Обзор методов защиты корпоративной информации

Алексей Парфентьев, *ведущий аналитик компании "СёрчИнформ"*

Общемировые траты на обеспечение информационной безопасности, по оценке Gartner[1], к концу 2017 года превысят $86 млрд. А еще через год компании потратят на защиту данных минимум 93 млрд. Производители предлагают клиентам новейшие разработки с элементами искусственного интеллекта и машинного обучения, а сервис-провайдеры – все более персонализированные услуги. Тем временем базовые методы ИБ неизменны. Разберемся, что это за методы и когда для их реализации достаточно даже встроенных средств операционной системы.

Защита от "человеческих" рисков

С точки зрения информационной безопасности "слабое звено" и наиболее вероятная внутренняя угроза – пользователь, который регулярно обращается к ресурсам и данным в корпоративной сети. Согласно результатам исследования IBM и Ponemon Institute[2], в 74% инцидентов роковую роль сыграла именно ошибка пользователя. Поэтому оставим за рамками обзора отказы и поломки оборудования, вирусные эпидемии, защиту от хакерских атак, инспекцию трафика, парсинг логов и другие методы противодействия технологическим угрозам. Сосредоточимся на пользователе как главной угрозе.

Повышение осведомленности пользователей

Почему пользователи совершают ошибки? Чаще всего – по незнанию и неосторожности. Устойчивость системы защиты информации прямо пропорциональна осведомленности и ответственности пользователей. Обучайте сотрудников, заставьте – буквально – выучить регламент работы с конфиденциальной информацией, исключите возможность получать привилегии "неофициально", в обход правил безопасности. Объясните серьезность потерь в случае халатности или незнания, закрепите личную ответственность за сотрудниками, в том числе финансовую.

Мониторинг прав доступа

Прежде всего необходимо провести аудит, чтобы определить уровни доступа и сценарии работы пользователей с документами и файлами.

В небольших фирмах разобраться в иерархии пользователей и уровней доступа под силу толковому системному администратору. Ему достаточно стандартных инструментов, чтобы следить за привилегиями и управлять правами доступа ко всем ресурсам и программам.

Для мониторинга прав в средних компаниях лучше воспользоваться централизованными инструментами, которые сканируют корпоративную сеть и автоматически определяют превышение полномочий или потенциально опасные действия пользователей с информацией. Таким инструментом служат, например, SIEM-системы.

В крупных компаниях рекомендуется еще более глубокая автоматизация аудита прав с помощью специализированных инструментов класса IDM. Внедрение и сопровождение IDM-решений – зачастую уникальный процесс, который учитывает особенности конкретной отрасли и каждого конкретного заказчика.

Главный принцип мониторинга, неважно, в "ручном" или автоматизированном режиме – ежедневный аудит всех объектов доступа. Цель заключается в том, чтобы ограничить пользователям возможность самостоятельно создавать новые объекты и тщательно следить за изменением привилегий доступа к уже созданным объектам. Иначе однажды в компьютере секретаря появится общедоступная папка с годовым финансовым отчетом.

Разграничение прав доступа

Следующий шаг – "урезание" прав: чем меньше у пользователя возможностей для умышленного или случайного нарушения, тем выше степень защиты информации. Разграничению прав предшествуют две важные процедуры.

Во-первых, следует составить список легитимных владельцев критичной информации в компании. Во-вторых – четко регламентировать обязанности сотрудников, определить ресурсы и документы, необходимые для бесперебойного рабочего процесса. Например, если бухгалтер останется без доступа к таск-трекеру отдела разработки

В крупных компаниях рекомендуется более глубокая автоматизация аудита прав с помощью специализированных инструментов класса IDM, нежели для среднего или небольшого бизнеса. Внедрение и сопровождение IDM-решений – зачастую уникальный процесс, который учитывает особенности конкретной отрасли и каждого конкретного заказчика.

[1] *http://www.gartner.com/newsroom/id/3784965*

[2] *http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2016_Cyber_Resilient_Organization_Executive_Summary_FINAL.pdf?__hssc=91022085.1.1479321260544&__hstc=91022085.b9ace5e69c9e94f7c9e7be3172a8cd77.1479321260544.14793212*

и не увидит, какие задачи в списке у отдела техподдержки, работа бухгалтерии не остановится. Если у инженера забрать доступ к администраторской части корпоративного сайта для редактирования новостей, процесс разработки продуктов не пострадает.

