УДК 004.89

Т. В. Іванюк

МОДУЛЬ ПЕРЕВІРКИ ВКЛАДЕНЬ ЕЛЕКТРОННИХ ЛИСТІВ

Вінницький національних технічний університет

Анотація

У данній статті розглянуто актуальні протоколи електронної пошти, розроблено алгоритм модуля перевірки вкладень електронних листів використовуючи сервіс VirusTotal.

Ключові слова: поштовий сервіс, алгоритм, електронний лист, аналіз файлів.

Abstract

In this article the actual protocols of e-mail are considered, the algorithm of the module of check of attachments of e-mails using VirusTotal service is developed.

Keywords: mail service, algorithm, e-mail, file analysis.

Вступ

Використання сторонніх поштових сервісів має негативний характер для безпеки: розміщення серверів у постачальника послуг, закритість алгоритмів захисту, можливість доступу до листів третіми особами ставить безпеку підприємства під загрозу, тому в цій роботі буде розглянуто побудову подібного сервісу для самостійного адміністрування та використання.

Мета роботи полягає у розробленні корпоративного поштового сервісу для обміну повідомленнями як в корпоративній мережі, так і з зовнішніми поштовими сервісами з перевіркою вкладень на наявність вірусів для підвищення безпеки.

Для досягнення вищевказаної мети необхідно:

– дослідити протоколи електронної пошти;

– реалізувати алгоритм роботи модулю перевірки вкладень електронних листів;

Аналіз протоколів електронної пошти

Всього існує три загальноприйнятих стандарту, використовуваних для обміну електронними листами (їх відправки та отримання) - це IMAP, POP3 і SMTP [1].

Простий протокол передачі пошти - SMTP (Simple Mail Transfer Protocol) був розроблений для передачі повідомлень електронної пошти від користувача на віддалений сервер для доставки кінцевому отримувачу. Даний протокол забезпечує перенаправлення поштових повідомлень (за допомогою записів MX, або записів програми обміну електронних повідомлень, і записів A, чи записів хоста в системі DNS), форматування поштових повідомлень і встановлення сеансів між поштовими клієнтами і серверами, тоді як POP (поштовий офісний протокол) або IMAP (протокол інтерактивного доступу до електронної пошти) використовуються для отримання цих повідомлень на стороні одержувача.

Поштовий офісний протокол (Post Office Protocol v. 3, POP3)[2]. Концепція поштового сховища - пошта на сервері зберігається тимчасово і в обмеженому обсязі. Користувач періодично звертається до сервера і забирає листа на свій локальний комп'ютер, а оригінали на сервері видаляються.

З метою усунення недоліків протоколу POP3 (зокрема проблеми розсилань повідомлень з різних робочих станцій) був розроблений протокол інтерактивного доступу до електронної пошти InteractiveMailAccessProtocol (IMAP) [3].

Протокол IMAP дозволяє клієнту створювати на поштовому сервері різні папки і розташовувати там повідомлення для зберігання. З'єднання з сервером пошти по протоколу IMAP може встановлюватися з будь-якої робочої станції. Прі цьому користувачі отримують доступ до одних і тих же папок і поштових скриньок. А головне - повідомлення завантажуються в робочу станцію тільки для відображення [4]. Фізичні їх копії продовжують залишатися на сервері в папці, де вони зберігалися до завантаження клієнту. Однак зберігання копій повідомлень на сервері створює певні проблеми для

адміністрування поштової системи, оскільки дисковий простір при цьому досить швидко заповнюється.

Алгоритм роботи модуля перевірки вкладень електронних листів

Алгоритм роботи перевірки вкладень в електронних листах базується на аналізі будь-якого листа з наявними вкладенням, які можуть нести потенційну загрозу як безпеці корпоративній мережі, так і персональному комп'ютеру, на якому дане вкладення може бути відкрито.

Отже, загальний алгоритму перевірки вкладень можна описати наступним чином:

Крок 1. Отримання електронного листа на POP3/IMAP сервері. На ньому відбувається перевірка DKIM підпису електронного листа. В залежності від певних факторів самого листа та його відправника, будуть можливі два варіанта: pass (пройдено) і false (заблоковано). Якщо перевірка пройдена, лист потрапляє далі на перевірку іншими модулями захисту (Крок 2), якщо ні – лист повертається відправнику.

Крок 2. Наступний модуль перевірки, який застосовується – перевірка структури повідомлення на спам (SpamAssasin). В залежності від результату перевірки структура листа залишиться без змін (лист не є спамом) або в заголовок та структуру листа додається повідомлення про те, що лист швидше за все є небажаною кореспонденцією і рекомендовано звернутись до адміністратору пошти (лист є спамом).

Крок 3. Перевірка листа на вкладення. Якщо лист не має будь-яких вкладень то перевірка вкладень не виконується. Перехід до кроку 4.

Крок 3.1. Якщо вкладення присутні, і аналіз вбудованого модуля перевірки вкладень виявив будь-яку загрозу, лист корегується, вкладення видаляється, в заголовку буде вказано що даний лист не пройшов перевірку системою захисту, копія листа буде надіслана адміністратору пошти.

Крок 3.2. Якщо вкладення присутні, і аналіз модуля перевірки вкладень не виявив загрози, відбувається надсилання вкладення на сервіс Virustotal, та отримання результату аналізу. Якщо необхідна кількість антивірусів, яка вказана в скрипті програми виявила вкладення як потенційну загрозу, лист корегується, вкладення видаляється, в заголовку та в тексті листа буде вказано що даний лист не пройшов перевірку системою захисту.

Крок 3.3 Якщо жодний з модулів захисту при перевірці вкладення не виявив його як загрозу, то модуль перевірки вкладень вважається пройденим. Перехід до кроку 4.

Крок 4. Можливість доступу до вкладення електронного листа отримувачу.

Структурна схема роботи розробленого модулю захисту зображена на рисунку 1 .

Висновки

Розроблений модуль перевірки вкладень електронних дозволяє підвищити захищеність користувачів електронної пошти від зовнішніх атак, проаналізувавши кожне вкладення поштової скриньки за допомогою декількох десятків антивірусних програм, на основі перевірки яких базується висновок про безпечність вкладення.

Використання розробленого модулю перевірки суттєво зменшує швидкодію поштового сервісу за рахунок подробного аналізу файлів та дублювання вкладення на кожну з віртуальних середовищ, що є закономірною платою за отриманий рівень захищеності.

Модуль перевірки було перевірено за допомогою наступних засобів :

- « ядро » поштового серверу hMailServer;
- графічний інтерфейс Roundcube WebMail;
- база даних MySQL;
- Операційна система Windows Server 2016 R2.

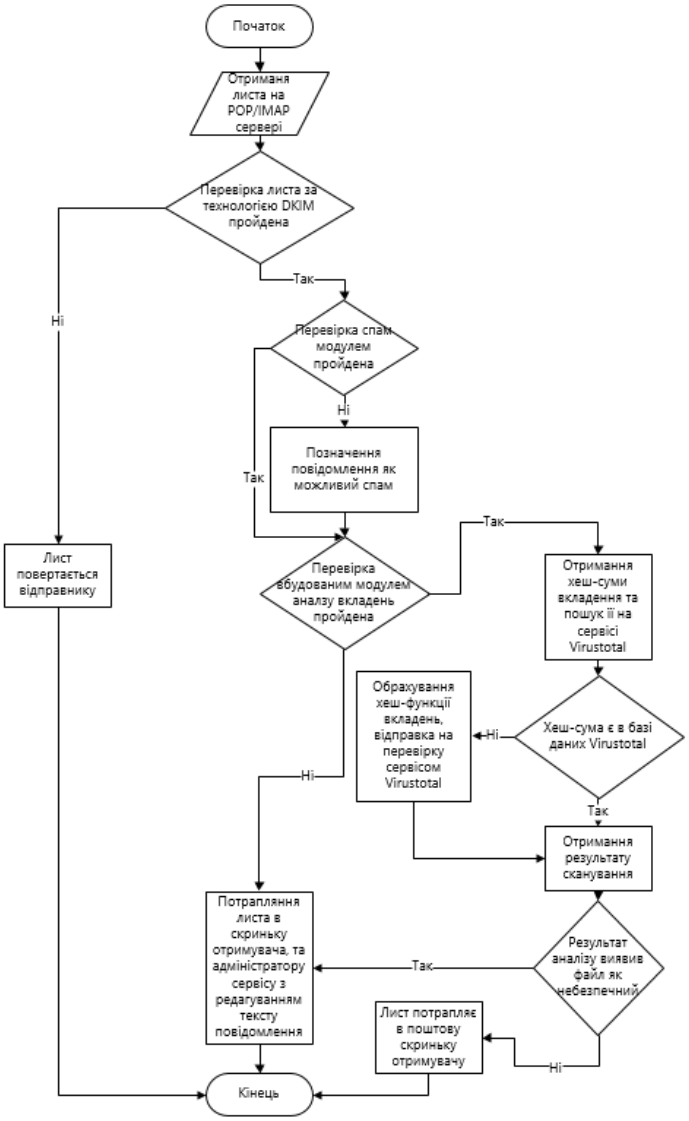

Рисунок 1 – Структурна схема роботи модулю перевірки вхідних листів

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kevin Thomas, Email Architecture, Design, and Implementations, 2nd Edition Kindle Edition, 2017 – 261c.

2. Philip Hazel, The Exim SMTP Mail Server: Official Guide for Release 4/ Philip Hazel, 2003. – 621 c.

3. Philip Hazel, The Mail Transfer Agent: The Mail Transfer Agent 1st Edition, Kindle Edition, 2001 – 624c.

4. John Rhoton, Programmer's Guide to Internet Mail: SMTP, POP, IMAP, and LDAP (HP Technologies)/ John Rhoton, 1999 - 291c.

Іванюк Тарас Володимирович — студент групи УБ-20м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: Ivanyuk.Taras.FMaIS@gmail.com

Азарова Анжеліка Олексіївна − к.т.н., професор каф. МБІС, заст. декана ФМІБ з наукової роботи та міжнародного співробітництва.

Ivanyuk Taras — Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email : e-mail: Ivanyuk.Taras.FMaIS@gmail.com

Azarova Anzhelika A. – PhD in technique, professor, deputy Dean of the Faculty of management and information security by scientific work and international cooperation.