Безопасная передача конфиденциальной информации в критичных и корпоративных сетях

Вячеслав Половинко, *руководитель направления собственных продуктов "АМТ-ГРУП"*
Илья Кондратьев, *заместитель директора Департамента информационной безопасности "АМТ-ГРУП"*

Как показывает практика 2019 и 2020 гг., все больше организаций реализуют меры защиты технологических процессов. Причины могут быть разными, например в результате категорирования в структуре компании были определены значимые ОКИИ и требуется реализация мер, определенных приказом ФСТЭК № 239.

Важную роль при реализации мер защиты играет сегментация сети передачи данных, причем практически везде осуществляется разделение на корпоративную (КСПД) и технологическую (ТСПД) сети передачи данных, или корпоративного и критичного сегментов. Однако современные и эффективные бизнес- и ИТ-процессы зачастую требуют информационного взаимодействия между КСПД и ТСПД. Для его безопасной реализации применяются различные способы: перенос данных через съемные носители, фильтрация трафика на МЭ, а также шлюзы однонаправленной передачи или, как их еще называют, диоды.

Следует отметить, что оснащенность средствами контроля и защиты КСПД и ТСПД в большинстве организаций заметно различается. Как показывает практика, в КСПД она значительно лучше. В КСПД, помимо ставших общепринятыми МЭ и средств антивирусной защиты, применяются и более продвинутые решения, например SIEM, WAF, DLP.

DLP и КИИ

О DLP хочется поговорить более подробно, особенно с учетом правоприменительной практики, в том числе уголовного преследования по ст. 274.1 УК РФ. Внимание на себя обращает тот факт, что вполне допустимой является трактовка судами фактов утечки информации ограниченного доступа за границы периметра КИИ как неправомерного воздействия на КИИ РФ[1]. Поэтому тема применения DLP на границах периметра и внутри КИИ требует обсуждения.

В большинстве случаев DLP применяется для контроля таких каналов утечки информации, как вывод на печать или копирование на съемные носители, электронная почта, вебдоступ к интернет-ресурсам. Даже общие папки на файловых серверах не остаются без внимания данных систем. Но при этом контроль утечек конфиденциальной информации фокусируется на внешнем периметре сети и АРМ КСПД, тогда как каналы связи и ПК, размещенные в ТСПД, далеко не всегда так же тщательно контролируются. Это происходит по следующим причинам, которые можно разделить на группы:

1. Технологические. На АРМ и серверы в ТСПД опасаются устанавливать средства защиты, дабы не нарушить работу технологического процесса.
2. Организационные. За корпоративный и критичный (технологический) сегмент отвечают разные подразделения/дочерние организации холдинга с различными задачами и приоритетами.
3. Психологические. ТСПД/критичный сегмент – особо защищенный и потому более доверенный, да и к тому же он отделен от КСПД межсетевым экраном или вообще однонаправленным шлюзом.

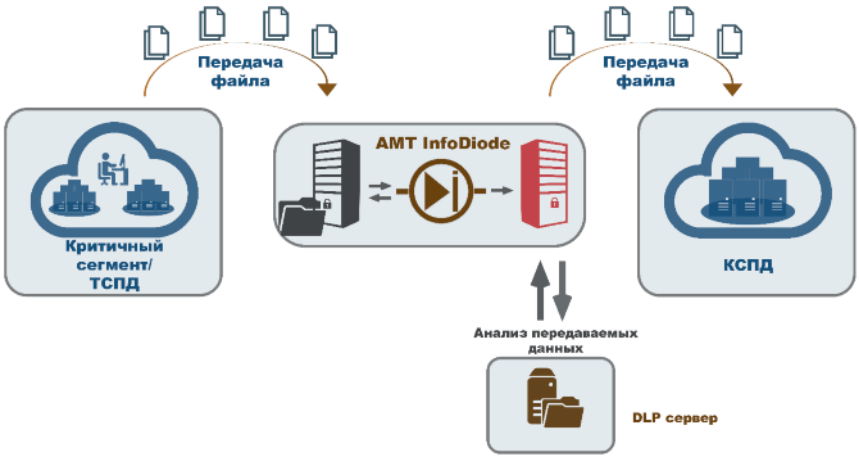
Таким образом, независимо от причин появляется вполне реально осуществимый и одновременно слабо контролируемый канал утечки – из информационных систем КСПД в критичный сегмент, внутри которого DLP зачастую не применяется. А если сетевое оборудование сегментов ТСПД и общих сегментов находится под единым управлением, то такой канал на практике не обнаруживается.

