Міністерство освіти і науки України

СОЦІАЛЬНА ІНЖЕНЕРІЯ

Конспект лекцій
для здобувачів першого (бакалаврського) рівня вищої освіти
галузь знань 12 (F) Інформаційні технології
денної та заочної форм навчання

Луцьк 2025

УДК 004.056 (07)
С59

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № _____ від «_____» _____ 20___ року.

Голова вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № _____ від « _____» _____ 20____ року.

Завідувач кафедри КІБ _____ Тарас ТЕРЛЕЦЬКИЙ

Укладач: _____ Оксана МІСКЕВИЧ, старший викладач кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ Сергій ГРИНЮК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

С59 **Соціальна інженерія**: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти галузь знань 12 (F) Інформаційні технології денної та заочної форм навчання / уклад. О.І.Міскевич. Луцьк: ЛНТУ, 2025. 76 с.

Конспект лекцій з дисципліни «**Соціальна інженерія**» складений відповідно до діючої програми курсу.

Призначений для здобувачів вищої освіти галузі знань 12 (F) Інформаційні технології.

ЗМІСТ

ВСТУП

Навчальна дисципліна «Соціальна інженерія» формує у студентів психологічні аспекти та уміння, які необхідні для успішної боротьби з кібератаками Основними завданнями курсу є: вивчення та оволодіння основними концепціями, методами та напрямами соціальної інженерії.

Програма курсу розподілена на два змістовні модулі, що забезпечують поступове поглиблення знань від видів соціальної інженерії до заходів протидії соціальній інженерії.

Змістовий модуль 1 «Теоретико-методологічні основи соціальної інженерії» охоплює види соціальної інженерії, психологію та основні схеми впливу, збір інформації за допомогою соціальних мереж та пошукових систем, підбір облікових даних. Студенти вивчають аналізувати, як і чому відбувається збір інформації через соціальні мережі та пошукові системи, користуватися OSINT-даними.

Змістовий модуль 2 «Атаки соціального інженера та заходи протидії соціальній інженерії» присвячений поглибленому вивченню цілі атак соціальної інженерії: отримання конфіденційної інформації, отримання доступу до систем та ресурсів, маніпулювання користувачами. Вміти реагувати на інцидент та відновлення систем.

Курс спрямований на вивчення основних методів та технік соціальної інженерії та засобів захисту від соціальних атак, включаючи навчання користувачів та встановлення політик безпеки.

ТЕМА 1. ПРЕДМЕТ І ЗАВДАННЯ КУРСУ «СОЦІАЛЬНА ІНЖЕНЕРІЯ»

1.1 Що таке соціальна інженерія?

Соціальна інженерія стала невід'ємною частиною кібершахраїв. Мова йде про спеціальну методику маніпуляції, яка допомагає змусити людину віддати зловмисникам необхідні дані. Яким чином? Використовуючи людські слабкості: емоції та природну поведінку жертви.

Соціальна інженерія – це мистецтво маніпулювання користувачами обчислювальної системи з метою розкриття конфіденційної інформації, яка може бути використана для отримання несанкціонованого доступу до комп'ютерної системи. Термін також може включати такі дії, як використання людської доброти, жадібності та цікавості для отримання доступу до будівель з обмеженим доступом або спонукання користувачів до встановлення бекдорного програмного забезпечення – це шкідлива або прихована програма, яка створює «обхідний шлях» (бекдор, від англ. back door) для доступу до комп'ютера чи мережі в обхід стандартних механізмів автентифікації та захисту. Сьогодні існує чимало методів використання соціальної інженерії. В основі – маніпуляція людськими страхами, зацікавленістю або довірою. Жертвою соціальної інженерії можна стати як під час особистого спілкування, так і по телефону або через цифрові гаджети. Зловмисники можуть «маскуватися» під установи, яким довіряє людина.

Наприклад, прикидаючись представниками оператора мобільного зв'язку або працівниками банку, вони можуть надсилати електронні листи з додатком або посиланням, за яким людина має ввести свої особисті дані. Жертві також можуть додатково зателефонувати із проханням відкрити цей додаток або ж перейти за посиланням. Вважається, що таке «живе» спілкування додає ситуації чималої правдоподібності і зазвичай змушує людей відкривати вкладення.

Знання трюків, які використовують хакери, щоб оманою змусити користувачів оприлюднити життєво важливу інформацію для входу, є фундаментальним для захисту комп’ютерних систем.

1.2 Як працює соціальна інженерія?

Збір інформації: це перший етап, на якому людина дізнається якомога більше про заплановану жертву. Інформація збирається з веб-сайтів компаній, інших публікацій, а іноді й шляхом розмови з користувачами цільової системи.

План атаки: зловмисники описують, як він або вона збирається здійснити атаку Інструменти отримання: це комп’ютерні програми, які зловмисник використовуватиме під час атаки та цикл соціальної інженерії представлено на рисунку 1.

Атака: використовуйте слабкі місця цільової системи.

Використовуйте набуті знання. Інформація, зібрана під час тактики соціальної інженерії, як-от імена домашніх тварин, дати народження засновників організації тощо, використовується в атаках, наприклад підбір пароля.

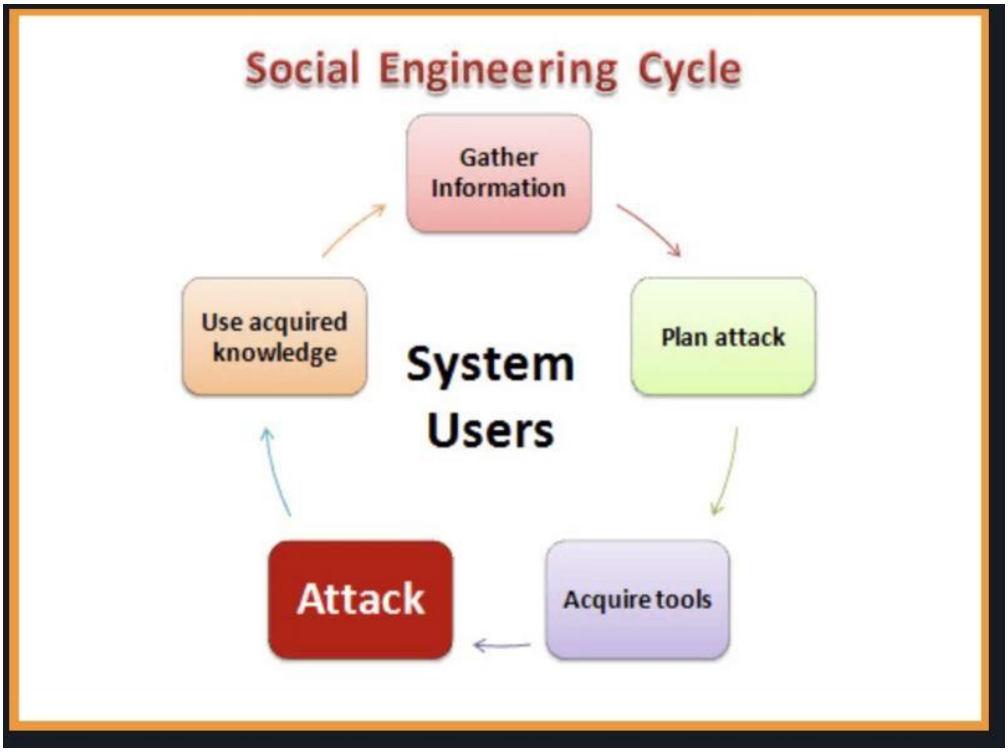

Рисунок 1.1 – Цикл соціальної інженерії

1.3 Поширені методи соціальної інженерії

Методи соціальної інженерії можуть приймати різні форми. Нижче наведено список поширених технік:

Експлойт знайомства: користувачі менш підозрілі щодо знайомих їм людей. Зловмисник може ознайомитися з користувачами цільової системи до атаки соціальної інженерії. Зловмисник може взаємодіяти з користувачами під час їжі, коли користувачі курять, він може приєднатися, на соціальних заходах тощо. Це робить зловмисника знайомим користувачам. Припустімо, що користувач працює в будівлі, яка вимагає код доступу або картку для отримання доступу; зловмисник може стежити за користувачами, коли вони заходять у такі місця. Користувачі найбільше люблять тримати двері відкритими, щоб зловмисник зайшов, оскільки вони знайомі з ними. Зловмисник також може запитати відповіді на запитання, наприклад, де ви познайомилися зі своєю дружиною, ім’я вашого вчителя математики в середній школі тощо. Користувачі, швидше за все, розкриють відповіді, оскільки довіряють знайомому обличчю.

Обставини , що лякають: люди, як правило, уникають людей, які лякають оточуючих. Зловмисник може прокинутися, що свариться по телефону, а насправді говорити зі спільником. Потім зловмисник може запитати у користувачів інформацію, яка буде використана для порушення безпеки системи користувачів. Користувачі, швидше за все, дають правильні відповіді, щоб уникнути конфронтації з зловмисником. Цей прийом також можна використовувати, щоб уникнути перевірки на контрольно-пропускному пункті.

Фішинг: ця техніка використовує хитрість і обман для отримання особистих даних від користувачів. Соціальний інженер може спробувати видати себе за справжній веб-сайт, а потім попросити нічого не підозрюючого користувача підтвердити ім’я облікового запису та пароль. Цю техніку також можна використовувати для отримання інформації про кредитну картку або будь-яких інших цінних особистих даних.

Переслідування : ця техніка передбачає стеження за користувачами позаду, коли вони входять у заборонені зони. З людської ввічливості користувач, швидше за все, впустить соціального інженера в зону обмеженого доступу.

Експлуатація людської цікавості : використовуючи цю техніку, соціальний інженер може навмисно кинути заражений вірусом флеш-диск у місце, де користувачі можуть легко його підхопити. Користувач, швидше за все, підключить флешку до комп'ютера. Флеш-диск може автоматично запускати вірус, або користувач може спробувати відкрити файл із такою назвою, як Employees Revaluation Report.docx, який насправді може бути зараженим файлом.

Експлуатація людської жадібності: використовуючи цю техніку, соціальний інженер може заманити користувача обіцянками заробити багато грошей в Інтернеті, заповнивши форму та підтвердивши свої дані за допомогою даних кредитної картки тощо.

Загроза безпеці визначається як ризик, який потенційно може завдати шкоди комп'ютерним системам і організації. Причина може бути фізичною, наприклад хтось викраде комп'ютер, який містить важливі дані. Причина також може бути нефізичною, наприклад вірусна атака.

Фізична загроза є потенційною причиною інциденту, який може призвести до втрати або фізичного пошкодження комп'ютерних систем.

У наведеному нижче списку фізичні загрози класифікуються за трьома основними категоріями;

Внутрішні: загрози включають пожежу, нестабільне електропостачання, вологість у приміщеннях, де розміщено обладнання тощо.

Зовнішні: ці загрози включають блискавку, повені, землетруси тощо.

Людина: ці загрози включають крадіжки, вандалізм щодо інфраструктури та/або обладнання, збої, випадкові чи навмисні помилки.

Щоб захистити комп'ютерні системи від вищезгаданих фізичних загроз, організація повинна мати засоби контролю фізичної безпеки. У наведеному нижче списку показано деякі з можливих заходів, які можна вжити:

Внутрішні: загрози пожежі можна запобігти, використовуючи автоматичні пожежні сповіщувачі та вогнегасники, які не використовують воду для гасіння пожежі. Нестабільному електроживленню можна запобігти за допомогою контролерів напруги. Для регулювання вологості в кімнаті інформатики можна використовувати кондиціонер.

Зовнішні: системи блискавкозахисту можуть використовуватися для захисту комп'ютерних систем від таких атак. Системи блискавкозахисту не є ідеальними на 100%, але певною мірою вони зменшують ймовірність того, що блискавка завдасть шкоди. Розміщення комп'ютерних систем у високогір'ях є одним із можливих способів захисту систем від повеней.

Люди: таким загрозам, як крадіжка, можна запобігти, використовуючи замкнені двері та обмежений доступ до комп'ютерних кімнат.

Нефізична загроза є потенційною причиною інциденту, який може призвести до: втрати або пошкодження системних даних; порушити бізнес-операції, які покладаються на комп'ютерні системи; втрати конфіденційної інформації; незаконного моніторингу діяльності в комп'ютерних системах; порушенню кібербезпеки та інші.

Нефізичні загрози також відомі як логічні загрози. Нижче наведено список поширених типів нефізичних загроз:

– вірус;
– трояни;
– черви;
– шпигунське програмне забезпечення;
– ключові реєстратори;
– рекламне ПЗ;
– атаки на відмову в обслуговуванні;
– розподілені атаки на відмову в обслуговуванні;
– несанкціонований доступ до ресурсів комп'ютерної системи, таких як дані Фішинг;
– інші ризики комп'ютерної безпеки.

Щоб захистити комп’ютерні системи від вищезгаданих загроз , організація повинна мати логічні заходи безпеки. У наведеному нижче списку показано деякі можливі заходи, які можна вжити для захисту від загроз кібербезпеці.

Для захисту від вірусів, троянів, хробаків тощо організація може використовувати антивірусне програмне забезпечення. Крім антивірусного програмного забезпечення, організація також може контролювати використання зовнішніх пристроїв зберігання даних і відвідування веб-сайтів, які швидше за все, завантажують неавторизовані програми на комп’ютер користувача.

Несанкціонований доступ до системних ресурсів комп’ютера можна запобігти за допомогою методів автентифікації. Методами автентифікації можуть бути ідентифікатори користувачів і надійні паролі, смарт-карти або біометричні дані тощо.

Системи виявлення або запобігання вторгненням можна використовувати для захисту від атак на відмову в обслуговуванні. Існують також інші заходи, які можна застосувати, щоб уникнути атак на відмову в обслуговуванні.

1.4 Протидія соціальної інженерії

Більшість методів, які використовують соціальні інженери, передбачають маніпулювання людськими упередженнями . Щоб протистояти таким методам, організація може:

Щоб протистояти експлойт знайомствам, користувачів потрібно навчити не нехтувати заходами безпеки при знайомствах. Навіть люди, з якими вони знайомі, повинні довести, що вони мають дозвіл на доступ до певних областей та інформації.

Щоб протистояти атакам залякування обставин, користувачі повинні бути навчені визначати методи соціальної інженерії, які виловлюють конфіденційну інформацію, і ввічливо відмовляти.

Щоб протистояти методам фішингу, більшість сайтів, використовують безпечні з’єднання для шифрування даних і доведення, що вони є тими, за кого себе видають. Перевірка URL може допомогти вам виявити підроблені сайти.

Уникайте відповідей на електронні листи з проханням надати особисту інформацію.

Щоб протистояти небезпечним атакам, користувачі повинні бути навчені не дозволяти іншим використовувати їхній дозвіл безпеки для отримання доступу до зон обмеженого доступу. Кожен користувач повинен використовувати власний дозвіл доступу.

