СЕКЦІЯ XV.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

МЕТОДИ ТА ЗАСОБИ КОМПЛЕКСНОГО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

Чинчик Дмитро Михайлович
студент І курсу магістратури, кафедра безпеки інформаційних технологій
Національний університет «Львівська політехніка», Україна

Коробейнікова Т.І.
кандидат технічних наук, доцент, доцент
кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Україна

1. Вступ

Пошуки найкращих рішень у галузі захисту корпоративних мереж (КМ) активно обговорюються і науковцями і безпосередньо на виробництві [1-6]. Кібератаки призводять до великих втрат: зростання кіберзлочинності зумовило збільшення виділених урядом США коштів на кібербезпеку. В Україні також відбувається постійний приріст кібератак. У зв'язку з цим, наукові задачі аналізу та вдосконалення методів та засобів захисту КМ є актуальними. Комплексний підхід є потужним рішенням під час побудови захисту КМ.

2. Огляд заходів інформаційної безпеки у корпоративних мережах

Заходи інформаційної безпеки містять зокрема: правові, організаційно-адміністративні та інженерно-технічні заходи.

В КМ правові заходи для забезпечення безпеки інформації базуються на міжнародних положеннях (угоди, ліцензії, патенти, авторські права тощо) та національних правових нормах (конституція, укази, нормативні акти, кодекси, інструкції тощо). Ці нормативні акти забезпечують відкритість, доступність, свободу обміну інформації, її достовірність та повноту, гарантують право на інформацію, а також визначають правомірність отримання, використання, поширення та збереження інформації. Крім того, до таких правових заходів відносяться норми, які регулюють відповідальність за кіберзлочини та захист авторських прав розробників програм. Ці правові заходи також призначені для визначення пріоритету міжнародного права над внутрішньодержавним та економічної доцільності.

Організаційно-адміністративні заходи є такими ж важливими, як і правові, у забезпеченні захисту інформації в мережах. Успішність стратегічного планування та правильного визначення методів і механізмів захисту даних корпоративної мережі визначають ефективність захисту. Організаційно-адміністративні заходи також включають планування захисту, керування системою захисту, безперервність процесу захисту інформації, гнучкість захисту, розділення доступу та багаторівневість захисту інформації.

Для ефективного захисту інформації у КМ, також необхідно застосовувати інженерно-технічні заходи. Їх вибір має відповідати потрібному рівню захисту даних

і буде індивідуальним для кожного випадку. Такі інженерно-технічні заходи можуть включати використання шифрів, захист від несанкціонованого доступу, обладнання для захисту від витоку інформації та мережевого обладнання для ефективного розподілу ресурсів у мережі. Крім того, в межах впровадження інженерно-технічних заходів, можуть бути встановлені системи пожежогасіння, контролю та управління доступом, резервного електроживлення та інші пристрої [7-8].

3. Огляд засобів захисту корпоративних мереж

Інженерно-технічні заходи забезпечення безпеки інформації у КМ за їх функціональним призначенням можна поділити на такі групи:

- фізичні засоби – засоби, які повинні створювати фізичні перешкоди на шляху зловмисників;
- апаратні засоби – різні технічні конструкції, які можуть протидіяти розголошенню відповідної інформації корпоративної мережі, її витоку та спробам несанкціонованого доступу до неї;
- програмні засоби – програми чи програмні комплекси, що можуть забезпечити захист інформації самостійно чи разом з іншими засобами захисту інформації корпоративної мережі;
- криптографічні засоби – алгоритми, за допомогою яких шифрується інформація корпоративної мережі, яка захищається [5].

Фізичні засоби захисту корпоративних мереж. Основним принципом фізичного захисту є його неперервність. Потрібно вживати всіх можливих заходів, щоб убезпечити будівлі, прилеглу територію, підтримуючу інфраструктуру, обчислювальну техніку та носії даних від ймовірних загроз. До фізичного захисту належать: фізичне керування доступом; захист підтримуючої інфраструктури; захист від перехоплення даних; захист мобільних систем [5].

Апаратні засоби захисту корпоративних мереж. Це такі технічні рішення, що можуть забезпечити безпеку інформації КМ. Пристрої чи прилади, що відносяться до апаратних засобів мають підтримувати безпечне середовище для ділової активності. На основі однотипних технічних пристроїв можна побудувати як прості, так і складні системи. Апаратні пристрої можуть займати досить багато місця, але й можуть бути надзвичайно малими.

Програмні засоби захисту корпоративних мереж. Саме програмні засоби є найпоширенішим видом захисту інформації в КМ. Таким засобам притаманні універсальність, простота реалізації. Ними легко керувати та постійно розвивати у потрібному для організації напрямку. Розглянемо деякі найпоширеніші програмні інструменти захисту інформації.

