История успеха

Когда лондонский аэропорт подвергся разрушительной кибератаке, принтеры HP распознали угрозу

Официальный итоговый отчет по утечке данных

Отрасль
Авиация

Цель
Выявить слабые звенья в обеспечении кибербезопасности и устранить их

Подход
Разработан план по обеспечению комплексной безопасности при сотрудничестве со специалистами компании HP в области безопасности

Преимущества для ИТ-отдела
- Применяемые меры безопасности для конечных точек IoT
- Активированные встроенные функции безопасности в принтерах HP
- Улучшенный мониторинг безопасности по всей сети

Преимущества для бизнеса
Повышенная кибербезопасность для защиты критически важной международной инфраструктуры и обеспечение безопасности пассажиров

Обзор

Лондонский аэропорт* ежедневно обслуживает более 300 000 пассажиров, которые вылетают в 94 страны по всему миру. В аэропорту работает около 50 000 человек из 300 компаний, что делает его практически густонаселенным городом.

По мере расширения аэропорта его инфраструктура стала более взаимосвязанной и автоматизированной. Внутренние системы, начиная с системы отопления, вентиляции и кондиционирования и заканчивая освещением и принтерами, теперь подключены к сети аэропорта. Печать, сканирование и копирование выполняется на более чем 60 МФУ HP, установленных по всему аэропорту.

23 апреля 2018 г. кибертеррорист, известный по прозвищу «The Wolf», использовал подключенные к сети аэропорта системы освещения для получения доступа и распространения своей вредоносной программы. Поскольку он известен тем, что использует недостаточно защищенные конечные точки, специалисты в области безопасности ИТ сразу же стали смотреть журналы угроз на своих принтерах HP Enterprise в рамках расследования с целью изолировать и остановить атаки. На удивление, в журналах содержалась подсказка от The Wolf относительно того, откуда началось проникновение. Впоследствии лондонский аэропорт обратился в компанию HP для дальнейшего повышения безопасности конечных устройств.

Что произошло

После того как The Wolf нашел уязвимость, вероятно, с помощью фишинговых сообщений пользователям в сети, ему удалось внедрить в систему IoT освещения вредоносную программу. Затем ему удалось распространить эту вредоносную программу по сети и создать себе плацдармы на других неконтролируемых оконечных устройствах.

Скрыв свое присутствие на неконтролируемых IoT устройствах, команде The Wolf удалось остаться незамеченной для систем мониторинга сети на то время, пока они разрабатывали несколько точек запуска крупной разрушительной атаки.

Руководство аэропорта лихорадочно пыталось отключать несколько систем, сохраняя работу критически важной инфраструктуры, обеспечивающей полеты самолетов и движение пассажиров.

Реагирование на атаку

Группа The Wolf была нанята для проведения атаки на сеть аэропорта. Сотрудники службы ИТ-безопасности *считали*, что сеть аэропорта надежно защищена от хакеров, но при этом они не видели угрозы, которые скрывались в IoT устройствах.

К счастью, установленные в аэропорту принтеры HP Enterprise были оснащены функцией HP Connection Inspector, которая остановила вредоносные программы, когда оно предприняла подозрительные попытки установить обратную связь по команде хакеров и управлять серверами.

Эти действия были зафиксированы в системных журналах принтера. После того как ИТ-специалисты поняли, что что-то не так, они проверили системные журналы, в которых нашли информацию об атаке. Однако когда вредоносные программы распространяются по сети, временной фактор играет определяющую роль. Если бы специалисты в области ИТ-безопасности подключили системные журналы обнаружения угроз принтеров к своей информационной системе безопасности и контроля событий, то они получили бы предупреждение о проникновении мгновенно.

Небывало надежная система безопасности

После нарушения системы безопасности ИТ-специалисты проанализировали методы обеспечения безопасности вместе со своим поставщиком услуг по аутсорсингу и управлению инфраструктурой печати и консультантами компании HP по вопросам безопасности.

После установки принтеров HP Enterprise лондонский аэропорт уже был на правильном пути. Только принтеры и МФУ HP Enterprise предлагают функцию выявления проникновения во время выполнения и решение HP Connection Inspector, которые распознают и останавливают вредоносные программы во время работы и выполняют перезагрузку устройств. Во время запуска HP Sure Start проверяет систему BIOS и в случае нарушения целостности программного кода может автоматически его восстановить, при этом также выполняет проверку микропрограммного обеспечения.

Поставщик услуг по аутсорсингу и управлению инфраструктурой печати развернул HP JetAdvantage Security Manager для автоматической проверки настроек безопасности при каждой перезагрузке принтера и сброса всех измененных настроек.

Специалисты по информационной безопасности аэропорта также подключили системные журналы принтера к своей системе SIEM. В отличие от принтеров других производителей, устройства HP могут предоставлять журналы по выявлению угроз в несколько систем SIEM, чтобы ИТ-специалисты могли получать оповещения в реальном времени обо всех возможных инцидентах в области безопасности. Таким образом, принтеры HP становятся «глазами» в своей сети.

Заключение

Благодаря установленным в аэропорту принтерам HP Enterprise и подсказкам, которые оставил The Wolf, специалистам службы безопасности удалось достаточно быстро изолировать атаку и предотвратить сбой в работе, появление негативной информации в прессе, штрафы за несоблюдение требований и ущерб репутации.

Применяя надежные методы безопасности, а также используя все возможности встроенных функций безопасности своих принтеров HP, аэропорт укрепил безопасность всей сети.

**Лондонский аэропорт является вымышленной организацией, которая подверглась крупной кибератаке в фильме HP Studio «THE WOLF: TRUE ALPHA».*

Для получения более подробной информации о решениях HP:
Безопасность печати: hp.com/go/reinventsecurity
Безопасность ПК: hp.com/go/ComputerSecurity
Чтобы просмотреть фильмы из серии «The Wolf», посетите веб-сайт: hp.com/thewolf

Следите за нашими новостями
hp.com/go/getupdated

Отправить коллегам

4AA7-3560RUE, август 2018 г.