**DeviceLock Discovery предотвратит утечку ценной информации**

Последние десять лет, являясь микроскопическим по историческим меркам периодом, стали целой эпохой в плане развития микроэлектроники широкого потребления, компьютерных и телекоммуникационных технологий. Невероятный прогресс в этих областях кардинально изменил подходы к предоставлению доступа к используемым в бизнес-процессах данным, способам и средствам их хранения и передачи.

Любые сотрудники – это в первую очередь люди, со своими потребностями, проблемами и взглядами. Все они имеют свои рабочие задачи, контактируют с коллегами, партнерами и клиентами, что в совокупности образует бизнес-измерение их жизни. В то же время все они имеют устоявшиеся отношения с семьей, друзьями, различные личные интересы, образующие уже другое – личное – социальное измерение. При этом, что крайне важно, сотрудники всех организаций живут в обоих измерениях в одно и то же время, не разделяя для себя часы личной жизни и рабочие, что обусловлено в том числе возможностью прозрачно использовать доступные технические средства и сетевые сервисы для всех потребностей и коммуникаций – и личных, и служебных.

**Новая реальность**

В то же время службы ИБ отвечают за защищенность корпоративных данных, вне зависимости от личных интересов и пристрастий сотрудников других бизнес-подразделений, и при этом не должны разрушать производственные процессы. Преимущества от предоставления пользователям возможности использовать различные современные устройства и коммуникационные каналы всегда тесно переплетаются с рисками, вытекающими из этих возможностей.

Удобство использования современных устройств (включая традиционные флеш-накопители) и интернет-сервисов (в особенности социальных медиа, облачных хранилищ и мессенджеров) не оспаривается, равно как и следствие в виде повышения эффективности производственных процессов. Однако же, наряду с массой пользовательских удобств технологический прогресс способствовал созданию благодатной среды для целого класса новых угроз и рисков ИБ, невиданных доселе опасности и масштабов как результата сближения ряда основных факторов.

Это прежде всего коммерциализация киберпреступности, которая интересуется данными и только данными, а не взломом ради взлома. Действия злоумышленников направлены на хищение у бизнеса и государства наиболее ценных данных с последующей продажей или использованием для прямой кражи денег (например, выводом с карточных счетов). Нельзя сбрасывать со счетов легкодоступность и простоту использования съемных накопителей. Демонстрация уязвимости BadUSB на летней конференции Black Hat в Лас-Вегасе еще раз подчеркнула, что отсутствие надлежащего контроля USB-портов в организации может привести к краже интеллектуальной собственности всей компании за считанные секунды, и для этого будет достаточно всего одной зараженной флешки.

Практически все сетевые приложения (социальные сети, облачные хранилища, мессенджеры), созданные для удобства пользователей, для удовлетворения их социальных потребностей – функционируют абсолютно без какой-либо обратной связи с инструментарием корпоративной безопасности и контроля.

Модель информационной безопасности потребительских приложений основывается на том, что все решения о способах и уровне авторизации, аутентификации и уровне доступа к данным принимает конечный пользователь, который далеко не всегда является владельцем данных, будучи также сотрудником какой-либо организации. Ярким примером является использование облачных файловых хранилищ, когда сам работник решает, какие файлы хранить в облаке – и кому уже потом, после размещения данных в облаке – предоставить к ним доступ. Следовательно, современная корпоративная модель ИБ, чтобы стать реально эффективной, должна быть информационно-центричной, опираться на совокупность контроля непосредственно данных и различных потоков их передачи и распространения.

**Утечки можно предотвратить**

Для контроля различных каналов передачи и средств хранения данных широко используются решения класса Data Leak Prevention – DLP-системы. Однако практически невозможно предсказать, какие ухищрения может использовать инсайдер, желающий использовать корпоративные документы за пределами офиса, не говоря уже о том, что ряд современных DLP-систем все еще существенно ограничен по ширине контролируемых каналов и сервисов.

