Защита конечных устройств: ручная или автоматическая?

Управление уязвимостями в российских компаниях далеко от идеала, причем еще дальше, чем можно было предполагать. Компания Positive Technologies провела собственное исследование по этому поводу в сентябре – октябре 2020 года. Опрос велся методом онлайн анкетирования, в опросе участвовали в основном специалисты по ИБ из госсектора, кредитно-финансовых организаций, промышленных и ИТ-компаний. Выяснилось, что у половины опрошенных больше всего времени уходит на то, чтобы убедить ИТ-отдел в необходимости установить обновления, причем 11% респондентов рассказали, что им приходится обосновывать устранение всех уязвимостей. Каждый десятый опрошенный ответил, что в его компании критически опасные уязвимости на важных активах не устраняются более полугода. Четверть респондентов не используют в своих компаниях специализированное ПО для выявления уязвимостей.

Эти факты не говорят прямо об уровне защищенности конечных устройств, но позволяют предположить, что и этот уровень, увы, далек от идеала. Под «конечными устройствами» теперь понимают уже не только персональные компьютеры пользователей и корпоративные сервера, но и мобильные устройства (смартфоны, планшеты, ноутбуки) и устройства IoT (Internet of Things).

Каждая уязвимость – это широко распахнутые ворота, через которые и случайные «зловреды», и элементы целевых атак могут свободно проникать внутрь корпоративных ИТ-систем. В такой среде решения для защиты

конечных точек, в том числе автоматизированные, приобретают особую ценность.

Автомат или механика?

Некоторые водители признают только механическую коробку передач. Обычно они мотивируют свой выбор тем, что им необходим полный контроль над автомобилем. Другие считают, что автомату, роботу, вариатору вполне можно доверять. Есть и такие, кто готов ездить только на беспилотных авто пассажиром. Чем меньше автоматизации, тем больше должен уметь и понимать сам водитель.

Корпоративное ПО для обеспечения безопасности конструируют похожим образом: есть приложения, где решения персонала не требуется, например Kaspersky Managed Detection and Response (MDR), сервис постоянной защиты от кибератак. Его обычно рекомендуют компаниям, где либо совсем нет специалистов по ИБ, либо они слишком загружены. Есть развитые сложные решения, для эксплуатации которых необходим очень квалифицированный персонал, например Kaspersky Endpoint Detection and Response (EDR). Но есть и промежуточный вариант – пакет, включающий большой объем полностью автоматизированных функций, но подразумевающий и принятие решений людьми: Kaspersky EDR для бизнеса Оптимальный. Любопытно, что если в автопроме продукт «с механикой» будет самым дешевым, а полностью автоматический автомобиль самым дорогим, то в ИТ-продуктах зависимость обратная, ведь пакеты с «ручным управлением» имеют более развитую функциональность и пригодны для решения более широкого круга задач.

Чем механическая коробка передач отличается от автомата представляют все водители и большинство пассажиров. Разница между программными продуктами, полностью ориентированными на использование специалистами по ИБ, и теми, где многие функции автоматизированы, не столь очевидна.

Чтобы в этом разобраться, стоит вспомнить, к какому виду приложений относятся оба продукта: Kaspersky Endpoint Detection and Response (KEDR) и Kaspersky EDR для бизнеса Оптимальный. The Endpoint Detection and Response Solutions (EDR) – так называется этот класс ПО. Согласно определению Gartner это решения, которые записывают и хранят сведения о поведении конечных устройств. Для выявления ненормального поведения системы они используют различные технологии анализа данных. Четыре базовые функции определяют, относится ли пакет к классу EDR: он должен выявлять инциденты безопасности, блокировать их на конечном устройстве, расследовать инциденты и предлагать возможные варианты действий для решения найденных проблем и устранения последствий атак. И тот, и другой продукт это делают, но в разном объеме.

Различия и сходство

Endpoint Protection Platform с включенной базовой EDR функциональностью – так строго определяется функциональность Kaspersky EDR для бизнеса Оптимальный, то есть это прежде всего система защиты конечных точек.

