McAfee Email Protection

Передовое средство защиты почтовых ящиков, работающее всегда и везде

Ключевые преимущества

Защита от целенаправленных фишинговых атак

- Обнаружение вредоносных URL-адресов в режиме реального времени с помощью ClickProtect
- Интеграция с McAfee Advanced Threat Defense для защиты от скрытых вредоносных программ
- Встроенная технология предотвращения утечки данных

Обеспечение безопасности почтовых ящиков на сторонних серверах

- Защита от целенаправленных атак независимо от маршрута электронного сообщения
- Пользовательские средства управления «серой» почтой
- Непрерывный доступ к электронной почте
- Детально настраиваемые функции предотвращения утечки данных и шифрования данных

Гибкие варианты развертывания

- Развертывание в полном соответствии с потребностями организации
- Возможен гибридный вариант развертывания с единой консолью для управления защитой и генерирования отчетов

Потребность компаний в передовых средствах защиты электронной почты сегодня как никогда высока. По данным SANS Institute, 95 % сетевых атак являются прямым результатом успешно проведенного целенаправленного фишинга.[1] Пользователи по-прежнему «клюют» на социотехнические приемы, а киберпреступники расширяют набор используемых ими методов, позволяющих застать врасплох даже организации, уделяющие большое внимание обеспечению собственной безопасности. Вредоносные программы повышенной сложности и утечка корпоративной интеллектуальной собственности становятся серьезными проблемами, чреватыми огромными негативными последствиями для любой организации. Кроме того, в последнее время компании начинают переходить к использованию почтовых ящиков, размещенных на сторонних серверах, что тоже может приводить к повышению уровня риска. Наконец, поиск лучшей альтернативы может быть мотивирован недостаточной свободой выбора, которую предоставляют прежние решения для защиты электронной почты. McAfee® Email Protection позволяет справиться с этими проблемами. Это эффективное решение обеспечивает корпоративный уровень защиты от целенаправленных фишинговых атак, а также включает в себя технологии предотвращения утечек данных (DLP) и обеспечения непрерывного доступа к электронной почте. Наличие нескольких вариантов развертывания (в облаке, локально или в виде комплексного гибридного решения) позволяет реализовать систему обеспечения безопасности электронной почты в полном соответствии с потребностями вашей компании.

Больше, чем просто социотехника: новые методы целенаправленного фишинга

В случае фишинговых атак самым слабым звеном оказывается пользователь. В «Отчете компании Verizon о расследовании утечек данных за 2014 год» (*2014 Verizon Data Breach Investigation Report*)[2] отмечается, что на ссылки в фишинговых сообщениях нажимает примерно каждый пятый пользователь. Киберпреступники продолжают использовать уязвимость пользователей с помощью приемов социотехники. Более того, они пошли еще дальше и изобрели ряд изощренных методов, затрудняющих задачу выявления угроз в электронной почте.

intel Security

Вот несколько примеров:

- **одноразовые URL-адреса:** после успешного проведения фишинговой атаки и заражения системы киберпреступники деактивируют вредоносные URL-адреса. Это затрудняет или даже делает невозможной задачу обнаружения угрозы и проведения компьютерно-технической экспертизы;
- **заражение с задержкой:** в некоторых случаях злоумышленники дожидаются того момента, когда электронное сообщение будет просканировано, одобрено и доставлено в корпоративные почтовые ящики, и лишь *затем* выгружают вредоносное содержимое на целевой веб-сайт. Сотрудники склонны доверять письмам, получаемым ими на работе, и поэтому могут нажать на вредоносную ссылку;
- **вредоносные программы, способные обнаруживать «песочницу»:** эта разновидность вредоносного кода избегает обнаружения, временно оставаясь скрытой и ожидая возможности нанести удар.

Передовые средства многослойной защиты

Защита при нажатии на ссылку

McAfee Email Protection обеспечивает несколько разных слоев защиты, помогающих отражать изощренные попытки целенаправленного фишинга и связанные с ними скрытые вредоносные программы. Используя лидирующий на рынке модуль McAfee Gateway Anti-Malware Engine,[3] входящий в состав McAfee Web Gateway, McAfee Email Protection обеспечивает защиту от вредоносных URL-адресов во время сканирования сообщения и во время нажатия на ссылку. Эта функция, позволяющая бороться с целенаправленными фишинговыми атаками на любом устройстве, носит название ClickProtect. ClickProtect обнаруживает и устраняет угрозы, исходящие от URL-адресов, включенных в сообщения электронной почты. Для этого ClickProtect проверяет стоящие за URL-адресами веб-страницы на наличие возможных изменений, произошедших между временем сканирования сообщения (каким бы безвредным оно ни казалось) и временем, когда пользователь нажал на ссылку.

