Одеський коледж комп’ютерних технології «Сервер»

Звіт з практичної роботи №7

З предмету «Технології захисту інформації»

Тема : «Аналіз поточної ситуації в Україні в напрямку кіберзлочинності»

Виконував :

Студент групи К21.1

Машков Володимир

Одеса 2024

ВСТУП

Метою цього звіту є дослідження поточної ситуації в Україні щодо кіберзлочинності, аналіз найбільш актуальних схем кіберзлочинності, методів боротьби з ними та надання рекомендацій для користувачів щодо захисту від кіберзагроз.

ПОТОЧНА СИТУАЦІЯ В УКРАЇНІ ЩОДО КІБЕРЗЛОЧИННОСТІ ТА ОСНОВНІ СХЕМИ КІБЕРЗЛОЧИННОСТІ

Кіберзлочинність в Україні, як і в усьому світі, постійно зростає за рівнем організованості та складності. В умовах діджиталізації суспільства та зростання використання інтернет-технологій, кіберзлочинці знаходять нові способи атакувати організації та користувачів. Найчастіше жертвами атак стають банки, державні установи та приватні особи, які не мають достатнього рівня кіберзахисту.

Основні схеми кіберзлочинності :

1. Вірусні атаки та шкідливе ПЗ

Одним із найбільш поширених способів здійснення кіберзлочинів є використання шкідливого програмного забезпечення (ПЗ), зокрема вірусів, троянських програм, руткітів, шпигунських програм. Кіберзлочинці використовують шкідливі програми для крадіжки конфіденційних даних, паролів, а також для шифрування файлів з метою отримання викупу.

1. Фішинг

Фішинг є однією з найпоширеніших форм соціальної інженерії, яка полягає у виманюванні конфіденційної інформації користувачів через підроблені веб-сайти або електронні листи. У результаті фішингових атак користувачі можуть втрачати доступ до своїх банківських рахунків, облікових записів у соціальних мережах тощо.

1. DDoS-атаки

Атаки типу "відмова в обслуговуванні" (DDoS) використовуються для виведення з ладу веб-сайтів та серверів шляхом перевантаження їхніми запитами. Такі атаки зазвичай спрямовані на бізнес-організації та державні установи з метою саботажу або вимагання.

1. Атаки на фінансові установи

Кібершахраї часто атакують банки та платіжні системи з метою викрадення грошей. Такі атаки можуть здійснюватись через впровадження троянських програм або експлуатацію вразливостей у системах захисту банківських установ.

МЕТОДИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ, ДЕРЖАВНІ ІНІЦІАТИВИ ТА ТЕХНІЧНІ ЗАХОДИ

Законодавчі та державні ініціатив проти кіберзлочинності

В Україні розроблено ряд законодавчих актів для боротьби з кіберзлочинністю:

* Закон України "Про основні засади забезпечення кібербезпеки України" (від 05.10.2017 № 2163-VIII). Закон визначає правові та організаційні основи забезпечення кібербезпеки.
* Кримінальний кодекс України (стаття 361-363-1). Відповідальність за несанкціоноване втручання в роботу комп'ютерних мереж.
* Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Закон регулює питання захисту інформації в електронних системах.
* Закон України "Про електронні довірчі послуги" (від 05.10.2017 № 2155-VIII). Регулює захист електронних підписів, сертифікатів, довірчих послуг.

Також слід нагадати, що Україні діють державні органи, що здійснюють моніторинг кіберзагроз та боротьбу з кіберзлочинністю:

* Національний координаційний центр кібербезпеки при РНБО.
* Кіберполіція України.
* CERT-UA – команда реагування на кіберінциденти.

ТЕХНІЧНІ ЗАХОДИ ТА РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

Для протидії кіберзлочинності використовуються такі технічні засоби:

* Використання сучасного антивірусного програмного забезпечення.
* Використання багаторівневих систем автентифікації.
* Шифрування конфіденційної інформації.
* Регулярне оновлення програмного забезпечення для закриття вразливостей.

Але ж, для зменшення ризиків стати жертвами кіберзлочинців користувачам рекомендується дотримуватися таких заходів безпеки:

1. Встановлюйте надійне ПЗ:

Використовуйте офіційне антивірусне програмне забезпечення та регулярно оновлюйте його.

1. Обережно ставтеся до електронної пошти:

Не відкривайте підозрілі листи або вкладення з невідомих джерел.

1. Використовуйте двофакторну автентифікацію:

Це додатковий рівень захисту для доступу до ваших облікових записів.

1. Регулярно змінюйте паролі:

Використовуйте складні паролі і змінюйте їх регулярно.

1. Шифруйте важливі файли:

Для захисту конфіденційної інформації використовуйте програмне забезпечення для шифрування.

1. Не підключайтесь до публічних мереж без VPN:

Використовуйте віртуальні приватні мережі (VPN), коли підключаєтесь до інтернету в публічних місцях.

1. Слідкуйте за оновленнями:

Регулярно оновлюйте всі програми та операційні системи для закриття вразливостей.

ВИСНОВОК:

Кіберзлочинність в Україні продовжує набирати обертів, зокрема у сфері фінансових операцій та державних установ. Для ефективної боротьби з кіберзлочинами необхідно посилювати законодавчу базу, активно впроваджувати новітні технології захисту та підвищувати обізнаність населення щодо правил кібербезпеки.