БЕЗОПАСНОСТЬ ДАННЫХ МОБИЛЬНОГО ПОЛЬЗОВАТЕЛЯ

ПОЧЕМУ ДЛЯ МОБИЛЬНОГО ПОЛЬЗОВАТЕЛЯ ОСОБЕННО ВАЖНА ПРОБЛЕМА СОХРАННОСТИ ИНФОРМАЦИИ

Удобство пользования информацией в электронном виде в бизнес-среде очевидно — большинство бизнес-процессов реализуются исключительно в электронной форме. Целые компании создаются и растут, не имея никаких производственных мощностей, работая только в сети Интернет.

Доступность, простота хранения, перемещения и копирования значительных объемов информации при помощи флэш-носителей, переносных USB-дисков имеет обратную сторону. Завладеть чужой информацией стало намного проще. Факт кражи бумажного документа можно обнаружить оперативно, а вот электронное письмо или тайно вынесенную из офиса флэшку с файлами можно и не заметить.

Однако флэш-носители все же менее привлекательны для злоумышленника, чем ноутбуки. На внешние устройства копируют обычно финальные (или промежуточные) версии документов для передачи коллегам, а вот в ноутбуке хранится всегда самая свежая и актуальная информация.

Согласно статистике последних лет, самым распространенным источником утечки информации является носитель, который хранит эту информацию дольше всего и в наибольшем объеме. На экране монитора помещается одна страничка текста, а по беспроводным интерфейсам информацию перехватить можно лишь в момент ее передачи. Другое дело — жесткий диск ноутбука. Объемы информации значительны, а срок хранения — несколько лет. Конечно, злоумышленнику потребуется физический доступ к устройству, но выкрасть ноутбук, пожалуй, дешевле, чем купить спецаппаратуру для перехвата изображения на дисплее. Именно поэтому проблема сохранности данных и защита их от утечки для владельцев портативных ПК выходит на первый план.

ПОЧЕМУ НЕОБХОДИМО ШИФРОВАТЬ ИНФОРМАЦИЮ НА НОУТБУКЕ

Для того чтобы ответить на этот вопрос, приведем пример. Весной 2009 года Министерство здравоохранения и социальных служб штата Оклахома (Oklahoma Department of Human Services, DHS) объявило о краже ноутбука, содержавшего персональные данные около миллиона человек. В результате утечки пострадали обычные жители, которые получали государственную поддержку или участвовали в государственных программах. По данным аналитического центра Perimetrix, на украденном компьютере хранились их имена, даты рождения и адреса, а также номера социального страхования. В официальном сообщении утверждалось, что компьютер был украден из машины сотрудницы министерства. По словам руководителя DHS Говарда Хендрика (Howard Hendrick), риск компрометации данных не очень велик, поскольку компьютер «использует систему парольной защиты». К сотруднице не применялись дисциплинарные меры, поскольку она не нарушила политику безопасности DHS.

Вполне возможно, что использованная защита действительно надежна и Говард Хендрик просто неправильно ее назвал, но описанный случай показывает: единственным способом защиты данных на мобильных устройствах от посторонних глаз является шифрование. Все остальные способы либо слишком ненадежны, либо чрезвычайно дороги.

Суть шифрования заключается в преобразовании информации к виду, который для стороннего наблюдателя, не знающего ключа шифрования, представляется бессмысленным набором символов. Наиболее удобным для бизнес-пользователя является вариант, когда шифрование выполняется прозрачно, то есть не нужно выполнять дополнительных действий по расшифровке файлов перед началом работы и зашифровывать их при завершении — информация всегда зашифрована, а работать с ней можно после прохождения процедуры аутентификации и до выхода из системы.

В ЧЕМ ЗАКЛЮЧАЮТСЯ ОСОБЕННОСТИ ВСТРОЕННЫХ СРЕДСТВ ШИФРОВАНИЯ WINDOWS

Любая современная операционная система содержит встроенную поддержку шифрования. Другой вопрос, насколько надежно предлагаемое шифрование и насколько удобно для пользователя оно реализовано. Например, в ОС Linux создать шифрованную папку и защитить ее паролем достаточно просто, более того, можно сделать шифрованным весь жесткий диск, но дружелюбных операционных систем на базе Linux, в которых комфортно работать неподготовленному пользователю, пока не так много. Да и в корпоративной сети в большинстве случаев администратору придется защищать данные в среде Windows. Компания Microsoft до недавнего времени для шифрования данных предлагала только Encrypting File System (EFS) — шифрованную файловую систему, к которой было много нареканий.

Появившаяся в Windows Vista и продолжившая свое развитие в Windows 7 технология BitLocker имеет ряд нововведений. Основное преимущество BitLocker перед конкурентами, то есть продуктами, имеющими сходный функционал, состоит в его бесплатности. Вполне возможно, что имея встроенное и полностью интегрированное с Active Directory решение по шифрованию данных, далеко не все пользователи платформ Microsoft будут искать ему замену.

Вместе с тем в нашей стране, в силу законодательных норм, действуют импортно-экспортные ограничения как на стойкость криптографии, так и на использование Trusted Plat form Module (TPM) — аппаратных модулей доверенной загрузки. Уточним, что TPM является важнейшим компонентом технологии BitLocker — в защищенной памяти устройства, размещенного на материнской плате, сохраняется ключ шифрования, а доступ к памяти самого устройства ограничивается паролем.