Рассмотрим сценарий заражения с задержкой, когда злоумышленник, собирающийся атаковать финансового директора организации, создает сообщение электронной почты с казалось бы безвредным URL-адресом. Используемое в организации решение для защиты электронной почты получает данное сообщение, изучает его, находит его безопасным и доставляет его в целевой почтовый ящик. Но после попадания электронного сообщения в почтовый ящик финансового директора злоумышленник размещает на той веб-странице, на которую ведет ссылка в сообщении, вредоносную программу. Если финансовый директор нажмет на эту ссылку, сеть организации будет заражена.

Если же в организации используется ClickProtect, то при нажатии на ссылку в сообщении электронной почты будет проведена повторная проверка данного URL-адреса на безопасность. Все URL-адреса в доставляемых сообщениях переопределяются и проверяются модулем McAfee Gateway Anti-Malware Engine. Для этого используется механизм эмуляции поведения, позволяющий выявлять вредоносное содержимое веб-сайтов без использования сигнатур.

Функция безопасного предварительного просмотра дает пользователям возможность безопасно просматривать вредоносные веб-сайты. Следование данной практике создает дополнительный слой защиты и снижает общий уровень риска. Пересылаемые сообщения остаются защищенными независимо от того, использует получатель ClickProtect или нет: защита повсюду следует за сообщением.

McAfee Email Gateway

Среды для виртуальных устройств и требования к системе

- VMware vSphere 4.x или выше
- VMware vSphere Hypervisor (ESXi) 4.x или выше
- Процессор: два виртуальных процессора
- Доступная виртуальная память: 2 ГБ
- Свободное место на диске: 80 ГБ

Аппаратное устройство

- Две модели, приобретается отдельно
- Возможен также вариант в виде блейд-сервера

Третий год подряд решение McAfee Email Protection **удостаивается рейтинга 5 звезд от журнала SC Magazine**.

Обнаружение и блокирование скрытых вредоносных программ

Интеграция с McAfee Advanced Threat Defense дает McAfee Email Protection возможность обнаруживать и блокировать вредоносные программы «нулевого дня», скрытые в подозрительных файловых вложениях, до того как они попадут в папку «Входящие». Этот инновационный подход к обеспечению многослойной защиты характеризуется сочетанием средств глубокого статического анализа кода («обратной разработки») с функциями динамического анализа (в «песочнице»), что позволяет анализировать реальное поведение вредоносных программ. Полный статический анализ кода позволяет получать подробную классификационную информацию о вредоносном ПО, обеспечивает более надежную защиту от тщательно замаскированных, трудноуловимых угроз и дает возможность выявлять родственное вредоносное ПО, в котором используется тот же код. Этапы отложенного и условного выполнения, зачастую не выполняемые в динамической среде «песочницы», можно обнаружить с помощью распаковки и полного статического анализа кода.

Встроенные функции предотвращения утечки данных

Проводя целенаправленные фишинговые атаки, злоумышленники в конечном итоге преследуют одну цель: получение ценных и конфиденциальных данных. В McAfee Email Protection интегрированы ведущие отраслевые технологии, используемые в наших решениях для предотвращения утечки данных (DLP). Наличие встроенных словарей содержимого, учитывающих требования защиты информации в индустрии платежных карт (PCI DSS), здравоохранении и финансовой сфере, а также требования региональных нормативных положений о конфиденциальности данных и пр., помогает организациям разрабатывать политики обеспечения нормативно-правового соответствия, регулирующие порядок идентификации, хранения и передачи конфиденциальных данных.

Создавая и сохраняя цифровые отпечатки выбранных документов, McAfee Email Protection «узнаёт», информацию какого содержания следует контролировать и защищать в соответствии с политиками безопасности. Использование регулярных выражений, настраиваемых словарей, пороговых счетчиков, функций глубокого анализа содержимого более 300 видов документов, а также белых списков дает возможность создавать и применять политики, касающиеся вложений и содержимого электронной почты, для разных групп пользователей в пределах компании.

