КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.318327
УДК 004.056:004.774

Крючкова Лариса Петрівна
д.т.н., професор, професор кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

Ємельяненко Михайло Олександрович
студент
Київський столичний університет імені Бориса Грінченка, Київ, Україна
moyemelianenko.fitu20@kubg.edu.ua

ЗАХИСТ WEB-РЕСУРСУ INTRANET ВІД ЗОВНІШНІХ І ВНУТРІШНІХ ЗАГРОЗ

Анотація. Публікація присвячена аналізу та розробці стратегій захисту вебресурсів INTRANET від зовнішніх і внутрішніх загроз. Підходи до захисту включають в себе використання мережевих заходів безпеки, таких як мережеві брандмауери та VPN, а також застосування ідентифікації користувачів і механізмів контролю доступу. У статті досліджується значення захисту даних на різних рівнях інфраструктури, від мережевого рівня до рівня додатків. Розглядаються ключові методи і технології захисту, такі як шифрування даних, мережеві аутентифікаційні протоколи та системи виявлення вторгнень (IDS). Додатково, у статті розглядаються стратегії з обмеження доступу, включаючи управління правами доступу і моніторинг активності користувачів. Висвітлюються важливі аспекти внутрішньої загрози, такі як виток інформації та несанкціонований доступ співробітників. Дослідження закінчується рекомендаціями щодо розробки комплексної стратегії захисту для забезпечення безпеки вебресурсів INTRANET.

Ключові слова: захист інтранету; зовнішні та внутрішні загрози; архітектура; системи захисту; політики безпеки.

ВСТУП

У світі, де цифрова технологія стає необхідною складовою у всіх сферах життя, безпека вебресурсів є невід'ємною частиною успішної діяльності будь-якої організації. Особливо важливою стає задача захисту внутрішньої мережі (INTRANET) від зовнішніх і внутрішніх загроз, оскільки це є основною платформою для обміну конфіденційною інформацією, співпраці та виконання бізнес-процесів в більшості підприємств.

Насущною проблемою є те, що із зростанням рівня цифрової залежності організацій також зростає кількість загроз та потенційних атак на їхні внутрішні мережі. Від витоків даних до кібератак з метою збирання конфіденційної інформації, загрози можуть бути як зовнішніми, так і внутрішніми. Тому виникає велика необхідність в розробці та впровадженні ефективних стратегій захисту, які забезпечать надійний захист внутрішньої мережі від цих загроз.

У даній статті детально розглядаються ключові аспекти захисту вебресурсу INTRANET від зовнішніх і внутрішніх загроз. Починаючи від аналізу потенційних загроз та їхніх можливих наслідків, а завершуючи розробкою комплексної стратегії захисту, стаття надасть чітке уявлення про те, як забезпечити безпеку внутрішньої мережі та захистити конфіденційні дані від небажаних втручань.

Постановка проблеми. Проблема захисту вебресурсів INTRANET від зовнішніх і внутрішніх загроз є актуальною та нагальною у сучасному цифровому світі. Організації стикаються з постійною загрозою кібератак, які можуть призвести до витоку конфіденційної інформації, порушення робочих процесів та значних фінансових втрат.

Ця проблема має як науковий, так і практичний аспекти. Наукове значення полягає в тому, щоб дослідити нові методи та технології захисту, що відповідають зростаючим загрозам кібербезпеки. Практичне значення полягає в розробці конкретних стратегій та заходів захисту, які допоможуть підприємствам ефективно захищати їхні внутрішні мережі та дані від потенційних атак.

Ця проблема також пов'язана з питанням дотримання законодавства щодо захисту даних, оскільки багато країн встановлюють строгі вимоги щодо збереження конфіденційності та безпеки персональної інформації. Таким чином, вирішення проблеми захисту вебресурсів INTRANET має важливе значення як для захисту приватності користувачів, так і для забезпечення законності та довіри до підприємства.

