RICOH
imagine. change.

Решения Ricoh в области безопасности

На страже вашего бизнеса

Кибератаки сегодня стали главной угрозой для стабильного и успешного функционирования бизнеса. Все компании, вне зависимости от их размера, постоянно подвергаются опасности стать жертвами вредоносных атак, таких как фишинг, DDoS или программы-шантажисты. Убыток от таких атак исчисляется миллионами. В 2017 г. специалисты института Ponemon установили, что среднемировая стоимость утечки данных составила $3,62 миллиона. В ближайшие годы эта сумма будет только расти, поскольку правительственные постановления, такие как «Общий регламент по защите данных» или GDPR, накладывают на компании обязательства по защите систем и данных, за нарушение которых предусмотрены значительные штрафные санкции. Во избежание таких штрафов компания должна обладать достаточными ресурсами для успешной защиты данных. Для этого необходимо оценить все уязвимые места компаний.

Серьезной проблемой на пути обеспечения кибербезопасности является переход компаний к цифровому документообороту, а также всевозрастающие объемы обрабатываемых данных. Зачастую они рассредоточены по разным устройствам, сетям и регионам. Наиболее уязвимой информация становится в результате обмена данными, так как необходимо обеспечить ее безопасность на каждом этапе. Учитывая эти риски, современные компании больше не могут функционировать без систем по защите и контролю данных. В то же время возможности офисных принтеров и многофункциональных устройств за последние годы возросли многократно. На сегодняшний день они обеспечивают ввод, вывод, передачу и хранение больших объемов корпоративных данных, поэтому эти устройства являются одним из самых эффективных способов борьбы с кибератаками, который незаслуженно недооценивают.

Многие современные компании предлагают средства защиты данных, однако именно Ricoh имеет многолетний опыт в этой сфере. Вот уже более 20 лет компания оснащает свои печатные устройства модулями полного удаления временных данных с жесткого диска.

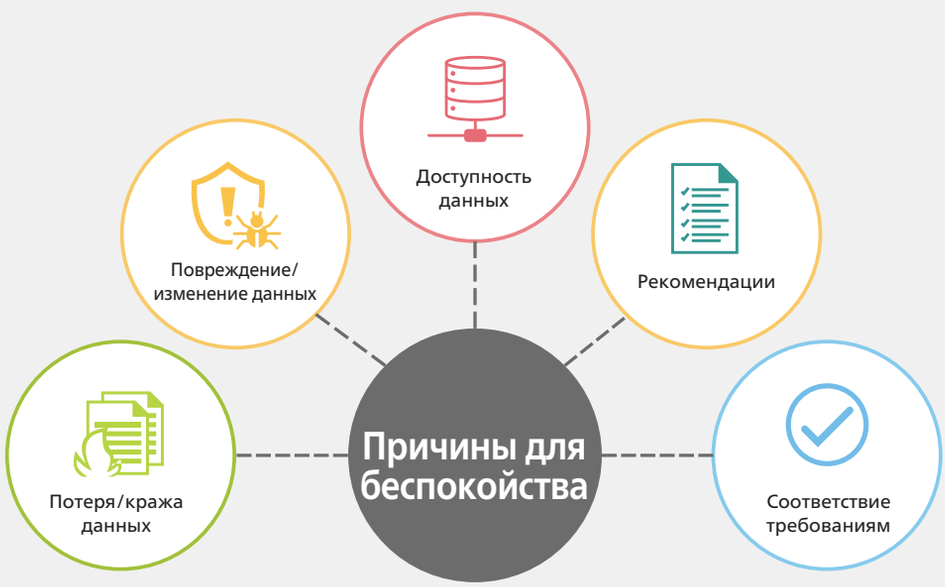
При создании нашей цифровой продуктовой линейки защита данных неизменно ставится во главу угла. На сегодняшний день установлено более четырех миллионов продуктов. Каждый наш продукт и каждая услуга сопровождаются встроенными возможностями безопасности. Также на многих продуктах Ricoh устанавливается собственная операционная система компании. Она обеспечивает необходимый уровень безопасности, который сложно достичь при работе с массово используемыми операционными системами, под которые зачастую и разрабатываются вредоносные программы.

Компания Ricoh предоставляет клиентам глобальный сервис и техническую поддержку, гарантируя эффективное функционирование средств защиты от кибератак по всему миру. Компания Ricoh не только использует в своих печатающих устройствах стандарт информационной безопасности IEEE 2600, но и является ведущим участником и разработчиком Ассоциации стандартов IEEE. Компания была отмечена сертификатом ISO 27001 и твердо намерена в дальнейшем соблюдать требования этой системы управления информационной безопасностью. При разработке своей продукции мы ориентируемся на потребности бизнеса и стремление наших клиентов защитить свои данные посредством различных глобальных инновационных клиентоориентированных программ.