McAfee Email Protection имеет функции доставки зашифрованных сообщений принудительно и по запросу, а также функции шифрования сообщений с использованием протоколов TLS, S/MIME и PGP. Соответствующий шлюз может быть развернут в виде виртуального устройства, аппаратного устройства или блейд-сервера без дополнительной платы.

Бесперебойная работа электронной почты для обеспечения непрерывности бизнес-процессов

Сбой в работе электронной почты еще не означает прекращения работы компании. В случае недоступности сети в результате стихийных бедствий, отключений электроэнергии или в ходе очередного техобслуживания McAfee Email Protection обеспечивает круглосуточный доступ сотрудников, клиентов, партнеров и поставщиков вашей компании к почте. Функция обеспечения бесперебойной работы электронной почты позволяет сохранить все сообщения, отправленные или полученные в период недоступности корпоративной электронной почты, и после возобновления работы ваших почтовых серверов точно синхронизировать данные обо всех операциях, совершенных за время недоступности серверов.

Сбор информации и анализ репутации угроз

В арсенале McAfee Email Protection есть еще один мощный инструмент — McAfee Global Threat Intelligence (McAfee GTI), служба сбора

информации об угрозах, самая комплексная из имеющихся в отрасли. Эта служба собирает и перераспределяет данные об угрозах в файлах, веб-трафике, электронной почте и сетях, получаемые с более чем 100 миллионов датчиков в режиме реального времени. Анализ репутации с помощью McAfee GTI позволяет минимизировать риск путем блокирования сообщений, приходящих из подозрительных источников, содержащих ссылки на подозрительные сайты или имеющих вложения в виде известных вредоносных файлов.

Значительно сократив вероятность проникновения вредоносных программ, фишинговых атак и постоянных угроз повышенной сложности в свою сеть, организация повышает уровень своей безопасности и снижает необходимость проведения дорогостоящих мер по восстановлению систем.

Проблемы безопасности электронной почты, размещенной на сторонних серверах

В настоящее время наблюдается увеличение количества корпоративных адресов электронной почты, предоставляемых такими почтовыми службами, как Microsoft Office 365, Google Apps for Work и др. Многие из таких почтовых служб имеют собственные функции обеспечения безопасности. Но достаточно ли этого? Похоже, что нет, ведь попытки фишинга, а также рассылка нежелательной и «серой» почты продолжаются. И встроенные функции безопасности не способны предотвратить кражу данных. Кроме того, перебои в работе, например, Office 365 могут привести к снижению производительности труда. McAfee Email Protection обеспечивает корпоративный уровень защиты от целенаправленного фишинга и сложных вредоносных программ на этапе тестирования, во время миграции и после миграции. Независимо от времени и места развертывания почтовых ящиков McAfee Email Protection обеспечивает полную защиту и непрерывный доступ к электронной почте.

Гибкие варианты развертывания сегодня и в будущем

McAfee Email Protection дает вам бóльшую свободу в выборе способа развертывания средств защиты электронной почты. Возможны следующие варианты развертывания: в виде облачного решения в категории «программное обеспечение как услуга» (Software-as-a-Service, SaaS), в виде локального решения (виртуального устройства, аппаратного устройства или блейд-сервера) или в виде гибридного сочетания первых двух вариантов. McAfee Email Protection позволяет развернуть средства защиты электронной почты таким образом, чтобы оптимально удовлетворить текущие потребности организации и дать ей возможность расширить инфраструктуру или изменить направление развития в будущем.

Независимо от того, какой вариант развертывания McAfee Email Protection выберет организация, в ее распоряжении будет единый, централизованный пульт управления, позволяющий консолидировать отчетность и легко измерять эффективность используемых организацией программ для защиты электронной почты. Действие политик распространяется как на облачный, так и на локальный компоненты решения.

За дополнительной информацией о McAfee Email Protection или для получения пробной версии решения обращайтесь к представителю McAfee или на страницу **www.mcafee.com/ru/products/email-and-web-security/email-security.aspx**.

1. **http://blogs.mcafee.com/business/security-connected/is-there-something-phishy-in-your-inbox**
2. **https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf**
3. AV-TEST: *McAfee Web Gateway Security Appliance Test* (Тестирование аппаратного устройства McAfee Web Gateway)

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com