Интеграция и управление IT-безопасности – новые возможности современного бизнеса

(А. Березин, ОАО «ЭЛВИС-ПЛЮС»,

CIO.RU Директор №11, 2002г.)

Проблема

Современный этап развития корпоративных информационных систем (КИС) характеризуется все большим обострением противоречия между двумя бизнес-задачами. С одной стороны, интересы бизнеса требуют увеличения мобильности сотрудников и доступности информации в любой точке и в любое время. С другой стороны, все возрастающее влияние информации на эффективность бизнеса требует гарантий обеспечения конфиденциальности и целостности критичной для бизнеса информации также в любой точке и в любое время.

Очевидно, что разрешить указанное противоречие без применения сложных современных технологий обеспечения безопасности информации невозможно, и в некоторых случаях грамотный подход к делу позволяет добиться хороших результатов. Но тут возникает другая проблема. Технологии безопасности есть. Их много. Более того, их становится все больше и больше. Каждый производитель IT-продуктов (и даже услуг) считает своим долгом включить какой-нибудь сервис безопасности в свой продукт, будь-то операционная система, СУБД, маршрутизатор, бизнес-приложение и даже материнская плата компьютера. Входящие в состав КИС аппаратные и программные компоненты буквально напичканы разнообразными сервисами безопасности! Но разве это решает проблему? Кто реально способен грамотно воспользоваться всеми этими сервисами? Или другими словами, кто может сказать, что эффективно **управляет** всем этим хозяйством?

Но самое главное даже не это! Сложившаяся ситуация приводит к неудержимому возрастанию **стоимости владения** системой безопасности КИС, новым неудобствам и ограничениям для пользователей, головной болью для CIO (как найти хороших администраторов безопасности?) и еще большей головной болью для самих администраторов. И т.д. А в целом - абсолютная непрозрачность системы безопасности для самого бизнеса!!!

Подобная ситуация, к сожалению, типична для IT-индустрии в целом. Производители наперегонки сообщают о новых достижениях в своей сфере. То, что вчера было вершиной индустрии, сегодня уже «прошлый век»! К тому моменту, когда система наконец-то внедрена, заказчик понимает, что внедрил, оказывается, что-то ужасно старое и мало эффективное! Все это приводит к ситуации, когда пользователи просто физически не успевают осваивать новые технологии. Отсюда возникло известное правило «восемьдесят на двадцать»: 80% пользователей, например, MS Word используют только 20% возможностей пакета. И если в случае текстового редактора с этим можно смириться, то 20%-ное использование возможностей технологий безопасности, можно предположить, оставляет 80% «дыр» попросту не закрытыми!

Решение

И что же делать, спросите Вы? Безусловно из этой ситуации есть выход, и, наверное, даже не один. Мы полагаем, что два принципа, на которых должна строиться эффективная система безопасности КИС, есть ИНТЕГРАЦИЯ и УПРАВЛЕНИЕ:

- интеграция – построение системы безопасности КИС не в виде «лоскутного объяла», когда каждый продукт или подсистема безопасности решает только свои выделенные задачи и никак при этом не взаимодействуя с другими продуктами и подсистемами, а в виде **комплексной архитектуры безопасности**, когда все применяемые продукты и подсистемы выполняют одну общую задачу, дополняя и поддерживая функциональность друг друга;
- управление – технологическая (а также политическая!) возможность **целостного** управления комплексной архитектурой безопасности на основе общей политики безопасности компании.

Очевидно, что реализовать первый принцип возможно только на основе технологически совместимых между собой продуктах и технологиях. И сделать это можно двумя способами: либо строить всю систему на базе продуктовой линейки одного производителя (типа IBM Tivoli SecureWay), либо использовать продукты, разработанные в полном соответствии с открытыми стандартами. При этом следует различать два типа совместимости: А) «горизонтальная» совместимость – это **технологическая** совместимость между продуктами одного класса (т.е. по сути с продуктами конкурентов!); Б) «вертикальная» совместимость – это **архитектурная** совместимость между комплиментарными продуктами безопасности (PKI и сервер доступа, proxy-сервер и средство контекстной фильтрации, межсетевой экран и система обнаружения вторжений и т.д.).