Чтобы иметь возможность отвечать жестким требованиям передовых методов обеспечения эффективной кибербезопасности, мы изначально максимально защищаем свои продукты и услуги от возможных кибератак. Мы верим, что такой комплексный подход по защите данных является крайне необходимым для стабильного функционирования современного бизнеса.

ПРОБЛЕМЫ КЛИЕНТОВ В ОБЛАСТИ БЕЗОПАСНОСТИ

ТЕНДЕНЦИИ. С увеличением объемов данных возрастает риск кибератак и штрафных санкций.



Защита и расширение возможностей цифровых рабочих сред

Компания Ricoh стремится помочь в налаживании и защите цифровой обработки данных. В условиях современной цифровой экономики такой подход подразумевает повышение эффективности рабочей среды и выход за рамки традиционного офиса. Организация удаленных рабочих мест и привлечение удаленных сотрудников повышает гибкость и производительность компаний, что позволяет лучше соответствовать ожиданиям и требованиям клиентов.

Однако именно работа в сети представляет самую серьезную опасность для компании. Данные, создаваемые такими работниками, а также удаленные устройства, используемые для их сбора и хранения, должны быть защищены надлежащим образом. Сотрудники часто работают в различных сетях и регионах, что значительно усложняет поставленную задачу. Правительственные постановления, такие как «Общий регламент по защите данных» или GDPR, предписывают безоговорочно защищать данные на протяжении всего жизненного цикла, в противном случае компании вынуждены платить высокие штрафы. По мере все большего перехода к цифровому документообороту процесс хранения данных становится все более сложным. Давайте рассмотрим его шаг за шагом.

На первой ступени находятся устройства ввода и сбора данных — важнейший компонент Ricoh для обеспечения безопасности. Далее данные необходимо передать по сетям и надежно сохранить. На этом этапе решающее значение имеет сохранение целостности данных. Системы Ricoh ограничивают доступ пользователей к функциям устройства и сети, тем самым гарантируя неприкасаемость данных во время их пересылки или хранения. К этим услугам относится управление доступом, шифрование и защита от копирования. Этот этап называется «Контроль».

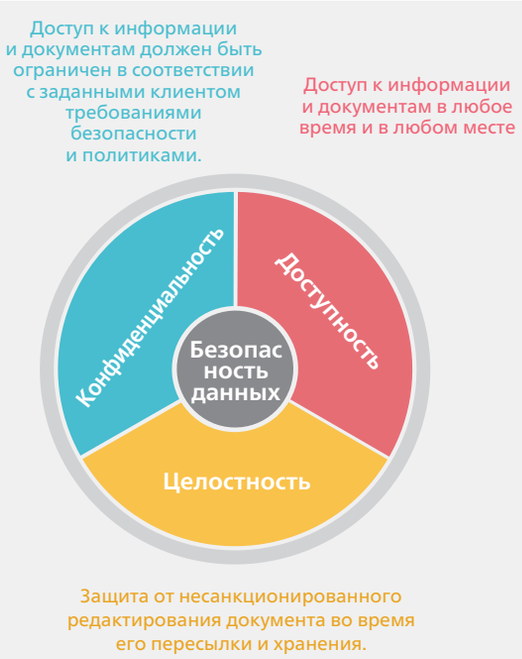
После сохранения документов следует обеспечить беспрепятственный доступ к данным заинтересованным лицам. От этого этапа зависит возможность их эффективного использования. Анализ данных является важнейшим компонентом продуктивного цифрового документооборота, при котором обеспечивается доступ к любым отделам компании. Средства авторизации предоставляют быстрый и защищенный доступ, независимо от местоположения пользователя или выбранного устройства. Крайне важно, чтобы средства защиты

от кибератак не препятствовали развитию или правильной работе компании, а также не вызывали у сотрудников негативное отношение. Этот этап называется «Сохранность».

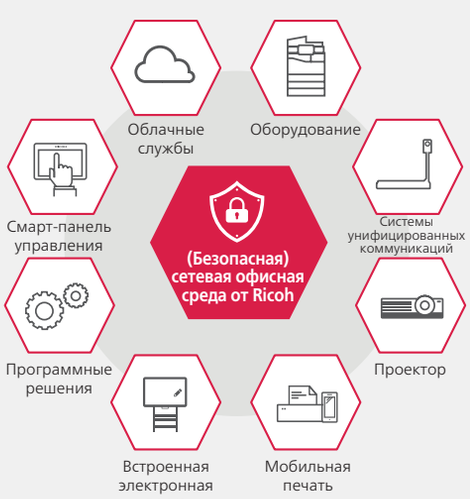
Наконец, эти данные необходимо удалить безопасным и контролируемым способом. Этот этап имеет крайне важное значение для соответствия нормативным требованиям и сводит к минимуму возможность последующей кражи или потери данных. Этот процесс фактически длится на протяжении всего периода существования документа, а также во время его окончательного удаления. После печати любого файла на жестком диске остается скрытое изображение многофункциональных устройств (МФУ), которое во избежание несанкционированного доступа необходимо перезаписать. Услуги утилизации данных, предоставляемые компанией Ricoh, включают очистку жесткого диска и памяти устройства, удаление ненапечатанного файла и стирание данных при выходе из системы для защиты остаточных данных от злоумышленников. Этот этап называется «Уничтожение».

