Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній рівень ***магістр***
(назва освітнього рівня)

кваліфікація
(код і назва кваліфікації)

на тему: *Виявлення та ідентифікація векторів атак на основі аналізу ключових метрик ІС*

Виконавець: студент *2* **курсу, групи** *КБм-21*

Казанцев Андрій Андрійович
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	Оцінка	Підпис
Науковий керівник	*Бабенко Т. В.*		
Рецензент	*Ткач В. М.*		
Нормоконтроль	*Фесенко А. О.*		

Київ 2022

Міністерство освіти і науки України

Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації

_____ Лукова-Чуйко Н.В.

«_____»_____20___року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту *КБм-21* (група) *Казанцеву Андрію Андрійовичу* (прізвище ім'я по-батькові)

Тема дипломної роботи *Виявлення та ідентифікація векторів атак на основі аналізу ключових метрик ІС*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *Процес виявлення та ідентифікації векторів атак. на основі ключових метрик інформаційних систем*

Предмет досліджень *Методи визначення ключових метрик ІС*

Мета *Виявлення та ідентифікація векторів атак на основі ключових метрик інформаційних систем*

Вихідні дані для проведення роботи *Існуючі кібератаки та методи управління ризиками. Дата майнинг.*

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *Зменшення часу реагування на нові кібератаки та підвищення здатності реагувати на атаки нульового дня завдяки реалізації та залученню дата майнингу у аналізі попередніх даних*

Практична цінність *зменшення збитків організацій в результаті кібератак за рахунок мінімізації кількості можливих сценаріїв для реалізації*

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Виконання
Розробка плану для досягнення мети роботи	29.10.2021 – 30.11.2021	*Виконано*
Аналіз літературних джерел	31.11.2021 – 30.03.2022	*Виконано*
Розробка методу виявлення та ідентифікації векторів атак на основі ключових метрик ІС	01.04.2022 – 30.04.2022	*Виконано*
Оформлення і друк пояснювальної записки	01.05.2022 – 17.05.2022	*Виконано*

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *Зниження збитків через викрадення, пошкодження, шифрування даних*

Соціальний ефект .

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____Бабенко Т.В.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ ____Казанцев А.А.
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____
Термін подання дипломної роботи до ЕК _____

УДК 004.492.2

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Виявлення та ідентифікація векторів атак на основі аналізу ключових метрик ІС» складається зі списку скорочень, вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел. Загальний обсяг роботи – 62 сторінки. Робота містить 15 рисунків. Список використаних джерел включає 31 джерело.

Об'єкт дослідження – процес виявлення та ідентифікації векторів атак на основі ключових метрик інформаційних систем.

Мета роботи – виявлення та ідентифікація векторів атак на основі ключових метрик інформаційних систем.

Предмет дослідження – методи визначення ключових метрик.

Метод дослідження – синтез наявних даних про кібератаки та стандарти у сфері управління ризиками, а також методів дата-майнингу, аналіз та оцінка консолідованої інформації.

Практичне значення роботи полягає у рекомендації методу, використання якого допоможе зменшити збитки організацій в результаті кібератак за рахунок мінімізації можливих сценаріїв для реалізації.

Результати здійснених у дипломній роботі досліджень можуть бути реалізовані спеціалістами із захисту інформації та при подальшому проведенні науково-дослідницьких робіт в сфері управління ризиками та побудови систем виявлення векторів атак. Пропонований метод може бути рекомендований для використання в корпоративних мережах для поглибленого аналізу ризиків інформаційної безпеки з можливістю визначення векторів атак, а також для оцінки ефективності системи захисту інформації в організації.

Напрямки подальших досліджень: покращення та оптимізація пропонованої методики способом тестування інших методів дата майнингу у даній сфері з метою

збільшення точності прогнозування, збільшення рівня абстракції на рівні прийому даних для більше швидкого винесення результату у ході аналізу отриманих даних.

Ключові слова: ризик, дата майнинг, оцінка ризику, управління ризиками, зменшення ризику, ризик інформаційної безпеки, інтелектуальні моделі оцінки ризику, аналіз ризиків інформаційної безпеки, інцидент інформаційної безпеки, дата майнинг, метрики інформаційної системи, прогнозне моделювання, кіллчейн, корпоративна мережа, загроза, вразливість, бекдор, експлойт.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АСУ – Автоматизована система управління

ІБ – Інформаційна система

ІТС – Інформаційно-телекомунікаційні системи

ОС – Операційна система

ПЗ – Програмне забезпечення

ПК – Персональний комп’ютер

API – Application programming interface

APT – Advanced Persistent Threat

HTTP – HyperText Transfer Protocol

IDS – Intrusion Detection System

SMB – Server Message Block

ВСТУП

Інформаційні технології з часом стали постійним супутником бізнесу та організацій будь-яких розмірів та форм власності. Для більше ефективного керування організації безупинно впроваджують нові програмні та мережеві рішення, тим самим все більш тісно пов’язуючи свою діяльність з інформаційним простором та з інформаційними та інформаційно-телекомунікаційними системами. Це, у свою чергу, приваблює багатьох хакерів до бажаної здобичі у вигляді фінансів або ж цінних даних, через що великими темпами збільшується кількість кібератак.

У зв’язку з постійним зростанням кількості кібератак на цільові системи, існує незмінна необхідність у захисті своїх інформаційних активів. На сьогоднішній день існує багато програмних засобів кіберзахисту від різних виробників, котрі необхідно використовувати у комбінації між собою. Проте, вони не надають повноцінного захисту від усіх кібератак, а особливо від так званих атак «нульового дня». Найбільш дієвим засобом боротьби з такими атаками можуть бути системи, які реагують на підозрілу активність, або ж попереднє налаштування систем з використанням дата майнингу, за допомогою якого стає можливим збір великої кількості даних та побудова унікальної моделі захисту, що дозволить не захисититися від атаки, але попередити її, завчасно визначивши потенційний вектор атаки, або той, що вже реалізується.

РОЗДІЛ І
РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ПОСТАНОВКА ЗАДАЧІ

1.1. Ризики інформаційної безпеки

Інформаційні технології на сьогоднішній день є дуже дієвим інструментом для ведення бізнесу, що призводить до збільшення загального об’єму використання їх для вирішення тих чи інших задач.

Лише факт використання інформаційних технологій передбачає можливі кібератаки, кінцевою метою яких можуть бути крадіжка даних, пошкодження даних або обладнання та, звісно, шифрування даних задля вимагання грошової суми для розшифрування.

За інформацією СБУ, кількість кібератак на електронні ресурси органів влади та стратегічно важливі об'єкти критичної інфраструктури. щорічно збільшувалася. Так, у 2019-му році загальне число атак склало 480, у 2020-му 600, а у 2021-му – вже 2200 кібератак.

Рисунок 1.1 - Інфографіка кібератак на державні органи України за даними СБУ станом на 15.02.2022

Лише у січні 2022-го року було зафіксовано 121 кібератаку тільки на інформаційні системи органів державної влади.

Українські державні органи, та й державні органи інших країн, є не єдиною мішенню зловмисників, атак зазнає і приватний бізнес. Згідно з даними Parachute Technologies, загальні фінансові втрати приватного сектору від кібератак у 2020-му році склали 945 мільярдів доларів, що на 50% більше, аніж прогнозовані втрати у 2018-му році (522.5 мільярдів доларів).

Також Parachute Technologies відмічають, що середня вартість втрат для організацій із повністю автоматизованою системою безпеки склала 2.45 мільйонів доларів, у той час як інші організації понесли збитків на 6.03 мільйони.

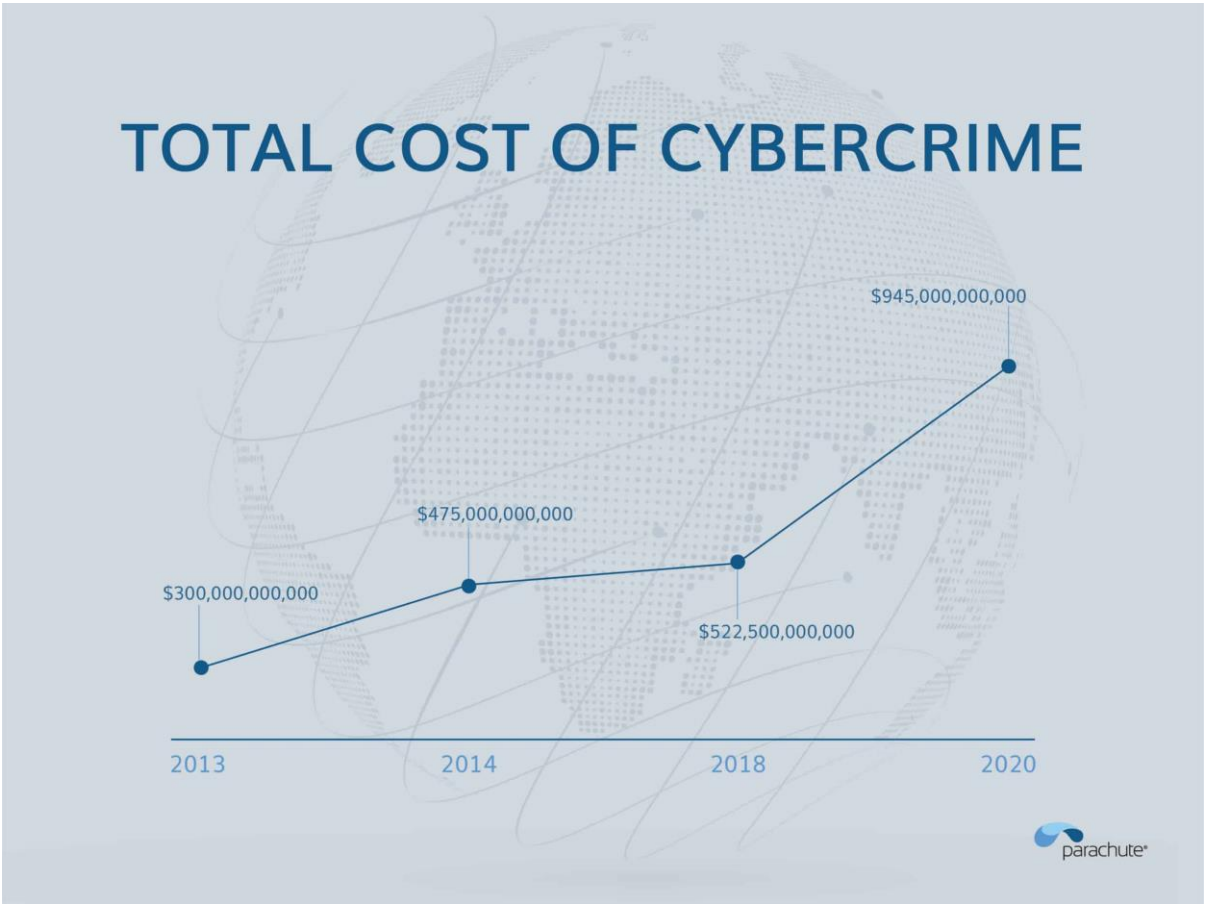

Рисунок 1.2 - Тенденція зросту втрат від кібератак з 2013-й по 2020-й роки відповідно до дослідження Parachute Technologies

Згідно з дослідження Cybint за 2020-й рік, 43% усіх кібер-атак прийшлися на малий бізнес. З цих компаній, 64% зазнали веб-орієнтованих атак, з яких, у свою

чергу: 62% - на основі фішингу та соціальної інженерії, 59% зазнали експлуатації шкідливого коду та атаки ботнетів, 51% відчули на собі DoS атаки.

За інформацією, зібраною Purplesec, у 2018-му році щодня відбувалося до 80 тисяч кібератак, або ж до 30 мільйонів на рік, з усіх досліджених файлів 21% не були ніяк захищені, а 41% компаній мають більше ніж тисячу файлів, у яких міститься критична інформація (номери кредитних карток, лікарняні записи пацієнтів тощо) без якого-небудь захисту, 65% опитаних організацій мають більш ніж 500 користувачів, які ніколи не змінювали свої паролі. Кількість атак з використанням програм-вимагачів збільшується щорічно на 350%, а кількість атак, спрямованих на IoT, збільшилася на 650%. Зловмисники знають, що багато підприємств не вкладаються у кібербезпеку власних цифрових інфраструктур через те, що більшу частину часу вкладені у засоби безпеки кошти ніяк не конвертуються у прибуток або відсутність втрат. Саме тому існує безліч випадків реалізацій ризиків інформаційної безпеки.

1.2. Оцінка ризиків інформаційної безпеки на рівні організації

Для кожної організації є важливим процес оцінки ризиків для формування процедури реакції та зменшення потенціальних збитків у майбутньому.

1.2.1. Процес оцінки ризиків

Одним з головних інструментів у боротьбі організацій з ризиками є управління ризиками.

Ризик інформаційної безпеки являє собою ймовірність реалізації вразливостей певними загрозами. Ціллю реалізації ризику може бути причинення збитків компанії, здобування чутливої інформації задля подальшого її викупу власниками або порушення працездатності окремих компонентів інфраструктури чи порушення основних характеристик інформації.

Загрозою ж називають можливість нанести шкоду відомими на сьогодні засобами, наприклад, за допомогою експлуатації вразливостей. Вразливість являє собою слабке місце у системі захисту, або ж безпосередньо у програмному продукті. Першопричинами виникнення вразливостей можуть бути недосконало впроваджені міри захисту, неякісний програмний код, неслідування політикам та процедурам безпеки. Як наслідок реалізації вразливостей, компанії та підприємства несуть збитки, які становлять еквівалент, необхідний для повернення системи або інформації у початковий стан.

