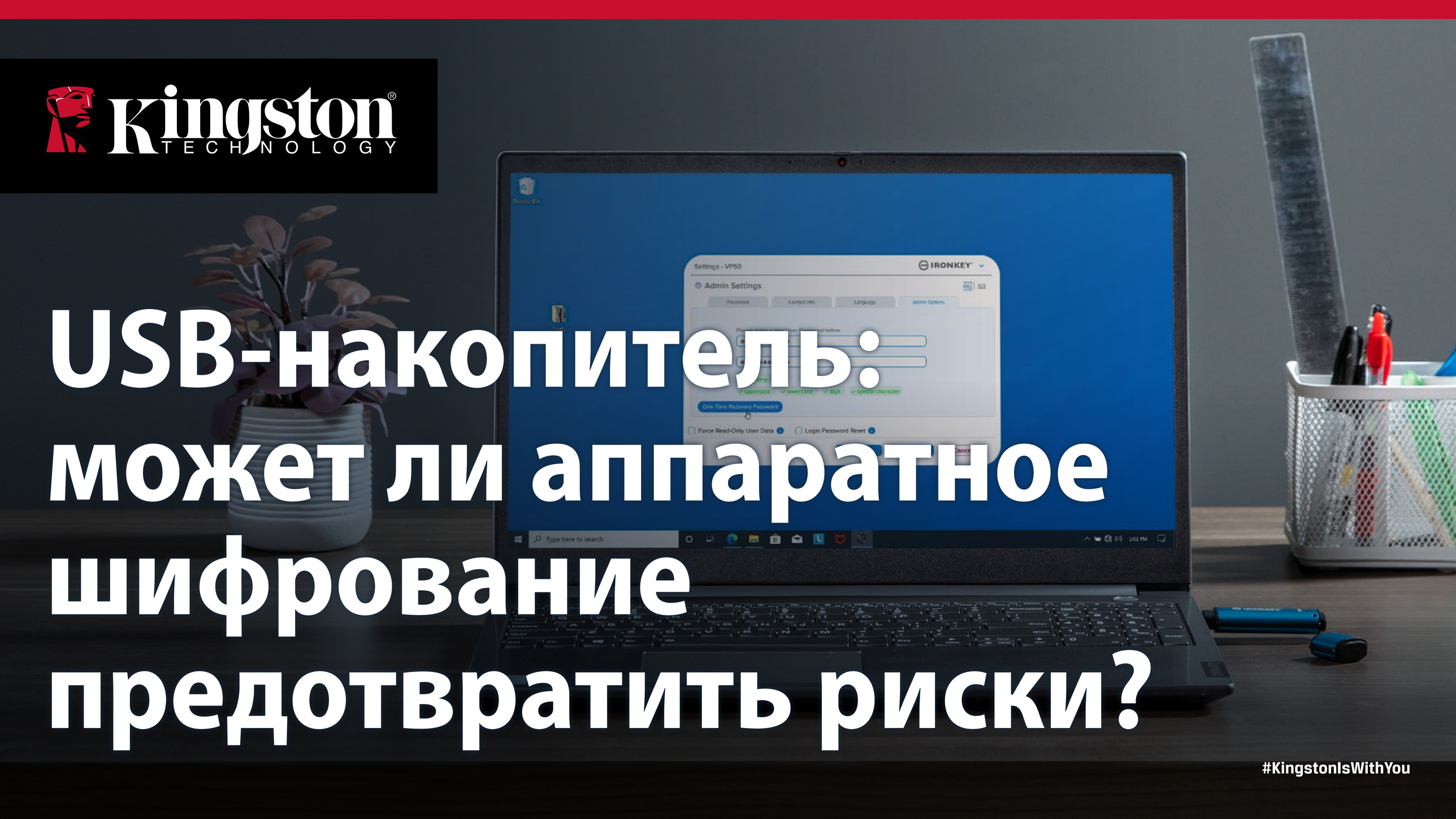

USB-накопитель: может ли аппаратное шифрование предотвратить риски?

