цьому підкреслюється, що 13 осіб уже заарештовані. Як вказується, це громадяни США, Франції, Італії, Косово, Сербії, Австралії, Великобританії. У Мін'юсті наголошують, що від дій шахраїв постраждали як США, так і інші країни.

У прес-релізі зазначено, що мережа кіберзлочинів, яка функціонує як онлайновий дискусійний форум під назвою Infraud, реалізувала складну схему, яка сприяла купівлі та продажу номерів соціального захисту, днів народження та паролів, викрадених з усього світу. Згідно з обвинувальним висновком, група працювала під гаслом «В шахрайство ми віримо» і була створена в 2010 році Святославом Бондаренко, 34-річним українцем.

В обвинувальному висновку також говориться, що від дій шахраїв постраждали мільйони людей. Так, були вкрадені майже 800 тис. облікових записів доступу в інтернет-банк HSBC, десятки акаунтів PayPal і велика кількість номерів кредитних карт. Крім того, на сайті Infraud можна було розміщувати рекламу шкідливого програмного забезпечення.

Закриття Infraud стане сигналом для інших кіберзлочинців, однак навряд чи серйозно знизить їх активність, оскільки в інтернеті існують близько 200 аналогічних форумів, багато з яких мають набагато більшу аудиторію, говорять в компанії Recorded Future, що спеціалізується на кібербезпеці.

Висновок. За прогнозами, кіберзлочинність стане одним з найбільш руйнівних видів шахрайства в найближчому майбутньому. хоча у більшості компаній є план дій в разі порушення кібербезпеки, але лише деякі з них провели оцінку кіберризиків.

Одержано 06.11.2018

УДК 004.6

Костянтин Євгенійович ЛИТВИНОВ,
провідний фахівець сектору безпеки
філії УкрНДІгаз АТ «Укргазвидобування»

АНАЛІЗ ТА СИСТЕМАТИЗАЦІЯ ПЕРСОНАЛЬНИХ ДАНИХ

Одна з найважливіших проблем у протидії з кіберзлочинністю та торгівлею людьми тісно пов’язана з накопиченням та аналізом персональних даних громадян. В сучасному світі ми майже не зустрічаємо людину, яка б не мала жодного аккаунту в соціальних мережах, мобільних додатках, інтернет-магазинах або онлайн банках.

Поняття накопичення персональних даних необхідно розглядати у двох аспектах: як пошук інформації з відкритих джерел інформації (використання методології пошуку OSINT) та систематизація персональних даних в єдине джерело з офіційних джерел інформації.

В першому випадку – дуже велику роль відіграє використання методології пошуку OSINT, яка полягає в пошуку, виборі і збору інформації, отриманої із відкритих джерел і її аналіз. Така діяльність не містить ознак кримінального правопорушення, так як термін «відкритий» вказує на загальнодоступність джерела. Процес збору інформації з відритих джерел інформації нажаль не врегульовано в національному законодавстві України, проте існує роз'яснення даного права Європейського суду з прав людини.

Таким чином, права на отримання інформації з відкритих джерел глобальної мережі Інтернет роз'яснено Європейським судом з прав людини, який у своїх постановах постійно підкреслює, що стаття 10 Європейської конвенції з прав людини надає право на отримання тільки тієї інформації, яку особа бажає передати. Виходячи з цього, особа, яка розміщує персональні дані в соціальних мережах, погоджуючись з Політикою конфіденційності такої соціальної мережі, розміщує відомості про себе у відкритому доступі глобальної мережі Інтернет, усвідомлюючи, що такі дані можуть бути використані іншими особами, для її персоніфікації.

Якщо розглядати другий випадок, то дана діяльність передбачає систематизацію персональних даних громадян на законодавчому рівні з метою забезпечення більш швидкого отримання необхідної інформації правоохоронними органами щодо підозрюваних осіб. На мою думку, законодавство України потребує впровадження нових технологій в сфері доступу до персональних даних громадян, проходячи перед цим певну процедуру ідентифікації працівником компетентних органів для недопущення негативних наслідків відносно певної категорії осіб.

Підсумовуючи вищевикладене необхідно зауважити наступне:

1. При створенні єдиного джерела персональних даних громадян необхідно забезпечити неперервний процес захист інформації, яка є досить важливою для забезпечення максимального захисту організації (установи) від внутрішнього і зовнішнього, випадкового і навмисного деструктивного впливу.

2. Привертання уваги персоналу до питань безпеки, додержання персоналом вимог впровадженої в організації (установі) політики безпеки та застосування персоналом у роботі низки методів і дій, необхідних для підвищення захисту інформаційного забезпечення.

Список бібліографічних посилань

1. Базенков Н. И., Губанов Д. А. Обзор информационных систем анализа социальных сетей. *Управление большими системами* : сб. трудов. 2013. № 41. С. 357-394.

Одержано 31.10.2018