Важливо розуміти різницю між переліченими поняттями, тому, розберемо їх трохи детальніше.

1. Рівень загрози – це міра актуальності загрози, а саме загальний рівень усіх факторів, які можуть навмисно або ненавмисно вплинути на активи шляхом використання вразливості.
2. Рівень вразливості – цей показник визначає те, наскільки легко зловмиснику проексплуатувати вразливість для обходу захисних механізмів і отримання несанкціонованого доступу до активів.
3. Рівень збитку – величина, яка визначає грошові або репутаційні втрати, спричинені інцидентом ІБ, що відбувся.

Згідно зі стандарту NIST 800-30 «Risk management guide for information technology systems» рівень ризику можна описати як функцію:

- Ймовірність спроби визначеного джерела загрози експлуатувати дану вразливість
- Величина впливу у результаті успешної реалізації вразливості
- Адекватність запланованих або впроваджених засобів контролю безпеки для мінімізації або усунення ризику.

У вигляді формули, ризик обраховується як добуток ймовірності настання інциденту ІБ та вартості активу, стосовно до якого відбувається інцидент:

$$R = N(t) \cdot L \tag{1.1}$$

де **R** – рівень ризику, **N(t) -** ймовірність реалізації загрози ІБ, **L –** потенційний об’єм збитків, ціна активу, який зазнає впливу.

Вразі необхідності врахування таких метрик безпеки як конфіденційність, цілісність та доступність, математично це можна представити наступним чином:

$$\boldsymbol{Rc} = \boldsymbol{Kc} \cdot \boldsymbol{N}(\boldsymbol{T}) \cdot \boldsymbol{N}(\boldsymbol{V}) \quad (1.2)$$

$$\boldsymbol{Ri} = \boldsymbol{Ki} \cdot \boldsymbol{N}(\boldsymbol{T}) \cdot \boldsymbol{P}(\boldsymbol{V}) \quad (1.3)$$

$$\boldsymbol{Ra} = \boldsymbol{Ka} \cdot \boldsymbol{N}(\boldsymbol{T}) \cdot \boldsymbol{N}(\boldsymbol{V}) \quad (1.4)$$

$$\boldsymbol{R}\text{ср} = \frac{\boldsymbol{Rc} + \boldsymbol{Ri} + \boldsymbol{Ra}}{\boldsymbol{3}} \quad (1.5)$$

де **Rc** – ризик порушення конфіденційності; **Kc** – коефіцієнт конфіденційності активу; **Ri** – ризик порушення цілісності; **Ki** – коефіцієнт цілісності активу; **Ra** – ризик порушення доступності; **Ka** – коефіцієнт доступності активу, **N(T)** – імовірність реалізації загрози; **N(V)** – імовірність використання уразливості;

У цьому випадку кінцевий ризик вираховується як середнє значення від суми трьох параметрів (**Rcp**).

За даними Purplesec на 2017-й рік, 70% опитаних організацій відчувають сильне зростання ризиків інформаційної безпеки і з роками загальна кількість ризиків зростає. Саме тому з’являється потреба в управлінні ризиками ІБ.

Управління ризиками являє собою процес виявлення, оцінки та контролю загроз активам організації. Також успішне управління ризиками допомагає визначити повний спектр можливих ризиків і передбачити взаємний вплив одних ризиків на інші при успішній їх реалізації (каскадний ефект). Походження загроз може бути різним, у тому числі природнім, але нас цікавлять ризики інформаційної безпеки.

Як зазначала Алла Валенте, провідний аналітик Forrester Research, спеціаліст з управління ризиками та відповідностей: «Ми не керуємо ризиками таким чином, що ми їх не маємо. Ми керуємо ризиками для того, щоб знати їм ціну і розуміти, які ризики варті нашої уваги, а які ризики ми можемо прийняти та сплатити за них певну ціну».

Спеціалісти IBM вважають, що для зменшення ризику організація повинна використовувати ресурси для того, щоб мінімізувати, моніторити і контролювати вплив негативних подій, збільшуючи до максимуму результат впливу позитивних подій. Системний та інтегрований підхід, на їх думку, допоможе визначити, як найкраще ідентифікувати, керувати та пом’якшити значні ризики.

Для кожної організації спочатку ризики та шкідливі події є невідомими та несподіваними, що може призвести до великих коштових та репутаційних втрат або ж навіть до згортання діяльності. Для зручного управління ризиками створюються Системи Менеджменту Інформаційної Безпеки (СМІБ).

Сам же процес включає у собі:

- складання плану, впровадження та моніторинг забезпечення безпеки;
- відповідність вимогам та цілям організації
- своєчасне реагування на виявлені загрози
- забезпечення відповідності міжнародним та внутрішнім політикам, стандартам і процедурам
- аудит на відповідність механізмів та актуальних цілей безпеки.

Оцінка ризиків та правильне розподілення ресурсів на протидію ним можуть значно скоротити витрати на організацію цього процесу.

Згідно стандарту ISO 31000 процес управління має наступний вигляд (Рисунок 1.3):

1. Визначення області дії, контексту та критеріїв.
2. Визначення ризику.
3. Аналіз визначеного ризику.
4. Оцінка визначеного ризику.
5. Обробка ризику (протидія, мінімізація тощо).

При цьому, весь процес супроводжується постійною комунікацією та консультаціями для запобігання випадків, коли визначні елементи процесу управління можуть випасти з поля зору.

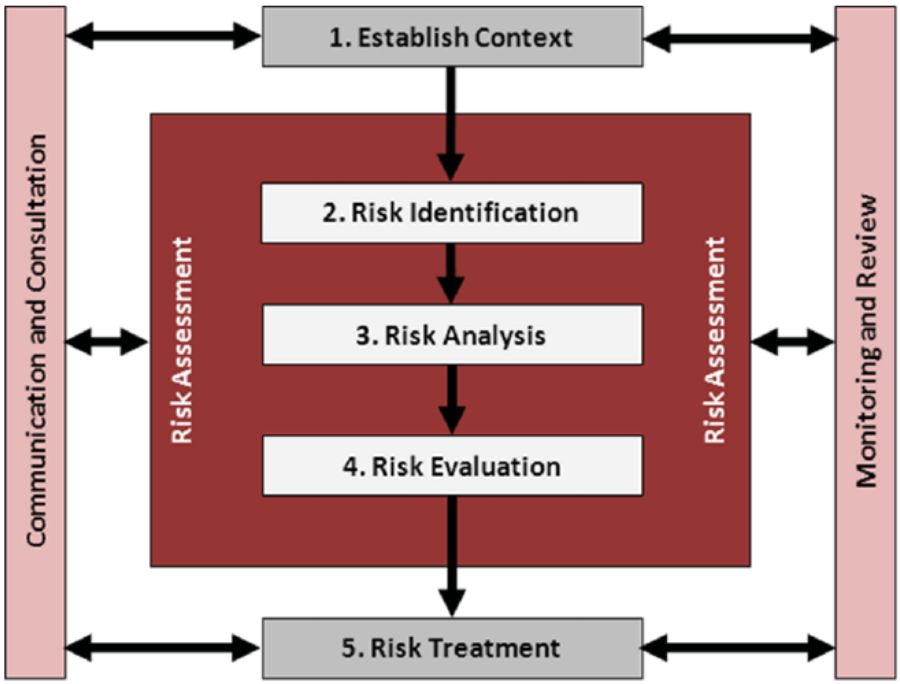

Рисунок 1.3 - Міжнародний стандарт управління ризиками ISO 31000

Дані етапи також варто розглянути у фокусі.

Першим важливим кроком є визначення прийнятного рівня ризику. Спеціалісти TechTarget для більшого зрозуміння пропонують представити це у вигляді автомобільного спідометра:

Рисунок 1.4 - Схема схильності до ризику та толерантності до ризику за версією TechTarget

- зеленим кольором (схильність до ризику) позначені ризики, які організація може прийняти і при цьому досягти своїх бізнес-цілей;
- жовтим кольором (толерантність до ризику) позначене прийнятне для організації відхилення від визначений об’ємів прийнятих ризиків;
- червоним кольором позначаються ризики, які компанія прийняти не може за будь-яких умов.

Другий крок, який являє собою ядро процесу управління ризиками, складається з ідентифікації, аналізу та оцінки ризиків.

Для прийняття корректного рішення ризики ІБ повинні бути правильно ідентифіковані та оцінені з точки зору збитків, які може понести організація у разі їх реалізації. При аналізі збитків визначається ступінь впливу ризику на активи компанії та ті бізнес-процеси, які пов’язані з активами. Оцінка може базуватися на виявленні та аналізі вразливостей, які пов’язані з активами, та загроз, реалізація яких можлива у разі експлуатації цих вразливостей.

Ідентифікація активів являє собою процес, що пов’язаний із оглядом усіх ресурсів організації, визначенням оцінки вартості даних активів та величиною їх впливу. Ідентифікація активів проводиться з урахуванням приорітету їх важливості для бізнес-процесів організації та збитків у разі необхідності відновлення.

Ідентифікація загроз являє собою процес визначення усіх факторів, які потенційно можуть шкідливо вплинути на активи. Джерело походження загроз може бути як випадковим, так і навмисним, а за природою виникнення вони можуть бути людськими або природніми. Після визначення джерела походження загрози необхідно визначити ймовірність її реалізації з використанням кількісної або якісної шкали.

Ідентифікація вразливостей являє собою процес виявлення слабких місць в системі захисту, які можуть бути скомпрометовані джерелом загрози. Вразливості можуть бути як технічними (програмне забезпечення, налаштування системи, апаратні засоби, фізичне середовище тощо) так і організаційними (менеджмент; персонал, бізнес-процеси та процедури). Наявність вразливості при цьому не завдає

шкоди у даний момент, бо для експлуатації вразливості необхідна реальна загроза. Результатом процесу ідентифікації вразливостей має бути список вразливостей з ідентифікацією загроз, які відносяться до кожної з перелічених вразливостей, а також оцінка ступеню простоти експлуатації тієї чи іншої вразливості.

Важливим також є ранжування ризиків за критеріями. Це допоможе у подальшій розробці плану реагування та протидії ризикам за визначеними приорітетами.

Слідом необхідно розробити план реагування на ризики та узгодити рішення щодо управління ними. Для обрання заходів реагування та ліквідації наслідків необхідно провести аналіз і провести порівняння з тим рівнем ризику, який організація може прийняти, а також узгодити рішення щодо управління. Можуть бути розглянуті наступні кроки:

- Уникнення ризику;
- Зниження ризику
- Прийняття ризику;
- Передача ризику;

Подальшим кроком є реалізація обраних заходів у рамках рамках реагування на ризики. Особи, що призначені відповідальними за цей процес, у визначені терміни описують необхідні заходи для реалізації процедур реагування на ризики. Не менш важливою є необхідність проведення аудиту подібних заходів для актуалізації задіяних методик. Аудит дозволить зрозуміти, чи були достатньо ефективними впроваджені рішення та чи є необхідність їх змінити, аби слідувати тренду сучасних процедур протидії ризикам.

1.2.2. Аналіз стандартів у сфері оцінювання ризиків

Управління ризиками охоплює аналіз та оцінку критичних сторін організації з точки зору реакції на зовнішній вплив, та планування запобіжних короткострокових та довгострокових дій. Управління ризиками є дуже важливою частиною стратегічних планів організацій.

Розробка стандартів та прийняття вже існуючих стандартів необхідні для досягнення прийнятних результатів у наступних питаннях:

- мета управління ризиками
- використовувана термінологія
- основні етапи та процес практичного застосування

На сьогоднішній день вже багато країн розробили стандарти у сфері аналізу та оцінки ризиків ІБ. Наприклад, до стандартів з управління ризиками відносяться наступні: ISO/IEC 31000, COSO II, FERMA, KING II. Рекомендації з менеджменту інформаційної безпеки описані у таких стандартах: ISO/IEC 27001, ISO/IEC 27005:2018, ISO/IEC 17799, BS7799, NIST 800-30, BSI-Standard 200-3, ISO/IEC 15408. Стандарти, до яких варто прислуховуватися у питаннях аудиту інформаційної безпеки: COBIT, SAS 55/78, SAC.

ISO/IEC 31000 являє собою серію стандартів, що включають у себе наступні документи:

- ISO Guide 73:2009 - Risk Management – Vocabulary (Управління ризиками. Термінологія)
- ISO 31000:2018 - Risk management - Principles and Guidelines on Implementation (Управління ризиками. Принципи і керівні вказівки по впровадженню)
- ISO/IEC 31010:2019 - Risk Management – Risk Assessment Techniques (Управління ризиками. Методи оцінки ризику)

ISO 31000:2018 є консолідацією основних принципів та рекомендацій щодо проектування, реалізації та підтримки процесів управління ризиками організації (Рис 1.3). Основна його мета - стандартизація та уніфікація основних понять та термінів у цій галузі.

NIST 800-30 (Guide for Conducting Risk Assessments: Керівництво по проведенню оцінок ризику) має за мету надання вказівок для оцінки ризиків інформаційних систем та організацій. Оцінка ризиків є частиною загального процесу управління ризиками та надає керівникам компанії інформацію, необхідну для визначення відповідних напрямків дій у відповідь на виявлені загрози.

ISO/IEC 27001:2013 містить вимоги в області інформаційної безпеки для розробки, впровадження, підтримки, моніторингу та вдосконалення Системи менеджменту інформаційної безпеки (СМІБ).

ISO/IEC 27005:2018 є загальним керівництвом з управління ризиками в сфері інформаційної безпеки. Підтримує загальні концепції, викладені у ISO/IEC 27001:2013, але також сприяє формуванню заходів ІБ на основі ризик-орієнтованого підходу.