#KingstonIsWithYou

USB-накопитель: может ли аппаратное шифрование предотвратить риски?

Предисловие и содержание

Вопросы кибербезопасности беспокоят компании больше, чем когда-либо. Однако слишком много организаций не информированы о киберугрозах и недостаточно подготовлены к ним. В США только в 50% предприятий есть план кибербезопасности; из них 32% не обновляли свои планы кибербезопасности с начала пандемии COVID-19, когда многие организации перешли на удаленные или гибридные модели работы (по данным UpCity). А частота кибератак только растет: во всем мире количество предприятий, пострадавших от атак программ-вымогателей, увеличилось с 37% в 2020 г. до 66% в 2021 г.[1]

Нарушения кибербезопасности могут иметь разрушительные последствия для бизнеса. Это связано не только с деньгами. Потеря данных, безопасности и репутации могут негативно повлиять на организации во многих отношениях как в краткосрочной, так и в долгосрочной перспективе.

Одним из распространенных носителей угроз кибербезопасности являются USB-накопители. Они широко используются во многих организациях из-за своей простоты: чтобы использовать накопитель, просто вставьте его в компьютер. Однако именно эта простота делает USB-накопители настолько уязвимыми для атак: все, что требуется злоумышленнику, чтобы получить доступ к потенциально конфиденциальным данным, – это один потерянный или украденный накопитель. Именно в этом случае шифрование может сыграть важную роль в обеспечении безопасности использования USB-накопителей и снижении любых связанных с этим рисков для отдельных лиц и организаций. В этой электронной книге мы ответим на следующие основные вопросы:

- Почему USB-накопители с шифрованием так важны для защиты от кибератак?
- Где организации сами делают себя уязвимыми?
- Что они могут сделать, чтобы защитить себя?

Содержание	Страницы

USB-накопитель: может ли аппаратное шифрование предотвратить риски?

Авторы

Эта электронная книга была создана при участии ведущего представителя отрасли в области ИТ и новых технологий, а также нашего собственного технического эксперта.

Дэвид Кларк

Дэвид признан одним из 10 ведущих инфлюенсеров по версии Thompson Reuter's «30 самых влиятельных экспертов и идеологов в области социальных сетей, управления рисками, соблюдения нормативных требований и регуляторных технологий в Великобритании» и входит в список 50 ведущих мировых экспертов по мнению компании Kingston Technology.

Паси Сиуконен

Паси руководит группой экспертов, оказывающих поддержку по продуктам Kingston для таких подразделений компании Kingston, как связи с общественностью, маркетинг, продажи на местах, техническая поддержка и обслуживание клиентов. В основном он специализируется на линейках флеш-памяти и твердотельных накопителей.

Различие между обычными накопителями и накопителями с шифрованием

В то время как обычные накопители (без шифрования) чрезвычайно просты в доступе и использовании, аппаратное шифрование добавляет несколько уровней безопасности, как физических, так и цифровых, которые значительно повышают безопасность USB-накопителей. Легкая доступность, низкая стоимость и портативность стандартных накопителей без шифрования означает, что, хотя они очень удобны для пользователя, они также удобны и для злоумышленников, стремящихся украсть конфиденциальные данные, внедрить вредоносное ПО или программу-вымогатель в сеть компании и так далее. Широкое использование USB-накопителей создает много возможностей для кибератак. Вот два основных риска, связанных с обычными накопителями:

- **Атаки с использованием программ-вымогателей.** Эти атаки на основе USB-накопителей включают в себя внедрение вредоносных программ в корпоративные сети, захват информации о компании и/или систем с целью получения выкупа путем их шифрования. Они часто связаны с BadUSB и стали самым известным типом вредоносных программ.
- **Украденные данные.** Всё, что нужно злоумышленнику, чтобы легко получить доступ к данным, хранящимся на накопителе (информация о клиентах, исходный код или конфиденциальные финансовые данные и показатели продуктивности), – это потерянный, украденный или оставленный без присмотра накопитель без надлежащих средств защиты.