Щоб протистояти людській цікавості , краще надати підібрані флеш- диски системним адміністраторам, які мають перевірити їх на наявність вірусів чи іншої інфекції, бажано на ізольованій машині.

Щоб протистояти методам, які використовують людську жадібність, співробітники повинні бути навчені щодо небезпеки попадання на такі шахрайства.

Контрольні питання

1. Що таке соціальна інженерія у контексті інформаційної безпеки?
2. У чому полягає основна мета соціального інженера?
3. Чим соціальна інженерія відрізняється від технічних атак?
4. Які задачі вирішує соціальна інженерія у сфері кібербезпеки?
5. Наведіть приклади типових методів соціального впливу, що використовуються в атаках.
6. Які етичні обмеження існують у дослідженні соціальної інженерії?

Література : [1], [2], [3].

ТЕМА 2. ВИДИ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Види атак
2.2 Соціальна інженерія в різних сферах життя

2.1 Види атак

Атаки соціальної інженерії можуть проявлятися в різних формах, маніпулюючи довірою та незнанням людей для доступу до конфіденційної інформації або систем. Розглянемо кілька найпоширеніших типів атак: фішинг, претекстинг, бейтинг, quid pro quo, tailgating і так далі.

Фішинг

Фішинг — це одна з найбільш поширених форм атак соціальної інженерії, при якій зловмисники видають себе за легітимні організації або осіб, щоб обманом змусити людей надати особисті дані, такі як паролі, банківські реквізити або іншу конфіденційну інформацію. Найчастіше фішинг відбувається через електронну пошту, фальшиві вебсайти, телефонні дзвінки або навіть соціальні мережі.

Електронна пошта: Зловмисники часто надсилають електронні листи, які виглядають як повідомлення від банків або популярних сервісів, пропонуючи «оновити» дані або змінити пароль.

Телефонні дзвінки: Шахраї можуть телефонувати, представляючись працівниками служби безпеки, і переконувати жертву розкрити паролі або коди доступу.

Соціальні мережі: Фальшиві повідомлення через соцмережі можуть спонукати користувачів перейти на підроблені сторінки для входу в акаунти.

Претекстинг

Претекстинг — це метод соціальної інженерії, коли зловмисник вигадує правдоподібну історію або «претекст» для отримання важливої інформації. В корпоративному середовищі це може бути хтось, хто видає себе за представника служби підтримки або юриста, щоб отримати доступ до даних компанії. Наприклад, зловмисник може звернутися до співробітника компанії,

представляючись IT-спеціалістом, який потребує доступу до робочого комп’ютера, нібито для «оновлення системи».

Бейтинг (Baiting)

Бейтинг – це атака соціальної інженерії, яка ґрунтується на викликанні у жертви цікавості або жадібності. Зловмисники “заманюють” людину, пропонуючи щось привабливе, що насправді є пасткою.

Цифровий бейтинг: Один із класичних прикладів – це пропозиція завантажити безкоштовну програму або файл, який насправді містить шкідливе програмне забезпечення.

Фізичний бейтинг: Також поширеним є використання заражених USB-накопичувачів, які залишають у публічних місцях, сподіваючись, що хтось підключить їх до свого комп’ютера.

Quid Pro Quo

Quid pro quo в перекладі з латини означає «послуга за послугу». У контексті соціальної інженерії це коли зловмисник пропонує жертві щось в обмін на важливу інформацію або доступ до системи. Приклад: Шахраї можуть видавати себе за співробітників техпідтримки та пропонувати «допомогу» в обмін на доступ до робочого комп’ютера або навіть пропонувати вигадані призи або гроші в обмін на особисті дані.

Tailgating (Слідування за іншими)

Tailgating — це фізична атака, коли зловмисник проникає в захищені приміщення, слідуючи за співробітником, який має доступ. Зазвичай це відбувається в офісах, де є контроль доступу. Приклад: Зловмисник може підійти до входу в будівлю і, тримаючи в руках коробки або інший предмет, попросити співробітника “допомогти відкрити двері”. Таким чином він проходить у захищену зону без перевірки. Щоб уникнути такого сценарію, важливо наголошувати на суворому дотриманні політики фізичного доступу, встановлювати системи контролю входу і навчати співробітників не пропускати незнайомців без перевірки.

Смішинг (Smishing)

Смішинг — це форма фішингу, яка здійснюється через текстові повідомлення (SMS). Зловмисники відправляють повідомлення, що містять фальшиві посилання або прохання про особисту інформацію. Приклад: Ви можете отримати SMS нібито від банку з проханням підтвердити свої банківські дані за допомогою посилання.

Вішинг (Телефонне шахрайство)

Вішинг — це телефонна атака, коли зловмисник намагається обдурити людину, щоб отримати важливу інформацію або кошти. Цей метод часто використовується для фінансових шахрайств. Приклад: Шахрай може зателефонувати, представляючись співробітником банку, і просити підтвердити ваші паролі або пін-коди.

Spear Phishing

Spear Phishing — це цільова форма фішингу, при якій зловмисники створюють персоналізовані повідомлення, спрямовані на конкретну людину або організацію. Вони збирають інформацію про жертву з відкритих джерел (наприклад, соціальні мережі) для створення переконливих атак. Приклад: Атака може виглядати як особисте повідомлення від вашого керівника або колеги, з проханням про термінове завантаження документу, що містить шкідливе ПЗ.

Фальшивий антивірус

Цей вид соціальної інженерії полягає у використанні підробленого програмного забезпечення, яке видає себе за інструмент безпеки. Зловмисники переконують жертву встановити це ПЗ, стверджуючи, що воно допоможе захистити комп’ютер, але насправді воно є шкідливим. Приклад: Популярним методом є поява спливаючих вікон у браузері, які попереджають про «вірус» і пропонують завантажити «антивірусну програму».

Клон-фішинг

Клон-фішинг є різновидом фішингу, при якому зловмисник створює копію реального повідомлення або електронного листа, що раніше надходило до жертви, але додає шкідливі посилання або вкладення.

Ці кілька основних типів атак соціальної інженерії показують, як зловмисники використовують психологічні та поведінкові методи для отримання

доступу до інформації або систем. Важливо бути пильними, розуміти ризики та впроваджувати ефективні заходи для захисту як на особистому, так і на корпоративному рівні.

2.2 Соціальна інженерія в різних сферах життя

Соціальна інженерія впливає на багато аспектів сучасного життя, від кібербезпеки до політики, бізнесу та повсякденного життя. Атаки на основі соціальної інженерії, використовуючи людські емоції та слабкості, можуть бути надзвичайно ефективними, особливо якщо вони використовуються в різних контекстах.

Соціальна інженерія в кібербезпеці:

У сфері кібербезпеки соціальна інженерія є одним із найпотужніших інструментів для хакерів, оскільки вона дозволяє обійти технічні засоби захисту шляхом маніпуляцій з людьми. Навіть найкращі технологічні системи можуть виявитися вразливими через людський фактор. Замість того, щоб ламати складні системи захисту, соціальні інженери використовують методи маніпуляції для отримання паролів або доступу до інформації.

Соціальна інженерія в політиці:

Політичні кампанії стали мішенями соціальної інженерії, оскільки зловмисники можуть маніпулювати громадською думкою, поширюючи дезінформацію або використовуючи маніпуляції з виборчими даними. Сучасні технології дозволяють легко поширювати фейкові новини та викликати масові емоційні реакції серед виборців.

Соціальна інженерія в корпоративних структурах:

Великі корпорації часто стикаються з атаками соціальної інженерії через своїх співробітників. Зловмисники використовують методи, які змушують співробітників ненавмисно розголошувати конфіденційну інформацію або здійснювати дії, що загрожують безпеці компанії. Серед найпоширеніших методів – шахрайство з керівниками (CEO fraud), коли зловмисники видають

себе за високопосадовців компанії, або схеми з підробленими рахунками (invoice scams), коли компанії оплачують фальшиві інвойси.

Соціальна інженерія у повсякденному житті:

Соціальна інженерія може також проявлятися у повсякденному житті через шахрайства, спрямовані на окремих осіб, особливо на вразливі категорії населення, такі як літні люди. Шахраї використовують телефонні дзвінки, електронні листи та соціальні мережі для виманювання грошей або персональних даних. Зловмисники можуть телефонувати літнім людям і переконувати їх надати банківські реквізити або оплатити фальшиві рахунки за якісь послуги. Водночас через соціальні мережі поширюються повідомлення про фальшиві благодійні кампанії.

Отже, соціальна інженерія – це потужний інструмент, який використовують зловмисники для маніпуляцій людськими емоціями та поведінкою, обходячи технологічні засоби захисту. Ми розглянули основні види атак, такі як фішинг, претекстинг, бейтинг та інші, а також приклади використання соціальної інженерії у кібербезпеці, політиці, корпоративному середовищі та повсякденному житті. Для захисту від цих загроз важливо підвищувати обізнаність, навчатися розпізнавати шахрайські методи та впроваджувати найкращі практики безпеки як на особистому, так і на організаційному рівні.

Контрольні питання

1. Які існують класифікації соціальних атак?
2. Що означає термін «human firewall» і яку роль він відіграє у кіберзахисті?
3. У чому полягає небезпека фішингових атак?
4. Як захистити сайт від індексації конфіденційних даних?
5. Що таке фальшивий антивірус?
6. Наведіть приклади бейтингу.

Література : [1], [2], [5].

ТЕМА 3. ПСИХОЛОГІЯ ТА ОСНОВНІ СХЕМИ ВПЛИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1 Психологічні методи

Соціальні інженери використовують психологічні методи, щоб маніпулювати людськими емоціями та поведінкою, обманом змушуючи жертв розкривати конфіденційну інформацію або виконувати дії, які можуть поставити під загрозу їхні безпеку та дані. Розуміння таких методів є ключем до захисту як окремих осіб, так і організацій.

Використання людської природи: експлуатація емоцій страху, жадібності та терміновості.

Соціальні інженери часто маніпулюють базовими людськими емоціями, такими як страх, жадібність або відчуття терміновості. Ці емоції можуть призводити до необдуманих рішень, і саме на них орієнтуються зловмисники.

Наприклад:

Страх: люди можуть отримати телефонний дзвінок із загрозою штрафу або навіть арешту, якщо вони не нададуть певну інформацію.

Жадібність: зловмисники можуть обіцяти вигоду, наприклад, виграш великої суми грошей або цінного призу, якщо жертва надасть свої дані або оплатить «невелику» комісію. Це поширена схема в онлайн-шахрайствах з фальшивими лотереями чи акціями.

Терміновість: коли людину змушують діяти негайно, вона не встигає обдумати ситуацію. Наприклад, електронний лист із темою «Ваш обліковий запис буде заблоковано протягом 24 годин» змушує жертву швидко реагувати та діяти без перевірки правдивості інформації.

3.2 Побудова довіри для обману

Атаки соціальної інженерії часто базуються на створенні довіри. Зловмисники можуть використовувати різні психологічні тактики, щоб виглядати авторитетними або довіреними особами. До найпоширеніших методів належать:

Авторитети: зловмисники часто видають себе за представників влади, таких як поліцейські, судові виконавці або працівники банків. Цей авторитет викликає у жертви повагу або навіть страх, через що вона легше піддається маніпуляції.

Соціальний доказ: люди, як правило, довіряють тому, що «всі інші роблять». Наприклад, шахраї можуть посилатися на «відгуки» або «успіхи» інших людей, щоб переконати жертву слідувати їхнім інструкціям.

Підозрілі маркери що свідчать про небезпеку. Щоб уникнути потрапляння в пастку, важливо розпізнавати попереджувальні сигнали. Серед них:

– несподівані запити про надання конфіденційної інформації.

– використання терміновості або погроз.

– незвичні або недоречні питання від невідомих людей або організацій.

– найпоширеніші вразливості людей.

Найчастіше шахраї експлуатують такі людські риси:

– Довіра: Люди за своєю природою схильні довіряти іншим, особливо тим, хто здається авторитетним або компетентним.

– Цікавість: зловмисники можуть використовувати цікавість жертви, пропонуючи щось незвичайне або провокуючи завантажити незнайомий файл.

– Готовність допомагати: люди часто готові допомогти іншим, і це може бути використано шахраями. Наприклад, люди можуть надати доступ до будівлі або інформації, якщо їм здається, що хтось у біді.

Щоб уникнути потрапляння на гачок соціальних інженерів, слід:

1) навчати співробітників та себе: регулярні тренінги допомагають підвищити обізнаність про тактики шахраїв і способи їх розпізнання;

2) перевіряти джерела інформації: ніколи не розкривайте конфіденційні дані без ретельної перевірки, хто і для чого їх запитує;

3) не піддаватися емоціям: якщо хтось чинить на вас тиск або використовує емоції (страх, терміновість), зупиніться і подумайте перед тим, як діяти;

4) соціальна інженерія використовує природні людські емоції та риси для досягнення своєї мети, тому знання про її методи – це перший крок до ефективного захисту.

Соціальна інженерія ґрунтується на використанні психологічних слабкостей людини.

Зловмисники апелюють до:

– довіри (авторитет, схожість, «знайомі люди»);

– страху (покарання, втрата грошей, блокування акаунту);

– жадібності (легкі гроші, призи, виграші);

– допитливості (цікаві посилання, «таємна інформація»);

– поспіху та неуважності (терміновість, дедлайн);

– бажання допомогти (людська доброта, колективність);

– автоматичних звичок (звичка «клікати», вводити пароль без перевірки).

Згідно з дослідженнями, близько 95% кібератак стається через людські помилки або невміння розпізнавати соціальну інженерію. Шахрайські електронні листи або дзвінки стають дедалі реалістичнішими, і більшість жертв навіть не підозрюють, що їх обманюють, поки не стає надто пізно.

3.3 Приклади схем впливу

Створення терміновості – «Ваша картка буде заблокована через 30 хвилин!» Результат – Людина діє поспіхом, не перевіряючи правдивість.

Апеляція до авторитету – Зловмисник видає себе за начальника, банківського працівника, поліцію. Результат – Працює через повагу й страх перед владою.

Виклик страху або паніки – «Ваш акаунт зламано, введіть пароль для відновлення!» Результат – Людина втрачає раціональність і виконує вимоги.

Виклик довіри та симпатії – Фейковий «друг» у соцмережі, знайомство в чаті. Результат – Жертва сама ділиться даними.

Створення приманки – «Скачай безкоштовну програму/гру/фільм». Результат – Жертва отримує вірус разом із «подарунком».

Соціальна перевірка (social proof) – «Усі вже скористалися цим сервісом, приєднуйтесь!» Результат – Працює ефект натовпу.

Апеляція до жадібності/вигоди – «Ви виграли iPhone! Просто введіть дані картки». Результат – Використання бажання швидкого зиску.

Довгострокове маніпулятивне спілкування (pretexting) – Зловмисник поступово вибудовує контакт, отримуючи все більше даних.