ISO/IEC 17799:2005 (BS7799-1) (Information technology - Security techniques - Code of practice for information security management: Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки) був опублікований у 2005-му році Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Сучасний стандарт є допрацьованою версію стандарту 2000-го року, яка була копією Британського стандарту BS 7799-1:1999, який містить практичні поради з управління інформаційної безпеки для розробників, або тих, хто впроваджує або обслуговує системи менеджменту інформаційної безпеки.

FERMA є стандарт з керування ризиками, що був розроблений у кооперації інституту управління ризиками Великобританії (The Institute of Risk Management), Асоціації ризик-менеджменту і страхування (The Association of Insurance and Risk Management) і Національного Форуму управління ризиками в Громадському Секторі (The National Forum for Risk Management in the Public Sector). Був прийнятий у 2002-му році. Даний стандарт визначає основні поняття, формалізує фактори ризику та загальні обов’язки менеджера, відповідального за упрвління ризиками, висвітлює процеси управління ризиками та технологію і методологію їх аналізу.

COSO II вирішує такі завдання, як визначення рівнів ризику відповідно у відповідності зі стратегією розвитку, удосконалення процесів прийняття рішень у рамках реагування на ризики та раціональний розподіл капіталу разом зі скороченням збитків. Був розроблений у 2001-му році в рамках проекту розробки принципів управління ризиками (Enterprise Risk Management Integrated Framework)

компанією «PriceWaterHouseCoopers» у кооперації з комітетом Committee of Sponsoring Organizations of the Treadway Commission.

KING II є збірникиком вже існуючих типових рішень, що застосовуються на практиці у сфері управління ризиками, де детально, але зрозуміло описана ідеологія цього процесу.

BS 7799 являє собою авторитетне першоджерело усіх міжнародних стандартів у сфері управління інформаційною безпекою. Був створений Міністерством торгівлі і промисловості Великобританії та опублікований BSI Group у 1995-му році, складається з декількох частин:

- BS 7799-1:2005. Information security management. Code of practice for information security management (Практичні правила управління інформаційною безпекою) містить у собі кращі практики управління інформаційною безпекою та практичні рекомендації з побудови систем ІБ, а також вимог до оцінювання систем менеджменту СМІБ. Після довгих міжнародних дискусій, у 2000-му році BS 7799-1 був затверджений під назвою ISO/IEC 17799:2000 (BS 7799-1:2000) Information technology - Security techniques - Code of practice for information security management (Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки), а вже після перегляду у 2005-му та 2007-му роках, був затверджений як ISO/IEC 27002;
- BS 7799-2:2005. Information Security Management Systems. Specification with guidance for use (Системи управління інформаційною безпекою. Специфікація з настановами щодо використання) був вперше опублікований BSI у травні 1999-го року і був зосереджений запровадженні системи управління інформаційною безпекою (СМІБ) з орієнтацією на організаційну структуру менеджменту та контролі безпеки. Був прийнятий як ISO/IEC 27001 в листопаді 2005-го року після адаптації;
- BS 7799-3:2006. Information security management systems. Guidelines for information security risk management (Системи управління інформаційною безпекою. Керування ризиками інформаційної безпеки) був опублікований у 2006-му році. Визначає процеси оцінки, аналізу і управління ризиками як частину системи

управління організації. Затверджений у якості міжнародного стандарту під назвою ISO/IEC 27005. Актуальною версією стандарту станом на 2020-й рік є BS 7799-3:2017.

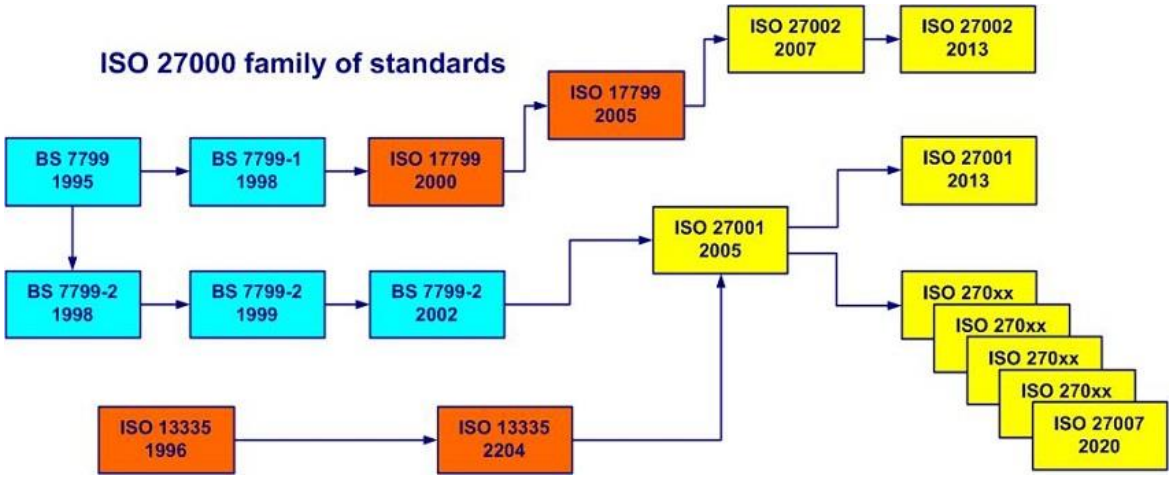

Рисунок 1.5 - Життєвий цикл сімейства стандартів ISO 27000

BSI-Standard 200-3 є німецьким стандартом, який побачив світ у 1998-му році під назвою «BSI-Standard 200-3. Risk analysis based on IT-Grundschutz». Являє собою довідник у форматі HTML, що описує методологію управління ІБ, основні компоненти інформаційних технологій, а також загрози і контрзаходи. Цей стандарт забезпечує просту у освоєнні та та реалізації процедуру, яка дозволяє компаніям цілеспрямовано контролювати свої ризики інформаційної безпеки.

ISO/IEC 15408. Information technology - Security techniques - Evaluation criteria for IT security (Інформаційні технології. Методи захисту. Критерії оцінки безпеки IT) був прийнятий у якості міжнародного у 2005-му році. Містить загальний набір вимог до функцій безпеки інформаційних систем, IT-продуктів та заходів, які застосовуються при виконанні оцінки безпеки.

Стандарт ISO/IEC 15408 складається з трьох частин:

- Part 1: Introduction and general model (15408-1) (Введення і загальна модель)

- Part 2: Security functional requirements (15408-2) (Функціональні вимоги безпеки)
- Part 3: Security assurance requirements (15408-3) (Гарантійні вимоги безпеки)

У стандарті описані функціональні вимоги безпеки та критерії для оцінки механізмів безпеки програмно-технічного рівня. Таким чином, він може бути використаний як інструмент оцінки ризику та ризик-менеджменту для визначення безпеки IT-продукту чи системи під час її проектування, розробки, підтримки та моніторингу.

COBIT представляє собою методологію управління інформаційними технологіями. Був створений Асоціацією контролю і аудиту систем (Information Systems Audit and Control Association - ISACA) у співпраці з Інститутом керівництва IT (IT Governance Institute - ITGI) у 1992-му році. Складається з близько 40 національних та міжнародних стандартів і керівництв у галузі управління IT та аудиту безпеки, які несуть у своїх основі аналіз та вдосконалення провідних практик та існуючих стандартів в області управління IT. COBIT також може бути використаний в якості інструменту управління ризиками, оскільки описує необхідні компоненти для побудови та підтримки ефективної системи управління ризиками та пояснює основні процеси управління ризиками, їх виявлення, аналізу, як реагувати на них та будувати звітність.

SAS 55/78 надає рекомендації для зовнішніх аудиторів щодо впливу запроваджених контролів на планування та виконання аудиту фінансової звітності організації.

SAC пропонує допомогу внутрішнім аудиторам у питаннях контролю та аудиту інформаційних систем та технологій.

Більш детального погляду заслуговують документи ISO/IEC 27001, BS 7799-3:2017 та NIST 800-30, які на сьогоднішній день прийняті світовою спільноною як еталон стандартів якості в даній галузі, через що вважаються рекомендованими і загальноприйнятими на підприємствах незалежно від масштабів та форм власності. Ці настанови є відправною основою при побудові компанією власної системи

управління ризиками, так як у цих стандартах надані відповіді на всі основні питання, що з’являються при формуванні системи управління ризиками, описана стала сучасна термінологія, етапи, та процеси, освітлена методологія управління ризиками, її мету управління та способи досягнення.

Кожна організація, яка обробляє чутливі дані, повинна регулярно проводити оцінку ризиків, відповідно до вимог ISO 27001.

Хоча ці стандарти й консолідують усі необхідні і важливі рекомендації для побудови процесу управління ризиками, все ж, деякі моменти залишаються невизначеними.

1.3. Постановка задачі дослідження

Згідно із сучасними стандартами, система захисту ІС має бути багатокомплексною, здатною оперативно реагувати на кібератаки та несанкціоновані дії (НСД), накопичувати базу знань про методи та прийоми протидії, та виявлення кібератак.

Одним з важливих компонентів розуміння походження кібератаки та здатності запобігти такій атаці у майбутньому є можливість визначити вектор здійсненої атаки. І хоча на сьогоднішній день існує багато інструментів, що допомагають виявляти кібератаки на етапі, коли вони реалізуються, проте, усе ще є актуальним питання виявлення та ідентифікації векторів атаки, яких система зазнає у поточний момент або ж може зазнати у майбутньому.

Хоча саме поняття кібератак є доволі зрозумілим, все ж, визначення кожного окремого вектора відносно до системи, до якої здійснюється кібератака, є нетривіальною задачею.

Таким чином, можна сформувати наступні задачі дослідження:

1. Виконання аналізу ключових метрик ІС.
2. Розробка алгоритму оцінки, що опирається на відомі методи вимірювання метрик ІС.

3. Розробка методу виявлення та ідентифікації векторів атак на основі аналізу ключових метрик ІС.

Розробка методики виявлення та ідентифікації векторів атак на основі аналізу ключових метрик має бути виконана з урахуванням реальних умов функціонування системи, обґрунтуванням вибору методів, що використовуються у ній та підвищенням адекватності експертних оцінок за допомогою підвищеного акценту до інтелектуальної надбудови над традиційними механізмами виявлення векторів атак. Сама методика має бути уніфікована з оглядом на можливість подальшого її використання до систем з різним набором параметрів.

Висновок до першого розділу

У першому розділі було розглянуто тендецію зростання кількості кібератак на приватний та держивний сектори та критичність цього питання з огляду на зростання фінансових та репутаційних втрат як наслідок цих атак.

Було розглянуто існуючи стандарти у сфері управління ризиками та інформаційною безпекою а також приділено окрему увагу кожному з них. Особливу увагу було приділено стандартам серії ISO 27001.

Визначені основні задачі дослідження.

РОЗДІЛ ІІ
ВЕКТОРИ АТАК НА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ. ДАТА МАЙНИНГ У КІБЕРБЕЗПЕЦІ

2.1. Аналіз векторів атак з досвіду сучасних кібератак

Для найбільш актуального погляду на існуючи вектори атак завжди необхідно розглядати актуальні кібератаки.

2.1.1. Існуючі вектори атак

Вектор атаки являє собою шлях або метод, за допомогою яких хакери отримують незаконний доступу до мережі або комп’ютера після спробс експлуатації вразливостей. Зазвичай для запуску атак зловмисниками використовуються численні вектори атак, у ході яких фокус наводиться на слабкі компоненти системи з огляду на їх захищеність, виконують злом даних або крадуть облікові дані для подальшого входу. Ці методи мають за мету поширення шкідливих програм і вірусів у цільовій системі, відправка працівникам організації шкідливих вкладень електронною поштою та веб-посилань, маючи за мету обманути працівника оргіназції або користувача.

Дуже часто вектори атак, спрямовані на безпеку організації, фінансово мотивовані. У цьому випадку зловмисники мають за мету вкрасти гроші або ж інші активи, такі як чутливі дані компанії та персональна інформацію співробітників (PII). Наступним кроком зловмисників у такому випадку буде вимагання викупу за вкрадені дані або активи. Цими хакерами можуть бути як незадоволені колишні працівники, так і групи хакерів (наприклад, Anonymous, Shadow Brokers), або навіть спонсоровані державою групи.

Важливо також не плутати вектори атак (attack vector) з поверхнею атак (attack surface). Кібератаки реалізуються з використанням векторів атаки. Їх реалізація можлива за допомогою зловмисного ПЗ, або ж після успішної фішингової атаки.

Поверхня атаки це загальна площа мережі організації або установи, яку зловмисник може використати як місце для запуску різних векторів кібератак і вилучення даних або отримання доступу до систем організації.

Програмні та апаратні пристрої, а також у більшій частині люди є своєрідними ланками кібератак, тому що переважна більшість вразливостей, таких як слабкі паролі або програмне забезпечення із логічними помилками у коді, можуть бути використані зловмисником.

У загальній картині вектори атак бувають активні та пасивні.

Пасивні вектори атак — це спроби отримати доступ до системи або використати системну інформацію, але не впливають на системні ресурси, такі як typosquating, фішинг та інші атаки на основі безпеки.

Активні вектори атаки — це спроби змінити поведінку системи або порушити її роботу у корисливих цілях, наприклад, за допомогою шкідливого програмного забезпечення, експлуатації невиправлених вразливостей безпеки, підробка електронної пошти, «man-in-the-middle» атаки, викрадення домену та шкідливе ПЗ-вимагач.