BadUSB – это атака, которая может использовать уязвимость USB-накопителей с незащищенным встроенным ПО, которое затем может быть запрограммировано вредоносной программой. Эти вредоносные инструменты невероятно распространены и легко доступны киберпреступникам, однако осведомленность о них остается низкой. Поэтому подобные атаки очень просто осуществить, заменяя встроенное ПО стандартного накопителя на взломанную прошивку, в которой USB-накопитель может маскироваться под клавиатуру и запускать, например, скрипты для атаки на брандмауэр. Множество кибератак осуществляется через ничего не подозревающих инсайдеров со злым умыслом или без такового. Поэтому невероятно важно, чтобы предприятия использовали накопители с шифрованием с защищенным встроенным ПО с цифровой подписью для их предотвращения. Это поможет снизить шансы киберпреступников на успех.

> **Стоимость восстановления инфраструктуры и, возможно, уплаты выкупа и удовлетворения других требований вымогателей огромна по сравнению со стоимостью управляемых USB-накопителей.**
> **- Дэвид Кларк**

Зачем использовать USB-накопители с шифрованием?

Накопители с шифрованием специально разработаны для защиты хранящихся на них данных, а также любых устройств, к которым может быть подключен накопитель. Таким образом, это ценные инструменты в ИТ-арсенале любой организации. Угрозы кибербезопасности становятся все более сложными, а вместе с ними совершенствуются и функции накопителей с шифрованием. Это помогает оставаться на шаг впереди киберпреступников, пытающихся использовать эти устройства. Как демонстрирует линейка накопителей Kingston IronKey™ с аппаратным шифрованием, такие функции, как как 256-битное шифрование AES в самом надежном режиме XTS, прочный и устойчивый к взлому корпус, встроенное ПО с цифровой подписью, виртуальные клавиатуры, режимы сложного пароля или парольной фразы и многие другие, которые разрабатывались и добавлялись на протяжении многих лет, гарантируют действительно хорошую защиту пользователей от всех видов атак.

Поскольку риски кибербезопасности часто осознаются плохо, многие компании предпочитают использовать стандартные накопители, несмотря на различные связанные с ними уязвимости. Здесь играет роль их доступность, низкая стоимость и использование программного шифрования, а также отсутствие корпоративного процесса одобрения флеш-накопителей. Слишком часто в организациях отсутствуют современные политики или процессы, отвечающие различным стандартам ИТ и кибербезопасности, таким как ISO27001, GDPR, SOC2 и рекомендованные для госучреждений практики WISP. Это означает, что риски часто оцениваются на основе мнений, а не фактов, что делает многие организации уязвимыми для атак.

Хотя некоторые могут использовать накопители диски с существующими инструментами программного шифрования, это часто может быть ложной экономией. Ведь многие накопители с программным шифрованием можно взломать с помощью бесплатных или платных инструментов, доступных в Интернете для всех. Программное шифрование также может быть удалено с накопителя простым переформатированием. Пользователем могут делать это для удобства или для использования накопителей на неподдерживаемых платформах ОС. В то же время USB-накопители с аппаратным шифрованием имеют постоянно включенное шифрование, которое нельзя отключить. Они специально сделаны для этого. Кроме того, они защищены от несанкционированного доступа, устойчивы к физическому взлому и используют встроенное ПО с цифровой подписью для обеспечения подлинности и целостности накопителя. Ограничение числа попыток ввода пароля (защита от атак методом подбора паролей) и виртуальные клавиатуры (защита от клавиатурных шпионов и регистраторов экрана) – это еще две функции накопителей с шифрованием, таких как IronKey VP50. Это означает их соответствие отраслевым рекомендациям по защите от злоумышленников, которые пытаются получить пароли у доверчивых пользователей.

Если накопитель IronKey обнаруживает изменение встроенное ПО, он блокируется и не загружается, тем самым повышая кибербезопасность.
- Паси Сиуконен

Кто подвергается риску?

