Александр ВЕСЕЛОВ
Руководитель отдела технического консалтинга ООО «С-Терра СиЭсПи»

ОСОБЕННОСТИ БАНКОВСКОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита нужна и важна. Целесообразность той или иной степени защиты определяет непосредственно банк, опираясь на аналитику современных угроз и требования регуляторов. При выборе перечня средств защиты учитывается множество факторов, основные — репутация продукта на российском и мировом рынке, функциональность и, конечно же, бюджет.

Финансовые организации всегда были удобной мишенью для злоумышленников. Основная причина такой ситуации — прямая связь объекта атаки с деньгами. Это понимают и сотрудники банков, и регуляторы, постоянно совершенствующие нормативную базу. Ситуация осложняется тем, что периодически появляются новые угрозы (в последнее время особенно актуальны внешние геополитические) и новые требования, и, как следствие, реализация защиты от текущих, уже известных угроз откладывается. Это может привести к печальным последствиям.

ВЫБОР — ДЕЛО НЕПРОСТОЕ

Выбор средств защиты информации огромен, но не все они удовлетворяют суровым банковским требованиям. Благодаря множеству отраслевых мероприятий, слава (или позор) того или иного продукта быстро становится достоянием всего банковского сообщества. Конечно, чаще хвалят западные продукты, но я, как представитель отечественной компании и участник многих банковских мероприятий, хочу отметить позитивный настрой в отношении решений российских производителей. Передовые представители финансового сектора уже поверили, проверили и используют отечественные средства информационной безопасности. Они делятся между собой положительным опытом, не забывая сообщать производителю обо всех возникших пожеланиях и рекомендациях. Такая обратная связь чрезвычайно важна, так как позволяет развивать продукты, чтобы они удовлетворяли всем потребностям и соответствовали ожиданиям заказчиков.

Наша компания — «С-Терра СиЭсПи» — уже более 12 лет работает на рынке сертифицированных средств сетевой защиты. Мы ориентируемся на мировые (IKE/ IPsec) и отечественные (ГОСТ 28147–1989, 34.10–2012, 34.11–2012 и т.д.) стандарты, но также важны для нас отзывы и пожелания от заказчиков и партнёров. Мы уделяем им особое внимание, учитывая при разработке следующих версий продуктов, расширяя перечень совместимых аппаратных платформ, оптимизируя условия технической поддержки, предлагая новые решения.

Уже сейчас в отечественных продуктах доступны многие удобные функции, например, привычный интерфейс (аналог Cisco IOS), стандартные протоколы, совместимость различных реализаций. Знакомый и дружественный интерфейс ускоряет процесс инсталляции продуктов, а также уменьшает количество инцидентов, связанных с человеческим фактором. Кстати, терминология, используемая в настройках продуктов С-Терра, является общепринятой и понятной каждому администратору. Поэтому начинающему инженеру потребуется лишь прослушать минимальный обучающий семинар для закрепления базовых навыков администрирования, а опытному специалисту для настройки и эффективной эксплуатации наших решений нужно только внимательно прочитать руководство.

ВЫПОЛНЯЕМ ТРЕБОВАНИЯ

Каждому банковскому «безопаснику» знаком Стандарт Банка России СТО БР ИББС-1.0–2014. Думаю, многие из них задавались вопросом — «Как выполнить все требования и при этом не создать в системе безопасности банка хаос вендоров?» Ответ вполне логичен — использовать продукты, реализованные на основе стандартных протоколов, условно независимых от производителя. И, поскольку персональные данные защищать необходимо, то этот производитель должен быть российским.

