КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.294303
УДК 004.05

Легомінова Світлана Володимирівна
доктор економічних наук, професор,
завідувач кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Щавінський Юрій Віталійович
кандидат технічних наук, доцент,
доцент кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-2319-8983
yushchavinsky@ukr.net

Рабчун Дмитро Ігорович
кандидат технічних наук,
доцент кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-5555-0910
rabchundima92@gmail.com

Запорожченко Михайло Михайлович
аспірант кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

Будзинський Олександр Володимирович
аспірант кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0002-2402-0711
oleksandr.email@gmail.com

НЕБЕЗПЕКА ІНСТРУМЕНТІВ OSINT ТА СПОСОБИ ПОМ'ЯКШЕННЯ НАСЛІДКІВ ЇХ ВИКОРИСТАННЯ ДЛЯ ОРГАНІЗАЦІЇ

Анотація. У статті розглядаються стратегії, спрямовані на пом'якшення негативних наслідків кібератак шляхом використання інструментів розвідки відкритих джерел (OSINT). Визнаючи факт неможливості повного запобігання збору даних про організацію через значну кількість інформаційних джерел, в тому числі і відкритих, починаючи зі ЗМІ, соціальних мереж і закінчуючи всім, що публікується в інтернеті, організаціям необхідно бути готовим до запобігання або протидії наслідкам використання цієї інформації зі злим наміром. Ключовим елементом цієї готовності є акцентування уваги на належному навчанні персоналу та формуванні ініціатив з підвищення обізнаності, що мають включати як правила поводження з інформацією (наприклад, щодо того, які дані не слід публікувати в соціальних мережах, якою інформацією не варто ділитися зі знайомими в усних розмовах чи листуванні), так і огляд сучасних тактик соціальної інженерії (SE), які використовують наявну у вільному доступі інформацію для маніпулювання співробітниками організації. Також керівництво організації повинно забезпечити створення надійних внутрішніх каналів комунікації, присвячених питанням інформаційної безпеки (ІБ). Крім того, у статті підкреслюється важливість моніторингу інформаційного простору як проактивного заходу, спрямованого на протидію потенційним кіберзагрозам. До того ж, було досліджено переваги, пов'язані з впровадженням сегментації мережі та ефективним управлінням правами користувачів в рамках організації. Зазначені аспекти повинні розглядатися комплексно, що дозволить

забезпечити багатогранний підхід до забезпечення стійкості організації перед обличчям постійно еволюціонуючих кіберзагроз.

Ключові слова: соціальна інженерія; OSINT; кіберрозвідка.

ВСТУП

У сучасному цифровому просторі, де значні об’єми інформації стають доступними у відкритому доступі, інструменти OSINT надають широкий спектр можливостей для отримання даних щодо фізичних та юридичних осіб з різних відкритих джерел. Хоча використання OSINT може бути спрямоване на корпоративну розвідку (Business Intelligence) для отримання конкурентної переваги в корпоративному сегменті або для виявлення та прогнозування загроз ІБ (OSINT-моніторинг), ці інструменти нерідко використовуються зловмисниками для планування та проведення кібератак на організації, які є особливо ефективними у поєднанні з методами SE.

Постановка проблеми. За останні роки по всьому світу можна спостерігати масштабні кібератаки, причиною яких стало вдале застосування кіберзлочинцями SE. Додатково до цього численні звіти щодо актуальних кіберзагроз підтверджують зростаючу популярність кібератак з використанням тактик SE, які постійно вдосконалюються за рахунок наявності значного обсягу інформації про користувачів, співробітників та інфраструктуру організацій у вільному доступі. З огляду на недостатню захищеність особистих даних співробітників, паролів, портів, а також наявність інших даних, які можуть бути використані для реалізації кібератаки, виникає потреба у впровадженні додаткового захисту з врахуванням знань зловмисника про дані, які можуть бути отримані ним внаслідок застосування інструментів OSINT.

