УДК 02:004.774:366.6

Антон Вітушко,
наук. співроб. аналітично-прогностичного відділу НЮБ НБУВ

ДІЯЛЬНІСТЬ БІБЛІОТЕК У СОЦІАЛЬНИХ МЕРЕЖАХ: ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті аналізуються можливі шляхи вирішення проблеми безпечного використання соціальних мереж у роботі бібліотечних установ. Пропонуються апаратні й програмні інструменти, покликані сприяти безпечному використанню соціальних мереж для інформаційного моніторингу й інформаційного обміну.

Ключові слова: Web 2.0, соціальні мережі, кіберзлочини, хакерські атаки, Twitter, Youtube, MySpace, LinkedIn, Facebook, DLP, Cisco Systems, Inc, персоніфікація, фітинг, клікджекінг, IPS.

Нові шляхи інформаційно-аналітичної діяльності сучасних бібліотек тісно пов'язані з використанням у роботі можливостей соціальних мереж, які поступово перетворюються на один з найважливіших комунікаційних інструментів. Сайти соціальних мереж є яскравим втілення ідей Web 2.0 і мають значний вплив на суспільство: ліквідовують розрив між співтовариствами, стирають кордони реального світу та допомагають людям й організаціям обмінюватись інформацією.

Можливості соціальних мереж привертають увагу багатьох дослідників. Зокрема, М. Кастельс, один із сучасних теоретиків суспільства мережевих структур, зазначав, що саме мережі становлять нову соціальну морфологію розвинутих суспільств [1]. Проблемам функціонування і використання соціальних мереж присвячені роботи Г. Фаррелла, Д. Дрезнера, В. Горового [2] та ін.

Не применшуючи позитивного впливу соціальних мереж на розвиток інформаційного простору, дослідники, зокрема фахівці з питань інформаційної безпеки, звертають увагу на використання соціальних мереж з негативною метою. Зокрема, унаслідок популярності й стрімкого зростання соціальні мережі стали привабливим об'єктом для кіберзлочинців. З 2007 р., коли розпочався бум соціальних мереж, фахівці спостерігають різке збільшення кількості атак, метою яких є додатки Web 2.0.

У соцмереж велика аудиторія, інформація тут поширюється швидко через зв'язки між людьми. Це спрощує кіберзлочинцям завдання

поширення шкідливих програм або посилань, даючи їм змогу здійснювати декілька фішингових атак одночасно.

Крім того, соцмережі дають багато можливостей для інформаційної розвідки на базі соціальної інженерії: кількість інформації, яку можна зібрати про потенційну жертву, прямо пропорційна кількості мереж, які використовує певна людина.

У своєму віртуальному колі користувачі соціальних мереж мають досить високий рівень довіри один до одного. Вони діляться інформацією, зображеннями й файлами найрізноманітніших типів, довіряють своїм кореспондентам і без перевірки використовують незнайомі посилання, завантажують нові програми. Хакерові, що проник у коло спілкування користувача, нескладно розповсюдити спамоподібні шпигунські програми через усі його контакти.

Шкідливі програми, поширювані через сайти соціальних мереж, мають набагато більший шанс знайти свою жертву, ніж ті ж самі програми, що розсилаються електронною поштою. Крім того, хакери можуть експериментувати в соцмережах з великою кількістю різних інструментів. Зокрема, із широким спектром додатків і функцій Web 2.0, таких як контент, що створюється користувачами Twitter, відеоролики Youtube і профілі MySpace або LinkedIn та ін.

Уже є випадки, коли було зламано і використано для поширення шкідливих програм і крадіжки інформації ряд популярних додатків Facebook, таких як CityFireDepartment, Mynameis, Pass-it-on і Aquariumlife. На Facebook мали місце великомасштабні спам-атаки, під час яких користувачам Facebook розсилалися підроблені повідомлення про скидання пароля з посиланням, за яким завантажувалася небезпечна програма.

Атаки на користувачів через соціальні мережі з кожним днем стають дедалі більш витонченими й небезпечними. Їх кількість зростає. Сьогодні хакери не обмежуються фішинг-атаками на дані звичайних користувачів. Коли вони потрапляють у мережу, то з легкістю можуть проникнути в «хмару» з інформацією, яку за звичаєм вважають безпечною.

Згідно з Законом України «Про інформацію» [3], забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених Законом. Але соціальні мережі надають таку можливість, оскільки користувачі не можуть захистити свої дані від зловмисників. Проблемою є і відстеження збирання інформації про певну особу.

