Лабораторна робота №4

Тема: Інформаційна безпека в соціальних мережах. Захист електронної пошти та власних акаунтів під час роботи в мережі.

Мета: ознайомитися з поняттям служби соціальної мережі та електронної пошти, основними джерелами та шляхами уникнення втрати інформації під час користування послугами соціальної мережі; особливостями захисту особистих даних і таємниці листування в процесі використання електронної пошти.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Однією з най масштабніших мереж загального користування є глобальна мережа Інтернет – система об'єднаних комп'ютерних мереж глобального загальнолюдського суспільства, яка в наш час покриває практично всю поверхню земної кулі. Однак, на базі мережі Інтернет почали з'являтися інші мережі – соціальні. Соціальна мережа — соціальна структура, утворена індивідами або організаціями. Вона відображає розмаїтті зв'язки між ними через різноманітні соціальні взаємовідносини, починаючи з випадкових знайомств і закінчуючи тісними родинними вузами. Вперше термін було запропоновано в 1954році Дж. А. Барнесом (в роботі Class and Committees in a Norwegian Island Parish, «Human Relations»). Максимальний розмір соціальних мереж становить близько 150 осіб, а середній — 123 (Хілл та Данбер, 2002).

Аналіз соціальних мереж (має стосунок із теорія мереж) перетворився на основний метод досліджень в сучасній соціології, антропології, географії, соціальній психології, інформатиці та дослідженні організацій, а також поширену тему для досліджень та дискусій. Дослідження в декількох академічних сферах показали, що соціальні мережі діють на багатьох рівнях, починаючи від родин, і закінчуючи цілими націями, та відіграють важливу роль в тому, як розв'язуються проблеми, працюють організації, та досягають успіху на шляху до власних цілей індивіди.

Соціальні мережі в Інтернеті

Служба соціальних мереж (англ. *socialnetworkingservice*) — веб-сайт або інша служба у Веб, яка дозволяє користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок та переглядати власний список зв'язків і списки інших користувачів. Природа та номенклатура зв'язків може різнитись в залежності від системи.

На відміну від служб соціальних мереж, в *інтернет-спільнотах* користувач не знаходиться в центрі системи; відношення користувача до інших учасників спільноти знаходиться на другому плані. Основна увага інтернет-спільноти зосереджена на внеску користувача в досягнення спільних цілей, цінностей та спілкуванні.

В соціальних мережах користувач знаходиться в центрі системи та може належати до декількох груп водночас.

Ні для кого не секрет, що соціальні мережі вже давно є привабливими платформами для різного роду кібер-злочинів, таких як спаммінг, фішинг, фармінг акаунтів і інших. Причина криється в ряді властивостей, якими володіють всі соціальні мережі і які можуть бути використані зловмисниками в своїх цілях.

Такими властивостями насамперед є:

- Величезна користувача база.
- Виникнення зв'язків довіри як між окремими користувачами так і між групами користувачів.
- Висока розподіл бази користувачів за географічним і тимчасовому параметрам.
- Комп'ютерна неграмотність користувачів соціальної мережі.

Людям знайомим з інформаційною безпекою не треба пояснювати, що при комбінації методів технічних та соціальної інженерії ці властивості дозволяють досягти бажаного результату в короткі терміни при витраті мінімальних зусиль.

Легітимна вразливість

На даний момент надання API для створення сторонніх додатків для соціальних мереж стало фактично стандартом де-факто. У більшості випадків передбачається, що додатки створювані за

допомогою даних API не будуть приносити шкоду і звичайно з-за величезної кількості створюваних додатків перевірка кожного з них видається нездійсненним завданням. Відповідно створювані додатки додаються в базу соціальної мережі без належної перевірки на те, чи є вони шкідливим ПЗ. Положення також посилюють згадані раніше зв'язки довіри і насамперед довіра до самої соціальної мережі. Незважаючи на те, що адміністрація всіляко вказує на те, що дані програми є продуктом сторонньої розробки більшість користувачів не звертає на це увагу, вважаючи за краще довіряти будь-якій програмі за умовчанням. Як результат - зловмисники мають можливість додавати і поширювати шкідливі програми засобами, що надається самої соціальною мережею. Велика соціальна мережа Facebook регулярно піддається атакам черв'яків. У побут навіть увійшов спеціальний термін - rogue app. Використовуючи абсолютно легітимні засоби, що надаються API Фейсбук, черв'яки поширюються розсилкою повідомлень друзям зараженого аккаунта. Звичайно основною метою цих черв'яків є поширення іншого шкідливого ПЗ, яке заражає машину користувача, відповідно створюючи ботнет. Подібних атак схильна і вітчизняна мережа ВКонтакте. В даному випадку мали місце і прямі атаки на машину користувача з використанням вразливостей в технології флеш.

