ПРОГРАММНОЕ ШИФРОВАНИЕ И СООТВЕТСТВИЕ НОРМАТИВНЫМ ТРЕБОВАНИЯМ: БОЛЕЕ ДЕШЕВОЕ РЕШЕНИЕ С СЕРЬЕЗНЫМИ РИСКАМИ ДЛЯ БЕЗОПАСНОСТИ

НОРМАТИВНЫЕ ТРЕБОВАНИЯ И ТРЕБОВАНИЯ СООТВЕТСТВИЯ

Раньше за безопасность данных несли ответственность только ИТ-отделы. Однако из-за постоянных утечек данных потребителей правительства во всем мире предъявляют к компаниям все больше и больше требований по шифрованию и защите всех данных, позволяющих установить личность.

Согласно таким нормативным актам, как HIPAA в здравоохранении, GDPR в регионе EMEA и CCPA в Калифорнии, шифрование классов защищенных данных является обязательным. Количество организаций, отслеживающих соблюдение нормативно-правовых требований, экспоненциально выросло за последние 3 с лишним года, поскольку резко возросло количество нормативных актов, а также связанные с ними штрафы и судебные риски.

На фоне этих изменений ИТ-отделы изо всех сил пытались справляться с безопасностью и растущими затратами. На протяжении всей пандемии COVID дополнительно инвестируются средства в оборудование и брандмауэры в ущерб вниманию к шифрованию данных.

На самом деле, широкое распространение получает программное шифрование с использованием Microsoft BitLocker® или программного обеспечения для управления оконечными устройствами от таких компаний, как Symantec, McAfee и других. Некоторые компании и потребители также используют стандартные USB-накопители с программными «хранилищами», предоставляемыми некоторыми поставщиками.

ШИФРОВАНИЕ И ПЕРЕМЕЩАЕМЫЕ ДАННЫЕ

Сотрудникам и потребителям необходимо брать с собой свои данные. У них есть такие варианты.:

1. Облачные службы. Отличный вариант, так как к ним можно получить доступ с любого устройства, которое может подключиться к Интернету. Однако придется поступиться гибкостью. Хранение данных в облаке лишает пользователя или компанию контроля над данными и сопряжено с потенциальным риском, поскольку мы наблюдали, как облачные серверы остаются незаблокированными или доступными.
2. Стандартные USB-накопители. Хотя ношение USB-накопителя кажется более безопасным, риск раскрытия данных из-за его потери может быть значительным. Например, существует множество историй о потерянных USB-накопителях с секретной информацией или о прачечных с ящиками, полными потерянных USB-накопителей.
3. USB-накопители с аппаратным шифрованием. Эти USB-накопители имеют заказную архитектуру, включающую встроенный контроллер шифрования и контроль доступа. Данные шифруются с использованием самого надежного протокола 256-битного шифрования AES в режиме XTS в целом, наряду с другими возможными мерами защиты для смягчения последствий физических атак и атак, основанных на встроенном программном обеспечении. Эти накопители производятся компаниями, специализирующимися на устройствах безопасности, и, хотя они дороже стандартных USB-накопителей, обеспечивают лучшую защиту данных. Накопители FIPS 197 или FIPS 140-2 уровня 3 обеспечивают более высокий уровень защиты и спокойствия.
4. Стандартные USB-накопители с программным шифрованием. Для обеспечения безопасности в соответствии с требованиями законодательства можно использовать программное шифрование с помощью BitLocker или других инструментов — это достойные варианты, поскольку они относительно недороги и обеспечивают такое же шифрование AES-256 XTS.

Неудивительно, что в большинстве случаев предприятия и отрасли склонны выбирать четвертый вариант, то есть использование стандартных USB-накопителей с программным шифрованием. В основном это связано с тем, что программное шифрование с помощью BitLocker или других утилит хранилищ данных является «бесплатным».

ПРОГРАММНОЕ ШИФРОВАНИЕ НЕ СООТВЕТСТВУЕТ НОРМАТИВНЫМ ТРЕБОВАНИЯМ

Специалисту по коммерческой безопасности программное шифрование может предоставить те же возможности шифрования, что и более дорогие USB-накопители с аппаратным шифрованием. Но так ли это? Бюджетные средства ограничены, поэтому предприятия переходят на программное шифрование в целях соблюдения нормативных требований, не подозревая о его негативных аспектах.