Выбор инструментов для разграничения прав доступа – "дело вкуса". Для этого подойдут и средства Active Directory, и Web-сервисы, и встроенные опции приложений – любой современный ИТ-продукт предоставляет возможность тем или иным способом организовать уровни доступа.

Важно только, чтобы разграничение прав пользователей в корпоративной экосистеме приобрело качества цикличной операции. По мере развития компании, изменения бизнес-процессов или штатного расписания неизбежно появляются пользователи с недостаточными или, наоборот, избыточными правами. Поэтому аудит и распределение ролей следует проводить регулярно.

Шифрование

В любой корпоративной сети всегда есть критичная информация, которую недостаточно защитить, ограничив к ней доступ. Простой и самый очевидный пример – персональные данные сотрудников. Дополнительную защиту чувствительных данных обеспечивают средства криптографии.

Шифрование – простой и доступный метод защиты информации. Он обеспечивает безопасное перемещение данных внутри компании и через Интернет, когда сотрудники пересылают информацию по сети, например, обмениваются документами через файл-сервер или рассылают письма. Еще шифрование защищает от физических угроз, включая кражи или потери ноутбуков, подключаемых устройств, внешних носителей информации. В любой из подобных ситуаций зашифрованные данные оказываются бесполезны для злоумышленников.

Линейка криптографических инструментов варьируется от встроенных средств операционной системы и аппаратных сетевых устройств для шифрования трафика до шлюзов шифрования каналов связи и специализированных средств шифрования, например шифрования баз данных.

Выбор инструментов для разграничения прав доступа – "дело вкуса".

Практически все алгоритмы шифрования, которые используются в ВТ-продуктах, надежны и способны защитить данные. Разница, безусловно, присутствует, но в реальной жизни роли не играет. Данные, зашифрованные даже самыми простыми средствами криптографии, в подавляющем большинстве случаев останутся недоступны для злоумышленников.

Другая особенность применения метода шифрования связана с влиянием на скорость рабочих процессов. Увлечение шифрованием сверх меры замедляет работу, например, использование чрезмерно криптостойких алгоритмов при копировании информации на флешку может отнять у пользователя в 2–3 раза больше времени, чем использование классических алгоритмов.

Адекватная мера шифрования означает выбор в пользу незаметного в работе, быстрого алгоритма без объективных рисков раскрытия данных. С позиции бизнеса нерационально тормозить работу компании сложными криптографическими алгоритмами только ради того, чтобы злоумышленники потратили не десятки, а сотни лет на расшифровку. Поэтому информация на конечных точках чаще всего шифруется либо не очень сложным специализированным софтом, либо встроенными средствами Windows.

При всех достоинствах шифрование не защищает от главной внутренней угрозы – человеческого фактора. У пользователей есть доступ к ресурсам и "ключи" от зашифрованных файлов. Чтобы обезопасить корпоративную информацию от инсайдерской активности, нужно двигаться дальше – к контентному анализу.

Контентный анализ

Контентный анализ отвечает на вопросы, с какой информацией работает пользователь и является ли эта информация (конкретный документ или файл) критичной для компании.

Для этого нужно провести "инвентаризацию" файлов и документов, которые хранятся в папках общего доступа и на жестких дисках пользовательских компьютеров, в базах данных, корпоративных NAS (сетевых хранилищах), SharePoint, Web-серверах и других объектах ИТ-системы. Требуется такой инструмент, который обнаружит информацию ограниченного доступа в любом "заброшенном уголке" корпоративной инфраструктуры. Данную задачу лучше других решают DLP-системы с функцией контроля данных "в покое" (Data at Rest).

Итого

Защита конфиденциальной информации – цикличный процесс, который в большей степени зависит от организационных, а не технических методов. Обучение пользователей правилам информационной безопасности, мониторинг и разграничение прав доступа, шифрование данных, внедрение DLP-системы – все перечисленные методы обеспечивают надежную защиту только при разумном и комплексном подходе. Грамотное сочетание основных методов способно многократно увеличить безопасность корпоративных данных и не допустить саму возможность случайных утечек данных или намеренного разглашения конфиденциальной информации. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru