УДК 004.056.5

А.В. Семенюк

ВИКОРИСТАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ ВІД ВЛПИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ПРИ КІБЕРАТАКАХ

Вінницький національний технічний університет

Анотація

Ця стаття розглядає використання методів машинного навчання та штучного інтелекту для захисту від впливу соціальної інженерії під час кібератак. Досліджується природа соціальної інженерії, види кібератак, їх цільова аудиторія та наслідки. В статті надається статистика випадків застосування соціальної інженерії та втрат, які зазнали жертви подібних кібератак. Особлива увага приділяється методам машинного навчання та штучного інтелекту як засобам захисту користувачів. Зроблено аналіз можливих застосувань цих технологій для протидії впливу соціальній інженерії.

Ключові слова: соціальна інженерія, кібератаки, машинне навчання, штучний інтелект, захист від кіберзлочинності.

Abstract

This article examines the use of machine learning and artificial intelligence techniques to protect against the effects of social engineering during cyberattacks. The nature of social engineering, types of cyberattacks, their target audience and consequences are investigated. The article provides statistics on cases of social engineering and losses suffered by victims of such cyberattacks. Special attention is paid to the methods of machine learning and artificial intelligence as means of protecting users. An analysis of the possible applications of these technologies to counter the influence of social engineering is made.

Key words: social engineering, cyberattacks, machine learning, artificial intelligence, cybercrime protection.

Вступ

Сучасний цифровий світ надзвичайно захоплюючий, але водночас і дуже небезпечний. Швидкий розвиток технологій та зростання комунікації через мережу Інтернет зробили нас вразливими перед новим видом загрози - кібератаками. Однією з найпоширеніших та найпідступніших технік кіберзлочинців є соціальна інженерія.

Соціальна інженерія - це мистецтво маніпулювання людьми з метою отримання конфіденційної інформації чи здійснення інших шкідливих дій. Використовуючи психологічні та соціальні методи, зловмисники намагаються отримати доступ до конфіденційної інформації або змусити жертву здійснити певні дії, які можуть викликати серйозні наслідки. З ростом популярності інтернету та залежності від цифрових технологій кількість випадків соціальної інженерії лише зростає, а зловмисники постійно вдосконалюють свої методи та стратегії.

Метою дослідження є розгляд використання методів машинного навчання та штучного інтелекту для захисту від впливу соціальної інженерії під час кібератак.

Об’єктом дослідження є кібербезпека та методи захисту від соціальної інженерії.

Предметом дослідження є використання методів машинного навчання та штучного інтелекту як засобів захисту від соціальної інженерії.

Головною задачею є визначення ефективних методів застосування машинного навчання та штучного інтелекту для виявлення та захисту від соціальної інженерії під час кібератак.

Види соціальної інженерії, що використовуються для кібератак

Розглянемо різні види соціальної інженерії, що використовуються для кібератак, разом з прикладами та цілями.

Фішинг електронною поштою:

- опис: зловмисник відправляє електронні листи, що виглядають як справжні листи від підприємств, банків або інших організацій з проханням надати конфіденційну інформацію або виконати певні дії;
- приклад: листи, що видаються як листи від банків, з проханням оновлення паролю або підтвердження ідентифікаційних даних;
- мета: отримання доступу до облікових даних, паролів або інших конфіденційних інформаційних ресурсів.

Активність у соціальних мережах та Інтернет-форумах:

- опис: зловмисники шукають особисту інформацію про потенційних жертв в соціальних мережах або на Інтернет-форумах, таку як дата народження, місце роботи, інтереси тощо, щоб використовувати цю інформацію для маніпулювання жертвою;
- приклад: використання інформації з профілю соціальних мереж для переконання жертви у підтвердженні різних транзакцій або наданні доступу до персональної системи;
- мета: здійснення шахрайських дій, отримання конфіденційної інформації або доступ до банківських рахунків.

Соціальний тиск:

- опис: зловмисники використовують тиск або вразливості(захоплення) жертви з метою здійснення певних дій, наприклад, надання доступу до системи або виконання фінансових операцій;
- приклад: вказівки на надійність або популярність діяльності, щоб спонукати жертву діяти без перевірки;
- мета: отримання доступу до конфіденційної інформації або здійснення фінансових операцій за рахунок жертви.

Співробітництво:

- опис: зловмисники використовують соціальні зв'язки або корпоративні відносини для отримання доступу до системи або інформації;
- приклад: використання довіри, яку мають співробітники(колеги) або члени родинного кола між собою для отримання доступу до конфіденційних даних;
- мета: отримання доступу до конфіденційної інформації або виконання шкідливих дій в корпоративній системі.

Ці види соціальної інженерії можуть призвести до втрати конфіденційної інформації, зупинки роботи підприємства, фінансових втрат або навіть до порушення репутації та втрати довіри.

Групи користувачів, які найбільш схильні до впливу соціальної інженерії здебільшого включають новачків, які є необізнаними в можливих техніках атак та мають низький рівень освіти в питаннях кібербезпеки, а також користувачів, які надмірно довіряють інформації, що надходить до них через соціальні мережі та електронну пошту.

Статистика кіберзлочинів з використанням соціальної інженерії

Соціальна інженерія є однією з найпоширеніших та найпідступніших технік кібератак, що використовуються зловмисниками. За даними досліджень, проведених у цій області, можна визначити масштаб проблеми та оцінити наслідки для потенційних жертв.

Ось деякі ключові статистичні дані щодо випадків застосування соціальної інженерії та втрат, які зазнали її жертви:

- за даними звіту Verizon 2019 року про кібербезпеку, майже половина збитків від кіберзлочинності в 2019 році були спричинені компрометацією електронної пошти, вони принесли шахраям 1,8 мільярда доларів США;
- у 2020 році IC3 повідомила про понад 240 000 індивідуальних жертв фішингу, яким завдали збитків понад 54 мільйони доларів США.