Тим не менш, більшість векторів атаки мають певну схожість, тому що зловмисник:

- визначає потенційну мету;
- збирає інформацію про ціль за допомогою соціальної інженерії, шкідливого програмного забезпечення, фішингу, OPSEC та автоматичного сканування уразливостей;
- використовує цю інформацію для визначення потенційних векторів атаки та створенює або експлуатує інструменти для їх використання;
- отримує несанкціонований доступ до системи і викрадає конфіденційні дані або встановлює шкідливий код;
- стежить за комп'ютером або мережею, викрадає інформацію або використовує ресурси комп'ютера.

Вектор атаки, який часто ігнорується — це сторонні постачальники та постачальники послуг. Незалежно від того, наскільки складною є ваша внутрішня

мережева та інформаційна безпека, якщо постачальники мають доступ до конфіденційних даних, вони становлять не менш значний ризик для вашого бізнесу.

Ось чому важливо вимірювати та пом’якшувати ризики, пов’язані з третіми сторонами та сторонніми постачальниками послуг. Це означає, що це має бути частиною політики інформаційної безпеки та програми управління інформаційними ризиками організації.

Варто розглянути найбільш популярні вектори атак більш детально.

Скомпрометовані облікові дані

Імена користувачів і паролі залишаються найпоширенішим типом даних для отримання доступу у систему або до інформації, які регулярно розкриваються в результаті витоку даних, фішингового шахрайства та шкідливого програмного забезпечення. Якщо вони втрачені, вкрадені або незахищені, вони дозволяють хакерам отримати до них вільний доступ. Ось чому компанії зараз інвестують в інструменти для постійного моніторингу втрати даних і вкрадених даних доступу. Менеджери паролів, двофакторна аутентифікація та біометричні методи можуть знизити ризик витоку даних доступу, що призведе до інциденту безпеки.

Слабкі облікові дані

Слабкі паролі та ті паролі, які використовуються повторно, означають, що злом даних у одному місці може призвести до багатьох інших зломів у майбутньому. Для протидії цьому достатньо навчити свою компанію створювати надійний пароль, інвестувати в менеджер паролів або інструмент єдиного входу.

Шкідливі інсайдери

Незадоволені працівники можуть розкрити конфіденційну інформацію або надати інформацію про вразливі місця, характерні для компанії.

Відсутнє або слабке шифрування

Поширені методи шифрування, такі як сертифікати SSL і DNSSEC, можуть запобігти атакам типу «man-in-the-middle» та захистити конфіденційність переданих даних. Відсутність шифрування неактивних даних або недостатнє шифрування може призвести до розкриття конфіденційних даних або інформації для входу в разі порушення чи витоку даних.

Помилки у конфігурації (місконфігурація)

Неправильна конфігурація хмарних служб, таких як Google Cloud Platform, Microsoft Azure або AWS, або використання облікових даних за замовчуванням може призвести до порушення захисту даних і їх подальшого витокуя. Необхідно перевіряти свої налаштування прав доступу S3 та автоматизувати керування конфігурацією, коли це можливо, щоб уникнути відхилень конфігурації.

Фішинг

Фішинг – це метод соціальної інженерії, при виконанні якого зв’язок із потенційною ціллю проводиться завдяки електронній пошті, телефону або текстовим повідомленням персоною, яка видає себе за колегу чи законну установу, щоб обманом змусити жертву надати конфіденційні дані, інформацію для входу або особисту інформацію. Щоб звести до мінімуму фішинг, необхідно розповісти своїм співробітникам про важливість кібербезпеки та запобігти підробці електронної пошти та тайпсквотингу (підробка посилання).

Вразливості

Щодня до CVE додаються нові вразливості, а вразливості нульового дня трапляються так само часто. Якщо розробник не випустив виправлення для вразливості нульового дня до того, як атака може використати його, запобігти її експлуатації може бути дуже важко.

Атака грубої сили (Bruteforce)

Атаки грубої сили покладаються на метод проб і помилок. Зловмисники можуть спробувати отримати доступ до вашого бізнесу безліччю спроб грубого перебору, доки атака не буде успішною. Це можна зробити шляхом атаки на слабкі паролі або шифрування, надсилання фішингових листів або надсилання вкладень електронних листів, заражених якимось типом зловмисного програмного забезпечення.

Розподілена відмова сервісу (DDoS)

DDoS спрямовані проти мережевих ресурсів, таких як центри обробки даних, сервери або веб-сайти, які можуть обмежити доступність комп’ютерної системи. Зловмисник наповнює мережевий ресурс повідомленнями, які сповільнюють його

роботу або навіть дають збій, роблячи його недоступним для користувачів. CDN та проксі є можливими засобами захисту.

SQL ін’єкції

SQL використовується для зв’язку з базами даних. Багато серверів, які зберігають конфіденційні дані, використовують SQL для керування даними у своїй базі даних. Ін’єкція SQL використовує шкідливий SQL-запит, щоб обманом змусити сервер розкрити інформацію, яку він інакше не розкрив би. Це є серйозним кіберризиком, якщо база даних зберігає інформацію про клієнтів, номери кредитних карток, інформацію для входу або інші особисті дані.

Трояни

Трояни – це шкідливі програми, які вводять користувача в оману, видаючи себе за легітимну програму. Вони часто поширюються через заражені вкладення електронної пошти або підроблене програмне забезпечення.

Міжсайтові скрипти (XSS)

Атаки типу XSS полягають у введенні шкідливого коду на веб-сайт, ціллю атаки є не сам сайт, а відвідувачі сайту. Поширеним методом для хакерів для виконання міжсайтових скриптових атак є вставка шкідливого коду в коментар, наприклад, вбудовування посилання на шкідливий JavaScript в області коментарів публікації в блозі.

Викрадення сессії

Коли ви входите в службу, служба зазвичай доставляє ключ сеансу або файл cookie на ваш комп’ютер, тому вам не потрібно входити знову. Цей файл cookie може бути використаний хакером для отримання доступу до конфіденційної або іншої чутливоїінформації.

“Man-in-the-middle” атаки

Публічні мережі Wi-Fi можна використовувати для здійснення атак «man-in-the-middle» та перехоплення трафіку, призначеного для інших цілей, наприклад, під час підключення до захищеної системи.

Сторонні вендори

Зростання аутсорсингу означає, що сторонні постачальники становлять серйозний ризик для кібербезпеки даних клієнтів і власних даних організації. Деякі з найбільших порушень даних були спричинені третіми сторонами.

2.1.2. Соціальні інженерія як окремий вектор атак

Соціальна інженерія один із найпоширеніших видів атак на сьогоднішній день. Цей термін використовується для визначення широкого спектру шкідливих дій, що здійснюються зловмисниками через взаємодію з людьми, працівниками або користувачами. Соціальна інженерія має ха мету психологічні маніпуляції, щоб змусити користувачів зробити помилки безпеки або розкрити конфіденційну інформацію.

Атаки соціальної інженерії відбуваються в один або кілька етапів. Зловмисник спочатку оглядає передбачувану жертву, щоб зібрати необхідну довідкову інформацію, а саме, потенційні точки входу та слабкі протоколи безпеки, необхідні для здійснення атаки. Потім зловмисник намагається завоювати довіру жертви та стимулювати наступні дії, які порушують методи безпеки, а саме, розкриття конфіденційної інформації або надання доступу до важливих ресурсів.

Соціальна інженерія складається з наступних етапів (Рисунок 2.1):

1. Дослідження. Підготовка до атаки
    a. визначення жертв;
    b. збір інформації;
    c. вибір методу атаки;
2. Обман жертви для отримання зачіпки у системі
    a. залучення цілі;
    b. зав’язка «легенди»;
    c. взяття контролю над взаємодією;
3. Гра. Отримання інформації впродовж певного проміжку часу
    a. розширення бази знань;
    b. реалізація атаки;

c. Порушення порядку роботи організації та/або викрадення даних

4. Вихід. Припинення взаємодії, в ідеалі без виклику підозри

a. прибирання слідів шкідливого ПЗ;

b. прибирання слідів активності зловмисника;

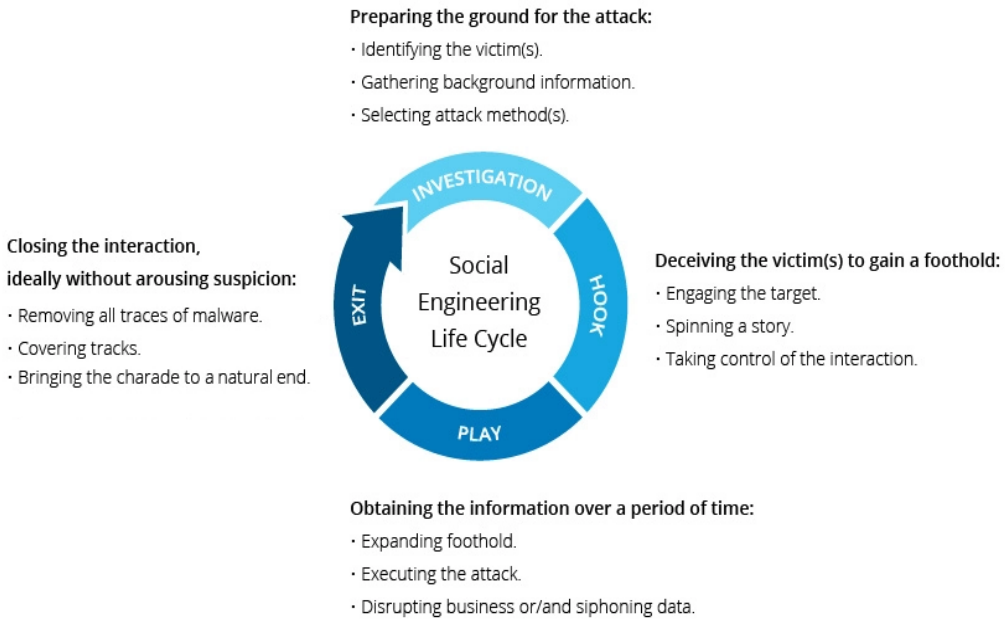

Рисунок 2.1 - Життєвий цикл кібератаки на базі соціальної інженерії за версією Imperva

Атаки соціальної інженерії мають багато різних форм і можуть здійснюватися скрізь, присутній людський фактор. Вони мають п’ять найпоширеніших форм цифрових атак соціальної інженерії.

Baiting

Як випливає з назви, атаки-приманки використовують фальшиву обіцянку, щоб викликати жадібність або цікавість жертви. Вони заманюють користувачів у пастку, яка краде їх особисту інформацію або заражає їх системи шкідливим програмним забезпеченням.

Найбільш зневажена форма приманки використовує фізичні носії для поширення шкідливих програм. Зловмисники розміщують приманку – як правило, заражені шкідливим програмним забезпеченням флеш-накопичувачі – на помітних місцях, де їх обов’язково побачать потенційні жертви (наприклад, туалети, ліфти

або стоянка цільової компанії). Приманка виглядає автентично, наприклад, з ярликом фонду оплати праці підприємства.

Жертви з цікавості підхоплюють приманку і вставляють її в робочий або домашній комп'ютер, що призводить до автоматичної установки шкідливого ПЗ в систему.

Шахрайство з приманками не обов'язково має відбуватися в реальному світі. Онлайн-форми приманки складаються із привабливої реклами, яка спрямовує на шкідливі веб-сайти або заохочує користувачів завантажувати програму, заражену шкідливим програмним забезпеченням.

Scareware

Scareware атакує жертв помилковими тривогами та вигаданими погрозами. Користувачів змушують повірити, що їхня система заражена зловмисним програмним забезпеченням, що змушує їх встановлювати програмне забезпечення, яке не має реального використання (за винятком зловмисника) або саме є шкідливим програмним забезпеченням. Scareware також відомий як обманне ПЗ (deception), ПЗ шахрайського сканера та шахрайське програмне забезпечення (fraudware).

Поширеним прикладом загрозливого програмного забезпечення є спливаючі банери законного вигляду, які з'являються у вашому веб-переглядачі під час серфінгу в Інтернеті з текстом на кшталт «Ваш комп'ютер може бути заражений шкідливими шпигунськими програмами». Він або пропонує встановити для вас інструмент (часто заражений шкідливим програмним забезпеченням), або перенаправляє вас на шкідливий веб-сайт, де він заражає ваш комп'ютер. Scareware також поширюється через спам-повідомлення, які видають фальшиві сповіщення або пропонують користувачам придбати послуги, що не мають користі або принесуть шкоду.

Pretexting

У цьому випадку зловмисник отримує інформацію за допомогою цілого ланцюжку вміло організованої брехні. Шахрайство часто ініціює зловмисник, який стверджує, що йому потрібна конфіденційна інформація від жертви для виконання важливого завдання.

Зловмисник зазвичай починає зі створення довіри від жертви до себе, видаючи себе за колегу, працівника поліції, банківського чи податкового чиновника або іншу особу, яка має право знати інформацію. Зловмисник задає питання, нібито необхідні для підтвердження особи жертви, і таким чином збирає важливі персональні дані.

Таким способом зловмисник збирає усю необхідну інформацію та документи, таку як номери соціального страхування, домашні адреси та номери телефонів, телефонні дані, дати відпустки співробітників, банківські реквізити та навіть інформацію про безпеку установки.

Phishing

Фішинг, як один із найпопулярніших видів атак соціальної інженерії, складається з поєднання атак на електронну пошту та смс-повідомлення, що спрямовані на те, щоб викликати у жертв відчуття невідкладності, цікавості чи страху. Люди, боячись розкриття конфіденційної інформації, натискають посилання на шкідливі сайти або відкривають вкладення, що містять шкідливе програмне забезпечення.