Контрольні питання

1. Як соціальний інженер може використати дані із соціальних мереж у своїй атаці?
2. Яким чином будується довіра для обману шахраями?
3. Що таке веб-шел?
4. Хто такий «інсайдер» у контексті кібербезпеки?
5. Як організація може швидко виявити підозрілу поведінку співробітника?
6. Що робити після інциденту, пов’язаного з інсайдером?
7. Назвіть приклади схем впливу?

Література : [1], [2], [12].

ТЕМА 4. ЗБІР ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ СОЦІАЛЬНИХ МЕРЕЖ ТА ПОШУКОВИХ СИСТЕМ

4.1 Основні компоненти розвідки на основі відкритих джерел (OSINT)

Простими словами, Розвідка на основі відкритих джерел (OSINT) – це мистецтво пошуку та аналізу корисної інформації у загальнодоступних ресурсах, як-от інтернет-сторінки, газети чи соціальні мережі.

Виникнення та еволюція розвідки на основі відкритих джерел (OSINT)

Розвідка на основі відкритих джерел (OSINT), відома своєю глибокою історією, і сягає корінням до часів, коли інформація збиралася переважно з друкованих медіа, таких як газети та журнали. Її еволюція відбувалася паралельно зі зростанням та розширенням доступу до інформації, перетворюючи OSINT з простого збору даних у складний аналітичний процес. Наприклад, в період холодної війни, OSINT стала ключовим інструментом у сфері розвідки, дозволяючи аналізувати відкриті джерела для отримання інформації про військові можливості та політичні стратегії противника.

Справжній розквіт OSINT припав на еру цифрових технологій. Інтернет, соціальні медіа, онлайн-бази даних стали неоціненним джерелом інформації. Технологічний прогрес зробив OSINT надзвичайно динамічною та мінливою областю, де інструменти та методи аналізу постійно оновлюються та вдосконалюються. Наприклад, використання великих даних (Big Data) та штучного інтелекту відкрило нові горизонти для аналізу та інтерпретації обсягів інформації, які раніше були недосяжними.

У світлі цього неперервного розвитку, OSINT трансформувалася з простого збору відкритої інформації у сферу, яка використовує складні аналітичні засоби для виявлення, аналізу та інтерпретації даних на новому рівні

глибини та точності. Від журналістських розслідувань до державної безпеки, OSINT продовжує відігравати ключову роль у формуванні сучасного розуміння світу, підкреслюючи цінність відкритої інформації у суспільстві.

До основних та самих дієвих способів отримання інформації з відкритих джерел можна віднести наступне:

1) Публічні реєстри, надаючи доступ до офіційних документів, таких як судові рішення, державні звіти та тендери, патенти та інші урядові записи, є критично важливими для OSINT. Ці джерела дозволяють розслідувачам збирати авторитетні та достовірні дані, які можуть використовуватися для створення повної та точної картини якоїсь ситуації або суб'єкта. Важливість цих документів полягає у їхній офіційності та загальнодоступності, що робить їх надійними джерелами для аналітичної роботи.

2) Медіа — це вікно у світ для OSINT-аналітиків. Традиційні медіа, такі як газети та телебачення, давно використовуються для збору інформації, але цифрова ера значно розширила можливості цієї сфери. Новинні онлайн платформи, блоги, телеграм канали стали цінними джерелами для OSINT. Цифрові медіа дозволяють швидко отримувати оновлення та мають ширше охоплення подій, що забезпечує більшу гнучкість та оперативність у зборі даних.

3) Інтернет-ресурси, включаючи соціальні мережі, форуми та вебсайти, є невід'ємною частиною OSINT. Соціальні мережі, як-от Facebook чи Twitter надають доступ до величезної кількості інформації, яка може використовуватися для відстеження трендів та настроїв, а також для збору даних про окремих осіб чи організації. Форуми та спеціалізовані вебсайти дозволяють аналітикам заглиблюватися в специфічні теми або спільноти. Ці інтернет-джерела не лише забезпечують широкий спектр інформації, але і є динамічними та постійно оновлюються, що робить їх незамінними для сучасної OSINT.

4) Супутникові знімки стали одним із найбільш вражаючих та ефективних інструментів у репертуарі OSINT. Завдяки супутникам, аналітики мають можливість спостерігати за змінами на поверхні Землі, відстежуючи такі події, як військові пересування, зміни в міському плануванні, навіть екологічні зміни. Такі компанії, як DigitalGlobe (тепер частина Maxar Technologies), надають

високоякісні зображення, які можуть використовуватися для детального аналізу віддалених або важкодоступних локацій. Супутникові знімки особливо цінні в ситуаціях, де збір інформації на місці є неможливим чи небезпечним, надаючи унікальну можливість «бачити» з висоти пташиного польоту.

4.2 OSINT у різних сферах життя

Кожна з наступних сфер демонструє унікальні можливості та переваги, які OSINT пропонує, від військових операцій до комерційного аналізу та академічних досліджень, підкреслюючи її важливість та універсальність у сучасному світі.

Уряди та військові підрозділи активно використовують OSINT для забезпечення національної безпеки. Яскравим прикладом цього є застосування OSINT українськими військовими та розвідувальними службами під час Російсько-Української війни. Використовуючи відкриті джерела, такі як супутникові знімки, соціальні мережі та новинні ресурси, українські військові змогли ефективно ідентифікувати та аналізувати переміщення та активності ворожих військ, що істотно сприяло плануванню оборонних та контрнаступальних дій. Використання OSINT в такому контексті демонструє його критичну роль у сучасній військовій стратегії та обороні країни.

У сфері бізнесу OSINT використовується для збору конкурентної розвідки. Наприклад, компанії, як-от Coca-Cola, використовують OSINT для відстеження трендів ринку, конкурентних дій та змін у споживацьких настроях, щоб краще позиціонувати свої продукти та стратегії.

У журналістиці OSINT використовується для проведення глибоких розслідувань. Один з найвідоміших прикладів — розслідування збиття Росією рейсу MH17 (Boeing 777) в Україні, проведене журналістами Bellingcat. Вони активно використовували відкриті джерела, такі як соціальні медіа, супутникові знімки, та інші інтернет-ресурси, для збору важливих доказів. Це розслідування надало ключову інформацію для міжнародного суду, ілюструючи роль OSINT у виявленні істини та сприянні справедливості в глобальному масштабі.

У академічному світі та наукових дослідженнях OSINT використовується для збору даних та аналізу тенденцій. Наприклад, університети часто використовують OSINT для дослідження глобальних соціально-економічних тенденцій, політичних рухів, екологічних змін тощо, залучаючи відкриті джерела для збагачення своїх наукових робіт.

Бізнес-розвідка з відкритих джерел (OSINT) є невід'ємною частиною сучасної стратегії інформаційного збору для бізнесу. Використання відкритих джерел даних, таких як інтернет, соціальні мережі, публічні бази даних і новинні портали, дозволяє компаніям отримувати цінну інформацію про своїх конкурентів, ринки, потенційних клієнтів та інші аспекти бізнесу. Метою бізнес-розвідки з відкритих джерел є збір, аналіз і інтерпретація різноманітних даних, що дозволяє підприємствам здійснювати обґрунтовані рішення, виявляти нові можливості та знижувати ризики. Це допомагає підприємствам отримати конкурентну перевагу, покращити стратегію маркетингу та збуту, виявити тенденції ринку та прогнозувати зміни в сфері бізнесу. Використання бізнес-розвідки з відкритих джерел вимагає високого рівня експертизи та спеціалізованих інструментів для збору та аналізу даних.

Важливо дотримуватись етичних норм і забезпечувати конфіденційність та захист особистої інформації. Завдяки бізнес-розвідці з відкритих джерел підприємства можуть ефективно аналізувати інформацію з публічних джерел та використовувати її для прийняття обґрунтованих рішень, що сприяє їхньому успіху та стійкому розвитку Використання бізнес-розвідки з відкритих джерел (OSINT) відкриває безліч можливостей для компаній будь-якого розміру. Завдяки доступності великого обсягу відкритої інформації, підприємства можуть отримувати цінні висновки та інсайти про своїх клієнтів, конкурентів та ситуацію на ринку. Метою бізнес-розвідки з відкритих джерел є збір інформації, яка допомагає уникнути непередбачених ризиків, виявити нові ринкові можливості, зрозуміти потреби та побажання споживачів, а також здійснювати ефективні маркетингові стратегії. Це дозволяє компаніям бути на крок попереду конкурентів і підтримувати свою конкурентоспроможність. Основними елементами бізнес-розвідки з відкритих джерел є пошук та збір інформації з веб-

сайтів, соціальних мереж, форумів, блогів та інших джерел, аналіз та інтерпретація отриманих даних. Використання спеціалізованих інструментів та технологій дозволяє автоматизувати процес збору та аналізу даних, що робить його більш ефективним та швидким. Основні категорії OSINT: бізнес, люди та інформація про кіберзагрози. А також деякі бізнес-інструменти OSINT для таких корисних завдань, як пошук імен керівників компаній, виявлення загальнодоступних файлів, збирання адрес електронної пошти та читання метаданих документів.

4.3 Практичне застосування: реальні приклади

Розвідка на основі відкритих джерел знайшла своє застосування у різних сферах життя, пропонуючи унікальні можливості для збору та аналізу інформації. Ось кілька конкретних прикладів, що показують, як OSINT впливає на різні аспекти нашого світу:

Компанія «IKEA» використовує OSINT для аналізу споживчих тенденцій та уподобань. Через моніторинг соціальних мереж, форумів та блогів вони адаптують свої продукти і маркетингові стратегії, щоб краще відповідати очікуванням клієнтів.

У 2020 році журналісти з The New York Times провели розслідування, використовуючи OSINT, щоб виявити та документувати випадки поліцейського насильства під час протестів Black Lives Matter у США. Вони аналізували відеоматеріали з соціальних мереж, щоб встановити хронологію та обставини інцидентів.

Вчені з Оксфордського університету використовували OSINT для вивчення впливу соціальних мереж на політичні процеси. Вони аналізували великі обсяги даних із соціальних медіа, щоб зрозуміти, як інформація поширюється серед користувачів.

Організація World Wildlife Fund (WWF) використовує OSINT для моніторингу незаконної торгівлі дикими тваринами. Аналізуючи онлайн-

маркетплейси та соціальні мережі, WWF збирає дані про нелегальну торгівлю, що сприяє боротьбі з цим явищем.

Під час пандемії COVID-19, дослідники з Університету Джонса Гопкінса розробили інтерактивну карту, що відстежує розповсюдження вірусу на глобальному рівні. Вони використовували OSINT для збору даних з офіційних медичних джерел та новинних агентств.

Human Rights Watch використовує OSINT для документування випадків порушень прав людини у конфліктних зонах. Зокрема, вони аналізують відеоматеріали, зроблені місцевими мешканцями, щоб виявити та документувати випадки насильства.

Активісти #MeToo використовують OSINT для виявлення та документування випадків сексуальних домагань. Вони аналізують свідчення, опубліковані в соціальних мережах, щоб підняти свідомість та підтримати жертв.

Ці приклади підкреслюють важливість OSINT як інструменту для різноманітних сфер, відкриваючи нові можливості для аналізу та збору інформації.

4.4 Інструменти та методології в OSINT

OSINT, або розвідка на основі відкритих джерел, використовує широкий спектр програмних інструментів та методологій для ефективного аналізу та збору інформації. Важливість штучного інтелекту в цьому процесі не можна недооцінювати, оскільки він дозволяє автоматизувати збір даних і підвищувати точність аналізу.

Програмні інструменти:

Maltego – це інструмент для візуалізації складних мереж зв’язків між людьми, організаціями, вебсайтами та соціальними мережами. Використання в OSINT: розслідувачі використовують Maltego для виявлення зв’язків між різними об’єктами, створення візуальних карти зв’язків, що допомагає у виявленні прихованих взаємозв’язків.

Shodan – це сервіс для пошуку пристроїв, підключених до інтернету, таких як камери, сервери та інші IoT-пристрої. Використання в OSINT: Розслідувачі використовують Shodan для ідентифікації вразливих пристроїв або систем, що можуть бути використані для кібератак або моніторингу.

Google Dorks – це техніка пошуку в Google, яка використовує спеціальні функції для фільтрації результатів та виявлення конкретної інформації. Використання в OSINT: застосування Google Dorks дозволяє OSINT розслідувачам швидко виявляти конкретну інформацію, таку як конфіденційні документи або специфічні дані.

TweetDeck– це платформа для моніторингу та управління декількома Twitter-акаунтами одночасно. Використання в OSINT: розслідувачі використовують TweetDeck для стеження за актуальними темами, хештегами, та активністю ключових осіб у Twitter.

Hunchly – це інструмент для автоматичного збору та документування інформації під час перегляду вебсторінок. Використання в OSINT: Hunchly допомагає розслідувачам вести облік переглянутих вебсторінок, зберігаючи важливі дані та запобігаючи необхідності повторного пошуку.

SpiderFoot – це автоматизований інструмент для збору великої кількості інформації з різних джерел. Використання в OSINT: SpiderFoot використовується для збору даних про IP-адреси, домени, особисту інформацію, виявлення цифрових слідів та з’ясування потенційних загроз.

Creepy – це інструмент для збору геолокаційної інформації з соціальних мереж. Використання в OSINT: розслідувачі використовують Creepy для відстеження розташування осіб чи подій на основі їх активності у соціальних мережах.

IntelTechniques – це набір інструментів для збору інформації з різних вебджерел. Використання в OSINT: IntelTechniques дозволяє збирати дані про осіб, адреси, телефонні номери тощо, сприяючи глибшому аналізу.

theHarvester – це інструмент для збору електронних адрес, імен доменів та іншої публічної інформації. Використання в OSINT: використовується для збору

контактних даних осіб або організацій, що може бути корисно при розслідуваннях.

Aircrack-ng – це набір інструментів для тестування безпеки Wi-Fi мереж. Використання в OSINT: розслідувачі використовують Aircrack-ng для виявлення вразливостей у бездротових мережах, що може сприяти збору важливої інформації.

4.5 Як стати OSINT розслідувачем: практичні поради та джерела знань

Стати OSINT розслідувачем – це захопливий шлях, що вимагає набуття спеціальних знань та навичок. Ось покроковий план для тих, хто бажає опанувати цю професію:

1. Основи інформаційної безпеки: розпочніть із вивчення основ інформаційної безпеки. Це допоможе зрозуміти, як захищати зібрану інформацію та ваші власні дані.
2. Ознайомлення з OSINT Інструментами: опануйте використання базових інструментів OSINT, таких як Maltego, Shodan, та Google Dorks. Практикуйтеся у використанні цих інструментів для збору даних.
3. Вивчення методологій: ознайомтеся з ключовими OSINT методологіями, такими як F3EAD та інші. Це допоможе систематизувати процес збору та аналізу інформації.
4. Розвиток аналітичних навичок: важливою частиною роботи OSINT розслідувача є здатність аналізувати та інтерпретувати зібрану інформацію. Працюйте над розвитком цих навичок.
5. Практичні заняття та курси: беріть участь у спеціалізованих OSINT курсах і воркшопах. Це дасть можливість отримати практичний досвід та глибше зрозуміння сфери.
6. Знання законодавства: ознайомтеся з законодавством, що регулює збір та використання інформації в Україні та інших країнах. Це важливо для законного ведення розслідувань.