Использование однонаправленных шлюзов

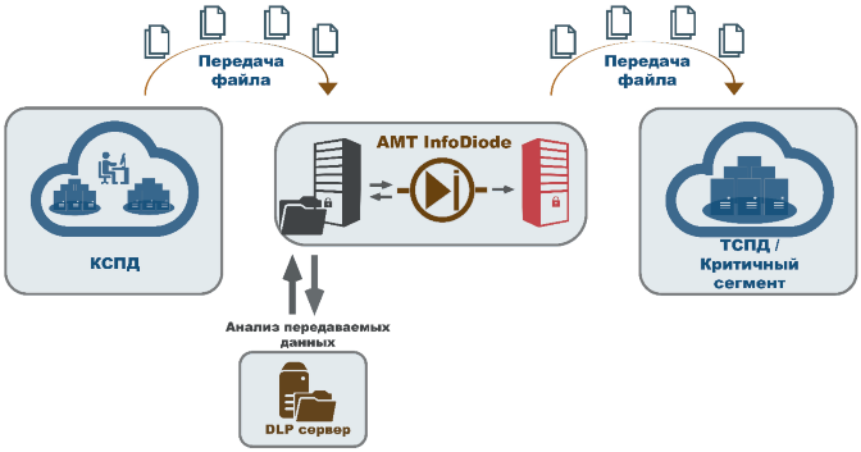
Рассмотрим более подробно ситуацию, когда для разделения критичного сегмента и КСПД применяются однонаправленные шлюзы. Типовой вариант применения однонаправленного шлюза предполагает его установку на границах критичного сегмента в целях гарантированной изоляции сегмента с меньшим уровнем доверия от сегмента с большим уровнем доверия.

[1] *Краткий обзор судебной практики по применению ст. 274.1 Уголовного кодекса РФ // Information Security/Информационная безопасность. 2020. № 2 .*

Сценарий 1



Сценарий 2



На практике наиболее распространены два сценария:

- сценарий № 1 – когда диод может быть "направлен"" из критичного сегмента;
- сценарий № 2 – когда диод может быть "направлен" внутрь критичного сегмента.

Оба случая требуют более детального рассмотрения в контексте применения DLP-решений.

Сценарий № 1

Утеря и/или хищение конфиденциальной информации происходит следующим образом: данные, хранящиеся в более доверенном сегменте, преднамеренно или непреднамеренно передаются через диод в менее доверенный сегмент.

В этом случае возможно реализовать промежуточную точку контроля для данных, передаваемых через диод. В ней осуществляется анализ передаваемых данных компонентом решения DLP, применяемого в КСПД. Это может быть как промежуточный файловый сервер, так и почтовый сервер, выполняющий роль MTA.

Такой сценарий представляется более простым с точки зрения интеграции с системой DLP.

Сценарий № 2

В этом случае, передавая предварительно полученные данные внутрь доверенного сегмента, злоумышленник использует АРМ или сервер в ТСПД для дальнейшего хищения данных и вывода их за границы периметра и не оставляет следов в силу ограниченности охвата ресурсов в ТСПД средствами контроля и защиты информации.

Предположим, бухгалтерская или CRM-система в корпоративном сегменте содержит данные конфиденциального характера. Такие данные, будучи похищенными, могут быть переданы в технологический сегмент, а оттуда – злоумышленнику скомпрометированным персоналом. Здесь важен как сам разовый факт утечки конфиденциальной информации, так и ситуация, при которой такие утечки в условиях отсутствия DLP в доверенном сегменте останутся незамеченными длительное время. Следовательно, сценарий № 2 более опасен.

Гарантированная защита

Эффективный контроль потоков при реализации как сценария № 1, так и сценария № 2 возможен с использованием интеграции между компонентами однонаправленного шлюза и DLP.

Наш опыт реализации комплексных проектов с применением однонаправленных шлюзов АПК InfoDiode показывает, что при организации взаимодействия с DLP следует ориентироваться на применение максимально универсального решения по интеграции "однонаправленный шлюз – DLP". Такое решение должно минимально зависеть от API конкретного производителя DLP и эффективно решать задачи выявления фактов передачи конфиденциальной информации в условиях применения разными заказчиками DLP-систем самых разных производителей.

В частности, для решения этой задачи каждый узел АПК InfoDiode предоставляет сетевой файловый доступ к содержимому и метаинформации по каждому передаваемому через себя сообщению. При включении соответствующей функции назначенной группе пользователей становится доступна папка dlp в корне файлового сервера. Содержимое этой папки состоит из набора пар файлов:

- <идентификатор сообщения>.data – содержимое передаваемого сообщения;
- <идентификатор сообщения>.meta – метаинформация о передаваемом сообщении, в том числе:
  - тип сообщения (File или Email);
  - полное исходное имя файла;
  - имя пользователя-отправителя;
  - объем принятого сообщения в байтах.

Предоставляемый таким образом доступ позволяет DLP-системе проводить регулярное сканирование папки файлового сервера с целью обнаружения передачи конфиденциальных данных.

С целью упрощения взаимодействия и необходимости реализации на системах DLP логики повторного сканирования файлов доступ через папку dlp предоставляется только к содержимому успешно принятых сообщений. Доступ к сообщениям, не принятым успешно, не предоставляется.

Прогрессивный подход к защите КИИ

Применение DLP-решений не только не теряет своей актуальности, но и выходит на новый уровень с учетом особенностей подходов по обеспечению защиты КИИ. Эффективное сочетание СЗИ повышает уровень защиты и минимизирует потенциальный ущерб организации от действий злоумышленников, направленных на похищение конфиденциальной информации. ●

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