KEDR предназначен для противодействия атакам от самых простых до сложных, комплексных, угрозам уровня APT (advanced persistent threat — «развитая устойчивая угроза»; иначе называемая «целевая кибератака»). Kaspersky EDR для бизнеса Оптимальный работает с угрозами от распространенных угроз до ряда сложных, включая шифровальщики и бесфайловые угрозы. По мнению аналитиков в последнее время именно этот тип «зловредов» быстро набирает популярность. Они хранятся только в оперативной памяти и не оставляют записей в файловой системе.

Оба продукта могут работать как локально, так и в облаке, но KEDR значительно требовательней к аппаратной части, требуется развертывание под него отдельного сервера. Только этот продукт способен работать с EPP (Endpoint Protection Platform) сторонних вендоров и только он предназначен для обнаружения комплексных и целевых атак. У KEDR есть возможность добавления собственных детектирующих логик и проактивного поиска угроз (Threat Hunting).

Глубокий анализ подозрительных файлов доступен в обоих продуктах, но в KEDR он выполняется во встроенной «песочнице» и при помощи инструментов расследования, а Оптимальный для автоматического анализа требует интеграции с Kaspersky Sandbox.

Различия в области реагирования на инциденты заключаются в том, что «Оптимальный» не представляет рекомендаций по расследованию и реагированию. Все остальное, включая автоматическое и полуавтоматическое реагирование, доступно.

В расследовании инцидентов между KEDR и «Оптимальным» различий больше. Детальная информация о подозрительных файлах, отправка файлов в «песочницу» в ручном режиме, ретроспективный анализ, инструментарий цифровой криминалистики и сопоставление с базой знаний тактик и техник злоумышленников MITRE ATT&CK доступны только пользователям KEDR. Именно в этой области более всего заметно принципиально различие между продуктами и их направленность на разные целевые аудитории: либо отдел ИБ может и хочет самостоятельно вести расследования, либо собственные глубокие расследования не планируются.

Большинство решений «Лаборатории Касперского» для защиты конечных станций находятся в Едином реестре отечественного ПО и имеют сертификаты ФСТЭК России и ФСБ России.

Пандемия и конечные устройства

Аналитики продолжают оценивать влияние эпидемии и массовой удаленной работы на разные сегменты ИТ-рынка. Недавний опрос, проведенный CTI и Cisco, показал, что 73 % компаний планируют модернизировать ИБ-решения. Первые приоритеты - подсистемы защиты каналов связи, обеспечения доступа в интернет, антивирусной фильтрации, анализа защищённости и управления уязвимостями. У 47% опрошенных компаний более половины сотрудников используют для работы личные устройства. Особый интерес представляет ответ на вопрос «Какой процент сотрудников останется на удаленке после снятия ограничений». 26% респондентов ответили, что в их компаниях таких

людей будет более 60%. Еще 34% опрошенных сообщили, что от 30 до 60% персонала продолжат работу из дома. Фактически это означает, что сколько бы еще не продлились официальные ограничения, компании уже поняли, что нет смысла массово возвращать людей в офисы. Этого не произойдет, и практически невероятно, чтобы всем этим сотрудникам внезапно купили служебные ноутбуки и телефоны. Значит, службы ИБ должны будут справляться с новыми вызовами и требованиями. Специалисты это прекрасно понимают: 86% опрошенных намерены пересмотреть риски ИБ в связи с пандемией. Защита конечных устройств в сложившейся ситуации оказывается одной из наиболее востребованных функций. Если усилить ее функционалом EDR, то риски снизятся сильнее, а выбор EDR-приложения зависит от бюджета и ресурсов на информационную безопасность.

Информационная безопасность

Журнал: Журнал IT-Manager [№ 11/2020], Подписка на журналы

Kaspersky lab | Лаборатория Касперского

https://www.it-world.ru/cionews/security/168082.html