Міжмережевий екран. Міжмережевий екран, (фаєрвол або брандмауер) – це програма, яка може захистити мережу, фільтруючи трафік відповідно до наперед встановленого набору правил безпеки. Фаєрвол аналізує вхідний трафік, що надходить з незахищених або підозрілих джерел, щоб запобігти атакам. Брандмауери аналізують трафік у вхідній точці комп'ютера – на порті, де відбувається обмін інформацією із зовнішніми пристроями. Може полегшити управління безпекою, попереджати доступ неавторизованих користувачів та, навіть, блокувати шкідливі дані.

Антивірус. Це програмні засоби, котрі здатні виявляти та знищувати віруси, які можуть заразити один пристрій чи усю КМ (тут «вірус» – це будь-який шкідливий код). Є такі антивірусні програми: детектори, фаги (лікарі), ревізори та фільтри. Існують індивідуальні та корпоративні пакети антивірусного захисту. Перші – індивідуальні пакети – використовуються на індивідуальних комп'ютерах, а другі,

зазвичай, використовують організації. Корпоративні пакети антивірусного захисту мають архітектуру «клієнт-сервер». Клієнтські програми встановлюються на окремих пристроях мережі, а сервер робить розсилку оновлень [7].

Для виявлення шкідливого коду, антивіруси використовують різні методи. Найпопулярнішими є метод сигнатур та евристичні методи. Метод сигнатур полягає у тому, що кожен тип вірусів містить у собі характерний лише для нього фрагмент коду, який, найвірогідніше, ідентифікує тип. Цей фрагмент коду і є сигнатурою. Евристичні методи виявляють віруси, ґрунтуючись на структурі шкідливого коду або поведінці вірусу.

IDS/IPS. Не менш важливу роль для безпечної роботи мережі організації відіграють системи виявлення вторгнень (англ. Intrusion Detection System, IDS) та системи попередження вторгнень (англ. Intrusion Prevention System, IPS). IDS/IPS – це комплекс програмних засобів, які виявляють факти і запобігають спробам несанкціонованого доступу до КМ. IDS/IPS використовуються для ідентифікації та попередження користувачів про відому або підозрілу діяльність. IDS зазвичай носять пасивний характер, тоді як IPS активний. Зазвичай IDS та IPS працюють в парі. Спочатку IDS повинна виявити небезпечний або підозрілий мережевий трафік. Після того, як IPS отримала попередження про небезпеку (alert) від IDS, вона може перевіряти (на основі сигнатур та аномальної поведінки) та аналізувати (підозрілої активності та підозрілих пакетів), діяти (помістити деякі пакети до карантину або відкинути їх), а також вести логи та надсилати звіти.

Системи виявлення і запобігання вторгнень можуть визначати шкідливу активність відповідно до наперед встановлених правил. Засновані на правилах IDS працюють за принципом: «ЯКЩО ситуація ТОДІ дія». Такі рішення потребують кваліфікованого фахівця для проведення налаштуваннь.

SIEM-системи. Досить потужним програмним засобом для забезпечення безпеки у комп'ютерній мережі є SIEM-системи (Security information and event management – управління інформаційною безпекою та подіями безпеки). Це такий програмний продукт, який аналізує в онлайн режимі події інформаційної безпеки, отримані від мережевих пристроїв і додатків. Так само як і IDS/IPS, SIEM-системи можуть використовуватися для запису даних у логи і створення звітів. SIEM-системи також призначені для зберігання інформації у зручному для користувача форматі. Сама SIEM порівнює отримані дані зі встановленим стандартом і намагається знайти невідповідності [11]. У собі цей програмний продукт поєднує управління подіями безпеки (англ. Security event management, SEM) та управління інформаційною безпекою (англ. Security Information management, SIM) [9].

Криптографічні засоби. Для підвищення рівня безпеки у корпоративних комп'ютерних мережах широко використовується шифрування. Зазвичай, в його основі лежать ключ та певний криптографічний алгоритм. Так, наприклад, для захисту веб-продуктів використовують протоколи SSL та HTTPS.

Протокол SSL – англ. Secure Sockets Layer – рівень захищених сокетів – шифрує дані на канальному рівні моделі OSI. Цей протокол забезпечує кодування на порті.

Протокол HTTPS призначений для забезпечення надійного захисту тільки гіпертекстових документів веб-сервера. Цей протокол гарантує авторизацію та захист веб-документів. Цей протокол не можна використати для захисту інших протоколів таких, як FTP чи SMTP.

4. Спеціалізовані механізми захисту корпоративних мереж

Frame Relay – це протокол канального рівня моделі OSI, що використовується для швидкої передачі кадрів до місця призначення. Протокол має мінімальний набір

послуг, що робить його простим у реалізації, але він не підтримує надійну передачу кадрів, що відносить його відповідальність на протоколи вищих рівнів, такі як TCP. Однією з головних переваг технології Frame Relay є гарантія пропускної здатності з'єднань мережі.

Технологія протоколів типу "точка-точка" використовується, коли IP-маршрутизатори з'єднуються безпосередньо фізичними лініями зв'язку. Стандартним протоколом Інтернет є протокол точка-точка (PPP), який має складну процедуру обміну параметрами зв'язку, включно із встановлення зв'язку, визначення автентичності користувача та виклик протоколу мережевого рівня. Протокол PPP має два варіанти для визначення автентичності користувача: протокол аутентифікації за паролем (PAP), який пересилає пароль у відкритому вигляді по лінії зв'язку, та протокол аутентифікації за викликом квітування (CHAP), який використовує передачу непрямих відомостей про паролі за допомогою хеш-функції.

IPSec є протоколом, що працює на мережевому рівні моделі OSI та може працювати в будь-якій мережі, оскільки базується на протоколі IP і може використовувати всі технології канального рівня. Механізм безпеки в IPSec забезпечується протоколами AH, ESP та IKE, які виконують функцію «безпечного з'єднання». Стандарти IPSec дозволяють кінцевим точкам безпечного каналу використовувати засоби «безпечного з'єднання» для передачі трафіку через всі проміжні точки публічної мережі. Цей підхід також дозволяє вибирати необхідний рівень деталізації захисту.

Детальніше розглянемо функції механізмів безпеки стеку протоколу IPSec. Протоколи AH, ESP та IKE складають основу IPSec. Завдання протоколу AH (Authentication Header) полягає у забезпеченні цілісності та автентичності даних. Протокол ESP (Encapsulating Security Payload) призначений для шифрування переданих даних і також може виконувати ті ж функції, що й протокол AH. Протокол IKE (Internet Key Exchange) грає допоміжну роль, забезпечуючи кінцевим точкам доступ до секретних ключів, необхідних для протоколів AH та ESP для встановлення безпечного каналу.

Сервіс AAA (автентифікація, авторизація, облік) ускладнює життя зловмисникам і одночасно допомагає легітимним користувачам отримувати доступ до мережевих ресурсів. Автентифікація вимагає від користувачів підтвердження їхньої ідентичності, щоб переконатися, що вони дійсно є тими, за кого себе видають. Під час авторизації сервіс вирішує, які ресурси можуть бути доступні користувачу і які права він має. Запис дій користувача зберігається для обліку та контролю. Механізм безпеки базується на трьох складових: автентифікації, авторизації та обліку.

Спочатку розглянемо процес автентифікації, який має дві основні моделі для корпоративних мереж. Перша модель – двостороння, в якій процедура автентифікації виконується тільки між учасниками діалогу без допомоги третьої сторони. Наприклад, цю модель використовують для автентифікації при віддаленому доступі до мережевих пристроїв через протоколи доступу (SSH або Telnet). Друга модель – тристороння, яка використовується для автентифікації великої кількості користувачів у мережі. Вона складається з користувача, сервера доступу до мережі, який є посередником між користувачем і мережею, та AAA-сервера, який перевіряє облікові записи користувачів за запитами посередника.

Друга A в абревіатурі сервісу AAA відповідає за авторизацію, яка визначає повноваження доступу конкретного користувача до ресурсів. Для здійснення такої авторизації потрібна відповідна інфраструктура. Користувач, який потребує доступу до певного ресурсу або послуги, укладає договір з організацією, що перевіряє, чи має

він право доступу. Організація, в свою чергу, укладає договір з провайдером, який використовує AAA-сервер для авторизації доступу до ресурсів або послуг. Далі діє обладнання, яке надає ці ресурси або послуги (наприклад, принтер або маршрутизатор).

Остання літера А в абревіатурі AAA позначає «облік» (англ. accounting). Під обліком ми розуміємо збір інформації про використання ресурсу з метою аналізу, контролю та розподілу вартості. Архітектура системи обліку не є складною. Починаючи з пристроїв мережі, які збирають інформацію про використання ресурсів та відправляють її на сервер обліку за допомогою протоколів аудиту, інформація обробляється сервером обліку. Сервер обліку об’єднує дані проміжного аудиту та ідентифікує записи, що повторюються. Він також розділяє події внутрішніх доменів та міждоменні події та виконує відповідну маршрутизацію трафіку.

GRE – це протокол інкапсуляції, який працює з IPSec для створення тунелів. Хоча сам по собі GRE не забезпечує безпечного передавання даних, він є необхідним для вирішення завдань, пов'язаних з динамічною маршрутизацією. При шифруванні великих обсягів даних навантаження на обладнання може бути значним. Механізм безпеки полягає у передаванні даних від протоколів динамічної маршрутизації, а самі дані можуть бути шифрованими. GRE дозволяє інкапсулювати різні типи протоколів у IPSec-тунелі, який використовується для безпечного з'єднання IP-мереж, що не мають прямого маршруту між собою. Структура інкапсульованого пакету GRE складається з протоколу доставки (наприклад, IP), протоколу інкапсуляції GRE та протоколу, який інкапсулюється («протокол-пасажир»). Протокол GRE має відому проблему з DF-бітом, яка може виникати при передачі фрагментованого трафіку.