Аналіз останніх досліджень і публікацій. У роботі [1] автор детально розглядає підхід до проведення цільових фішингових атак у тестах на проникнення, базуючись на інформації, зібраній з відкритих джерел. Однак, слід відзначити, що у цьому дослідженні акцент робиться переважно на SE, тоді як аспекти захисту від таких атак детально не розглядаються. У роботі [2] автори проводять аналіз інструментів OSINT в контексті ІБ, класифікуючи різні види кібершахрайства та методи розслідування інцидентів, використовуючи OSINT. У статті [3] автори виконують докладний аналіз інструментів OSINT, співставляючи їх з етапами Cyber Kill Chain та використовуючи у симуляціях кібератаки. В той же час тема захисту від подібних атак у згаданих роботах залишається недостатньо висвітленою. Отже, важливо подальше наукове дослідження зосередити на розробці та вдосконаленні стратегій захисту та пом’якшення наслідків від використання інструментів OSINT проти організації, враховуючи висновки зазначених робіт.

Метою статті є аналіз способів пом’якшення наслідків здійснення проти організації кібератак з використанням інформації, зібраної за допомогою інструментів OSINT.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

OSINT (Open-source intelligence), або розвідка по відкритим джерелам, представляє собою збір і аналіз інформації, яка була отримана з різноманітних загальнодоступних інформаційних джерел. В широкому розумінні до таких джерел відносяться [4]:

– традиційні ЗМІ (газети, радіо, телебачення, журнали);

- все, що публікується в інтернеті (соціальні мережі, блоги, форуми, онлайн-бази даних, в яких можна знайти особисті думки, враження, неформальні обговорення та іншу інформацію про окремих осіб чи організації);
- корпоративні дані, доступні для громадськості (фінансові звіти або інша інформація про організацію, яка дозволяє отримати розуміння питань стратегії розвитку, ефективності управління та інших ключових аспектів її діяльності);
- урядова інформація (судові справи, публічні слухання, публічні документи);
- конференції та семінари, наукові статті, журнали, тези, дисертації, дослідження (відомості про новітні технології, наукові відкриття та напрямки розвитку у відповідних галузях);
- фотографії (візуальне уявлення про об'єкти, події чи обставини, що може бути важливим для повноти зібраної інформації);
- геопросторова інформація (картографічні дані, координати та інші параметри, що додають просторовий контекст до зібраної інформації).

На сучасному етапі розвитку IT-середовища, OSINT переважно визначається як процес збору та аналізу інформації, яка оприлюднена у мережі Інтернет. Часто зловмисники використовують методологію OSINT для планування атаки на організацію, оскільки для збільшення ймовірності успішності атаки їм необхідно мати значний обсяг інформації щодо структури організації та її персоналу. Це включає в себе, зокрема, пошук інформації про використовуване програмне забезпечення (ПЗ), апаратні компоненти, мови програмування, виявлення нових точок входу, доменні імена, а також облікові записи, які можуть бути активними в цільових веб-додатках. Пошук також може допомогти виявити можливі вразливості в системі та інші аспекти, що можуть бути використані для отримання несанкціонованого доступу.

Особливо цінними ресурсами для зловмисників, які не вживають просунутих технологічних інструментів, таких як експлойти нульового дня чи складне шкідливе ПЗ, і надають перевагу SE, є різноманітні місця публічного спілкування, які включають в себе чати, форуми, соціальні мережі та месенджери. Такі платформи надають зловмисникам можливість взаємодіяти з потенційними жертвами, вивчати їхні звички та схильності і використовувати цю інформацію для вдалих атак з використанням прийомів SE.

Законність та етичність OSINT. Законність використання інструментів OSINT в значній мірі визначається юрисдикцією та використовуваними методами збору даних. Загальною характеристикою OSINT є збір інформації із загальнодоступних джерел, доступ до яких у багатьох країнах вважається законним, проте законність цієї діяльності може ставати під питання при аналізі способу отримання інформації, цілей її збору та подальшого використання [5]. Наприклад, в ЄС практику OSINT регулюють різноманітні нормативні акти, основним з яких вважається Загальний регламент про захист даних (GDPR), основна увага в якому приділяється фундаментальним правам людини в цифрову епоху, обов'язкам тих, хто обробляє дані, методам забезпечення їх дотримання, а також санкціям для тих, хто порушує встановлені правила. Незважаючи на те, що GDPR не забороняє використання інструментів OSINT, він встановлює певні вимоги в контексті обробки персональних даних (PII), наприклад, збір PII повинен бути проведений законно, прозоро та має обмежуватися лише тими даними, які необхідні для досягнення конкретної цілі. І хоча збір даних з метою особистого збагачення може розглядатися в рамках закону, використання їх у комерційних цілях, а також для наклепу чи маніпуляцій, може призвести до виникнення юридичних наслідків.

