Грани безопасности электронного бизнеса

Игорь Кадощук, Татьяна Савельева, Елена Турская ОАО"Элвис+"
Сетевой журнал №11.2000

Защищать необходимо все - ведь достаточно проделать брешь хотя бы в одном месте.

Глобальность и доступность - тенденции сегодняшнего бизнеса. Это накладывает довольно значительные ограничения на способы обеспечения информационной безопасности бизнеса. Особенность бизнеса сегодня - существование в открытой среде, в открытых сетях Интернета с широко известными интерфейсами, протоколами, адресами и способами доступа и пр.

В самом деле, главными принципами современного бизнеса, наряду с глобальностью и доступностью являются интегрируемость и контактность практически всех элементов бизнеса: бизнес-процессов, информации и людей! Это, в частности, предполагает принципиальную готовность к интеграции и взаимодействию с широким спектром разнообразных программных средств самого различного назначения и локализации: от операционных систем до библиотек графических интерфейсов пользователя, производимых и поставляемых огромным количеством самых разнообразных фирм.

Мы живем в мире динамического многообразия - «все течет, все изменяется», причем быстрее и быстрее. Это одновременно и одна из главных причин появления методологии открытых систем, и одна из основных трудностей при обеспечении информационной защиты!

Меняется все: технологии информационной защиты, протоколы, криптоалгоритмы, процедуры аудита и управления информационных систем, процедуры сертификации, политики безопасности...; всевозможные модели и схемы - PKI, DCE, компоненты открытой среды - коммуникации, платформы, программное обеспечение промежуточных слоев..; уязвимые моменты, угрозы атак и сами атаки, опасность потери целостности и конфиденциальности данных, нелегальные вторжения...; появляются новые способы неавторизованных транзакций, воровства, вандализма как вовне так и внутри корпоративных сетей; растет число и повышается квалификация хакеров и «крекеров»; совершенствуются не только хакеры, но и их вирусы, «троянские кони», сетевые сканеры и многие другие специальных приложения; безопасность стоит все дороже из-за значительного объема «ручных» операций, отсутствия централизации, невозможности интеграции средств защиты и пр; цена повышается также из-за быстрого роста требований к квалификации персонала по безопасности (рост требований к качеству защиты - подразумевается!); изменяются требования пользователей к информационным системам вообще и к системам информационной безопасности в частности; изменяются требования как к технологиям информационной защиты, так и к функциям самих систем информационной защиты.

Но есть еще одна важнейшая особенность систем информационной безопасности: защищать необходимо все уязвимые места - ведь нападающему достаточно проделать брешь хотя бы в одном из них.

Основа информационной защиты - комплексность и всеохватность!

Собственно, поэтому и существует такое множество технологий, методов, средств и методик информационной защиты. Они возникали как способы борьбы с разнообразными способами нападения, и собрать их в единую управляемую интегрированную систему информационной безопасности для защиты данных в корпоративной сети - задача, требующая профессиональной квалификации и опыта!

Интегрируемость в принципе невозможна без следования согласованным стандартам и функциональным спецификациям самого высокого уровня! В том числе и, если угодно, в первую очередь в области информационной безопасности!

Комплексная функциональность: от антивируса - до PKI

Контролируемая сложность есть суть компьютерного программирования. Керниган
Чем обеспечивается комплексность и всеохватность системы информационной безопасности? На наш взгляд, несколькими факторами одновременно: и функциональной полноценностью защиты, и интегрируемостью поставляемых компонентов системы, и методически выверенным подходом к созданию системы информационной безопасности, и профессиональным умением организовать все проектные работы, и еще многим другим. Но давайте по порядку.
В состав комплексных решений входят следующие функциональные области:

- разграничение доступа к информационным ресурсам, а также защита от несанкционированного доступа к информации;
- защита информации, передаваемой по открытым каналам связи с применением технологии защищенных виртуальных частных сетей VPN;
- комплексная защита от внешних угроз при подключении к общедоступным сетям (например, к Интернету), а также управление доступом из сети Интернет с использованием технологии межсетевых экранов (Firewall) и фильтрации содержимого (Content Inspection);
- защита от вирусов с помощью специализированных комплексов антивирусной профилактики и защиты;
- обеспечение конфиденциальности, целостности и подлинности информации методами надежного преобразования данных (кодирования);
- гарантия идентификации и аутентификации пользователей с применением технологии токенов (смарт-карты, touch-memory, ключи для USB-портов и т. п.);
- управление однократным доступом к разнообразным информационным ресурсам (Single Sign On);
- надежное хранение информации, основанное на технологии защиты на файловом уровне (кодирование файлов и каталогов);
- активное исследование защищенности информационных ресурсов с помощью технологии обнаружения атак (Intrusion Detection);
- обеспечение централизованного управления системой информационной безопасности в соответствии с согласованной и утвержденной политикой (Administration, Auditing и Policy Compliance);
- поддержка полнофункциональной инфраструктуры открытых ключей (PKI, Directory and Certificate Services).

