дав змогу розробити весь функціонал додатку. Оточення Node JS допомогло виконати з'єднання з базою даних а вільна система керування реляційними базами даних My SQL допомогло зберігати дані локально.

Список літератури

1. Онлайн курс Jonas Schmedtman(Udemy) – «Complete Java Script»[Електронний ресурс] – Режим доступу до ресурсу : https://www.udemy.com/course/the-complete-javascript-course/learn/lecture/5869076#overview.
2. Документація Java Script [Електронний ресурс] – Режим доступу до ресурсу: https://developer.mozilla.org/ru/
3. Документація по HTML5 [Електронний ресурс] – Режим доступу до ресурсу: http://htmlbook.ru/html
4. Документація по Bootstrap [Електронний ресурс] – Режим доступу до ресурсу: https://getbootstrap.com/

УДК 004.056

Войтко Б. С., студент 4 курсу спеціальності 122 «Комп'ютерні науки та інформаційні технології»
Марченко М. М., студент 4 курсу спеціальності 122 «Комп'ютерні науки та інформаційні технології»
Антонов Ю. С., к.ф.-м.н., доцент, доцент кафедри інформаційних технологій

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ІНСТРУМЕНТ ДЛЯ ПРОНИКНЕННЯ У ІНФОРМАЦІЙНУ СИСТЕМУ ПІДПРИЄМСТВА

Донецький національний університет імені Василя Стуса, м. Вінниця

Соціальна інженерія це вид атаки, яка спирається на взаємодію людей і часто супроводжується маніпулюванням цими людьми з порушенням нормальної процедури безпеки і є передовою практикою з метою отримання доступу до систем, мереж або для отримання фінансової вигоди.

Зловмисники використовують методи соціальної інженерії, щоб приховати свої справжні особистості і мотиви і видати себе за довірену людину або джерело інформації. Мета атаки полягає в тому, щоб маніпуляцією або обманним шляхом змусити користувача надати конфіденційну інформацію або доступ зловмиснику в межах організації. Багато вдалих атак в області соціальної інженерії просто покладаються на готовність людей бути корисними. Наприклад, зловмисник може претендувати на роль співробітника, у якого є якась термінова проблема, що вимагає доступу до додаткових мережевих ресурсів [1].

Першим кроком в більшості атак соціальної інженерії є проведення дослідження або своєрідна розвідка, з метою дізнатися про об'єкт атаки якомога більше. Серед зловмисників, що використовують соціальну інженерію,

популярна тактика, яка полягає в тому, щоб зосередитися на поведінці співробітників з невисоким рівнем повноважень, але з початковим доступом, наприклад, охоронцем або людиною, яка сидить на стійці реєстрації. Злочинці можуть переглядати профілі в соціальних мережах цих співробітників, з метою отримання інформації, і, таким чином, вивчати їх поведінку як у онлайн так і звичайному житті особисто. На основі зібраної інформації, злочинець може розробити план нападу, скориставшись вразливостями, виявленими в ході етапу розвідки.

Якщо атака проходить успішно, шахраї отримують доступ до конфіденційних даних – таким, як кредитні картки або банківська інформація, і скориставшись цими даними крадуть гроші або отримують доступ до захищених систем або мереж. До популярних типів атак соціальної інженерії відносяться: фішинг, претекстинг, приманка, QuidProQuo, Tailgating [2].

Дуже часто «батьком соціальної інженерії» називають відомого хакера К.Мітніка, що не є правильним. Мітнік одним з перших почав застосовувати мистецтво маніпулювання людиною відносно комп'ютерної системи, взламуючи не «програмне забезпечення», а людину яка працює за комп'ютером. Саме після цього все, що пов`язано з крадіжкою інформації за допомогою маніпулювання людиною, стали називати соціальною інженерією.

Насправді, всі методи маніпулювання людьми відомі досить давно, одним з найвідомішим прикладів нападу з використанням соціальної інженерії може послужити легендарна Троянська війна, в ході якої греки змогли потрапити в місто Трою і виграти війну, сховавшись в гігантській дерев'яної коня, яка була представлена троянської армії як дар світу. Більш сучасні ж методи в більшості випадків пішли з арсеналу різних спецслужб.

Одним із недавніх прикладів є випадок який стався в липні 2018 року коли кілька американських державних та місцевих урядових установ повідомили про отримання дивних листів звичайною поштою, які містять завантажені шкідливим ПЗ компакт-диски (CD), явно відправлені з Китаю. Цей конкретний приклад, хоч грубий і спрощений, залежить від цікавості одержувачів, які можуть бути спокушені засунути компакт-диск в комп'ютер. Згідно непублічному попередженню, переданому державним і місцевим урядовим установам Центром обміну і аналізу інформації між штатами (MS-ISAC), шахрайство надходило в конверті з поштовим штемпелем на китайській мові і включало в себе «набраний лист з рідкісними китайськими ієрогліфами, що вводять в оману» [3].

Також цікавим був випадок, коли у 2015 році кіберзлочинці отримали доступ до особистого AOL e-mail аккаунту директора ЦРУ Джона Бреннана. Один з шахраїв розповів ЗМІ, що він використовував методи соціальної інженерії, щоб видавати себе за техніка Verizon і запитувати інформацію про обліковий запис Бреннана у телекомунікаційного гіганта. Як тільки зловмисники отримали дані облікового запису Бреннана від Verizon, вони зв'язалися з AOL і використовували раніше отриману інформацію для того, щоб дати правильні

відповіді на питання безпеки для отримання доступу до облікового запису електронної пошти Бреннана [4].