Чтобы надежно обезопасить рабочие данные на протяжении всего жизненного цикла, компания Ricoh прибегает к принципам конфиденциальности и безопасности CIA. Конфиденциальность, доступность, целостность - это те основополагающие принципы, которыми мы руководствуемся при создании своих продуктов и решений для соответствия необходимым стандартам и постановлениям. Такой подход обеспечивает эффективное развитие и инновационность рабочей среды при сохранении оперативности и безопасности рабочих процессов.

ПОДХОД RICOH К ВОПРОСАМ БЕЗОПАСНОСТИ



Мы руководствуемся принципами конфиденциальности и безопасности CIA: конфиденциальность, целостность и доступность



Безопасность — наш приоритет. Продукты и услуги, предлагаемые компанией Ricoh, изначально включают в себя возможности для защиты данных

Компания Ricoh предлагает полный спектр продуктов и услуг по обеспечению безопасности для защиты всего жизненного цикла документа. Давайте подробно рассмотрим каждый ключевой этап процесса защиты данных: контроль, сохранность, уничтожение и поддержка.

ЧЕТЫРЕ УРОВНЯ ЗАЩИТЫ ЦИФРОВОЙ РАБОЧЕЙ СРЕДЫ

1 КОНТРОЛЬ

Эффективные средства управления данными имеют важнейшее значение для сохранения конфиденциальности и целостности данных. Корпоративная информация - это основной актив компании, поэтому она нуждается в надежной защите. Сегодня офисное оборудование выступает в качестве информационных терминалов, наиболее уязвимых для кибератак, поэтому для контроля и защиты данных компания Ricoh применяет различные инструменты аутентификации пользователя и управления устройствами. Сюда относятся настройки физических устройств, разрешающие и запрещающие доступ к некоторым функциям и данным. Ограничение доступа сотрудников к информации, пересылаемой посредством любого офисного многофункционального устройства (МФУ), является важнейшим и наилучшим способом защиты данных. На этапе контроля также предусмотрена защита устройств от вредоносных программ посредством применения трехуровневого подхода Ricoh к встроенному ПО.

Защита от несанкционированного копирования

В качестве средства защиты от несанкционированного копирования компания Ricoh предлагает функциональное решение по обеспечению безопасности печатных копий документов. Функция защиты от копирования заключается в следующем: во время печати или копирования на документ наносится специальный невидимый рисунок, встраиваемый в его фон. В случае копирования и/или сканирования печатного или скопированного документа встроенные рисунки проявляются на копиях. Благодаря модулю защиты данных от несанкционированного копирования МФУ обнаруживает встроенные рисунки и заливает копируемое изображение серым цветом, предотвращая утечку информации. Эта функция особенно необходима при печати конфиденциальной информации. Предотвращение дублирования конфиденциальной информации обеспечивает ее безопасность.

Блокировка печати

Документ, полученный с ПК, можно сохранить на жестком диске МФУ. При отправке документа функция блокированной печати просит указать пароль, который следует ввести с МФУ для его последующей печати. Благодаря функции блокированной печати документ невозможно распечатать до тех пор, пока его владелец не введет пароль на устройстве. Таким образом, любые операции с документом полностью контролируются его владельцем.

Усиленная защита сбора данных

Все решения Ricoh с усиленной защитой сбора данных обеспечивают соответствующие уровни шифрования и расшифровки на всех этапах процесса сбора данных. Администраторы наделены полномочиями разрешать доступ к очередям заданий посредством ввода данных пользователя или группы пользователей. К дополнительным уровням безопасности относится использование языка разметки деклараций безопасности (SAML) для технологии единого входа (SSO), проверка подлинности личности (PIV) и шифрование на основе инфраструктуры открытых ключей (PKI).

Встраиваемые функции аутентификации

Контроль доступа к устройствам и управление протоколами аутентификации для решений Ricoh можно осуществлять централизованно посредством идентификационной карты, PIN-кода, ввода регистрационных данных или комбинацией вышеперечисленных способов. Многоуровневая аутентификация повышает безопасность, но может замедлить работу занятых пользователей. Технология единого входа (SSO) позволяет пользователям свободно получать доступ к любым устройствам. Более того, на каждом устройстве установлены такие функции Ricoh, как быстрая аутентификация и программное обеспечение для аутентификации по идентификационным картам по принципу swipe-and-go («провел — и готово»), упрощающее доступ к документам. Считывающее или записывающее устройство с технологией NFC существенно упрощает процесс входа в систему, при этом обеспечивая эффективную защиту от

несанкционированного доступа к данным МФУ. Такой контроль доступа также осуществляется совместно с заданными настройками разрешений для МФУ, что ограничивает доступ пользователей к функциям устройств в соответствии с требованиями заказчика.

