Преимущества и стратегическое значение

Kaspersky Web Traffic Security

как компонента Kaspersky Security для интернет-шлюзов

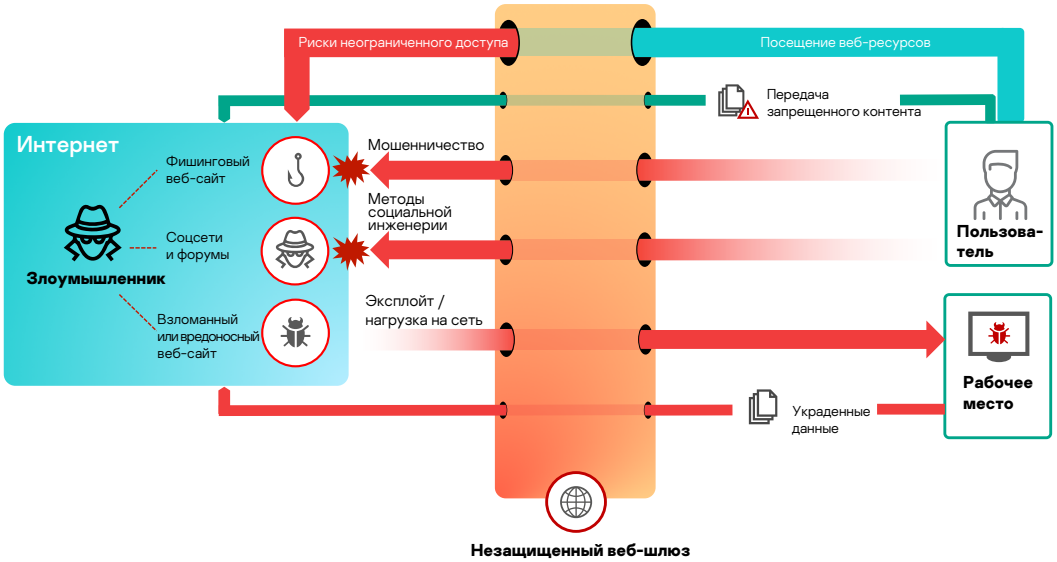
kaspersky

Интернет-шлюз как первая линия обороны

Несмотря на активное включение мобильных устройств в рабочие процессы, защищенный интернет-шлюз продолжает служить первой линией обороны в большинстве сценариев корпоративной безопасности. И ситуация не изменится, даже когда на смену традиционному придет облачный шлюз. Являясь точкой обмена трафиком между корпоративной инфраструктурой и внешней средой, шлюз предоставляет отличную возможность минимальными усилиями сдерживать угрозы на ранних этапах.

В рамках концепции многоуровневой защиты благодаря снижению вреда от угроз до того, как они достигнут конечного устройства, можно добитьсязначительного сокращения рисков, например:

- На уровне конечного устройства в расчет принимается человеческий фактор, влияние которого трудно предсказать. Благодаря правильному использованию социальной инженерии, особенно, если рабочий процесс не позволяет применять строгие политики безопасности, можно обойти даже надежную защиту конечных устройств. Решение Kaspersky Web Traffic Security не подвержено этим рискам.
- Снижение риска в случае, если внедрение уровня безопасности шлюза выходит за рамки типовой модели подготовки/тестирования для большинства вредоносных программ. Злоумышленники специально проводят исследование конечного устройства, и их обходные маневры, как правило, направлены на его конкретную среду. Кроме того, для тестирования вредоносных программ проще всего воссоздать защиту конечного устройства. Но защита прокси-сервера — это совсем другая история, и большинство злоумышленников не занимаются воссозданием системы защиты шлюза с целью тестирования.
- Когда средства защиты конечного устройства успешно блокируют вредоносные программы, то они, как правило, уведомляют об этом пользователя и администратора. Если атака массовая — или вредоносная программа проникла в кэш прокси-сервера — отправлять тревожные сигналы пользователям и администраторам может вся сеть. Скорее всего, эта ситуация приведет к нарушению бизнес-процессов, и это особенно касается предприятий малого бизнеса, в штате которых имеется недостаточно много ИТ-специалистов или у которых нет эффективной платформы для разрешения такого рода ситуаций. В таких условиях каждый час, потраченный на обращение в службу поддержки, увеличивает финансовую напряженность — вдобавок к потерянной прибыли из-за нарушения работы в целом. Очевидно, что блокировка угроз на раннем этапе, на входе в сеть, позволит сэкономить больше времени и денег.
- Последний и самый простой пример: в связи с характером задач, для выполнения которых используются некоторые конечные устройства, для них могут намеренно не использоваться средства обеспечения безопасности. Таким образом, крайне важно защитить их на уровне шлюза.



