УДК 004.056
DOI: 10.31673/2409-7292.2022.033238

Роде О.О., Лавровський І.М.

ТЕХНОЛОГІЯ ЗАХИСТУ ЕЛЕКТРОННОЇ ПОШТИ ВІД СПАМУ НА ОСНОВІ DMARC

У статті досліджуються питання захисту інформаційно-комунікаційних систем та електронної пошти від небажаного спаму або спам-атак. Приведено теоретичні відомості про спам, та його види. Сформульовано основні технології та способи захисту комунікаційних систем від спаму та спам атак. Розглянуто вплив спаму на діяльність та роботу корпоративної мережі. На практичному прикладі розроблено технологію протидії та показано, як спам може впливати на роботу мережі та яким способом можна захиститись від спам-атак з використанням технології DMARC.

Ключові слова: спам, спам-атака, вразливість корпоративної мережі, DMARC, SPF, DKIM.

Вступ

Захист мережі критично важливий для будь-яких проектів в інтернеті - незалежно від галузі, в якій працює компанія, і розмірів бізнесу. Під прицілом хакера може виявитися будь-яка інформаційно-комунікаційна система, навіть зовсім маленька. Мета зловмисника - заробити гроші, а способів монетизації корпоративних,наприклад, дуже багато.

Щодня надсилається майже 200 мільярдів спаму, що свідчить про приблизний стократний приріст порівняно з 2,4 мільярдами спаму на день у 2021 році. Близько 95 відсотків цих повідомлень надсилаються ботами, зміст яких зазвичай затуманений і неоднозначний. Глобальний обсяг спаму в першій половині 2021 року показує різну кількість перехопленого спаму щотижня. Це коштує компанії величезних технологічних витрат через такі елементи, як кількість обробної потужності сервера електронної пошти, необхідної для подолання потоку, і кількість часу, який повинен витратити персонал IT-служби на боротьбу з проблемою.

Метою даної роботи є дослідження особливо важливих засобів ефективного захисту інформаційних систем від спам атак та розробки технології, для забезпечення ефективного захисту корпоративної мережі.

Види спаму

Реклама. Цей різновид спаму трапляється найчастіше. Деякі компанії рекламують свої товари чи послуги за допомогою спаму. Вони можуть розсилати його самостійно, але частіше замовляють це тим компаніям (чи особам), які на цьому спеціалізуються. Привабливість такої реклами в її порівняно низькій вартості і досить великому охопленню потенційних клієнтів.

Нігерійські листи. Іноді спам використовується для того, щоб виманити гроші в одержувача листа. Найпоширеніший спосіб одержав назву «нігерійські листи», тому що дуже багато таких листів приходило з Нігерії.

Фішинг. В цьому разі спамер намагається виманити в одержувача листа номер його кредитних карток чи паролі доступу до систем онлайнових платежів тощо. Такий лист, зазвичай, маскується під офіційне повідомлення від адміністрації банку.

Розсилання листів **релігійного змісту**.

Масове розсилання для **виведення поштової системи з ладу** (Відмова сервісу).

Масове розсилання **від імені іншої особи**, з метою викликати до неї негативне ставлення.

Масове розсилання листів, що містять **комп'ютерні віруси** (для їхнього початкового поширення).

Шкідливі веб посилання. Посилання, також відомі як URL-адреси, поширені в електронних листах загалом, а також у фішинг-листах. Шкідливі посилання перенаправлять користувачів на веб-сайти-самозванці або на сайти, заражені шкідливим програмним забезпеченням, також відомим як шкідливе програмне забезпечення.

Шкідливі вкладення. Вони виглядають як законні вкладення файлів, але насправді заражені шкідливим програмним забезпеченням, яке може скомпрометувати комп'ютери та файли на них. У випадку з вимогами – різновидом шкідливих програм – усі файли на ПК можуть стати заблокованими та недоступними. Або можна встановити реєстратор натискань клавіш для відстеження всього, що вводить користувач, включаючи паролі.

Можливості щодо захисту електронної пошти на основі DMARC

DMARC вводить нові можливості у світ електронної пошти і спрямований на вирішення проблеми, яка мучить електронну пошту з самого початку: Не існує надійного способу визначити, чи є електронна пошта справжньою чи просто справді гарною підробкою. Основні технології, які пов'язують домен з електронною поштою, існують вже давно, і люди намагалися з усіх сил у різних контекстах, щоб зробити ці технології корисними.

SPF – це спосіб публікації списку серверів, яким дозволено надсилати електронну пошту від імені домену – існує з 2003 року.