7. Розвиток мережевих зв’язків: встановлюйте контакти з іншими фахівцями у галузі. Це дозволить обмінюватися досвідом, інформацією та методами роботи.

8. Постійне оновлення знань: технології та методи в OSINT постійно змінюються. Тому важливо регулярно оновлювати свої знання, слідкуючи за новинами галузі.

9. Практика та дослідження: практикуйте набуті навички, проводьте власні невеликі розслідування. Це допоможе закріпити знання та навички.

10. Етика та відповідальність: завжди пам’ятайте про етичні та правові аспекти при зборі та аналізі інформації. Ваша робота повинна відповідати високим моральним стандартам.

Контрольні питання

1. Які превентивні дії по прив’язці акаунтів соціальних мереж до поштових адрес ви можете порекомендувати?
2. Що таке «патерн» електронної пошти організації? Яким чином він може бути використаний зловмисником?
3. Які шляхи опосередкованого одержання приватної адреси особистості може використовувати соціальний інженер?
4. В чому є небезпека creeper ів в соціальних мережах?
5. Які дані профілю можуть бути використані соціальним інженером?
6. Що таке OSINT?
7. Які інструменти та методології в OSINT вам відомі?

Література : [2], [4], [11].

ТЕМА 5. ПІДБІР ТА ПІДМІНА ОБЛІКОВИХ ДАНИХ

5.1 Підбір облікових даних

Підбір скомпрометованих облікових даних (Credential Stuffing) – тип кібератаки, коли зловмисники використовують викрадені комбінації імен користувачів та паролів, часто внаслідок витоку даних, щоб отримати несанкціонований доступ до кількох облікових записів. Автоматизуючи спроби входу на різні сайти, зловмисники користуються повторним використанням паролів користувачів.

Підбір – це спроби вгадати правильні логін/пароль шляхом багаторазових переборів.

Є кілька підвидів:

— Brute-force (повний перебір) – послідовне випробовування великого простору паролів (рідко застосовується прямо через захисти, але може бути частиною атаки на слабкі паролі).

— Password spraying – атака, коли атакуючий пробує невелику кількість поширених паролів (напр., 123456, Password1) на велику кількість логінів, щоб уникнути блокувань.

— Targeted guessing – користується персональною інформацією (дати народження, імена домашніх тварин).

Мета: знайти правильний пароль/комбінацію для входу.

Індикатори: багато невдалих логінів з однієї IP або в межах одного аккаунта; зростання помилок авторизації; повторні блокування.

Захист: обмеження спроб входу, lockout, rate-limiting, CAPTCHA, 2FA, обмеження за IP/геолокацією, моніторинг аномалій.

5.2 Порівняння підбору облікових даних з іншими атаками

На відміну від брутфорс-атак, які систематично підбирають паролі, підбір облікових даних ґрунтується на відомих викрадених облікових даних. Зловмисники використовують ботнети або автоматизовані інструменти для перевірки цих облікових даних у різних сервісах, часто уникаючи виявлення через проксі-сервери або VPN.

Як працює підбір облікових даних?

Збір даних: зловмисники отримують викрадені облікові дані з витоків, часто доступні на нелегальних платформах.

Автоматизовані спроби входу: боти масово перевіряють облікові дані, щоб знайти достовірні збіги.

Експлуатація: отримавши доступ, зловмисники витягують цінні дані або монетизують скомпрометовані акаунти.

Реальні приклади:

— Yahoo (2014-2016): атаки підбору облікових даних призвели до порушень, які зачепили мільярди акаунтів.

— Amazon (2018): зловмисники намагалися здійснити несанкціоновані покупки, використовуючи викрадені облікові дані.

— Shopify (2020): зловмисники отримали доступ до облікових записів продавців, розкривши конфіденційні дані про транзакції.

Про ці та інші знакові витоки даних ви зможете знайти більше інформації за цим посиланням.

Чому зростає кількість атак з підбором облікових даних?

Часті витоки даних: дедалі більша кількість витоків надає зловмисникам величезні списки облікових даних.

Повторне використання паролів: багато користувачів продовжують використовувати одні й ті ж паролі на різних сайтах.

Розширена автоматизація: зловмисники використовують ботів для ефективного виконання масштабного тестування облікових даних.

Наслідки атак з підбором облікових даних

Фінансові втрати: несанкціоновані транзакції та шахрайство призводять до грошових збитків.

Крадіжка особистих даних: зловмисники отримують доступ до особистої інформації, що призводить до її неправомірного використання.

Пошкодження репутації: організації страждають від втрати довіри клієнтів та регуляторних санкцій.

Використання для подальших атак: скомпрометовані облікові дані використовуються для фішингу та схем соціальної інженерії.

Стратегії запобігання та захисту :

1. Багатофакторна автентифікація (MFA): додає додатковий рівень безпеки, окрім паролів.

2. Менеджери паролів: заохочують користувачів зберігати та генерувати унікальні паролі.

3. CAPTCHA та виявлення ботів: допомагає запобігти спробам автоматичного входу в систему.

4. Відбитки пальців і обмеження швидкості: виявляє та обмежує підозрілу поведінку при вході в систему.

5. Безпарольна автентифікація: зменшує залежність від традиційних паролів, мінімізуючи вектори атак.

Передові механізми захисту:

— Штучний інтелект і машинне навчання: виявляє підозрілі моделі поведінки в режимі реального часу.

— Шифрування та хешування: захищає збережені облікові дані від витоку.

— Постійна автентифікація: відстежує поведінку користувачів після входу в систему для виявлення аномалій.

Netwrix пропонує рішення з безпеки, включаючи виявлення загроз, впровадження паролів і поведінкову аналітику, для захисту від атак з підбору облікових даних і підвищення безпеки облікових записів.

Як, наприклад, Netwrix Auditor для AD/EntraID. Він допомагає з виявленням та усуненням критичних загроз безпеки, таких як слабкі паролі, або виявлення підозрілих подій входу в систему, які могли статися.

Отже, атаки з підбором облікових даних становлять загрозу кібербезпеці, яка активно зростає через широке розповсюдження повторного використання паролів та їх автоматизацію. Впровадження надійних заходів безпеки, таких як MFA та поведінкова аналітика, значно знижує ризик компрометації акаунтів. Варто бути пильними та використовувати найкращі практики для захисту своєї цифрової присутності.

5.3 Що таке «підміна облікових даних»

Термін «підміна» використовують у двох близьких значеннях, які часто плутають.

1. Credential stuffing (авторизація через повторне використання злитих паролів)

Атакувальники використовують бази злитих логінів+паролів (breach leaks) і автоматично «підставляють» ці комбінації на інших сайтах/сервісах, де жертва могла повторно використати пароль.

Мета: зайти, використовуючи валідні (але викрадені) облікові дані.

Відмінність від підбору: тут не вгадують — використовують вже відомі пари. Часто дуже швидко й масштабно (багато обліків перевіряються одночасно).

2. Підміна (заміна) облікових даних у акаунті жертви

Це коли нападник вже отримав доступ і змінює email/телефон/пароль (щоб «відрізати» власника від доступу).

Мета: утримати контроль, ускладнити відновлення доступу власником, підготувати подальший шахрайський сценарій.

Індикатори: власник не може зайти, приходять повідомлення про зміну паролю/пошти/реквізитів, незвичні «вихід з усіх сесій», змінені recovery-опції.

Атака з використанням облікових даних – це метод, коли кіберзлочинець застосовує набір викрадених логінів і паролів, щоб спробувати отримати доступ

до великої кількості облікових записів одночасно. Підміна облікових даних є надзвичайно ефективною, оскільки майже дві третини користувачів Інтернету повторно використовують свої паролі. Зловмисники вводять ці дані на тисячах сайтів протягом декількох хвилин або годин, скомпрометувавши все – від соціальних мереж до корпоративного ПЗ. Порівняльний аналіз аідміни та підбору представлений у таблиці 1.

Таблиця 5.1 – Порівняння підбору та підміни облікових даних

Аспект	**Підбір (guessing)**	**Підміна (credential stuffing / заміна)**
Джерело паролів	генеруються або вгадуються	використовуються попередньо вкрадені пари або вже має доступ
Шанс успіху	залежить від слабкості пароля	високий, якщо користувач повторно використовує пароль
Методи	brute-force, password spraying	автоматизовані скрипти + база злитих даних; після доступу — зміна рековері
Індикатори	багато невдалих входів	багато успішних логінів з різних IP; повідомлення про зміни акаунта
Захист	rate limiting, 2FA, CAPTCHA	2FA, блокування повторного використання паролів, моніторинг leaks

Різниця між підміною облікових даних і розпиленням паролів. На відміну від credential stuffing, розпилення паролів (password spraying) передбачає використання одного поширеного пароля для великої кількості акаунтів. При цьому перевіряється, чи підійде цей пароль до когось із користувачів. Якщо ж говорити про підміну облікових даних, то тут використовуються реальні злиті логіни та паролі, і атака спрямована саме на повторне використання одних і тих самих даних на різних ресурсах.

Кіберзлочинці, розраховуючи на звичку користувачів використовувати один і той самий пароль, можуть за допомогою всього одного набору облікових даних отримати доступ до всіх акаунтів людини. Часто для цього застосовуються BotNet-мережі, які атакують одночасно з кількох пристроїв, значно розширюючи масштаб вторгнення.

Наслідки таких атак. Якщо підміна облікових даних виявляється успішною, зловмисник потенційно отримує повний контроль над: банківською інформацією; акаунтами в соцмережах; поштою та іншими онлайн-сервісами.

Це може призвести до крадіжки грошей, шантажу, або навіть викрадення особистих даних з подальшим використанням у шахрайських схемах.

5.4 Як виявити атаку підміни облікових даних

Раннє виявлення дає змогу швидко зреагувати та захистити себе. Одна з перших ознак – несподівані повідомлення про вхід у ваші акаунти, особливо з незвичних пристроїв або локацій. Якщо ви отримали SMS із кодом підтвердження або електронний лист із повідомленням про вхід, якого ви не здійснювали – це вже тривожний сигнал.

Також важливо регулярно перевіряти історію входів у свої акаунти, особливо на поштових сервісах, у банкінгу та соціальних мережах. Незвичні IP-адреси, локації або часи активності можуть свідчити про спроби доступу.

Окремо варто згадати про сервіси моніторингу витоків даних, такі як Have I Been Pwned або внутрішні механізми браузерів (наприклад, Google Password Checkup), які сповіщають, якщо ваші облікові дані з’явились у злитих базах. Такі попередження – привід негайно змінити пароль і ввімкнути багатофакторну автентифікацію.

Для персональних користувачів. Один із найефективніших способів – використання багатофакторної автентифікації (MFA). Вона додає додатковий бар’єр до входу, вимагаючи, окрім пароля, ще один фактор: код із SMS, підтвердження в додатку або біометричний параметр. Якщо хтось намагається увійти у ваш акаунт, а ви отримуєте несподіваний код – це сигнал про потенційне вторгнення.

Для бізнесу. На підприємствах рекомендовано використовувати детектори аномалій трафіку з ботами, які відстежують незвичну активність і фіксують спроби підміни. Додатковий рівень безпеки – технології ідентифікації пристроїв:

визначення браузера, пристрою, IP-адреси, які допомагають виявити зловмисників до того, як буде здійснено реальний вхід.

Загалом, своєчасне реагування на підозрілу активність і використання сучасних засобів захисту допомагає звести до мінімуму ризики несанкціонованого доступу та зберегти контроль над своїми цифровими ресурсами.

Як розпізнати та запобігти атакам підміни облікових даних:

— Якщо бачиш багато неправильних спроб входу → підозра на підбір. Блокуй IP, включай CAPTCHA, застосуй rate limiting.

— Якщо сервер фіксує багато успішних входів із різних IP, особливо з незвичних локацій, та відразу зміну рековері → підміна/credential stuffing або повний takeover. Терміново: скинути паролі, відключити сесії, повідомити користувачів, включити 2FA.

— Якщо отримав повідомлення про зміну email/телефону – це критичний IOC: відновлюй через офіційні канали, звертайся в службу підтримки, змінюй паролі і перевіряй логи.

Захист повинен починатися з паролів. Встановлюйте надійні та унікальні паролі для кожного сервісу. Рекомендовано створювати комбінації щонайменше з 16 символів, що містять великі й малі літери, цифри та символи. Для цього зручно користуватися генераторами паролів, а для зберігання – менеджерами паролів, де ви зберігаєте всі дані під одним головним паролем.

Не менш важливо – ввімкнути MFA для всіх сервісів, де це можливо. Навіть якщо зловмисник дізнається ваш пароль, без другого фактора він не зможе отримати доступ до акаунта.

Захист користувача:

— Ніколи не повторно використовуй паролі.

— Використовуй менеджер паролів + унікальні паролі для кожного сервісу.

— Включай 2FA (аплікаційний або апаратний) – це суттєво знижує ризик і підбору, і підміни.

— Слідкуй за повідомленнями про витоки (HaveIBeenPwned), змінюй паролі при попаданні у leak.

— Налаштуй оповіщення про входи та зміни рековері.

Захист бізнесу від Credential Stuffing – компаніям варто не лише дбати про власний захист, а й забезпечити грамотне поводження з паролями з боку співробітників.

Основні кроки:

1. Використання менеджерів бізнес-паролів з централізованим управлінням.

2. Встановлення обов'язкової багатофакторної автентифікації.

3. Контроль дотримання політик безпеки з боку IT-відділу.

Такі інструменти дозволяють стежити за надійністю облікових даних та зменшують ризики скомпрометованих акаунтів.

5.5 Credential Stuffing – як хакери перевіряють логіни й паролі

На практиці credential stuffing дуже часто використовується як спосіб валідації злитих даних. Наприклад, як під час гучної атаки на Duolingo, де було злито дані понад 2,6 мільйона користувачів, зокрема номери телефонів. Зловмисники використали платформу не як головну ціль, а як засіб перевірки – чи ще діє логін і пароль із минулої бази витоку.

Коли система дозволяє такі атаки, під загрозою опиняються не лише цільові акаунти, а й сам ресурс. Боти створюють величезне навантаження, і сайт стає недоступним для справжніх користувачів.

Основні методи захисту від Credential Stuffing

Серед базових (але обов'язкових) заходів:

— CAPTCHA – перевірка на «людяність» користувача.

— Rate limits – обмеження кількості запитів за певний час.

— Геофільтрація – блокування IP з певних країн (не завжди ефективно через VPN).

— Блокування за IP – запобігає атакам з одного джерела, але не працює при розподілених атаках.

Отже можна зробити висновок, Credential Stuffing – це один із найбільш масових і небезпечних типів атак, який щороку набирає обертів. Надійні паролі, MFA, захищені платформи для зберігання облікових даних і пильність – ось головна зброя проти зловмисників. Розуміння механізму атаки – перший крок до її запобігання.

