DOI: 10.59647/978-617-520-936-3/1

Оцінка вразливостей та шляхи зараження вірусами в корпоративному середовищі

Ярослав Невмержицький, студент [1 i] (ORCID: 0009-0006-7613-2028)

[1] *Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна*

АНОТАЦІЯ

Стаття розглядає основні вразливості та шляхи зараження вірусами у корпоративних мережах. В сучасному світі кіберзагрози є важливим аспектом діяльності будь-якої компанії, а неефективний захист від вірусів може призвести до значних фінансових втрат та порушення діяльності бізнесу. Робота аналізує ключові загрози, такі як фішинг, шкідливі файли, уразливості в програмному забезпеченні та слабкі паролі. Результати дослідження включають рекомендації щодо покращення кібербезпеки, зокрема впровадження багаторівневих систем захисту та навчання персоналу.

Ключові слова: віруси, кібербезпека, корпоративні мережі, фішинг, уразливості, захист.

1. АКТУАЛЬНІСТЬ ПРОБЛЕМИ:

Сучасний бізнес в значній мірі залежить від інформаційних технологій, що робить комп'ютерні системи і дані цінними активами. Вірусні атаки представляють серйозну загрозу для безпеки корпоративних систем, що може призвести до фінансових втрат, порушення діяльності та шкоди репутації. Наприклад, атака WannaCry у 2017 році вразила понад 200 тисяч комп'ютерів у 150 країнах, завдавши збитків у мільярди доларів. Це підкреслює важливість розуміння шляхів зараження і способів запобігання атакам.

2. МЕТА ДОСЛІДЖЕНЬ:

Метою даного дослідження є вивчення ключових способів зараження комп'ютерних систем вірусами в корпоративному середовищі, аналіз уразливостей, що використовуються зловмисниками, а також розробка рекомендацій для підвищення рівня кібербезпеки компаній. Вивчення основних видів вірусних атак дозволить створити ефективні стратегії захисту і мінімізувати ризики для бізнесу.

3. ОСНОВНІ РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ:

3.1 Аналіз шляхів зараження:

Електронна пошта: Найпоширеніший спосіб зараження, включаючи фішинг-повідомлення з шкідливими вкладеннями або посиланнями. Згідно з даними Symantec, близько 70% всіх вірусних атак починаються з електронної пошти.

Заражені файли: Шкідливе програмне забезпечення може бути приховане в інсталяційних файлах або документи з макросами. Зловмисники часто використовують техніку соціальної інженерії для примусу користувачів до відкриття таких файлів.

Шкідливі веб-сайти: Веб-сайти, які містять експлойти або шкідливі скрипти, можуть автоматично заражати системи при відвідуванні. Зловмисники використовують уразливості веб-браузерів або плагінів для розподілу вірусів.

Заражені файли та **шкідливі вебсайти** також є серйозними загрозами. Зловмисники часто використовують соціальну інженерію, щоб змусити користувачів завантажити заражені документи або програми. Вебсайти, які містять експлойти, можуть заражати систему через вразливості у веббраузерах або плагінах. Це підкреслює важливість регулярного оновлення програмного забезпечення, зокрема браузерів, та впровадження додаткових заходів безпеки, таких як використання фаєрволів і систем виявлення вторгнень

Одним із важливих шляхів зараження комп’ютерних систем є використання незахищених мережевих підключень. Зловмисники можуть проникати в корпоративні мережі через вразливі або погано захищені з’єднання, застосовуючи атаки типу "людина посередині" або експлуатуючи вразливості в протоколах передачі даних. Це особливо небезпечно для тих компаній, де співробітники працюють віддалено і підключаються до мережі через публічний або незахищений Wi-Fi. Для захисту тут важливо використовувати VPN та забезпечити шифрування всього трафіку.

Крім того, варто згадати про зовнішні пристрої, як-от USB-флешки або зовнішні жорсткі диски. Віруси можуть бути приховані на цих носіях і запускатися автоматично після підключення до комп’ютера. Це ставить під загрозу безпеку корпоративної системи, тому важливо контролювати доступ до таких пристроїв і використовувати інструменти, які блокують неавторизовані підключення або сканують їх на наявність шкідливого ПЗ.

4. ОЦІНКА ВРАЗЛИВОСТЕЙ:

Недостатнє оновлення програмного забезпечення: Багато вірусів експлуатують відомі уразливості в застарілому програмному забезпеченні. Регулярне оновлення систем та додатків є критично важливим для захисту.

Слабкі паролі: Використання простих або легко вгадуваних паролів робить системи вразливими до атак методом брутфорсу. Рекомендується застосовувати складні паролі та двофакторну аутентифікацію.

Відсутність антивірусного захисту: Компанії, які не використовують антивірусні програми або системи захисту від шкідливого ПЗ, значно підвищують ризик зараження.

5. ВПЛИВ НА БІЗНЕС:

Фінансові витрати: Атаки можуть призвести до значних фінансових витрат через втрату даних, необхідність відновлення систем і можливі штрафи за порушення норм захисту даних.

Втрати даних: Заражені системи можуть зазнати втрати важливих даних, що вплине на функціонування бізнесу та може призвести до тривалих перерв у роботі.