Streamline NX (SLNX)

Модуль управления печатной инфраструктурой, встроенный в платформу Ricoh Streamline NX, представляет собой программное решение Ricoh для контроля и мониторинга устройств в сети. С помощью этого программного решения администраторы могут просматривать или настраивать параметры безопасности для устройств, используя для этого преднастроенные пакеты шаблонов и пользовательские параметры. К важным параметрам безопасности относится включение и отключение проколов, параметры IP-адреса, пароли пользователей с правами администратора, адреса электронной почты для оповещений, параметры шифрования и т. д. Программное обеспечение SLNX также наделено функцией отправки отчетов о любых принтерах, которые не соответствуют требованиям, указанным в политике клиента.

Защита устройств от вредоносных программ

В целях защиты от вредоносных программ на всех устройствах Ricoh используется трехуровневый подход. Во-первых, управлять устройствами Ricoh можно только с помощью собственного машинного языка или операционной системы Ricoh. Во-вторых, для защиты программного обеспечения устройств от вредоносного вмешательства обновления встроенного ПО должны быть написаны и утверждены исключительно на машинном языке Ricoh. И в-третьих, каждое обновление встроенного ПО должно иметь цифровую подпись компании Ricoh. Такой трехуровневый подход защищает устройства Ricoh от использования не утвержденного встроенного ПО, тем самым исключая возможность появления вредоносных программ, шпионского ПО и вирусов.

Физические средства защита документов

Наиболее эффективные методы защиты не всегда являются самыми сложными. В офисах всегда многолюдно, поэтому печатные копии документов подвергаются наибольшей опасности из-за халатности сотрудников и возможности их кражи. Компания Ricoh предлагает целый ряд дополнительных физических средств защиты печатных копий документов от несанкционированного доступа. Так, например, замки на выдвижных ящиках с бумагами защищают от кражи конфиденциальных документов, например, бланков для рецептов в медицинских учреждениях. При размещении всех кабелей за закрывающими панелями значительно снижается вероятность вредоносного вмешательства изнутри компании. Решение для безопасной печати документов (Print-to-me) гарантирует печать документов только в присутствии их владельца, исключая риск кражи.

2 СОХРАННОСТЬ

В соответствии с новыми нормативными требованиями компании должны обеспечивать не только конфиденциальность информации, то есть ее защиту от кражи или утечки, но и ее постоянную целостность, то есть ее защиту от внесения изменений. Для этого компании должны строго контролировать доступ к конфиденциальным документам, обеспечить их защиту от несанкционированного изменения или фальсификации. Эти меры также обеспечивают защиту от целенаправленных и ситуативных атак.

Использование мобильных устройств усложняет любой план обеспечения кибербезопасности. Для безопасного обмена файлами необходимо применять дополнительные меры защиты. Такие файлы должны быть защищены как во время обмена между сетями и устройствами, так и во время хранения. Для защиты и сопровождения данных на протяжении всего их жизненного цикла эффективно используется технология сложного шифрования. Она применима не только к документам, но и для защиты сохраненных паролей, параметров макросов и адресных книг. Такое шифрование защищает целостность любой используемой информации даже в случае взлома: если злоумышленникам все же удастся получить доступ к сети, извлечь саму информацию не удастся.

Возможность бесперебойной работы имеет первостепенное значение во многих областях, поэтому непредвиденные обстоятельства, такие как стихийные бедствия, представляют прямую угрозу для компаний. Особенно уязвимыми в этом случае являются бумажные документы. Использование безопасного облачного хранилища для оцифрованных документов существенно повышает устойчивость к серьезным внешним воздействиям, таким как катастрофы природного или техногенного характера. Однако для сохранения цифровых данных необходимо принять соответствующие меры безопасности.

Шифрование важной информации

Чтобы защитить пересылаемую информацию, при перемещении данных на жесткий диск МФУ от Ricoh или их хранении на нем, можно применить шифрование. Встроенные программные средства выполняют комплексное шифрование сканируемых и печатаемых файлов с помощью ключа инфраструктуры открытых ключей (PKI) пользователя. Такой механизм отражает атаки с перехватом, осуществляемые изнутри информационной среды клиента.

Для дополнительной защиты данных предусмотрен модуль полного удаления временных данных с жесткого диска (DOSS) от Ricoh с функцией многократной перезаписи данных, подробное описание которого приведено в разделе «Уничтожение».

Защита BIOS и операционной системы

Все МФУ Ricoh оснащены доверенным платформенным модулем (TPM), который представляет собой защищенный от несанкционированного изменения аппаратный модуль безопасности. Модуль TPM выполняет криптографические функции и отвечает за безопасное хранение криптографических данных. На устройствах Ricoh модуль TPM отвечает за хранение корневого ключа шифрования, защищающего ключ шифрования данных жесткого диска и цифровой сертификат МФУ. С его помощью администраторы могут выполнять надежную загрузку: перед выдачей разрешения на выполнение этой операции модуль подтверждает подлинность встроенного ПО МФУ.