Контрольні питання

1. Що таке підбір облікових даних ?
2. Які види підбору Вам відомо?
3. Що таке підміна (заміна) облікових даних у акаунті жертви?
4. Як розпізнати та реагувати на підбір та підміну облікових даних?
5. Пояснити, як можна захиститися від підбору паролів.

Література : [1], [2], [3], [8].

ТЕМА 6. БЕКДОР У WINDOWS ТА ANDROID

6.1 Що таке бекдор?

Бекдор – це прихований спосіб доступу до комп'ютера або мобільного пристрою (Windows, Android), який дозволяє зловмиснику обходити стандартні засоби безпеки для віддаленого керування пристроєм. Він може бути встановлений у вигляді програми, руткіта або ж як початкові, невидалені функції налагодження, які можуть бути як ненавмисно створені, так і навмисно вбудовані розробником. Основне завдання – підтримувати зв'язок з атакуючим, якщо інші заблоковані.

1. Прихований доступ: це спеціально створений або випадково залишений «чорний хід» для несанкціонованого доступу до системи. Бекдор – це тип шкідливого програмного забезпечення або функціональність, яка забезпечує несанкціонований доступ до комп'ютера, мережі або програмного забезпечення.

2. Віддалене керування: бекдор дозволяє зловмиснику дистанційно керувати пристроєм, як якщо б він був його законним власником. Він дозволяє зловмисникам обходити стандартні процедури аутентифікації та безпеки, отримуючи доступ до системи, навіть якщо інші захисні механізми працюють

3. Непомітність: головна небезпека бекдору в тому, що він працює непомітно для звичайного користувача, залишаючись прихованим від антивірусних програм та системних перевірок. Бекдори можуть бути впроваджені у легітимне програмне забезпечення або існувати як окреме шкідливе програмне забезпечення.

Основні типи бекдорів:

— Програмні бекдори – встановлюються через шкідливе програмне забезпечення.

— Апаратні бекдори – впроваджуються на рівні апаратного забезпечення.

— Мережеві бекдори – відкривають порти або використовують протоколи доступу до мережі.

— Бекдори ПЗ – створюються зловмисно для доступу.

6.2 Як бекдори потрапляють у систему?

— Встановлення шкідливого ПЗ: бекдор може бути частиною шкідливої програми (наприклад, вірусу чи трояна), яка інфікує пристрій, як пояснюють експерти з кібербезпеки. Через фішинг зловмисник надсилає шкідливе програмне забезпечення у вигляді електронної пошти.

— Руткіти: це спеціальні програми, що приховують свій власний код і дії від системних інструментів, включаючи антивіруси.

— Невидалені функції налагодження: деякі функції, що використовуються розробниками для налагодження, можуть бути залишені у фінальній версії програми та стати бекдором.

— Слабка автентифікація: іноді бекдором може слугувати початковий пароль, який користувач так і не змінив.

— Користувачі несвідомо встановлюють шкідливе програмне забезпечення.

Як працює бекдор?

— Бекдор часто працює в фоновому режимі, непомітно для користувача.

— Він може зберігатися в системі після перезавантаження або оновлення, якщо його не видалити.

Зловмисники використовують бекдори для:

— Отримання доступу до конфіденційної інформації.

— Встановлення іншого шкідливого програмного забезпечення.

— Вчинення інших шкідливих дій.

Захист від бекдорів:

— Оновлення: регулярно оновлюйте операційну систему та всі програми, оскільки оновлення часто містять патчі безпеки, які усувають відомі бекдори.

— Антивірус: використовуйте надійне антивірусне програмне забезпечення і регулярно скануйте ним пристрій.

— Обмеження доступу: уникайте завантаження файлів з невідомих джерел, не переходьте за підозрілими посиланнями та не відкривайте вкладення в електронних листах від невідомих відправників.

— Навчайте співробітників: пояснюйте, що таке фішинг і як його уникнути.

— Використовуйте міжмережевий екран (Firewall) – він блокує різноманітні спроби та заважає зловмисникам отримати доступ.

6.3 Приклади бекдорів

1. Вбудовані бекдори: деякі функції налагодження або початкові паролі можуть служити бекдорами, якщо їх не видалити або не змінити.
2. Шкідливе програмне забезпечення: бекдори можуть бути частиною вірусів, троянів або інших шкідливих програм.
3. Вразливості в програмному забезпеченні: бекдори можуть використовувати слабкі місця в мережевих або файлових системах.
4. Бекдори у Windows та Android: у Windows та Android бекдори можуть бути впроваджені як у системні файли, так і в програми.

Одними з найвідоміших атак з використанням бекдорів були атаки, які здійснювала група кіберзлочинців TeleBots. Зловмисники стали відомими завдяки глобальному поширенню NotPetya – загрози, яка спричинила збитки в розмірі мільярдів доларів США.

Win32/Industroyer – одна з найбільш відомих загроз, яку створила група. Основним компонентом цього шкідливого ПЗ, призначеного для підриву важливих промислових процесів, був бекдор. Він використовувався

кіберзлочинцями для управління атакою та міг встановлювати і контролювати інші компоненти. Також він підключався до віддаленого серверу для отримання команд та надання інформації зловмисникам.

У квітні 2018 року спеціалісти ESET виявили бекдор групи TeleBots – Exaramel. Код циклу команд і реалізацій деяких з них дуже схожий з тими, що використовувались в загрозі Industroyer.

SolarWinds у 2020 році зловмисники використали для доступу у державні установи США.

BackOrifice був із перших бекдорів, який керував віддалено у Windows.

Зловмисники можуть використовувати бекдори для отримання доступу до особистих даних, контролю над пристроєм або для розповсюдження шкідливого програмного забезпечення.

Для захисту від бекдорів важливо використовувати антивірусне програмне забезпечення, регулярно оновлювати систему та програми, а також уникати завантаження та встановлення програм з ненадійних джерел.

Важливо пам'ятати, що бекдори можуть бути дуже складними для виявлення, тому важливо бути обережним та використовувати надійні засоби захисту.

6.4 Бекдорне програмне забезпечення та його основні характеристики

Бекдорне програмне забезпечення (Backdoor software) – це шкідлива або прихована програма, яка створює «обхідний шлях» (бекдор, від англ. *back door*) для доступу до комп’ютера чи мережі в обхід стандартних механізмів автентифікації та захисту.

Основні характеристики бекдорного ПЗ:

— Прихований доступ: зловмисник може керувати системою дистанційно без відома користувача.

— Обхід захисту: не потребує звичайного логіну/пароля чи дозволів.

— Функціонал: дає змогу зчитувати/змінювати дані, встановлювати інше шкідливе ПЗ, запускати програми, перехоплювати трафік.

— Способи проникнення: може бути вбудованим у легальне ПЗ, потрапляти через віруси, трояни або після злому системи.

Приклад: хакер встановлює бекдор на заражений комп'ютер і згодом може підключатися до нього як «адміністратор», навіть якщо користувач змінив паролі.

Небезпека бекдорів:

— Витік персональних даних.

— Використання комп'ютера у ботнетах.

— Повний контроль над системою сторонніми особами.

Експлойт (Exploit) – це спеціальна програма, скрипт або набір команд, які використовуються для зловживання вразливістю у програмному забезпеченні, операційній системі чи мережевому сервісі з метою отримання несанкціонованого доступу або виконання шкідливих дій.

Основні характеристики експлойта:

— Використовує помилку, недоопрацювання чи слабке місце в програмі.

— Може застосовуватися як хакерами, так і спеціалістами з кібербезпеки (для тестування).

— Часто стає основою для створення шкідливого ПЗ (наприклад, вірусів чи троянів).

Види експлойтів:

1. Локальні – працюють лише тоді, коли зловмисник уже має доступ до системи (наприклад, підвищення привілеїв).

2. Віддалені – дають змогу атакувати комп'ютер через мережу чи інтернет.

3. Zero-day (нульового дня) – використовують ще невідомі вразливості, для яких немає виправлень.

Наслідки застосування експлойта:

— Виконання шкідливого коду.

— Отримання доступу до даних або системи.

— Встановлення бекдорів чи вірусів.

Приклад: експлойт може використати вразливість у веб-браузері, щоб завантажити та запустити шкідливий код без відома користувача.

6.5 Масштаб мобільних загроз

Домінуюче шкідливе програмне забезпечення: трояни, які зосереджують переважну більшість мобільних шкідливих програм (понад 95%).

Банківська справа та шахрайство: практично всі атаки на мобільний банкінг спрямовані на пристрої Android, яким сприяє їхня частка ринку та можливість бічне завантаження.

Шахрайство та фішинг: кампанії фішинг, смайлінг а шахрайство в соціальних мережах вимагає отримання облікових даних та даних.

Витоки та нульовий день: прогалини від груба сила, інсайдери або вразливості нульовий день експлуатовано до виходу патчу; інструменти для дізнатися, чи ваш телефон був зламаний допомога у виявленні.

Інтернет речей та поверхня атаки: оркестровий телефон гаманці, пов'язані з домом та роботою, що збільшує ризик.

Бекдор на Android: бекдор, про який вам слід знати, і як захистити себе:

— Бекдор забезпечує прихований, постійний доступ до пристрою та координує роботу із серверами C2.

— Він поширюється через модифіковані програми, маніпульовані пристрої та трояни RAT з модулями на вимогу.

Це дозволяє використовувати програми-вимагачі, крадіжку даних, ботнети та криптоджекінг без відома користувача.

Захист: програми з перевірених джерел, патчі, двофакторна аутентифікація (2FA), захист від шкідливого програмного забезпечення та придбання сертифікованого обладнання.

Вразливості iPhone проти шкідливого програмного забезпечення Android: зловмисники віддають перевагу Android через його масштабованість та відкритість, тоді як iOS вирізняється своєю більш контрольованою, але не надійною екосистемою.

Більшість мобільних шкідливих програм є троянами; оновлення, обмеження дозволів та запобігання завантаженню несанкціонованих програм значно знижують ризик.

У підприємствах MDM, Apple Business Manager та Android Enterprise є ключовими для шифрування, політик та видимості.

Ефективна безпека поєднує дизайн платформи, швидке встановлення патчів та звички користувачів з автентифікацією та верифікацією додатків.

IOS (контрольована екосистема): App Store з суворим оглядом, шифрування за замовчуванням, пісочниця, підпис коду, та такі елементи, як Безпечний анклав, Face ID та Touch ID. Детальні дозволи та розподіл швидкі та одночасні оновлення на сумісні пристрої. У свою чергу, користувач має менше можливостей для налаштування.

Android (відкритість та різноманітність): платформа з відкритим кодом з широкою екосистемою виробників. Багаторівнева безпека: Захистити Google Play аналізує програми, деталізує дозволи, повне шифрування, біометрія та покращення модернізації компонентів. Android Enterprise (робочі профілі, повністю керований режим) та такі технології, як Samsung Knox передбачає потенційні загрози безпеці, автоматично реагувати на них і розширювати захист за межі мобільних пристроїв на IoT-пристрої та мережеві точки кінця.

В обох системах, рішення користувачів та IT є вирішальними: активувати оновлення, огляд дозволів, вибирати пристрої з гарною підтримкою, а уникнення невідомих джерел значно зменшує ризик.

Контрольні питання

1. Що таке бекдор?
2. Яка різниця між бекдором і троянцем?
3. Назвіть 3 способи персистентності бекдора у Windows.
4. Як працює «fileless» бекдор? Чому він складніший для виявлення?

5. Які особливості архітектури Android впливають на механізми бекдорів (порівняно з Windows)?
6. Як бекдор може отримати права SYSTEM у Windows?
7. Які сновні характеристики бекдорного ПЗ?

Література : [3], [6], [7], [9].

ТЕМА 7. ОСНОВНІ ЕТАПИ СОЦІОІНЖЕНЕРНОЇ АТАКИ

7.1 Основні етапи атаки
7.2. Послідовність етапів соціальної інженерії

7.1 Основні етапи атаки

Атака із застосуванням соціальної інженерії – це один із найбільш вражаючих варіантів пентестингу. Пентестинг – це модельована кібератака, яка імітує дії зловмисника для виявлення та усунення вразливостей у комп'ютерних системах, мережах та додатках. Мета – знайти слабкі місця, перш ніж це зробить справжній хакер, та оцінити рівень безпеки, щоб запобігти реальним атакам. Результатом пентесту є детальний звіт з переліком знайдених вразливостей та рекомендаціями щодо їх усунення.

Але перш ніж приступити до атак, потрібно чітко засвоїти процес їх виконання на всіх етапах. Якщо ви цього не зробите, можуть виникнути проблеми із законом або, що ще гірше, ви можете завдати шкоди психічному здоров'ю об'єкта, якого атакуєте. Є два важливі процеси для виконання OSINT та соціальної інженерії – фреймворк соціальної інженерії та цикл OSINT OODA.

(Observe-Orient-Decide-Act, спостереження-орієнтація-рішення-дія) – та обговоримо операційні системи, які ви можете використовувати для цього погодження з клієнтом. Першим кроком підготовки до атаки є координація дій із клієнтом, будь то безпосередній замовник, ваш менеджер чи інша команда у вашій компанії. Навіть після того, як ви завершили початковий процес ознайомлення із завданням, не соромтеся ставити питання, що стосуються виконання роботи. На карту можуть бути поставлені ваша репутація, засоби існування і навіть судимість, тому переконайтеся, що ви чітко знаєте, що робити можна, а чого не можна і чому це так.

Ознайомлення із завданням

На етапі ознайомлення із завданням слід тісно поспілкуватися з клієнтом, щоб точно визначити, яким буде ваше тестове вторгнення і як воно буде

відбуватися. Цей етап включає з'ясування того, хто буде вашою контактною особою, а також розгляд термінів (наприклад, кількість годин, відведених на завдання; час доби, тижня або місяця, протягом якого буде проводитися тест, і періоди, коли ви не можете пройти тестування). Також слід обговорити юридичні аспекти, переконавшись, що в договорі є формулювання, які захистять вас від юридичних проблем. Ось чому розумно найняти юриста. Вам потрібні пункти договору, які страхують вас на випадок випадкового пошкодження та інших непередбачених обставин. Нарешті, обговоріть масштаб вашої атаки, наприклад, кількість дзвінків або електронних листів.

Ви та ваш клієнт повинні задокументувати результати етапу визначення області Технічного завдання (ТЗ) – частини договору, в якій чітко зазначено, що ви маєте і не уповноважені робити в рамках завдання. Переконайтеся, що в ТЗ прописані відповідні правила проведення атакуючих дій. У ньому повинні бути детально описані будь-які заборонені або рекомендовані виправдання, адреси електронної пошти, вихідні або цільові IP-адреси та інші обмеження або вимоги, що стосуються роботи.

Також переконайтеся, що ви вказані по імені в договорі і ТЗ. Найкраще назвати всіх тестувальників, які беруть участь у виконанні договору, якщо це можливо, а також компанію, в якій ви працюєте.