DKIM – метод додавання захищеної від втручання доменної печатки до частини електронної пошти – існує з 2005 року

DMARC об'єднує послідовність налаштування цих існуючих технологій, щоб при отриманні частини електронної пошти можна було виконати просту перевірку, чи справді електронна пошта надходить із домену, про який вона повідомляє, що надходить.

Основні принципи роботи DMARC

Щоб зробити всі електронні листи домену легкими для ідентифікації, DMARC надає власникам доменів уявлення про те, як їх домени використовуються в Інтернеті. Ця видимість надається у формі звітів про зворотний зв'язок, які створюються організаціями, які обробляють вхідну пошту.

DMARC базується на двох існуючих технологіях, які використовуються для асоціювання частини електронної пошти з доменом. SPF, що розшифровується як Sender Policy Framework, і DKIM, що позначає DomainKeys Identified Mail, працюють різними, але взаємодоповнюючими способами, щоб створити зв'язок між електронною поштою та доменом.

SPF та DKIM – це окремі технології, які існують вже багато років і можуть використовуватися незалежно від DMARC. Самі по собі SPF та DKIM можуть пов'язати електронну пошту з доменом. Мовою DMARC SPF та DKIM генерують «автентифіковані ідентифікатори». DMARC намагається пов'язати результати SPF та DKIM - автентифікованих ідентифікаторів із вмістом електронної пошти: конкретно з доменом, знайденим у заголовку електронної пошти «Від кого».

Рис. 1. SPF та DKIM ідентифікатори

Домен, знайдений у заголовку електронної пошти «Від кого» це сутність, яка пов'язує всю обробку DMARC. Зараз, оскільки кожен може придбати домен і поставити SPF і DKIM на робочу систему (включаючи злочинців!), Результати обробки SPF і DKIM - тобто автентифікованих ідентифікаторів – повинні бути пов'язані з доменом, який знаходиться в заголовку «Від кого» ,який в свою чергу пов'язаний з DMARC. Ця концепція називається «вирівнювання ідентифікатора». Отримання ідентифікаторів для вирівнювання закінчується великою частиною роботи з розгортання DMARC.

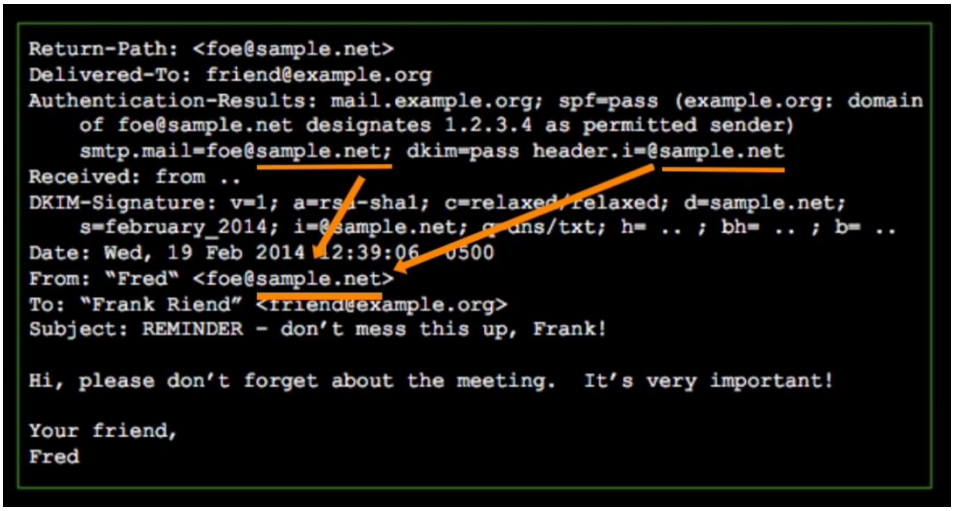

Рис. 2. Метод «вирівнювання ідентифікатора»

Щоб зробити можливим для когось, хто володіє доменом електронної пошти, точно розгортати SPF та DKIM, DMARC описує, як можна надіслати відгук власнику домену щодо того, як їх електронний домен використовується в Інтернеті.

Переваги технології DMARC

DMARC – це не продукт, це швидше доступна технічна специфікація, яка додає нові функції до електронної пошти. Зараз DMARC широко підтримується в Інтернеті, що дозволяє кожному, хто володіє доменом електронної пошти, скористатися перевагами функцій DMARC. Коли люди говорять про розгортання DMARC, вони говорять про: використання функцій DMARC для виявлення всіх законних джерел електронної пошти, впевненість що кожне, або окреме джерело надсилає електронні листи, що відповідають методу DMARC, оприлюднення звіту про те, що кожне, або окреме джерело відповідає стандартам DRARC, та його можна використовувати по всьому світу

Приклад роботи DMARC

Отже, DMARC працює за технікою «Вирівнювання ідентифікатора» результатів SPF та DKIM. І щоб більш наглядно зрозуміти як це працює, потрібно навести приклади різних комбінацій автентифікованих ідентифікаторів з метою продемонструвати, чому вирівнювання ідентифікаторів важливо з точки зору одержувача електронної пошти.