Проверка встроенного ПО

Корневой ключ и криптографические функции постоянно находятся в модуле TPM и защищены от изменения в обход брандмауэра, тем самым предотвращая злоупотребление или вредоносное вмешательство в наши продукты. Этот процесс гарантирует эффективную проверку встроенного ПО МФУ, удостоверения устройств и безопасности жесткого диска. Это еще один хороший пример того, что компания Ricoh создает МФУ, исходя из интересов безопасности своих клиентов.

Управление паролями

Устройства Ricoh выполнены с возможностью настройки несколькими пользователи с правами администратора, выполняющими на этих устройствах разные функции и использующие разные пароли. Пароли для этих пользователей настраиваются удаленно с помощью инструментов веб-администрирования и регулярно проверяются. Таким образом можно добиться разделения обязанностей, которое регламентируется многими государственными постановлениями, регулирующими деятельность компаний.

Ограничение доступа пользователя

С помощью инструмента Ricoh по управлению пользователями системные администраторы могут ограничивать привилегии доступа пользователей. Так, например, администратор может настроить привилегии таким образом, чтобы доступ к записанной на МФУ адресной книге могли получать только выбранные пользователи. Таким способом блокируется несанкционированный доступ к личной информации и к записям, хранящимся на офисных устройствах.

Функция блокировки пользователей

В случае последовательного ввода неправильных паролей для входа в систему МФУ Ricoh оценивает, является ли это действие попыткой взломать пароль. В результате включается функция блокировки имени подозрительного пользователя. Заблокированное имя пользователя не сможет пройти проверку подлинности, даже если впоследствии будет введен правильный пароль. Снять блокировку можно только по истечении определенного периода времени или при участии администратора, что является эффективной мерой защиты от потенциальных злоумышленников.

3 УНИЧТОЖЕНИЕ

Безопасное удаление данных является неотъемлемой частью любой комплексной киберзащиты. Крайне ошибочно полагать, что обязательства компании заканчиваются в тот момент, когда данные покидают пределы организации. Во многих нормативных документах предусмотрен комплексный подход к процессу уничтожения данных, что предотвращает любой риск последующей кражи или злоупотребления. Обязательства компании по защите данных нельзя считать выполненными, пока это не будет доказано.

Устройства с истекшим сроком службы и возвращенные офисные устройства могут служить скрытым источником конфиденциальной бизнес-информации. Компания Ricoh предлагает сертифицированные и контролируемые сервисы удаления данных из принтеров с истекшим сроком службы. Сюда входят материалы, о которых зачастую забывают пользователи, такие как сохраненные параметры сети, данные пользователей, данные жесткого диска и даже наклейки, оставшиеся на устройстве. Такие неудаленные данные несут серьезную угрозу раскрытия конфиденциальной корпоративной информации и сведений о сотрудниках. В целях соблюдения всех нормативных требований этот процесс также необходимо регулярно выполнять на протяжении всего срока службы изделия. Таким образом, гарантируется максимальный уровень контроля имеющихся данных.

Перезапись скрытых данных: модуль полного удаления временных данных с жесткого диска (DOSS)

В памяти жестких дисков МФУ сохраняются скрытые изображения данных документов для обработки заданий. Модуль полного удаления временных данных с жесткого диска от Ricoh стирает несохраненную информацию перед выполнением следующих заданий. Следовательно, даже в случае получения злоумышленниками доступа к жесткому диску, они не смогут воспользоваться «следами» каких-либо данных, оставшимися после выполнения предыдущих заданий. Компания Ricoh гордится тем, что вот уже более 20 лет это надежное решение успешно защищает конфиденциальные данные.

Услуги очистки данных по истечении срока службы

Компания Ricoh предлагает услугу полной очистки данных, которая предоставляется по истечении срока службы МФУ и принтеров, на которых все модули памяти и дисковый накопитель очищаются сертифицированными решениями обеспечения безопасности без возможности последующего восстановления. ИТ-услуги компании Ricoh также предполагают утилизацию оборудования, включая многоуровневые сертифицированные услуги стирания данных.

Замена жесткого диска и съемные носители

Компания Ricoh также предлагает услугу утилизации жестких дисков, которая дает возможность клиентам сохранить старый жесткий диск, заменив его новым пустым жестким диском по возвращении оборудования после истечения срока аренды. Таким образом, компании получают возможность полного и безусловного контроля своей информационной среды.

4 ПОДДЕРЖКА

С расширением компании также неизбежно растет число подключений между устройствами и сетями. Чтобы обеспечить расширение такой инфраструктуры без ущерба для безопасности, компаниям нужны надежные решения. Для этого необходимо обнаружить слабые места в системе и предпринять действия, упреждающие возникновение целенаправленных и ситуативных угроз.