При визначенні обсягу завдання переконайтеся, що ваша участь в соціальній інженерії відповідає певним вимогам. Серед іншого, переконайтеся, що у вас є належний дозвіл і правовий захист на виконання соціальної інженерії і що особа, яка підписує контракт, уповноважена дати вам на це дозвіл. Якщо ви внутрішній співробітник, який тестує власну компанію,

Отримати письмовий дозвіл від керівництва. Якщо ви займаєтеся виконанням тестових замовлень від інших організацій, спробуйте оформити спеціальну страховку від помилок і упущень (E&O), щоб захистити себе на законних підставах. E&O страхування, також зване страхуванням професійної відповідальності (страхування професійної відповідальності, PLI), покликане захистити вас від необхідності оплачувати повну вартість позову про недбалість в цивільному суді (якщо ви програєте цей суд).

Фаза ознайомлення із завданням задає тон всій взаємодії. Неправильна оцінка роботи може завдати неприємностей обом сторонам. Це може надмірно ускладнити взаємодію, змушуючи вас витрачати більше часу на телефонні дзвінки в невідповідний час або виконувати роботу неналежним чином. Неправильна оцінка завдання також може зіпсувати вашу репутацію фахівця, якщо компанія, де ви працюєте, вважатиме вас неспеціалістом.

Визначення цілей

Після підписання договору і створення технічного завдання ще раз обговоріть з клієнтом цілі майбутнього тестування. Чи буде результат тестування використаний як обґрунтування для впровадження нових інструментів, продуктів і технологій безпеки бізнесу? Чи буде він використаний для оцінки потреб у людському капіталі? Може бути, тест потрібен якраз для перевірки дотримання внутрішніх правил компанії? Або клієнт буде використовувати його для оцінки роботи команди безпеки (наприклад, в рамках оцінки ефективності або для прийняття рішення про просування по службі)? Відповіді на ці питання не повинні впливати на те, наскільки добре ви виконуєте свою роботу, але вони повинні допомогти вам зрозуміти, чого очікувати і як будувати свої комунікації.

Визначення методів

Методи, які ви використовуєте, мають вирішальне значення для вашої участі. Чи будете ви використовувати неправильно написане доменне ім’я, дуже схоже на доменне ім’я клієнта (особливо ефективна стратегія, якщо правильне написання допускає друкарську помилку), або купите доступний домен з таким же ім’ям та іншим доменом верхнього рівня (наприклад, nostarch.us замість законного nostarch.com)? Ви будете прикидатися постачальником, клієнтом або партнером? Використовуєте завантаження шкідливих документів або просто збираєте облікові дані? Чи будете ви використовувати вішинг і фішинг разом? Клієнт хоче, щоб ви використовували автоматизоване рішення, або ви повинні надавати пріоритет ручній праці?

Знання технології, яку використовує ваш клієнт, і де зосередити свої зусилля, буде важливим фактором успіху атаки. Перш за все, перевірте, чи можна зібрати інформацію з відкритих джерел про технології, які використовує ваш

клієнт, а потім спробуйте скористатися цією інформацією. У такого підходу є додаткові переваги: він надає клієнту метод виявлення і, можливо, приписування будь-яких інших атак, а також дозволяє перевірити, що клієнт правильно впровадив і використовував свої технології. Ваш клієнт напевно залишиться задоволений, якщо отримає більше інформації, ніж замовив.

Розробка вдалих прийменників

Розробляючи приводи для взаємодії, постарайтеся знайти події в оточенні вашої жертви, які могли б бути використані проти неї. Ви можете претендувати на роботу в організації, яка надає хмарне сховище або послуги електронної пошти компанії-жертві, і запросити додаткову інформацію у зв'язку з «інцидентом безпеки». Для збору додаткових OSINT-даних можна подивитися сторінки і групи в локальних соціальних мережах.

Різноманітні міркування перетворять вашу фішингову атаку з випадкової на цілеспрямовану, що значно збільшить її шанси на успіх. Виділення часу на знайомство з жертвою та її оточенням значно полегшить вашу роботу, але обов'язково поділіться інформацією та порадами, які ви отримаєте у своєму звіті, а також у тренінгу, який вас можуть попросити провести за результатами тестування.

На основі зібраної інформації розробляйте свої сценарії і приводи. Покажіть клієнту три-п'ять кращих варіантів, і нехай він вибирає, який з них краще використовувати. По можливості підтвердьте терміни, в які буде здійснена ваша атака, але не точний час. Це тримає ваших клієнтів у напрузі та дає вам елемент несподіванки.

Хоча жоден клієнт не повинен інформувати співробітників про вибрані вами сценарії, це трапляється досить часто. Наприклад, в одному з із контрактів клієнт обмежував можливі виправдання і сценарії, а потім прописував точний час, коли можна відправляти фішингові листи і здійснювати вішингові дзвінки. При цьому був зроблений важливий нюанс: якщо під час дзвінка попросять передзвонити пізніше з яких-небудь причин, то це можна зробити без додаткового узгодження.

Наприклад, під час дзвінка можна створити багато дуже гучних фонових шумів та імітувавати розрив зв’язку. Між шумом і «відключенням телефону» вдається змусити близько двох третин співрозмовників просити передзвонити їм.

7.2 Послідовність етапів соціальної інженерії

Кожен крок у цьому процесі виглядає наступним чином

Огляд – це етап визначення області завдання соціальної інженерії, коли ви задаєте питання своєму клієнту, щоб переконатися, що у вас є вся необхідна інформація.

Розвідувальний – це дослідження, ви намагаєтеся визначити ключових співробітників компанії; продавців, партнерів, постачальників, використовувані технології; використовувані домени та субдомени; адреси електронної пошти та стандартний синтаксис адрес електронної пошти компанії (наприклад, ім’я та прізвище, розділені крапкою). Після того, як контракт на місію підписаний, ви можете почати розвідку в терміни, зазначені в контракті. За умови дотримання договору та проведення розвідувальних робіт відповідно до вашого часові рамки (наприклад, не витрачати 12 годин на збір OSINT по одній цілі в атаці, розрахованій на 4 години), ніяка кількість OSINT не буде зайвою. Однак ви можете виявити, що деякі організації підтримують належну безпеку операцій (OpSec), не використовуючи соціальні мережі або навіть вживаючи активних заходів для навмисного розміщення оманливої або неправдивої інформації у своїх облікових записах, щоб уникнути таких загроз. Цей процес є активною дезінформацією.

Проектування та затвердження – час, щоб переконатися, що OSINT-інформація, яку ви збираєте, є актуальною, а потім використовувати її таким чином, щоб допомогти співробітникам організації-жертви рости і вчитися. Зрештою, навіть якщо ви намагаєтеся отримати доступ до системи або інформації, в ідеалі вас спіймають, і ви захочете, щоб клієнти вчилися на тому, що ви робите.

Етап проектування та затвердження передбачає придумування можливих приводів для встановлення контакту, які ваш клієнт повинен розглянути та затвердити. Поділіться з ними деталями виправдання, номерами телефонів, з яких ви будете дзвонити, адресами електронної пошти, з яких будете відправляти електронні листи, і часовим інтервалом, протягом якого ви плануєте почати і закінчити тест. Також поясніть свою мету. Наприклад, це може бути підрахунок кількості кліків по посиланнях в електронному листі. Або, можливо, ви спробуєте отримати конфіденційну інформацію від співробітників компанії або розгорнете шкідливе програмне забезпечення або віддалені крапельниці оболонок (програмне забезпечення, яке дозволяє віддалено підключатися та встановлювати шкідливе програмне забезпечення).

Реалізації – етап впровадження ви встановлюєте та налаштовуєте правильне програмне забезпечення. Він включає таку інфраструктуру, як облікові записи електронної пошти, веб-сервери, документи Microsoft Office із підтримкою макросів, шкідливі програми, USB-накопичувачі та інші приманки. Ви також можете отримати доступ до сміттєвих баків організації та зібрати документи, щоб винести їх з місця для подальшого аналізу. Ви будете використовувати приводи, схвалені вашою контактною особою на стороні клієнта, і застосовувати їх на практиці, здійснюючи фішинг, вішинг та інші атаки, зазначені в ТЗ.

Виявлення – захисники спробують виявити ваші дії, а потім вжити заходів, щоб зменшити їх ефективність або вплив. Залежно від масштабу атаки, захисники можуть знати, а можуть і не знати, що напад санкціоновано.

Якщо це частина роботи червоної команди, вони, швидше за все, не дізнаються заздалегідь. Хоча ця фаза здається менш захоплюючою, ніж сама атака, вона є найважливішою частиною процесу. Пам’ятайте, що ваша кінцева мета – навчити організації виявляти та пом’якшувати атаки соціальної інженерії.

Вимірювання – ви збираєте таку інформацію, як кількість людей, які стали жертвами ваших трюків, скільки часу знадобилося для виявлення нападу, коли жертви повідомили про це, скільки таких повідомлень було та багато інших

показників. Після того, як ви зібрали та проаналізували цю інформацію, вам потрібно скласти її у звіт для клієнта.

Складання звіту – ви берете зібрані показники та об’єднуєте їх разом із технічним навантаженням, резюме ідеї та плану атаки, резюме того, як проходила взаємодія, та будь-які висновки зі збору даних OSINT або виконання завдань. Для написання звіту можна використовувати шаблон. Надішліть цей звіт клієнту на розгляд. Якщо ви вирішите зберегти копію звіту, необхідно захистити документ, оскільки інформація, яка в ньому міститься, потенційно може бути використана для атаки на клієнта.

На додаток до цього процесу соціальної інженерії, вам може бути корисно звернутися до циклу спостереження-орієнтація-рішення-дія (NORD), щоб зібрати дані OSINT. Цикл пропонує вам спостерігати за своїми висновками і побудувати гіпотезу (фаза орієнтації), а потім шукати додаткову інформацію, щоб спробувати підтвердити те, що у вас вже є.

Отримавши достатньо даних, ви можете вирішити, що з ними робити. Чи варто займатися фішингом або вішингом, або вам потрібно більше інформації, щоб досягти успіху? Чи достатньо у вас інформації для проведення замовленого тесту на проникнення або бою команди з належним ступенем скритності? Потім, в залежності від результатів цих рішень, ви переходите до дій.

Дії можуть включати виконання атаки або написання звіту (якщо OSINT – це все, що хоче клієнт), або вони можуть ініціювати додаткові ітерації циклу NORD. Немає правильної чи неправильної відповіді; Це залежить від ваших цілей і часових обмежень, викладених у вашій клієнтській угоді.

Однак ви можете застосувати цей цикл до будь-якої атаки, будь то проникнення на веб-сервер або отримання прав адміністратора мережі.

Послідовні фази атаки

Всі етичні хакери зазвичай дотримуються певної послідовності фаз атаки, гарантуючи, що вся необхідна інформація збирається і використовується. Ця послідовність зазвичай складається з наступних кроків: розвідка, сканування та лістинг, отримання доступу, підтримка доступу, видалення слідів та звітність.

Детальніше про ці етапи можна прочитати на сторінці https:// www.cybrary.it/ blog/2015/05/summarizing-the-five-phases-of-penetration-testing/.

У вересні 2019 року пара пентестерів, які працюють на Coalfire, була заарештована за спробу проникнути в будівлю суду округу Даллас в Аделі, штат Айова. Хоча конкретні подробиці про цей інцидент наразі недоступні, ми знаємо, що вони діяли в рамках тесту на проникнення, санкціонованого Судовою адміністрацією штату Айова (SCA). У заяві Ars Technica SCA визнає, що уповноважила Coalfire перевірити безпеку електронних записів суду. Випробувачі і Coalfire стверджують, що тест на проникнення повинен був визначити вразливість записів і оцінити реакцію правоохоронних органів. Хоча такий підхід не позбавлений здорового глузду, той факт, що тестувальники провели у в'язниці кілька годин і повинні були внести заставу, свідчить про відсутність належного розуміння на етапі ознайомлення із завданням. Виходячи з наданої інформації, пентестери могли діяти по-іншому. Необхідно частіше спілкуватися зі співробітниками служби безпеки вашого клієнта.

Як можна пом'якшити або запобігти негативним наслідкам:

— задавайте більше питань, щоб прояснити сферу своїх повноважень;

— підтримуйте робочий діалог з вашою контактною особою електронною поштою. Усне спілкування допомагає швидше досягти мети, але погано підходить для правового захисту;

— керівництво замовника має чітко вказати не лише те, що дозволено, а й те, що заборонено, у контракті та дозвільних документах. Це має бути частиною процесу підготовки договору.

Контрольні питання

1. Які основні етапи атаки?
2. Що таке пентестинг?
3. Яка послідовність етапів атаки?
4. Хто такий «інсайдер» у контексті кібербезпеки?
5. Які методи протидії соціальній інженерії використовуються?

Література : [1], [2], [14].

ТЕМА 8. ВИЗНАЧЕННЯ ЦІЛІ АТАКИ СОЦІАЛЬНОГО ІНЖЕНЕРА В МЕСЕНДЖЕРАХ

Сьогодні месенджери стали невід'ємною частиною нашого життя. За допомогою них можливо розвиватися, знайомитися з різними людьми, проводити вільний час. Месенджери є доступним для всіх. Але разом з тим є люди, які мають недоброчесні наміри, спілкуючись з вами.

Чому месенджери – легке поле для соціальних інженерів?

Масова популярність – великий «поле» потенційних жертв.

Швидкість спілкування – користувачі реагують емоційно й імпульсивно.

Часто персональні (зв'язок із близькими) і професійні контакти змішуються.

Месенджери дозволяють надсилати посилання, файли, голосові/відео – вектор доставки шкідливого контенту.

8.1 Основні цілі атаки в месенджерах

Крадіжка облікових даних – фішингові посилання на фальшиві сторінки логіну; видобуток коду підтвердження.

Доставка шкідливого програмного забезпечення / інфраструктурний компроміс – надсилання файлів/посилань, що запускають malware чи інсталятори.

Соціальне/фінансове шахрайство – прохання про переказ, оплата «термінового рахунку», фальшиві вакансії.

Розвідка / OSINT – збір деталей про організацію/людину (запити про робочі процеси, інструменти, графік).

Розповсюдження дезінформації / вплив – поширення фейків для маніпуляції позицією або поведінкою.

Контроль / шантаж (extortion, doxxing) – отримання компрометувальної інформації для шантажу.

Перевірка легітимності (spray-and-pray / verification probes) – невинні запити, що тестують, хто відгукнеться, хто дасть більше інформації.

Психологічні тригери, що використовує атакуючий:

1. Терміновість / паніка («Терміново!», «24 години»).
2. Авторитет (представлення як начальник/адмін/банк).
3. Ексклюзивність / виграш (лото, бонус).
4. Дружність / соціальна близькість (вдавати знайомого).
5. Допомога / прохання про послугу (маніпулювання емпатією).
6. Страх покарання (загроза блокування/штрафу).