Прикладом може служити електронний лист, надісланий користувачам онлайн-сервісу з повідомленням про порушення політики, що вимагає негайних дій, наприклад зміна пароля. Електронний лист містить посилання на незаконний веб-сайт, який виглядає майже так само, як і легітимна версія, і просить нічого не підозрючого користувача ввести свої поточні дані для входу та новий пароль. Після надсилання форми інформація надсилається зловмиснику.

Оскільки фішингові кампанії надсилають однакові або майже ідентичні повідомлення всім користувачам, поштовим серверам із доступом до платформ обміну загрозами набагато легше виявляти та блокувати їх.

Spear Phishing

Представляє собою більш цілеспрямовану версію фішингової атаки, коли зловмисник вибирає конкретних людей або компанії. Потім вони адаптують свої повідомлення до характеристик, професійних позицій та контактів своїх жертв, щоб надати їх атаці менш підозрілого вигляду. Спір-фішинг вимагає від зловмисника набагато більше зусиль, і для його успіху можуть знадобитися тижні або навіть

місяці. Його набагато важче виявити, і він має кращі показники успіху при вмілому виконанні.

У ході сценарію спір-фішингу зловмисник, наприклад, видає себе за IT-консультанта компанії та надсилає електронний лист одному або кільком співробітникам. Він сформульований і підписаний так само, як і консультант, і змушує одержувачів вважати, що це автентичне повідомлення. У повідомлення описане прохання до одержувачів змінити свій пароль за посиланням, яке перенаправляє їх на шкідливий сайт, де зловмисник тепер перехоплює їхні дані для входу.

Вразливості нульового дня (Zero-day)

Це діра в безпеці, про яку ніхто не знає, поки її не використають (звідси назва нульового дня, оскільки між атакою і випуском немає часу). Порушення безпеки). Якщо розробник не випустив виправлення для вразливості нульового дня до того, як зловмисник використає цю вразливість, наступна атака називається атакою нульового дня. Створення POC-експлойтів Червоною командою є способом знешкодити вразливості нульового дня.

2.2. Приклади сучасних кібератак

У зв’язку з розвитком інформаційних технологій, весь бізнес, у тій чи іншій мірі, починає використовувати інформаційні технології, аби підвищувати темпи зростання та мати змогу конкурувати на ринку. Слідом за цифровізацією підприємств з’являється і ризик стати жертвою кібератаки, що може призвести до значних втрат або навіть до закриття організації.

Однією з найвизначніших атак за останні роки була атака з використанням шкідливого ПЗ Petya. Перша згадка про це ПЗ з’явилася у 2016-му році. Основна ціль Petya – ураження головного завантажувального запису (MBR) систем на базі Microsoft Windows. Після ураження MBR шкідливим кодом відбувалося шифрування файлової системи таблиці завантаження ОС, внаслідок чого користувач ніяк не міг завантажити системи, а замість цього бачив на головному екрані

повідомлення, у якому йшлося про грошовий викуп на рахунок Bitcoin для повернення доступу до системи (Рисунок 2.2).

У березні 2016-го року Petya був частково розповсюджений через заражені вкладення у електронних листах. У червні 2017-го року новий варіант вірусу Petya був застосований при глобальній кібератаці, переважно на українські організації. Цього разу новий варіант вірусу був розповсюджений завдяки вразливості EternalBlue, яка була задіяна лише місяцем раніше у атаці під назвою WannaCry. Одна з лабораторій дослідження кіберзагроз найменувала цей вірус як NotPetya через його відмінності у механізмі розповсюдження, на відміну від версії 2016-го року.

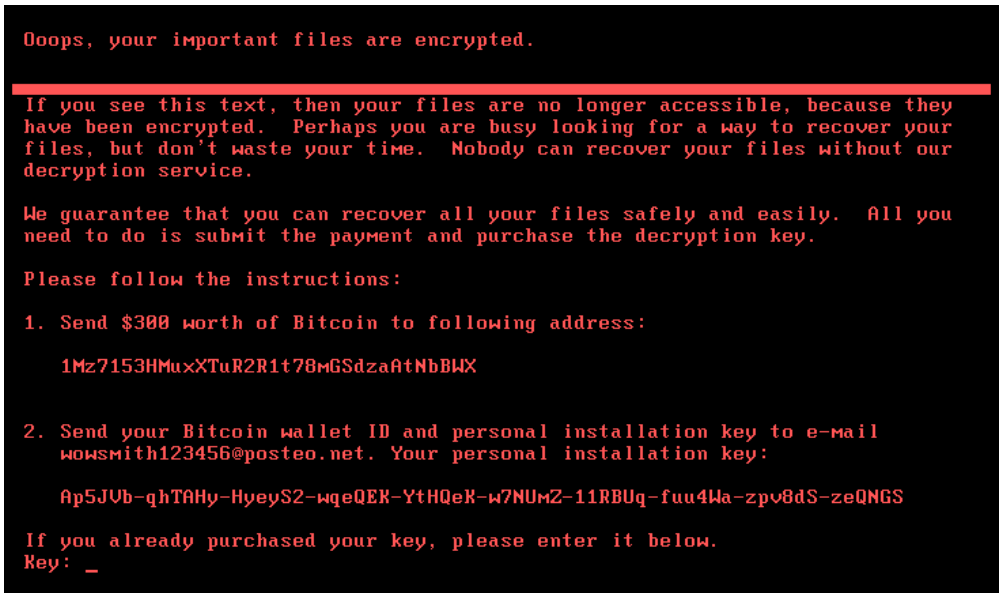

Рисунок 2.2 - Повідомлення про необхідність внести плату для повернення доступу на екрані користувачів систем, що були заражені Petya

WannaCry являє собою іншу кібератаку, що відбулася у травні 2017-го року. За кінцевим результатом була схожою з Petya – вірус шифрував дані користувачів, котрим пропонувалося відправити грошовий переказ на Bitcoin-гаманець для розшифрування даних (Рисунок 2.3). Також WannaCry мав здатність самопоширюватися. Вірус сам сканував системи на наявність вразливостей, після чого проникав до них, реалізуючи експлойт EternalBlue, а потім за допомогою інструмента DoublePulsar встановлював та запускав копію самого себе.

Цікавим є той факт, що вразливість EternalBlue скоріш за все була розроблена Агенством Національної Безпеки США (NSA) і пізніше вкрадена організацією The

Shadow Broker. EternalBlue представляє собою експлойт вразливості у реалізації SMB від Microsoft, який дозволяє дистанційно виконати програмний код, у тому числі шкідливий.

Рисунок 2.3 - Повідомлення про необхідність внести плату для повернення доступу на екрані користувачів систем, що були заражені WannaCry

DoublePulsar – бекдор, також розроблений групою The Shadow Broker, який був використаний у процесі росповсюдження WannaCry по цільовим системам.

Ці дві кібератаки принесли компаніям величезних збитків не лише в Україні (хоча 80% систем, що були вражені вірусом Petya та NonPetya, були розташовані саме в Україні), а й по всьому світу приблизно у 14 мільярдів доларів США.

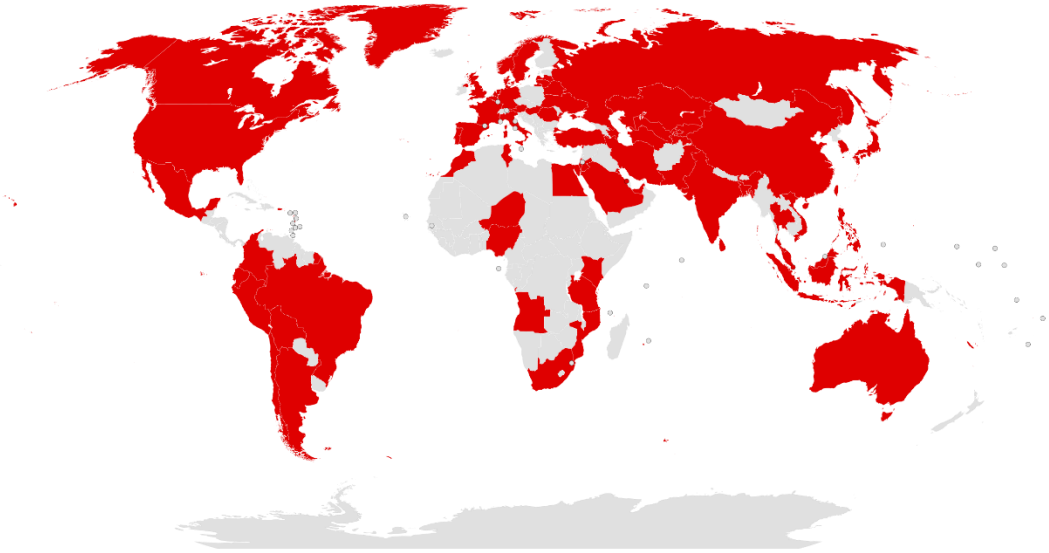

Рисунок 2.4 - Червоним позначені країни, у яких системи зазнали атаки WannaCry

Все це відбулося не дивлячись на те, що багато розробників захисного ПЗ та Microsoft попереджали власників про вразливість EternalBlue і оновлення з виправленням було випущено також до експлуатації вразливостей.

В цілому процес дослідження наявних та пошуку нових вразливостей займає багато часу і є безперервним. Одним з інструментів у цьому процесі є дата майнинг.

2.3. Дата майнинг у кібербезпеці

Інтелектуальний аналіз даних (або ж дата майнинг) — це аналіз інформації, виявлення нових закономірностей і даних, а також передбачення майбутніх тенденцій. Він часто використовується в наукових дослідженнях, розвитку бізнесу, відносинах з клієнтами та багатьох інших сферах.

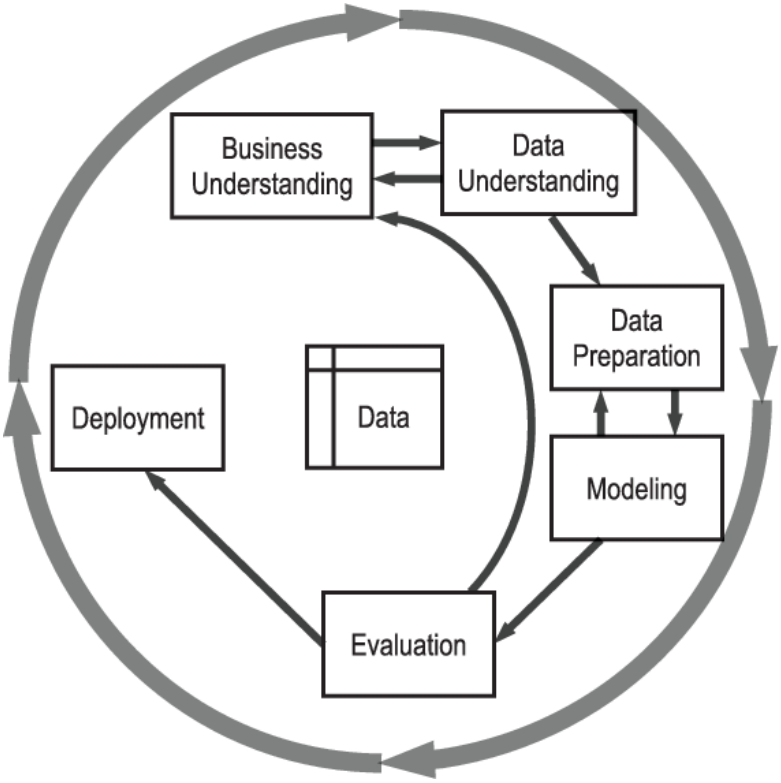

Рисунок 2.5 - Схема процесу дата майнингу

Термін «інтелектуальний аналіз даних», який іноді називають «відкриттям знань у базах даних», був придуманий лише в 1990-х роках. Однак його основа базується на трьох взаємопов'язаних наукових дисциплінах: статистиці (чисельне дослідження між даними), штучному інтелекті (інтелект, подібний до людини, представлений програмним забезпеченням та/або машинами) та машинне навчання (алгоритми, здатні навчатися та робити прогнози на основі даних). Те, що було старим, знову стає новим, оскільки технологія інтелекту даних постійно розвивається, щоб не відставати від безмежного потенціалу великих даних і доступної обчислювальної потужності.

Протягом останнього десятиліття досягнення в потужності та швидкості обробки дозволили нам перейти від ручних, виснажливих і трудомістких методів до швидкого, простого й автоматизованого аналізу даних. Чим складніші зібрані набори даних, тим більший потенціал для отримання відповідної інформації. Серед іншого, роздрібні торговці, банки, виробники, оператори зв'язку та страхові компанії використовують аналіз даних для виявлення взаємозв'язків – від оптимізації цін до рекламних акцій і демографії, до того, як економіка, ризики,

конкуренція та соціальні медіа впливають на їхні бізнес-моделі, дохід, операції та відносини з клієнтами.

Дата майнинг представлений у кількох різних моделях, кожна з яких має власні техніки, що мають свої переваги та недоліки в залежності від області їх застосування.

Описове моделювання: виявляє подібність або кластери в історичних даних, щоб визначити причини успіху або невдачі, наприклад, категоризувати клієнтів за перевагами продукту або настроєм. Приклади техніки включають:

- кластеризація: групування подібних записів;
- виявлення аномалій: ідентифікація багатовимірних викидів;
- вивчення правил асоціації: розпізнавання зв'язків між записами;
- аналіз принципових компонентів: розпізнавання зв’язків між змінними;
- формування групи спорідненості: групування людей зі спільними інтересами або схожими цілями (наприклад, люди, які купують X, часто купують Y і, можливо, Z).