Можно предположить, что реализация второго принципа возможна в случае, когда технологическая и архитектурная совместимость продуктов и технологий достигнет того уровня, когда станет возможно **общее управление всей системой безопасности**. Идеальный случай - управление с одной интегрированной консоли!

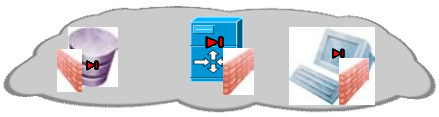
Следует сказать, что такое «идеальное» управление может быть только автоматизированным: ни один нормальный человек не в состоянии держать в голове всю функциональность управляемых устройств и все нюансы их настроек. Другими словами, такое управление возможно только на основе ПОЛИТИКИ. Работа администратора безопасности должна заключаться лишь в правильном программировании общей (или глобальной) политики безопасности компании и отслеживании ее изменений, а уж реализации этой политики применительно к каждому конкретному устройству – это «дело рук» системы управления.

Продукт

Очевидно, что описанный выше «идеальный случай» - это мечта. Вернее сказать, это вектор развития IT-индустрии безопасности, скорость движения по которому во многом зависит от активности и требовательности заказчиков. То, что мы имеем на сегодняшний день, это отдельные компоненты описанной выше управляемой архитектуры безопасности, которые в разной степени ее покрывают. В качестве примеров можно привести тот же Tivoli SecureWay, Symantec Enterprise Security Manager, CheckPoint Policy Editor и т.д. Мы надеемся, что одним из таких компонентов, **применительно к области сетевой безопасности**, может стать и отечественная разработка - последняя версия известных в России программных VPN продуктов ЗАСТАВА – ЗАСТАВА версии 3.3. Почему мы можем на это надеяться?

ЗАСТАВА 3.3 разработана **в полном соответствии с описанными выше принципами** – ИНТЕГРАЦИЯ и УПРАВЛЕНИЕ - что позволяет обеспечить как горизонтальную (VPN vs VPN), так и вертикальную (VPN vs PKI/NMS/AAA/LDAP) совместимость продукта в составе общей корпоративной архитектуры безопасности. Продукт состоит из следующих функциональных элементов:

- VPN агенты ЗАСТАВА 3.3 (ЗАСТАВА-Клиент, ЗАСТАВА-Сервер, ЗАСТАВА-Офис) – программные средства сетевой защиты информации, устанавливаемые на рабочие станции пользователей, серверные платформы и шлюзы (gateways). VPN-агенты ЗАСТАВА 3.3 обеспечивают полную реализацию принципа «сквозной безопасности» (end-to-end security) корпоративной политики безопасности; надежную защиту от атак, осуществляемых методами сетевого доступа как из локальной сети, так и из Интернет; реализацию разнообразных возможностей передовых протоколов безопасности IPSec/IKE; совместимость с комплиментарными средствами безопасности других производителей (IPSec, NMS, PKI, LDAP) а также удобную интеграцию с разнообразными токенами безопасности (iKey, e-token, smart-card и др.



- Центр управления безопасностью - Trusted Global Security Manager(TGSM) – высокоинтеллектуальная консоль управления агентами ЗАСТАВА 3.3, а также наиболее популярными на рынке VPN/FW агентами Cisco (IOS/PIX) и Check Point FW-1/VPN-1. TGSM реализует концепцию управления информационной

безопасностью корпоративной сети на уровне глобальной политики безопасности (на основе бизнес – объектов и бизнес – правил их взаимодействия), автоматизируя тем самым рутинную и изобилующую ошибками работу администратора безопасности по настройке конкретных средств защиты информации на местах. Применение TGSM для управления безопасностью распределенной корпоративной сети позволяет легко, быстро и безошибочно осуществлять эту операцию силами всего одного администратора. Тем самым существенным образом снижается общая совокупная стоимость владения (TCO) системой безопасности.

