УДК 338.2

В. М. Нам'ясенко,
аспірант, Хмельницький національний університет, м. Хмельницький

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ОДНА ІЗ ЗАГРОЗ ЕКОНОМІЧНІЙ БЕЗПЕЦІ, ЩО СПРИЧИНЯЄ НЕГАТИВНИЙ ВПЛИВ НА ЕФЕКТИВНІСТЬ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

V. Namyasenko,
Postgraduate, Khmelnitsky National University, Khmelnitsky

SOCIAL ENGINEERING AS ONE OF THE THREATS TO ECONOMIC SECURITY THAT CAUSING A NEGATIVE IMPACT ON THE EFFICIENCY OF THE ENTERPRISE

Одним із найактуальніших діяльності в сучасних умовах глобальної економіки є постійне забезпечення високої ефективності діяльності та розвитку, а також збереження отриманих надбань. За збереження цих надбань відповідає система економічної безпеки системи. В сучасних умовах однією із головних загроз цій безпеці є напади із використанням методів соціальної інженерії.

У статті розглянуто основні принципи та ознаки і методи соціальної інженерії; пояснено чому немає ефективних бар'єрів захисту та запропоновано превентивні інструменти захисту.

Abstract — The economic security of the enterprise is one of the fundamentals of its economic efficiency. This issue is the particularly relevant in the context of the globalization and the unfair competition. The social engineering is one of the most dangerous methods of this type of competition.

We have consolidated the main causes of attack danger of these methods: the lack of consistency and the overall action plan; almost complete absence of repetition action. We also came to the conclusion that the effective algorithms for build protective barriers for protect against this type of threat virtually are absent. The reason for this is that the target is the least protected element of any modern system — people — workers. The use of the imperfection of human nature, namely the use of emotions and experiences is at the core of the work of the social engineers. The main instruments of the protection and combat such attacks are the warning employees about this threat and its main features, and careful selection of staff.

So, the social engineering is one of the major threats to economic security and efficiency of modern enterprises. Develop methods to combat this danger must become to the one level with other dangers, for example such as the fight against the hackers.

Ключові слова: економічна безпека, соціальна інженерія, ефективність діяльності, безпека, методи захисту.
Key words: economic security, social engineering, the effectiveness of, security, protection methods.

ПОСТАНОВКА ПРОБЛЕМИ

Соціальна інженерія є одним із основних напрямів дослідження філософії як наука, що вивчає вплив різних факторів на побудову соціальної системи. Водночас з тим у сучасному світі соціальна інженерія набула ще одного значення — маніпулювання людьми для досягнення певних цілей та отримання необхідної інформації. Саме у даному аспекті поняття стає цікавим і з погляду економіки, а саме: економічної безпеки.

Важливість даного питання полягає у тому, що велика кількість підприємств не надає адекватної уваги щодо вирішення даного питання, що робить їх практично незахищеними від даного типу негативного впливу. Економічна безпека є однією зі складових, що формує умови для ефективної економічної діяльності підприємств будь-якого типу.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблемам соціальної інженерії як галузі філософії (зокрема соціології) приділено досить багато уваги. Дослідження ж даного питання як проблеми безпеки значно нижче; в розрізі економіки — дослідження практично відсутні.

Однією із основних ненаукових праць, що має хоч якийсь зв'язок із економічною безпекою є "Мистецтво обману" Кевіна Д. Митника та Вільяма Л. Саймона. В даній книзі приводяться приклади дій соціальних інженерів у реальних умовах, а також те як нібито незначна інформація може призвести до критичних наслідків для сторони, що зазнала впливу.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Основною ціллю статті є явище соціальної інженерії та маніпулюванням людьми з погляду економічної безпеки; її негативного впливу на економічну ефективність. Виділити основні інструменти, що зможуть підвищити рівень захисту підприємств від впливу "зовнішніх нападників", що застосовують інструменти даного типу. Основною причиною даної проблеми відсутності системності та логіки при вчиненні даних дій.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

У сьогоднішніх умовах глобалізації економіки досить часто використовуються методи нечесної конкуренції. Дані дії спрямовані на те, щоб отримати додаткові конкурентні переваги в певному секторі шляхом здійснення дій, спрямованих на дискримінацію конкурента або ж отримання даних, що стосуються "ексклюзивних" переваг. Одним із таких шляхів є соціальна інженерія.