Прогнозне моделювання: це моделювання проводиться глибше, щоб класифікувати майбутні події або оцінити невідомі результати – наприклад, використовуючи кредитний скоринг, щоб визначити ймовірність того, що хтось поверне кредит. Прогнозне моделювання також дає уявлення про відтік клієнтів, реакцію кампанії чи втрати кредиту. Приклади технік:

- регресія: міра міцності зв’язку між залежною змінною та набором незалежних змінних;
- нейронні мережі: комп’ютерні програми, які розпізнають закономірності, роблять прогнози та навчаються;
- дерева рішень: деревовидні діаграми, на яких кожна гілка представляє ймовірне явище;
- опорні векторні машини: моделі навчання під керівництвом із відповідними алгоритмами навчання.

Рекомендаційне моделювання: із збільшенням кількості неструктурованих даних з Інтернету, полів коментарів, книг, електронних листів, PDF-файлів,

аудіофайлів та інших текстових джерел використання інтелектуального аналізу тексту як пов’язаної дисципліни з аналізом даних надзвичайно зросло. Потрібно вміти успішно аналізувати, фільтрувати та трансформувати неструктуровані дані, щоб включити їх у прогнозні моделі і таким чином підвищити точність прогнозів.

Незалежно від обраної моделі, процес дата майнингу можна розділити на чотири етапи:

1. Збір даних. Відповідні дані для аналітичного додатка ідентифікуються та звіряються. Дані можуть перебувати в різних вихідних системах, у сховищі даних або в області даних (data lake), дедалі більш поширеному сховищі в середовищах великих даних, яке містить поєднання структурованих і неструктурованих даних. Також можливе використання зовнішніх джерел даних. Незалежно від того, звідки надходять дані, спеціаліст з даних часто переміщує їх в озеро даних для наступних кроків процесу.

2. Підготовка даних. Цей етап включає серію кроків для підготовки даних до «майнингу». Він починається з аналізу даних, профілювання та попередньої обробки, а потім очищення даних для виправлення помилок та інших проблем із якістю даних. Дані також трансформуються, щоб зробити набори даних узгодженими, якщо спеціаліст із даних не хоче проаналізувати необроблені, нефільтровані дані для певної програми.

3. Здобування «майнинг» даних. Після того, як дані були підготовлені, спеціаліст з даних вибирає відповідну техніку аналізу даних, а потім реалізує один або кілька алгоритмів для виконання «майнингу». У програмах машинного навчання алгоритми зазвичай потрібно навчати на прикладах наборів даних, щоб знайти інформацію, яку вони шукають, перш ніж застосовувати до повного набору даних.

4. Аналіз та оцінка даних. Результати аналізу даних використовуються для створення моделей аналізу, які можуть допомогти у прийнятті рішень та інших бізнес-метрик. Дослідник даних або інший член команди з науки про дані також повинні повідомити про результати керівникам і користувачам, часто за допомогою візуалізації даних і використання методів розповіді даних.

Завдяки своїм перевагам дата майнинг є дуже дієвим інструментом у рамках процесу управління ризиками.

Висновок до другого розділу

У другому розділі було розглянуто існуючі на сьогоднішній день вектори атак з огляду на сучасні тенденції.

Також було приділено увагу сучасним резонансним кібератакам, що нанесли компаніям по всьому світу багато збитків.

Було розглянуто поняття дата майнингу та існуючі моделі реалізації цього процесу.

РОЗДІЛ ІІІ
РОЗРОБКА МЕТОДОЛОГІЇ ВИЗНАЧЕННЯ ТА ІДЕНТИФІКАЦІЇ ВЕКТОРУ АТАК НА ОСНОВІ КЛЮЧОВИХ МЕТРИК ІС НА ОСНОВІ ДАТА МАЙНИНГУ

3.1 Дата майнинг у кібербезпеці

Виявлення шкідливих програм

При розробці захисного програмного забезпечення розробники використовують методи аналізу даних, щоб підвищити швидкість і якість виявлення шкідливих програм і виявити атаки нульового дня. Існує три основні стратегії знаходження шкідливого ПЗ:

- виявлення аномалій;
- виявлення некоректного спрацювання;
- гібридне виявлення.

Виявлення аномалій включає моделювання нормальної поведінки системи або мережі для виявлення відхилень від нормальних моделей діяльності. Методи, засновані на аномалії, можуть навіть виявляти раніше невідомі атаки та використовуватися для встановлення сигнатур детектора зловживань.

Однак виявлення аномалії також може позначати законну діяльність, якщо вона відхиляється від норми, що призводить до помилкових сповіщень.

Виявлення зловживань, також відоме як виявлення на основі сигнатур, визначає лише відомі атаки за допомогою прикладів їхніх сигнатур. Цей метод має нижчу частоту помилкових тривог, але не може виявити атаки нульового дня.

Гібридний підхід поєднує методи виявлення аномалій і зловживань, щоб збільшити кількість виявлених атак при зменшенні кількості помилкових спрацьовувань. Гібридні алгоритми виявлення не створюють власних шаблонів. Замість цього вони використовують інформацію як із шкідливих програм, так і з легальних програм, щоб створити класифікатор, який представляє собою набір

правил або шаблон виявлення, згенерований алгоритмом майнінгу. Потім частина системи, яка займається виявленням аномалій, шукає відхилення від нормального шаблону, а частина системи, яка займається виявленням зловживань, шукає сигнатури зловмисного програмного забезпечення в коді.

Яку б стратегію ви не вибрали, розробка системи виявлення зловмисного програмного забезпечення включає два кроки:

- виокремлення переваг шкідливого ПЗ;
- класифікація і кластеризація;

Спочатку алгоритм аналізу даних витягує характеристики шкідливого програмного забезпечення із записів запитів API, n-грам, двійкових рядків, поведінки програми та інших подій. Ви можете застосувати статичне, динамічне або гібридне сканування, щоб отримати характеристики шкідливого програмного забезпечення з потенційно небезпечних файлів.

Під час етапу класифікації та групування ви можете використовувати відповідні методи для поділу файлів зразків на групи на основі аналізу ознак. На цьому етапі вам потрібно створити класифікатор за допомогою таких алгоритмів класифікації, як RIPPER, Дерево рішень, штучна нейронна мережа, наївний байєс або машини опорних векторів.

Використовуючи методи машинного навчання, кожен алгоритм класифікації створює модель, яка представляє як доброякісні, так і шкідливі класи. Навчаючи класифікатор із такої колекції зразків файлів, можна навіть виявити нещодавно випущене шкідливе програмне забезпечення.

Виявлення вторгнення

Зловмисники можуть здійснювати шкідливі втручання через мережі компанії, бази даних, сервери, веб-клієнти та операційні системи. Використовуючи методи аналізу даних, ви можете аналізувати результати аудиту та виявляти аномальні закономірності. Ви можете виявити вторгнення, сканування мережі та системи, атаки відмови в обслуговуванні та атаки проникнення.

Методи аналізу даних особливо ефективні для виявлення таких типів вторгнень:

- атаки на базі хоста: зловмисник фокусується на конкретній машині або ж на групі машин;
- атаки на базі мережі: зловмисник атакує всю мережу (наприклад, щоб викликати перевантаження буферу)

Щоб виявити атаки на основі хостів, захисне програмне забезпечення має проаналізувати функції, отримані з програм. Виявлення мережевих атак вимагає такого рішення для аналізу мережевого трафіку. Як і в разі виявлення шкідливого програмного забезпечення, ціллю пошуку може бути ненормальна поведінка, або випадки зловживання.

Системи виявлення атак, як правило, засновані на методах класифікації, групування та правил асоціації. Ці методи дозволяють витягувати характеристики атак з бази даних, систематизувати їх і позначати всі нові записи однаковими характеристиками. Деякі з алгоритмів, які ви можете використовувати тут, — це дерева регресії та рішень, байєсівські мережі, K-найближчі сусіди, навчальні автомати та ієрархічна кластеризація.

Ви також можете додати функції прогнозування до системи виявлення зловмисників. Для обчислення ймовірності майбутнього вторгнення можна використовувати такі методи, як класифікація та аналіз часових рядів. Використання алгоритмів штучного інтелекту полегшує виявлення раніше невідомих прихованих або підозрілих дій.

Виявлення шахрайства

Виявлення шахрайства є проблемою, оскільки шахрайська діяльність зазвичай добре прихована, а кіберзлочинці постійно винаходять нові моделі шахрайства.

Методи аналізу даних, які використовують машинне навчання, можуть виявити багато видів шахрайства, від фінансового шахрайства до телекомунікаційного шахрайства та комп’ютерного вторгнення. Машинне навчання особливо корисне для виявлення шахрайства, оскільки допомагає:

- масштабувати, щоб врахувати зміни кількості та складності ваших баз даних;
- навчитися визначати та прогнозувати нові види шахрайства;

- точно розрахувувати ймовірності шахрайських дій.

Можна використовувати контрольовані та неконтрольовані алгоритми машинного навчання для виявлення шахрайства.

У контрольованому машинному навчанні усі доступні набори даних класифікуються як шахрайські або не шахрайські. Ця класифікація потім використовується для навчання моделі для виявлення можливого шахрайства. Основним недоліком цього методу є його нездатність виявляти нові види атак.

Методи навчання без контролю вивчають моделі шахрайства з немаркованих наборів даних. Вони створюють власну класифікацію та описи ознак шахрайської діяльності. Навчання без контролю допомагає виявити проблеми конфіденційності та безпеки даних без проведення статистичного аналізу. Він також здатний аналізувати та виявляти нові види шахрайства.

Збір інформації про загрози

Докази загроз кібербезпеці зазвичай розкидані по всій мережі компанії. Ці набори даних можна використовувати для створення навчальних наборів даних, створення моделей дослідження та підвищення точності прогнозів. Однак проблема полягає в тому, щоб знайти відповідні дані в терабайтах наборів даних.

Алгоритми аналізу даних допомагають виявити ці приховані дані та перетворити їх у структуровану базу даних загроз. Вони можуть використовувати кластеризацію, правила асоціації та методи узагальнення, щоб виявити такий тип інформації:

- тактична: маркери компрометації, незвичайний трафік, поведінкові зміни та невдалі спроби логіну користувачів;
- операційна: характеристика поведінки атакуючого зловмисника, час атаки, її ціль та природа;
- стратегічна: тренди кібербезпеки, зміни у середовищі загроз.

Інтелектуальний аналіз даних часто використовується лише для перших кроків аналізу загроз: виявлення та структурування даних. Потім експерт з кібербезпеки повинен вручну переглянути виявлені дані та вирішити, як з ними

поводитися. Однак вони також можуть використовувати методи аналізу даних для створення системи на основі машинного навчання для збору та обробки даних.

Тобто, у кібербезпеці дата майнинг посідає важливу роль і звичайно, має за мету зібрати якнайбільше даних, щоб кінцевий результат аналізу був найбільш точним. З огляду на короткі інтервали часу між появою загроз та їх реалізацію, дуже важливим є поняття ситуаційної обізнаності.

Ситуаційна обізнаність у кібербезпеці означає розуміння середовища кіберзагроз, в якому працюють організації, пов'язаних з ними ризиків і впливів, а також адекватності заходів щодо зменшення ризику. Повне знання середовища загроз може допомогти краще зрозуміти вразливі місця, щоб на ранній стадії вжити відповідних заходів щодо зменшення ризику.

Ситуаційна обізнаність є процесом, що складається з наступних повторюваних етапів (Рисунок 3.1):

1. Створення плану ситуаційної обізнаності.
2. Збір і аналіз даних щодо ситуаційної обізнаності.
3. Обробка і обмін інформацією, що необхідна для прийняття вірного рішення.
4. Покращити процес та технології ситуаційної обізнаності на основі отриманих даних.

Рисунок 3.1 - Етапи ситуаційної обізнаності

Підвищеня ефективності цього процесу досягається комбінуванням засобів та інструментів кібербезпеки. Сприйняття загального поля загроз передбачає збір доказів ситуацій в інформаційній інфраструктурі. Сприйняття полягає в отриманні знань про елементи мережевого середовища, наприклад, тривоги системи виявлення вторгнень (IDS), журнали брандмауера, звіти аналізу, а також час, коли вони були відбулися.

Розуміння передбачає аналіз доказів, щоб визначити точний рівень загрози, тип атаки напад і пов'язані або взаємозалежні ризики. Це вимагає ряду відповідних методів а також процедур аналізу, узагальнення, співвіднесення та агрегування доказів, зібраних в інформаційній інфраструктурі.

Ситуаційна обізнаність включає сприйняття атак і сліди атак, розуміння моделей атак кореляції, а також прогноз того, що відбудеться найближчим часом з точки зору рівень впливу та загрози на інформаційну інфраструктуру.

Ситуаційна обізнаність – це процес перетворення даних, уточнення й оцінки доказів, який по суті відповідає життєвому циклу, якому повинні слідувати дані з кібербезпеки. Протягом цього життєвого циклу дані набувають різних форм, починаючи з вихідних даних датчиків через очищені, об’єднані, корельовані дані, сприйняті події та контексти. На виході, життєвий цикл даних безпеки в основному стосується попередньої обробки даних, розподілених сховищ даних і злиття даних, тоді як нижня частина життєвого циклу даних безпеки в основному стосується обробки подій, оцінки та моделювання ситуації, послідовного розпізнавання та аналізу образів, контексту висновки та управління, а також візуалізації ситуації.

Взаємодія цієї схеми (Рисунок 3.2) є інтегрованим процесом від збору даних безпеки до створення моделі ситуації кібербезпеки. Потік інформації від датчиків безпеки до ситуаційних моделей формує інформаційний ланцюжо, тобто багаторівневу структуру аналізу, яка у кінцевому результаті надасть ситуаційну обізнаність.

Протягом життєвого циклу даних безпеки існують етапи, на яких дані збираються, агрегуються, обробляються, співвідносяться та вилучаються для отримання значень вищого рівня. На кожній фазі системи, методи та інструменти

пов’язані з ключовими необхідними функціями. Крім того, ситуаційна обізнаність за своєю природою розроблена як інфраструктура розподіленої обробки даних.

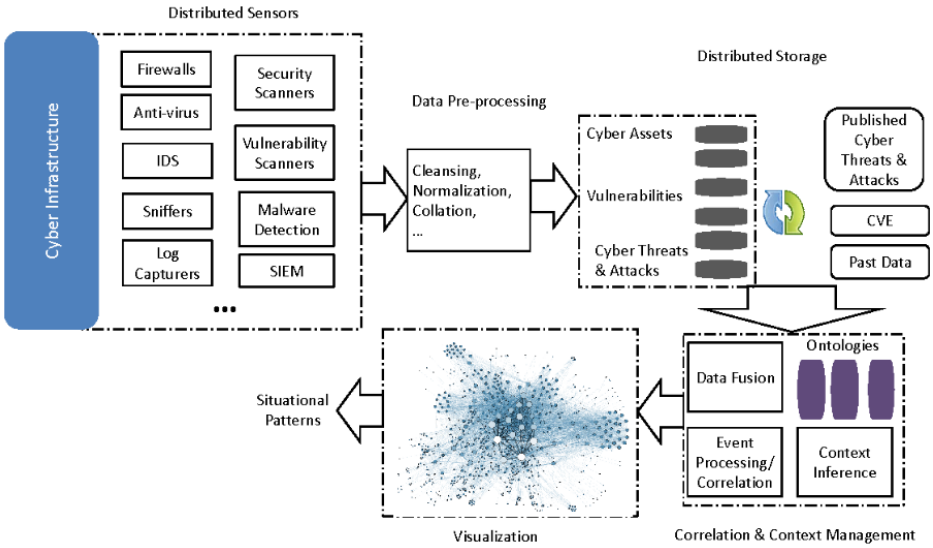

Рисунок 3.2 - Схема взаємодії компонентів системи захисту в рамках процесу ситуаційної обізнаності у кібербезпеці

Ситуаційна обізнаність починається з перевірки безпеки. Моніторинг безпеки полягає у фіксації загального явища комп’ютерної системи або мережі, в якій дані постійно змінюються. Використовуючи інструменти центру безпеки, ситуаційна обізнаність може збирати мережеві, системні журнали та журнали програм, а також сповіщення датчиків у реальному часі по всій інформаційній інфраструктурі. Збір, зберігання та обробка даних

Збір, зберігання та обробка даних повинні мати розподілену структуру, тобто кожен тип даних повинен проходити обробку відповідно до даних, зібраних контрольованою інформаційною інфраструктурою, що важливо для подальшої потенційної масштабованості системи.

Усі зібрані дані очищаються, нормалізуються та зберігаються в розподіленій структурі, яку вже можна використовувати для підтримки управління інформацією та візуалізації моделі безпеки. Очищення даних може включати усунення дублікатів, калібрування даних і фільтрацію необроблених даних із датчиків безпеки, таких як

IDS, брандмауери, мережеві та системні журнали, захист інформації та керування подіями (SIEM) і NetFlow тощо.

Управління кореляцією та контекстом включає злиття даних, обробку подій і кореляцію. Злиття даних — це техніка, яка використовується для об'єднання даних з різних джерел і створення практично різних структур даних у цілісному сенсі. Об'єднання даних – це техніка, яка використовується для об'єднання наборів доказів про передбачувану ситуацію. Теорія самоочевидності Демпстера-Шейфера — це звичайна методика злиття даних, яка полягає в синтезі достовірності кожного блоку даних з різних джерел, щоб ефективно зменшити кількість помилкових спрацьовувань і помилкових негативів у попередженнях безпеки. Крім того, комплексна обробка подій, яка виявляє та корелює події, може використовуватися для вилучення значень вищого рівня з даних.

Зрештою, візуалізація безпеки — це перетворення організованих даних та інформації у значущі шаблони або послідовності, які можна переглядати. Це частина рівня розуміння ситуативної обізнаності. Оскільки всі дані та події утворюють цілісну загальну картину, користувачів можна підказувати, поглиблювати й інформувати за допомогою спільної операційної картини, яка підкріплена ситуаційною обізнаністю. Він складається з уразливостей, активів, ризиків та інформації про безпосередній стан. Така консолідована картина кібербезпеки дозволяє особам, які приймають рішення, виконувати комплексний аналіз ризиків і планувати дії щодо виправлення ситуації.

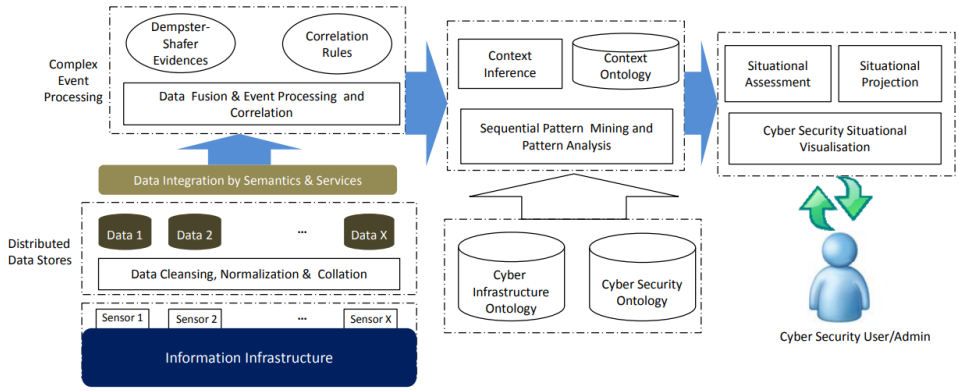

Рисунок 3.3 - Багаторівнева структура аналізу ситуаційної обізнаності у кібербезпеці

Ситуаційна обізнаність у кібербезпеці — це, по суті, система кіберзахисту, що модулюється та будується на основі отриманих даних. Ситуаційна обізнаність організації відображає її ефективність реагування на атаки, оскільки її кінцевою метою є виявлення та ідентифікація передових кібератак.

З огляду на основний принцип ситуаційної обізнаності, важливим і корисним доповненням до зібраних даних у створенні моделі була б інформація про природу вектору кібератаки.

3.2 Дата майнинг як інструмент визначення векторів атак

Виявлення кібератак на основі аналізу даних включає п’ять загальних етапів (Рисунок 3.4), а саме:

- моніторинг системи та збір даних за допомогою різних датчиків та систем попередження, ведення журналів мережі/системи/процесу, а також демонів/агентів сніфферів;
- попередня обробка даних (очищення, фільтрація, нормалізація тощо) у локальних сховищах даних;
- кореляція подій та виділення функцій (наприклад, за допомогою обробки даних Hadoop Distributed File System (HDFS) та MapReduce);
- аналіз даних (зменшення розмірності, класифікація, кластеризація) для виявлення зловживань або аномалій;
- візуалізація та інтерпретація результатів видобутку.

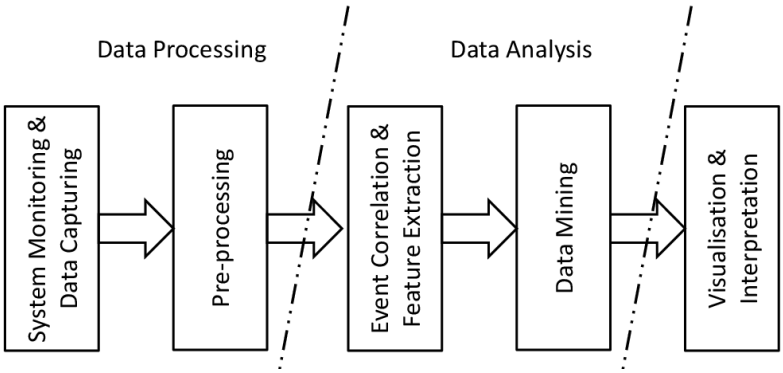

Рисунок 3.4 - Етапи виявлення кібератак на основі аналізу даних

Виявлення на основі аналізу даних, якщо його правильно налаштувати, може стати центральною нервовою системою мережі. Виявлення на основі аналізу даних може запропонувати деякі корисні похідні функції, наприклад, моніторинг у режимі реального часу та керування інцидентами для подій, пов'язаних із безпекою, зібраних з мережі, пристроями безпеки, системами та додатками. Це забезпечує робочий процес, який допомагає відстежувати та ескалувати інцидент. Його також можна використовувати для керування та консолідації журналів, а також для створення звітів про відповідність вимогам. Іншими словами, виявлення на основі аналізу даних пропонує повний спектр відповідних компонентів.

У підсумку, ці рівні можна розділити на три етапи: обробка, аналіз і візуалізація. У такій інтерпретації обробка охоплює перші два рівні (моніторинг та попередню обробку), а аналіз — два середніх (кореляцію подій та аналіз даних).

Для розуміння, яким чином дата майнинг може допомогти у визначенні та ідентифікації вектору атаки, необхідно розглянути поняття кіллчейну кібератаки.

Ланцюжок кібератак (також відомий як ланцюг кіберзнищення) допомагає зрозуміти послідовність подій, які відбуваються під час зовнішньої атаки на IT-середовище компанії. Кіллчейн кібератаки спочатку був розроблений компанією Lockheed Martin, яка прийняла термін «kill chain», який розбиває структуру військової атаки (наступальної або оборонної) на модель, що складається з визначених фаз.

Кіллчейн за версією Lockheed Martin розбиває зовнішню атаку на сім кроків:

1. Розвідка. Зловмисник обирає ціль, вивчає її та шукає вразливості.
2. Озброєння. Зловмисник розробляє шкідливе ПЗ для експлуатації вразливості.
3. Доставка. Зловмисник доставляє шкідливе ПЗ через електронну пошту або будь-який інший засіб передачі (наприклад, бекдор у системі, що дозволяє віддалене виконання коду).
4. Експлуатація. Шкідливе ПЗ виконується на цільовій системі.

5. Встановлення. Шкідливе ПЗ встановлює власний бекдор або інший метод проникнення, що буде доступний зловмиснику.

6. Управління та контроль. Зловмисник отримує повний контроль над системою або мережею жертви.

7. Виконання цілі. Зловмисник реалізує кінцеву мету, таку як викрадення даних, зміна даних або знищення даних.

Хоча початкова модель кіллчейну кібернетиків Lockheed Martin є корисною відправною точкою для спроб моделювання та протидії атакам, слід мати на увазі, що як і будь-яка модель безпеки, кожна реалізація ІТ-загрози є унікальною, і що атаки, як правило, не слідують шаблону.

З роками ландшафт атак розвивався, і багато хто стверджував, що ланцюжок кіллчейну, хоча й корисний, потребує оновлення, щоб відобразити, що традиційний периметр змінився. За думкою деяких експертів, традиційного периметру вже зовсім не існує.

За даними дослідження Forrester Research, сьогодні приблизно 80% порушень безпеки пов’язані з привілейованим доступом до інформації. Щоб краще проілюструвати компонент привілейованої загрози сучасних кібератак, BeyondTrust випустила оновлену модель ланцюга кібератак у 2017 році разом із покроковими інструкціями про те, як знешкодити атаку. Фактично, ці кроки є більш формалізованим відображенням запропонованої Lockheed Martin моделі.

Перший крок полягає у експлуатації периметру. Він включає у себе початкові спроби скомпрометувати систему, використовуючи наступні техніки:

- експлуатація відомих вразливостей у програмному та апаратному забезпеченні;
- використання прийомів соціального інженірингу (як, наприклад, фішинг) для здобування доступу до паролів та інших облікових даних;
- прямий хакінг з ціллю пошуку відкритих портів або інших точок входу.

Другий крок передбачає підвищення привілеїв у системі та етап ескалації з ціллю отримання доступу до більш привілейованих облікових записів (наприклад, обліковий запис системного адміністратора всієї мережі).

Третій крок включає у себе латеральний рух (Lateral movement) з метою пошуку можливостей підвищення привілеїв, доступу до привілейованих облікових записів та пошуку інших можливих вразливостей у системі. Даний прийом зловмисник виконує, рухаючись поміж робочих станцій та облікових записів у мережі організації, сподіваючись знайти якнайбільше корисних для нього бекдорів.

Побудова моделі захисту системи, яка може протидіяти подібним крокам, можлива з використанням комбінованих рішень побудови системи захисту інфраструктури, проте, це все ще залишає зловмисникам деякий простір для маневрування, особливо, коли йде мова про вразливості нульового дня.

В якості рішення пропонується впровадження дата майнингу з використанням прогнозного моделювання для визначення потенційних або вже реалізованих векторів атак у мережі організації. Для досягнення позитивного результату є необхідність аналізу не тільки вхідних даних системи, для якої будується модель, але й інших систем, що вже стали жертвами певних кібератак або мають схожу конфігурацію. Не дивлячись на те, що нова модель сучасних кібер атак від спеціалістів BeyondTrust дещо узагальнена, а окремі експерти вважають, що ландшафт атак сильно змінився, більш точним буде твердження про те, що ландшафт атак пристосувався до сучасних засобів захисту інформаційних інфраструктур. Через це зловмисникам довелося шукати нові способи реалізації атак, але, як показує практика, чимала кількість сучасних кібератак відбувалася завдяки реалізації старих вразливостей, про які навіть було відомо.

