positive technologies

ВОЗДУШНЫЕ ВОРОТА СЕВЕРНОЙ СТОЛИЦЫ

обеспечивают защиту ИТ-инфраструктуры аэропорта Пулково от вредоносных программ с помощью песочницы PT Sandbox

Согласно исследованию Positive Technologies, порядка 40% кибератак на объекты критической информационной инфраструктуры (КИИ) связаны с вредоносным программным обеспечением. Нарушение работы систем КИИ не только создает угрозу здоровью и жизни людей, но и негативно влияет на экономическую, политическую и социальную устойчивость государства. Непрерывное функционирование объектов КИИ даже в случае кибератак — основополагающий принцип обеспечения их безопасности. Поэтому защита от вредоносных программ является одним из приоритетных направлений службы ИБ аэропорта Пулково.

ПРОФИЛЬ КОМПАНИИ

ООО «Воздушные Ворота Северной Столицы» — главный оператор аэропорта Пулково. Пулково — международный аэропорт, относящийся к объектам критической информационной инфраструктуры.

4000+
человек работает в аэропорту

> 20,4 млн
человек — пассажиропоток в год

1350 гектаров
площадь аэропорта

ГЛАВНЫЙ ПРИОРИТЕТ КОМПАНИИ — БЕЗОПАСНОСТЬ ПАССАЖИРОВ

ЗАДАЧА

В начале 2022 года службе ИБ «Воздушных Ворот Северной Столицы» поставили задачу модернизировать архитектуру безопасности аэропорта Пулково для эффективного противостояния информационным угрозам. Одним из приоритетных направлений для организации, относящейся к объектам КИИ, стала защита от вредоносных программ по нескольким каналам передачи данных.

ГЛАВНЫЙ ВОПРОС, КОТОРЫЙ СТОЯЛ ПЕРЕД СПЕЦИАЛИСТАМИ, — КАК ПРИ ПОСТРОЕНИИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ВЫБРАТЬ РЕШЕНИЯ, НА КОТОРЫЕ МОЖНО ПОЛАГАТЬСЯ

На основе приоритетных направлений были определены требования к средствам защиты от вредоносного программного обеспечения, которые необходимо было внедрить в инфраструктуру аэропорта. В первую очередь они должны были обеспечить высокий уровень обнаружения вредоносных программ и контролировать объекты во всех каналах, необходимых службе ИБ аэропорта.

ВЫБРАННОЕ РЕШЕНИЕ

Одним из основных средств, способных обеспечить защиту от ВПО на должном уровне, являются решения класса «песочница». Для поддержания безопасности всех источников, выбранных организацией, была выбрана песочница компании Positive Technologies — PT Sandbox. Она защищает от новых вирусов, эксплойтов нулевого дня, программ-вымогателей и других сложных нелегитимных программ. Песочница не только обнаруживает ВПО, но и не допускает его проникновения в контур компании, обеспечивая комплексную защиту от целенаправленных атак и массовых угроз. Отличительное преимущество PT Sandbox — простая интеграция с любыми системами ИТ и ИБ. Это позволило аэропорту Пулково быстро защитить от вредоносного ПО все необходимые каналы.

Для оценки возможностей PT Sandbox было организовано пилотное тестирование на почтовом трафике организации. Песочница Positive Technologies успешно прошла испытания, поэтому следующим этапом стало полноценное внедрение продукта в инфраструктуру аэропорта в 2023 году.

Благодаря разнообразию методов анализа вредоносного ПО и поддержке множества источников PT Sandbox гибко встроился в инфраструктуру, не нарушая существующих бизнес-процессов, и обеспечивает непрерывную работу всех приложений. На базе PT Sandbox реализуются два сценария проверки объектов на вредоносность:

Защита почтового трафика в режиме блокировки, предотвращающем попадание ВПО в контур компании

С внедрением PT Sandbox удалось выстроить систему, которая локально контролирует вредоносные объекты в почтовом трафике, обеспечивая непрерывную защиту в автоматическом режиме. Кроме того, специалисты по ИБ могут настраивать процессы анализа и обнаружения под специфику и потребности компании.

Проверка всех объектов, попадающих в сетевые папки, для контроля угроз извне

PT Sandbox взял на себя задачу автоматической проверки поступающих объектов на вредоносность. Внешний пользователь передает на FTP-сервер файл, который проверяется антивирусом, после чего поступает в песочницу. Песочница проверяет файл и перемещает его в сетевую структуру внутри периметра. Таким образом служба ИБ аэропорта смогла ускорить перенос данных извне вовнутрь и освободить ценное время своих специалистов для работы с инцидентами.

РЕЗУЛЬТАТЫ

Внедрение PT Sandbox позволило службе ИБ ООО «Воздушные Ворота Северной Столицы» контролировать поступающий извне контент и решать задачу оперативного обнаружения и блокирования ВПО. Благодаря своим широким интеграционным возможностям, песочница Positive Technologies защищает электронную почту аэропорта Пулково от вредоносных вложений и нелегитимных ссылок, а также полностью контролирует поступление файлов в контур организации. За несколько месяцев работы PT Sandbox обнаружил такие вредоносные программы, как эксплойты и трояны. В среднем за месяц PT Sandbox обрабатывает порядка 700 000 заданий на потоке, в которых находит около 30 опасных объектов и более 1500 подозрительных файлов.

«В отличие от других песочниц PT Sandbox предлагает простую и удобную интеграцию с любыми ИБ- и ИТ-системами. Благодаря широкому набору подключаемых источников мы покрыли защитой все необходимые каналы, а также легко можем добавлять новые. Отдельно хотелось бы отметить отзывчивую и внимательную техподдержку: специалисты вендора сопровождали нас на всех этапах проекта, консультировали и помогали, что позволило быстрее закончить внедрение, — комментирует Сергей Савченко, начальник службы по обеспечению информационной безопасности ООО «Воздушные Ворота Северной Столицы»

Записаться на демонстрацию PT Sandbox