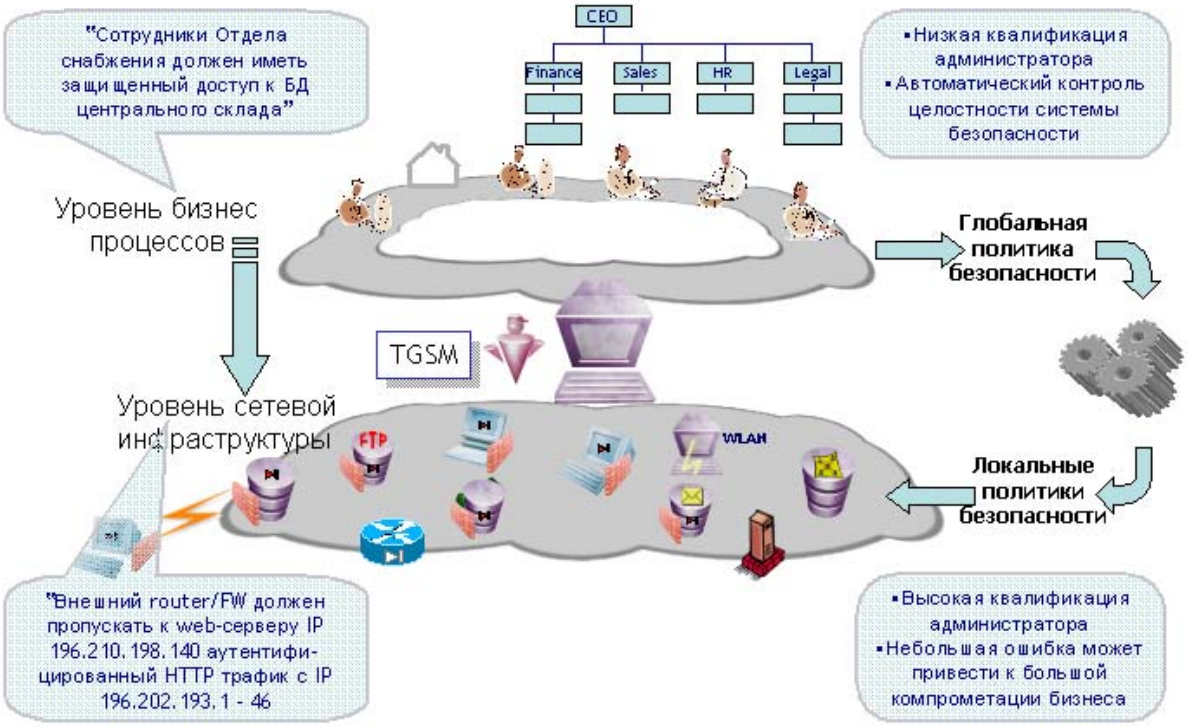


Рис. 1 Управление безопасностью корпоративной сети на основе политики.

Управление безопасностью корпоративной сети, реализуемое TGSM, основано на следующих трех концептуальных положениях (см. Рис.1):

- Управление безопасностью корпоративной сети должно осуществляться на уровне глобальной политики безопасности (ГПБ) – наборе правил безопасности для сколь угодно сложного множества взаимодействий между разнообразными объектами корпоративной сети, а также между объектами корпоративной сети и внешними объектами;
- ГПБ должна максимальным образом соответствовать бизнес – процессам компании; для этого должен существовать способ описания свойств безопасности бизнес - объектов и требуемых для их реализации сервисов безопасности, основанный на их бизнес - ролях в структуре компании;
- Формирование локальных политик безопасности (ЛПБ) для отдельных средств защиты и их трансляция должны осуществляться автоматически на основе анализа правил ГПБ и топологии защищаемой сети с обязательной автоматической проверкой их корректности, целостности и непротиворечивости ГПБ.