Індикатори підозрілих повідомлень у месенджерах. Технічні та мовні сигнали:

— Непрошене посилання або файл від невідомого контакту.

— Невідповідність номера/імені й профілю (відсутність фото, недавно створений акаунт).

— Граматичні помилки або дивні фрази — часто вказують на шаблон/переклад.

— Прохання про код підтвердження/OTP або PIN — майже завжди шахрайство.

— Попросити «перевести на цей рахунок», «надішли скриншот паспорту», «скачуй додаток з посилання» — червоні прапорці.

— Зайвий тиск («виконай зараз, інакше…»).

— Посилання із скорочувачів (bit.ly) без додаткового контексту — ризик.

— Коли контакт просить змінити канали («напиши у Telegram/Signal зараз») – може бути спроба обійти моніторинг.

Прикладом є популярні месенджери, де соціальні інженери експлуатують можливості та вразливості:

8.2 Telegram

З початку 2022 року різко зросло використання ботів для вилучення облікових даних. З появою штучного інтелекту ChatGPT, кіберзлочинці винайшли нові методи для написання шкідливих програм. Хоч ШІ і відмовляє в генерації шкідливого програмного забезпечення, хакери активно намагаються обійти всі обмеження за допомогою OpenAI API(адже поточна версія поки має дуже мало заходів проти зловживань).

На підпільному форумі організація CheckPoint Research знайшла кіберзлочинця, який рекламував нещодавно створений сервіс - бота Telegram, який використовує API OpenAI без будь-яких обмежень.

«Кіберзлочинець створив базовий скрипт, який використовує OpenAI API для обходу обмежень проти зловживань», - зазначили дослідники.

Огляд типових атак на Telegram

У контексті Telegram атаки соціальної інженерії можуть бути особливо ефективними, так як, по-перше, цей месенджер є одним з найпопулярніших месенджерів у світі; по-друге, для створення облікового запису, окрім номеру телефону, нічого більше не потрібно; і по-третє, оскільки платформа покладається на спілкування користувачів і обмін інформацією, зловмисникам легше застосувати різні види маніпуляцій та тактики соціальної інженерії, щоб обманом змусити користувачів надати облікові дані для входу чи особисту інформацію, або переконати їх встановити зловмисне програмне забезпечення.

Шахрайство варіюється від традиційних фішингових схем до складних атак ботів, які маскуються під законних агентів служби підтримки клієнтів. Розглянемо деякі з них, про які застерігає нас Джорі Маккей, письменник і редактор із питань кібербезпеки:

Канали-повторюшки. Це канали, що повністю копіюють інші популярні,

з метою видати себе за них. Вони можуть мати однакові імена та зображення профілю, включати одні й ті самі закріплені повідомлення та мати адміністраторів з іменами користувачів, майже ідентичними первинним. Однак незабаром інші користувачі або адміністратори почнуть зв'язуватися з вами, щоб спробувати змусити вас натиснути посилання або надати особисту інформацію, яку вони можуть використати для крадіжки особистих даних або зламу ваших облікових записів;

Фейкова служба підтримки клієнтів. Шахраї можуть представлятися представниками служби підтримки клієнтів із Telegram і пропонувати користувачам допомогу у вирішенні проблем із обліковим записом. Вони можуть запитувати облікові дані для входу або іншу особисту інформацію, щоб вирішити проблему, але насправді вони просто намагатимуться вкрасти інформацію користувача;

Фішинг сками за допомогою ботів. Хакери використовують ботів, видаючи себе за авторитетних представників компаній, організацій і т.п. Повідомлення, які надсилають ці боти, зазвичай просять користувача натиснути посилання або надати свої облікові дані для входу чи іншу особисту інформацію. Щойно користувач надає цю інформацію, шахраї можуть використовувати її для доступу до облікового запису або викрадення особи користувача;

Романтичні сками. Часто зосереджені на короткочасних забавах або вмісті для дорослих. Шахраї, встановивши з жертвою або ж романтичні, або ж сексуальні відносини, просять надіслати їм фотографії чи відео сексуального характеру, які потім використовують для шантажу;

Претекстинг. Зловмисник видає себе за друга, члена сім'ї, колегу жертви(обстеживши їхні соціальні мережі, вивчивши звички та манеру спілкування для більш переконливого сценарію) з метою отримати конфіденційну інформацію;

Викрадення каналів. Тип атаки, коли зловмисник отримує несанкціонований доступ до каналу Telegram і контролює вміст або учасників. Цей тип атаки може бути особливо шкідливим, якщо канал має велику кількість підписників, або використовується для бізнесу чи інших професійних цілей.

Зазвичай це відбувається через недотримання всіх мір безпеки адміністраторами(використання слабких паролів, відсутність двофакторної автентифікації, необачність при переході за невідомим посиланням і т.д.).

Атаки соціального інженера в месенджерах становлять одну з найнебезпечніших форм психологічного впливу в цифровому середовищі. Через довіру користувачів до особистих чатів та швидкість обміну повідомленнями зловмисники отримують можливість ефективно збирати інформацію, поширювати шкідливі посилання, підмінювати особи або маніпулювати емоціями.

Основна загроза полягає не у технічних вразливостях самих месенджерів, а у людському факторі – неуважності, довірливості чи недостатній обізнаності користувачів.

Для мінімізації ризиків важливо:

– не відкривати підозрілі посилання та вкладення навіть від знайомих контактів;

– перевіряти профілі співрозмовників і джерела інформації;

– використовувати двофакторну автентифікацію;

– навчати користувачів методам розпізнавання соціальної інженерії.

Отже, ефективна протидія атакам у месенджерах можлива лише через поєднання технічного захисту та інформаційної гігієни користувачів.

8.3 Discord

На початку 2021 року кількість фішингових атак на Discord зросла на 1200% порівняно з попереднім роком. Також з 2022 року збільшилася кількість атак, пов’язаних з криптографічними токенами, а саме NFT, через зламані облікові записи користувачів Discord.

Аналітики з TRM Labs, компанії, що займається аналізом блокчейнів, помітили, що існує декілька схожих патернів моделі поведінки та низка тактик хакерів, а саме:

Використання складної соціальної інженерії, такої як фішинг, а також створення шахрайських облікових записів, що видають із себе адміністратора каналу;

Використання вразливостей ботів, що дозволяє адміністраторам автоматично надавати та видаляти ролі, а також надсилати повідомлення спільноті;

Зміна налаштувань адміністратора з метою заборони модераторам Discord втручатися в роботу хакерів.

8.4 WhatsApp — цілі атак соціального інженера

Основні цілі:

Викрадення облікового запису – отримати контроль над акаунтом (через код верифікації), щоб видаватися жертвою, шантажувати знайомих або розповсюджувати шкідливі посилання.

Крадіжка конфіденційної інформації – паролі, фінансові дані, персональні дані або корпоративні документи, які користувач може переказати у чаті.

Фінансове шахрайство (social-payments) – підроблені прохання про перекази, «термінові» платежі від імені керівника або колеги.

Розповсюдження шкідливих посилань / файлів – фішингові посилання, завантаження шкідливих APK (на Android) або документів із макросами.

Розвідка / OSINT – збір інформації про контакти, структуру організації, графи зв’язків для подальших атак.

Соціальний інжиніринг для доступу в інші системи – отримання одноразових кодів, паролів для сервісів, відновлення доступу тощо.

Репутаційні атаки / дезінформація – поширення фейків або компрометуючих матеріалів під чужим акаунтом.

Підірвання довіри всередині організації – підробка команд керівництва, видалення/фальсифікація повідомлень.

У 2022 році стався масштабний злив номерів користувачів месенджера - майже 500 млн номерів були виставлені на продаж на форумі певного кола

хакерів. І це, на жаль, не єдиний випадок атак, націлених на WhatsApp. У 2017 році, був виявлений величезний баг, що дозволив кіберзлочинцям взяти під контроль облікові записи користувачів додатка. А з настанням пандемії кількість та різноманіття атак зросли в рази і, як ми можемо бачити, досі розвиваються, а хакери знаходять все нові та нові методи отримання бажаного.

Контрольні питання

1. Що розуміють під соціальною інженерією в месенджерах?
2. Які месенджери найчастіше використовуються соціальними інженерами для атак?
3. У чому полягає різниця між фішингом і спуфінгом у контексті месенджерів?
4. Як соціальний інженер використовує OSINT для підготовки до атаки через месенджер?
5. У чому полягає небезпека QR-кодів і скорочених посилань у чатах?
6. Які рекомендації можна надати користувачам для безпечного спілкування в месенджерах?

Література : [1], [2], [4], [9].

ТЕМА 9. ПРОФІЛАКТИКА ТА ПОМ'ЯКШЕННЯ НАСЛІДКІВ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

9.1 Профілактика атак соціальної інженерії
9.2 Методи протидії
9.3 Пом'якшення наслідків атак

9.1 Профілактика атак соціальної інженерії

Метою соціальних хакерів можуть бути будь-які ресурси: від встановлення майнера на ваш комп'ютер до крадіжки вашої криптовалюти, від розсилки спаму до крадіжки комерційної таємниці, і від поширення комп'ютерного вірусу до військового шпигунства тощо.

Ці дані підкреслюють поширеність і небезпеку атак, що базуються на соціальній інженерії у сфері кібербезпеки. Як же боротися з цими атаками?

Профілактика атак соціальної інженерії:

1. Освіта та підвищення обізнаності

Регулярні тренінги для співробітників з теми фішингу, телефонного шахрайства та інших методів соціальної інженерії.

Ознайомлення персоналу з актуальними прикладами атак і способами їх розпізнавання.

Створення культури «підозріливого запиту»: навчати перевіряти будь-які незвичні запити чи інструкції.

2. Контроль доступу та автентифікація

Використання багатофакторної автентифікації (MFA) для критичних систем.

Мінімізація прав користувачів — лише необхідний доступ.

Регулярне оновлення паролів та заборона повторного використання старих паролів.

3. Технічні заходи

Використання антивірусного та антифішингового ПЗ.

Фільтрування підозрілих листів та вкладень на рівні поштових серверів.

Регулярне оновлення систем та програм для закриття вразливостей.

4. Політики та процедури

Введення політик щодо перевірки незвичних фінансових або конфіденційних запитів (наприклад, підтвердження через телефон).

Регламентація обробки персональних даних та доступу до корпоративної інформації.

Статистика соціальної інженерії:

2023: 98% кібератак включали деяку форму соціальної інженерії.

2023: 92% шкідливих програм доставляються електронною поштою.

2023:75% спеціалістів з безпеки вважають соціальну інженерію «найнебезпечнішою» загрозою.

2023: Найпоширеніша атака на малий бізнес – це фішинг/соціальна інженерія, яка становить 57% усіх атак.

2022: 84% організацій стали жертвами фішингових атак.

2021: Середньостатистична організація щороку стає мішенню понад 700 атак соціальної інженерії.

9.2 Методи протидії

1. Навчання персоналу

Ефективним і дієвим рішенням для будь-якої організації у протистоянні соціальній інженерії є навчання свого персоналу. Це перший і найважливіший крок до захисту організації від подібних атак. Регулярні тренінги та розвиток критичного мислення допомагають поліпшити навички розпізнавання обману та маніпуляцій, а також дають змогу підвищити рівень безпеки. Однак одних лиш тренінгів буде недостатньо.

2. Тестування знань і навичок

Навчання має працювати з тестуванням знань і навичок. Це допоможе виявити рівень засвоєння матеріалу та слабкі місця, які потребують доопрацювання. Логіка тестування застосовується та сама, як і при тестуванні на проникнення – «зламай себе сам перш, ніж це зробить хакер». Симуляція

соціальної інженерії – це найефективніший метод виявлення психологічних і соціальних вразливостей груп користувачів Інтернет.

Однак як виконати цю симуляцію грамотно? Які сценарії фішингу застосувати? Як обійти штатні антивіруси та інші засоби захисту? Як швидко виконати симуляцію фішингу в обсязі кількох сотень або навіть тисяч користувачів? На допомогу приходить аутсорсинг сервісів безпеки.

3. Ефективний сервіс із протидії соціальній інженерії

Різні компанії пропонують комплексні підходи до захисту від соціальної інженерії. Спеціальне навчання користувачів дає змогу забезпечити основу захисту від цього типу атак. Проведення пентестів із використанням імітації фішингу, цільового фішингу та вейлінгу (VIP-фішингу) дає змогу впевнитися в практичному засвоєнні знань користувачами та в надійності вашої системи безпеки. Виконати тестування соціальної інженерії в рамках тестування на проникнення, Red Team. Тестування груп користувачів будь-якої величини.

9.3 Пом’якшення наслідків атак

1. Реагування на інцидент

Мати чіткий план реагування на інциденти соціальної інженерії.

Швидке повідомлення IT-відділу або служби безпеки про підозрілий лист чи дзвінок.

Відключення заражених або підозрілих облікових записів до завершення розслідування.

2. Відновлення систем

Використання регулярних резервних копій для відновлення даних.

Перевірка та оновлення систем після інциденту, щоб усунути можливі точки компрометації.

3. Інформування та навчання

Аналіз інциденту та навчання співробітників на реальних прикладах.

Розробка внутрішніх «case studies» для запобігання повторним атакам.

4. Юридичні та репутаційні заходи

Інформування відповідних органів у разі порушення законодавства про захист персональних даних.

Підготовка повідомлень для клієнтів або партнерів, якщо їх дані могли бути скомпрометовані.

Контрольні питання

1. У чому полягає профілактика атак соціальної інженерії?
2. Які психологічні прийоми найчастіше використовують зловмисники для маніпуляцій?
3. Яким чином обмеження прав доступу допомагає знизити наслідки успішної атаки?
4. Що означає пом’якшення наслідків атаки соціального інженера?
5. Які етапи реагування потрібно виконати після виявлення атаки?
6. Як правильно зберігати та передавати конфіденційну інформацію, щоб уникнути її витоку?
7. Яку роль у протидії соціальній інженерії відіграє корпоративна культура?

Література : [1], [2], [5], [14].

ТЕМА 10. ЗАХОДИ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ

10.1 Основні заходи протидії соціальній інженерії

Соціальна інженерія – це не про складний хакінг комп'ютерних систем, а про спробу атакуючого, шляхом обману або психологічних маніпуляцій, змусити людину добровільно надати доступ або передати облікові дані, банківські реквізити, конфіденційну інформацію або виконати дії, які йдуть на користь зловмисникам. Це може бути що завгодно: від «термінового» запиту на пароль до встановлення шкідливого програмного забезпечення. Суть у тому, що жертва діє за власним бажанням, не усвідомлюючи обману.

1. Освітні та інформаційні заходи:

— Навчання співробітників – регулярні тренінги з кібербезпеки та соціальної інженерії; розбір реальних кейсів атак і наслідків.

— Інформаційні кампанії – поширення пам'яток, постерів і електронних бюлетенів з правилами безпеки.

— Роз'яснення правил роботи з конфіденційною інформацією – не передавати паролі, дані доступу або внутрішню документацію стороннім особам.

