МОДЕРНИЗАЦИЯ С ПРИЦЕЛОМ НА ЗАЩИТУ

Березин Андрей Сергеевич
менеджер по работе с партнерами ОАО «ЭЛВИС+»

Сетевой журнал
№2.2001

При разработке программы модернизации корпоративной сети сегодня любой грамотный IT-менеджер обязан позаботиться о модернизации (а может быть, и о создании) подсистемы информационной безопасности.

Можно выделить целый ряд причин, по которым стоит задуматься об информационной безопасности корпоративной сети. Во-первых, разнообразными функциями обеспечения информационной безопасности нынче в достаточной мере снабжены существующие продукты и технологии построения корпоративных информационных и телекоммуникационных систем, и игнорировать эти возможности было бы просто неразумно. Во-вторых, современный бизнес немыслим без активного использования публичных сервисов, предоставляемых открытыми сетями связи, и прежде всего Интернетом. По этой причине корпоративная сеть должна быть подключена к открытым сетям, что опять же требует обеспечения безопасности этого соединения. В-третьих, грамотно спроектированная и аккуратно реализованная подсистема информационной безопасности может существенным образом расширить функциональные возможности самой корпоративной сети: построение системы удаленного защищенного доступа мобильных сотрудников к информационным ресурсам корпоративной сети; использование дешевых Интернет-коммуникаций для передачи информации между различными подразделениями компании; построение системы компьютерной телефонии и т. д. И наконец, чаще всего стоит просто вспомнить о немалой стоимости накопленных за многие годы информационных ресурсов, хранимых и обрабатываемых в рамках корпоративной сети, или о степени влияния оперативности и достоверности получаемой информации на качество принимаемых решений. Другими словами, требование обеспечения информационной безопасности корпоративной сети сегодня можно смело считать обусловленным простым здравым смыслом!

Четыре уровня безопасности

Для успешного выполнения поставленной задачи проектировщик подсистемы информационной безопасности прежде всего должен четко представлять себе эту систему на самом общем, концептуальном уровне, с тем чтобы правильно определить основные приоритеты ее построения и взаимосвязь между ее отдельными компонентами. Для наглядности рассмотрим упрощенную модель подсистемы информационной безопасности корпоративной сети на базе «исторического подхода», т. е. по типовым этапам ее построения. Такой подход интересен тем, что, во-первых, именно так строится большинство подсистем информационной безопасности на практике, во-вторых, это даст нам возможность экстраполировать результаты моделирования на ближайшее будущее.

Итак, построение любой корпоративной сети начинается с установки рабочих станций, следовательно, подсистема информационной безопасности корпоративной сети начинается с защиты именно этих объектов. Для этого можно (и нужно!) использовать всем давно и хорошо известные штатные средства защиты операционных систем; антивирусные пакеты; дополнительные устройства аутентификации пользователя и средства защиты рабочих станций от несанкционированного доступа; средства шифрования прикладного уровня т. д. На базе перечисленных средств защиты информации стоится первый уровень подсистемы

информационной безопасности корпоративной сети - уровень защиты рабочих станций сети (см. рисунок).

На втором этапе развития корпоративной сети (который на практике часто происходит одновременно с первым) отдельные рабочие станции объединяются в локальные сети, устанавливаются выделенные серверы и (сегодня это случается все чаще и чаще) организуется выход из локальной сети в Интернет. На данном этапе в бой вступают средства защиты информации второго уровня - уровня защиты локальной сети: средства безопасности сетевых ОС; средства разграничения доступа к разделяемым ресурсам; средства защиты домена локальной сети; серверы аутентификации пользователей; межсетевые экраны и proxy-серверы; средства организации VLAN; средства обнаружения атак и уязвимости защиты локальной сети и т. д. Очевидно, средства защиты информации второго уровня гораздо более сложны технологически, нежели таковые средства первого уровня, что, естественно, отражается на их стоимости и трудоемкости установки и сопровождения.

Третий этап развития корпоративной сети состоит в объединении локальных сетей нескольких филиалов компании в общую корпоративную intranet-сеть на базе современных ИТ-технологий поддержки QoS (ATM, Frame Relay, DiffServ, MPLS и др.), с использованием в качестве коммуникационной среды публичных сетей, включая, конечно, и Интернет. При этом безопасность обмена информацией через открытые сети обеспечивается применением технологий Virtual Private Network (VPN), которые и составляют основу третьего уровня подсистемы информационной безопасности корпоративной сети. Технологии VPN, как правило, достаточно глубоко интегрированы с средства защиты информации первого (средства аутентификации пользователя и защиты от несанкционированного доступа) и второго (межсетевые экраны и сетевые ОС) уровней, и защищенный VPN-канал может «доходить» не только до маршрутизаторов доступа и пограничных межсетевых экранов, но и до конкретных серверов и рабочих станций локальной сети, составляя, таким образом, своего рода скелет подсистемы информационной безопасности корпоративной сети.