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" (як правило, соціальні інженери діють експромтом), харизма та привабливість, що допомагають заслужити довіру та прихильність жертви, а також "розуміння людської сутності". Саме таке "розуміння", а не навички психолога відіграють важливішу роль. Це пов'язано з тим, що психологу потрібно більше часу, щоб знайти підхід до людини, а в соціальних інженерів, як правило, такого часу немає.

Соціальна інженерія в розрізі економічної безпеки не бере до уваги багаторівневі технічні та технологічні системи захисту — вона використовує найменш захищену частину будь-якого підприємства — людську складову. Саме людський фактор є тією, складовою, що нівелює усі багаторівневі системи захисту. Від даного типу впливу повністю не захищенні жодна із систем де є участь людини: від маленького підприємства де немає ніякої автоматизації до міжнародного гіганта, де більшістю процесів керують автоматизовані системи; від підприємств, що повністю побудовані на людській праці до надсучасних замкнених систем, де все автоматизовано і для контролю потрібен лише один оператор центральної системи. Теоретично нівелювати даний вплив можливо лише у майбутньому, коли буде побудовано повністю автоматизовану та самодостатню систему, але все ж залишаться люди, які її розроблятимуть та знатимуть основні принципи та схеми дій.

Небезпека даного інструменту також полягає у високій ймовірності того, що виникне досить тривалий часовий лаг між здійсненням нападу та моментом, коли з'явиться розуміння того, що було здійснено такі дії; час до здійснення реальних дій щодо зменшення негативних наслідків буде ще більшим. Водночас це є також однією із особливостей даного інструменту — напад теоретично може бути взагалі невиявленим. Саме такий довгий часовий лаг, або взагалі відсутність інформації щодо таких дій може спричинити більш катастрофічні наслідки, ніж прямий доступ до інформаційної системи чи промислові диверсії. Наслідком цього може стати постійна втрата ефекту від інновацій, новітніх розробок, неефективність маркетингових компаній та інші, що в кінцевому результаті буде призводити до постійної втрати клієнтів.

Основним фактором, що робить даний інструмент водночас простим та ефективним є відсутність якоїсь системності у діях злочинців. Так, наприклад, при хакерських атаках злочинцю потрібно отримати доступ до одного із цифрових пристроїв, що підключений до однієї мережі із кінцевим пристроєм-ціллю, який містить потрібну інформацію, або є "ключем" до здійснення намірів. Тому у служби безпеки та IT-відділу є "стандартний" перелік можливих шляхів нападу: мережа Internet, порти для підключення зовнішніх пристроїв на наявному обладнанні та інші більш-менш прогнозовані джерела безпеки; нападник діє за схемою, що у спрощеному вигляді представляє собою наступну послідовність: отримати доступ до мережі — обійти перепони — отримати потрібну інформацію/ ввести потрібні зміни в роботу системи — вийти з системи. В такому випадку можна завчасно розставити потрібні бар'єри та проводити певні профілактичні дії. У випадку ж соціальною інженерією різновидів нападу може бути безкінечна кількість: від простого дзвінка як потенційного клієнта до "павутини" із багатьма зв'язками; ціллю ж в даному випадку є людина — фактично ціль одна, але вона знову ж розростається до кількості усіх працюючих на підприємстві. На практиці це все призводить до того, що фактично бар'єри розставляти фактично неможливо, оскільки немає параметрів для такого бар'єру. З погляду економічної безпеки це є досить складно та небезпечно, тоді як з погляну "нападника" це гра, яка за п'ять хвилин простого дзвінка може принести більший результат, ніж місяці детально спланованої комп'ютерної атаками.