Мета статті. Метою дослідження є вивчення та аналіз загроз безпеці вебресурсу INTRANET з метою розробки та реалізації ефективних стратегій захисту. Основний акцент буде зроблено на ідентифікації та класифікації зовнішніх і внутрішніх загроз, а також на розробці методів захисту для запобігання атакам та недозволеним діям. Мета полягає в створенні надійної системи безпеки, яка забезпечить цілісність, конфіденційність та доступність вебресурсу INTRANET для користувачів та запобігатиме потенційним загрозам.

Аналіз останніх досліджень і публікацій. Інтране́т [1] — внутрішньокорпоративна мережа, що використовує стандарти, технології і програмне забезпечення Інтернету. Комп'ютерна мережа, що використовує технології інтернету, але в той же час є приватною корпоративною мережею. Мережа підтримує сервіси Інтернет, наприклад, такі, як електронна пошта, вебсайти, FTP-сервери тощо, але в межах корпорації. Інтранет-мережа, підключається до зовнішніх мереж, у тому числі і до інтернету, як правило, через засоби захисту від несанкціонованого доступу. Інтранет може бути ізольований від зовнішніх користувачів або функціонувати як автономна мережа, що не має доступу ззовні.

В Intranet використовуються стандартні для Internet служби, в тому числі HTML, HTTP, TCP/IP, SMTP, FTP, CGI, система доменних імен і Web-браузери, що отримують і відображають інформацію з розміщених по підприємству Web-серверів.

У найближчому майбутньому *Intranet* буде доповненням до локальних мереж, але в жодному разі не стане їх заміною. Старі технології локальних мереж надають більші можливості, є гнучкішими, забезпечують надійнішу систему безпеки, поставляються переважно в готовому вигляді, що не потребує ніякої доробки чи підгонки на місці. Тим не менше, простежується тенденція використання *Intranet*-технологій та інструментів для задоволення всезростаючих потреб спілкування та обміну інформацією: зв'язок з колегами електронною поштою і проведення конференцій, збір, зберігання та поновлення найновішої інформації з мінімальними затратами на управління та високим ступенем безпеки.

Приклади застосування *Intranet* [2]:

1. Централізований сховище. Внутрішня мережа дозволяє зберігати документи та інші файли в централізованому місці і керувати доступом до них. Вам не доведеться покладатися на кілька баз даних або джерел інформації.
2. Внутрішня комунікація. Рішення для внутрішньої мережі допоможе вам покращити внутрішню бізнес-комунікацію, роблячи каталоги персоналу, новини компанії та організаційні діаграми легко доступними.

3. Оптимізована співпраця. Внутрішні мережі сприяють співпраці, дозволяючи вашим співробітникам мати приватне та безпечне простір для вирішення ідей, обміну думками та проведення корисних обговорень.
4. Персоналізація. Внутрішні мережі персоналізують досвід для кожного працівника, надаючи матеріали, адаптовані до їхніх ролей та відповідальностей у вашій організації. З правильними налаштуваннями контролю доступу ви зможете контролювати, хто що може бачити.
5. Управління проєктами. Ви можете інтегрувати ваше рішення для внутрішньої мережі з інструментами для управління проєктами, відстеження завдань та автоматизації робочих процесів для покращення ефективності вашої організації.

Аналіз актуальних атак на вебресурси [3]. Аналіз здійснено із використанням існуючих статистичних даних за 2015 рік. Наведено не тільки опис атак і відсоток вебресурсів, до яких вони можуть бути застосовані, автором також запропоновані адекватні методи протидії таким атакам. Для наочності результати зведено в таблицю (рис. 1).

Найбільш популярною атакою є «Insufficient transport layer protection» — отримання даних під час передавання. Дана атака може бути виконана для 70% ресурсів. Для виключення можливості проведення таких атак достатньо використовувати протокол HTTPS.

Ще одною формою атаки є «Витік інформації» («Information leakage»). Дану атаку можна виконати на 56% ресурсів. Витік інформації з додатків виникає в результаті відмови або неправильної роботи програми, а також у разі порушення її логіки. Для виключення можливості проведення атаки необхідно ретельно тестувати програмну частину ресурсу, проводити перевірку повідомлень на стороні сервера моніторинг оповіщень про помилки.