Что же ожидает корпоративные сети в ближайшие 5-10 лет? Четвертым этапом их развития станет, видимо, организация защищенного межкорпоративного обмена информацией (externet-сети), который потребует качественно новых технологий обеспечения информационной безопасности для работы «всех со всеми», т. е., другими словами, для формирования системы электронного бизнеса. Наиболее вероятным кандидатом на роль технологической и методологической основы для создания инфраструктуры электронной бизнес-системы является группа технологий и методов, позволяющих строить системы управления публичными ключами и сертификатами - Public Key Infrastructure (PKI). Соответственно PKI, скорей всего, является последним количественным уровнем подсистемы информационной безопасности корпоративной сети.

Следует подчеркнуть, что, как известно, PKI - это лишь IT-технология поддержки работоспособности довольно сложной административной системы, которая призвана выполнять всего две функции (даже и в рамках страны, а в перспективе - и планеты): генерацию и корректное (протоколированное) распространение ключей и сертификатов; отслеживание «жизненного цикла» выданных ключей и сертификатов в режиме реального времени.

Очевидно, что после получения от PKI необходимых параметров защищенный информационный обмен между отдельными компаниями (вернее - их корпоративные сети) будет строиться на базе совсем других технологий, и прежде всего технологий поддержки электронно-цифровой подписи

и VPN. Таким образом, с технической точки зрения е-бизнес станет возможен лишь при условии, что используемые «внешние» средства защиты информации (т. е. средства защиты информации второго и третьего уровней) различных компаний «понимают» не только друг друга, но и соответствующие приложения PKI некоторой заранее неизвестной (по крайней мере для одной из компаний) третьей стороны. Очевидно, что это реально только в том случае, когда упомянутые средства являются совместимыми, т. е. (если вспомнить о глобальной природе е-бизнеса) все они построены на базе открытых мировых стандартов. Применительно к нашей конкретной задаче это означает, что если ваша компания планирует свое участие в е-бизнесе, необходимо изначально строить подсистему информационной безопасности на базе открытых стандартов (благо сегодня это сделать совсем несложно, так как абсолютное большинство производителей средств защиты информации сегодня ориентируются именно на них).

Следует заметить, что применительно к информационной безопасности корпоративной сети проблема совместимости различных средств защиты информации актуальна не только по причине заманчивости перспектив е-бизнеса. Хорошо известно, что подсистема информационной безопасности - это по определению комплексная система, состоящая из большого числа отдельных элементов, выполняющих свои определенные функции. Такая система может быть надежной (а именно это является основным ее качеством и главной целью создания) только в случае ее глубокой интегрированности. Другими словами, стойкость подсистемы информационной безопасности не должна зависеть от стойкости самого «слабого» средства защиты информации (хотя в настоящее время именно такой принцип главенствует); в интегрированной подсистеме информационной безопасности компрометация одного из элементов защиты должна надежно компенсироваться противодействием других ее элементов, что может быть обеспечено только их слаженной работой в рамках единой системы. К сожалению, на современном этапе развития технологий информационной безопасности использование явления синергизма в масштабах всей корпоративной подсистемы информационной безопасности пока еще невозможно из-за незрелости открытых стандартов и отсутствия четко выраженных требований рынка. Однако тенденция развития средств защиты информации в этом направлении уже прослеживается достаточно явно: объединение средств защиты от несанкционированного доступа со средствами шифрования прикладного уровня; интеграция межсетевых экранов с антивирусными пакетами и VPN; средств аутентификации -- с технологиями PKI и т. д.

Возвращаясь к построенной нами модели подсистемы информационной безопасности корпоративной сети, хочется сделать еще одно важное замечание. Первые три уровня «пирамиды» можно отнести к средствам защиты информации в традиционном их понимании, поскольку эти средства призваны обеспечить собственную информационную безопасность корпоративной сети. Верхние два уровня явно относятся уже к обеспечению е-бизнеса, поскольку VPN служат для построения защищенного обмена информацией между компаниями, а PKI предоставляет VPN-устройствам необходимые для формирования защищенных каналов ключи и сертификаты). Таким образом, как мы видим, VPN-технологии исторически позиционированы как связующий элемент между чисто внутрикорпоративной задачей - обеспечением информационной безопасности распределенной корпоративной сети и глобальной бизнес-задачей компании - обеспечением интеграции в систему мирового электронного бизнеса XXI века!

Строим подсистему информационной безопасности

Как показывает опыт, построение подсистемы информационной безопасности корпоративной сети далеко не всегда является сугубо технической задачей. Гораздо чаще она представляет собой задачу организационно-техническую, в которой от решения организационной составляющей во многом зависит состав и сложность реализации составляющей технической. В общем случае построение подсистемы информационной безопасности корпоративной сети целесообразно разделить на несколько этапов.

На первом этапе рекомендуется провести четкую классификацию имеющихся информационных ресурсов компании по степени их конфиденциальности. Мы намеренно не рассматриваем случай, когда среди корпоративных информационных ресурсов существует информация, составляющая государственную тайну или коммерческую тайну другой компании (материнской компании,

компании-партнера, заказчика и т. д.). Это особый (и достаточно сложный!) случай, который необходимо рассматривать отдельно. Но в рамках любой компании вполне обоснованным является требование о придании информации, например, финансового отдела или отдела разработки статуса конфиденциальной информации, доступ к которой необходимо ограничить, и прежде всего для сотрудников самой компании*. Эту задачу, как правило, можно решить как организационными методами, так и техническими средствами, однако наиболее эффективно применение некоего комбинированного решения. В последних двух случаях, скорей всего, потребуется пересмотр (или переконфигурирование) топологии существующих локальных сетей или up-grade сетевого оборудования с тем, чтобы иметь возможность четко выделить те сегменты корпоративной сети, в которых обрабатывается конфиденциальная информация, а также ограничить число (контролируемых!) точек взаимодействия этих сегментов с остальными сегментами корпоративной сети. Взаимодействие с открытыми сетями рабочих станций и серверов этих сегментов, если это необходимо, лучше всего организовать не напрямую, а через доверительную среду корпоративной сети.

На втором этапе следует сформировать собственную политику безопасности корпоративной сети в виде, например, некой системы требований к подсистеме информационной безопасности применительно именно к данной компании. Скорей всего, без надлежащего опыта это удастся сделать лишь на самом общем уровне, часто недостаточном для решения данной задачи. На самом деле делать этого и не нужно, поскольку как отечественными, так и западными специалистами по информационной безопасности уже составлены необходимые документы, в которых четко классифицированы разные уровни обеспечения информационной безопасности корпоративной сети и необходимые для этого технические средства, а также организационные мероприятия. Можно, например, рекомендовать комплект «Руководящих документов» Гостехкомиссии при Президенте РФ , или более развернутый документ «Evaluation criteria to IT Security». Взяв за основу перечисленные там требования, можно в большой степени быть уверенным в том, что необходимая комплексность подсистемы информационной безопасности корпоративной сети будет обеспечена. На данном этапе нелишне снова задуматься о перспективах развития корпоративной сети, например о том, с кем из партнеров или заказчиков планируется строить защищенные взаимодействия в ближайшие пять лет? Очевидно, что состав и жесткость требований к вашей подсистеме информационной безопасности должны быть как минимум не ниже соответствующих параметров подсистемы информационной безопасности вашего партнера или заказчика.

На третьем этапе можно приступить непосредственно к выбору технических средств, которые в совокупности с организационными мерами позволили бы успешно решать поставленные перед подсистемой информационной безопасности задачи. Некоторым ориентиром для выполнения этого этапа работ может служить таблица, в которой рассмотрено (в первом приближении) соответствие наиболее популярных средств защиты информации общим требованиям по защите корпоративных информационных систем (или функциональности подсистемы информационной безопасности корпоративной сети).

Следует заметить, что наличие крестиков в одной строке таблицы для различных средств защиты информации отнюдь не означает, что эти средства являются полностью взаимозаменяемыми. Например, задачу защиты локальной сети от атак извне (см. п. 3.1 таблицы) обозначенные пять средств защиты информации решают абсолютно по-разному, закрывая, таким образом, свою часть «дыр» в защите локальной сети. Очевидно, что максимальную надежность подсистемы информационной безопасности можно обеспечить лишь путем применения максимально комплексного решения, что на практике, к сожалению, не всегда возможно. Поэтому искусство проектировщика подсистемы информационной безопасности на данном этапе заключается в том, как «меньшими средствами решить большую задачу».

