УДК 004.056

Сергій Миколайович Бортник,
доктор юридичних наук, перший проректор Харківського національного університету внутрішніх справ

Соціальна інженерія як метод вчинення злочинів

Із кожним днем по всьому світу розвиток інформаційних технологій набирає все більших обертів, вони застосовуються майже в усіх сферах людської діяльності. Злочинці теж не стоять на місці, зловживають даними можливостями й вигадують і застосовують кожного разу більш витончені способи та методи досягнення своїх цілей. Одним із основних сучасних інструментів, який є в арсеналі шахраїв і швидко розвивається, є соціальна інженерія.

Соціальна інженерія – це метод керування діями індивідууму без використання технічних засобів, що ґрунтується на використанні слабкостей людського фактора. Найчастіше соціальну інженерію розглядають як незаконний метод отримання інформації, тому сьогодні її активно використовують в інтернеті для отримання закритої інформації або інформації, яка являє велику цінність.

Соціальна інженерія є небезпечним фактором у контексті безпеки роботи підприємства, установи чи організації в цілому, тому що системи захисту створюють для зловмисника бар'єр, який досить складно подолати без спеціальних знань і навичок. У цьому випадку неважливо, якого саме працівника вдалося ввести в оману зловмиснику, тому що результатом є доступ до всіх внутрішніх ресурсів з обминанням бар'єру захисту. Атаки за допомогою методів соціальної інженерії нерідко орієнтуються на працівників, у яких є найбільші права доступу до конфіденційної інформації. Однією з важливих причин поширення соціальної інженерії як методу атаки є те, що це досить дешевий вид нападу. При цьому зловмисник може не бути фахівцем у сфері інформаційних технологій.

Найпопулярнішим серед численних сучасних інструментів соціальної інженерії є фішинг, метою якого може бути заволодіння обманним шляхом інформацією приватного характеру. Попри те, що про нього

широко відомо, успіх фішингу продовжує зростати через недостатню освіченість, низький рівень так званої кіберкультури людей.

Фішинг застосовується за певною схемою. Зловмисники можуть маскуватися під установи, яким довіряє людина. Наприклад, прикидаючись представниками оператора мобільного зв'язку або працівниками банку, вони можуть надсилати електронні листи з додатком або посиланням, за яким людина має ввести свої особисті дані. Потенційній жертві соціальної інженерії також можуть додатково зателефонувати з проханням відкрити певний додаток або перейти за надісланим посиланням. Вважається, що таке «живе» спілкування додає ситуації чималої правдоподібності та зазвичай змушує людей відкривати вкладення. Слід зазначити, що на такий «гачок» потрапляють не лише звичайні громадяни, а й навіть досвідчені експерти з кібербезпеки різних підприємств, установ та організацій.

Зважаючи на актуальність цієї проблеми, є необхідність у дослідженні й аналізі найбільш поширених алгоритмів злочинних дій у мережі Інтернет і виокремленні проблем, що виникають під час профілактики та боротьби з кіберзлочинністю, а також у наданні рекомендацій щодо протидії використанню різноманітних технік соціальної інженерії для здійснення шахрайських дій у мережі Інтернет.

Слід зазначити, що основними недоліками у сфері запобігання негативним проявам соціальної інженерії є відсутність системної роботи щодо її виявлення та подолання, низький рівень проінформованості населення щодо можливих загроз соціальної інженерії (варто відзначити позитивну роботу деяких банків у цій сфері), а також висока латентність таких злочинів, що унеможливлює виявлення та притягнення до відповідальності всіх винних осіб.

Одержано 01.11.2019