Умовно все ж можна виділити деякі шляхи та форми нападу:

1. За допомогою комп'ютерних мереж (фішинг — суть методу полягає у створенні підробленої сторінки сайту банку чи іншої установи з метою "витягнути" у користувача пари логін/пароль від його акаунта. Це дасть можливість зловмисникам, наприклад, перевести всі гроші з банківського рахунку жертви на власні. Частіше за все, фішинг розрахований на неуважних користувачів, які не звертають уваги на незвичайні назви сайтів, частіше за все з помилками, незвичайний зовнішній вигляд знайомих ресурсів та нехтують основним правилами сучасної кібербезпеки. "Гарячі листи" — суть методу дещо інша ніж класичний фішинг. Фактично, зловмисники не чекають поки користувачі самі потраплять на підроблений сайт, а самі спонукають їх це зробити. Це здійснюється за допомогою фальшивих повідомлень від банків чи інших установ. "Емоційна буря" — це "гра" на природній цікавості та емоційності користувачів. Вони мають вигляд коротких повідомлень від друзів на пошту, у соцмережах, месенджерах, зміст яких має спонукати перейти за посиланням у тілі повідомлення. "ОГО! Подивись, яка прикольна річ. Я був у шоці!" — класичний приклад такого методу соціальної інженерії) [4].

2. За допомогою телефонів — суть даного методу полягає у тому, що за допомогою звичайного телефонного дзвінка та правильно побудованого діалогу зловмисник може отримати всю необхідну інформацію. В даному випадку "ключове" запитання "заховане" в ряді простих загальних питань, що знижує увагу жертви та будує "атмосферу" довіри.

Це два основних шляхи нападу. Рідше використовується особистий контакт. Дані способи дають змогу створити "умови" сумбуру, що не дає жертві як слід зважити всі "за" і "проти".

Тепер перейдемо до можливих варіантів "захисту" від такого нападу.

Зокрема "Агентство активного аудиту" пропонує послугу "Тест на проникнення методами соціальної інженерії". Загальна схема тесту наведена на рисунку 1.

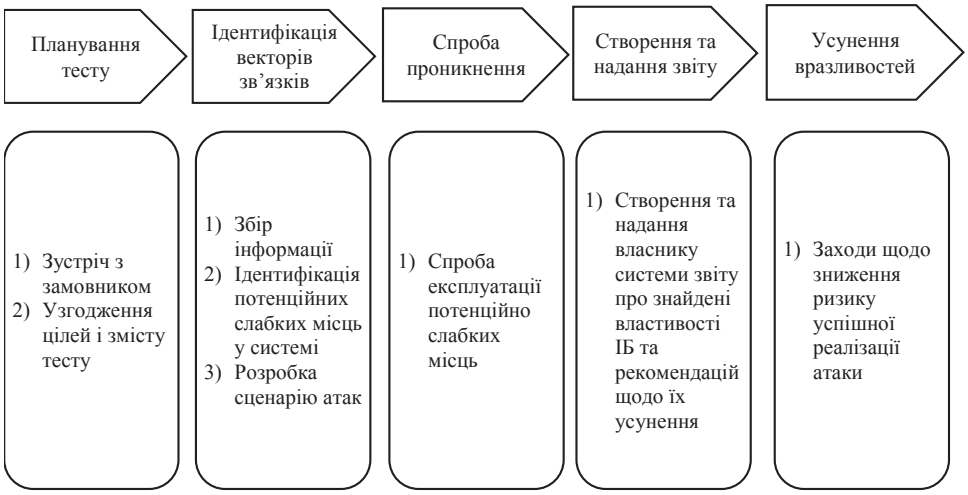

Рис. 1. Тест на проникнення методом соціальної інженерії

Джерело: [5].

Даний тест дає змогу перевірити вразливість системи до впливу соціальних інженерів. Але даний захід є лише індикатором і неправомірно говорити про усунення небезпеки нападу соціальних інженерів по його результатах. Фактично ми не згодні із ствердженням даного агентства про те, що останній етап — це усунення вразливостей, насправді ж можна говорити лише про певні превентивні дії. Також говорити про те, що один тест дасть змогу оцінити усі небезпеки також неправомірно. Це пов'язано з тим, що практично неможливо відтворити саме той сценарій, який буде використано злочинцями в реальних умовах. Загалом даний тест є лише частковим індикатором на можливість проникнення одним із багатьох способів.

