История успеха

Хакерскую атаку на швейцарский конференц-центр можно было предотвратить с помощью средств обеспечения безопасности компьютеров HP

Официальный итоговый отчет по утечке данных

Отрасль
Проведение мероприятий

Цель
Проверка методов обеспечения безопасности для более эффективной защиты данных конференц-центра и конфиденциальной информации клиентов

Подход
Анализ методов обеспечения безопасности и определение проблем совместно с консультантом по вопросам безопасности

Преимущества для ИТ-отдела
- Переход на парк компьютеров HP Elite со встроенными средствами защиты от вредоносных программ
- Отключение неиспользуемых портов, предотвращающее несанкционированный доступ
- Интеграция подключаемого модуля HP Manageability Integration Kit в программу Microsoft® System Center Configuration Manager (SCCM) для удаленного управления парком ПК

Преимущества для бизнеса
Оптимизация мер по обеспечению кибербезопасности для более эффективной защиты сети от изощренных атак и восстановления доверия клиентов

Обзор

В швейцарском конференц-центре, расположенном близ Женевы, ежегодно проводится более 230 различных мероприятий. Этот популярный центр в Европе с успехом служит отраслевым лидерам всего мира площадкой для проведения бизнес-конференций и масштабных презентаций новых продуктов и решений.

Руководство центра вложило большие средства в технологическую инфраструктуру, которая должна обеспечить гостям высочайшее качество обслуживания, самые современные технические возможности и индивидуальный подход. К сожалению, парк компьютеров не был обеспечен такими же современными технологиями для обеспечения безопасности.

23 апреля 2018 года злоумышленник, назвавший себя «The Wolf», проник в систему одного из компьютеров в конференц-центре, чтобы прервать важнейшую презентацию для международной аудитории. После этой атаки руководство швейцарского конференц-центра обратилось к консультанту по вопросам безопасности, чтобы он помог найти и устранить уязвимости для кибератак.

Что произошло

Швейцарский конференц-центр, одно из самых престижных мест для проведения корпоративных мероприятий, всегда предлагал своим гостям высочайший уровень обслуживания и самые современные технические возможности. Но только не в сфере кибербезопасности. Злоумышленник, назвавший себя The Wolf, загрузил вредоносное ПО на один из компьютеров центра, а затем заменил презентацию докладчика на собственную презентацию. В обстановке хаоса и волнения в лекционном зале специалисты по ИТ-безопасности центра пытались восстановить контроль над сетью.

Атаки и срывы не ограничились одной презентацией. Потеря прибыли в результате отмены бронирований в настоящее время оценивается суммой в 3,2 миллиона евро.

Как это произошло

Все, что нужно было сделать злоумышленнику The Wolf, чтобы проникнуть в систему незащищенного компьютера, это обманом заставить одного из сотрудников центра перейти по вредоносной ссылке в сообщении электронной почты или загрузить на первый взгляд невинное вложение. Или, поскольку он физически находился рядом с компьютером, он мог просто вставить флешку в USB-порт.

Компьютеры швейцарского конференц-центра не были оснащены средствами защиты, которые могли бы изолировать вредоносную программу и предотвратить ее распространение по сети. Несмотря на то, что антивирусное ПО *было* установлено, ни один из компьютеров не имел встроенных аппаратных средств обеспечения безопасности.

Укрепление безопасности

Вместе со своим консультантом по вопросам безопасности швейцарский конференц-центр провел тщательную проверку существующих средств по обеспечению кибербезопасности. После этой проверки весь парк компьютеров был заменен на компьютеры HP Elite со встроенной защитой от вредоносных программ, включая программу HP Sure Start Gen4, которая способна автоматически выявлять, останавливать атаки на систему BIOS и производить восстановление после повреждения при запуске или во время выполнения.[1]

На новых ПК HP Elite также устанавливается программа HP Sure Click, которая обеспечивает надежную защиту путем физической изоляции каждой вкладки браузера или загруженного файла PDF, или документа Microsoft Office на виртуальной машине для предотвращения распространения вредоносных программ из Интернета или вложений электронной почты на другие подключенные устройства в сети.[2]

Теперь ИТ-специалисты используют решение HP Device Access Manager для управления портами и съемными носителями, а также HP Manageability Integration Kit for Microsoft SCCM, чтобы повысить безопасность и оптимизировать администрирование системы BIOS всего парка устройств.[3]

Заключение

Швейцарский конференц-центр потерпел убытки, а также потерял доверие среди влиятельных клиентов. Однако после развертывания компьютеров HP с комплексом мер безопасности и эффективными решениями для управления центр теперь уделяет больше внимания проблеме кибербезопасности.

**Швейцарский конференц-центр является вымышленной компанией, которая подверглась кибератаке в фильме HP Studio «THE WOLF: TRUE ALPHA».*

Для получения более подробной информации о решениях HP:

Безопасность ПК: hp.com/go/computersecurity
Безопасность печати: hp.com/go/reinventsecurity

Чтобы просмотреть фильмы из серии «The Wolf», посетите веб-сайт:

hp.com/thewolf

[1] Программа HP Sure Start Gen4 поставляется на компьютерах HP Elite и HP Pro 600, оснащенных процессорами Intel® или AMD 8-го поколения.
[2] Решение HP Sure Click установлено на большинстве компьютеров HP и поддерживает Microsoft® Internet Explorer и Chromium™. В качестве вложений поддерживаются файлы Microsoft Office (Word, Excel, PowerPoint) и файлы PDF в режиме только для чтения, если установлено приложение Microsoft Office или Adobe Acrobat.
[3] Решение HP Manageability Integration Kit предварительно не установлено, оно доступно на веб-сайте по адресу hp.com/go/clientmanagement.

Следите за нашими новостями
hp.com/go/getupdated

Отправить коллегам

4AA7-3561RUE, месяц 2014 г.