2. Технічні заходи:

— Контроль доступу – використання багатофакторної автентифікації (MFA); розмежування прав доступу до інформації.

— Моніторинг та логування – відстеження підозрілих спроб доступу до систем; логування дій користувачів у критичних системах.

— Антивірусні та антиспам рішення – фільтрація електронної пошти для блокування фішингових листів; захист від шкідливих програм та підозрілих вкладень.

3. Організаційні заходи:

— Політики безпеки – чіткі інструкції щодо обробки конфіденційної інформації; регламентоване спілкування з клієнтами та партнерами.

— Верифікація запитів – підтвердження особи, яка запитує інформацію, через незалежний канал.

— Обмеження інформаційного шуму – мінімізація публічної інформації про компанію та її співробітників.

4. Практичні заходи протидії:

— Тестування персоналу – проведення «фішинг»-тестів та симуляцій атак.

— Застосування принципу обережності – не відкривати підозрілі посилання та вкладення; не відповідати на підозрілі телефонні дзвінки чи листи.

— Регулярне оновлення програмного забезпечення – патчі безпеки зменшують ризик експлуатації вразливостей.

5. Культура безпеки:

— Формування у колективі атмосфери обережності та відповідальності.

— Заохочення повідомляти про підозрілі ситуації без страху покарання.

— Якщо хочеш, я можу зробити коротку та зручну інфографіку або таблицю «Загроза → Як захиститися», щоб швидко запам’ятати всі заходи протидії соціальній інженерії.

10.2 Як захиститися: комплексний підхід до кібербезпеки

Повністю уникнути зіткнення з соціальною інженерією в сучасному світі майже неможливо, адже вона постійно еволюціонує і націлена на людську природу. Однак, можна значно знизити ризики для себе та своєї організації, застосовуючи комплексний підхід до кібербезпеки, що поєднує технології та обізнаність.

1. Регулярні тренінги з обізнаності співробітників

Людський фактор є найважливішим. Регулярні та інтерактивні тренінги з обізнаності співробітників про безпеку є першою та найефективнішою лінією

захисту. Співробітники можуть просто не знати про складність і небезпеку соціальної інженерії, або з часом забувати деталі. Проведення регулярних тренінгів, семінарів та постійне оновлення інформації про нові загрози, а також проведення практичних симуляцій (наприклад, контрольованих фішингових розсилок, які допомагають виявити вразливих співробітників) допоможуть виробити «імунітет» до подібних маніпуляцій. Важливо створити корпоративну культуру, де кожен співробітник розуміє свою роль та відповідальність у забезпеченні безпеки даних.

2. Сучасні антивірусні програми та засоби захисту кінцевих точок

Навіть якщо атака соціальної інженерії була успішною на психологічному рівні, її технічні наслідки можна пом’якшити. Основною технічною мірою є встановлення надійного антивірусного захисту та інших інструментів безпеки кінцевої точки (Endpoint Detection and Response, EDR) на всіх пристроях користувачів. Сучасні засоби захисту, такі як платформи від наших надійних партнерів, здатні виявляти та блокувати явні фішингові повідомлення, а також будь-які посилання на шкідливі вебсайти або IP-адреси, перераховані в актуальних базах даних загроз. Вони також можуть перехоплювати та блокувати шкідливі процеси, що виконуються на пристрої користувача, навіть якщо початкова маніпуляція була успішною. Наприклад, компанія Cynet пропонує комплексну XDR-платформу, яка поєднує можливості EDR, мережевого виявлення та реагування (NDR), аналітики поведінки користувачів (UEBA) та автоматизації реагування (SOAR), забезпечуючи багатошаровий захист.

3. Тестування на проникнення та симуляції атак

Для виявлення неочевидних слабких місць існують послуги етичного хакінгу та тестування на проникнення (пентести). Це дозволяє виявити потенційні вразливості у вашій організації, перш ніж їх знайдуть кіберзлочинці. Тест на проникнення, що імітує компрометацію чутливих систем саме через соціальну інженерію, допоможе вам ідентифікувати найбільш вразливих співробітників, перевірити ефективність внутрішніх політик та процедур, а також виявити конкретні методи соціальної інженерії, до яких ваша компанія

може бути особливо схильна. Це також чудовий спосіб оцінити ефективність проведених тренінгів з безпеки.

4. Системи SIEM та UEBA: розумний моніторинг поведінки

Незважаючи на всі превентивні заходи, атаки соціальної інженерії, на жаль, неминучі. Тому вкрай важливо мати інструменти, які дозволяють швидко збирати дані про інциденти безпеки, виявляти підозрілі події, що відбуваються в мережі та на кінцевих точках, та негайно сповіщати співробітників служби безпеки для вжиття заходів. Саме тут незамінними стають системи SIEM (Security Information and Event Management) та UEBA (User and Entity Behavior Analytics).

Наприклад, Exabeam Security Management Platform – це система управління подіями та інформацією про безпеку нового покоління (New-Scale SIEM™), заснована на потужному аналізі поведінки користувачів та сутностей (UEBA). Exabeam збирає події безпеки та журнали по всій вашій організації, використовує алгоритми машинного навчання для визначення «нормальної» поведінки користувачів та сповіщає вас про будь-які аномальні або підозрілі дії. Будь то перехід користувача за незвичною вебадресою, аномальний доступ до конфіденційних файлів або запуск шкідливого процесу на пристрої, UEBA допоможе вам ідентифікувати атаки соціальної інженерії на ранніх стадіях та швидко відреагувати. Це включає автоматичні сценарії реагування на інциденти, що мінімізує потенційні негативні наслідки. Tufin спеціалізується на автоматизації політик мережевої безпеки, що доповнює можливості SIEM та UEBA у захисті від таких атак, забезпечуючи, що зміни в мережі не створять нових вразливостей.

Компанія NWU є надійним партнером у світі кібербезпеки. Її мета - ефективний захист від соціальної інженерії, який вимагає не тільки використання передових технологій, але й глибокого розуміння людського фактора та постійного оновлення стратегій захисту. Саме тому пропонує комплексні рішення, що поєднують провідні платформи та багаторічний досвід наших експертів. Забезпечує професійне налаштування, навчання співробітників та

постійну технічну підтримку, гарантуючи, що інвестиції в безпеку принесуть максимальну віддачу.

10.3 Як запобігти кібератаці

Це правда, що кіберзагрози ховаються в кожному куточку Інтернету, але є кілька способів захистити від них себе та свою компанію. Дотримуйтесь, порад, які допоможуть запобігти кібератаці та підвищити загальну безпеку в Інтернеті.

Встановіть антивірус. Антивірус – це перша лінія захисту від шкідливих програм. Він захистить пристрій і допоможе зменшити шкоду, якщо шкідливий код все ж таки на нього потрапить. Крім того, можна користуватися функцією NordVPN Threat Protection Pro™, яка виявляє заражені файли, попереджає користувача, якщо посилання веде на шахрайський вебсайт, а також блокує трекери та нав'язливу рекламу.

Регулярно оновлюйте програмне забезпечення своїх пристроїв. Оновлення ПЗ – це не просто додавання нових функцій до програми. Адже воно містить важливі виправлення вразливостей, якими в іншому випадку могли б скористатися злочинці.

Уникайте загальнодоступних Wi-Fi. Злочинці люблять публічні точки доступу. Слабкий захист мережі і безліч жертв на вибір роблять всіх, хто підключений до неї, легкою здобиччю.

Використовуйте VPN. Використання загальнодоступного Wi-Fi іноді дуже допомагає. Саме тоді й виручає VPN. Він шифрує інтернет-з'єднання, щоб ніхто не міг шпигувати за вашими діями в Інтернеті.

Обмежте кількість інформації про себе в Інтернеті. Дата вашого народження або назва міста, в якому ви виросли, для злочинців має неоціненне значення. Чим більше інформації вони знають про жертву, тим більше можливостей мають її обдурити (або відповісти на секретні запитання в її акаунтах).

Використовуйте безпекове розширення браузера. Браузери пропонують безліч розширень, призначених для захисту в Інтернеті: від засобів блокування реклами й антитрекерів до блокування шкідливих вебсайтів.

Завантажуйте програми лише з авторитетних джерел. Завантажувати програми виключно із захищених джерел, а саме офіційні магазини додатків. Додатки там проходять ретельну перевірку, що знижує ймовірність того, що вони містять приховане шкідливе ПЗ.

Не переходьте за незнайомими посиланнями. Для протидії атакам з використанням соціальної інженерії вкрай важливо зберігати розсудливість. Перш ніж перейти за посиланням, що пропонує швидкий заробіток, подумайте, чи не є пропозиція легких грошей лише наживкою. Якщо так, кінцевою ціллю може бути шахрайство. Якщо вам дійсно потрібно перейти за посиланням, наведіть на нього курсор миші, перш ніж натиснути.

Убезпечте свій домашній Wi-Fi. Використовуйте для домашнього Wi-Fi надійний пароль та змініть облікові дані для входу, що встановлені від виробника.

Заходи кібербезпеки для бізнесу – дотримуйтесь порад і захистить інформацію у своєму бізнес-середовищі:

Регулярно оновлюйте програмне забезпечення. Підтримуйте в актуальному стані всі корпоративні операційні системи, програми та програмне забезпечення. Оновлення зазвичай містять виправлення безпекових вразливостей.

Створіть резервну копію даних. Регулярно створюйте резервні копії важливих бізнес-даних. Використовуйте віддалене хмарне сховище для зберігання файлів на випадок кібератаки або апаратного збою.

Навчайте правил безпеки свій персонал. Навчіть своїх співробітників правилам безпеки в Інтернеті, а також як розпізнавати та протидіяти кібератакам.

Обмежте права користувачів. Надавайте доступ тільки до тієї інформації, яка необхідна співробітнику для виконання його роботи. Такий захід допоможе запобігти витоку важливої інформації у ситуації, якщо обліковий запис працівника буде зламано.

Використовуйте мережеві брандмауери. Встановіть у своїх комп'ютерних мережах надійний брандмауер, що захищає від зовнішніх кібератак і несанкціонованого доступу до внутрішніх даних.

Використовуйте корпоративний VPN. Корпоративний VPN шифрує онлайн-трафік, що захищає інформацію від перехвату під час віддаленої роботи.

Захист пристроїв та документів. Запровадьте заходи безпеки, щоб зловмисники не могли фізично отримати доступ до приміщень вашого офісу та серверних кімнат.

Проводьте аудит та оцінку безпеки. Регулярний аудит та оцінка виконання правил кібербезпеки допоможе захистити конфіденційну інформацію, виявити та усунути вразливості.

Підготуйте план реагування на інциденти. Підготуйте комплексний план реагування у разі, якщо у систему сталося втручання, у разі кібератаки та інших інцидентів, пов'язаних з безпекою.

Соціальна інженерія залишається однією з найпідступніших і найефективніших загроз у кіберпросторі, яка постійно еволюціонує. Вона вимагає від організацій пильності та комплексного підходу до захисту, що поєднує технічні засоби, навчання персоналу та проактивний моніторинг. Поєднуючи обізнаність співробітників, надійні антивірусні рішення, сучасні SIEM/UEBA системи ви значно підвищуєте свою здатність протистояти цим загрозам.

Контрольні питання

1. Як соціальні мережі можуть бути використані для підготовки соціальної атаки і як цьому запобігти?
2. Які ознаки шкідливих вкладень або посилань у повідомленнях варто знати кожному користувачу?
3. Назвіть основні принципи безпечної поведінки в інформаційному середовищі.
4. Яку роль у профілактиці відіграє двохфакторна автентифікація (2FA)?
5. Яким чином обмеження прав доступу допомагає знизити наслідки успішної атаки?

Література : [1], [2], [12], [14].

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Соціальна інженерія. URL: https://termin.in.ua/sotsialna-inzheneriia/#Falsivij_ antivirus (дата звернення: 28.09.2024).

2. Соціальна інженерія. URL: https://hackyourmom.com/kibervijna/ soczialna-inzheneriya/ (дата звернення: 01.10.2025).

3. Стьопочкін І.В, Ільїн К.І. Теорія та методи соціальної інженерії в кібербезпеці: навч. посіб. для студентів спеціальності 125 «Кібербезпека та захист інформації». Київ: КПІ ім.Ігоря Сікорського, 2023. 35 с. URL: https://ela.kpi.ua/handle/123456789/67176 (дата звернення: 01.10.2025).

4. Зоренко Д.С., Лех Р.В., Кулик Д.О., Червяков О.І. Використання інструментів та методів OSINT для отримання пошукової інформації: практичний порадник. Харків: Інститут підготовки юридичних кадрів для Служби безпеки України, 2023. 36 с URL: https://dspace.nlu.edu.ua/jspui/ bitstream/123456789/19712/1/P_OSINT.pdf (дата звернення: 01.10.2025).

5. Міскевич О.І. Дослідження загроз від кібератак та захист персональної інформації. *Комп'ютерно - інтегровані технології: освіта, наука, виробництво*. 2021. Вип. 45. С. 84-89.

6. Міскевич О.І. Аналіз роботи мережевих утиліт в командному вікні Windows. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2023. Вип. 50. С. 84-89.

7. Що таке Бекдор? Визначення, приклади, бекдор-атаки. URL: https://gridinsoft.ua/backdoor (дата звернення: 02.10.2025).

8. Що таке підбір облікових даних? URL: https://corewin.ua/blog/what-is-credential-stuffing (дата звернення: 02.10.2025).

9. Типи та приклади шпигунського ПЗ. Мобільні шпигунські програми. URL: https://gridinsoft.ua/spyware (дата звернення: 03.10.2025).

10. Онлайн-блог. URL: https://surl.li/blog/uk (дата звернення: 03.10.2025).

11. Онлайн-курс. URL: https://www.udemy.com/ (дата звернення: 04.11.2025).

12. Персональна гігієнга. URL: https://osvita.diia.gov.ua/courses/personal-cyberhygiene (дата звернення: 04.11.2025).

13. Хакінг у практичному застосуванні та соціальна інженерія. URL: https://hackyourmom.com/kibervijna/nastupalna-soczialna-inzheneriya-pidgotovka-do-ataky-chastyna-3/ (дата звернення: 04.11.2025).

14. Кібергігієна: як захиститися від фішингу. URL: https://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisingu (дата звернення: 04.11.2025).

С59 **Соціальна інженерія**: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти галузь знань 12 (F) Інформаційні технології денної та заочної форм навчання / уклад.О.І.Міскевич. Луцьк: ЛНТУ, 2025. 76 с.

Конспект лекцій з дисципліни «**Соціальна інженерія**» складений відповідно до діючої програми курсу.

Призначений для здобувачів вищої освіти галузі знань 12 (F) Інформаційні технології.

Комп’ютерний набір О.І. Міскевич

Редактор О.І. Міскевич

Підп. до друку «___» _____ 2025р.
Формат 60х84/16. Папір офс. Гарнітура Таймс.
Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоцій
Луцького національного технічного університету
43018, м. Луцьк, вул. Львівська, 75