Репутаційні збитки: Публікація про атаки на компанію може завдати серйозної шкоди репутації, що призведе до втрати довіри клієнтів і партнерів, та навіть, закриття організації, компанії.

6. АТАКИ МЕТОДОМ БРУТФОРСУ:

Брутфорс є одним з найпоширеніших методів зламу паролів, що використовується кіберзлочинцями. Суть атаки полягає в послідовному підборі можливих комбінацій символів до тих пір, поки не буде знайдено правильний пароль. Такий тип атак особливо ефективний, коли системи захисту компанії використовують прості або застарілі паролі, які легко вгадати. Згідно з даними в інтернеті, атаки методом брутфорсу є основною причиною більш ніж 80% усіх компрометацій даних через слабкі або вкрадені паролі.

Цей метод може використовувати як ручні, так і автоматизовані засоби для атак на корпоративні мережі, зокрема з використанням ботнетів. Якщо компанії не впроваджують двофакторну автентифікацію або складні паролі, їх системи стають більш вразливими до таких атак. Окрім того, використання спеціальних програмних інструментів для брутфорс-атак значно пришвидшує процес підбору паролів.

Атаки методом брутфорсу є однією з найефективніших і найчастіше використовуваних тактик зловмисників для отримання несанкціонованого доступу до систем. Основний принцип таких атак полягає в автоматичному переборі можливих паролів або ключів до тих пір, поки не буде знайдено правильну комбінацію.

Варто зазначити, що **брутфорс** може бути двох видів:

- **Прямий** (класичний), коли програми перебирають усі можливі комбінації паролів.
- **Словниковий** — спрощений варіант, де атака базується на списках часто вживаних паролів.

Якщо паролі не відповідають сучасним вимогам безпеки, атака методом брутфорсу може бути здійснена досить швидко. Наприклад, **короткі або прості паролі**, такі як "123456" або "password", можуть бути підібрані за лічені хвилини.

Для протидії таким атакам компаніям необхідно впроваджувати **складні паролі**, що включають великі й малі літери, цифри та спеціальні символи, а також використовувати **двофакторну аутентифікацію**. Крім того, важливо впроваджувати обмеження на кількість невдалих спроб входу в систему, що значно ускладнить зловмисникам проведення таких атак.

Захист від брутфорс-атак: Для зниження ризику атак методом брутфорсу рекомендується впровадження наступних заходів безпеки:

1. Використання складних паролів, що містять великі та малі літери, цифри та спеціальні символи.
2. Впровадження двофакторної автентифікації (2FA), яка забезпечує додатковий рівень безпеки, навіть якщо пароль було зламано.
3. Використання системи блокування облікових записів після декількох невдалих спроб входу.
4. Регулярне оновлення паролів та уникнення повторного використання одного і того ж пароля для різних облікових записів.

7. ВИСНОВКИ І ПРОПОЗИЦІЇ:

Впровадження комплексних систем захисту: Рекомендується використовувати багатошарові системи безпеки, включаючи фаєрволи, антивірусні програми та системи виявлення вторгнень.

Регулярне оновлення програмного забезпечення: Оновлення систем та програм до останніх версій для закриття вразливостей та запобігання їх експлуатації.

Створення планів реагування на інциденти:

Розробка і впровадження планів реагування: Важливо мати чіткий план дій у випадку атаки, який включає оперативні та юридичні кроки для мінімізації наслідків.

Моніторинг і аудит:

Регулярний моніторинг систем: Постійний моніторинг і аудит допоможуть виявляти і реагувати на загрози на ранніх стадіях.

Проведення навчання для персоналу: Навчання співробітників з питань кібербезпеки допоможе зменшити ризик зараження через людський фактор Для забезпечення ефективної кібербезпеки важливо використовувати багатошарові системи захисту, такі як фаєрволи, антивірусні програми та системи виявлення вторгнень. Оновлення програмного забезпечення до останніх версій є ключовим елементом, це допомагає закрити вразливості.

Список літератури:

[1] Symantec. (2019). Internet Security Threat Report. Symantec Corporation. URL: https://www.symantec.com.

[2] Verizon. (2020). Data Breach Investigations Report. Verizon Enterprise. URL: https://www.verizonenterprise.com/resources/reports/dbir/.

[3] Zeltser, L. (2018). Phishing Attacks: Defenses Against Social Engineering. SANS Institute.URL: https://www.sans.org.

[4] Ma, W., Campbell, K. (2020). Analysis of Vulnerabilities in Corporate Networks. Journal of Cybersecurity, Vol. 5, No. 3, 45-61. URL: https://www.journalofcybersecurity.com.

[5] Williams, P. (2017). Evaluating the Impact of WannaCry Ransomware on Global Businesses. Cybersecurity Review, 8(2), 92-102. URL: https://www.cybersecurityreview.com.

[6] National Institute of Standards and Technology (NIST). (2021). Cybersecurity Framework. NIST. URL: https://www.nist.gov/cyberframework.

[i] *Робота виконана під керівництвом к. т. н., доц. Євгенії Шабали*