Найбільше від соціальної інженерії страждають як приватний бізнес, так і великі корпорації. Одна з основних причин полягає в тому, що зловмисники, отримавши доступ лише до одного корпоративного аккаунту, можуть отримати доступ до всієї системи в цілому. Це може включати доступ до конфіденційної інформації, клієнтських баз даних, фінансових ресурсів та інших важливих активів компанії. Такі атаки можуть призвести до серйозних втрат і пошкоджень, а також порушення довіри клієнтів та партнерів.

Ці статистичні дані свідчать про серйозність проблеми соціальної інженерії та її вплив на корпоративний та особистий сектори.

Застосування методів машинного навчання та штучного інтелекту для захисту від впливу соціальної інженерії

Сучасні технології штучного інтелекту та машинного навчання надають потужні інструменти для виявлення та захисту від атак з використанням соціальної інженерії.

Аналіз поведінки користувачів. Використання алгоритмів машинного навчання для аналізу типової поведінки користувачів у мережі може допомогти виявляти аномальні взірці, що можуть вказувати на спроби фішингу або інші види соціальної інженерії. Наприклад, можна вивчити звичайні патерни активності користувачів, їх звички у використанні електронної пошти чи соціальних мереж, щоб виявити несподівані зміни в їх поведінці, які можуть свідчити про потенційну атаку.

Фільтрація спаму та фішингових атак. Розширені алгоритми машинного навчання можуть використовуватися для автоматичного виявлення та блокування спаму та фішингових листів. Вони можуть аналізувати вміст листів, їх структуру, відправників та інші параметри, щоб відокремити справжні повідомлення від шкідливих. При цьому враховуються не лише текстові дані, а й прикріплені файли, відомості про адресу відправника та інші метадані.

Використання навчальних моделей для ідентифікації підозрілих повідомлень. Розвиток глибоких навчальних моделей може сприяти ефективному виявленню та класифікації підозрілих повідомлень, в тому числі спаму, фішингу, обманних схем тощо. Застосовуються методи, що базуються на аналізі тексту, зображень та інших характеристик повідомлень для автоматичного виявлення шкідливого контенту.

Моніторинг соціальних мереж. Аналіз текстових даних з соціальних мереж за допомогою методів обробки природної мови та машинного навчання може допомогти виявляти підозрілі активності, такі як спроби фішингу, обманні схеми або розповсюдження шкідливого контенту. Для цього можна використовувати методи моніторингу публічних обговорень, аналізу семантичного змісту повідомлень, виявлення незвичайних тенденцій тощо.

Створення систем виявлення інцидентів. Розробка систем виявлення інцидентів на основі аналізу журналів подій та моніторингу мережевого трафіку дозволяє вчасно виявляти та реагувати на потенційні загрози, пов'язані з соціальною інженерією. Ці системи можуть автоматично реагувати на підозрілу активність, блокуючи атаку або ізолюючи заражені ресурси для подальшого аналізу.

Ці інноваційні підходи до застосування машинного навчання та штучного інтелекту можуть допомогти підвищити рівень безпеки та захисту від соціальної інженерії в онлайн середовищі.

Висновки

У цій статті ми детально розглянули проблему соціальної інженерії в контексті кібербезпеки та розглянули різноманітні методи захисту від цієї загрози. Загалом, можна зробити наступні висновки:

Зростаюча загроза соціальної інженерії. Соціальна інженерія продовжує бути серйозною загрозою для користувачів та організацій, оскільки зловмисники намагаються використовувати соціальні та психологічні маніпуляції для отримання конфіденційної інформації.

Необхідність інноваційних рішень. Традиційні методи боротьби з цією загрозою часто виявляються недостатньо ефективними. Для успішного протистояння соціальній інженерії необхідно використовувати інноваційні підходи та передові технології, такі як машинне навчання та штучний інтелект.

Роль машинного навчання та штучного інтелекту: Машинне навчання та штучний інтелект можуть значно підвищити ефективність захисту від соціальної інженерії шляхом аналізу великих обсягів даних, виявлення аномалій та автоматизації процесів виявлення і реагування на загрози.

Необхідність комплексного підходу: Боротьба з соціальною інженерією вимагає комплексного підходу, який включає в себе не лише технічні заходи, але і навчання персоналу, вдосконалення процедур та регулярний аудит безпеки.

Постійний моніторинг та адаптація: Швидкість змін у методах атак соціальною інженерією вимагає постійного моніторингу та адаптації заходів захисту. Важливо не лише реагувати на існуючі загрози, але й передбачати майбутні тенденції та розробляти відповідні стратегії захисту.

Ці висновки підкреслюють необхідність постійного удосконалення заходів захисту від соціальної інженерії та важливість використання передових технологій у цій сфері.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Wikipedia (2023). "Соціальна інженерія". URL: https://uk.wikipedia.org/wiki/Соціальна_інженерія
2. Secureframe (2023). "60+ Social Engineering Statistics for 2023". URL: https://secureframe.com/blog/social-engineering-statistics
3. Crowdstrike (2023). "10 Types of social engineering attacks". URL: https://www.crowdstrike.com/cybersecurity-101/types-of-social-engineering-attacks/

Семенюк Андрій Васильович - Інститут докторантури та аспірантури, Вінницький національний технічний університет, м. Вінниця, e-mail: andrew.semeniuk.university@gmail.com

Semeniuk Andrew V. - Institute of doctoral and postgraduate studies, Vinnytsia National Technical University, Vinnytsia, e-mail: andrew.semeniuk.university@gmail.com