ИПМ им.М.В.Келдыша РАН

Абрау-2024 • Труды конференции

Г.М.Михайлов, А.М.Чернецов

Обзор технологий обеспечения безопасности и защиты систем электронной почты в научной организации

Рекомендуемая форма библиографической ссылки

Михайлов Г.М., Чернецов А.М. Обзор технологий обеспечения безопасности и защиты систем электронной почты в научной организации // Научный сервис в сети Интернет: труды XXVI Всероссийской научной конференции (23-25 сентября 2024 г., онлайн). — М.: ИПМ им. М.В.Келдыша, 2024. — С. 217-222.
https://doi.org/10.20948/abrau-2024-14
https://keldysh.ru/abrau/2024/theses/14.pdf

Видеозапись выступления

Презентация к докладу

Обзор технологий обеспечения безопасности и защиты систем электронной почты в научной организации

Г.М. Михайлов, А.М. Чернецов

ФИЦ ИУ РАН

Аннотация. В работе представлен обзор современных технологий, применяемых при обработке почтовых сообщений, проведено их описание. Приведены рекомендуемые настройки для успешного функционирования.

Ключевые слова: e-mail, SPF, DMARC, DKIM.

Review of technologies for ensuring security and protection of email systems in a scientific organization

G.M. Mikhaylov, A.M. Chernetsov

FRC CSC RAS

Abstract. The paper provides an overview of modern technologies used in processing mail messages and describes them. Recommended settings for successful operation are provided.

Keywords: e-mail, SPF, DMARC, DKIM.

Архитектура электронной почты в Интернете состоит из «мира пользователей» в виде почтовых агентов (Message User Agent, MUA) и «мира передачи» в виде службы обработки сообщений (Message Handling Service, MHS), состоящей из агентов пересылки сообщений (Message Transfer Agent, MTA).

Задача обеспечения защиты электронной почты от спама (spam) стоит уже много десятилетий [1]. Технологий для решения этой задачи придумано великое множество. Последнее десятилетие также характеризуется ростом фишинговых атак (интернет-мошенничество для достижения идентификационных данных пользователей).

1. Обзор некоторых существующих технологий получения доверенной электронной почты

В [2] введено применение ряда протоколов для решения задачи получения доверенной электронной почты. Для этого описаны и рекомендованы к применению следующие протоколы и стандарты:

- *STARTTLS:* расширение безопасности SMTP, позволяющее клиенту и серверу SMTP договориться об использовании TLS (Transport Layer Security) для того, чтобы наладить закрытый обмен данными с аутентификацией по Интернету.
- *S/MIME (Secure Multipurpose Internet Mail Extensions)*: обеспечивают аутентификацию, целостность, невозможность отказа (nonrepudiation, посредством цифровых подписей) и конфиденциальность (посредством шифрования) сообщений SMTP.
- *DANE (DNS-Based Authentication of Named Entities)*: предназначен для исправления недостатков системы *центров сертификации* (CA) за счет создания альтернативного канала аутентификации открытых ключей на основе DNSSEC. В результате те же самые отношения доверия, которые используются для сертификации IP-адресов, используются для сертификации серверов, работающих по этим адресам.

SPF (Sender Policy Framework)[3]: позволяет владельцу домена указать IP-адреса MTA, уполномоченных отправлять почту от имени домена. SPF использует DNS для того, чтобы владельцы доменов могли создавать записи, связывающие доменное имя с конкретным диапазоном IP-адресов или уполномоченных MTA. Получатель просто сличает *текстовую запись* SPF (типа TXT) в DNS, чтобы проверить, имеет ли право предполагаемый отправитель сообщения использовать такой исходный адрес. Почта, поступающая не с уполномоченных IP-адресов, может отбрасываться.

- *DKIM* (*DomainKeys Identified Mail*)[4]: позволяет «акторам» электронной почты (авторам или операторам) надежно приписать к сообщению свое доменное имя с помощью криптографических методов, чтобы механизмы фильтрации могли выработать точную репутацию домена. MTA могут подписывать выбранные заголовки и тело сообщения. Такая подпись подтверждает исходный домен письма и обеспечивает целостность тела сообщения.
- DMARC *(Domain-based Message Authentication, Reporting, and Conformance)*[5]: публикует требование того, чтобы доменное имя автора было аутентифицировано по DKIM и/или SPF, чтобы владелец домена затребовал от получателя обработку неаутентифицированной почты с помощью этого домена, а также механизм отчетности для отправки

отчетов от получателей владельцам доменов. DMARC сообщает отправителям о пропорциональной эффективности их политик SPF и DKIM, а также сигнализирует получателям, какие действия нужно предпринять в различных ситуациях индивидуальных и массовых атак.

Остановимся подробнее на особенностях трех технологий – SPF, DKIM и DMARC. С остальными технологиями можно ознакомиться в работе [6].

Наличие SPF снижает вероятность попадания письма в спам при приеме почтового сервера адресата. Важно помнить, что SPF - запись может быть только одна для одного почтового домена. В рамках одной SPF может быть несколько записей серверов.

Использование SPF решает следующую проблему: в нынешней инфраструктуре электронной почты любой хост может поставить любое доменное имя в любой идентификатор в заголовке письма: не требуется, чтобы хост ставил обязательно имя домена, где он сам находится. SPF заставляет почту идти по определенному пути и ломается, когда легитимная почта отклоняется от этого пути – в частности, когда сообщение проходит через список рассылки.

Подпись DKIM добавляется в служебные заголовки письма и не видна для пользователя. DKIM использует два ключа шифрования - открытый и закрытый [7]. С помощью закрытого ключа формируются заголовки для всей исходящей почты, а открытый ключ как раз добавляется в DNS в виде записи типа TXT. Подпись создается автоматически в MTA – т.е. SMTP-сервером [8].

Проверка DKIM происходит автоматически на стороне получателя. Если домен в письме не авторизован для отправки сообщений, то письмо может быть помечено как «***подозрительное»*** или помещено в спам в зависимости от политики получателя.

Технология DMARC (аутентификация сообщений, предоставление отчётов и проверка соответствия на базе доменного имени) помогает помечать «***подозрительными***» сообщения по принципу наличия записей SPF и DKIM. DMARC - это подпись, которая позволяет принимающему серверу решить, что делать с полученным письмом. DMARC использует DKIM и SPF. Если отправленное сообщение не прошло проверку DKIM и SPF, то оно не пройдет и DMARC. Если же сообщение успешно прошло хотя бы одну проверку (DKIM или SPF), то и проверку DMARC сообщение пройдет успешно.

2. Настройка для ВЦ ФИЦ ИУ РАН

В 2023 году Минобрнауки издало распоряжение по подведомственным организациям о необходимости использования технологий SPF, DKIM и DMARC вместе для почтовых серверов (Письмо

Минобрнауки России от 17 августа 2023 г. № МН-19/634 «О направлении типовых рекомендаций»). Соответственно сервера ВЦ ФИЦ ИУ РАН были перенастроены с использованием указанных технологий.

В указанном выше письме приводились настройки для почтовых серверов Postfix, Exim и Exchange. К сожалению, для распространенного почтового сервера Sendmail настроек не приводилось. В ВЦ ФИЦ ИУ РАН почтовый домен ccas.ru работает на Sendmail 8.13.6 на ОС Solaris 10, в качестве SMTP-сервера с 2017 г. используется Sendmail 8.14.4 на ОС CentOS [9].

Для SPF сделаны следующие настройки: отправка реализуется со всех MX-серверов с явно прописанными адресами SMTP-серверов. Для всех остальных адресов стоит запрет.

Для DKIM, как уже указано выше, необходимо создать для домена пару открытый/закрытый ключ. Открытый ключ публикуется в DNS. Все сообщения автоматически подписываются с использованием закрытого ключа. В силу недоступности в РФ в 2023 году репозитория для ОС Solaris провести установку пакета openDKIM не удалось, поэтому наши работы ограничились проведением всех настроек только на SMTP-серверах на базе CentOS. В качестве электронной подписи (ЭП) использовалась запись с ключом длиной 1024 бит.

