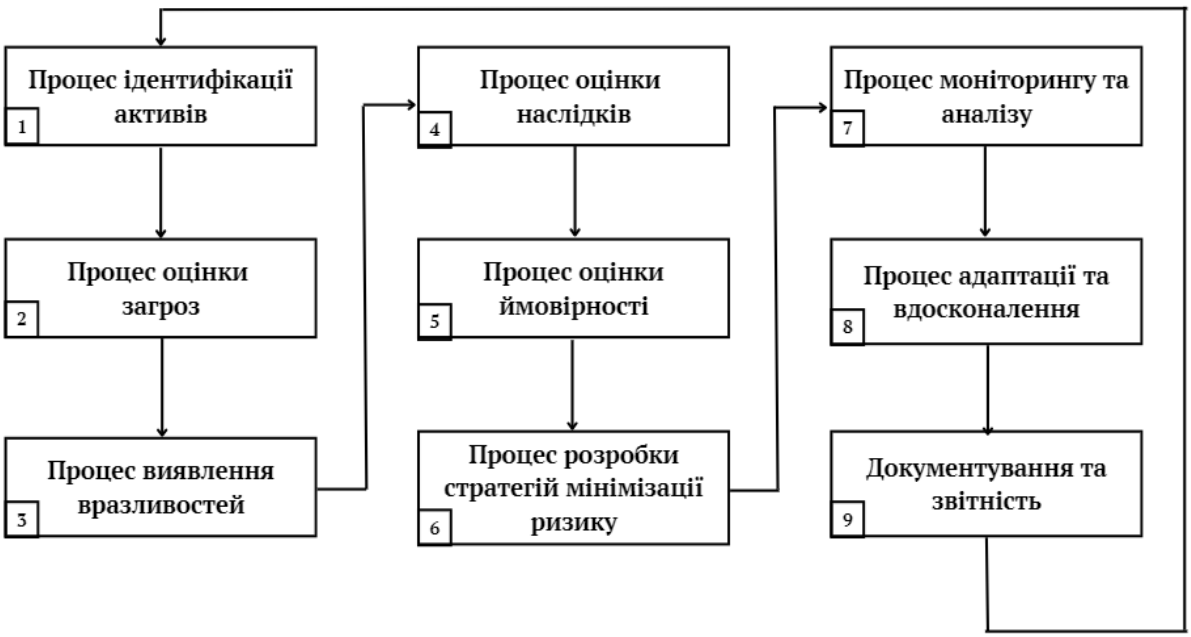

Рисунок 2 - Технологічний ланцюжок визначення ризиків мережевої безпеки

Авторська розробка

Процес оцінки потенційних загроз.

Під час цього етапу проводиться аналіз потенційних загроз, які можуть вплинути на безпеку активів вашої мережі. Перш ніж оцінювати загрози, їх необхідно ідентифікувати. Це може включати в себе різноманітні типи загроз, такі як зловмисне ПЗ (віруси, троянці, хробаки), атаки хакерів, соціальний

інжиніринг, природні катастрофи та інші. Після ідентифікації загроз оцінюється ймовірність того, що кожна загроза може реалізуватися. Це дозволяє визначити, наскільки серйозним може бути вплив кожної загрози на безпеку вашої мережі.

Процес виявлення вразливостей.

Під час цього етапу відбувається аналіз потенційних вразливостей вашої мережі, які можуть бути використані для експлуатації або атаки. Це включає систематичне тестування мережі за допомогою різних інструментів, таких як сканери портів та вразливостей, а також проведення аудиту безпеки для ідентифікації слабких місць та потенційних ризиків.

Процес оцінки наслідків.

Під час цього етапу аналізуються можливі наслідки реалізації виявлених загроз та вразливостей. Це охоплює оцінку впливу на конфіденційність, цілісність та доступність інформації, а також фінансові збитки, втрату репутації, правові наслідки та інші можливі шкоди для організації. Оцінка наслідків допомагає визначити, наскільки серйозними є ризики для бізнесу та які заходи забезпечення слід приймати для їх запобігання або зменшення.

Процес оцінки ймовірності ризиків.

Під час цього етапу аналізується ймовірність того, що потенційна загроза або вразливість буде використана для атаки чи спричинить проблему. Оцінка ймовірності зазвичай базується на історичних даних, статистиці, експертних оцінках та інших джерелах інформації. Вона дозволяє визначити, наскільки ймовірним є виникнення певного інциденту та які заходи забезпечення потрібно вжити для зменшення цієї ймовірності або для підготовки до її можливого виникнення. Результати оцінки ймовірності служать основою для прийняття обґрунтованих рішень щодо управління ризиками та визначення пріоритетів у впровадженні заходів забезпечення мережевої безпеки.

