УДК 007:658

Легенченко К.О., студентка групи 125м-16-1
Науковий керівник: Тимофєєв Д.С., ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

УПРАВЛІННЯ ОБІЗНАНІСТЮ ПЕРСОНАЛУ В ПИТАННЯХ ПРОТИДІЇ МЕТОДАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Важливим фактором захисту інформації на підприємствах є акцент на протидії методам соціальної інженерії. Будь-яка інформація, незалежно від її формату та стану - обробляється вона процесором, передається по каналах зв'язку, зберігається на диску - повинна входити в межі контролю системи забезпечення ІБ. Але технічні засоби, крім основного функціоналу, мають інтерфейси взаємодії з людиною, тому важливим елементом захисту інформації є сам співробітник компанії. Якщо по відношенню до технічних засобів завжди можна описати можливі ситуації, визначити і оцінити ризики, знайти способи захиститися (обмежити доступ, зашифрувати і т.п.), то в разі дій людини виникає проблема.

Виходячи з цього внутрішні загрози можуть утворюватися внаслідок:

- непрофесійних дій працівників;
- низького стану виховної та профілактичної роботи в організації;
- недосконалої системи заробітної плати та стимулювання праці персоналу;
- порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи в організації;
- психологічних та комунікаційних особливостей працівників;
- відсутності нормативної бази організації, яка б установлювала режими їх діяльності та правила поведінки персоналу. [1]

До сих пір не існує чіткої, всеосяжної математичної моделі, яка описує поведінку людей в різних ситуаціях, реакцію на той чи інший вплив або сформовані умови, можливі помилки. Природно, що цей фактор відіграє на руку зловмисникам.

В атаках, що використовують методи соціальної інженерії, можна виділити 3 основних етапи: збір, профілювання і реалізація.

1. Збір даних про мету атаки є найбільш важливою стадією. Роботи полягають у визначенні характеристик об'єктів атаки, в тому числі шляхом зовнішнього впливу. Джерелом даних можуть бути соціальні мережі, публічно доступна інформація і ін. Також ефективними є спілкування з членами сім'ї, друзями і колегами, спостереження за діяльністю мети і навіть взаємодія з нею.

2. На етапі профілювання виконується аналіз зібраної інформації для побудови моделі атаки. Виділяються характеристики, що властиві цілі, а також її слабкості, на підставі чого вибираються канали взаємодії (пошта, телефонні дзвінки, особисте спілкування і т.п.), методи реалізації (вербування, неформальне спілкування, тиск і т.п.) і можливі вектори атаки, які можуть бути ефективними проти конкретної мети.

3. На етапі виконання атаки реалізується її модель, вироблена на стадії профілювання. Тут вступають в повну силу психологія, НЛП і технічні засоби. У разі вдалої реалізації першої хвилі атаки можна повернутися до етапу збору інформації з новими вхідними даними і ітеративно повторювати виконання етапів до тих пір, поки продовжує виявлятися нова інформація, або поки атака не досягне бажаної глибини. [2]

Активне використання інтернету, крім плюсів, має ряд значних мінусів. Це і додаткові канали комунікації з жертвою, і залишені жертвою «сліди», вивчивши які, можна скласти портрет потенційної мети атаки. Інтернет дає зловмисникам можливість автоматизувати свою роботу, що значно скорочує «трудовитрати» на виконання атаки.

У той же час багато компаній і бояться, і не розуміють, навіщо їм потрібна оцінка свого персоналу, заснована на застосуванні методів соціальної інженерії. Бояться зазвичай внаслідок того, що такий процес не регламентований законодавством або міжнародними стандартами. Він більшою мірою експертний, часто його результативність залежить від навичок конкретного виконавця. [3]

Крім застосування технічних заходів захисту інформації (розмежування доступу, мінімізації повноважень, моніторингу подій і трафіку і т.п.), які протидіють відомим шаблонами атак, основним заходом захисту від використання прийомів соціальної інженерії є метод «Безпека через навчання». Навчання має бути регулярним, простим і зрозумілим. Часто в організаціях до процесу навчання вимогам і практикам ІБ підходять формально. Тому виникає ситуація, коли працівники компаній мають низький рівень поінформованості та грамотності з питань інформаційної безпеки. Це тягне за собою їх халатне, неуважне ставлення до вхідних інформаційних потоків. Крім навчання, також варто підвищувати пильність співробітників шляхом їх періодичного тестування. [4]

На завершення необхідно відзначити, що гуманітарну проблему не можна вирішити виключно технічними методами. Тільки комплексний підхід може захистити від атак із застосуванням методів соціальної інженерії. Шляхом збору, обробки, порівняння та аналізу досліджень в сфері протидії атакам з використанням методів соціальної інженерії, необхідно описати і організувати систему заходів і методів підвищення кваліфікації персоналу в сфері протидії атакам з використанням методів соціальної інженерії.

Напрямок досліджень:

- вивчити раніше проведені дослідження в області протидії атакам з використанням методів соціальної інженерії;
- розробити теоретичну базу, де слід викласти основні поняття в сфері протидії атакам з використанням методів соціальної інженерії;
- класифікувати типи і види атак з використанням методів соціальної інженерії (з прикладами);
- проаналізувати існуючі методи протидії атакам даного типу;
- запропонувати унікальні методи протидії атакам з використанням соціальної інженерії;
- проаналізувати ефективність запропонованих методів протидії;
- розробити ряд методик для підвищення кваліфікації персоналу протидії методам соціальної інженерії;
- розробити спеціальне програмне забезпечення, що дозволяє дохідливо і ефективно піднести дані методики для персоналу підприємств.

ПЕРЕЛІК ПОСИЛАНЬ

1. Будник М.М. ,Тимофєєв Д.С. Внутрішні загрози інформаційної безпеки та заходи по їх мінімізації (Електрон. ресурс) / Спосіб доступу: URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1666/7.pdf?sequence=1

2. Резник Ю.М. Соціальна інженерія: предметна область і межі застосування // Соціологічні дослідження, 1994, № 2.

3. Соціальна інженерія // Сучасна західна соціологія: Словник. М., 2015.

4. Романенко Е.А., Тимофеев Д.С. Методы обучения персонала по вопросам информационной безопасности (Електрон. ресурс) / Спосіб доступу: URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1667/14.pdf