Сервіс VPN (англ. Virtual Private Network – віртуальна приватна мережа) застосовується для захисту корпоративних мереж. Однією з головних переваг цього сервісу є більш ефективний розподіл ресурсів мережі під час комутації пакетів, порівняно з комутацією каналів. Також відсутність зв'язку із зовнішнім середовищем надійно захищає мережу від зовнішніх атак та суттєво знижує ймовірність «прослуховування» мережевого трафіку. Це досягається завдяки механізмам безпеки, таким як шифрування трафіку, автентифікація користувачів та контроль доступу до мережі.

Сервіс VPN обмежує доступ до мережі, дозволяючи обмінюватися пакетами лише вузлам в мережі, оскільки лише вони мають відповідну технічну можливість. Це завдання є складним для VPN, оскільки пакети віртуальної приватної мережі повинні пройти через ті ж канали та мережеві пристрої, що й пакети зовнішніх вузлів. Технологія VPN дозволяє адресувати вузли мережі із всього діапазону IP-адрес, включаючи приватні адреси, тому обмеження на вибір IP-адрес вузлами віртуальної приватної мережі відсутні. Однією з вагомих переваг VPN є наявність окремих ліній зв'язку, що дозволяє точніше передбачити продуктивність мережі. Технологія віртуальних приватних мереж передбачає відсутність зв'язків із "зовнішнім світом", що серйозно обмежує доступ зовнішніх користувачів. Такі заходи істотно збільшують рівень захисту інформації у корпоративних мережах.

5. Висновки

Для досягнення максимальної безпеки корпоративних мереж, необхідно вдосконалювати методи та засоби захисту на постійній основі, оскільки шпигунські програми та хакерські атаки постійно еволюціонують. Крім того, важливо мати на увазі, що найкращим рішенням для кожної компанії може бути унікальна комбінація методів та засобів, яка відповідає її потребам та особливостям. Крім технічних заходів, також важливо вдосконалювати процедури управління доступом до мережі

та навчати персоналу відповідної кваліфікації для виявлення та запобігання можливих загроз. Навчання користувачів базовим принципам безпеки комп'ютерних мереж також може допомогти зменшити ризик несанкціонованого доступу до мережі.

Список використаних джерел:

1. Технології захисту локальних мереж на основі обладнання CISCO : навч. пос. / Т. І. Коробейнікова, С. М. Захарченко. – Л.: Вид-во Львівської політехніки, 2021. – 188с.
2. 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.
3. Система обміну миттєвими повідомленнями в корпоративній мережі / Коробейнікова Т. І., Савицька Л. А., Карплюк С. В. // Актуальні досягнення сучасних наукових досліджень: XX Міжн. наук.-пр. конференція: тези доповідей, Дніпро, 17 вересня 2019 р. – Ч. 1. – Дніпро: ГО «НОК», 2019 – с. 19-24.
4. Методи та засоби безпечної передачі даних в корпоративних мережах / Коробейнікова Т. І., Куцак Ю. В. // Зб. мат.XLVIII наук.-техн. конф. ФІТКІ (2019). Реж. доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2019/paper/view/6606/5491.
5. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навч. пос. – Вінниця: ВНТУ, 2009. – 268 с
6. Метод паралельного моніторингу параметрів корпоративних мереж / Коробейнікова Т.І., Каневський М. В. // Зб. мат. XLVIII Наук.-техн. конф. ФІТКІ (2019). Реж. доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-019/paper/view/6972/5687.
7. 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.
8. Методи та засоби захисту комп'ютерної інформації. [Ел. рес.] // Укр. академія друкарства. Каф. ПМФ – Режим доступу до ресурсу: http://pmf.uad.lviv.ua/storage/uploads/лекція%20інформаційнв%20безпека.pdf.
9. Що таке SIEM система? [Ел. рес.] // Софтліст. – 2019 – Режим доступу до ресурсу: https://ua.softlist.com.ua/articles/.
10. Чинчик Д. М. Методи та засоби комплексного захисту корпоративної мережі / Д. М. Чинчик, 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. 433-450. – ISBN 978-88-32012-34-7. DOI 10.51582/interconf.7-8.11.2021.
11. Chynchyk D. Specialized mechanisms for protecting the corporate network in terms of network security / D. Chynchyk, T. Korobeinikova // "Information protection and information systems security" : Materials of VIII-th International Scientific and Technical Conference, November 11 – 12, 2021. – Lviv: NULP, 2021 – С. 51-53.