№ за/п	Вид атаки	Вразливість веб-ресурсів, %	Протидія
1	Insufficient transport layer protection	70 %	Використання протоколу HTTPS.
2	Information leakage	56 %	Тестування програмної частини ресурсу, перевірка повідомлень на стороні сервера, моніторинг оповіщень про помилки
3	Cross-site scripting	47 %	Очищення та валідація вхідних даних
4	Brute force	29 %	Використання паролів високої складності, налаштування сервера на аналіз вхідних запитів
5	Content spoofing	26 %	Відмовитися від використання фреймів і не передавати в параметрах абсолютні або локальні шляхи до файлів
6	Cross-site request forgery	24 %	Перевірка вхідних даних з форм
7	URL redirector abuse	16 %	Валідація вхідних даних
8	Predictable resource location	15 %	Контроль доступу до файлів сервера

Рис. 1. Класифікація видів атак

Атаку «Cross-site scripting» (міжсайтове використання сценаріїв) можливо виконати на 47% ресурсів. Атака може містити JavaScript-код, що обробиться браузером жертви. Вразливості, що мають такий характер, називають HTML-ін'єкціями, через то, що механізм їхнього впровадження дуже схожий із SQL-ін'єкціями, але на відміну від останніх, впроваджуваний код виконується в браузері користувача. Для захисту від цього виду атак необхідно проводити очищення та валідацію вхідних даних.

Генерацію великої кількості запитів або підбір паролів («Brute force») можливо виконати на 29% ресурсів. Для захисту необхідно забезпечити використання паролів високої складності, налаштування сервера на аналіз вхідних запитів.

Атака «Content spoofing» (підміна даних через заміну контенту сторінок) можлива для 26% ресурсів. Використовуючи цю техніку, зловмисник змушує користувача повірити, що сторінка згенерована вебсервером, а не передана із зовнішнього джерела. Для захисту від даного виду атак потрібно відмовитися від використання фреймів і, найголовніше, ніколи не передавати в параметрах абсолютні або локальні шляхи до файлів.

Вид атак на відвідувачів вебсайтів, який використовує недоліки протоколу HTTP, називається «Cross-site request forgery». Коли жертва авторизується на сайті, створений зловмисником, від його імені таємно відправляється запит на сторонній сервер (наприклад, на сервер сторонньої платіжної системи), і на ньому здійснюють шкідливу операцію (наприклад, переказ на сторонній рахунок, що належить зловмиснику). Дану атаку можливо виконати на 24% ресурсів. Для захисту необхідно проводити перевірку вхідних даних з форм, наприклад шляхом додавання унікального доданка.

Переправлення на інші сайти через підміну початкових посилань («URL redirector abuse»), також як і багато інших перерахованих вище, є різновидом помилок перевірки вхідних даних і є можливим на 16% ресурсів. Вирішенням є валідація вхідних даних.

Ще однією популярною атакою є «Predictable resource location», тобто знаходження прихованого функціоналу та даних. Така атака доступна на 15% ресурсів і вирішується шляхом контролю доступу до файлів сервера.

З кожним роком статистика атак змінюється. Так, у 2014 році найпопулярнішою формою була «Cross-site scripting», а в 2013 — витік інформації («Information leakage»). Виходячи з наведених даних, можна зробити висновки про те, що для захисту від більшості популярних видів атак достатньо належним чином перевіряти вхідні дані. Також рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих програмних каркасів (*Frame-work*), в якому вбудовані механізми перевірки, шифрування та валідація вхідних даних

Також варто зауважити, що в даному дослідженні не розглянуті атаки на мережеві служби, наприклад DoS та DDoS, найкращим методом захисту від яких є використання хмарних технологій і перевірених конфігурацій серверів.