Як же ж тоді убезпечитись від нападу зловмисників, що володіють навичками соціальної інженерії? Загалом ми виділили та пропонуємо наступні підходи:

1) диференціація важливої інформації між декількома співробітниками, як в її розголошенні, так і в доступі до агрегованої бази даних;

2) лекції для працівників на дану тематику: інформація про даний вид небезпеки, якою володіють працівники дає змогу значно збільшити шанси на те, що напад може не вдатись;

3) побудова системи "раціональної довіри" на підприємстві, що передбачає побудову дружньої атмосфери на підприємстві (один із базисів — відсутність страху перед керівництвом), але знову ж із диференціацією інформації між працівниками та тренінгами, що передбачають "пояснення" якою інформацією та з ким можна ділитись;

4) ретельний відбір кандидатів на заміщення вакантних місць;

5) максимальна автоматизація важливих процесів.

Фактично — це комплекс превентивних заходів, ефективність яких є наперед невизначеною. Це пов'язано із тим, що людський фактор фактично немає визначених параметрів стійкості: причиною ефективної атаки може стати навіть сам керівник, який активно бореться з даним явищем.

ВИСНОВКИ

Розвиток глобального ринку все більше посилює конкуренцію між виробниками, що часто стає причиною використання методів нечесної конкуренції.

Одним із таких методів являє собою "напад" із використанням інструменті соціальної інженерії. Цей метод не є новим, але такий спосіб його використання набув такого вигляду лише в останні десятиліття.

Небезпека нападів соціальних інженерів полягає у відсутності будь-якої системності та загального сценарію їх дій. Єдине, що точно визначено — це ціль — людина. Основою даного методу є використання людського фактора, як найбільш незахищеного елемента будь-якої відкритої системи, якими на сьогодні є усі підприємства. Теоретично абсолютний захист системи можливий при абсолютному виключенні людини із цієї системи та побудова несистемного алгоритму даної системи.

Сьогодні ж захист підприємств можливий саме завдяки превентивним методам — донесення інформації до працівників про можливість такого нападу, тоді як "абсолютних" бар'єрів захисту вибудувати практично неможливо.

Література:

1. Кевін Д. Митник. Мистецтво обману [Текст] / Кеввін Д. Митник, Вільям Л. Саймон. — М.: Видавництво АйТі, 2004. — 360 с.

2. Соціальна інженерія (безпека) [Електронний ресурс]/ Вікіпедія: Вільна енциклопедія. — Режим доступу: https://uk.wikipedia.org/wiki/Соціальна _інженерія_(безпека)

3. Соціальна інженерія [Електронний ресурс]/ Режим доступу: http://wiki.tntu.edu.ua/Соціальна_інженерія

4. Соціальна інженерія або маніпуляції свідомістю [Електронний ресурс]/ Офіційний веб-сайт антивірусу Zillyu!. — Режим доступу: http://zillya.ua/sotsialna-inzheneriya-abo-manipulyatsi-svidomistyu

5. Тест на проникнення методами соціальної інженерії [Електронний ресурс]/ Офіційний веб-сайт компанії "Агентство Активного Аудиту". — Режим доступу: http://auditagency.com.ua/?r=social_engineering&lang=ua

References:

1. Kevin, D. Mytnyk, and Viliam, L. Saimon (2004), Mystetstvo obmanu [The art of deception], IT, Moscow, Russia.

2. Wikipedia (2013), "Social engineering (security)", available at: https://uk.wikipedia.org/wiki/Соціальна_інженерія_(безпека) (Accessed 16 January 2016).

3. The site of Ternopil Ivan Puluj National Technical University Wiki (2011), "Social engineering", available at: http://wiki.tntu.edu.ua/Соціальна_інженерія (Accessed 16 January 2016).

4. The official site of Zillyau! Antivirus (2015), "Social engineering or manipulation of consciousness", available at: http://zillya.ua/sotsialna-inzheneriya-abo-manipulyatsi-svidomistyu (Accessed 16 January 2016).

5. The official site of the company "Active Audit Agency", "Penetration test using social engineering methods (social engineering)", available at: http://auditagency.com.ua/?r=social_engineering&lang=ua (Accessed 16 January 2016).

Стаття надійшла до редакції 20.02.2016 р.