Процес розробки стратегій мінімізації ризику містить комплекс заходів, що спрямовані на запобігання та зменшення можливих загроз. Це охоплює встановлення технічних засобів захисту, таких як брандмауери та антивірусне ПЗ, а також розробку політик безпеки для користувачів та адміністраторів. Навчання персоналу про правила безпеки та проведення регулярних аудитів безпеки є також необхідними. Важливою частиною стратегії є створення резервних копій даних для відновлення інформації у випадку втрати. Постійне вдосконалення стратегій шляхом аналізу інцидентів та адаптації до нових загроз допомагає забезпечити ефективний рівень захисту.

Процес моніторингу та аналізу. Під час цього процесу постійно відслідковується активність в мережі, виявляються аномалії та потенційні загрози, і проводиться їх аналіз для вчасного виявлення та реагування на можливі інциденти безпеки. Моніторинг охоплює такі активності, як перевірка журналів подій, аналіз мережевого трафіку, виявлення спроб несанкціонованого доступу та інші заходи для забезпечення постійного контролю за безпекою мережі. Після збору даних здійснюється їх аналіз для виявлення вразливостей та недоліків, а також для визначення ефективності заходів безпеки. Важливою частиною цього процесу є реагування на виявлені загрози шляхом прийняття відповідних заходів забезпечення та вжиття заходів для запобігання майбутнім інцидентам.

Процес адаптації та вдосконалення в мережевій безпеці – це постійний процес, спрямований на підтримку та підвищення ефективності заходів безпеки відповідно до змін у технологіях, загрозах та вимогах. Містить аналіз інцидентів для виявлення слабких місць та вдосконалення політик безпеки, оновлення технічних засобів захисту, постійне навчання персоналу та реагування на нові загрози шляхом впровадження нових стратегій та заходів захисту.

Документація та звітність становлять важливий аспект управління ризиками та забезпечення ефективності заходів безпеки. Політики безпеки встановлюють стандарти та вимоги для забезпечення конфіденційності, цілісності та доступності інформації, що документуються для внутрішньої згоди та розуміння вимог безпеки в організації. Плани відновлення після інцидентів визначають процедури та кроки для відновлення роботи після кібератак або природних катастроф. Журнали подій використовуються для реєстрації активності в мережі та аналізу аномальної активності. Звіти про аудити та інциденти відображають результати аудитів безпеки, оцінку вразливостей та деталі інцидентів, їх причини та наслідки, що служить основою для контролю та вдосконалення стратегій безпеки.

Висновки.

В даній роботі запропоновано технологічний ланцюжок визначення ризиків мережевої безпеки, який є важливим інструментом для забезпечення безпеки інформаційних систем та мереж. Цей процес охоплює 9 етапів, які містять ідентифікацію активів, оцінку потенційних загроз, виявлення вразливостей, оцінку наслідків і ймовірності ризиків, розробку стратегій мінімізації ризику, моніторинг та аналіз, а також адаптацію та вдосконалення. Кожен з цих етапів важливий для ефективного управління ризиками та забезпечення безпеки мережевих інфраструктур.

Правильна ідентифікація активів та оцінка загроз допомагають визначити заходи безпеки. Моніторинг та аналіз виявляють потенційні загрози в реальному часі, а процес адаптації дозволяє підтримувати високий рівень захисту. Документація та звітність є важливими для управління ризиками та розуміння вимог безпеки.

У цілому, технологічний ланцюжок визначення ризиків мережевої безпеки є необхідним інструментом для забезпечення безпеки інформаційних систем та мереж і допомагає організаціям ефективно управляти ризиками та захищати свої активи та дані.

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. Технології використання мережевих ресурсів для підготовки молоді до дослідницької діяльності : Монографія / О. Ю. Буров, В. В. Камишин, Н. І. Поліхун, А. Т. Ашеров; За ред. О. Ю. Бурова. – К. : ТОВ «Інформаційні системи». – 2012. – 416 с.

6. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

7. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Вид. група BHV, 2009. – 608 с.

8. Тернопільський національний технічний університет ім. І. Пулюя. Лекція 10 Основні мережеві пристрої. [Електронний ресурс] / Тернопільський національний технічний університет ім. І. Пулюя – Режим доступу: https://studfile.net/preview/7825935/page:9/.

9. Почепцов ГГ., Чукут С.А. Інформаційна політика: Навч. посіб. – К.: Знання, 2006. – 663 с.

10. 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.

11. 19. 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.

Abstract. *This paper examines methods and tools for assessing network security risks, which constitute a variety of approaches and instruments aimed at identifying potential threats, vulnerabilities, and possible consequences for information systems and networks. The main concepts of network infrastructure protection, challenges in the field of network infrastructure protection are discussed here. Special attention is paid in the section to the formation of a technological chain for solving the task of protecting the company's network infrastructure.*

Keywords: *network security risks, security threats, vulnerabilities, assets, information security, technological chain of protection for the company's network infrastructure.*

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

Стаття надіслана: 16.05.2024 р.