Визитка

МИХАИЛ ВЫЧИЖАНИН, сетевой инженер компании «СПАМОРЕЗ»

Как защитить электронную почту?
Методы и системы фильтрации*

Сегодня никого не удивишь разнообразием проблем, связанных с электронной почтой, с которыми сталкиваются как пользователи, так и сисадмины. Разработано немало средств, которые способны эффективно бороться с фильтрацией нежелательной корреспонденции. Что принципиально нового можно предложить в этом направлении?

Технические аспекты реализации эффективной защиты

Рассмотрим структуру системы, отвечающей требованиям отказоустойчивости, надежности, масштабируемости и защищенности, при этом эффективно справляющейся со своей основной задачей по фильтрации электронной почты:

- Алгоритмы/механизмы/методы фильтрации:
  - Защита и оптимизация доставки трафика на уровне SMTP-сессии.
  - Анализ SMTP-протокола, защита от SMTP-DDoS.
  - SMTP-таймауты.
  - Серые списки (greylisting).
  - Черные и белые списки.
  - Фишинг-проверка (Phishing Check).
  - Географические списки (Geographical blacklisting).
  - DNSBL-списки (DNS blacklisting).
  - SPF-технология (Sender Policy Framework).
  - DCC-технология (Distributed Checksum Clearinghouse).
  - Razor-технология (Spam signature database Vipul's razor).
  - Эвристический анализ (Spam heuristics).
  - DKIM-технология (DomainKeys Identified Mail).
  - Проверка гипертекстовых ссылок (Spam URL check).
  - Ключевые слова (Spam keyword).
  - Обратная зона (Reverse DNS zone).
  - Байесовская классификация (Spam Bayesian Classifier).
  - Поверхностный анализ тела письма (Light spam structure check).
  - Глубокий анализ тела письма, лингвистический и сигнатурный анализ.
  - Анализ истории.
- Инфраструктура. Многоуровневость и иерархичность системы – ключ к правильному ее построению:
  - Площадки фильтрации в различных ЦОД. Доставка и перенаправление писем на площадку в зависимости от критериев: BGP (можно использовать anycast), средняя и текущая нагрузка площадки, географическая близость.
  - Площадка фильтрации, представленная облачным хостингом со всеми преимуществами облаков. Гибкая масштабируемость ресурсов (процессор, память) в зависимости от нагрузки, плавная и прозрачная миграцией внутри облака между серверами виртуализации с синхронизацией состояний памяти, дисков и процессоров.
  - МультиЦОД. Синхронизация данных между площадками в режиме реального времени для обеспечения равномощности и идентичности критериев обработки.
  - Многоуровневая фильтрация на уровне площадки выделенного ЦОД. Распределение различных алгоритмов и методов по определенным участкам площадки. При этом самые «тяжелые» методы необходимо применять на последних этапах фильтрации в фильтрах тонкой очистки, и, наоборот, методы, отсеивающие корреспонденцию на 80-90%, использовать как фильтры грубой очистки.
- Предоставление клиенту методов оценки качества предоставляемых услуг. Использование соглашения об уровне предоставления услуг (SLA). Критериями для определения KPI могут выступать параметры:
  - Соотношения: спам, отброшенный спам и маркированный спам.
  - Ложные срабатывания.
  - Среднее время прохождения письма через систему.
  - Среднее время отклика системы.
  - Средняя пропускная способность.
  - Средняя доступность, выраженная как среднее число сбоев на период предоставления сервиса.
- Возможность мониторинга, автоматическая/автоматизированная система, позволяющая оперативно реагировать на инциденты внутри системы.
- Наличие службы техподдержки, позволяющей взаимодействовать с клиентами и реагировать на их запросы (примерами могут служить обновление белых списков, трекинг сообщений в системе), а также иные обращения, связанные с усовершенствованием системы.

- Наличие аналитической службы (анализ трендов и новых направлений в массовых рассылках, а также разработка методов их распознавания и фильтрации).

Как показывает практика, совокупность этих методов, позволяет эффективно бороться со спамом и обрабатывать при этом большие объемы данных. Ясно, что нельзя пользоваться только одним инструментом по защите от спама, инструментов и методов должно быть несколько и при этом каждый метод необходимо использовать только на выделенном участке фильтрации в определенной последовательности или даже зависимости. Универсальных решений не существует.