В чем проблема USB-накопителей с программным шифрованием? Разве хранимые и перемещаемые данные не шифруются с помощью алгоритма AES-256 XTS? В целом, шифруются. Но проблема состоит в том, что программное шифрование считается «удаляемым».

Погодите. Удаляемым? Означает ли это, что пользователь может отключить шифрование USB-накопителя с программным шифрованием?

Ответ — «да». Пользователи могут удалить функцию программного шифрования со своих USB-накопителей. Зачем это им, спросите вы? Потому что они могут — и потому что они хотят просто получить доступ к файлам без использования пароля или просто забыли пароль, но им нужно использовать USB-накопитель.

КАК ОТКЛЮЧИТЬ ПРОГРАММНОЕ ШИФРОВАНИЕ НА USB-НАКОПИТЕЛЕ С ШИФРОВАНИЕМ

Для пользователя, который не хочет заниматься вводом сложных или каких-либо других паролей для доступа к своим данным, процесс прост:

1. Подключите накопитель с программным шифрованием к компьютеру.
2. Отформатируйте накопитель.
3. После форматирования накопителя всё шифрование удалено.
4. Скопируйте файлы с секретной или конфиденциальной информацией на накопитель для быстрого доступа.

Пользователи могут легко сделать это, используя компьютер, на который не распространяются ограничения: ИТ-отделы ограничивают использование команд форматирования на компьютерах компании, но это можно сделать на любом другом компьютере, не принадлежащем компании.

С точки зрения соответствия нормативным требованиям: легкость удаления шифрования данных означает, что накопитель, предоставленный компанией, теперь не зашифрован, хотя данные, которые были зашифрованы на накопителе, считаются утерянными навсегда после удаления шифрования с помощью описанного выше метода (ключи шифрования привязаны к данным). Любые данные, скопированные на устройство после удаления шифрования, считаются незащищенными и потенциально не соответствующими нормативным требованиям, что может привести к нарушению правил HIPAA, GDPR, CCPA и многих других.

ПОСЛЕДСТВИЯ ПОТЕРИ НЕЗАШИФРОВАННОГО НАКОПИТЕЛЯ

Если предоставленный компанией USB-накопитель потерян и найден, даже если компания сначала не знает об этом, но узнает об этом позже через социальные сети, для компании вступают в силу особые требования соответствия, в рамках которых, возможно, потребуется:

1. провести судебную экспертизу, чтобы определить, какие данные были потеряны;
2. определить после консультации с юридическим отделом, имело ли место нарушение закона;
3. определить, необходимо ли уведомить клиентов.

Именно в этом случае потеря одного USB-накопителя может обойтись очень дорого. С учетом стоимости услуг юристов, превышающей многие сотни долларов в час, такой процесс обеспечения соответствия может привести к расходам в многие тысячи долларов. И это помимо потенциальных штрафов, исков со стороны клиентов и других судебных исков, а также позора из-за неспособности защитить данные.

При рассмотрении программного шифрования с точки зрения его низкой стоимости эти риски и их огромные финансовые последствия не учитываются.

Есть еще одна опасность, связанная с разрешением использования незашифрованных USB-накопителей в корпоративной сети. Она обычно называется «BadUSB». BadUSB — это класс вредоносных программ, которые злоумышленники используют для взлома брандмауэра компании и внедрения вредоносного ПО в систему киберзащиты компании через USB-накопители.

BadUSB

Когда USB-накопитель подключается к компьютеру, контроллер набора микросхем компьютера запускает квитирование с контроллером USB-накопителя через встроенное программное обеспечение. Этот обмен происходит до того, как операционная система, такая как Microsoft, macOS или Linux, узнает о подключении USB-накопителя. На каждом USB-накопителе есть встроенное ПО, которое запускается, когда накопитель подключается к USB-порту.