Наименование функции	Штатные	Антивирусные	Средства	Средства	Сервер	VLAN	Межсе-	Средства	VPN

подсистемы информационной безопасности корпоративной сети	средства ОС	средства	защиты от несанкциониро-ванного доступа	шифрования прикладного уровня	аутентифика-ции пользователей		тевые экраны	обнаружения уязвимости	
Защита информационных ресурсов локальной рабочей станции от несанкционированного доступа									
Аутентификация пользователя	x		x		x				
Разграничение доступа к информационным ресурсам рабочей станции	x		x		x	x			
Защита информационных ресурсов рабочей станции		x		x				x	
Защита локальной сети									
Разграничение доступа и защита разделяемых информационных ресурсов	x		x	x	x	x		x	x
Защита внутренних каналов связи				x		x			x
Сегментирование локальной сети						x	x		x
Защита межсетевого взаимодействия									
Защита от удаленных атак		x		x			x	x	x
Защита внешних каналов связи				x					x

При окончательном выборе уже конкретного средства защиты информации конкретного производителя, на наш взгляд, помимо базовых требований к продукту (набор функциональности; относительная стоимость необходимых функций; совместимость с другими средствами защиты информации; условия технической поддержки продукта производителем или дистрибьютором и т. д.) необходимо уделить внимание следующим двум критериям: быстродействию данного средства защиты информации; наличию сертификата соответствия.

Требование по быстродействию средств защиты информации относится главным образом к средствам защиты межсетевого взаимодействия (межсетевые экраны, proxy-серверы, VPN-устройства), поскольку именно здесь, как правило, возникает жесткое требование к скорости обработки информации. Прежде всего это относится к средствам защиты, применяющим методы криптографического преобразования (кодирования) информации (средства шифрования прикладного уровня, VPN-устройства и др.), поскольку подобная обработка трафика в реальном масштабе времени требует очень серьезных вычислительных ресурсов, которые необходимо предварительно оценить.

Наличие сертификата соответствия на выбранное средство защиты информации является обязательным только для государственных учреждений, а также для негосударственных, если они используют информацию, отнесенную государством по существующему законодательству к конфиденциальной или секретной информации. Например, для учреждений, работающих по государственному заказу или имеющих доступ к персональной информации граждан или сведениям о добыче и обработке стратегических полезных ископаемых и т. д. Прочие организации при построении подсистемы информационной безопасности своих корпоративных сетей могут использовать как сертифицированные, так и не сертифицированные средства защиты информации. Многие компании (и не без оснований) считают, что «настоящий брэнд» лучше всякого сертификата, и потому об этом просто не задумываются.

На самом деле процедуру сертификации средств защиты информации государственными органами необходимо воспринимать не более как элемент государственного механизма, призванного осуществлять защиту прав потребителя, который должен, в принципе, одинаково эффективно защищать право потребителя есть качественную колбасу и использовать качественные средства защиты информации. Применительно к практике построения подсистем информационной безопасности это означает, что если вы применили несертифицированные средства защиты информации и вашу систему «взломали», то ответственность за это несете только вы сами. В этом случае привлечь производителя средств защиты информации к ответственности, тем более материальной, удается крайне редко. Если же вашу подсистему информационной безопасности взломали «по вине» сертифицированных средств защиты информации, то бремя ответственности перекладывается на сертифицирующий государственный орган, т. е., читай, на государство, и уже оно обязано задействовать всю мощь гражданского, арбитражного и уголовного права для защиты интересов собственника информации, наказания виновных и возмещения понесенных убытков. К сожалению, эта сама по себе прекрасная идея в России еще не воплотилась в работающий механизм, хотя определенные и заметные усилия в этом направлении уже явно прослеживаются.

Пока же сертификат соответствия на средства защиты информации или хотя бы возможность его получения для «любимого брэнда», в принципе, можно считать необходимым в следующих случаях:

1) когда вам хочется убедиться (или убедить своего начальника!) в том, что данное средство защиты информации является тем, что о нем говорит производитель;

2) если средство защиты информации соответствует тому классу защищенности, который требуется для защиты информации вашего уровня конфиденциальности;

3) в случае необходимости в ходе выполнения работ документирования возможностей вашей подсистемы информационной безопасности для представления, например, партнеру, органу по аттестации, или (почему бы и нет!?) страховой компании.