СПАМОРЕЗ – сервис для защиты электронной почты

Хотелось бы обратить внимание читателя на систему защиты почтового трафика СПАМОРЕЗ. Она разрабатывается и продвигается с 2005 года, насчитывает большую клиентскую аудиторию и постоянно развивается. Среди основных результатов можно выделить полное соответствие той модели эффективно функционирующей системы, которая была представлена в предыдущем пункте. СПАМОРЕЗ – это комплексная защита почтового трафика от различных видов ИТ-угроз. Решение представляет собой SaaS-сервис, легко интегрирующийся с различными почтовыми системами, он может быть легко включен в почтовую систему небольших, средних и крупных компаний. СПАМОРЕЗ позволяет:

- Определять и блокировать спам, вирусы, фишинг-, фарминг-, скамминг- и bounce-сообщения.
- Защищать от атак на SMTP.
- Определять и блокировать вредоносные коды во вложениях писем.
- Корректно обрабатывать большинство известных типов архивов.
- Изолировать зараженные объекты и спам в карантине.
- Вести статистику, учитывающую аспекты работы системы.
- Логировать почтовые сообщения по требованию клиента.
- Информировать клиента об инцидентах.

Ключевым моментом структуры системы является ее конфиденциальность. Технологии, реализованные в СПАМОРЕЗе, позволяют обеспечить надежность и сохранность почтовой переписки клиентов. Данные моменты юридически закрепляются в договоре на оказание услуг фильтрации.

Преимущества СПАМОРЕЗА:

- Высокое качество защиты электронной почты.
- Уровень распознавания спама 99,99%.
- Возможность подключения неограниченного количества почтовых ящиков и доменов.
- Масштабируемость.
- Высокая производительность и стабильность работы.
- Снижение общих затрат на обеспечение безопасности электронной почты.
- Гибкость настроек и удобство администрирования.
- Простота подключения и интеграции в существующую почтовую инфраструктуру.
- Журнал сообщений, журнал очередей.
- Персональный карантин и хранение на мощностях СПАМОРЕЗа.
- Персональные правила фильтрации на уровне учетной записи, домена, конечного почтового ящика.
- Гибкие тарифные планы, в том числе и бесплатные.
- Бесплатное двухнедельное тестирование.
- Техническая поддержка по телефону и e-mail, а также выделение персонального менеджера.

Гибкость СПАМОРЕЗа проявляется еще в различных режимах подключения. Несмотря на основной режим подключения по модели SaaS, существует возможность обслуживания клиента на выделенном, персонально закрепленном за этим клиентом сервере в ЦОД СПАМОРЕЗа, а также установки системы фильтрации уже в ЦОД клиента.

Подробную информациию вы всегда можете получить, пройдя по следующей ссылке: http://www.spamorez.ru.

Стоимость решений

Что эффективнее с точки зрения бизнеса: использовать сервис по фильтрации или приобретать специализированное ПО и оборудование? По мнению разработчиков СПАМОРЕЗа, фильтрация почтового трафика по модели SaaS сегодня наиболее эффективное и в то же время дешевое решение для компаний разного уровня. И выгоды очевидны:

- Экономия на покупке дорогостоящего оборудования, лицензионного программного обеспечения.
- Экономия на внедрении и постоянном обслуживании.
- Внедрение системы фильтрации занимает 10 минут, а обслуживание и профессиональная техническая поддержка включена в стоимость услуги.
- Нет необходимости изменять корпоративную почтовую инфраструктуру, SaaS-сервис легко интегрируется с любой почтовой системой, установленной у клиента.
- Гарантия бесперебойной работы, исключение времени простоя на починку или замену оборудования, т.к. система построена по «облачной» технологии. Все оборудование расположено в профессионально оборудованных ЦОДах. ЦОДы находятся под круглосуточной охраной, резервным электропитанием и резервными каналами доступа в Интернет.
- Значительная экономия входящего трафика, т.к. до 90% спама до конечного пользователя не доходит и «оседает» на серверах поставщика услуги.
- Не требуется специальных знаний для управления системой фильтрации, все управление осуществляется через интуитивно понятный веб-интерфейс.

Перспективы

Спам рентабелен для рекламодателя или клиента спамера. Компании готовы платить деньги за рассылки, несмотря на фильтрацию, доставку всего 1% рекламной корреспонденции и минимальную реакцию конечных корреспондентов, получивших спам. Ваша компания имеет название, товарный знак, домен, почту? Значит, проблема фильтрации спама вас не миновала. Как ваша компания борется или планирует бороться с такой корреспонденцией? Посчитайте ваши затраты на эту борьбу, время системных администраторов и сотрудников, впустую используемые ресурсы оборудования, загрузку каналов связи, трафик. С большой вероятностью ваша компания несет убытки. В независимости от того, на каком этапе вы находитесь: используете электронную почту для вашей компании или только планируете, СПАМОРЕЗ рекомендует доверять фильтрацию спама только профессионалам – это будет существенно дешевле, качественнее и надежнее. EOF

** На правах рекламы*