Ще одна небезпека, що може трапитися з користувачем соціальної мережі це викрадення аканту. Ціль викрадення може бути різна – наприклад, для подальшої перепродажі спамерам, для розсилки спаму самостійно, для помсти. Основні методи викрадення наведено нище.

1. Взлом через е-мейл. Цей метод діє через функцію відновлення пароля. Як відомо, пароль можна отримати поштою, на яку зареєстрована сторінка. Для цього використовується функція відновлення пароля. Частенько, зламати поштову скриньку простіше, ніж аккаунт, тому віднесіться уважно до безпеки своєї пошти – вибирайте складний пароль, використовуйте популярні і надійні сервіси. Уважно віднесіться до складання секретного питання. Відповідь на нього повинні знати лише ви. Ваші друзі не повинні зуміти відповісти на секретне питання. Краще всього буде, якщо сама адреса пошти, на яку ви реєструєте свої аккаунти, буде зареєстрована окремо і не буде вашим основним e- mail'ом. Не варто говорити про нього вашим знайомим, зберігайте його, як і пароль – в таємниці. Тоді задача хакера доволі ускладниться, адже не знаючи пошти, на яку зареєстровано аккаунт, незрозуміло яку пошту ламати! Крім того, більшість сервісів дозволяє використовувати підтвердження на мобільнийтелефон. Користуйтеся цим. Не нехтуйте зайвими мірами захисту – все що ускладнює життя зловмисникові, допомагає вам;

Засоби захисту: Використовуйте завжди складні паролі, використовуйте окрему поштову скриньку для реєстрації, використовуйте підтвердження на мобільний телефон.

2. Брутфорс (підбір пароля) – це досить старий метод і більшість сервісів вимагають від своїх користувачів використовувати надійні паролі, а також не дозволяють більш ніж 3-5 помилок. Після цього на деякий час користувач блокується. Так що цей метод зараз можна не приймати до уваги – звісно, якщо ви дійсно маєте надійні паролі. Також бажано їх час від часу міняти, а також мати різні паролі для різних сервісів;

Засоби захисту: Використовуйте завжди складні паролі.

3. Взлом через cookie. Cookie – це файл на комп'ютері користувача, в якому зберігається його e-mail і зашифрований пароль. Завдяки цим файлам Вам не доводиться кожного разу при вході вводити пароль, адже він збережений в cookie, і ви потрапляєте прямо на сайт. Якщо хакер отримає цей файл cookie, то взнає ваш e-mail і пароль (правда в зашифрованому вигляді). Розшифрувати пароль не складно, якщо він короткий і простий, але якщо пароль складений відповідно до пункту 2 – задача крадія буде дуже ускладнена. Крадуть cookie різними способами, але, щоб цього уникнути, слідуйте наступними порадам: не вводьте в рядок браузера незнайомі скрипти, адже вони можуть зберігати cookies; не встановлюйте жодні доповнення для соціальних мереж з сумнівних джерел; на жодних сайтах не залишайте значення своїх cookies (зараз дуже популярні безкоштовні дарунки в однокласниках, безкоштовний рейтинг в контакті і так далі); не залишайте своїх знайомих за вашим комп'ютером одних, якщо не довіряєте їм, вкрасти cookies займе 5-10 сек, якщо підійти із знанням справи;

Засоби захисту: не вводьте в рядок браузера незнайомі скрипти, не встановлюйте жодні доповнення для соціальних мереж з сумнівних джерел, на жодних сайтах не залишайте значення своїх

cookies, не залишайте своїх знайомих за вашим комп'ютером одних.

