Может показаться, что безопасность – это одни расходы. Но на самом деле это совсем не так. Давайте оценим прибыль, которую информационная безопасность приносит

Андрей Шпаков, *ведущий инженер-консультант*
Александр Веселов, *руководитель отдела технического консалтинга ООО «С-Терра СиЭсПи»*

Защита СХД и ЦОД

Эффективная защита высокопроизводительных каналов связи

Традиционно на производителей продуктов информационной безопасности и интеграторов в этой сфере смотрят как на «продавцов страха» и «помощников выполнения требований». В некоторой степени это так.

Особенно это актуально после принятия поправок в КоАП РФ, с учетом которых нарушение правил хранения персональных данных может караться штрафом в сумме до 200 000 рублей. Для сравнения: ранее сумма ограничивалась 10 000 рублей.

В такой ситуации риск понести финансовые убытки от нарушения законодательства значительно увеличивает рентабельность проектов информационной безопасности, особенно для малых и средних организаций.

Однако часто такие организации не имеют своих собственных подразделений информационной безопасности (ИБ). Внедрение и дальнейшее администрирование средств информационной безопасности становится головной болью подразделений ИТ. В связи с этим возникает разумное желание переложить такую ответственность на стороннюю организацию. Можно воспользоваться услугами аутсорсинговой компании либо перевести существующие сервисы или их часть в облачную инфраструктуру, под контроль сервис-провайдеров.

Второй подход дает явные преимущества, такие как сокращение капитальных инвестиций, улучшение качества поддержки, а главное, позволяет получить более качественную услугу в целом, но тоже стоит денег.

Не только расходы

Таким образом, может показаться, что безопасность – это одни расходы. Но на самом деле информационная безопасность – сервис для бизнеса (а не бизнес для «безопасников»).

Как бизнес может оценить качество сервиса? Очевидно, что для этого требуется сопоставить расходы и доходы. Определить расходы довольно легко – консалтинг, лицензии на программное обеспечение, аппаратные платформы, внедрение, поддержка и фонд оплаты труда сотрудников,

которые этим занимаются. А вот как быть с доходами?

Принято считать, что защищенность не приносит прибыли. На самом деле это не совсем так, точнее, совсем не так. Оценить прибыль от защищенности довольно сложно, но вполне реально. Конечно, определить ее с точностью до рубля не в наших силах, но можно оценить ее влияние на другие бизнес-процессы компании.

Продемонстрируем это на примере защиты сети хранения данных.

Пример из жизни

Постановка задачи. Основной и резервный центры обработки данных (ЦОД) некоей организации находятся на значительном расстоянии друг от друга, репликация данных происходит по протоколу iSCSI. Организация использовала арендованные выделенные каналы связи. За последний год использования произошло два инцидента – технический сбой у провайдера (устраненный в рамках соглашения об уровне услуг) и замечание от внешнего аудитора безопасности.

Трудно судить, чем был вызван технический сбой и что происходило с трафиком до и во время устранения неисправности, тем более что условия договора не были нарушены. Замечание внешнего аудитора касалось условий договора с оператором, согласно которому защита трафика не обеспечивалась. Кроме того, от пользователей в ИТ-отдел поступило несколько жалоб на низкую скорость передачи данных по каналу связи.

Решение. Для решения возникших проблем было предложено изменить тип канала связи – организовать защищенный канал с повышением пропускной способности. Затраты на выполнение этих работ можно было запланировать в расходной части бюджета следующего года.

Но заказчик выбрал альтернативный вариант. Он решил сменить провайдера, арендовать более дешевый канал связи, но с большей пропускной способностью и без услуг по защите.

Систему защиты решено было построить собственными силами и сетевую безопасность реализовать сертифицированными средствами защиты информации компании «С-Терра СиЭсПи». VPN-шлюзы и межсетевой экран разместили в виртуальной среде, которая была развернута ранее и имела существенный запас по ресурсам. Это позволило снизить капитальные затраты – не покупать новые аппаратные платформы (АП).

Задача была локальной и типовой, поэтому проектирование, внедрение и приобретение лицензий для виртуальных машин обошлись довольно дешево – они окупятся в течение двух лет (с учетом нового более дешевого провайдера).

Производительность канала нового провайдера с учетом системы защиты оказалась более высокой по сравнению с предшественником – соответственно была решена проблема со скоростью, поднятая ранее. Количество жалоб от смежных подразделений снизилось, что также является показателем эффективного решения стоящей задачи.

С появлением собственной системы защиты организация выполнила предписания аудитора – канал связи защищен, причем с использованием сертифицированных регуляторами средств. Все документировано, копии сертификатов приложены. Еще один показатель эффективности.

Еще один аргумент, о котором сотрудники подразделения ИБ скорее всего никому не скажут, но очень ему рады – это уверенность. Решение работает, оно под их контролем, они меньше зависят от провайдера, поэтому спокойны (но всегда начеку).

Мы рассмотрели эффективность безопасности на примере защиты канала между ЦОДами. Нам не удалось оценить ее с точностью до рубля. Но мы смогли показать целесообразность затрат и их окупаемость по сравнению с текущей ситуацией.

На этапе выбора решения некоторые тезисы были гипотезами, но спустя некоторое время после окончания реализации проекта заказчик сравнил параметры новой и старой систем – цену, инциденты, замечания аудитора и количество жалоб коллег. Результаты сравнения были более чем удовлетворительные.

За год использования построенной системы защиты не произошло ни одного инцидента ИБ в части защиты данных, передаваемых по каналу связи, т.е. их количество снизилось с 1 до 0. Число жалоб от отдела ИТ сократилось с 5 до 1. Виновниками единственной жалобы оказались сами «сетевики». У аудитора претензий не возникло.

На этом этапе можно утверждать, что не просто «стало лучше» или «стало безопаснее», а конкретно:

- Количество инцидентов уменьшилось на 100%, фактически они отсутствуют.
- Количество жалоб смежных подразделений уменьшилось на 80% (на самом деле тоже на 100%).
- Аудит пройден без замечаний.

За год использования построенной системы защиты не произошло ни одного инцидента ИБ в части защиты данных, передаваемых по каналу связи

Немного подробностей

Вопреки тренду перехода к сервисной модели заказчик решил построить собственную систему защиты с использованием С-Терра Виртуальный Шлюз. Основные аргументы – стандартный протокол, ГОСТ-алгоритмы шифрования, сертификация ФСБ России и ФСТЭК России и, конечно же, цена.

Закупка четырех лицензий на ПО даже не потребовала проведения конкурса – стоимость вместе с поддержкой была менее 500 000 рублей. Аппаратные платформы закупать не пришлось – были задействованы серверы из числа имеющегося у заказчика оборудования. Теперь заказчик уверен, что его данные надежно защищены.

Безопасность – сервис для бизнеса. Ее эффективность – величина не точная и трудноизмеримая. Частично ее можно выразить в финансовом эквиваленте. Изменение (уверены, что к лучшему) других параметров можно проследить через некоторое время, а в ходе планирования опираться на прогнозы и экспертные оценки. ADV