Соціальні мережі можуть також служити інструментом для завдання удару по репутації бібліотечної установи, оскільки в разі публікації певної

негативної інформації, від моменту публікації до моменту ухвалення рішення власниками ресурсу про її спростування, інформація здатна розійтися багатотисячним накладом шляхом копіювання на комп'ютери або тиражування по інших сайтах.

Не можна не враховувати й того факту, що останнім часом у соціальних мережах набули поширення вірусні епідемії і атаки на сервери. Велика кількість додаткових плагінів і додатків, доступних на сайтах мереж, здатні поставити під загрозу безпеку комп'ютера користувача й корпоративну мережу, у якій він перебуває, оскільки, замість нешкідливого плагіна, користувачеві може бути наданий троянський вірус або зловмисний код, що відкриває доступ до локальної машини.

Крім того, деякі співробітники використовують соціальні мережі, як й інші сервіси на зразок сервісів миттєвих повідомлень, для ділового листування, що також ставить під загрозу корпоративні інтереси організації.

Отже, соціальні мережі можуть стати серйозною загрозою безпеці IT-системи організації, якщо вона не буде турбуватися про захист своїх віртуальних сховищ. У зв'язку з цим зростає кількість організацій та установ, які закривають доступи до серверів соціальних мереж, інтернет-сервісів, зокрема таких як ICQ і Skype. З'являється інтерес до пристроїв класу DLP, тобто серверів оцінки ризиків і протидії просочуванням інформації.

Разом з тим такі обмеження, особливо в роботі інформаційно-аналітичних структур бібліотек, негативно позначаються на якості їхніх продуктів і послуг, оскільку дещо звужують джерельну базу. Щоб вирішити проблему, необхідно провести ряд заходів. Зокрема, організувати відповідну навчально-роз'яснювальну роботу з кадрами: провести тренінги, що підвищують рівень знань про інформаційну безпеку; підвищувати дисципліну персоналу і відчуття відповідальності за використання інформації.

Що треба знати співробітникам бібліотек, які використовують соціальні мережі в робочих процесах? Розглянемо чотири найбільш значні чинники ризиків.

Шкідливе програмне забезпечення.

За даними дослідників, у 2010 р. соціальні мережі стали основною середою спілкування для багатьох користувачів, які проводили в одній лише мережі Facebook у цілому понад 700 млрд хв на місяць. Ця обставина робить сайти таких мереж ідеальним «майданчиком» для впровадження шкідливого програмного забезпечення. За повідомленням

компанії Sophos, розробника і виробника засобів захисту інформації, до 40 % власників комп'ютерів користувалися шкідливим ПО, яке вони отримували із сайтів підтримки соціальних мереж. Кібератаки ж найчастіше виходили від тих, хто вважався «другом» у мережі. Зокрема, певні користувачі намагалися хитрістю нав'язати іншим інформацію з метою залучення їх у чергову фінансову піраміду.

Ось декілька типів шкідливого ПО, що є найбільш поширеним на сайтах соціальних мереж:

1. Фішинг. З появою нових технологій у кіберзлочинця виникає дедалі більше можливостей успішно видавати себе за іншу людину й переконати користувача в наданні йому такої важливої інформації, як логін і пароль доступу. Шахраї розраховують на те, що більшість людей для всіх своїх облікових записів використовують один і той же пароль. Таким чином, вони мають шанс дістати доступ і до серйозних облікових записів. Ось чому дедалі більше фішингових атак проводиться на малозначущі на перший погляд облікові дані користувачів соціальних мереж.

2. Клікджекінг. Шахраї в соціальних мережах усіма способами вимушують нас «кликнути» по посиланню, яке для зручності розміщують на нашій «стіні». Така операція сприяє встановленню на комп'ютері користувача шкідливого ПО у вигляді скрипта або виконуваного коду. Це ПО може бути використано «господарем», щоб у зручний момент вкрасти інформацію або навіть встановити контроль над комп'ютером. Технологію клікджекінга побудовано на динамічному характері спілкування в соціальних мережах і загальноприйнятій довірі до всіх посилань. За допомогою цієї технології також збираються адреси для спам-розсилань.

Захистом від цих методів атак вважаються DLP-системи й репутаційні технології, які інтегровано в різні антивірусні продукти.

Розголошування даних.

Соціальні мережі дають людям можливість спілкуватися, обмінюватися досвідом й інформацією, проте не всі відомості, які туди потрапляють, призначені для суспільного розголосу. Наприклад, це стосується внутрішньої, «інсайдерської» інформації. Відомі випадки, коли співробітники публікували в мережі на форумах фрагменти коду пропрієтарного [4] програмного забезпечення, яке належить до інтелектуальної власності і тому є тією самою «чутливою» інформацією (не конфіденційною, але не бажаною для публікації). Навіть якщо такі дії є неусвідомленими, вони потенційно можуть бути визнані порушенням тих або інших правових актів.

Слід зазначити, що на сьогодні компанії, які займаються розробкою продуктів для захисту корпоративних мереж, уміють цілеспрямовано фільтрувати веб-сервіси, з яких складаються соціальні мережі. Такі продукти дають змогу заборонити окремі сервіси, групи сервісів або окремі функції соціальних мереж.

Збільшення трафіку.

Спілкування в соціальних мережах (залежно від кількості користувачів) створює навантаження на інтернет-канал й уповільнює роботу необхідних для роботи мережевих програм. Про це говорить той приклад, що, коли американський уряд дозволив вільний доступ до соціальних мереж в установах, мережевий трафік збільшився на 25 %. На одне лише відео в режимі онлайн у мережах потрібна пропускна спроможність від 500 кб/с до 1,2 Мб/с, а відео високого дозволу (HD) може збільшити навантаження на мережу на 4–7 Мб/с. Тому вважається доцільним обмеження кількості співробітників, які працюють з матеріалами соцмереж.

Захист своєї діяльності.

Оскільки в сучасній інформаційній діяльності бібліотекам потрібні електронні ресурси соціальних мереж, немає жодної причини відмовлятися від них через високі ризики безпеки. Треба провести відповідні заходи, які дають змогу захистити діяльність і знизити рівень цих ризиків. З цією метою можна використовувати:

– мережевий екран, що працює в режимі реального часу. Соціальні мережі – це мінливе середовище, щоб протистояти в ньому хакерам, треба стати настільки ж непередбачуваними, як і вони. Вельми корисно проводити аналіз інтернет-трафіку організації, який дасть змогу розпізнавати загрози заздалегідь. Аналіз у режимі реального часу дає можливість переглядати окремі з'єднання і виявляти чинники ризику, забезпечуючи своєчасний захист діяльності співробітників у соціальних мережах і в Інтернеті в цілому;

– вибірковий контроль використання соціальних мереж. Для правильного використання інформації в межах концепції створеної бібліотекою в соцмережах сторінки або групи керівник такої роботи має залишити за собою право стежити за діями працівників на сайтах соціальних мереж. Зокрема, необхідно контролювати завантаження текстових файлів, фотографій і відеозаписів;

– роботу з використанням кеш-пам'яті (кешування). Не слід допускати, щоб трафік від використання соціальних мереж негативно позначався на роботі мережевих програм, важливих для інших видів роботи. Можна

зменшити вплив соціальних мереж на пропускну спроможність каналу за допомогою кешування на сервері сторінок сайтів, які часто використовуються. Після початкового завантаження з мережі файли даних, що приймаються, і відеофайли зберігатимуться на локальному сервері. Це дасть змогу зменшити трафік і поліпшити час реакції на запит користувача. При цьому можна буде отримувати доступ на сайти соціальних мереж (на локальний сервер, де вони зберігаються й оновлюються), не знижуючи пропускну спроможність мережі організації;

– гнучку мережеву політику. Бібліотеці важливо виробити правильну позицію у всіх питаннях, що стосуються соціальних мереж, що допоможе забезпечити зручну роботу з корисними мережевими програмами. Зокрема, можна заблокувати доступ на фейсбуковий FarmVille або дозволити його, але з найнижчим пріоритетом. Таким чином робота з важливими ресурсами не постраждає. Коли мережева політика гнучка, є можливість вільно змінювати пріоритети додатків і контролювати роботу людей у мережі, тимчасово дозволяючи або забороняючи їм доступ на певні сайти. Здатність провести чітку лінію між важливими й неважливими для роботи ресурсами – це критичний момент, що визначає ефективність здійснюваної політики. При гнучкій політиці соціальні мережі не будуть джерелами загрози для організації. Для цього досить побудувати правильну систему безпеки.

Ступінь впливу соціальних мереж на інформаційну безпеку організації дуже істотний. Імовірність сценарію, коли співробітник бібліотеки розголошує конфіденційну інформацію, дуже велика. Щоб цьому протидіяти, необхідний функціонал DLP-систем. Але далеко не будь-яка DLP-система зможе ефективно протистояти подібним витокам, і, крім того, вона вимагає особливого настроювання.