4. Використовування фейків – фейк (від англійської fake – підробний, фальшивий) – це спеціальна сторінка, яка цілком виглядає так, як оригінальна для вводу логіну та пароля в соціальній мережі. Ціль зловмисників – заставити вас ввести ваші логін та пароль – після чого вони будуть переслані їм. Після вводу вас перенаправлять на оригінальній сайт. Фейки зараз дуже популярні – їх легко зробити, та легко використовувати. Більшість користувачів не дивляться на адресу сторінки, де вони знаходяться. Дуже часто фейкові сторінки пропонують у вигляді спаму з уже зломаних аккаунтів. Будьте уважні – не переходьте на посилання тільки тому, що воно прийшло від знайомого, особливо якщо до цього він ніколи вам подібного нічого не присилав. Не переходьте за посиланням якщо вам пропонують щось "бесплатно"– пам'ятайте де буває безплатний сир.

Засоби захисту: не переходьте на посилання тільки тому, що воно прийшло від знайомого, не переходьте за посиланнями, якщо вам пропонують щось "бесплатно" та "безвозмездно", будьте уважні.

5. Взлом через програми – це дуже популярний спосіб злому – особливо для таких мереж як ВКонтакте. Пам'ятайте – використовувати треба тільки ті програми, які ви отримали із надійного джерела. Надійними джерелами є тільки ті, що рекомендує безпосередньо адміністрація цієї мережі. Всі інші – ви використовуєте на свій страх та ризк. До речі – аргументація типа – "Друг Вася використовує і нічого …" – це не дуже розумно. Якщо вже вам так необхідні "примочки" – шукайте тільки ті, що розповсюджуються з відкритим вихідним кодом. Якщо програма розповсюджується задарма, але розробник не відкриває її код, подумайте ще раз – де буває той дешевий сир.

Засоби захисту: не використовуйте програми з ненадійних джерел.

Що не варто писати в соціальних мережах

Явки і паролі. Першими під заборону потрапили логіни і паролі. Виявилося, що соціальні мережі використовуються не тільки для спілкування, але й для зберігання та обміну секретними даними. Причому деякі користувачі можуть "виставити на загальний огляд" пароль і від самої соціальної мережі. Тому особливо наївним радять відразу ж змінити пароль, після того, як він потрапив у чий-небудь чужий ящик.

Дівоче прізвище. Продовжуючи тему безпеки в мережі, не можна не згадати і про кодових словах, які використовуються для відновлення забутого пароля. Ні для кого не секрет, що найпопулярнішими з кодових питань є або дівоче прізвище матері, або номер школи. Саме з цієї причини користувачів, що бажають надати про себе якомога більше інформації, застерігають від афішування прізвищ родичів і номерів навчальних закладів.

"Стіна" ганьби. Наступними в списку заборонених дій в соціальних мережах виявилися публікації повідомлень особистого характеру на так званій "стіні". Не треба забувати про те, що шедеври на "стіні" бачить не лише одержувач, але й інші користувачі. Тому перед тим, як відправити чергове повідомлення провокаційного змісту, задумайтеся, чи не зашкодить воно адресату.

Принада для шахраїв. Контактні дані, зокрема адресу та телефон, також не варто залишати у відкритому доступі. Пам'ятайте, що зловмисники в будь-який момент можуть використовувати цю інформацію в незаконних цілях, особливо якщо знають, о котрій годині вас не буває вдома.

Плани на вечір. Для обговорення планів на вечір або вихідні краще використовувати особисту переписку або створювати закриті групи. Інакше інформація про барвистий вікенд може бути використана проти вас же самих (дивіться попередній пункт).

Бережіть свій гаманець. Інформація про ваше фінансове становище є, мабуть, однією з найбільш секретних. Ні в якому разі не можна повідомляти про розмір вашої заробітної плати та про те, де ви її отримуєте і зберігайте.

Ви і ваша робота. Під грифом секретності повинна залишитися і інформація про вашу організацію. Так, компанія Sophos, що займається питаннями інформаційної безпеки, провела дослідження і з'ясувала, що близько 63% організацій побоюються зайвої балакучості своїх співробітників, які не замислюючись про наслідки можуть опублікувати цінну інформацію. Одним з найяскравіших прикладів подібного випадку є історія з компанією Microsoft. Через профілі співробітників "комп'ютерного гіганта" у соціальній мережі Linkedin журналістам неодноразово

вдавалося отримувати дані про які-небудь новинки чи плани компанії за кілька місяців до їх офіційного оприлюднення.