Окрім юридичних аспектів, важливу роль відіграють етичні міркування. Сам факт того, що інформація перебуває в публічному доступі, не означає автоматичної етичної обґрунтованості її збору або поширення. Важливо дотримуватися принципів етики та поважати нюанси конфіденційності, навіть під час обробки, на перший погляд, загальнодоступної інформації. Деякі країни навіть вживають заходів для захисту від неправомірного використання OSINT, вимагаючи попереднього декларування намірів перед отримання доступу до даних.

Таким чином, незважаючи на те, що OSINT в значній мірі функціонує у сфері публічного доступу і в більшості своїй не вважається незаконним, це не надає необмежених прав на збір чи використання інформації.

Захист від OSINT. Ускладнення захисту від OSINT обумовлене переважно пасивним характером цього методу збору інформації, цифрові сліди діяльності якого практично неможливо відстежити. У статті не розглядаються методи активної розвідки, що передбачають взаємодію з інфраструктурою організації, такі як сканування портів, перебір директорій тощо. Ці методи породжують значну кількість log-файлів в SIEM-системах і тригерів в SOC, тому активна діяльність легко виявляється. Проте навіть при відсутності єдиного універсального методу захисту існують різноманітні практики, які сприяють захисту організації та її персоналу.

Навчання, підвищення обізнаності персоналу та внутрішні комунікації. Для захисту від наслідків використання OSINT через співробітників важливо здійснювати навчання, підвищувати рівень обізнаності персоналу та удосконалювати внутрішню комунікацію. Оскільки соціальні мережі часто виступають основним джерелом інформації для OSINT, а отримані результати можуть бути використані для проведення кібератак, зокрема з використанням SE, організації слід приділяти особливу увагу людському фактору.

Однією з причин успішності кібератак з використанням SE вважаються недостатньо налаштовані внутрішні комунікації з питань кібербезпеки. Для багатьох працівників організації, таких, як відділ продажів, логістика, бухгалтерія тощо, кібербезпека не вважається пріоритетним завданням, тобто для деяких з них рекомендації щодо базових заходів безпеки, наприклад, уникання використання однакових паролів чи утримання від завантаження підозрілих вкладень, можуть бути незрозумілими або невідомими.

Тому в першу чергу необхідно вдосконалити внутрішні комунікації з питань ІБ [6]. В ідеалі відповідальна за це особа повинна мати технічний бекграунд, володіти знаннями щодо загроз і методів захисту від них, а також володіти навичками ефективного спілкування з персоналом. Це може бути працівник відділу внутрішніх комунікацій, а у випадку відсутності такого відділу в організації, можна залучити співробітника відділу кадрів (HR) та надати йому/їй відповідні навички. Зазвичай працівники відділу HR добре обізнані з роботою зі співробітниками та їхніми обов'язками, що сприяє ефективному визначенню ризиків, яким піддаються відділи, і визначенню пріоритетів у наданні інформації співробітникам різних спеціалізацій.

Під час навчання необхідно приділяти особливу увагу таким темам, як потенційні загрози, актуальні тактики SE в контексті діяльності організації, а також методи захисту та процедури реагування на підозрілу активність. Два ключові аспекти, які слід враховувати, полягають у тому, щоб, по-перше, переконатися, що весь персонал розуміє ризики та наслідки розміщення чутливої інформації про себе чи організацію в соціальних мережах або інших загальнодоступних джерелах, і, по-друге, проводити тренування та навчання персоналу з реагування на електронні листи, телефонні дзвінки та

повідомлення, які спонукають до вчинення потенційно небезпечних дій. Співробітники повинні мати чітке розуміння того, що вважається потенційно небезпечними діями, а також мають виявляти готовність до відповідного реагування на такі ситуації.

