Остановите киберпреступников, обратив ситуацию в свою пользу

Подробнее

60 % директоров по информационным технологиям считают, что проигрывают в войне с киберпреступниками[1]. Как разработать успешную стратегию обеспечения безопасности?

Стоило вам решить, что полностью устранили все бреши в сети — как на горизонте появляется новая кибератака. Еще более изощренная и напористая, чем предыдущие, готовая нанести серьезный ущерб вашему бизнесу. Создается впечатление, что эти атаки могут эволюционировать до бесконечности. Вот почему 68 % директоров по ИТ считают, что их средства для обеспечения безопасности конечных устройств не способны справиться с задачей[1].

Это бессилие наглядно продемонстрировала атака с использованием вредоносного ПО, сегодня известного как LoJax, которой в 2018 г. подверглись системы BIOS нескольких крупных организаций[2]. Атаки на BIOS уже давно вызывают серьезную обеспокоенность, поскольку их почти невозможно обнаружить, чрезвычайно сложно устранить и они предоставляют хакерам практически тотальный контроль над зараженным компьютером.

Несмотря на то, что такие атаки всегда были возможны, в реальности бизнес никогда им не подвергался — до сих пор.

Если направить LoJax против любой системы, она будет уязвима к атаке, как только вы включите компьютер. Антивирусное ПО и другие программные решения сторонних производителей не смогут надежно защитить вашу сеть — ведь они неспособны отслеживать изменения на уровне BIOS. Поэтому, чтобы не попасть в число 79 % компаний, которые полагаются исключительно на антивирусное ПО[3], необходимо разработать альтернативную стратегию обеспечения безопасности. Как? Ответом являются многоуровневые решения для обеспечения безопасности, встраиваемые непосредственно в аппаратное обеспечение.

При выборе компьютера всегда необходимо учитывать вопрос безопасности. Поэтому разрабатывая компьютеры, рабочие станции и системы кассовых терминалов семейства HP Elite, мы уделяли максимум внимания безопасности.

Например, HP EliteBook x360 с опциональными процессорами Intel® Core™ i7 8-го поколения оснащен средствами безопасности, которые встроены в «железо», что дает вашему бизнесу многоуровневую тотальную защиту.

Ваши сотрудники — мобильная цель визуальных хакеров

Инновационные функции безопасности, например HP Sure View Gen2,[4] — опциональный встроенный экран конфиденциальности, который обеспечивает мгновенную защиту от визуального взлома. Или функция HP Sure Click,[5] благодаря которой конечному пользователю больше не придется беспокоиться о проверке безопасности веб-сайта. Компьютер сам создает изолированный сеанс поиска в Интернете и предотвращает распространение вредоносного ПО с одной зараженной вкладки на другую.

Если же вашу компанию атакует LoJax, вы сможете спокойно продолжать работать, зная, что в компьютер встроена усиленная защита. Первая и единственная технология защиты BIOS с автоматическим восстановлением, HP Sure Start Gen4[6] автоматически обнаруживает атаку вредоносного ПО, даже если впервые встречается с таким видом атак, и восстанавливает систему BIOS.

Однако защитить бизнес с помощью таких ультрасовременных устройств — задача непростая. На помощь придут такие вычислительные решения, как HP Device as a Service (DaaS)[7]. HP DaaS упрощает процесс обеспечения ваших сотрудников необходимым оборудованием, комплектующими и сервисами жизненного цикла, благодаря гибкому подходу, учитывающему ваши требования к безопасности.

Чтобы узнать, как усилить безопасность вашего бизнеса и какие меры можно принять для защиты от кибератак, прочитайте наше Руководство по кибербезопасности.

Источники:

[1] https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
[2] Исследование ESET: «LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group» (LoJax: первый руткит UEFI, обнаруженный в естественных условиях, при непосредственном участии группы Sednit), октябрь 2018 г., https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group
[3] ИД исследования на портале Statista: 622857, Small and medium sized enterprises in the U.S (Предприятия малого и среднего бизнеса в США), исследование, проведенное агентством Statista в октябре 2016 г.
[4] Встроенный защищенный экран HP Sure View является дополнительной функцией, которая должна быть сконфигурирована при покупке.
[5] HP Sure Click доступен на большинстве компьютеров компании HP и поддерживает Microsoft® Internet Explorer, Google Chrome и Chromium™. Поддерживаемые вложения: Microsoft Office (Word, Excel, PowerPoint) и PDF-файлы в режиме только для чтения, если установлены Microsoft Office или Adobe Acrobat.
[6] Технология HP Sure Start Gen4 доступна в продуктах HP Elite и HP Pro 600, оснащенных процессорами AMD или Intel® 8-го поколения.
[7] Планы и (или) включенные компоненты HP DaaS зависят от региона или уполномоченного сервисного партнера HP DaaS. Чтобы получить подробную информацию по вашему региону, обратитесь к местному представителю HP или уполномоченному партнеру DaaS. Услуги HP регулируются условиями и положениями HP, применимыми к предоставляемой услуге или определенными в момент покупки. Заказчик может иметь дополнительные законные права в соответствии с применимыми местными законами. Такие права не затрагиваются условиями и положениями оказания услуг HP или ограниченной гарантией HP, предоставляемой с продуктом HP.

4AA7-5353RUE, апрель 2019 г.