Дитячі фотографії. Нешкідливі на перший погляд фотографії дітей насправді можуть зіграти злий жарт із їхнім власником. По-перше, не можна забувати про людей, хворих педофілією, а, по-друге, інформація про те, що дитина може залишитися вдома одна, що може призвести до наслідків, описаним у пункті 4.

Мисливці за компроматом. Інформація з вашого профілю також може бути використана іншими сервісами і в підсумку спрямована проти вас. Існує чимало курйозних випадків, коли людина, відпросившись з роботи з причини поганого самопочуття, замість кабінету стоматолога проводила час на якій-небудь вечірці, а роботодавець випадково отримував фотографії "важко хворого співробітника", танцюючого і щасливого.

Сам собі ворог. Довірливо публікувати інформацію про себе, сподіваючись лише тільки на те, що навряд чи хтось побачить її крім самих близьких людей, - помилка багатьох користувачів. Пам'ятайте, що велика частина додатків соціальних мереж призначена для доступу до конфіденційної інформації.

Електронна пошта - традиційні засоби зв'язку, що дозволяють обмінюватися інформацією, принаймні, двом абонентам.

Основні протоколи передачі пошти (SMTP, POP3, IMAP4), як правило, не здійснюють надійної автентифікації, що дозволяє легко створити листи з фальшивими адресами. Жоден із цих протоколів не використовує криптографію, яка могла б гарантувати конфіденційність електронних листів. Хоча існують розширення цих протоколів, рішення про їх використання повинне бути прийняте як складова частина політики адміністрації поштового сервера. Деякі такі розширення використовують уже наявні засоби автентифікації, а інші дозволяють клієнтові й серверові погодити тип автентифікації, який використовуватиметься в цьому з'єднанні.

Адресі відправника в електронній пошті Інтернету не можна довіряти, тому що відправник може вказати фальшиву зворотну адресу, або заголовок може бути модифікований у ході передачі листа, або відправник може сам з'єднатися з SMTP-портом на машині, від імені якої він хоче відправити лист, і ввести текст листа.

Заголовки й вміст електронних листів передаються в чистому вигляді. У результаті зміст повідомлення може бути прочитаний або змінений у процесі передачі його через Інтернет. Заголовок може бути модифікований, щоб приховати або змінити відправника, або для того, щоб перенаправляти повідомлення.

Поштова бомба — це атака за допомогою електронної пошти. Система, що атакується, переповнюється листами доти, поки вона не вийде з ладу. Як це може спричинитися, залежить від типу поштового сервера і того, як він сконфігурований.

Деякі провайдери Інтернету дають тимчасові логіни кожному для тестування підключення до Інтернету, і ці логіни можуть бути використані для початку подібних атак.

Типові варіанти виходу поштового сервера з ладу:

1. Поштові повідомлення приймаються доти, поки диск, де вони розміщаються, не переповниться. Наступні листи не приймаються. Якщо цей диск є також основним системним диском, то вся система може аварійно вимкнутися.
2. Вхідна черга переповнюється повідомленнями, які потрібно обробити й передати далі, доти, поки не буде досягнутий граничний розмір черги. Наступні повідомлення не потраплять до черги.
3. У деяких поштових систем можна встановити максимальну кількість поштових повідомлень або максимальний загальний розмір повідомлень, які користувач може прийняти за один раз. Наступні повідомлення будуть відкинуті або знищені.
4. Може бути перевищена квота диска для цього користувача. Не буде можливості прийняти наступні листи або виконувати інші дії. Відновлення може виявитися важким для користувача, тому що йому може знадобитися додатковий дисковий простір для видалення листів.

5. Великий розмір поштової скриньки може утруднити для системного адміністратора одержання системних попереджень і повідомлень про помилки.

6. Посилка поштових бомб у список розсилання може призвести до того, що його члени можуть відписатися від списку.