Чутлива інформація, яку персонал може розміщувати у загальнодоступних джерелах, включає, але не обмежується такими елементами:

- персональна інформація (імена, фізичні та електронні адреси, номери телефонів колег, членів керівництва);
- професійна інформації (деталі проєктів, над якими працює організація, конфіденційних робочих завдань працівників);
- фінансова інформація (деталі щодо прибутку, витрат, прибутковості та інших фінансових аспектів організації);
- корпоративні події (внутрішні заходи, семінари, конференції, в яких приймає участь організація);
- кадрові питання (інформація про зайнятість, процес підбору персоналу та інші кадрові аспекти, взаємини з колегами);
- партнерські відносини (чутлива інформація про клієнтів, партнерів, постачальників);
- фотографії виробничих приміщень чи обладнання (будь-які зображення, які можуть ненавмисно розкривати технічні аспекти роботи, особливості технічної інфраструктури, застосовуваних IT-технологій);
- інформація про внутрішні процеси (внутрішні аспекти виробництва, логістики чи інших ключових функції організації) і т. д.

Організація навчання персоналу вищезазначеним аспектам може бути здійснена різними способами. Можна використовувати власні ресурси, розробляючи та проводячи програму тренінгів, а також формуючи інструкції з ІБ для нових співробітників. Також існує можливість залучити зовнішніх спеціалістів для проведення тренінгів та навчання, або використовувати інтерактивні платформи для підвищення обізнаності персоналу. Кожен із цих підходів має свої переваги та може бути адаптований під конкретні потреби та наявні ресурси організації.

Контррозвідка або OSINT-моніторинг. OSINT-моніторинг представляє собою систематичне проведення розвідки щодо власної організації або клієнтів власними силами, через послуги аудиту чи інші спеціалізовані сервіси. Цей процес включає в себе збір та аналіз інформації з різноманітних відкритих джерел, таких як соціальні мережі, форуми, даркнет, з метою моніторингу бренду, репутації, а також виявлення потенційних загроз та кібершахрайства [7]. Для цього можна використовувати різноманітні інструменти в залежності від цілей пошуку, наприклад, Shodan, Maltego, Recon-ng, theHarvester тощо.

Однією з головних переваг OSINT-моніторингу є можливість для організації побачити свою інформацію через очі потенційних зловмисників. Особливо важливою стає можливість виявлення та реагування на активність зловмисників на етапі збору інформації, коли їхня основна мета може бути не сама кібератака, а продаж інформації іншим кіберзлочинцям. Так, наприклад, знання про те, що дані про організацію виставляються на продаж у даркнеті, дозволяє їй вчасно виявити потенційні атаки і краще підготувати працівників та аналітиків ІБ та вжити відповідних заходів для попередження цих атак, базуючись на розумінні того, який обсяг інформації є у розпорядженні зловмисників. Наприклад, це може включати в себе видалення чутливих даних, посилення моніторингу, або навіть поширення дезінформації для збентеження зловмисників.

Оскільки методи OSINT визначаються передусім пасивно-спостережливим характером, виявлення самого процесу збору даних та навчання користувачів ефективному поводженню себе з метою запобігання збору інформації зловмисниками виявляється надзвичайно складним завданням. У численних випадках джерелами інформації для OSINT можуть бути облікові записи користувачів, проте організація не завжди може змусити користувача видалити конкретні дані з соціальних мереж, якщо лише це не суперечить правам інтелектуальної власності чи іншим юридичним нормам.

Під час впровадження та реалізації програми OSINT-моніторингу пріоритетним завдання слід вважати пошук даних, які могли б потенційно становити ризики для діяльності організації. Одним з етичних аспектів OSINT-моніторингу є важливість уникання його використання як інструменту для ведення спостереження чи втручання в особисте життя працівників.

