НАЦІОНАЛЬНА БЕЗПЕКА

Андронік О.М., Гнатюк І.В.
студенти,
Науковий керівник: **Сєвідова І.О.**
доктор економічних наук, професор кафедри,
Харківський національний університет внутрішніх справ

АТАКИ НА ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Хакерська атака (кібератака) – спроба реалізації загрози. Тобто, це дії кібер-зловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Під атакою на інформаційну систему розуміють дії (процеси) або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загроз інформаційним ресурсам, шляхом використання вразливостей цієї інформаційної системи [1].

Існує безліч видів атак на інформаційні системи та технології. Ось деякі з них.

Mailbombing найстаріший вид атак. Значно збільшується трафік і кількість надісланих повідомлень, що генерує збій в роботі сервісу. Це викликає параліч не тільки Вашої пошти, а й роботи самого поштового сервера. Ефективність таких атак в наші дні вважається нульовою, оскільки тепер провайдер має можливість встановити обмеження трафіку від одного відправника [2].

Принцип атак шляхом *переповнення буфера* – програмні помилки, при яких пам’ять порушує свої ж кордони. Це, в свою чергу, змушує або завершити процес аварійно, або виконати довільний бінарний код, де використовується поточний обліковий запис. Якщо обліковий запис – адміністраторський, то дані дії дозволяють отримати повний доступ до системи [2].

Тип атак через *віруси, трояни, поштові черв’яки, сніффери* об’єднує різні сторонні програми. Призначення і принцип дії такої програми може бути надзвичайно різноманітним, тому немає сенсу докладно зупинятися

на кожній з них. Всі ці програми об'єднує те, що їх головна мета – доступ і «зараження» системи [2].

Вид атаки *Man-in-the-Middle*, коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всього потоку інформації, що передається між абонентами. При отриманні доступу на такому рівні зловмисник може модифікувати інформацію потрібним йому чином, щоб досягти своєї цілі. Мета такої атаки – незаконне отримання, крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі. Такі атаки вкрай складно відстежити, оскільки зазвичай зловмисник знаходиться всередині організації [3].

Соціальна інженерія стала невід'ємною частиною атак кібершахраїв. Мова йде про спеціальну методику маніпуляції, яка допомагає змусити людину віддати зловмисникам необхідні дані. Яким чином? Використовуючи людські слабкості – тобто емоції та природну поведінку жертви [4].

Інструмент соціальної інженерії досить цікавий внаслідок практично відсутніх фінансових витрат. Тоді як в кінцевому результаті це може стати ключем до отримання інформації або ж «дій», які можуть принести величезні вигоди. Основними інструментами, що використовує злочинець є інтелект та жвавий розум, що дозволяють знайти підхід до жертви, а також обрати вірний шлях дій у випадку, коли щось пішло «не так» [5].

Зловживання функціональністю – це метод атаки, при якому використовуються власні функції і можливості веб-сайту для атаки на себе або інших. Зловживання функціональністю можна описати як зловживання передбачуваної функціональністю додатка для досягнення небажаного результату. Ці атаки призводять до різних результатів, таким як споживання ресурсів, обхід засобів контролю доступу або витік інформації. Потенціал і рівень зловживань будуть варіюватися залежно від об'єкту. Атаки із зловживанням функціональністю часто являють собою комбінацію інших типів атак або використовують інші вектори атак [6].

Підводячи підсумок можна з упевненістю сказати що атаки на інформаційні системи – конкретна проблема у сьогоденні. Безліч видів та способів таких атак (особливо соціальна інженерія) є конкретною проблемою, яка несе негативні наслідки для інформаційних систем та технологій. Часом навіть через нашу необережність та надмірну довірливість ми можемо стати жертвою або винуватцем таких атак.

Список використаних джерел:

1. Хакерська атака. *Вікіпедія*, від 13 вер. 2020. URL: https://uk.wikipedia.org/w/index.php?curid=1581873 (дата звернення: 19.10.2020).

2. Види хакерських атак на веб-ресурси. InSite It Company. 2020. URL: https://insite.cc/blog/code/vidi-hakerskih-atak-na-veb-resursi.html (дата звернення: 19.10.2020).

3. Грищук Р.В. Атаки на інформацію в інформаційно-комунікаційних системах. *Сучасна спеціальна техніка.* 2011. № 1(24). С. 61–66.

4. Савчук Т. Соціальна інженерія : як шахраї використовують людську психологію в інтернеті. *Радіо Свобода*, від 30 серп. 2018. URL: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html (дата звернення: 19.10.2020).

5. Нам'ясенко В.М. Соціальна інженерія як одна із загроз економічній безпеці, що спричиняє негативний вплив на ефективність діяльності підприємства. *Економіка та держава.* 2016. № 3. С. 90–92.

6. Auger R. The WASC Threat Classification. *Web Application Security Consortium*, від 23 черв. 2011. 172 р. URL: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf (дата звернення: 19.10.2020).

Дука В.Д., Янова Л.І.
студенти,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

МІЖНАРОДНА БЕЗПЕКА КРІЗЬ ПРИЗМУ ІНФОРМАЦІЙНОЇ РЕВОЛЮЦІЇ

Якщо на зорі історії головною ареною суперництва була суша, то з часом протиборство охопило море, глибини океану, повітря, космос. У XXI ст., як вважають багато експертів, головною ареною стає глобальний інформаційний простір (кіберпростір) [1, с. 216].

Найбільш серйозні загрози часто знаходяться на системному рівні. Можна ціною великих витрат підвищити надійність окремих елементів, структур, однак, як правило, це не підвищує безпеку в цілому. Відповідь на можливу загрозу також повинен бути комплексним і системним [1, с. 230].