УДК 004.8

Лещенко М.С., студент 4 курсу
спеціальності 122 «Комп'ютерні науки»
Потапова Н. А., к.е.н, доцент, доцент
кафедри інформаційних технологій

ЗАХИСТ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ЕЛЕКТРОННОЇ ПОШТИ

Донецький Національний університет імені Василя Стуса, м. Вінниця

Електронна пошта стає все більш важливим елементом для повсякденної діяльності. Підприємствам потрібні спеціалісти для налаштування надійності електронної пошти, щоб допомогти співробітникам правильно її використовувати, зменшити ризик навмисного або ненавмисного неправильного її використання, і щоб гарантувати, що офіційні документи, які передаються за допомогою електронної пошти, правильно обробляються. У процесі розширення використання систем електронної пошти в сучасному діловому світі стрімко зростає і кількість конфіденційних даних, які передаються по мережі Інтернет. В результаті стає актуальною проблема автоматизації та захисту документообігу, що здійснюється за допомогою засобів електронної пошти.

Електронні поштові скриньки зберігають не тільки величезний обсяг особистих та робочих даних (листів), але й зазвичай прикріплені до аккаунтів у соціальних мережах, менеджерах, хмарних сервісах тощо. Тому несанкціонований доступ до поштової скриньки може мати серйозні наслідки, такі як отримання інформації конфіденційного характеру, зміна паролів до сайтів, акаунтів без відома їх власників, отримання доступу до особистих фотографій та відео, розсилання спаму від імені інших осіб тощо.

У процесі розширення використання систем електронної пошти в сучасному діловому світі стрімко зростає і кількість конфіденційних даних, які передаються по мережі Інтернет. В результаті стає актуальною проблема автоматизації та захисту документообігу, що здійснюється за допомогою засобів електронної пошти.

Можна виділити основні загрози, пов'язані з електронною поштою [1]:

1. Фальшиві адреси відправника. Адресі відправника в електронній пошті в Інтернеті не можна довіряти, тому що відправник може вказати фальшиву зворотну адресу, або заголовок може бути модифікований в ході передачі листа, або відправник може сам з'єднатися з SMTP-портом на машині, від імені якої він хоче відправити лист, і ввести його.
2. Перехоплення листа. Заголовки і вміст електронних листів передаються в чистому вигляді. В результаті вміст повідомлення може бути прочитано або змінено в процесі передачі його через Інтернет.
3. Поштові бомби. Поштова бомба – це атака за допомогою електронної пошти. Система, на яку здійснюється атака переповнюється листами до тих пір, поки вона не вийде з ладу.

З метою уникнення негативних наслідків у випадку втрати або викрадення носіїв інформації необхідно [2]:

1. Встановити паролі на усі пристрої, що перебувають у користуванні (PIN-коди, паролі на вхід до всіх облікових записів, паролі на планшетах та ноутбуках тощо);
2. Систематично робити резервне копіювання важливих файлів;
3. Блокувати пристрої щоразу після закінчення роботи з ними.

Деякі провайдери дають тимчасові логіни для тестування підключення до Інтернету, і ці логіни можуть бути використані для початку подібних атак. Типові варіанти виходу поштового сервера з ладу[3]:

1. Поштові повідомлення приймаються до тих пір, поки диск, де вони розміщуються, максимально не переповниться. Наступні листи не приймаються. Якщо цей диск є також основним системним диском, то вся система може аварійно відключитися.
2. Вхідна пошта переповнюється повідомленнями, які потрібно обробити і передати далі, до тих пір, поки не буде досягнутий граничний розмір черги. Наступні повідомлення не потраплять в чергу.
3. У деяких поштових систем можна встановити максимальне число 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 даного користувача. Це завадить прийняти наступні листи, і може перешкодити йому виконувати інші дії. Відновлення може виявитися важким для користувача, так як йому може знадобитися додатковий дисковий простір для видалення листів.
5. Великий розмір поштової скриньки може зробити важким для системного адміністратора отримання системних попереджень і повідомлень про помилки.
6. Отримання поштових бомб в список розсилки може привести до того, що його члени можуть анулювати свою підписку.

Також виділяють листи з погрозами. Якщо ви вказали вашу поштову адресу на певному веб-сайті, він може продати вашу адресу для поштового спаму. Деякі веб-браузери самі вказують вашу поштову адресу, коли ви відвідуєте веб-сайт, тому ви можете навіть не зрозуміти, що ви його дали. Для безпечної атаки може використовуватися анонімний ремейлер. Коли хтось хоче надіслати образливий або лист із погрозами і при цьому приховати свою особистість, він може скористатися анонімним ремейлером. Якщо людина хоче надіслати електронного листа, не розкриваючи свою домашню адресу тим, хто може загрожувати йому, він може теж використовувати анонімний ремейлер. Якщо він почне раптом отримувати небажані листи за своєю поточною адресою, він може відмовитися від нього і взяти новий [1].

Таким чином, усі співробітники підприємств повинні використовувати електронну пошту так само, як і будь-який інший офіційний засіб організації. Коли лист надсилається, як відправник, так і одержувач повинен гарантувати, що взаємодія між ними здійснюється відповідно до прийнятих правил захисту.

Захист листів, поштових серверів і програм повинен відповідати ступеню важливості інформації, яка передається по мережі. Тобто, має здійснюватися централізоване управління сервісами електронної пошти. Повинна бути розроблена політика, в якій вказувався б потрібний рівень захисту. Для вирішення задач із забезпечення безпеки інформації, що надсилається через електрону пошту в усьому світі все активніше застосовуються технології криптографічного захисту з використанням відкритих ключів.

Список літературних джерел.

5. Волокита А., Мухін В., Стешин В..Специфіка інформаційних систем на основі технології cloud computing. URL: http://archive.nbuv.gov.ua/ portal/natural/vcndtu/ 2011_53/29.htm.
6. Інформаційна безпека при роботі у мережі Інтернет. URL: https://khm.gov.ua/uk/content/informaciyna-bezpeka-pry-roboti-u-merezhi-internet.
7. Гутман Б., Бегвілл Р. Політика безпеки при роботі в Інтернеті. URL: http://citforum.ru/internet/security_guide/glava8.shtml#8_7.

УДК 316.772.5:[004.056:351.86](043.2)

Македонський Б. О. студент 3 курсу спеціальності 125 «Кібербезпека»
Зелінська О.В. доцент, доцент кафедри інформаційних технологій

СОЦІАЛЬНИЙ ФАКТОР У ПРОБЛЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ

Донецький національний університет імені Василя Стуса, м. Вінниця

Одним із основних методів протизаконного отримання інформації є соціальна інженерія. Соціальна інженерія – метод отримання необхідного доступу до інформації, що ґрунтується на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних та інших захищених систем. Хоча термін соціальної інженерії виник недавно, такий спосіб отримання інформації використовується досить довго [1]. Кожен із нас стикається з таким майже щомісяця, коли через телефонні дзвінки повідомляють, що із вашої картки списуються грошові суми і просять продиктувати данні картки. Це підтверджує, що саме ви є її власником і блокує рахунок. І все, усі данні уже відправлені зловмисникам, особисто власником карти. Їм залишається лише забрати гроші жертви. Це один із найпримітивніших методів використання соціальної інженерії. Для такого не потрібні ніякі технічні знання, знання програмування, потрібно лише знати психологію людини, і вміти правильно говорити.