Зачастую для анализа инфраструктуры компании и выявления уязвимых мест требуется помощь специалистов в области информационной безопасности. Многие компании не могут себе позволить содержание в штате ИТ-специалистов, обладающих необходимыми знаниями для обеспечения кибербезопасности. Такое бездействие чревато для компаний опасными последствиями.

Информационно-техническая поддержка, предоставляемая компанией Ricoh, включает в себя ИТ-обеспечение и услуги настройки, а также удаленный мониторинг, помощь службы поддержки и возможности управления пересылкой для дополнительного сопровождения процесса обеспечения кибербезопасности. Кибербезопасность зависит от целостного понимания рисков, которым подвергается компания. Группа Ricoh по реагированию на инциденты, связанные с безопасностью (SIRT), доводит до ведома клиентов по всему миру аналитическую информацию о серьезных угрозах безопасности и немедленно принимает координированные ответные действия.

Оценка безопасности инфраструктуры

Модуль управления печатной инфраструктурой Ricoh Streamline NX (SLNX) предназначен для выполнения важной функции контроля соответствия требованиям политики безопасности. С помощью SLNX руководители отделов информационных технологий могут настраивать устройства в соответствии с политикой компании, распределять эти параметры и анализировать их на основе наглядно представленного отчета. SLNX также имеет функцию оповещения управляющего персонала о несоответствии устройства политике компании.

Оптимизация процесса защиты печати

Наряду с профессиональными и управляемыми консультативными услугами для выявления слабых мест в системе обеспечения безопасности, сопряженных с использованием устройств, компания Ricoh предлагает комплексную услугу оптимизации процесса защиты печати (PSO). Этот наглядный веб-инструмент позволяет получить представление о текущем состоянии, на основании которого специалисты Ricoh могут дать рекомендации по продуктам с целью снижения риска.

Группа по реагированию на инциденты, связанные с защитой данных продукта (PSIRT)

Активным реагированием на новые угрозы и разработкой эффективных контрмер занимается группа Ricoh по реагированию на инциденты, связанные с защитой данных продукта (PSIRT). Эта программа Ricoh предназначена для обеспечения постоянного обновления всего продуктового пакета (аппаратного и программного обеспечения) и их защиты от новых угроз и атак. Таким образом мы поддерживаем неизменно высокий уровень обслуживания во всех странах мира и сводим к минимуму вероятные атаки на продукты Ricoh.

Сопроводительная документация

Подготовка и обучение являются неотъемлемыми составляющими процесса обеспечения кибербезопасности. Клиент должен получить всю необходимую вспомогательную документацию, руководства пользователя, техническую документацию по безопасности и обучающую документацию. Как и многие элементы кибербезопасности, безусловное соответствие требованиям имеет первостепенное значение, поэтому эти документы играют ключевую роль в защите чистого дохода компании.

ВОЗМОЖНОСТИ RICOH

Уникальная позиция Ricoh по предоставлению ведущих решений обеспечения безопасности всей информационно-технологической и печатной среды основывается, в частности, на сохранении глубокого понимания меняющихся рыночных условий и сообразного развития нашей деятельности. Наши решения предназначены для защиты любой информации на протяжении всего жизненного цикла и тесно связаны с четырьмя принципами обеспечения безопасности данных, представленными в настоящем отчете.

Мы работаем с опытными профильными специалистами, которые отвечают за анализ потребностей рынка, в том числе отраслевых требований, под которые могут быть созданы новые решения или адаптированы уже существующие.

Мы также активно работаем над развитием наших внутренних возможностей для разработки и развертывания решений по обеспечению безопасности.
С этой целью внутри организации по разработке услуг мы сформировали специализированные команды, занимающиеся разработкой новых услуг для правительства, услугами по управлению рисками, соблюдением требований, а также услугами обеспечения кибербезопасности.

Аутентификация и авторизация пользователя

- Блокировка печати
- Стандартное встроенное в SOP-панель программное решение для аутентификации
- Аутентификация пользователя и ограничение доступа
- Технология единого входа
- Несколько ролей администратора
- Защита паролем файлов PDF (пароль для сканированного документа)
- Защита от несанкционированного копирования
- Управление доступом на основе диапазона IP-адресов
- Безопасное управление устройствами и печатью
- PKI (инфраструктура открытых ключей) и поддержка смарт-карт
- Защищенная печать (функция print-to-me и блокировка печати)

Защита устройств от вредоносных программ

- Серверы
- Полная защита или меньшая подверженность действиям вредоносных программ
- Смарт-панель управления (SOP) на базе ОС Android с усиленной защитой
- Собственная ОС Ricoh (язык машинного управления) для МФУ
- Трехуровневый подход — цифровая подпись, скачивание через инструмент Ricoh, возможность записи только на специальном языке управления