У разі рішення організації впроваджувати власну програму OSINT-моніторингу, важливо визначити параметри та межі аналізу. При цьому належить визначити, що необхідно перевіряти, коли і в який спосіб проводити тестування. Оскільки співробітники можуть оприлюднювати інформацію в будь-який момент, доцільним рішенням є використання періодичного тестування (щомісячне, щоквартальне) для ефективного моніторингу. До додаткових аспектів, які потребують уваги, можна віднести визначення типу тестування (автоматизоване, ручне), встановлення бюджету (з метою оцінки можливості залучення третіх сторін та користування платними сервісами), визначення рівня глибини взаємодії, охоплення, а також розробку методів забезпечення дотримання права співробітників на приватне життя і можливість публікації повідомлень у соціальних мережах.

У процесі OSINT-моніторингу важливо враховувати, що організація повинна зберігати певний контроль над інформацією, що розміщується у відкритому доступі постачальниками, співробітниками, підрядниками та партнерами. Проте, необхідно утримуватися від моніторингу особистого обміну інформацією між співробітниками або їхніми друзями. Заборонено змушувати осіб встановлювати зв’язок у соціальних мережах та використовувати підроблені облікові записи для спроб долучення до списків друзів. В подібних практиках важливо дотримуватися високих стандартів конфіденційності та етики, щоб забезпечити не тільки безпеку інформації, але й захист особистого середовища працівників.

З метою збереження етичного характеру рекомендується передавати функції OSINT-моніторинг на аутсорсинг. Це сприяє збереженню відстані між командою з ІБ організації та особистими обліковими записами співробітників, що зменшує ймовірність звинувачень у переслідуванні [8]. Окрім цього, залучення спеціалізованих третіх сторін є більш ефективним рішенням за рахунок того, що вони систематично відсіюють сторонню інформацію, що не стосується питань безпеки, часто за допомогою автоматизованих веб-сканерів та надають організації лише актуальні дані.

Сегментація мережі та управління правами користувачів. У випадку, коли зловмисник набуває контролю над хостом, він може використовувати його вразливості для отримання НСД до внутрішньої мережі та зараження інших хостів. З метою запобігання цьому сценарію важливим заходом є належна сегментація мережі. Сегментація мережі є методом забезпечення мережевої безпеки, що полягає у розділенні мережі на менші, ізольовані підмережі (рис. 1) [9]. Цей підхід дозволяє мережевим адміністраторам відокремлювати підмережі та налаштовувати унікальні заходи безпеки для кожної із них, такі, як визначення політик та параметрів безпеки, а також обмеження потоку даних між цими підмережами. Це дозволяє зменшити ризик розповсюдження

атаки по мережі, оскільки компрометація одного сегменту автоматично не веде до компрометації інших. Крім того, такий підхід полегшує впровадження і управління заходами безпеки та обслуговуванням мережі в цілому.