Если защита на уровне шлюза отсутствует, риск заражения вредоносным ПО возрастает

Прокси-сервер – наравне с электронной почтой, является узким местом обмена трафиком между интернетом и корпоративной сетью, где можно сдержать входящие угрозы на ранних этапах атак. Средства обеспечения безопасности прокси-сервера защищают корпоративную сеть от веб-угроз, а также повышают продуктивность работы сотрудников путем регулирования использования интернет-ресурсов. Kaspersky Security для интернет-шлюзов, основным компонентом которого является Kaspersky Web Traffic Security, решает эти и другие задачи, позволяя полностью заменить или дополнить корпоративный интернет-шлюз универсальным программным устройством безопасности. Интеграция с платформой защиты от целевых атак Kaspersky Anti Targeted Attack позволяет построить систему автоматического реагирования на угрозы.

Ключевые возможности и преимущества

- Защита от большинства современных вредоносных программ и программ-вымогателей. Поскольку старые вредоносные программы очень часто используются повторно, статические алгоритмы на основе машинного обучения и использование принципа «песочницы» (анализатора на основе эмуляции угроз) позволяют фильтровать 95% входящих угроз.

- Новые угрозы точно определяются без каких-либо ложных срабатываний сразу же после их обнаружения «Лабораторией Касперского» с помощью сети Kaspersky Security Network — не нужно ждать обновления.

- Решение представляет собой универсальное, готовое к использованию виртуальное устройство безопасности, в состав которого входят прокси-сервер и система его защиты.

- Архитектура решения позволяет осуществлять контроль корпоративного трафика (corporate traffic surveillance). Решение контролирует и защищает веб-трафик с SSL/TLS-шифрованием, которое фактически становится стандартом в интернет-коммуникациях.

- Осуществляет всесторонний анализ угроз наряду с использованием специализированных эвристических алгоритмов для блокирования вредоносных и фишинговых веб- сайтов еще до того, как пользователь подвергнется атаке.

- Решение является масштабируемым (что особенно важно для систем с высокой нагрузкой) и обеспечивает возможности иерархического развертывания и управления несколькими узлами.

- Хотя предприятия малого бизнеса реже подвергаются направленным атакам, чем крупные предприятия, они могут подвергаться атакам как компоненты цепочек на пути к достижению более крупной цели. Степень успешности подобных атак существенно снижается благодаря доступности баз данных, содержащих сведения о целевых атаках, которые постоянно обновляются экспертами «Лаборатории Касперского».

  Если ваше предприятие может позволить себе платформу Kaspersky Anti-Targeted Attack (KATA), то Kaspersky Web Traffic Security интегрируется в KATA в качестве веб-датчика, улучшая функции обнаружения угроз платформы в будущем.

- Передача определенных типов файлов в сеть и из сети может быть ограничена контентной фильтрацией. Это позволяет снизить риск заражения системы и утечки конфиденциальных данных.

- Можно внедрить эффективные сценарии веб-контроля, чтобы ограничить доступ к определенным категориям веб-ресурсов; также можно создать уникальные правила. Это помогает повысить продуктивность работы сотрудников благодаря устранению отвлекающих факторов, а также сократить риск заражения корпоративной сети — это связано с тем, что некоторые веб-ресурсы, например те, которые распространяют пиратское программное обеспечение или незаконные материалы, могут одновременно являться вредоносными веб-сайтами.

- Обеспечение достаточной прозрачности является ключевым условием успешного реагирования на инциденты. Kaspersky Web Traffic Security имеет широкие возможности, которые помогают администраторам оперативно реагировать на события, требующие их внимания. К таким возможностям относится веб-панель для отслеживания событий, средства анализа событий и интеграция с существующими системами управления данными и инцидентами безопасности (SIEM).

