История успеха

Тест на проникновение показывает, что брешь в системе безопасности Torvik Industries, которую использовал «The Wolf», удалось закрыть с помощью принтеров HP

Официальный итоговый отчет по утечке данных

Отрасль
Морские грузоперевозки

Цель
Проанализировать и устранить уязвимости сети

Подход
Тест на проникновение с целью поиска уязвимостей, которые привели к атаке

Выводы и рекомендации
- Научите пользователей проявлять осторожность при открытии подозрительных сообщений электронной почты и вложений на печать
- Установите принтеры HP с функцией обнаружения угроз
- Настройте все оконечные точки с учетом требований по безопасности, включая инфраструктуру, которая была перенесена или находится во временном помещении

Важные аспекты для бизнеса
Применяйте более строгие меры безопасности для предотвращения простоев в работе и повышения доверия к бренду. Улучшите политики контроля сетевых оконечных точек во временных помещениях.

Обзор

Torvik Industries* ежегодно перевозит 8 миллионов контейнеров. Для 22 000 производителей и оптовых продавцов компания Torvik является важным связующим звеном между продуктами и людьми во всем мире. Холдинг компании включает погрузочные площадки, суда, склады, а также все технологии, которые обеспечивают работу обширной сети Torvik.

Компания выросла, и ее технологической инфраструктуре пришлось адаптироваться. Несмотря на то, что специалисты в области ИТ-безопасности настроили серверы компании, безопасность некоторых принтеров в дополнительных офисах или временных помещениях осталась без внимания.

23 апреля 2018 г. кибертеррорист, известный по прозвищу «The Wolf», использовал незащищенный принтер, чтобы нарушить работу компании Torvik Industries, от персональных компьютеров до кранов и кораблей, перевозящих контейнеры. Консультант компании по вопросам безопасности выполнил тестирование на возможность проникновения, чтобы проанализировать это событие, и предоставил рекомендации по повышению безопасности и обучению специалистов.

Что произошло

Лидерство компании Torvik Industries привело к началу «игры с высокими ставками». Компания просто не ожидала, что хакеры настолько глубоко проникнут в ее сеть, что смогут отключить погрузочные краны и отправить корабли в открытый океан.

Для этого хакеру The Wolf потребовалось всего лишь взломать широкоформатный принтер на строительной площадке. После этого ему удалось пройти по сети компании к крупным объектам, участвующих в работе компании. В одно мгновение эта ведущая транспортная компания столкнулась с большим сбоем в работе, тщательными международными проверками и тысячами разгневанных заказчиков.

Как это произошло

Специалисты в области ИТ-безопасности компании считали, что компания надежно защищена. Технические специалисты и логисты компании постоянно контролировали работу компании по всему миру, отслеживая потенциальные проблемы в области безопасности. Были даже предусмотрены процедуры безопасности для оконечных устройств, таких как принтеры. Однако кое-что они забыли: настроить функции безопасности широкоформатного принтера, который временно находился в строительном вагончике.

Хакеру даже не потребовалось получать доступ к принтеру напрямую — он просто отправил по электронной почте сообщение с вложенным файлом PDF сотруднику компании Torvik, который отвечал за широкоформатную печать документов. В этот PDF-файл был встроен скрытый вредоносный файл Postscript, который открывался и запускался автоматически при отправке файла PDF на принтер. После того как сотрудник отправил задание на печать, вредоносная программа внедрилась в принтер, а затем распространилась по сети. Прикрепив вредоносную программу к безобидному вложению сообщения электронной почты, хакер смог обойти антивирусное программное обеспечение на компьютерах компании.

Взлом оказался возможным, потому что на широкоформатном принтере отсутствовала надежная встроенная система безопасности, например распознавание угроз. Кроме того, компания не осуществляла мониторинг и управление конфигурациями каждого принтера в своем парке, например тех, которые временно были установлены в дополнительных офисах.

Устранение нарушения в системе безопасности

Компания Torvik Industries наняла ведущую фирму по тестированию проникновения, чтобы провести тщательный анализ системы кибербезопасности организации.

Специалисты по тестированию возможности проникновения порекомендовали установить принтеры HP со встроенными функциями безопасности, включая принтеры серии HP DesignJet с функциями безопасной загрузки и проверки микропрограммного обеспечения на основе белого списка. Эти функции позволяют принтеру распознавать вредоносный код и отключаться, а затем оповещают ИТ-специалистов о необходимости повторно установить правильную микропрограммного обеспечение HP.

Они также порекомендовали использовать функцию безопасности Instant-On в приложении HP JetAdvantage Security Manager — программе управления безопасностью всего парка устройств, чтобы автоматически применять политики безопасности сразу же после добавления устройств в сеть. HP Security Manager также позволяет создавать отчеты о соответствии требованиям, в котором показаны все принтеры HP, включая даже те, которые установлены во временных помещениях. Это помогает продемонстрировать, что конфигурации безопасности парка устройств остались без изменений.

Кроме того, консультант по безопасности предложил программу обучения, чтобы научить сотрудников распознавать подозрительные сообщения, присылаемые по электронной почте, и избегать печати неизвестных вложений.

Заключение

Torvik Industries все еще оправляется от последствий нарушений безопасности в работе, а также от повышенной гласности необычных взглядов и преступных действий ее президента. Пока организация стремится выработать новый курс к лидерству, в области кибербезопасности все достаточно понятно: использование принтеров и решений HP поможет предотвратить следующую вылазку The Wolf.

**Torvik Industries является вымышленной компанией, которая стала мишенью для крупной кибератаки в фильме HP Studio «THE WOLF: TRUE ALPHA».*

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

Следите за нашими новостями
hp.com/go/getupdated

Отправить коллегам

4AA7-3562RUE, август 2018 г.