Злоумышленники научились внедрять вредоносные программы с помощью этого механизма квитирования, заменяя встроенное ПО USB-накопителя другим, вредоносным ПО, которое внедряет вредоносные программы в целевую компьютерную систему во время ее взаимодействия с USB-накопителем. Во встроенном программном обеспечении стандартного USB-накопителя, которое выполняется его контроллером, отсутствует защита. Так и появились атаки типа BadUSB, в которых хорошие USB-накопители использовались для проникновения через брандмауэры и взлома киберзащиты.

Многие компании пытаются запретить использование USB-накопителей в своих системах или даже заливают USB-порты эпоксидной смолой. Однако они обнаружили, что сотрудники определенных классов должны носить с собой данные на USB-накопителях. Например, руководители, которые хотят взять с собой для работы или предоставления внешним юридическим или финансовым консультантам данные, отсутствующие в облаке компании; подрядчики компании, которым нужны данные для работы, однако их доступ к базам данных компании ограничен; финансовые аналитики, которые спешат закрыть ежемесячные отчеты и должны работать с электронными таблицами дома.

Как показывает предыдущий анализ, использование стандартного USB-накопителя с программным решением для шифрования сопряжено со значительным риском. То, что на первый взгляд казалось дешевле, оказывается потенциально очень вредоносным и намного более дорогим. Стоимость всего лишь 2–3 часов консультации с юристом по поводу возможной утечки данных сводит на нет любую экономию от использования более дешевого решения.

USB-НАКОПИТЕЛИ С АППАРАТНЫМ ШИФРОВАНИЕМ — ЛУЧШИЙ ВАРИАНТ ДЛЯ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ НОРМАТИВНЫМ ТРЕБОВАНИЯМ

Вот что делает USB-накопители с аппаратным шифрованием лучшим вариантом для сфер применения с нормативно-правовым регулированием.

1. Шифрование USB-накопителей с аппаратным шифрованием включено всегда. Пользователи не могут отключить шифрование, сбросить правила для паролей (минимальная длина, сложность) и отключить ограничение на автоматические повторные попытки ввода пароля. В отличие от программного шифрования, которое не предотвращает подбор пароля с помощью программных атак перебором по словарю, аппаратные версии ограничивают количество повторных попыток ввода пароля и блокируют данные, если неверный пароль вводится 10 раз, а иногда и меньше. Это очень безопасно в эпоху суперкомпьютеров.
2. Накопители с аппаратным шифрованием используют контроллеры шифрования премиум-класса и включают множество функций безопасности. Хотя мы не всегда раскрываем все контрмеры для обеспечения безопасности, есть меры противодействия для защиты от BadUSB. На заводе-изготовителе, когда встроенное ПО загружается на накопители с аппаратным шифрованием, оно снабжается цифровой подписью. Это означает, что при подключении зашифрованного USB-накопителя контроллер шифрования сначала проверяет целостность встроенного ПО с помощью цифровой подписи и загружает его только в том случае, если проверка пройдена. Любая попытка заменить встроенное ПО заблокирует накопитель, и он перестанет работать. Никакой угрозы!
3. USB-накопители с аппаратным шифрованием можно снабдить индивидуальными идентификаторами продукта (PID), настроенными для конкретной компании. На этих накопителях премиум-класса может быть запрограммирован цифровой идентификатор, который при подключении накопителя к внутреннему или внешнему брандмауэру компании позволяет идентифицировать накопитель как выпущенный компанией. Например, если сотрудник потеряет накопитель компании и приобретет такую же модель, вновь приобретенный накопитель не пройдет проверку в сети компании. Эта настройка добавляет еще один уровень безопасности при использовании USB-накопителей.
4. Накопители с аппаратным шифрованием очень быстро экономят деньги. Именно благодаря снижению и устранению рисков цикл окупаемости становится очень коротким.

Компания Kingston — крупнейший в мире производитель USB-накопителей с шифрованием, предлагающий семейства накопителей с различными функциями и в разных ценовых категориях. Свяжитесь с Kingston напрямую, чтобы обсудить, как мы можем помочь вам обеспечить соответствие нормативным требованиям с помощью USB-накопителей с шифрованием для руководителей, сотрудников, подрядчиков и т. д.