Запобігання ризикам через вибір інструментів [4]. Перший рівень захисту має бути забезпечений захистом внутрішньої мережі. Як правило, бажано встановити брандмауер: це інструмент, який дає змогу захистити мережу компанії від нерозпізнаного зовнішнього доступу. Також можна використовувати інші технології, наприклад проксі-сервери. Це компоненти комп'ютерного обладнання, які виступають посередниками в обміні між двома хостами. Це може бути, наприклад, комп'ютер: в цьому випадку доступ до Інтернету має тільки проксі-сервер. Якщо користувачі з інших комп'ютерів хочуть отримати доступ до Інтернету з мережі, вони можуть зробити це лише через безпечне з'єднання з проксі-сервером.

З цифровим робочим місцем Microsoft 365 у вас є повністю безпечне середовище. Щоб забезпечити захист від зловмисних вторгнень, ви можете використовувати 100% захищені розширення Microsoft 365, такі як Mozzaik365, які не містять жодних даних клієнтів.

Запобігання ризикам шляхом нагляду, моніторингу та контролю використання наданих інструментів [4]. Надійний захист від вірусів та інших кібератак вимагає постійного моніторингу, оновлення та нагляду за наявними у співробітників інструментами. У цьому відношенні електронна пошта має бути особливо захищеною, оскільки через неї щодня проходять сотні елементів даних. Крім того, поширення культури ризику серед співробітників у поєднанні з механізмом моніторингу, призначеним для виявлення попереджувальних ознак злому, має бути на передньому краї завдань ІТ-відділу.

Одним із головних ризиків, якому слід запобігти, є тіньовий І, коли працівники використовують інструменти та технології, які не надаються (а отже, не регулюються) компанією. Ця практика наражає компанію на численні порушення безпеки, дозволяючи невідомим інструментам отримати доступ до конфіденційних даних. Боротьба з тіньовими ІТ повинна вестися різними способами, зокрема шляхом інформування працівників про проблеми безпеки та контролю за використанням ІТ. Таким чином, компанія повинна чітко дати зрозуміти, що жоден працівник не повинен використовувати інструмент або програму без дозволу ІТ-відділу.

Нарешті, обмеження доступу до конфіденційних даних має бути пріоритетом для ІТ-відділу. Цілком ймовірно, що більшості співробітників під час щоденної роботи не потрібен доступ до всієї системи даних компанії. Таким чином, обмеження доступу до конфіденційних даних лише для тих, хто їх потребує, зменшує ризик доступу третьої сторони до даних і їх використання.

Зовнішні загрози [5] стосуються кібератак, які походять із-за меж мережі організації, як правило, від зловмисників або груп, які прагнуть використати вразливі місця та отримати несанкціонований доступ до конфіденційних даних. Ось кілька прикладів їхніх атак:

Атаки зловмисного програмного забезпечення: зловмисне програмне забезпечення, скорочення від шкідливого програмного забезпечення, є типом програмного забезпечення, призначеного для шкоди комп'ютерній системі чи мережі. Зловмисне програмне забезпечення може бути у багатьох формах, включаючи віруси, трояни та програми-вимагачі, і може завдати значної шкоди даним і репутації організації.

Фішингові атаки. Фішинг — тип атаки соціальної інженерії, коли зловмисник видає себе за законну особу, наприклад банк або постачальника послуг електронної пошти, і надсилає шахрайські електронні листи чи повідомлення, щоб обманом змусити користувачів надати конфіденційну інформацію, наприклад облікові дані для входу. Фішингові атаки є найпоширенішим способом зловмисників отримати несанкціонований доступ до мережі організації.

DDoS-атаки: розподілена атака типу «відмова в обслуговуванні» (DDoS) передбачає перевантаження мережі або веб-сайту трафіком, щоб зробити його недоступним для користувачів. DDoS-атаки часто запускаються ботнетами, які є мережами заражених комп'ютерів, якими зловмисники можуть дистанційно керувати.

Експлойт нульового дня: експлойт нульового дня — це вразливість у програмному забезпеченні, яка невідома постачальнику програмного забезпечення чи спільноті кібербезпеки. Зловмисники можуть використати ці вразливості, щоб отримати неавторизований доступ до мережі організації до того, як буде доступне виправлення або виправлення.