На самом деле, риску подвергаются любые компании, которые не могут контролировать доступ через USB. И часто они не осознают, в чем именно заключаются эти риски. Однако есть факторы, которые могут сделать некоторые компании более привлекательными – и уязвимыми – целями для кибератак.

Данные компаний в сфере здравоохранения и финансов не только гораздо более привлекательны для киберпреступников, но и более серьезно влияют как на сами организации, так и на их клиентов. В Великобритании кибератака 2017 года, нацеленная на Национальную службу здравоохранения (NHS), привела к отмене более 19 000 назначений и обошлась NHS в 92 миллиона фунтов стерлингов в виде упущенной выгоды, а также затрат на восстановление данных и систем. Это не только помешало пострадавшим пациентам получить медицинскую помощь, но и вызвало резкую критику Национальной службы здравоохранения за то, что она не реагировала быстро или достаточно активно на предыдущие предупреждения о киберугрозах. Несомненно, все организации должны быть в курсе последних событий и хорошо осведомлены о кибербезопасности. Однако тем, кто имеет дело с конфиденциальной информацией, особенно с данными специальной категории, следует быть бдительными в отношении киберрисков вдвойне.

Чем выше стоимость компании (измеряемая ее оборотом), тем больше вознаграждение для злоумышленников и, следовательно, тем выше риск киберугроз, с которыми компания сталкивается. Однако это не означает, что небольшие организации не должны беспокоиться о кибербезопасности. Хотя крупные предприятия могут быть и более привлекательными целями для атак, у них часто также есть ресурсы и выделенный персонал для борьбы с киберугрозами. С другой стороны, во многих малых и средних компаниях нет специальных групп по кибербезопасности, и там делают исключения для руководителей высшего звена, чтобы избежать управления USB-доступом. И это делает такие компании особенно уязвимыми и ведет к разрушительным последствиям. Ряд исследований показывает, что малый и средний бизнес больше подвержен кибератакам.

Риск еще выше для сотрудников, занимающих высшие руководящие должности. Этих людей легко отследить, и они часто имеют исполнительные полномочия в своих организациях, а это означает, что к ним не применяются меры киберконтроля, такие как процедуры управления USB-доступом. В результате они становятся выгодными целями для киберпреступников. Именно в этом случае накопители с постоянно включенным аппаратным шифрованием, а также хорошая осведомленность о кибербезопасности и использование передовых методов и процессов, могут в значительной степени помочь в снижении риска и защите от атак.

Многие из последних успешных атак были совершены злоумышленниками, которые специализируются на использовании помощи инсайдеров (добровольной или неосознанной).
- Дэвид Кларк

Кто подвергается риску?

Организации делают недостаточно для противодействия угрозам кибербезопасности.
- Дэвид Кларк

Цепочка поставок – еще одна потенциальная точка уязвимости организаций, и атаки на цепочку поставок очень распространены. В 2013 году американский ритейлер Target столкнулся с одной из крупнейших утечек данных в истории розничной торговли, в результате которой была раскрыта информация о дебетовых и кредитных картах более 40 миллионов клиентов. Хотя сама компания Target была очень обеспокоена кибербезопасностью и внедрила обширную систему кибербезопасности за 6 месяцев до атаки, злоумышленники проникли в систему одного из сторонних поставщиков Target и через него получили доступ к основной сети передачи данных Target. Всего против Target было подано 90 исков, и, как результат утечки данных, компания потеряла 61 миллион долларов. Хотя она, возможно, и не несет прямой ответственности за атаку, этой слабости в кибербезопасности цепочки поставок было достаточно, чтобы нанести как финансовый, так и репутационный ущерб.

Обходные пути, используемые сотрудниками, также могут быть источником уязвимости. Хотя они и позволяют сотрудникам более эффективно выполнять свою повседневную работу, при этом слишком часто игнорируются основные процессы безопасности и рекомендации, такие как управление паролями. Хотя рекомендации NCSC и CISA довольно просты, реализовать их на практике часто сложнее, особенно для сотрудников, которые не знакомы с ИТ и кибербезопасностью. Хотя наличие специальной группы по кибербезопасности и может помочь, предоставление сотрудникам нужных инструментов, таких как накопители с аппаратным шифрованием, позволяет значительно снизить риски, связанные с обходными путями.

