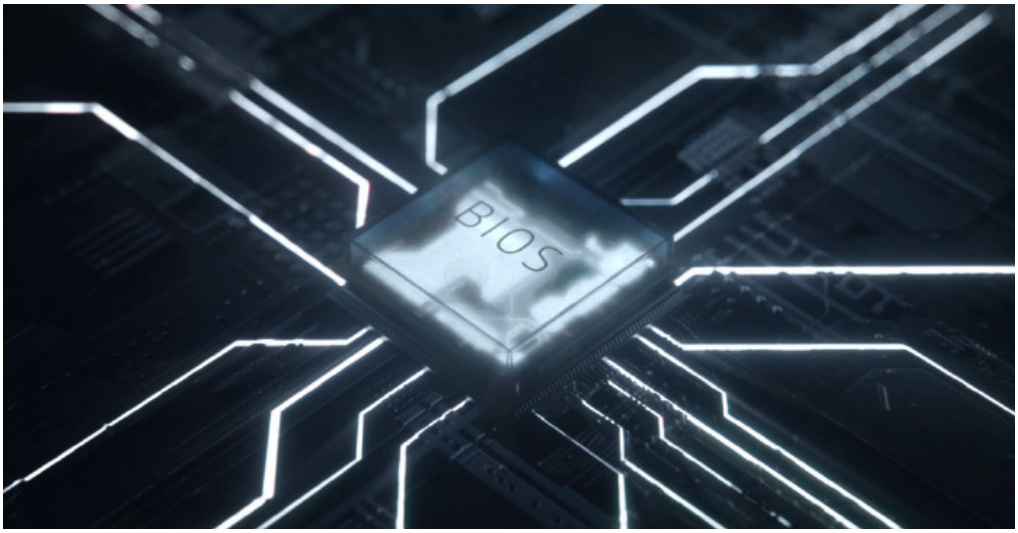
Каким образом автоматическая защита поможет спасти ваши бизнес-устройства?

Перейти



Как бороться с угрозой, которая глубоко в тылу? Внедрять автоматизацию.

338 миллиардов фунтов стерлингов в год. Такова текущая сумма убытков от киберпреступности по всему миру[1]. Эта цифра увеличивается по мере того, как совершенствуются навыки и техники хакеров. Одной из самых современных скрытых атак, ставших кошмаром ИТ-менеджеров, является атака на систему BIOS.

Миллионы компьютеров имеют уязвимые системы BIOS, т. е. их может взломать даже хакер с самыми скромными способностями. Несколько лет назад на одной из конференций исследователи Зено Ковач и Кори Калленберг представили новый тип атаки, которая позволяет в течение нескольких часов удаленно взломать и заразить BIOS на нескольких устройствах[2]. Поскольку большинство систем BIOS основаны на одном и том же коде, достаточно один раз взломать его, чтобы через некоторое время научиться обходить защиту многих других компьютеров.

Опасность атаки этого типа состоит в том, что она нацелена на практически незащищенный участок системы. Между операционной системой и оборудованием есть скрытый участок, который традиционно игнорируется. Ваша сеть может быть несокрушимой, а устройства могут находиться под защитой лучших в мире систем обеспечения безопасности – и тем не менее, остается это короткое мгновение между загрузкой системы и включением защиты. Именно в этот момент атака на BIOS может нанести серьезный ущерб вашей системе.

Поскольку ПО для обеспечения кибербезопасности, как правило, размещается на уровне операционной системы, оно не сможет обнаружить проникновение вредоносного ПО в BIOS (перед загрузкой с последующей передачей в режим управления системой). После этого хакеры заменят вашу BIOS на свою версию, которой можно управлять удаленно в течение неограниченного периода времени. Что хуже всего, обнаружить это нарушение безопасности и заражение может быть практически невозможно.

Лучший способ обеспечить безопасность устройств компании – использовать многоуровневую защиту. Вашим ИТ-специалистам больше не придется тратить время на бесконечные проверки и ручные исправления. HP предоставляет автоматический ответ (в рамках широкого ассортимента решений для обеспечения безопасности) – HP Sure Start.

«Это решение стало результатом наших совместных усилий с HP Labs, направленных на то, чтобы помочь компаниям в управлении рисками и защите пользователей и ИТ от вредоносных атак, ошибок обновления и других непредвиденных или неизвестных угроз»,

– говорит Вали Али, главный технический специалист по безопасности и обеспечению конфиденциальности в подразделении HP PC.

Каким образом автоматическая защита поможет спасти ваши бизнес-устройства?

HP Sure Start – это защита на уровне BIOS с функцией самовосстановления. Мы называем этот подход устойчивостью к кибератакам. Система создает «первичный эталон» BIOS, который шифруется непосредственно на устройстве. Таким образом, при попытке взлома BIOS она автоматически перезапускается и загружает «первичный эталон», стирая зараженный файл и сообщая об атаке. Иными словами, компьютер сам себя «лечит».

Это позволяет избежать перерывов в работе. И сократить расходы. И обеспечить соответствие устройств нормативным требованиям. И, кроме всего прочего, так намного проще работать.

Если вы ищете простейший способ предоставления устройств с функцией HP Sure Start вашим пользователям, рассмотрите решение HP Device as a Service. Это современная модель использования ПК, благодаря которой коммерческие организации смогут экипировать своих сотрудников нужным аппаратным обеспечением и аксессуарами, управлять парком устройств с разными ОС и получать дополнительные услуги в течение срока службы этих устройств. HP DaaS предоставляет простые универсальные планы с оплатой за каждое устройство, которые обеспечат бесперебойную и эффективную работу сотрудников.

Конечные устройства и точки доступа должны контролироваться на всех уровнях. Пришло время пролить свет на скрытые участки наших устройств. Каждый пользователь, каждая компания и организация по всему миру могут укрепить безопасность и отказоустойчивость с помощью предложений HP, включая HP EliteBook серии 800 с опциональными процессорами Intel® Core™ 8-го поколения. Эти устройства из семейства HP Elite включает технологию обеспечения безопасности, в том числе встроенную функцию HP Sure Start.

Читайте последний официальный документ о решении HP Sure Start, чтобы узнать больше о защите устройств компании и преимуществах решений HP по обеспечению безопасности для вашего бизнеса.

Источники:

1. https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf
2. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/
3. Разные поколения HP Sure Start доступны для некоторых конфигураций систем HP Elite и HP Pro.

4AA7-3219RUE, Май 2018 г.