Лабораторна робота 2

Дослідження та ідентифікація сучасних загроз

Цілі та задачі

Дослідження можливостей забезпечення функцій безпеки, які використовуються організаціями для збереження даних.

Частина 1: Дослідження загроз, які витікають від кібератак

Частина 2: Тріада CIA (конфіденційність, цілісність і доступність)

Довідкова інформація/Сценарій

Загрози сучасного кіберсвіту є реальною небезпекою. Ці загрози можуть призвести до хаосу у сучасному комп'ютер-центричному світі. Про ці загрози повинен знати кожен, однак повністю нейтралізувати їх зможуть тільки професіонали, які зможуть розпізнавати загрози та нейтралізувати кібер-злочинців. Силами таких організацій, як CompTIA, Cisco Systems та ISC2 та інших створені та реалізуються програми для навчання та сертифікації спеціалістів у галузі кібербезпеки.

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Part 1: Дослідження загрози від кібератак

Кібератаки очолюють рейтинг списку загроз, з якими стикаються країни всьому світу. У свідомості суспільства загрози національній або світовій безпеці найчастіше асоціюється з фізичними нападами або зброєю масового знищення. В дійсності, кібер-загроза очолює список загроз більше, ніж у двадцяти країнах світу. Перше місце в рейтингу кібератак, розкриває багато аспектів того, як суспільство змінилося. Комп'ютери та комп'ютерні мережі впливають на те, як ми навчаємось, здійснюємо покупки, спілкуємось, подорожуємо та живемо. Комп'ютерні системи контролюють практично усі аспекти нашого життя. Збій комп'ютерних систем та комп'ютерних мереж може мати руйнівний вплив на сучасне життя. Цілями кібератак є все: системи виробництва та розподілу електроенергії, системами очищення та подачі води, транспорт та фінансові системи. Кожна з таких систем вже була жертвою кібератак. Переглянути відео, посилання на яке наведено нижче. Поділіться на групи по 3-4 особи. Після перегляду відео, дайте відповідь на наступні питання.

Step 1: Дослідження загроз.

На кроці 1 ви будете досліджувати загрози.

a. Натисніть тут щоб переглянути відео. Згідно думки авторів відео, що є найнебезпечнішою зброєю у світі? Чому? Чи згодні ви з такою думкою?

_____

_____

b. Перерахуйте п'ять способів порушення закону за допомогою комп'ютерів. Чи можуть наслідки перерахованих злочинів вплинути на вас особисто? Ви чи ваші рідні були жертвами таких злочинів?

_____

_____

c. Чи скоювались реальні злочини, що пов’язані з загрозами, які зображені на відео? Натисніть тут, і тут щоб дізнатися більше про ці атаки.

_____

_____

Step 2: Дослідження недавніх атак.

a. Вплив і масштаби недавніх кібератак викликає занепокоєння у багатьох ділових колах та державних структурах. Натисніть тут щоб прочитати про найбільші кіберінциденти у 2022-2023 роках.

   Які галузі та країни найбільш постраждали від витоку даних?

   _____

   _____

b. Назвіть 10 найбільш небезпечних вразливостей 2022 та 2023 років.

   _____

   _____

   _____

Part 2: Тріада CIA

Конфіденційність, цілісність та доступність (Confidentiality, integrity, and availability, CIA) - є трьома основними принципами кібербезпеки. Ці три принципи складають тріаду CIA. Елементи тріади є трьома найважливішими елементами кібербезпеки. Кожен з спеціалістів з кібербезпеки повинен добре розуміти ці основні принципи.

Step 1: Дослідіть тріаду CIA.

a. Натисніть тут щоб переглянути відео. Що таке конфіденційність даних? Чому конфіденційність даних, що належать приватним осібам та організаціям є настільки важливою?

   _____

   _____

b. Що таке цілісність даних? Вкажіть три способи порушення цілісності та достовірності даних.

   _____

   _____

c. Що таке доступність системи? Що може статися, якщо критично важлива комп'ютерна система стане недоступною?

   _____

   _____

Step 2: Дослідіть кібератаки.

Натисніть тут, щоб переглянути відео. Що спробували добитись кіберзлочинці? У який час доби здійснено атаку? Чи правильним є твердження, що мережеві атаки найчастіше здійснюються у неробочий час? Чому?

_____

_____