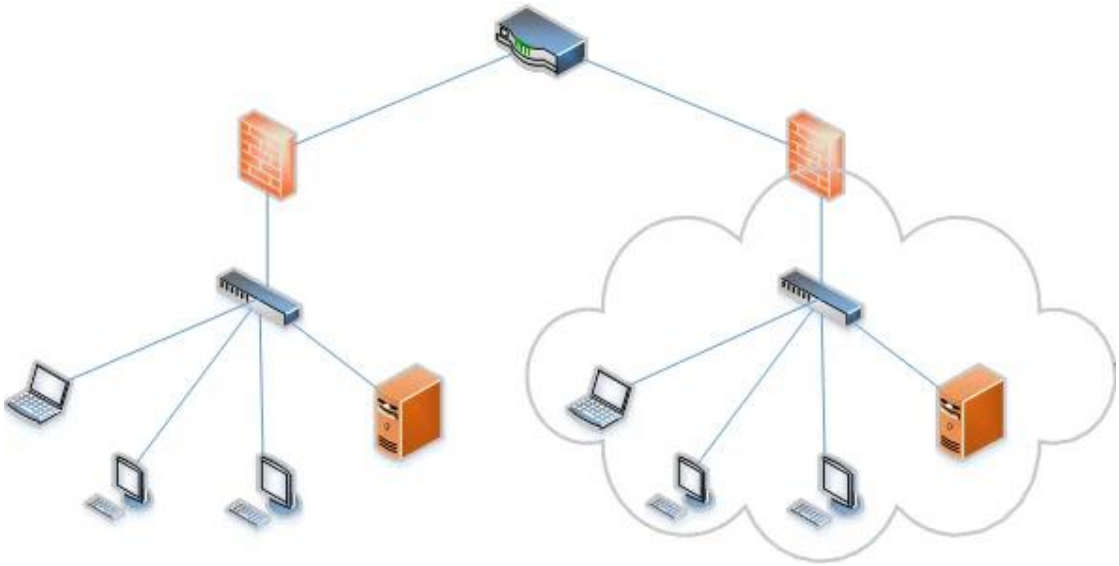

Рис. 1. Принцип сегментації мережі [9]

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Інструменти OSINT є доволі потужним інструментом, як в руках кіберзлочинців, так і спеціалістів з ІБ. Варто пам’ятати, що чим більшим обсягом інформації про організацію володіє зловмисник, тим більша ймовірність для неї зазнати збитків від вдалої кібератаки. Не існує універсального інструменту для захисту від збору даних про організацію, проте існують превентивні заходи, які дозволяють пом’якшити наслідки інцидентів:

- вдосконалення внутрішніх комунікацій щодо ІБ, навчання та підвищення обізнаності персоналу для обмеження оприлюднення чутливої інформації, яка в подальшому може бути використана для проведення соціоінженерних атак та інших загроз, а також з метою забезпечення захисту від таких атак;
- проведення OSINT-моніторингу для отримання чіткого розуміння того, яка інформація щодо організації може перебувати в розпорядженні потенційних атакуючих, сприяючи належній підготовці до можливих інцидентів;
- впровадження сегментації мережі, ефективного управління правами користувачів та інших програмно-апаратних заходів безпеки з метою обмеження поширення інцидентів по мережі організації.

Таким чином, впровадження ефективних заходів захисту від збору інформації за допомогою відкритих джерел є невід’ємною складовою стратегії забезпечення кібербезпеки для сучасних організацій. Наведені в статті превентивні заходи сприяють зменшенню ризиків кіберзагроз і визначають необхідність постійного вдосконалення заходів ІБ. Такий підхід дозволяє організаціям ефективно протидіяти потенційним загрозам та забезпечувати стабільність їхньої інформаційної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Meyers J. (2018). *Training Security Professionals in Social Engineering with OSINT and Sieve. All Theses and Dissertations.* https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=7863&context=etd
2. Tabatabaei, F., & Wells, D. (2016). OSINT in the Context of Cyber-Security. *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications.* https://doi.org/10.1007/978-3-319-47671-1_14
3. Yamin M., Ullah M., Ullah H., Katt B., Hijji M., & Muhammad K. (2022). Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. *Mathematics, 10(12):2054.* https://doi.org/10.3390/math10122054
4. Weber, J. (2023). *Is OSINT legal? The legal and ethical concerns of using open-source intelligence.* https://corma-investigations.com/uncategorized/is-osint-legal-the-legal-and-ethical-concerns-of-using-open-source-intelligence/
5. Molfar. (n. d.). *From Public Data to Deep Web: Advanced OSINT Techniques Revealed.* https://molfar.com/en/blog/top-osint-techniques
6. Moreau, P. (2024). *The Crucial Role of HR in Communicating with Employees After a Cyber Attack.* https://www.linkedin.com/pulse/crucial-role-hr-communicating-employees-after-cyber-dr-phyllis-rgs9c?trk=public_post_main-feed-card_feed-article-content
7. Gray, J. (2021). *Practical Social Engineering. A Primer for the Ethical Hacker.*
8. Flynt, R. (2024). *Open-Source Intelligence (OSINT) for Business: Gaining a Competitive Edge.* https://www.linkedin.com/pulse/open-source-intelligence-osint-business-gaining-edge-robert-flynt-93llf
9. Kambic, D., & Fricke, J. (2020). *Network Segmentation: Concepts and Practices.* Carnegie Mellon University, Software Engineering Institute's Insights (blog). https://doi.org/10.1184/R1/13118312.v1
10. *Nate Lord. What is the Principle of Least Privilege (POLP)?* (2023). https://www.digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Svitlana Lehominova
Doctor of Economic Sciences, Professor,
Head of Department of Information and Cyber Security Management
Work place: State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Yurii Shchavinsky
PhD, Associate Professor,
Professor of Department of Information and Cyber Security Management
Work place: State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-2319-8983
yushchavinsky@ukr.net

