Фізична безпека

План лекції

Вступ
1. Загрози фізичній безпеці
2. Об’єкти загроз
Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с.
2. 2Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл. URL: https://univd.edu.ua/science-issue/issue/4315.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 72–73.
6. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 65–67.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

Текст лекції

Вступ

Фізична безпека є невід'ємною частиною захисту установи від втручання в роботу її комп'ютерних систем. Але чому? Справа в тому, що маючи фізичний доступ, порушник може безпосередньо взаємодіяти із системою та обійти існуючі механізми захисту. Тому розглянемо загрози, пов'язані з недотриманням правил фізичної безпеки, та рекомендації щодо захисту.

1. Загрози фізичній безпеці

У 2009 році заводи у місті Натанзе (Іран), які збагачували уран у рамках ядерної програми, зазнали безпрецедентної кібератаки. Було уражено близько 200 000 комп'ютерів та 1000 одиниць спеціального обладнання виведено з ладу.

Згідно зі звітом «Business Blackout» збитки становили близько 243 млрд дол. США та змусили Іран припинити свою ядерну програму.

Питання: вищезгадані об'єкти не були підключені до мережі Інтернет. Тож як злочинцям вдалось доставити шкідливий програмний код?
Відповідь: за допомогою флеш-носія, який співробітник заводу вставив у свій комп'ютер. І це – питання фізичної безпеки.

Загроза – проникнення на територію і до приміщень організації.
Зловмисники можуть спробувати потрапити на територію установи, до якої доступ мають тільки авторизовані особи. Відомі методи такого проникнення наступні.

«Вхід на плечах» (Tailgating). Зловмисник намагається приєднатись до групи авторизованих осіб, які заходять до будівлі, видаючи себе за людину, яка теж працює у цій установі (рис. 1).

Рис. 1. Неавторизований прохід «Вхід на плечах» (Tailgating)

«Зайняті руки». Зловмисник видає себе за авторизовану особу, демонструє зайняті руки (наприклад, якимось пакунком/речами/кавою) та нібито не має можливості відчинити двері або пред'явити перепустку. Він сподівається, що авторизовані особи допоможуть йому та пропустять, відкриваючи двері/турнікет своєю карткою (рис. 2а, 2б).

а)

б)

Рис. 2. Неавторизований прохід «Зайняті руки»

«Доставка». Зловмисник маскується під кур'єра доставки або працівника якої-небудь служби забезпечення тощо (рис. 3).

Рис. 3. Неавторизований прохід «Доставка»

Потрібно пам'ятати

- Особа, що намагається потрапити до контрольованої території без атрибутів авторизації (перепустка/картка), є потенційним зловмисником.
- Будь-яке несвідоме сприяння порушенню правил фізичної безпеки не звільняє від відповідальності.
- Потрапляння на контрольовану територію будь-кого повинно регламентуватися визначеними процедурами.

Крадіжка комп'ютерних пристроїв, носіїв даних та ключів (карток) доступу. Зловмисник фізично здійснює крадіжку носіїв даних, які містять цінну інформацію.

Встановлення програми несанкціонованого віддаленого доступу. Отримавши фізичний доступ до комп'ютерного пристрою, зловмисник намагається встановити шкідливу програму, що забезпечує в подальшому несанкціонований віддалений мережевий доступ до системи.

Несанкціонована зміна системних налаштувань для перенаправлення мережевого трафіку на контрольований вузол («людина посередині», man-in-the-middle). Маючи фізичний доступ до комп'ютера, зловмисник змінює мережеві налаштування системи, що дозволяє в подальшому перехоплювати мережевий трафік з пристрою (рис. 4).

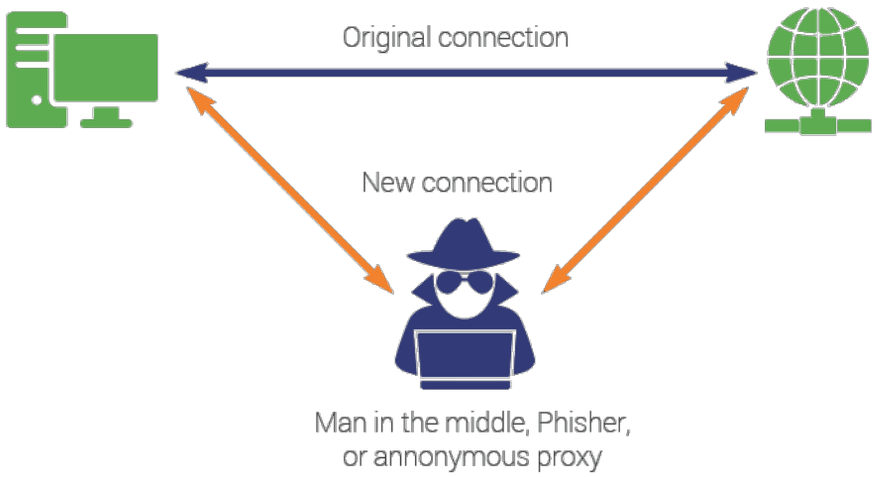

Рис. 4. Атака «людина посередині», man-in-the-middle

Підглядання (shoulder surfing). Зловмисник підглядає за користувачем, коли він вводить у систему чутливі дані: pin-коди, паролі, дані облікових записів, персональну інформацію тощо (рис. 5).

Рис. 5. Підглядання (shoulder surfing)

2. Об’єкти загроз

Об’єктами загроз при фізичному доступі зловмисника до комп’ютерних пристроїв є наступні дані.

Дані банківських карток (рис. 6).

Рис. 6. Дані банківських карток як об’єкт загроз

Паролі розблокування доступу комп’ютерних пристроїв (рис. 7).

Рис. 7. Паролі розблокування доступу комп’ютерних пристроїв як об’єкт загроз

Паролі підключення до Wi-Fi мережі (рис. 8).

Рис. 8. Паролі підключення до Wi-Fi мережі як об'єкт загроз

Флеш-накопичувачі. Флеш-накопичувачі є засобом розміщення ШПЗ, яке в подальшому вручну або автоматично активізується в системі при під'єднанні до комп'ютера.

Дослідження

В 2015 році дослідники з компанії «Google», Університет штату Іллінойс та Університет штату Мічиган провели експеримент[2] щодо ефективності доставки ШПЗ в систему жертви через флеш-накопичувач. На території університетів з метою аналізу поведінки людей та визначення успішності такої атаки було розкидано 297 флешок (рис. 9). Важливо зазначити, що цільова аудиторія була технічно обізнана.

(a) Unlabeled drive (b) Drive with keys (c) Drive with return label (d) Confidential drive (e) Exam solutions drive

Рис. 9. Експериментальні флешки з ШПЗ (https://zakird.com/papers/usb.pdf)

Результат дослідження показав, що 98% людей забрали флеш-носії та 48% відкрили файли. Найкоротший проміжок часу від моменту підняття до відкриття файлу становив 6 хвилин, середній час – 6,9 годин. 68% опитаних

[2] Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein, Michael Bailey. Users Really Do Plug in USB Drives They Find / Conference: 2016 IEEE Symposium on Security and Privacy (SP). URL: DOI:10.1109/SP.2016.26.

сказали, що хотіли повернути пристрої власникам, а 18% сказали, що їм був цікавий зміст файлів. Деякі користувачі зазначили, що флеш-накопичувачі з ключами спонукали їх знайти власника. «Хтось не зможе потрапити до квартири/дому, тому я хотів повернути його якомога швидше».

Користуючись людською психологією і бажанням допомогти/суто почуттям цікавості, зловмисники можуть успішно отримати віддалений контроль над пристроєм та реалізовувати інші атаки.

Висновки

Загальні рекомендації із дотримання фізичної безпеки комп'ютерних систем.
Контроль фізичного периметра:

- перевірка особи, яка намагається потрапити до будівлі;
- заборона допомагати потрапити до будівлі без перевірки особи;
- перевірка кур'єрів і іншого технічного персоналу, які нібито отримали виклик;
- не залишати сторонніх осіб без супроводу всередині установи;
- зачиняти за собою двері.

Нагляд або блокування доступу до пристроїв:

- не залишати пристрої без нагляду;
- налаштувати автоматичне блокування пристроїв у разі тимчасової відсутності поряд із пристроєм.

Блокування доступу для ОС Windows:

- клавіші Windows+L;
- клавіші Ctrl-Alt-Del і обрати «Заблокувати»;
- через налаштування параметрів автоматичного блокування після 5 хвилин відсутності активності.

Блокування доступу для MacOS:

- клавіші Command+Control+Q;
- яблуко у верхньому лівому куті – «Заблокувати екран»;
- «Налаштування» -> «Безпека та приватність» -> «Вимагати пароль відразу».

При введенні чутливих даних (паролі від облікових записів, банківські дані, персональна інформація тощо) слід прикривати другою рукою клавіші, що натискаються.

Політика чистого столу – не залишати на столі носіїв з чутливими даними.

Не використовувати невідомі або чужі комп'ютерні пристрої або носії даних.