В якості прикладу і підтвердження необхідності впровадження дата майнингу у процес визначення векторів кібератак, розглянемо кіллчейн структуру кібератаки WannaCry, яка відбулася у травні 2017-го року.

Основним «вхідним квитком» для WannaCry був бекдор-інструмент DoublePulsar, який був оприлюднений хакерською групою The Shadow Broker на початку 2017-го року. Перший варіант цього бекдору був помічений спеціалістами Symantec ще у березні 2016-го року, проте, це не завадило зловмисникам вразити даним бекдором більше ніж 200 000 комп’ютерів під управлінням ОС Windows лише за кілька тижнів, не викликавши при цьому жодних підозр.

Іншим важливим компонентом цієї атаки був експлойт EternalBlue, опублікований все тією ж групою хакерів The Shadow Broker у квітні 2017-го року, який вони попередньо вилучили з серверів NSA. Перші сліди реалізації цього експлойту були знайдені ще у березні 2016-го року в рамках APT-атаки, реалізованої китайською групою хакерів. Сам експлойт EternalBlue представляє собою використання вразливості у реалізації протоколу Server Message Block (SMB) від Microsoft. Не дивлячись на відкритий доступ до деталей про ці кібератаки та патч безпеки, що вийшов у березні 2017-го року, у червні того ж року була здійснена ще одна кібератака з використанням експлойту EternalBlue. На початок 2018-го року вже всі системи під управлінням ОС Windows, починаючи з версії Windows 2000, були заражені експлойтом EternalBlue, що також у майбутньому призвело до зламів систем, як, наприклад, масштабна атака на місто Балтімор, США у 2019-му році. Основною причиною тих атак вважається все ж той факт, що велика кількість систем була не оновлена, але свіжі дослідження ринку вказують, що навіть компанії, які вкладають величезні гроші у кіберзахист, страждають від зламів систем, втрати, викрадення даних та порушення роботи організації та її компонентів.

На прикладі першого етапу реалізації атаки WannaCry розглянемо, яким чином дата майнинг допоміг би якщо не ліквідувати повністю, то хоча б знизити втрати від реалізації атаки.

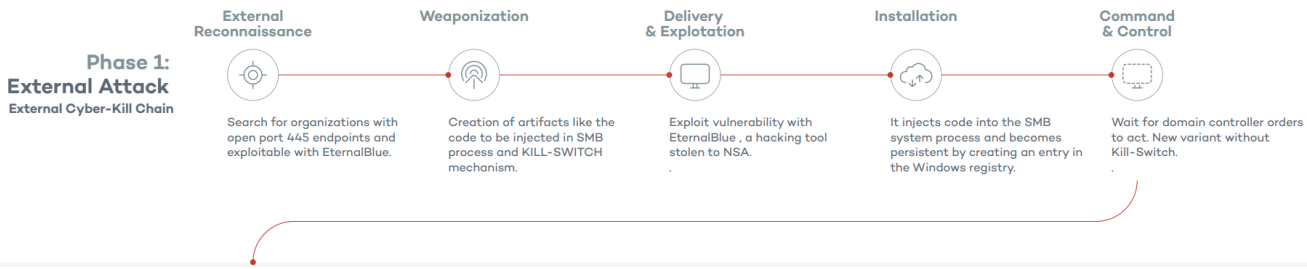

Рисунок 3.5 - Перший крок кіллчейну WannaCry

Перший крок (Розвідка) першого етапу передбачає собою розвідку цільової системи і пошук відкритих портів у системі. Порт 445 є загальним для переважної більшості систем та мереж, тому, на цьому етапі автоматизованій системі з долученням дата майнингу було б важко виділити підозрілу активність. Зовнішня розвідка системи дуже часто використовується зловмисниками саме по 445 порту, тому загальний зріст запитів, що надходять на цей порт з зовнішньої мережі, вже можуть відмічатися автоматизованою системою як потенційна майбутня загроза за допомогою побудови прогнозійної моделі.

Другий крок (Озброєння) має за мету підготувати шкідливе ПЗ до втручання у систему через SMB та вплинути на механізм kill-switch, який виконує функцію «тривожної кнопки», за допомогою якої можна зупинити атаку. На цьому кроці попередній аналіз ландшафту безпеки у своїй та суміжній мережах може дати розуміння того, що протокол SMB скомпрометований. Додатково на користь цього каже третій крок, який пов’язаний з доставкою та експлуатацією вразливості. Можливість реалізації експлойту EternalBlue закладена у протокол SMB. Якби налаштована автоматизована система мала інформацію про схожу активність у інформаційній системі у 2016-му році, спеціалісти безпеки змогли б не тільки відреагувати, але й запобігти існуванню можливості реалізації даної кібератаки впровадивши патчі безпеки, випущені Microsoft. Використання прогнозної моделі дата майнингу дозволить будувати системи захисту інформаційної системи не лише «на сьогодні», але і з урахуванням можливих майбутніх загроз, а також визначати за первинними ознаками, який потенційний вектор кібератаки реалізується на даний момент або може бути реалізований з огляду на актуальну конфігурацію системи.

Висновок до третього розділу

У третьому розділі були освітлені існуючи способи застосування дата майнингу у кібербезпеці. Було також розглянуто поняття ситуаційної обізнаності у кібербезпеці, що є основою для розуміння поточних та майбутніх загроз для

організації і лягає в основу необхідності використання дата майнингу для постійного оновлення наявної бази знань аби підтримувати її в актуальному стані.

Описано запропонований метод виявлення та ідентифікації векторів атак на основі ключових метрик ІС, метод розглянуто на прикладі кіллчейну кібератаки WannaCry.

ВИСНОВКИ

Метою дослідження було формування методу виявлення векторів атак на основі ключових метрик ІС. В якості рішення задачі було запропоновано поєднання існуючих інструментів управління ризиками, інформаційною безпекою з методами дата майнингу для збору більшого об’єму даних, що дозволить у кінцевому результаті передбачати атаки, уникаючи необхідності нести збитки.

Найбільш придатним методом обрано прогнозне моделювання, так як воно найчастіше має більш точний результат і спрямоване на прогнозування кінцевого результату. Уніфікація вхідних даних цільової системи може бути забезпечена завдяки прийняттю моделі ситуаційної обізнаності у кібербезпеці, яка не має прив’язки до сталих параметрів системи, а завдяки комбінованому використанню програмних засобів захисту інформаційної структури зможе надати більшу вибірку даних для аналізу і подальшого надання прогнозу з визначення вектору атаки, який експлуатується або може бути проексплуатований.

В якості додаткового джерела інформації для подібного методу можуть бути типові шаблонні кіллчейни, які можуть розробляти аналітики безпеки з оглядом на тренди у сучасному середовищі атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO. ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements [Електронний ресурс], ISO, ISO/IEC. – 2013. – Режим доступу до ресурсу: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en..

2. Рубан І. В. КЛАСИФІКАЦІЯ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ [Електронний ресурс], І. В. Рубан, В. О. Мартовицький, С. О. Партика, Системи озброєння і військова техніка. – 2016. – Режим доступу до ресурсу: https://openarchive.nure.ua/bitstream/document/3418/1/soivt_2016_3_24.pdf.

3. King N. ISO 27001 risk assessments: How to identify risks and vulnerabilities [Електронний ресурс], Nicholas King. – 2019. – Режим доступу до ресурсу: https://www.vigilantsoftware.co.uk/blog/iso-27001-risk-assessments-identify-risks.

4. Intelligent interfaces [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www2.deloitte.com/xe/en/insights/focus/tech-trends/2019/human-interaction-technology-intelligent-interface.html.

5. Кібератаки на держоргани України: скільки інцидентів було заблоковано [Електронний ресурс], "Слово і діло". – 2022. – Режим доступу до ресурсу: https://www.slovoidilo.ua/2022/02/15/infografika/bezpeka/kiberataky-derzhorhany-ukrayiny-skilky-incydentiv-bulo-zablokovano.

6. Lao K. What is a threat vector and why is it important to define [Електронний ресурс], Kapua Lao. – 2020. – Режим доступу до ресурсу: https://www.paubox.com/blog/what-is-a-threat-vector/.

7. Кононова В. О. ОЦІНКА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ [Електронний ресурс], В. О. Кононова, О. В. Харкянен, С. В. Грибков. – 2014. – Режим доступу до ресурсу: https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6630/17-99-105.pdf.

8. Ревізорова К. Оцінка критичності вразливостей в операційних системах [Електронний ресурс], К. Ревізорова, Т. Гріненко, GLOBAL CYBER SECURITY FORUM 2019. – 2019. – Режим доступу до ресурсу: https://openarchive.nure.ua/bitstream/document/10553/1/REVIZOROVA.pdf.

9. Дячков Д. В. МЕТОДИЧНІ ПІДХОДИ ДО ОЦІНКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА [Електронний ресурс], Д. В. Дячков – Режим доступу до ресурсу: http://dspace.pdaa.edu.ua:8080/bitstream/123456789/2572/1/%D0%A1%D0%A2%D0%90%D0%A2%D0%A2%D0%AF_%D0%A1%D0%A3%D0%9C%D0%98_%D0%94%D0%AF%D0%A7%D0%9A%D0%9E%D0%92.pdf.

10. 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends [Електронний ресурс], Purplesec. – 2021. – Режим доступу до ресурсу: https://purplesec.us/resources/cyber-security-statistics/#:~:text=Cyber%20Security%20Risks,and%20health%20records%20left%20unprotected.

11. Cyber-Attack Chain [Електронний ресурс], BeyondTrust – Режим доступу до ресурсу: https://www.beyondtrust.com/resources/glossary/cyber-attack-chain.

12. An Anatomy of the WannaCry Cyberattack [Електронний ресурс], Panda Security. – 2017. – Режим доступу до ресурсу: https://www.pandasecurity.com/en/mediacenter/news/infographic-wannacry-cyberattack/.

13. Sobers R. 134 Cybersecurity Statistics and Trends for 2021 [Електронний ресурс], Rob Sobers, Varonis. – 2021. – Режим доступу до ресурсу: https://www.varonis.com/blog/cybersecurity-statistics.

14. 2022 Cyber Attack Statistics, Data, and Trends [Електронний ресурс], Parachute Technologies. – 2022. – Режим доступу до ресурсу: https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/.

15. 15 Alarming Cyber Security Facts and Stats [Електронний ресурс], Cybint. – 2020. – Режим доступу до ресурсу: https://www.cybintsolutions.com/cyber-security-facts-stats/.

16. Stonebumer G. Risk Management Guide for Information Technology Systems [Електронний ресурс], G. Stonebumer, A. Goguen, A. Feringa, NIST. – 2002. – Режим доступу до ресурсу: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf.

17. What is risk management? [Електронний ресурс], IBM – Режим доступу до ресурсу: https://www.ibm.com/topics/risk-management.

18. Tucci L. What is risk management and why is it important? [Електронний ресурс], Linda Tucci, TechTarget. – 2021. – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important.

19. International standard for risk management: ISO 31000: 2009 [Електронний ресурс], Standards Australia. – 2009. – Режим доступу до ресурсу: https://www.researchgate.net/figure/International-standard-for-risk-management-ISO-31000-2009-Standards-Australia-2009_fig1_274570189.

20. The ISO 31000 standard Risk management: principles and guidelines [Електронний ресурс], Risk Engineering. – 2017. – Режим доступу до ресурсу: https://risk-engineering.org/ISO-31000-risk-management/.

21. What is an Attack Vector? [Електронний ресурс], Fortinet – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/attack-vector.

22. Attack Surface [Електронний ресурс], Fortinet – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/attack-surface.

23. Social Engineering [Електронний ресурс], Imperva – Режим доступу до ресурсу: https://www.imperva.com/learn/application-security/social-engineering-attack/.

24. Tyas Tunggal A. What is an Attack Vector? 16 Common Attack Vectors in 2022 [Електронний ресурс], Abi Tyas Tunggal, UpGuard. – 2022. – Режим доступу до ресурсу: https://www.upguard.com/blog/attack-vector.

25. Yatsenko M. Using Data Mining Techniques in Cybersecurity Solutions [Електронний ресурс], M. Yatsenko, A. Beliiba, Apriorit. – 2022. – Режим доступу до ресурсу: https://www.apriorit.com/dev-blog/527-data-mining-cyber-security.

26. Data Mining. What it is & why it matters [Електронний ресурс], SAS – Режим доступу до ресурсу: https://www.sas.com/en_us/insights/analytics/data-mining.html.

27. Cyber Security Situational Awareness [Електронний ресурс], The Government of the Hong Kong – Режим доступу до ресурсу: https://www.ogcio.gov.hk/en/our_work/information_cyber_security/awareness/.

28. Situational Awareness [Електронний ресурс], Carnegie Mellon University. – 2016. – Режим доступу до ресурсу: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-SA_0.pdf.

29. Tianfield H. Cyber Security Situational Awareness [Електронний ресурс], Tianfield, 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). – 2016. – Режим доступу до ресурсу: https://www.semanticscholar.org/paper/Cyber-Security-Situational-Awareness-Tianfield/ff6b922623731899d42bdc942b2d27243f39e376#extracted.

30. Saheed Ganiyu I. 5 Top Data Models in Data Mining in 2022 [Електронний ресурс], Isola Saheed Ganiyu, Hevodata. – 2022. – Режим доступу до ресурсу: https://hevodata.com/learn/data-models-in-data-mining/#3.

31. Tianfield H. Data Mining Based Cyber-Attack Detection [Електронний ресурс], Hua Tianfield. – 2017. – Режим доступу до ресурсу: https://www.researchgate.net/publication/321491605_Data_Mining_Based_Cyber-Attack_Detection.