Слід зазначити, що існуючі методи боротьби на корпоративному рівні будуть ефективні за умови, коли розроблювач засобів боротьби з інформаційними загрозами регулярно оновлює свої розв'язки й включив до них відомості про нові погрози, що поширюються через соціальні мережі, і засоби їх мінімізації.

Як правило, у бібліотеках політика інформаційної безпеки стосовно соціальних мереж не дуже відрізняється від політики використання інших інтернет-ресурсів. Очевидно, у концепції цієї політики мають бути пункти про те, яку інформацію можна публікувати в соціальних мережах.

З технічної точки зору сайти соціальних мереж не створюють проблем, принципово відмінних від тих, з якими мають справу ті, хто користується Інтернетом. Головна проблема тут у тому, як впоратися з чинниками

ризиків, що виникають унаслідок більш активного обміну інформацією, не забороняючи користуватися цими сайтами.

Щоб знизити рівень ризику, можна зробити ряд простих заходів, що дають змогу створити певну лінію оборони. До соціальних мереж слід застосовувати ті ж заходи захисту, що й до інших сайтів Інтернету. По-перше, користувачі повинні розуміти, що у віртуальному колі спілкування слід дотримуватися тих правил, як і при поштовому листуванні або на інших ресурсах Інтернету. Слід використовувати надійні засоби захисту своєї особистої інформації, починаючи з використання різних паролів достатньої стійкості для різних облікових записів і правильної установки параметрів конфіденційності. Співробітникам слід уникати публікації надмірних подробиць організаційного характеру. Їм рекомендується поводитися в мережах відповідально й обачно – так, як і в житті.

Сприятимуть безпеці мережі організації також грамотна архітектура інформаційного захисту з якісним міжмережевим екраном і потужною системою IPS для виявлення змішаних загроз і захисту від самих різних способів НСД [5]. Також слід упровадити повнофункціональне вирішення захисту мережевого устаткування, покликане захистити систему від черв'яків, троянів, шпигунів і інших шкідливих програм, що загрожують нормальному функціонуванню мережі бібліотечної установи і вимагають трудомісткого усунення неполадок, знижують продуктивність праці співробітників і підвищують ризики крадіжки даних. Цей тип захисту разом із грамотними правилами нормативно-правової відповідності й регулярним оновленням модулів допоможе запобігти випадкам фішингу.

Web 2.0 має багато переваг не лише для приватних користувачів, але й для бібліотечних організацій. Після того як організації встановлять контроль над чинниками ризиків для систем IT, пов'язаних із соціальними мережами, вони почнуть активніше користуватися цими мережами й зможуть реалізувати весь спектр їх переваг.

Розглянувши найбільш поширені типи загроз інформаційній безпеці в комп'ютерних мережах, можна зробити висновок, що визначальну роль у захисті інформації відіграє безпосередньо людина. Саме від професійної підготовки співробітників відповідних ланок залежить інформаційна безпека організації.

На сьогодні одним з найважливіших завдань для бібліотек є донесення знань про базові принципи безпеки в соціальних мережах до осіб, які мають безпосереднє відношення до інформаційної безпеки й стратегічних масивів даних, але не є фахівцями у сфері IT.

Список використаних джерел

1. *Кастельс М.* Становление общества сетевых структур / М. Кастельс // Новая постиндустриальная волна на Западе. Антология. – М. : Academia, 1999. – С. 494–505; Кастельс М. Информационная эпоха: экономика, общество, культура / М. Кастельс. – М. : ГУ ВШЭ, 2000.

2. *Горовий В. М.* ІТ-субкультури в структурі сучасного суспільства / В. М. Горовий // Україна: події, факти, коментарі. – 2012. – № 5. – С. 76–85.

3. Про інформацію : Закон України [Електронний ресурс] // Відомості Верховної Ради. – 1992. – № 48, ст. 650 : офіц. веб-сайт Верховної Ради України. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?Nreg=2657–12. – Назва з екрана.

4. *Андреев Э. М.* Социальные проблемы интеллектуальной уязвимости и информационной безопасности/ Э. М. Андреев, А. В. Миронов // Социально-гуманитарные знания. – 2000. – № 4. – С. 169–180.

5. *Попов В. Б.* Основы информационной безопасности. Информационные технологии и право / В. Б. Попов // Основы компьютерных технологий. – 2002. – С. 175–187.