Настройка для DMARC в нашем случае сводится к созданию единственной записи - отчёты с адресом отправления электронной почты dmarc@frccsc.ru. Если поставить жесткие условия на почту, то возможны ложные отказы в приеме нужной почты, что в нашем случае научной организации неприемлемо. В других случаях можно, например, настроить непрохождение проверки, как отказ в приеме письма.

3. Заключение

В данной работе представлены настройки записей для почтового сервера научной организации. Конечно, к сожалению, использование описанных механизмов не дает полной гарантии доверия к доставляемой корреспонденции, но уровень доверия при их использовании может быть повышен.

Литература

1. Копытов М.А., Рогов Ю.П. Электронная почта. Администрирование и проблемы надежности. Тезисы доклада в сборнике Всероссийской научной конференции "Научный сервис в сети Интернет"

(г.Новоросийск, 23-28 сентября 2002 года). – М.: Изд-во МГУ, 2002. – С. 128-129.
2. National Institute of Standards and Technology, “Trustworthy Email,” NIST Special Publication 800-177, September 2016.
3. SPF RFC. — https://datatracker.ietf.org/doc/html/rfc7208
4. DKIM HomePage — https://www.dkim.org/
5. DMARC HomePage: — https://dmarc.org/
6. У. Столингс “Всеобъемлющая безопасность электронной почты в Интернете” (пер. с. англ.)// Интернет изнутри, 2018, №10 URL: https://ii.org.ru/vseobemlyushhaya-bezopasnost-yelektron/
7. National Institute of Standards and Technology, “Introduction to Public Key Technology and the Federal PKI Infrastructure,” NIST Special Publication 800-32, February 2001.
8. Г.М. Михайлов, Ю.П. Рогов, А.М. Чернецов. Организация внешнего почтового smtp-сервера в научной организации // Научный сервис в сети Интернет: труды XVII Всероссийской научной конференции (21–26 сентября 2015 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2015. — С. 237–239.
9. Михайлов Г.М., Жижченко М.А., Чернецов А.М. Обеспечение плавной перенумерации сети при смене провайдера // Научный сервис в сети Интернет: труды XIX Всероссийской научной конференции (18-23 сентября 2017 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2017. —С. 351-355.

References

1. Kopytov M.A., Rogov Iu.P. Elektronnaia pochta. Administrirovanie i problemy nadezhnosti. Tezisy doklada v sbornike Vserossiiskoi nauchnoi konferentsii "Nauchnyi servis v seti Internet" (g.Novorosiisk, 23-28 sentiabria 2002 goda). – M.: Izd-vo MGU, 2002. – C. 128-129.
2. National Institute of Standards and Technology, “Trustworthy Email,” NIST Special Publication 800-177, September 2016.
3. SPF RFC. — https://datatracker.ietf.org/doc/html/rfc7208
4. DKIM HomePage — https://www.dkim.org/
5. DMARC HomePage: — https://dmarc.org/
6. U. Stolings “Vseobieemliushchaia bezopasnost elektronnoi pochty v Internete” (per. s angl.) // Internet iznutri, 2018, №10 URL: https://ii.org.ru/vseobemlyushhaya-bezopasnost-yelektron/
7. National Institute of Standards and Technology, “Introduction to Public Key Technology and the Federal PKI Infrastructure,” NIST Special Publication 800-32, February 2001.

8. G.M. Mikhailov, Iu.P. Rogov, A.M. Chernetsov Organizatsiia vneshnego pochtovogo smtp-servera v nauchnoi organizatsii // Nauchnyi servis v seti Internet: trudy XVII Vserossiiskoi nauchnoi konferentsii (21–26 sentiabria 2015 g., g. Novorossiisk). — M.: IPM im. M.V.Keldysha, 2015. — S. 237–239.
9. Mikhailov G.M., Zhizhchenko M.A., Chernetsov A.M. Obespechenie plavnoi perenumeratsii seti pri smene provaidera // Nauchnyi servis v seti Internet: trudy XIX Vserossiiskoi nauchnoi konferentsii (18-23 sentiabria 2017 g., g. Novorossiisk). — M.: IPM im. M.V.Keldysha, 2017. —S. 351-355.