У минулому, коли Інтернет був дослідницькою мережею, його комерційне використання було заборонене. Крім того, занадто мало компаній і людей мали доступ до Інтернет-пошти, тому було недоцільно використовувати її з комерційною метою. Зараз Інтернет розширився й дозволяється використовувати його в комерційних цілях, тому компанії почали підтримувати списки розсилання для обміну інформацією зі своїми клієнтами. Як правило, клієнти повинні надіслати запит для того, щоб потрапити в список розсилання. Коли великі онлайнові сервіси почали шлюзувати листи в Інтернет, несподівано виявилося, що в такий спосіб можна передати інформацію набагато більшій аудиторії. Так народився маркетинг в Інтернеті за допомогою посилання окремих поштових повідомлень.

Через те що будь-яка людина у світі може послати вам лист, не так просто змусити її припинити посилати їх вам. Люди можуть розпізнати вашу адресу зі списку адрес організації, списку осіб, що підписалися на список розсилання, або листів у Usenet. Якщо ви вказали вашу поштову адресу на якому-небудь веб-сайті, то він може продати вашу адресу «поштовим сміттярам». Деякі веб-браузери самі вказують вашу поштову адресу, коли ви відвідуєте вебсайт, тому ви можете навіть не знати, що ви її дали. Багато поштових систем мають можливості фільтрації пошти, тобто пошуку зазначених слів або словосполучень у заголовку листа або його тілі, і наступного вміщення його в певну поштову скриньку або видалення. Але більшість користувачів не знає, як використовувати механізм фільтрації. Крім того, фільтрація в клієнта відбувається після того, як лист вже отриманий або завантажений, тому утруднюється видалення великих обсягів листів.

Для безпечної атаки може використовуватися анонімний ремайлер. Коли хтось хоче послати образливий або загрозливий лист і при цьому приховати свою особу, він може скористатися анонімним ремейлером. Якщо людина хоче послати електронний лист, не розкриваючи свою домашню адресу тим, хто може загрожу-вати їй, вона може теж використовувати анонімний ремейлер. Якщо вона почне раптом одержувати небажані листи на свою поточну адресу, вона може відмовитися від неї і взяти нову.

Одним із поширених засобів захисту, до якого часто вдаються деякі користувачі Usenet, є конфігурація своїх клієнтів для читання новин у такий спосіб, що в полі Reply-To (зворотна адреса) листа, який посилається ними в групу новин, міститься фальшива адреса, а реальна адреса міститься в сигнатурі або в тілі повідомлення. Тому робота програм збирання поштових адрес, які збирають адреси з поля Reply-To, виявиться марною.

У конгресі США було подано кілька біллів про обмеження на роботу таких програм-сміттярів. В одному пропонувалося створити списки стоп-слів і поміщати слово «реклама» у рядок теми листа. В іншому пропонувалося вважати їх просто незаконними.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Зайдіть під власним акаунтом на одну з соціальних мереж, в якій зареєстровані.
2. Проаналізуйте анкету, яку заповнює кожен учасник даної соціальної мережі.
3. Запишіть до звіту назви полів, з яких складається дана анкета, опишіть які з них можливо приховувати, можливі варіанти доступу до них інших учасників, оцініть степінь безпечності розголошення даної інформації по 5-бальній шкалі. Зробіть в звіті аналіз можливих небезпек в результаті доступу до інформації, яку розміщує учасник даної соціальної мережі.
4. Зробіть аналіз власної анкети з точки зору роботодавця. Яка інформація буде для вас цікавою? Що може вплинути на ваше рішення взяти цю людину до себе на роботу? Висновки запишіть до звіту.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Дайте визначення поняття служби соціальних мереж.
2. Назвіть основні властивості служби соціальних мереж.
3. Охарактеризуйте основні методи викрадення аканту користувача соціальної мережі та

засоби захисту від них.

4. Що не варто писати в соціальних мережах?
5. Що таке електронна пошта? Назвіть основні способи втрати інформації під час роботи з даним сервісом.
6. Що називається поштовою бомбою?
7. Назвіть та опишіть типові варіанти виходу поштового сервера з ладу.
8. Опишіть способи боротьби із втратою інформації під час роботи з електронною поштою.
9. Сформулюйте правила під час спілкування в соціальній мережі.
10. Сформулюйте основні правила для користувача електронною поштою.