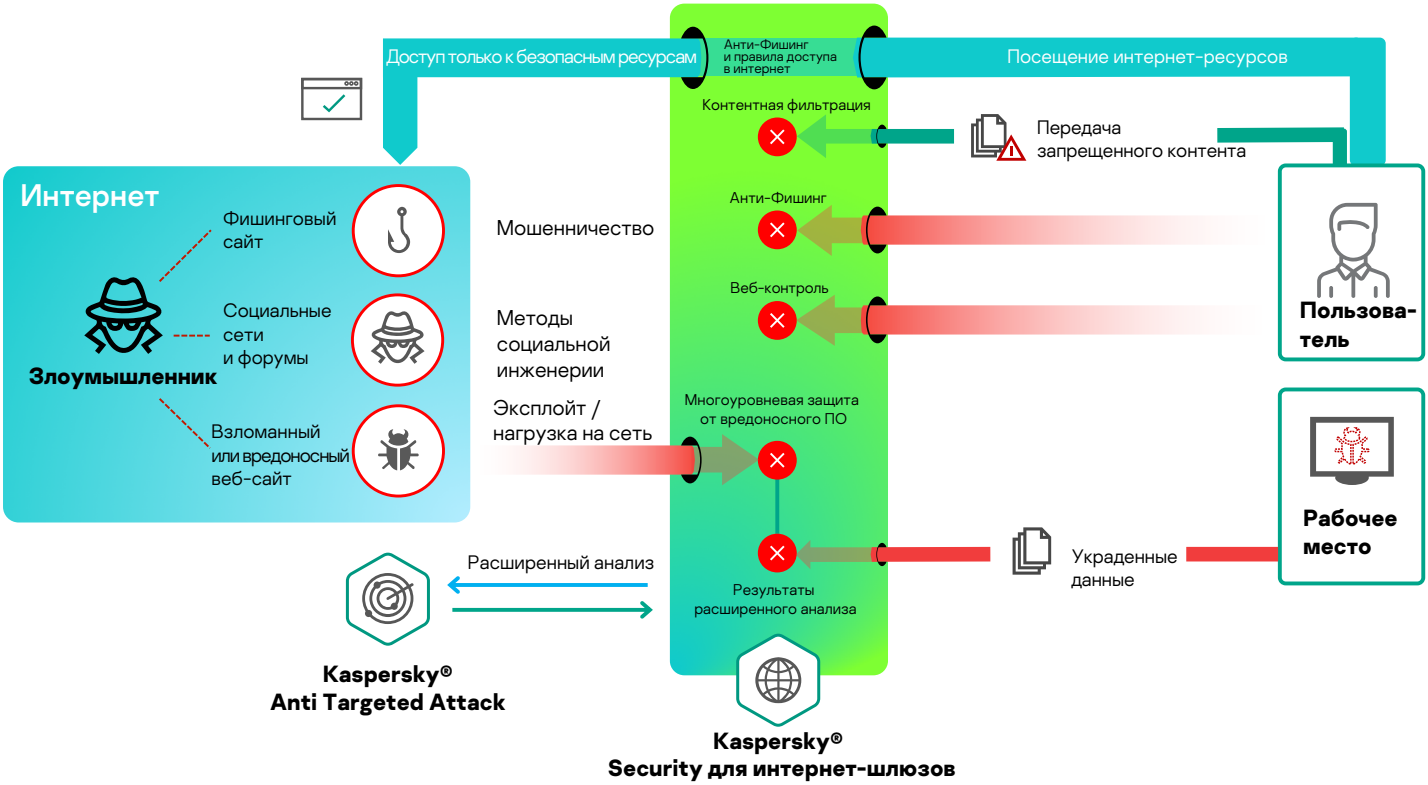
- Поддержка рабочих областей упрощает администрирование защиты в компаниях с распределенной филиальной структурой. Каждой рабочей области назначается собственный администратор с определенным набором прав, в зависимости от его роли и локальных политик. При этом ко всем рабочим областям можно применять глобальные политики безопасности.

- Kaspersky Web Traffic Security может стать дополнением к существующей системе защиты интернет-шлюзов в компаниях и организациях, работающих с конфиденциальными данными и (или) имеющих жесткие требования к информационной безопасности.

- Гибкие возможности развертывания (в виде отдельного приложения или полноценного программного устройства безопасности) позволяют интегрировать решение как в качестве полноценного прокси-сервера с системой защиты, так и обеспечивать защиту уже существующего в корпоративной сети интернет-шлюза.

Заключение

Значение средства превентивной защиты для обеспечения безопасности любой компании трудно переоценить. Обеспечение безопасности на каждом уровне вашей IT-инфраструктуры с помощью комплексных средств защиты «Лаборатории Касперского», гарантирует безопасность корпоративных данных и непрерывную работу бизнеса.



Kaspersky Security для интернет-шлюзов блокирует атаки до того, как они достигнут цели

www.kaspersky.ru