Именно поэтому в составе комплексных DLP-решений наряду с системами защиты от утечек данных при доступе к ним и их передаче исключительно важно применение компонентов поиска и предотвращения утечек хранимых данных, которые в англоязычном лексиконе обозначаются термином “content discovery”. Задачей таких discovery-компонентов является поиск и обнаружение в корпоративной ИТ-инфраструктуре конфиденциальных документов и данных, что позволяет своевременно выявить несанкционированное хранение данных сотрудниками и выполнить задачу превентивной защиты от утечки. Попросту говоря, X-фактор в проблематике утечки данных, когда заранее неизвестно, какой канал утечки, кем и когда может быть задействован, может быть успешно блокирован за счет discovery-компонента DLP-системы, то есть утечки данных могут быть пресечены еще до того, как инсайдер совершит попытку передачи или несанкционированного выноса конфиденциальных данных за пределы корпоративной инфраструктуры.

В октябре 2014 г. на рынке стран СНГ был представлен программный продукт DeviceLock Discovery, как самостоятельный функциональный компонент программного комплекса DeviceLock DLP Suite, позволяющий организациям контролировать местоположение и уровень защищенности конфиденциальных корпоративных данных, хранимых в ИТ-инфраструктуре, в целях проактивного предотвращения их утечек и обеспечения соответствия корпоративным стандартам безопасности и требованиям отраслевых и государственных регуляторов.

Посредством автоматического сканирования данных, размещенных на рабочих станциях Windows внутри и вне корпоративной сети, внутренних сетевых ресурсах и системах хранения данных, DeviceLock Discovery обнаруживает документы и файлы, содержимое которых нарушает политику безопасного хранения корпоративных данных и осуществляет с ними различные опциональные превентивно-защитные действия, заданные в DLP-политике. Кроме того, при обнаружении документов, хранимых с нарушением политики, DeviceLock Discovery может инициировать внешние процедуры управления инцидентами, направляя оперативные тревожные оповещения в SIEM-системы, используемые в организации.

DeviceLock Discovery обнаруживает текстовые данные в файлах и архивах множества форматов, при этом использует различные методы анализа содержимого, включая поиск по ключевым словам и шаблоны регулярных выражений (RegExp) с поддержкой морфологического анализа словоформ. Для облегчения задачи создания правил контентной фильтрации продукт поставляется со встроенными промышленными и геоспецифичными терминологическими словарями, предопределенными шаблонами регулярных выражений для наиболее распространенных видов конфиденциальной информации, таких как номера паспортов, кредитных карт, транспортных средств и банковских счетов, адреса, и многое другое. Кроме того, DeviceLock предоставляет администраторам возможность разработки собственных словарей и шаблонов, а также модификации встроенных.

Встроенный модуль оптического распознавания символов (OCR) позволяет DeviceLock Discovery проверять текстовое содержимое графических файлов и изображений, встроенных в документы и другие объекты данных. Уникальной особенностью DeviceLock Discovery является наличие встроенного модуля OCR во всех компонентах комплекса DeviceLock DLP Suite, что значительно повышает общую производительность, сферу применения и надежность решения. В силу того, что графические объекты сканируются и проверяются встроенными в агенты модулями OCR непосредственно на контролируемых компьютерах, существенно снижается нагрузка на Discovery Server и каналы связи корпоративной сети.

В случае обнаружения в сканируемых документах и файлах содержимого конфиденциального характера DeviceLock Discovery может автоматически выполнить превентивные действия по устранению выявленных нарушений, такие как удаление (файла, архива или контейнера), изменение прав доступа или шифрование, а также тревожное оповещение администратора или уведомление пользователя о выявленном нарушении.

Компонент DeviceLock Discovery может приобретаться и использоваться как самостоятельный продукт независимо от прочих компонентов комплекса DeviceLock DLP Suite, так и как часть полнофункциональной DLP-системы.