Таким образом, сочетание уникальных функциональных, технических и эксплуатационных характеристик продукта ЗАСТАВА 3.3. делают его de-facto продуктом мирового уровня. Применительно к российским условиям важно отметить полную легитимность использования ЗАСТАВА 3.3. на территории РФ: сертификат Гостехкомиссии России № 653 от 30 июля 2002 года, сертификаты ФАПСИ на СКЗИ «Криптон» и «Верба», поддерживаемые продуктом. Все это позволяет строить на базе продукта множество разнообразных решений, направленных на решение актуальных бизнес – задач (см. Рис.2).

В заключении еще раз отметим самое главное: ИНТЕГРАЦИЯ и УПРАВЛЕНИЕ – два «столпа» IT-безопасности, следование которым наконец-то позволит российским заказчикам реально отойти от политики «латания дыр» и начать строить полномасштабную, надежную и управляемую корпоративную архитектуру безопасности.

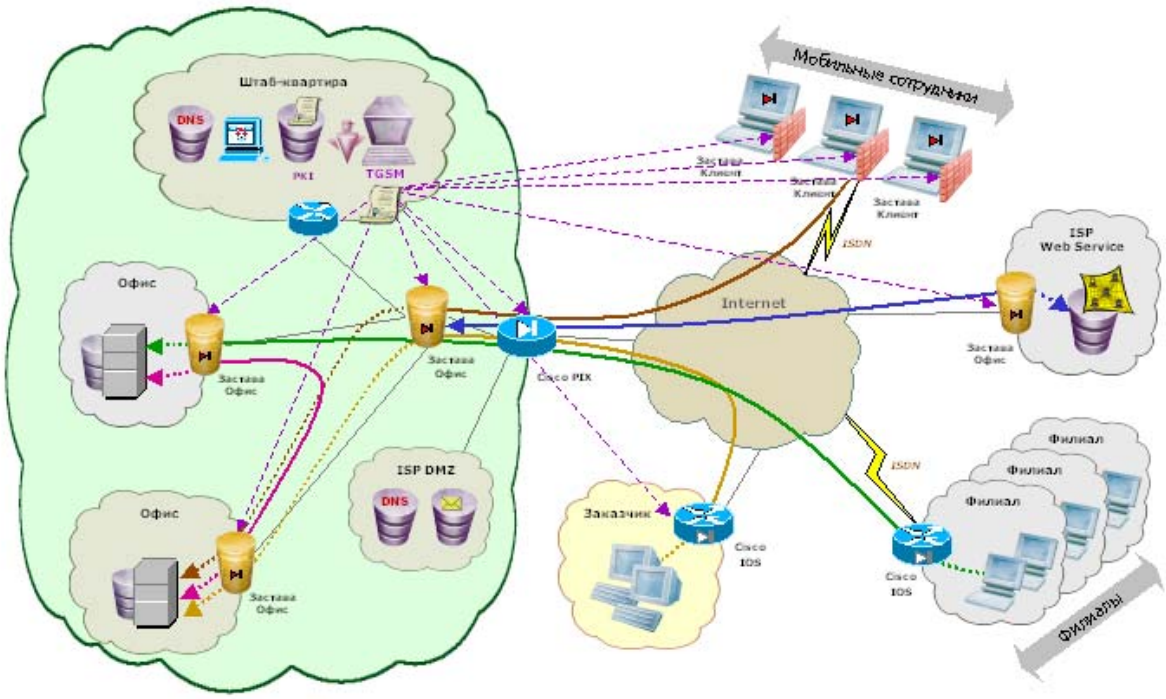


Рис.2. Корпоративная архитектура безопасности на базе ЗАСТАВА 3.3.