Сегодня USB-накопители с аппаратным шифрованием можно легко внедрить и интегрировать в существующие политики кибербезопасности. Доступны модели с различными интерфейсами (графический, клавиатура, сенсорный экран), с широкой поддержкой операционных систем и в вариантах емкости, которые удовлетворят потребности любой организации. - Паси Сиуконен

Как организации могут снизить риск подвергнуться кибератакам?

С организационной точки зрения есть ряд вещей, которые можно сделать для защиты оконечных устройств и данных. Без GRC (управление, риски, соответствие требованиям) кибербезопасность обречена на провал, поэтому знание и соблюдение процессов невероятно важно для защиты компаний. Наличие надежного программного обеспечения для защиты оконечных устройств также может нейтрализовать ряд киберугроз, а также позволит реагировать максимально быстро, если потребуется устранение каких-либо уязвимостей безопасности.

Внедрять ли обязательные политики шифрования или нет – это такой же важный или, возможно, даже более важный вопрос для управления рисками, как и вопрос о том, хотите ли вы создавать резервную копию своих данных… или нет. - Паси Сиуконен

Однако на индивидуальном уровне оборудование с шифрованием может значительно снизить уязвимость к угрозам кибербезопасности. С распространением моделей удаленной и гибридной работы, особенно в сочетании с увеличением числа кибератак в прошлом году, исключительно важным становится обеспечение безопасности обработки, передачи и считывания данных компании сотрудниками на всех уровнях организации. USB-накопители с аппаратным шифрованием позволяют пользователям получить преимущество портативности и простоты флеш-накопителей, а также значительно снижают связанные с ними риски. В то время как потерянный или украденный обычный накопитель может означать потерю данных, денег, репутации и так далее, накопители с аппаратным шифрованием обеспечивают защиту конфиденциальных данных от широкого спектра атак. И по мере того, как киберпреступники разрабатывают новые способы атак, накопители с шифрованием также будут продолжать совершенствоваться, чтобы противостоять этим новым вызовам.

В целом, затраты на устранение последствий кибератаки могут быть огромными. И, хотя внедрение и использование накопителей с шифрованием на организационном уровне может потребовать более тщательного согласования и настройки, это может сэкономить компании много денег – как с точки зрения выплаты сумм, требуемых вымогателями, так и с точки зрения упущенной выгоды из-за испорченной репутации – в долгосрочной перспективе. Одни только судебные издержки, связанные с нарушением безопасности, могут легко покрываться дополнительными расходами на USB-накопители с аппаратным шифрованием.

Благодаря долгосрочным обязательствам по предоставлению отличных USB-решений с шифрованием, портфель продуктов Kingston позволяет любой организации выбрать вариант в соответствии со своими конфигурациям кибербезопасности – обязательное аппаратное шифрование, отвечающее отраслевым стандартам, конструкция, соответствующая политике защиты оконечных устройств, возможности управления устройствами. - Паси Сиуконен

Выводы

Специалисты Kingston всегда следят за развитием событий в сфере кибербезопасности, обеспечивают соответствие накопителей IronKey с шифрованием актуальным требованиям и удовлетворяют потребности в кибербезопасности как больших, так и малых организаций. Поскольку кибербезопасность по-прежнему вызывает все большую обеспокоенность во всем мире, мы уверены, что правильные инструменты и знания помогут организациям хорошо подготовиться к решению этих проблем, в то же время защищая себя, своих сотрудников и клиентов.

О компании Kingston

За более чем 35 лет работы компания Kingston накопила знания, позволяющие выявлять и решать проблемы заказчиков, связанные с мобильными данными. Благодаря этому ваши сотрудники смогут работать легко и безопасно, не ставя под угрозу свою организацию.

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021