Атаки на ланцюг постачань: Атака на ланцюг постачання передбачає націлювання на стороннього постачальника або постачальника для отримання доступу до мережі організації. Ці атаки може бути важко виявити, оскільки вони часто не спрямовані безпосередньо проти організації. Натомість зловмисники використовуватимуть уразливості в мережі сторони.

Внутрішні загрози [5] стосуються кіберзагроз, які надходять зсередини організації, часто стосуються авторизованих користувачів, які мають доступ до мережі та даних організації. Ось кілька прикладів:

Внутрішні атаки: вони зазвичай здійснюються співробітниками, які навмисно чи ненавмисно завдають шкоди системам або даним організації. Наприклад, незадоволений працівник може навмисно пошкодити системи, щоб спричинити простої або перешкодити організації вести бізнес. Або цей працівник може вкрасти та оприлюднити конфіденційну інформацію, що може виявитися навіть дорожчим, ніж простой системи.

Випадкові порушення даних. Порушення відбуваються, коли співробітники ненавмисно відкривають конфіденційні дані, наприклад, надсилають електронний лист не тому одержувачу або не можуть захистити пристрій, що містить конфіденційні дані. Дуже важливо забезпечити навчання працівників, щоб допомогти їм зрозуміти важливість безпеки даних.

Погане керування паролями: слабкі або легкодоступні паролі можуть поставити під загрозу безпеку організації. Наприклад, працівник може використовувати той самий пароль для кількох облікових записів, що може призвести до каскадного злому в кількох системах.

Зловживання привілеями: це відбувається, коли авторизований користувач із підвищеним доступом зловживає своїми привілеями, щоб завдати шкоди організації. Наприклад, IT-адміністратор може зловживати своїми правами доступу, щоб установити зловмисне програмне забезпечення в мережі.

Недбала поведінка: відноситься до співробітників, які нехтують політикою безпеки та беруть участь у ризикованій поведінці, яка може призвести до витоку даних. Наприклад, працівник може використовувати незахищену загальнодоступну мережу Wi-Fi для доступу до даних компанії або залишити пристрій, що містить конфіденційні дані, у громадському місці.

Брандмауер [6] для INTRANET мережі відіграє критичну роль у забезпеченні безпеки та захисту даних. Його основна функція — контроль трафіку, що входить і виходить з мережі, а також фільтрація небезпечного трафіку. Брандмауер дозволяє створювати правила доступу, які регулюють, який трафік може проходити через мережу і який має бути заблокований. Це дозволяє встановлювати обмеження для користувачів і застерігати від можливих атак ззовні та від внутрішніх загроз. Брандмауер також може виявляти аномальний трафік і сповіщати адміністраторів про потенційні проблеми безпеки. В цілому, використання брандмауера в INTRANET мережі допомагає створити надійний захист і забезпечити безпеку обміну даними всередині організації.

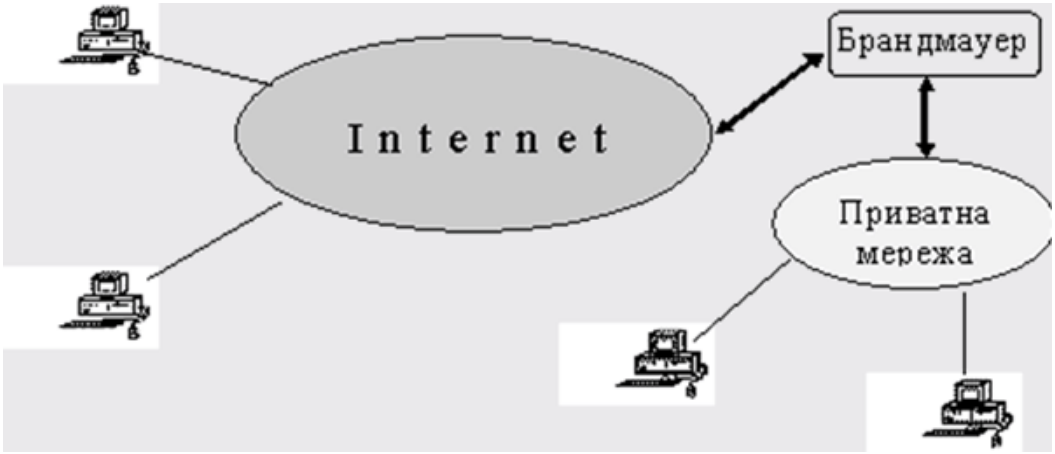

Рис. 2. Взаємодія віртуальної мережі з Internet

Види брандмауерів [7]:

1. засновані на статичній фільтрації пакетів через аналіз IP-адрес та типу сервісів (каналів); дуже швидкі в роботі та не потребують спеціальних апаратних засобів;
2. засновані на динамічній фільтрації пакетів (stateful inspection). Виконують моніторинг стану з'єднання з аналізом IP-адреси та MAC-адрес (адрес канального рівня) і фактично є розширенням маршрутизаторів;
3. Proxy-сервер [8], виступає як посередник з'єднання клієнтів; функціонує на прикладному рівні (в моделях OSI [9] та TCP/IP [10]) і має дві типові реалізації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Результати дослідження показують, що захист веб-ресурсу INTRANET від зовнішніх і внутрішніх загроз є складною, але досяжною задачею при належній увазі та застосуванні відповідних стратегій захисту. Виявлено, що зовнішні загрози можуть включати кібератаки, спрямовані на порушення цілісності та конфіденційності даних, а також внутрішні інциденти, такі як недбале оброблення даних або несанкціонований доступ до системи.

У результаті дослідження виявлено, що для ефективного захисту вебресурсу INTRANET необхідно впровадження комплексних заходів безпеки, таких як мережеві брандмауери, системи виявлення вторгнень, шифрування даних та механізми аутентифікації та контролю доступу.

Додатково виявлено, що персонал організації відіграє ключову роль у забезпеченні безпеки вебресурсу INTRANET. Своєчасне навчання та інструктаж з питань кібербезпеки, а також встановлення правильних процедур та політик безпеки можуть суттєво зменшити ризик інцидентів безпеки та забезпечити стійку захищеність вебресурсу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Виконані дослідження підтверджують, що захист веб-ресурсу INTRANET від зовнішніх і внутрішніх загроз є складною, але важливою задачею. На основі аналізу встановлено, що ефективний захист потребує комплексного підходу, що включає в себе застосування різноманітних технологій та стратегій безпеки.

Подальші перспективи досліджень можуть включати аналіз нових загроз та розробку інноваційних методів захисту, оцінку ефективності вжитих заходів безпеки, а також вивчення впливу соціальних інженерних атак на безпеку веб-ресурсу INTRANET. Додаткові дослідження в цій області можуть допомогти розширити наші знання та покращити практичні стратегії захисту, забезпечуючи надійну безпеку веб-ресурсів у цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Contributors to Wikimedia projects. (2002). *Intranet - Wikipedia*. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Intranet
2. Intranet Security Best Practices: How to Protect Your Network. (n.d.). *AnyforSoft*. https://anyforsoft.com/blog/intranet-security/
3. Ganore, P. (2017). What Is A Web Server And How Does It Function? Milesweb. https://www.milesweb.com/blog/hosting/web-server-function/
4. *Good practices to ensure the security of your Intranet.* (n.d.). MOZZAIK. https://www.mozzaik365.com/intranet/best-practices-for-intranet-security
5. *External and Internal Threats | WithSecure*. (n.d.). Cybersicherheitslösungen für Unternehmen| WithSecure™. https://www.withsecure.com/en/expertise/blog-posts/external-and-internal-threats
6. Firewall for Intranet Security. (n.d.). researchgate. https://www.researchgate.net/publication/347774798_Firewall_for_Intranet_Security
7. *Financial activities on the Internet: corporate and private networks. (*2011). osvita.ua. https://ru.osvita.ua/vnz/reports/bank/19820/
8. Contributors to Wikimedia projects. (2002). *Proxy server - Wikipedia*. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Proxy_server
9. Piddubnyi, M. (2023). *The OSI model is simply*. dou.ua. URL: https://dou.ua/forums/topic/46215/#:~:text=%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C%20Open%20Systems%20Interconnection%20(OSI,%D0%B2%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B0%D1%94%2C%20%D1%8F%D0%BA%20%D0%B2%D1%96%D0%B4%D0%B1%D1%83%D0%B2%D0%B0%D1%82%D0%B8%D0%BC%D0%B5%D1%82%D1%8C%D1%81%D1%8F%20%D0%BE%D0%B1%D0%BC%D1%96%D0%BD%20%D0%B4%D0%B0%D0%BD%D0%B8%D0%BC%D0%B8
10. Participants in Wikimedia projects. (2006). *TCP/IP — Wikipedia*. Wikipedia. https://uk.wikipedia.org/wiki/TCP/IP#:~:text=Стабільну%20версію%20було%20перевірено%2014,») %20і%20TCP%20(англ

