Защита на уровне «железа»

текст: Григорий Рудницкий

Решения для безопасности данных на ПК сегодня предлагают не только софтверные компании, но и производители компьютеров, у которых есть дополнительные возможности по реализации защитных механизмов. Об этом нам рассказал Андрей Терляков, менеджер по развитию коммерческих мобильных систем компании HP в России.

Почему компания HP, производитель оборудования, уделяет пристальное внимание вопросам информационной безопасности?

Пользователь, сотрудник компании, выходит за пределы замкнутого контура, то есть своей корпоративной сети, или инфраструктуры. Мы все часто работаем вне офиса — дома, в командировках, в кафе, в коворкинге, подключаемся удаленно к своим корпоративным сетям через различные точки доступа или сотовую связь. Но мы не можем быть стопроцентно уверены в надежности этого входа и, так или иначе, подвергаем сеть своего предприятия определенным рискам.

Но ведь есть штатные средства защиты данных, почему их недостаточно?

С каждой новой версией ОС Windows совершенствуются механизмы защиты. Однако все эти технологии реализуются на программном уровне. Компания Microsoft не имеет доступа к «железу», установленному производителем компьютера. Совокупность программных и аппаратных возможностей повышает защиту от угроз.

АНДРЕЙ ТЕРЛЯКОВ,
менеджер по развитию коммерческих мобильных систем компании HP в России

Дополнительно к средствам Windows мы готовы предложить собственные решения для безопасности устройств и данных. Так, Microsoft не может защитить компьютер до момента непосредственной загрузки системы. Мы же готовы сделать такие предложения.

Первое из них называется HP Sure Start и позволяет не только защитить BIOS компьютера, но и восстановить его в случае возникновения непредвиденных сбоев и атак. На защищенном флэш-накопителе записан эталонный образ BIOS, поэтому при расхождении контрольной суммы между реальной версией BIOS и эталонной происходит автоматическое восстановление, которое занимает всего 30 секунд, и мы получим работоспособный компьютер. Мы продвигаем эту технологию уже второй год. В первых версиях контрольная сумма проверялась только при загрузке, в нынешней версии сравнение проводится раз в 15 минут, поскольк-

ку злоумышленники или зловредное ПО могут попытаться внести изменения в код BIOS и во время обычной работы ПК.

Следующая технология — HP WorkWise — защищает доступ к устройству, когда пользователь отошел куда-то, а свой рабочий компьютер не заблокировал. Чтобы этого избежать, можно установить на свой смартфон небольшую программу, которая предоставит целый набор возможностей для удаленной работы с вашим девайсом. Можно настроить расстояние от ПК до смартфона, на котором автоматически происходит блокировка компьютера. Разумеется, разблокировка тоже выполняется автоматически, как только вы вернулись. На экране смартфона в приложении WorkWise вы увидите все, что происходит с ним в ваше отсутствие. Это могут быть попытки несанкционированного входа, подбора пароля, подсоединения USB-устройства, перезагрузки и т. д. Еще одна полезная функция HP WorkWise — датчик температуры удаленного рабочего ПК. В целом очень нужная технология; совместима со смартфонами под любыми ОС.

Но ведь информацию можно украсть, не только получив непосредственный доступ к компьютеру, но и подсмотрев за спиной пользователя. В банкоматах уже поддерживается технология, размывающая изображение для зрителя, находящегося к нему под углом. Реализовано ли что-то подобное для настольных компьютеров?

Мы часто работаем в общественных местах и в транспорте. У нашей компании и раньше была технология сужения углов обзора, которое достигалось благодаря специальной пленке, помещаемой на экран. Если отклоняешься больше чем на 30 градусов, картинка мутнеет. Но были и недостатки, такие как потеря яркости. И тогда мы предложили новую технологию HP Sure View — встроенный в экран поляризационный фильтр, он включается и выключается с помощью горячих клавиш. Эта технология особенно понравится тем, кто часто путешествует.

Частенько данные похищаются, когда на компьютер жертвы попадают зловредные программы: вирусы, черви, трояны. В частности, их можно подхватить, пройдя по вредоносной ссылке в фишинговом письме или открыв вложенный файл из зараженного письма. Блокированием таких угроз успешно занимаются антивирусы, но, насколько мне известно, технологии блокировки вредоносных элементов предлагает и компания HP?

Нередко мы можем получить новейший вирус, которого пока нет в базах антивирусных компаний либо он является видоизмененной версией уже известных вредоносных программ. В итоге компьютер заражен со всеми возможными последствиями. Мы разработали технологию HP Sure Click, представляющую собой виртуальную машину, работающую внутри операционной системы. Любая веб-страница может быть открыта и любое приложение запущено в этом замкнутом пространстве, в «песочнице». Если активированное приложение окажется зараженным и червь захочет выйти за пределы «песочницы», мы получим соответствующее уведомление о попытке изменения файлов на жестком диске. В этом случае приложение или веб-страницу можно просто закрыть, в результате весь кэш и все содержимое самоуничтожится без каких-либо последствий. Кстати, виртуальная машина занимает вдвое меньше системных ресурсов, чем обычный антивирус. Наконец, следует упомянуть технологию HP Drive Encryption, шифрующую данные на SSD-накопителе, только, в отличие от Microsoft Bitlocker, делается это не программным, а аппаратным способом. Аппаратное шифрование не приводит к потере производительности системы.

И последний вопрос. На каких моделях ПК уже поддерживаются все эти технологии безопасности?

Пока на всех HP Elitebook 1000-й серии, а некоторые из них и на более младших сериях, например HP WorkWise начиная с 400-й серии. В дальнейшем мы планируем расширять список моделей корпоративных ПК, в том числе и десктопов, как только оборудование будет полностью их поддерживать. А потому мы с полной уверенностью можем утверждать, что корпоративные компьютеры HP — одни из самых надежных и безопасных.