УДК 004.056
М. Турчиняк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТЕХНОЛОГІЇ ВПЛИВУ СОЦІАЛЬНИХ МЕРЕЖ НА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

UDC 004.056
M. Turchyniak

TECHNOLOGIES OF THE INFLUENCE OF SOCIAL NETWORKS ON ENSURING INFORMATION SECURITY

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ)[1] із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

Разом з тим, феномен «соціальних медіа» пов'язаний більше з культурним позиціонуванням, ніж з технологічними можливостями. Соціальні мережі швидко набули популярності і стали одним із найкращих способів проведення вільного часу та залучення клієнтів. Вони дозволяють людям підтримувати зв'язок з друзями та родиною, надають можливості пошуку кар'єрних можливостей, обміну власними думками, почуттями та ідеями в Інтернеті. Однак, використання соціальних медіа також може мати негативий вплив на особисте життя людини.

Із зростанням репутації LinkedIn, Facebook, Telegram зростають і ризики їх використання. Вільне спілкування не є безкоштовним. Зменшивши вартість інформації, втрачається її цінність і збільшується ймовірність її фальсифікації. Щоб відновити здоров'я інформаційної екосистеми, необхідно зрозуміти вразливі місця перевантаженого розуму та те, як можна використати економіку інформації, щоб захистити людей від введення в оману.

Згідно матеріалів The New York Post щодня лише у Facebook зламують 160 000 облікових записів, а дослідники Університету Фенікса що близько 66% облікових записів громадян США було хоч раз зламано (це означає, що якщо ви знаєте ім'я собаки свого менеджера соціальних мереж, ви на півдорозі до брут форсінгу облікового запису вашої організації). На відміну від інших активів, служби безпеки не можуть відключити зламаний обліковий запис у соціальних мережах, тобто зловмисник може зберігати контроль протягом годин, якщо не днів. Вартість? Кожна секунда, коли ви не контролюєте свій обліковий запис, спричиняє каскад вірусної інформації, що призводить до шкоди стосункам із брендом і клієнтом, втрати бізнесу, кошмарів зі зв'язків із громадськістю та витрат на підтримку клієнтів.

В доповіді наведено детальний аналіз[2] найбільш відомих атак на соціальні мережі. Надано пропозиції щодо забезпечення інформаційної безпеки в інтернет середовищі. До найбільш відомих атак належать:

- фішинг,
- викрадення особистих даних,
- розповсюдження зловмисного програмного забезпечення,
- соціальна інженерія та
- компрометація облікових даних банківського або системного входу.

Зокрема зазначено, що багато нападників координують свої зусилля серед білого дня. Відомо, що атаки розподіленої відмови в обслуговуванні (DDoS) використовують певний хештег Twitter для координації атаки. Зловмисники, особливо хактивісти, краудсорсингують учасників атак через кампанії з хештегами та керують DDoS-атакою в Twitter, публікуючи IP-адреси,

домени, інструменти атаки, час атаки та бажану ціль. Оскільки атаки використовують громадські місця для участі, команди безпеки можуть підготувати стратегію захисту, наприклад, ховати вхідні запити або координувати дії з мережевими командами, професійними службами та постачальниками послуг Інтернету (ISP). Команди безпеки також можуть стежити за розмовами учасників загрози, щоб виявити, чи згадується їх організація. Це одні з найчистіших, найдешевших, найактивніших і доступних у реальному часі даних про загрози. Дивно, але така публічна балаканина досить поширена. Аналізуючи, хто говорить і контекст ключової фрази, служби безпеки можуть отримати вирішальну систему раннього попередження проти атак. Зловмисники часто афішують або хваляться своїми успіхами в соціальних мережах. Вони також рекламують викрадені дані, які можуть продавати. Подібно до того, як соціальні медіа є основною рушійною силою діяльності легального ринку, ними також користуються продавці на чорному ринку. Організації можуть інтегрувати конфіденційну інформацію, виявлену на сайтах соціальних мереж, у фреймворки DLP, щоб швидше визначати, коли стався злом, і ефективніше починати дії з усунення. Витоку або викрадених даних частіше торгують у відкритому доступі, ніж усвідомлюють. Якщо облікові дані співробітників або конфіденційні файли виявлені в соціальних мережах або цифрових каналах, наприклад на сайтах вставлення, служби безпеки можуть оновити тренінги компанії, скинути облікові дані співробітників або відстежити, де заходи запобігання потенційній втраті даних (DLP) не змогли запобігти конфіденційним файлам, таким як медичні записи, інтелектуальну власність або інформацію облікового запису від виходу з мережі.

Для шахрая соціальні медіа є новим потужним інструментом для використання дуже специфічної масової групи користувачів, наприклад підписників певного бренду. Соціальні мережі [3] дозволяють шахраям націлюватися на цих користувачів, оскільки списки підписників бренду та залучення користувачів до фірмового хештегу є загальнодоступними. Таким чином, шахрай має безпрецедентну можливість отримати список жертв і розпочати цілеспрямовану атаку. Шахрайство, орієнтоване на клієнтів, зазвичай обіцяючи винагороду за певну вартість участі та використовує фальшиві логотипи бренду або історії успіху з інших облікових записів маріонеткових учасників, які вказують на те, що шахрайство є «законним». Ці шахрайства процвітають у соціальних мережах, тому що їх дуже легко створити та поширювати серед цільової аудиторії у великих масштабах. Навіть нетехнічний шахрай може створити групу фальшивих облікових записів, створених для коментування один одного та надання довіри, маючи лише підключення до Інтернету з будь-якої точки світу.

Соціальні медіа є неминучою константою для ведення бізнесу в сучасному світі. Оскільки маркетологи, рекрутери, продавці та рекламодавці постійно розширюють свою присутність, групи безпеки повинні працювати разом з ними, щоб гарантувати, що це робиться безпечно та надійно. Щоб усунути ризики соціальних мереж, служби безпеки повинні тісно співпрацювати з кількома іншими відділами. Усі інші департаменти стикаються з ризиками в соціальних мережах, і тепер командам безпеки доручено усунути ризики, одночасно забезпечуючи безпечне використання каналів соціальних мереж. Найголовніше, що команди безпеки повинні очолити цю ініціативу. Ризики в соціальних мережах залишаються.

Для зменшення ризиків[3] необхідно реєструватися не у всіх соцмережах, а лише у тих, які викликають довіру та пропонують надійні механізми аутентифікації і розмежування доступу до особистої інформації користувача, особливу увагу слід приділяти посиланням, які надходять від інших користувачів – вони можуть бути частиною фішингової чи фармінгової атаки.

Література

1. Інформаційна та кібербезпека: соціотехнічний аспект. URL: http://ippi.org.ua/sites/default/files/dovsmib_46_2_2015_0.pdf (дата звернення: 10.09.2022).
2. Рапорт компанії Norton. URL: https://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf (дата звернення: 12.09.2022).
3. Забезпечення інформаційної безпеки у соціальних мережах. URL: http://dspace.kntu.kr.ua/jspui/ bitstream/123456789/4999/1/AUConferenceCyberSecurity_November2016_p204.pdf (дата звернення: 20.09.2022).