Утилизация жесткого диска

- Утилизация жесткого диска, перезапись скрытых данных
- Услуга полной очистки данных
- Услуга по окончании срока службы: уничтожение данных в модулях памяти и на дисковом накопителе

Управление устройствами

- Настройка квот и лимит учетных записей
- DMNX — одна панель для прозрачного контроля безопасности, управления паролями, мониторинга и внесения изменений

Защита BIOS и операционной системы

- Безопасная загрузка с помощью доверенного платформенного модуля (TPM)

Перезапись скрытых данных и съемные запоминающие устройства

- Модуль полного удаления временных данных с жесткого диска (DOSS)
- Съемный жесткий диск

Шифрование данных

- Шифрование жесткого диска с помощью доверенного платформенного модуля (TPM)
- Ключи шифрования через TPM
- Сквозное шифрование печатных и сканированных файлов с помощью ключа PKI
- Жесткий диск с сертификатом FIPS (Федеральный стандарт обработки информации).
- Сквозное шифрование для печати
- Сквозное шифрование для сканирования

Обновления встроенного ПО и управление паролями

- Удаленный контроль паролей
- Функция блокировки пользователей
- Проверка встроенного ПО через TPM

Соответствие промышленным стандартам

- Сертификация ISO 27001
- Сертификация IEEE 2600.2 для выбранных продуктов
- Сертификация ISO 15408 для выбранных продуктов
- Документация по безопасности и обучение

МНОГОУРОВНЕВЫЙ ПОДХОД RICOH К ЗАЩИТЕ УСТРОЙСТВ

Нет никаких сомнений, что роль поставщика МФУ давно вышла за рамки простого транзакционного, однопланового предоставления оборудования для фактического управления данными. На сегодняшний день МФУ выполняют намного больше функций: от сбора информации из многоканальных точек ввода до классификации собранных данных и интегрирования рабочих потоков и их безопасного, надежного хранения и анализа. В этом сложном наборе многочисленных жестких нормативных правил и требований к хранению – в сочетании с внутренними и внешними угрозами, подвергающими записи риску потери, уничтожения или несанкционированного доступа, — мы применяем многоуровневый подход для защиты устройств, чтобы ваше МФУ и системы, с которыми оно соединено, гарантировало высокую степень защиты.

1. Устройство

Во главе любой модели Ricoh находится устройство. Безопасность является одним из ключевых условий при разработке, изготовлении и внедрении продукции. Собственная операционная система Ricoh лишена недостатков, характерных для многих массовых коммерческих операционных систем. Кроме того, наши устройства полностью отвечают сертификационным требования стандарта IEEE2600.2. Такие меры защиты, как шифрование жесткого диска с перезаписью данных, гарантируют абсолютную конфиденциальность обрабатываемых данных.

2. Смарт-панель управления (SOP) с удобным пользовательским интерфейсом

Как МФУ компании смарт-панель управления оснащена собственной операционной системой Ricoh. Здесь нет ни одного ненужного компонента, а доступ с правами суперпользователя отсутствует. Компания Ricoh усердно работаем над тем, чтобы введение смарт-панели управления не повлияло на защиту устройств.