BitLocker не в состоянии обеспечить действительно надежную защиту данных без TPM. Однако если основными аргументами при выборе средства защиты для пользователя являются безопасность, стоимость и удобство управления, то следует обратить внимание на иной класс решений. Речь идет о продуктах для шифрования данных с централизованным управлением и резервным копированием информации. Такие решения используют методы аутентификации с применением USB-ключей или смарт-карт.

КАКОВЫ ОСНОВНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ ШИФРОВАНИЯ

К выбору системы шифрования нужно подходить взвешенно. Прежде всего, от таких систем требуется безупречное выполнение основной задачи — надежной защиты информации вне зависимости от того, хранится она в системном разделе, внешнем носителе или специальном файле-контейнере. При всем многообразии средств шифрования далеко не все они корректно выполняют шифрование системного раздела, поддерживают «спящий режим» и шифруют дамп памяти при системном сбое. А ошибки разработчиков при реализации тех или иных функций системы могут привести к полной потере всех данных (криптографические преобразования необратимы при отсутствии ключа шифрования). Гарантией высокой надежности системы может стать опыт вендора в разработке систем защиты информации и многолетняя история продукта.

Другой важный аспект, на который надо обратить внимание, — удобство и простота использования. Пользователь откажется хранить данные на защищенном диске, как ни угрожай приказами и ни пугай политиками информационной безопасности, если применение средств защиты будет идти вразрез с удобством. Допустим, для доступа к шифрованным данным нужно вводить длинный и сложный, и что еще хуже — регулярно меняющийся пароль. Забыв такой пароль несколько раз, рано или поздно пользователь запишет его в легкодоступном для злоумышленника месте. С другой стороны, слабая парольная политика таит угрозу взлома всей системы путем элементарного подбора. Разумным выходом представляется использование упомянутых аппаратных электронных USB-ключей для аутентификации владельца ПК при доступе к данным. В профессиональной среде эти устройства называют токенами. Высокая степень безопасности позволяет надежно сохранять в защищенной памяти токена логины, пароли и др. Наиболее широкий модельный ряд токенов представлен в линейке продуктов eToken. К слову, разработчик линейки уделяет пристальное внимание вопросу сертификации своей продукции, что подтверждает качество проработки и надежность заявленной функциональности.

В ЧЕМ СОСТОЯТ ПРЕИМУЩЕСТВА АППАРАТНЫХ СРЕДСТВ ШИФРОВАНИЯ

Решения, поставляемые с токенами, стоят дороже, чем чисто программные продукты, но при этом имеют более высокую надежность. Тот же eToken входит в состав комплексного решения Secret Disk, чья история насчитывает более десятка лет. Наличие в составе решения токена снимает необходимость запоминать сложные пароли: для доступа к данным нужны два фактора — аппаратный ключ и ПИН-код от него, вся остальная секретная информация (цифровые сертификаты, пароли для доступа) сохраняется в защищенной области памяти токена. Современные токены имеют встроенное ограничение на количество попыток ввода ПИН-кода, что защищает систему от попыток перебора.

В силу высокого уровня безопасности системы шифрования, имеющие токены, прежде всего, востребованы в корпоративной среде, в частности среди топ-менеджеров крупных компаний, информация на ноутбуках которых стоит десятки и сотни тысяч долларов. Простота и удобство применения таких решений одновременно позволяет устанавливать их и на ноутбуки рядовых пользователей, а централизованное управление и резервное копирование ключевой информации упрощает администрирование в организации вне зависимости от ее размера.

Специальные «облегченные» версии систем шифрования с токенами могут использоваться и в среде домашних пользователей, благо, что один и тот же токен может применяться для решения ряда задач помимо шифрования: безопасный доступ к интернет-сайту банка, обеспечение безопасности при работе с электронными кошельками, хранение паролей и кодов доступа от различных приложений и веб-сайтов и т.д.

ЧТО ВАЖНО ШИФРОВАТЬ В ПЕРВУЮ ОЧЕРЕДЬ

Во избежание ситуации, при которой человеческий фактор оказывается ахилессовой пятой в системе безопасности, необходимой функцией системы защиты данных, хранящихся и обрабатываемых на ноутбуке, является шифрование системного раздела.

Шифруя раздел целиком, не нужно заботиться о том, на каком именно диске и в какой папке пользователь размещает файлы, не предназначенные для чужих глаз. Обрабатываются ли на ноутбуке финансовые отчеты, строятся ли планы по выводу новых продуктов или сохраняются данные конкурентной разведки — вся эта информация, независимо от места дислокации, должна быть надежно защищена.

В системном реестре, кэшах браузера и логах операционной системы могут оказаться весьма значительные сведения. Шифрование отдельных или выбранных папок может быть удобно для домашнего пользователя, который самостоятельно настраивает систему шифрования и использует ее для защиты небольшого числа редко меняющихся объектов. Например, можно защитить папку со старыми фотографиями на внешнем диске. В организации, а также при интенсивной работе с данными, которые нужно защищать, такой подход становится слишком громоздким и неудобным.