Стандарт Банка России
СТО БР ИББС-1.0-2014
Обеспечение информационной безопасности организации банковской системы Российской Федерации

7.4.14. При осуществлении доступа на участке телекоммуникационных каналов и линий связи, в том числе беспроводных, не контролируемых организацией БС РФ, должны использоваться сетевые протоколы, обеспечивающие защиту сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии двухсторонней аутентификации. …
7.7.3. СКЗИ, применяемые для защиты персональных данных, должны иметь класс не ниже КС2. …

Безусловно, я всегда рекомендую продукцию компании «С-Терра СиЭсПи». С каждой следующей версией продукты С-Терра становятся всё более мощными, быстрыми, функциональными. При этом, ведется огромная работа по соответствию законодательству, а именно — сертификация регуляторами — ФСБ России и ФСТЭК России. В частности, упомянутое требование по классу сертификации КС 2 выполняется как для программных VPN-клиентов, так и для программно-аппаратных шлюзов безопасности. Для тех, у кого модель угроз предполагает более жесткие требования к обеспечению безопасности, а именно — класс КС 3, мы также можем предложить несколько вариантов VPN-продуктов разной мощности.

ПЕРЕДОВОЙ ОПЫТ

Некоторые банки уже сейчас используют отечественные продукты (С-Терра, само-собой!) для решения самых разных современных задач по обеспечению безопасности. Приведу лишь несколько примеров:

Защита трафика банкоматов. Средства безопасности С-Терра защищают одну из самых масштабных сетей банкоматов в России. Программный продукт С-Терра Клиент установлен непосредственно в операционную систему каждого банкомата банковской сети, которая также защищена шлюзами безопасности С-Терра. Управление осуществляется централизованно и удаленно с помощью системы управления С-Терра КП. Применение этого простого и изящного решения позволило значительно сократить расходы на закупку и сопровождение средств защиты.

Поддержка скоростей шифрования 10Гб/сек и выше. Высокопроизводительные каналы связи обычно используют для взаимодействия между центральным офисом и ЦОД или между основным и резервным ЦОДами. Задача защиты таких каналов сама по себе нетривиальна, так как требует применения оборудования с особыми параметрами. Но если необходимо защитить перенос данных при миграции ЦОДа, то не обойтись без узкоспециализированных решений.

Поэтому, когда у одного из крупных банков возникла задача переезда ЦОД из одного региона в другой, наши специалисты предложили виртуозное решение для выполнения данной процедуры, да еще и без остановки пользовательских сервисов ЦОД. Оно основано на использовании программного модуля СТерра L2, использующего возможности шифрования на канальном уровне и интегрированного в мощные шлюзы безопасности. После завершения переезда нет нужды искать применение таким «навороченным» устройствам — их легко обновить и использовать для защиты корпоративной сети.

Защита удаленных рабочих мест сотрудников (в том числе с мобильных устройств). Региональные представительства, дополнительные офисы, филиалы, банковские пункты обслуживания в торговых центрах — сотрудники всех подразделений одного банка обычно имеют единую информационную базу. Доступ удаленных сотрудников банковских структур к этой информации надежно защищают продукты С-Терра, которые устанавливаются непосредственно на рабочее место — это клиент безопасности (С-Терра Клиент), либо устройство, обеспечивающее доверенный сеанс связи (С-Терра «Пост»), либо мобильный клиент (С-Терра Клиент-М). Неоспоримыми преимуществами решения являются совместимость всех продуктов С-Терра между собой, сертификация регулятором (вспоминаем требования!), удобство и экономичность использования.

РАЗДЕЛЯЙ И ВЛАСТВУЙ!

Следующий важный фактор в организации защиты информации — преодоление бюрократических проблем, а именно — разделение полномочий (бюджетных, эксплуатационных) между «безопасниками» и «айтишниками», а порой и сторонними аутсорсинговыми компаниями.

На этом этапе применяются в большей степени организационные меры, и поэтому он довольно трудоемкий и ответственный. Функциональность средств сетевой защиты для разделения полномочий сможет значительно его облегчить. Например, администратор ИБ занимается обновлением ключевой информации, ИТ-администратор — сетевой частью, служба эксплуатации — мониторингом. Эта важная функция тоже реализована отечественными производителями средств безопасности, в частности, мы предусмотрели ее выполнение в продуктах С-Терра версии 4.2. Кроме этого в следующей версии будет много полезного и интересного: поддержка мониторинга по SNMP, логирование Syslog и интеграция с популярными SIEM-системами Arcsight (Hewlett-Packard) и MaxPatrol SIEM (Positive Technologies).

* * *

Конечно, выбор средств защиты информации — непростая задача. Но желание, деньги и труд — все перетрут.