Компаниям, которые (по разным причинам) изначально ориентируются только на сертифицированные средства защиты информации, следует также иметь в виду, что средства защиты информации, использующие методы криптографического преобразования информации, в общем случае должны иметь два сертификата: Сертификат соответствия, выдаваемый Гостехкомиссией при Президенте РФ, который подтверждает соответствие технической реализации средств защиты информации нормативным требованиям «Руководящих документов» самой Гостехкомиссии, степень соответствия ТУ на данный продукт, отсутствие в продукте недекларированных возможностей, «тайных ходов» и т. д. Сертификат соответствия, выдаваемый ФАПСИ, подтверждающий корректность реализации того модуля продукта, который осуществляет функции криптографического преобразования информации, или всего продукта, если эти функции «жестко» в него встроены.

Кроме того, сертификат Гостехкомиссии может быть одного из трех видов: сертификат на конкретный образец изделия; сертификат на партию изделий; сертификат на производство изделий.

Преимущества последнего сертификата очевидны, поскольку компания может закупать любое количество продуктов и все они автоматически будут сертифицированы. Первые два типа сертификата означают, что за сертификацию необходимого комплекта продуктов нужно платить дополнительно (стоимость сертификата либо включена в стоимость продукта, либо, чаще всего, оплачивается отдельно как дополнительная опция).

Сертификат на производство до сих пор имеют только отечественные производители средств защиты информации, и, видимо, это правило сохранится до тех пор, пока западные производители не перенесут свое производство на территорию РФ. Кроме того, необходимо иметь в виду, что сертификаты западных продуктов при одинаковой или даже большей функциональности, как правило, гораздо «слабее» сертификатов отечественных средств защиты информации, поскольку западные производители, например, не горят желанием предоставлять исходные коды своих программ на сертификацию в Россию. По этой же причине, а также из-за отсутствия реализации отечественного криптоалгоритма ГОСТ 28147-89, западным средствам криптографической защиты информации крайне затруднительно получить сертификат ФАПСИ.

Однако вернемся к построению подсистемы информационной безопасности. После того как на основе выбранных организационных и технических требований удалось определить круг необходимых средств защиты информации, наконец-то настало время этапа технического проектирования подсистемы информационной безопасности и всех хорошо известных последующих этапов на пути к вводу готовой системы в эксплуатацию. Заметим только, что для некоторых типов компаний (упомянутых ранее) этапу ввода подсистемы информационной безопасности в эксплуатацию должна предшествовать аттестация подсистемы информационной безопасности на соответствие требованиям российского законодательства к системам защиты отдельных категорий информации. И только после подтверждения корректности реализации подсистемы информационной безопасности внешним государственным органом систему можно вводить в эксплуатацию.

Спроектировать и построить бронированный автомобиль гораздо сложнее, чем автомобиль обычный. Поэтому ни у кого не возникает вопросов, почему первый стоит в несколько раз дороже второго. По аналогии, и защищенная корпоративная сеть должна стоить «в разы» дороже незащищенной, при этом «количество раз» зависит как от требований внутрикорпоративной политики безопасности, так и от спектра применяемых средств защиты информации. Однако на практике следует стремиться к тому, чтобы стоимость подсистемы информационной безопасности не превышала 10-20% от стоимости самой корпоративной сети.

Житейская мудрость говорит нам, что сделать «с нуля» всегда легче и дешевле, чем переделывать готовую систему заново. Поэтому вопрос о построении подсистемы информационной безопасности корпоративной сети целесообразно поднимать именно на этапе модернизации корпоративной сети, когда еще возможно учесть требования политики безопасности на уровне топологии корпоративной сети и тем самым довольно значительно сэкономить материальные средства. Дополнительным источником экономии может служить вариант построения подсистемы информационной безопасности силами компании - системного интегратора, которая проводит основной объем работ по модернизации корпоративной сети. Проблема с выбором такого системного интегратора сейчас практически не стоит, поскольку большинство этих компаний в настоящее время активно расширяют свой традиционный бизнес с построением подсистемы информационной безопасности корпоративной сети. Очевидно, что привлечение сторонней компании к построению подсистемы информационной безопасности не должно снижать стойкость самой системы, в том числе и за счет возможной утечки информации. Для этого, как правило, достаточно руками администратора по информационной безопасности компании-заказчика выполнить все ключевые завершающие фазы построения подсистемы информационной безопасности: назначение и организацию хранения паролей доступа, генерацию секретных ключей, программирование устройств аутентификации пользователей, контроль окончательной настойки межсетевых экранов и т. д. Такой подход, а также качественное документирование возможностей подсистемы информационной безопасности позволят вам обеспечить надежное функционирование этого нового и необходимого элемента современной корпоративной сети.