Не виключено, що останні події, пов'язані з витоком персональних даних співробітників Ощадбанку , мали місце завдяки цьому інструменту. Він відмінно підходить для такого типу атаки, і з його допомогою можна також проводити масову розсилку клієнтам Ощадбанку від імені співробітників, чия база вже знаходиться в руках зловмисників. В цілому, Social-Engineer Toolkit - потужний інструмент, яким поки немає рівних. У більш ранніх версіях була функція відправки SMS від імені будь-якого абонента і будь-якої організації, але пізніше розробники відключили модуль. І якби він діяв в даний час, то проникнення в систему було б набагато легше, оскільки SMS-підтвердження як додатковий захист зараз поширене

Метод соціальної інженерії - це тонке мистецтво. Оволодівши їм, можна бути впевненим, що бажаний результат буде отримано в 90-95% - все залежить від кмітливості зловмисника і від підходу до певної жертві. Як правило, на цю вудку трапляються неуважні люди, які не так вимогливі до власної безпеки і рідко звертають увагу на незначні на перший погляд деталі (посилання в браузерному рядку, текст та інше). Слід зазначити, що досвідчені користувачі теж потрапляють на це, хоча і рідше.

Як же уникнути подібних неприємностей? Якщо ви використовуєте соціальні мережі для спілкування, то обов'язково крім введення логіну і паролю використовуйте двофакторну аутентифікацію, тим самим ви створите складність зловмисникові для проникнення в ваш профіль.

Уважно дивіться на посилання в браузерному рядку - як правило, він дуже схожий з оригіналом, різниця в парі букв або цифр. Так що неуважний користувач може і не помітити обману. Завжди краще перевірити ще раз, якщо є можливість: як правило, офіційні сайти справжніх організацій знаходяться на самому першому рядку пошукових систем. Якщо вам прийшла підозріла посилання або прохання від одного, подруги, колеги, то не полінуйтеся зв'язатися з адресатом іншим способом і уточнити, чи він її надіслав. Будьте пильні, бережіть свої дані.

Мирошниченко В.О. - доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

ДЕЯКІ АСПЕКТИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ У ДЕРЖАВАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

Без сумніву, можна стверджувати, що інформаційно-комунікаційні технології мають фундаментальний вплив на суспільство. У цьому сенсі можливості "інформаційного суспільства" є важливими для економічного зростання, освіти, конкуренції, комунікації та інформаційного обміну, можливостей мобільності та працевлаштування. Однак суспільство постійно

стикається з загрозою комп'ютерної злочинності і очевидним є те, що загроза повинна розглядатися в рамках глобальної проблеми, яка ставиться перед кримінальним правосуддям усіх країн шляхом розробки та широкого використання нових підходів для вирішення цієї проблеми. Усвідомлюючи цю ситуацію, Рада Європи представила для прийняття в листопаді 2001 року Конвенцію про кіберзлочинність, також відому як "Договір про кіберзлочинність" [1]. Цей договір відкритий для ратифікації світовим загалом, і ратифікований також Сполученими Штатами та ще декількома десятками країн. Договір містить положення, що стосуються як кримінального права, так і кримінально-процесуального законодавства та кримінального розслідування, а також взаємної допомоги при розслідуванні комп'ютерних злочинів. За баченням розробників Договору, вони поділяються на чотири основні категорії:

1) правопорушення проти конфіденційності та цілісності, незаконний доступ, незаконне перехоплення, перешкоджання передачі даних, системне втручання та неправильне використання пристроїв;

2) комп'ютерні правопорушення, такі як підробка та комп'ютерне шахрайство;

3) правопорушення, повязані із змістом контента, зокрема виробництво, розповсюдження та зберігання дитячої порнографії, поширення расистських та ксенофобських ідей;

4) правопорушення, повязані з порушенням авторських і суміжних прав.

Метою Договору є спонукання країн, що його ратифікують, до адаптації свого національного кримінально-процесуального законодавства до технологічних змін, у цьому сенсі Договір містить конкретні процедурні правила. Крім того, в положеннях Договору викладено ряд загальних принципів, що стосуються міжнародного співробітництва, екстрадиції, взаємодопомоги та обміну інформацією. З метою стимулювання міжнародного співробітництва передбачено низку правил щодо видачі підозрюваних за певних умов, а також встановлення інших форм співробітництва у сфері кримінального розслідування та кримінального переслідування за допомогою мережного контакту з доступністю 24/7.

Договір про кіберзлочинність став першим але вже не єдиним важливим міжнародним обов'язковим юридичним інструментом для вирішення питання про кіберзлочинність. 24 лютого 2005 року Рада Європейського Союзу прийняла Рамкове рішення 2005/222 / про кібератаки на інформаційні системи (далі - Рамкове рішення) з метою посилення співпраці між судовими та іншими компетентними органами, у тому числі поліції та інших спеціалізованих правоохоронних органів шляхом наближення національних норм кримінального законодавства у сфері кібератак на інформаційні системи [2]. Рамкове рішення складається з визначень "незаконного доступу", "втручання в дані" та "системного втручання" як кримінального правопорушення. Мета Рамкового рішення полягає у вирішенні значних прогалин та розбіжностей у національних

законодавчих актах, які можуть заважати боротьбі з організованою злочинністю та тероризмом, а також ускладнюють поліцейську та судову співпрацю у сфері боротьби з кібератаками на інформаційні системи.

Що стосується незаконного доступу до інформаційних систем, то Рамкове рішення встановлює, що держави-члени можуть вирішити, що це правопорушення буде здійснюватися лише тоді, коли доступ буде отримано "шляхом порушення заходів безпеки". Крім незаконного доступу, зазначені документи розглядають проблеми спаму, шпигунського програмного забезпечення, загального доступу та прав користувачів.

Напевно, нереально очікувати, що коли-небудь буде консенсус стосовно всіх заходів, необхідних для боротьби з кіберзлочинністю, і ще навіть не реалістичніше чекати, що кіберпростір буде вільним від кіберзлочинності. Хороша новина, однак, полягає в значному прогресі у пошуку загальних шляхів вирішення цього питання, і вони базуються на широкому і всебічному визначенні кіберзлочину. Безумовно, всі проблеми, пов'язані з кіберзлочинністю, ще не були розглянуті або навіть виявлені, але загальне визначення поняття кіберзлочинність та досягнення суттєвої адаптації законодавства є, як мінімум, двома важливими кроками у боротьбі проти цієї все більш важливої нової форми злочинів.

Використані джерела

1. CONVENTION ON CYBERCRIME, European Treaty Series - No. 185, Budapest, 23.XI.2001 . [Електрон. ресурс] / Режим доступу: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

2. COUNCIL FRAMEWORK DECISION 2005/222/JHA of 24 February 2005. [Електрон. ресурс] /Режим доступу: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32005F0222 On attacks against information systems, Official Journal of the European Union, L 69/67

Міхальский Я.В. - аспірант кафедри кібербезпеки та інформаційного забезпечення;
Форос Г.В. - професор кафедри кібербезпеки та інформаційного забезпечення, кандидат юридичних наук, доцент (Одеський національний університет внутрішніх справ)

СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОЇ ВІЙНИ В УКРАЇНІ

У сучасних умовах проблеми інформаційних воєн та їх протидії актуалізувалися у зв'язку з бурхливим розвитком інформаційних процесів та технологій, що дозволяють експлуатувати інформаційний простір країни, та маніпулювати засобами масової інформації та їх аудиторією.

Виникають все більше і більше інформаційних загроз інтересів людини і громадянина, суспільства та держави, національних інтересів України. Тому