У першому прикладі (рис. 3) одержувач електронної пошти отримав електронний лист, де домен DMARC (тобто домен, що міститься в заголовку «Від кого») – «bank.com». Крім того, перевірка SPF дала домен «bank.com». На електронному листі не було підпису DKIM, тому наш рядок позначено як «немає». Одержувач електронної пошти шукає будь-який позитивний сигнал про те, що електронну пошту можна простежити до домену «bank.com», і одержувачу електронної пошти байдуже, чи надходить цей сигнал від SPF або DKIM – головне, що сигнал є. У цьому прикладі автентифікованим ідентифікатором, який надійшов від SPF, було «bank.com», що точно відповідає домену DMARC, тому електронна пошта відповідає DMARC.

From:	SPF	DKIM
bank.com	bank.com	(none)

Рис. 3 Позитивна перевірка листа через SPF

У наступному прикладі (рис. 4) все майже однаково, за винятком того, що автентифікований ідентифікатор, який надав SPF, є субдоменом bank.com - mail.bank.com. Для людини, що є необізнаною, ці два домени очевидно пов'язані. Однак виявляється, що в Інтернеті не існує стандартного способу з'ясувати, чи bank.com - це домен верхнього рівня, наприклад .com або .org, або домен другого рівня. Використовуючи деякі ресурси з Інтернету, зокрема список публічних суфіксів, який веде Фонд Mozilla, одержувач електронної пошти може з'ясувати цей банк. com - це організаційний домен, а mail.bank.com - це субдомен, який використовує той самий організаційний домен, що і bank.com. У цьому випадку електронна пошта відповідає DMARC.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)

Рис. 4. Автентифікований ідентифікатор є субдоменом

Третій приклад (рис. 5) показує, що замість того, щоб SPF надав автентифікований ідентифікатор bank.com або субдомен bank.com, автентифікованим ідентифікатором є banknewsletter.com. Наскільки нам відомо, banknewsletter.com - це реальний домен, який належить і управляється тим самим суб'єктом, який володіє bank.com. АБО banknewsletter.com належить і управляється злочинцями, які хочуть обдурити людей, щоб вони думали, що вони законні. Немає способу надійно підтримувати та передавати такі асоціації між доменами – або самими відправниками, які створюють бази даних асоціацій, або одержувачами, що підтримують свої власні – і те, і інше є завданнями, які можуть бути чреватими неточностями і в основному підривати корисність DMARC. Отже, цей електронний лист НЕ відповідає DMARC і на нього впливає політика DMARC.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)

Рис. 5. Неточність в адресі відправника

В четвертому прикладі, (рис. 6) електронна пошта така сама, за винятком того, що ми вперше бачимо підпис DKIM. У цьому прикладі DKIM створив автентифікований ідентифікатор bank.com, що робить приклад сумісним із DMARC. Тобто отримувач електронної пошти переглядає автентифікований ідентифікатор, який надійшов від SPF, і бачить, що banknewsletter.com не має нічого спільного з bank.com, і просто ігнорує його. Оскільки приймач шукає будь-який позитивний сигнал про те, що повідомлення

справді надійшло від bank.com, а DKIM надає такий сигнал, електронне повідомлення проходить перевірку DMARC.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com		bank.com

Рис. 6. Позитивна перевірка листа через DKIM

В п’ятому прикладі (рис 7) показує електронну пошту, яка повністю відповідає DMARC. І SPF, і DKIM дали автентифіковані ідентифікатори bank.com. Приймач піклується лише про пошук позитивного сигналу, тому наявність 2 позитивних сигналів подвійно хороший, але не означає нічого більше, ніж «позитивний сигнал».

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com

Рис. 7. Повна відповідність DMARC

Цей 6-й приклад (рис. 8) показує те саме що і приклад на рисунку 3.5, з тією різницею, що “news.bank.com” є автентифікованим ідентифікатором як для SPF, так і для DKIM. Це досить поширена практика для великих організацій делегувати субдомен провайдеру послуг електронної пошти, щоб постачальник послуг міг надсилати електронні листи від імені організації. У цьому прикладі власники bank.com могли делегувати субдомен «новини» своєму постачальнику маркетингу, щоб він міг надіслати електронний лист, сумісний з DMARC, за допомогою bank.com.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com
bank.com	news.bank.com	news.bank.com