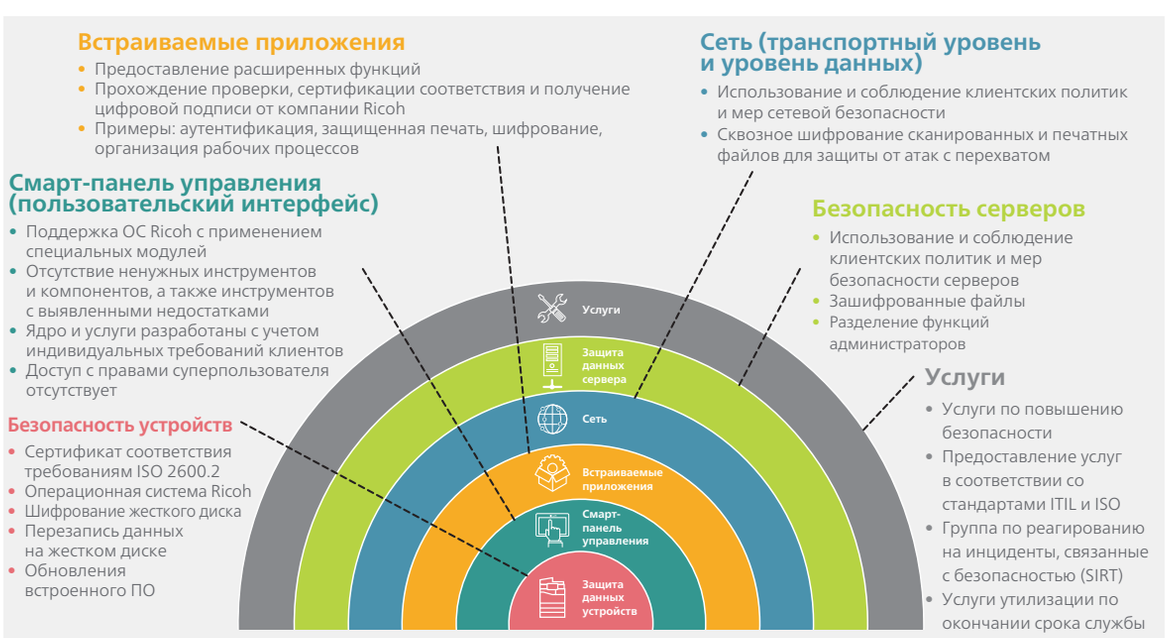
3. Приложения Smart

Такие приложения могут быть встроены в смарт-панель управления для расширения функциональных возможностей пользователя, включая организацию рабочих процессов и сбор данных. Некоторые приложения предоставляют важнейшие средства обеспечения безопасности. К ним относится защищенная печать, доступ по карте и шифрование. Разработкой приложений занимаются сотрудники компании Ricoh или участники Программы поддержки сторонних разработчиков Ricoh. Перед запуском на смарт-панели все приложения проходят проверку на совместимость Ricoh и должны иметь цифровые подписи.

4. Сеть и серверы

Независимо от того, кто управляет информационной инфраструктурой, компания Ricoh гарантирует, что предоставляемые ею продукты и услуги будут соответствовать вашим требованиям политики безопасности, предъявляемым к информационной среде и сети. Сквозное шифрование печатных и сканированных файлов, шифрование данных на серверах и разделение обязанностей администраторов — вот те методы, которые используются для защиты от атак с перехватом или внутренних угроз.

Мы предлагаем комплекс услуг по обеспечению безопасности. Сюда входит консультационная поддержка, услуги по мониторингу, оптимизации и контролю документов, а также информационная безопасность. Кроме того, по окончании срока службы устройств мы предлагаем услуги с полной очисткой оперативной памяти и жесткого диска устаревших устройств перед их утилизацией.



ЗАЩИТА ЦИФРОВЫХ РАБОЧИХ МЕСТ ОТ RICOH

Наши клиенты сталкиваются с целым рядом проблем, связанных с безопасностью, и все они объединены одной особенностью: с увеличением объемов данных также возрастает их уязвимость, повышается риск атак и увеличиваются штрафные санкции. Защита конфиденциальных данных от несанкционированного использования требует постоянной работы. Так, например, ежемесячно специалисты компании Ricoh отражают около 8 миллиардов атак брандмауэра. Существуют десятки тысяч международных, национальных и отраслевых предписаний по обеспечению безопасности данных, и компании должны постоянно подтверждать соблюдение каждого из них. Разумеется, все организации, независимо от размера, хотят найти партнера, на которого они смогут положиться, который поможет им обеспечить полную защиту данных благодаря комплексу решений с контролем всех рабочих процессов.

Компания Ricoh разработала целый ряд решений по устранению всевозможных рисков, с которыми сталкиваются компании. Природа кибератак развивается невероятно быстро, поэтому компания Ricoh использует в своей деятельности программы анализа мнения клиентов Voice of the customer, на основании результатов которых мы совершенствуем свои услуги.

Консультативные конференции с потребителями организуются в качестве основных стратегических фокус-групп, на которых мы можем лучше разобраться в тенденциях, движущих факторах и приоритетах, являющихся базисными для наших клиентов. Консультативные технологические конференции позволяют получить важные аналитические данные от ведущих руководящих сотрудников. На таких конференциях специалисты технических и научно-исследовательских отделов компании Ricoh узнают мнение клиентов об идеях, концепциях и прототипах. И наконец, компания Ricoh работает в сотрудничестве с отдельными клиентами над созданием новых усовершенствованных функций по обеспечению безопасности для клиентов вертикального и широкого рынков. Такой подход с привлечением клиентов не только помогает нам утвердить план разработки продуктов, но и дает нашим клиентам возможность получить доступ к глобальной сервисной сети.

Современная цифровая рабочая среда должна меняться в соответствии с возникающими киберугрозами, а также быть гибкой, под стать методам работы. Именно поэтому мы уверены, что кибербезопасность должна распространяться на все технологии наших заказчиков. Тот факт, что в своей организации мы безоговорочно руководствуемся стандартами ISO 27001 и все все наши продукты, а также развертываемая на них наша собственная операционная система Ricoh, соответствуют требованиям IEEE 2600, говорит в пользу того, что вы получаете передовые средства обеспечения безопасности, независимо от того, строите ли вы свой бизнес, или расширяете его.

Угрозы безопасности, законодательные требования и сложные отраслевые стандарты в совокупности ставят под удар репутацию и бюджет компании как никогда прежде. Пришло время объединить усилия с надежным партнером, который поможет вам обезопасить наиболее уязвимые активы вашей компании и добиться поставленных задач.

RICOH
imagine. change.

www.ricoh.ru