Об’єктом дослідження є використання соціальної інженерії в відношенні студентів та викладачів.

Особливе значення соціальна інженерія надає психологічним факторам і засобам впливу, оскільки занадто довірливі користувачі (в даному випадку викладачі) досить легковажно відносяться до власної кібербезпеки і не усвідомлюють, що неуважність може коштувати їм втрати або оприлюднення персональної інформації, або може завадити адекватному проведенню навчального процесу [5, 6].

Існує багато засобів і способів соціальної інженерії за допомогою яких недобросовісні студенти можуть заволодіти конфіденційною інформацією або вторгнутись до вашої системи задля власних корисних цілей.

Тому, проаналізувавши типи атак, які найчастіше загрожують викладачам, було виділено декілька основних, такі як:

- **Фішинг** – Приклад: Створення відповідної поштової скриньки з даними майже ідентичними до даних іншого співробітника і відправка e-mail повідомлення з проханням перейти за посиланням та перевірити працездатність сайту із подальшим введенням логіну та паролю (сайт при цьому заздалегідь замаскований під офіційний сайт університету, тощо.)
- **Quid Pro Quo** – Приклад: Студент від свого імені відправляє e-mail повідомлення на електронну скриньку викладача з проханням перевірити заархівоване індивідуальне завдання, лабораторну роботу (за допомого спеціального софту під видом архіву маскується RMS вірус дистанційного керування)

Для захисту користувачів від соціальної інженерії можна застосовувати як технічні, так і антропогенні засоби.

Антропогенний захист: залучення уваги людей до питань безпеки; усвідомлення користувачами всієї серйозності проблеми і прийняття політики безпеки системи; вивчення та впровадження необхідних методів і дій для підвищення захисту інформаційного забезпечення. Дані методи мають один спільний недолік: вони пасивні. Величезний відсоток користувачів не звертає увагу на попередження, навіть написані самим помітним шрифтом.

Тому слід застосовувати технічний захист, до якого можна віднести засоби, що заважають отримати інформацію і засоби, що заважають скористатися отриманою інформацією [7]

Загалом експерти з безпеки рекомендують IT-відділам регулярно проводити тестування на проникнення з використанням методів соціальної інженерії в своїй організації. Це допоможе адміністраторам дізнатися, які типи користувачів становлять найбільший ризик для конкретних типів атак, а також визначити, які співробітники вимагають додаткового навчання.

Як мінімум, організації повинні мати захищені поштові та веб-шлюзи, які будуть сканувати електронні листи на наявність шкідливих посилань і

фільтрувати їх, тим самим зменшуючи ймовірність того, що співробітник натисне на нього. Також важливо стежити за оновленнями програмного забезпечення так само як і відстежувати співробітників, які працюють з конфіденційною інформацією і забезпечити складнішу систему їх аутентифікації, проводити регулярні курси або тренінги з персоналом.

Список літератури

1. Wikipedia. Соціальна інженерія [Електронний ресурс] / Wikipedia. – 2015. – Режим доступу до ресурсу: https://cutt.ly/Zyy3a5u.

2. EFSOL. Социальнаяинженерия – как не стать жертвой [Електронний ресурс] / EFSOL. – 2019. – Режим доступу до ресурсу: https://efsol.ru/articles/social-engineering.html.

3. Krebs B. StateGovts. WarnedofMalware-Laden CD SentViaSnailMailfromChina [Електронний ресурс] / BrianKrebs // KrebsonSecurity. – 2018. – Режим доступу до ресурсу: https://krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/.

4. Нефедова М. Школьник взломал почту директора ЦРУ [Електронний ресурс] / Мария Нефедова. – 2015. – Режим доступу до ресурсу: https://xakep.ru/2015/10/20/cia-director-hacked-by-school-student/.

5. Антонов Ю.С., Римар П.В., Антонова О.Г. Проблема DoS/DDoS атак навчальних ресурсів студентами. Сучасний захист інформації. 2019. № 4(40). С. 52-62

6. Студент устроил DDoS-атаку на школьную систему в США [Електронный ресурс] // - Режим доступа: https://threatpost.ru/student-ustroil-dDoS-ataku-na-shkolnuyu-sistemu-v-ssha/8504/ (22.04.2020)

7. Green. Методы защиты [Електронний ресурс] / Green. – 2017. – Режим доступу до ресурсу: https://sites.google.com/site/abcsocialnaainzeneria/home/tehniki-socialnoj-inzenerii/mery-protivodejstvia.

УДК 004.9

Гнатюк М. А., студент 3 курсу
спеціальності 122 «Комп'ютерні науки»
Крикун І. Г., к.ф.-м.н., доцент
кафедри прикладної математики

ІТ У БОРОТЬБІ ІЗ КОРОНОВІРУСОМ

Донецький національний університет імені Василя Стуса, м. Вінниця

Пандемія коронавірусу [1]

Протягом останніх 2 місяців життя в Україні та світі різко змінилося внаслідок пандемії коронавірусу. Вірус 2019-nCoV вперше зафіксували в китайському місті Ухань у грудні 2019 року, але він вже встиг на сьогодні стати причиною глобальної пандемії із високою смертністю.

Нижче наведена динаміка кількості інфікованих у світі [2]: