**Міністерство освіти та науки України**

**Державний торговельно-економічний університет**

***Кафедра інженерії програмного забезпечення та кібербезпеки***

**ЗВІТ**

***З ЛАБОРАТОРНОЇ РОБОТИ № 3***

*з дисципліни*

**«ОСНОВИ КІБЕРБЕЗПЕКИ»**

**НА ТЕМУ:**

ІДЕНТИФІКАЦІЯ ЗАГРОЗ

(назва теми)

**Виконала:** студентка факультету інформаційних технологій

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Ковальова Людмила Ігорівна

Київ 2024

**Лабораторна робота №3**

**Тема**: ідентифікація загроз

**Ціль**: вивчення можливостей забезпечення функцій безпеки, які використовуються організаціями для збереження даних.

**Хід роботи:**

**Частина 1**: Дослідження загрози від кібератак

1. Дослідження загроз
   1. Згідно думки авторів відео за наданим посиланням, найнебезпечнішою зброєю в світі є комп’ютер в руках злочинця, бо за допомогою нього можна стерти особистість людини, зруйнувати Уолл-стріт, посадити літаки, вивести з ладу електромережу, сіяти хаос в економіці.

Я цілком згодна з цією думкою, адже сучасні технології надзвичайно потужні і вони можуть використовуватися злочинцями для разноманітних злочинних дій. Окрім сказаного в відео, атаки кіберзлочинців можуть використовуватися частиною воєнних дій, що використовуються для впливу на військові стратегії, комунікаційні системи та контроль використання зброї.

* 1. П'ять способів порушення закону за допомогою комп'ютера:
     1. Хакерство і несанкціонований доступ до комп'ютерних систем
     2. Фішинг і шахрайство
     3. Розповсюдження вірусів та шкідливого програмного забезпечення
     4. Кібервандалізм
     5. Кібершантаж і викрадення даних

Наслідки таких злочинів можуть вплинути на мене особисто або моїх рідних, оскільки ми всі користуємося комп'ютерами та інтернетом у повсякденному житті, але через достатню обізнаність про кібергігієну, це не має часто завдавати проблем.

В дитинстві ж, в наслідок завантаження піратського програмного забезпечення, частим явищем було отримання вірусів та шкідливого програмного забезпечення.

* 1. Подібні злочини, зображені в відео, реально скоювалися, хоч і кожен з цих сценарієв потребує великого рівня компетентності, ресурсів та доступу до надскладних технологій.

Наприклад, у 2015 році кіберзлочинці викрали дані з електромережі України, що призвело до масштабного відключення електроенергії.

Або, у 2014 році хакерська група, яка вважається пов'язаною з Північною Кореєю, зламала комп'ютерні системи Sony Pictures Entertainment. Ця атака призвела до викрадення конфіденційної інформації, включаючи особисту кореспонденцію, електронні версії фільмів та інші документи, а також до витоку незаконних копій фільмів.

Багато фінансових установ були жертвами кібератак, включаючи крадіжки грошей, кібершантаж та інші види фінансової маніпуляції. Наприклад, у 2016 році хакери вкрали мільйони доларів з банківських систем за допомогою вірусу SWIFT.

1. Дослідження недавніх атак
   1. Одним з найбільш руйнівних кібер-зламів 2015 року був витік даних Управління кадрової служби США (United States Office of Personnel Management, OPM). Він став одним з найбільших кіберзлочинів в історії Сполучених Штатів. У цьому витіку було викрадено мільйони записів з особистою інформацією співробітників урядових установ США, включаючи дані з охорони та інші конфіденційні дані. Орієнтовно, цей витік даних вплинув на близько 21.5 мільйонів осіб, що стало одним з найбільших порушень безпеки даних у історії США.
   2. У 2015 році британський інтернет-провайдер TalkTalk став жертвою серйозної кібератаки. Злочинці, які стояли за цією атакою, були групою молодих хакерів, один з яких виявився неповнолітнім. У результаті кібератаки, злочинці викрали різноманітні дані, включаючи особисту інформацію, таку як імена, адреси, номери телефонів, адреси електронної пошти, а також дані банківських карток, в тому числі частину або всі цифри номера картки і код безпеки CVV2. Крім того, кіберзлочинці також здійснили кілька фінансових транзакцій, використовуючи вкрадені дані, та вимагали від TalkTalk викуп за відновлення доступу до вкрадених даних. У результаті цієї атаки та її наслідків, десятки тисяч клієнтів TalkTalk стали жертвами шахрайства та крадіжки особистих даних.

**Частина 2**: Тріада CIA

1. Дослідження тріади CIA.
   1. Конфіденційність даних - це забезпечення захисту конфіденційної інформації від несанкціонованого доступу, використання чи розголошення. Конфіденційність даних для приватних осіб та організацій є критично важливою з кількох причин:
      1. Конфіденційні дані можуть містити особисту інформацію, таку як імена, адреси, номери телефонів, соціальні номери, медичні записи тощо. Забезпечення конфіденційності цих даних важливо для захисту особистої приватності та запобігання можливим випадкам шахрайства або ідентифікаційного зловживання.
      2. Для бізнесів конфіденційні дані можуть включати комерційну інформацію, секрети виробництва, патенти, стратегічні плани розвитку, клієнтські списки та інші конфіденційні дані. Витік або неправильне використання цих даних може призвести до серйозних фінансових втрат та втрати конкурентоспроможності.
      3. Дотримання законодавства
      4. Довіра клієнтів і партнерів
   2. Цілісність даних - це властивість даних, що гарантує їхню недоторканність, стабільність та відсутність змін або порушень без належних авторизованих дозволів.

Три способи порушення цілісності та достовірності даних:

1. Неавторизована модифікація даних. Це може призвести до втрати важливої інформації, спотворення даних або виконання небажаних дій.
2. Шкідливі програми, такі як віруси, черви, троянці та інші, можуть впливати на цілісність даних, шифруючи, видаляючи або модифікуючи їхній вміст. Це може призвести до втрати чи пошкодження важливих даних.
3. Фізичні пошкодження обладнання або систем збереження даних також можуть порушити їхню цілісність. Наприклад, пожежі, повені, збої жорстких дисків або інші природні катастрофи можуть призвести до втрати даних або їхнього пошкодження.
   1. Доступність системи - це властивість системи, що забезпечує неперервну доступність та функціональність для користувачів у встановленому часовому інтервалі. Якщо критично важлива комп'ютерна система стане недоступною, це може призвести до серйозних наслідків:
      1. Збитки в бізнесі
      2. Порушення послуг інформаційних технологій
      3. Втрата даних
      4. Порушення безпеки
4. Дослідження кібератак

*(Посилання на відео не робоче)*

Твердження, що мережеві атаки найчастіше здійснюються у неробочий час для компанії, може бути правильним у певних випадках:

1. У неробочий час для компанії може бути менше персоналу на місці, а також менше активного моніторингу мережі. Це може зробити компанію менш вразливою до виявлення та реагування на атаки.
2. У неробочий час для компанії може бути менше викликів або повідомлень до технічної підтримки.
3. Залежно від типу атаки та мотивації атакувача, неробочий час може забезпечити більшу ймовірність успіху атаки.
4. Це може полегшити атакувачам у хованні слідів.