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023

Larysa Kriuchkova
Doctor of sciences, professor, professor of Volodymyr Buriachok
Department of Information and Cybersecurity
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

Mykhailo Yemelianenko
student
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
moyemelianenko.fitu20@kubg.edu.ua

PROTECTION OF THE INTRANET WEB RESOURCE FROM EXTERNAL AND INTERNAL THREATS

Abstract. This article focuses on the analysis and development of strategies to protect INTRANET web resources from external and internal threats. Protection approaches include the use of network security measures such as firewalls and VPNs, as well as the implementation of user identification and access control mechanisms. The importance of data protection at various levels of infrastructure, from the network level to the application level, is explored. Key protection methods and technologies such as data encryption, network authentication protocols, and intrusion detection systems (IDS) are discussed. Additionally, access restriction strategies, including access rights management and user activity monitoring, are addressed. Important aspects of internal threats such as information leakage and unauthorized employee access are highlighted. The research concludes with recommendations for developing a comprehensive protection strategy to ensure the security of INTRANET web resources.

Keywords: intranet security; external and internal threats; architecture; security systems; security policies.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Contributors to Wikimedia projects. (2002). *Intranet - Wikipedia*. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Intranet
2. Intranet Security Best Practices: How to Protect Your Network. (n.d.). *AnyforSoft*. https://anyforsoft.com/blog/intranet-security/
3. Ganore, P. (2017). What Is A Web Server And How Does It Function? Milesweb. https://www.milesweb.com/blog/hosting/web-server-function/
4. *Good practices to ensure the security of your Intranet.* (n.d.). MOZZAIK. https://www.mozzaik365.com/intranet/best-practices-for-intranet-security
5. *External and Internal Threats | WithSecure*. (n.d.). Cybersicherheitslösungen für Unternehmen| WithSecure™. https://www.withsecure.com/en/expertise/blog-posts/external-and-internal-threats
6. Firewall for Intranet Security. (n.d.). researchgate. https://www.researchgate.net/publication/347774798_Firewall_for_Intranet_Security
7. *Financial activities on the Internet: corporate and private networks. (*2011). osvita.ua. https://ru.osvita.ua/vnz/reports/bank/19820/
8. Contributors to Wikimedia projects. (2002). *Proxy server - Wikipedia*. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Proxy_server
9. Piddubnyi, M. (2023). *The OSI model is simply*. dou.ua. URL: https://dou.ua/forums/topic/46215/#:~:text=%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C%20Open%20Systems%20Interconnection%20(OSI,%D0%B2%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B0%D1%94%2C%20%D1%8F%D0%BA%20%D0%B2%D1%96%D0%B4%D0%B1%D1%83%D0%B2%D0%B0%D1%82%D0%B8%D0%BC%D0%B5%D1%82%D1%8C%D1%81%D1%8F%20%D0%BE%D0%B1%D0%BC%D1%96%D0%BD%20%D0%B4%D0%B0%D0%BD%D0%B8%D0%BC%D0%B8

10. Participants in Wikimedia projects. (2006). *TCP/IP — Wikipedia*. Wikipedia. https://uk.wikipedia.org/wiki/TCP/IP#:~:text=Стабільну%20версію%20було%20перевірено%2014,») %20і%20TCP%20(англ