Рис. 8. Домен та субдомен

Цей вигаданий приклад (рис. 9) показує, що кожен може зареєструвати домени та встановити SPF та DKIM. Те, що SPF та DKIM передають і видають автентифікований ідентифікатор, ще не означає, що з електронною поштою все добре.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com
bank.com	news.bank.com	news.bank.com
bank.com	crime.net	badguys.com

Рис. 9. Вигаданий приклад електронної пошти

Останній приклад (рис. 10) показує, що SPF дав автентифікований ідентифікатор «bark.com». Це добре відома атака, яку деякі шахраї використовують для обману людей, які вручну перевіряють шматки електронної пошти для визначення законності. Швидкий погляд може обдурити око і змусити когось подумати, що відправник насправді є банком. Гірше того, можна скористатися деякими прийомами кодування символів, щоб відтворені гліфи виглядали точно так, як відображається домен. Але машину таким способом обхитрити не вийде.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com
bank.com	news.bank.com	news.bank.com
bank.com	crime.net	badguys.com
bank.com	bark.com	(none)

Рис. 10. Підробка способом «схожого слова»

Як DMARC формує звіти

Коли одержувач електронної пошти обробляє шматок електронної пошти в контексті DMARC, одержувач витягує домен, знайдений у заголовку «Від кого». Цей домен лежить в основі того, де приймач шукає будь-який відповідний запис DMARC. Приймач ляпає префікс underbar-dmarc домену і запитує DNS для запису TXT. У наведеному тут прикладі витягнутим доменом є EUROPE.ENG.EXAMPLE.ORG. Одержувач додасть underbar-dmarc до цього домену та запитує DNS, щоб спробувати знайти запис TXT. Якщо запит відхилено або

нічого не знайдено, то одержувач витягує організаційний домен із домену. В нашому випадку EXAMPLE.ORG і повторює спробу знайти запис DMARC, додаючи under-dmarc перед доменом і запитуючи запис TXT.

Рис. 11. Покриття субдоменів за допомогою одного домену

Записи DMARC – це прості списки пар тегів / значень. Це приклад домену, який опублікував запис DMARC. Ми точно можемо сказати що це DMARC-запис, оскільки він починається з «v = DMARC1;». Він має політику ap = none та просить надіслати всі зведені звіти на основі XML до report@example.org для обробки. DMARC був розроблений, щоб дозволити доменам збирати інформацію, не впливаючи на електронну пошту, і саме так це робиться – «вмикаючи» політику ap = none.

Усі записи DMARC повинні починатися з тегу версії протоколу. Після цього політику можна налаштувати. Можна налаштувати політику, яка застосовуватиметься до будь-яких субдоменів, наприклад: якщо ви знаєте, що ваш домен ніколи не використовує піддомени, ви можете задати політику sp = reject, збираючи дані лише у вашому організаційному домені, використовуючи p = none. Тег pct схожий на повзунок, який переходить від 0 до 100, так що будь-яка опублікована політика може бути розгорнута повільно, наприклад: якщо ви задасте pct = 1, тоді лише на 1 із кожних 100 електронних листів вплине політика DMARC. Останні теги стосуються налаштування форматів звітів, інтервалів та часу надсилання відредагованих копій окремих електронних листів, які не відповідають DMARC.

Висновки

У статті розібрано як працює ефективна технічна специфікація DMARC. Наведені плюси та мінуси даного виду захисту від спаму, а також показано як формуються звіти для детального аналізу. Дані рекомендації можуть бути використані системними адміністраторами та адміністраторами безпеки при налаштуванні системи захисту корпоративних webресурсів або звичайними користувачами при налаштуванні домашньої системи захисту.

Варто зазначити, що створені рекомендації не дають стовідсоткової гарантії забезпечення необхідного рівня безпеки інформації. Створені рекомендації дозволяють збільшити тривалість проведених атак, а також унеможливити успішність атаки у випадку обмеженості технічних ресурсів порушника.

Перелік посилань

1. «Основы веб-хакинга. Нападение и защита» / Юрій Жуков // Видавнитство – Пітер. 2012 - 208с

2. «Безпека веб сайтів або зворотній відлік до злому». [Електронный ресурс] – Режим доступу: World Wide Web. – URL: filandor.com

3. Список інструментів технічної специфікації DMARC

4. DMARC – загальні відомості [Електронный ресурс] – режим доступу: World Wide Web. – URL: wikipedia.com

4. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 р. № 851-IV;

5. Закон України "Про захист інформації в автоматизованих системах"

6. Інформаційна сторінка технології DMARC. [Електронный ресурс] – Режим доступу: World Wide Web. – URL: dmarcian.com

7. «Anti-Spam Measures: Analysis and Design» [Книга] / Guido Schryen

Надійшла: 26.08.2022 Рецензент: д.т.н., професор Кожухівський А.Д.