Dmytro Rabchun
PhD, Associate Professor of Department of Information and Cyber Security Management
Work place: State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-5555-0910
rabchundima92@gmail.com

Mykhailo Zaporozhchenko
PhD student of Department of Information and Cyber Security Management
Work place: State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

Oleksandr Budzynskyi
PhD student of Department of Information and Cyber Security Management
Work place: State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0002-2402-0711
oleksandr.email@gmail.com

THE THREATS OF OSINT TOOLS AND WAYS TO MITIGATE THE CONSEQUENCES OF THEIR APPLICATION FOR THE ORGANIZATION

Abstract. This article examines strategies aimed to mitigate the negative effects of cyberattacks through the use of open-source intelligence (OSINT) tools. Accepting the fact that it is impossible to completely prevent the collection of data about organizations through a significant number of information sources, including open sources (media, news, forums, social media and almost everything published on the Internet), organizations need to be prepared to prevent or counteract the consequences of using this information with malicious intent. A key element of this readiness is to focus on proper staff training and awareness-raising initiatives that include both rules for handling information, such as what information should not be posted on social media, shared with colleagues in verbal conversations or correspondence, and an overview of modern social engineering tactics that use publicly available information to manipulate the organization's employees. The organization's management should also ensure the creation of reliable internal communication channels dedicated to information security issues. In addition, the article emphasizes the importance of monitoring the information space as a proactive measure aimed at countering potential cyber threats. In addition, the benefits associated with the implementation of network segmentation and effective management of user rights, such as the Principe of least privilege (PoLP)—the principle of providing access to resources, where each process, user or program should have access only to the information and resources that are minimally necessary for the successful completion of their work tasks, within the organization were investigated. The mentioned aspects should be considered in a comprehensive manner, which will ensure a multifaceted approach to ensuring the organization's resilience in the face of constantly evolving cyber threats.

Keywords: social engineering; OSINT; threat intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Meyers J. (2018). *Training Security Professionals in Social Engineering with OSINT and Sieve. All Theses and Dissertations.* https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=7863&context=etd
2. Tabatabaei, F., & Wells, D. (2016). OSINT in the Context of Cyber-Security. *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications.* https://doi.org/10.1007/978-3-319-47671-1_14
3. Yamin M., Ullah M., Ullah H., Katt B., Hijji M., & Muhammad K. (2022). Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. *Mathematics, 10(12):2054.* https://doi.org/10.3390/math10122054
4. Weber, J. (2023). *Is OSINT legal? The legal and ethical concerns of using open-source intelligence.* https://corma-investigations.com/uncategorized/is-osint-legal-the-legal-and-ethical-concerns-of-using-open-source-intelligence/
5. Molfar. (n. d.). *From Public Data to Deep Web: Advanced OSINT Techniques Revealed.* https://molfar.com/en/blog/top-osint-techniques
6. Moreau, P. (2024). *The Crucial Role of HR in Communicating with Employees After a Cyber Attack.* https://www.linkedin.com/pulse/crucial-role-hr-communicating-employees-after-cyber-dr-phyllis-rgs9c?trk=public_post_main-feed-card_feed-article-content
7. Gray, J. (2021). *Practical Social Engineering. A Primer for the Ethical Hacker.*
8. Flynt, R. (2024). *Open-Source Intelligence (OSINT) for Business: Gaining a Competitive Edge.* https://www.linkedin.com/pulse/open-source-intelligence-osint-business-gaining-edge-robert-flynt-93llf
9. Kambic, D., & Fricke, J. (2020). *Network Segmentation: Concepts and Practices.* Carnegie Mellon University, Software Engineering Institute's Insights (blog). https://doi.org/10.1184/R1/13118312.v1
10. *Nate Lord. What is the Principle of Least Privilege (POLP)?* (2023). https://www.digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance