УДК 316.422

Д.О. Козак

СОЦІАЛЬНИЙ ФАКТОР У ПРОБЛЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

Описано можливі причини розголошення конфіденційної інформації, наслідки впливу соціальної інженерії на роботу персоналу підприємства та методи захисту від атак соціального інженера.

Ключові слова: *інформаційна безпека, конфіденційна інформація, захист інформації, соціальна інженерія, захист персоналу підприємства*

Abstract

Possible reasons for the disclosure of confidential information, the consequences of the impact of social engineering on the work of enterprise personnel and methods of protection against attacks by a social engineer are described.

Keywords: *information security, confidential information, information protection, social engineering, enterprise personnel protection*

Вступ

Сьогодні людський фактор в забезпеченні інформаційної безпеки відіграє набагато важливішу роль, ніж двадцять років тому, коли користувачами Інтернету були лише фахівці з комп'ютерних систем. Інформаційні процеси проникли в усі сфери діяльності людини, адже практично кожній людині доводиться виконувати різні завдання, взаємодіючи з численними елементами IT-інфраструктури. Залежність кожного індивіда від інформаційних систем і мереж постійно зростає.

Користувач комп'ютерної системи є найслабшим місцем в системі інформаційної безпеки, тому саме він піддається впливу соціальної інженерії.

Технології безпеки, яким люди звикли довіряти, – міжмережеві екрани, пристрої ідентифікації, засоби шифрування, системи виявлення мережевих атак та інші – малоефективні в протистоянні з зловмисниками, що використовують методи соціальної інженерії.

Проблема соціальної інженерії є дуже актуальною. Людина, під дією соціальної інженерії, здатна здійснювати нелогічні дії і несвідомо нанести шкоду не лише собі, а й оточуючим. Навіть найсучасніші комп'ютери та новітні технології не можуть захистити людей від впливу на їх свідомість і дій спеціалістів з соціальної інженерії.

Соціальна складова забезпечення інформаційної безпеки

Термін «соціальна інженерія» використовується для опису цілої низки низькотехнологічних підходів, розроблених шахраями для того, щоб ввести людину в оману, аби змусити її вчинити певні дії, необхідні зловмисникам. Шахраї можуть змусити потенційну жертву повідомити особисті дані, конфіденційну інформацію, яка представляє велику цінність або взяти участь у діях, які можуть зробити комп'ютер вразливим до атак [1].

Психологічною передумовою застосування методів соціальної інженерії є така особливість людської психіки, як когнітивні упередження. Тому надійність комп'ютерної системи є не вищою, ніж надійність її оператора.

Соціальна інженерія є багатогранним і складним способом отримання конфіденційної інформації від користувачів із застосуванням методів переконання і технологічних засобів. Такий метод управління діями людей, заснований на використанні психологічних слабкостей людей та можливості маніпулювання ними. Будь-яка людина в сучасному світі є вразливою до такого виду небезпеки, а отже, повинна постійно чітко знати з ким вона взаємодіє як в режимі онлайн, так і віч-на-віч.

Для досягнення поставленої мети зловмисник може використовувати різні тактики. Зокрема: видавати себе за іншу особу; відвертати увагу потенційної жертви; нагнітавати психологічну напругу, здійснювати моральний тиск на жертву тощо [2].

Зловмисник, послуговуючись відомостями про симпатії жертви, її страхи, реактивність і довіру вводить у дію й наступні психологічні важелі:

- входження в певну роль;
- примушення жертви відігравати певну роль;
- збивання жертви з думки;
- досягнення із жертвою моменту згоди;
- формування в жертви бажання допомогти.

Жертвами соціальних інженерів можуть бути не тільки працівники IT-компанії, а і будь-якої фірми, де застосовуються елементи IT-інфраструктури.

У сучасних організаціях потенційними жертвами соціальних інженерів можуть бути працівники з різними правами доступу до конфіденційної інформації: адміністратори, начальники підрозділів, користувачі та, навіть, знайомі будь-кого зі згаданих категорій осіб.

В таблиці 1 показано ступінь (із трьох можливих: 1 — низький; 2 — середній; 3 — високий) ймовірного отримання доступу соціального інженера з рівнем підготовки новачок, аматор і професіонал до різних засобів застосування, на різних рівнях взаємовідносин та до різних категорій персоналу організації. Врахуємо, що дії такої особи ґрунтуються передусім на особливостях аргументації (так званих когнітивних упередженнях), згідно з якими людина ухвалює певне рішення.

Таблиця 1 – Імовірність отримання несанкціонованого доступу різних рівнів до інформації з обмеженим доступом через персонал наявних категорій [3].

Клас атак	Підготовленість зловмисника		
	Новачок	Аматор	Професіонал
Засоби застосування			
Телефон	3	3	3
Електронна пошта	2	3	3
Звичайна пошта	1	3	3
Розмова в інтернеті	3	3	3
Особиста зустріч	1	2	3
Рівень спілкування (відносини)			
Офіційний	2	3	3
Товариський	3	3	3
Дружній	1	2	3
Ступінь доступу			
Адміністратор	1	2	3
Начальник	1	2	3
Користувач	3	3	3
Знайомий	2	3	3

Незважаючи на те, що співробітники підприємства (організації, установи) можуть стати джерелом загрози, його керівництво часто відмовляється це визнавати. Таку поведінку можна пояснити довірою керівництва до співробітників, що спирається на особисті симпатії; упевненістю керівництва в порядності і відданості співробітників; переконанні керівництва в силі впливу корпоративної етики.

Причинами розголошення інформації з обмеженим доступом можуть бути:

- прагнення людини до самоствердження, популярності й слави;
- прагнення співробітників до фінансової винагороди;
- недієва робота служби безпеки компанії;
- невідповідність адміністративних заходів із покарання за розголошення інформації з обмеженим доступом;
- випадкове розголошення інформації з обмеженим доступом у бесідах з іншими особами чи спілкуванні із засобами масової інформації;
- безконтрольне використання інформаційних і копіювальних засобів на фірмі, установлення недозволеного програмного забезпечення;
- психологічні конфлікти між співробітниками підприємства, а також між співробітниками й керівництвом.

Збереження інформації з обмеженим доступом на 80% залежить від правильного підбору, розміщення та виховання кадрів, персоналу, відданого підприємству. Єдино правильний шлях, який дозволить запобігти розголошенню конфіденційної інформації — це ретельний підбір персоналу з неодмінним обмеженням його доступу до такої інформації.

Для захисту будь-якої компанії, в тому числі і IT, від шахрайства необхідно навчати персонал розпізнавати соціальну інженерію і правильно на неї реагувати, заборонити співробітникам обмінюватися паролями або мати один загальний, забезпечити захист клієнтських баз та іншої конфіденційної інформації, застосовувати особливу процедуру підтвердження для осіб, які звертаються до доступу до будь-яких даних.

Для запобігання атак з використанням методів соціальної інженерії необхідно розробити чіткі інструкції для всіх категорій співробітників, в яких будуть покроково розписані їхні дії в разі виявлення атак соціальної інженерії, і цю інформацію розмістити в доступному місці.

В організації повинні існувати правила доступу до конфіденційної інформації. Навіть відомості, які в більшості випадків не вважаються особливо важливими, можуть бути корисними соціальному інженеру, що збирає крихти інформації, цілком придатної в професійних руках для створення атмосфери довіри і симпатії.

Програма компанії з протидії атакам соціальної інженерії одним із завдань повинна ставити зміну норм ввічливості, а саме — розробку ввічливого відхилення запиту про надання важливої інформації, поки не буде встановлено особу, яка подавала запит на її право на доступ до цієї інформації.

В організації повинен бути розроблений процес перевірки особистості і авторизації людей, які звертаються за інформацією або вимагають якихось дій від співробітників компанії.

Співробітники ніколи не повинні отримувати від керівництва вказівок обійти протокол безпеки, і жоден співробітник не повинен бути покараний за те, що буде дотримуватися протоколу безпеки, навіть якщо отримав від керівництва вказівку його порушити.

Важливим є навчання персоналу навичкам протидії методам соціальної інженерії, розробка тренінгів по становленню пильності персоналу і періодична перевірка знань і навичок співробітників шляхом проведення спеціальних перевірок.

Аби уникнути розголосу інформації з обмеженим доступом, керівництво має дбати про підвищення продуктивності праці та прибутків, помітне поліпшення життєвого рівня співробітників, створення позитивного психологічного клімату в колективі, формування у співробітників почуття причетності до спільної справи, а також про мінімізацію плинності кадрів і негативних проявів людського фактора в системі забезпечення комплексної безпеки.

Висновок

Отже, продуманий, комплексний захист працівників та керівництва від атак соціальних інженерів є необхідним для нормального функціонування будь-якого підприємства. Вирішення даної проблеми є актуальним та дуже важливим, адже мінімальний витік інформації з компанії може призвести до втрати цінних працівників та невиправних матеріальних втрат.

На підприємстві повинна бути чітко побудована ієрархія доступу до інформації з обмеженим доступом.

Керівники будь-якої фірми мають проводити постійну, потужну роботу з персоналом, навчати співробітників застосуванню політики безпеки і технікам протистояння соціальним інженерам. Особливу увагу потрібно приділяти новопризначеним працівникам та співробітникам, схильним до імпульсивних вчинків. Тільки при такій злагодженій роботі співробітників та керівництва система безпеки на підприємстві буде приносити бажані результати.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке «соціальна інженерія»? *Скайп:* веб-сайт. URL: https://support.skype.com/uk/faq/FA10921/shcho-take-sotsial-na-inzheneriya (дата звернення 21.02.2021).

2. Соціальна інженерія. *Вікіпедія:* веб-сайт. URL: https://uk.wikipedia.org/wiki/social_engineering (дата звернення: 21.02.2021).

3. Бурячок В.Л., Толубко В.Б., Хорошко В.О. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Львів: «Магнолія 2006», 2018. 320 с.

Козак Діана Олегівна – студентка групи УБ-17б, факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: fm.ub17b.kozak@gmail.com

Kozak Diana O. – student of UB-17b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: fm.ub17b.kozak@gmail.com