Для реализации основных функциональных компонентов системы информационной безопасности используют различные механизмы и методы:

- стандартные коммуникационные протоколы;
- сертифицированные средства криптографии;
- наиболее прогрессивные механизмы авторизации и аутентификации;
- современные средства контроля доступа к рабочим местам сети и из сетей общего пользования;
- надежные антивирусные комплексы;
- самые интеллектуальные программы аудита и обнаружения атак;
- развитые средства централизованного управления контролем доступа пользователей и безопасного обмена пакетами данных и сообщениями любых приложений по открытым IP-сетям;
- хорошо интегрируемые средства поддержки инфраструктуры открытых (асимметричных) ключей и пр.

Межсетевые экраны

Один из распространенных путей обеспечения информационной безопасности состоит в применении межсетевых экранов. В соответствии с масштабами организации и установленной политикой безопасности используются различные типы межсетевых экранов, стоимость которых, в зависимости от производителя, сложности разработки и богатства функциональности, может быть различной.

С помощью межсетевых экранов решаются следующие задачи:

- безопасное взаимодействие пользователей и информационных ресурсов, расположенных в extranet- и intranet-сетях, с внешними сетями, например с Интернетом;
- создание технологически единого комплекса мер защиты для распределенных и сегментированных локальных сетей подразделений предприятия;
- иерархическое построение систем защиты, предоставляющих адекватные по степени закрытости средства обеспечения безопасности для различных сегментов корпоративной сети.

На российском рынке предлагается набор межсетевых экранов ряда известных фирм с различной производительностью, возможностями установки на те или иные операционные системы, наличием гибкого и централизованного управления и т. д., отвечающие всем требованиям, пожеланиям и ожиданиям.

Например, семейство межсетевых экранов CheckPoint Firewall компании CheckPoint. Межсетевой экран Firewall-1, сертифицированный Гостехкомиссией России, функционирует на операционных системах Windows NT, Solaris, HP-UX и AIX. CheckPoint Firewall-1 определяет, каким сервисам позволено устанавливать соединения защищенной сети с внешним миром при помощи фильтрации пакетов и сервисов proxy. Он позволяет описывать настройки системы для каждого пользователя (в том числе разграничивать доступ в Интернет по времени), выбирать метод авторизации, сервисы и сетевые интерфейсы. Firewall-1 имеет удобный графический интерфейс пользователя, прост в настройке и установке, обеспечивает удобный мониторинг и обработку системных сообщений. Он реализует множество самых необходимых функций, в том числе осуществляет балансировку нагрузки между несколькими серверами сети, обеспечивает функции повышенной отказоустойчивости, производит фильтрацию URL, скрывает адреса внутренней сети (NAT) различными способами, включая трансляцию и подмену адресов.

Firewall-1 осуществляет интеграцию с различными системами и средствами обнаружения атак и с антивирусными комплексами; управляет списками контроля доступа межсетевого экрана Cisco PIX Firewall и маршрутизаторов компаний Cisco, Bay, 3Com; накапливает записи о всевозможных событиях, включая попытки несанкционированного доступа, и многое другое.

Если речь идет о программно-аппаратных устройствах, то можно использовать межсетевой экран Private Internet Exchange (PIX) компании Cisco. Он функционирует на собственной операционной системе и также сертифицирован Гостехкомиссией России. Его отличает высокая производительность, повышенная

надежность при установке в режиме «горячего» резервирования и возможность расширять и изменять IP-сети, эффективно решая проблему нехватки адресов IP. Эти замечательные свойства имеют вполне объективную основу.

Производительность PIX, в отличие от типичных proxy-сервисов, определяется, в частности, выбором специальной (не Unix-подобной) операционной системы реального времени. А также использованием схемы защиты, базирующейся на алгоритме адаптивной безопасности (adaptive security algorithm, ASA) и технологии «сквозного посредника» (Cut-Through Proxy), которая позволяет после успешной идентификации пользователя, в соответствии с политикой обеспечения безопасности на прикладном уровне, контролировать поток данных между абонентами на уровне сессии. Высокие показатели производительности дают возможность поддерживать более 64 тыс. одновременных соединений. При полной загрузке PIX обеспечивает пропускную способность до 170 Мбит/с, что существенно выше аналогичного показателя для межсетевых экранов, базирующихся на ОС Unix или ОС Windows NT.

Проблема нехватки адресов IP эффективно решается с помощью технологии трансляции сетевых адресов Network Address Translation (NAT), что делает возможным использование как существующих адресов, так и резервных адресных пространств для частных сетей. PIX также может быть «настроен» для совместного использования транслируемых и нетранслируемых адресов, используя и адресное пространство для частных сетей IP, и зарегистрированные адреса IP.

Защищенные виртуальные частные сети

- Для построения защищенных виртуальных частных сетей VPN, обеспечивающих защиту информации при передаче по протоколам TCP/IP по открытым каналам связи, используют программные продукты на основе международных стандартов IPSec и достижений в области PKI, работающие в операционных системах Windows 95/98/NT и Solaris. В сетях VPN поддерживается:
- защита (конфиденциальность, подлинность и целостность) передаваемой по сетям информации;
- контроль доступа в защищаемый периметр сети;
- идентификация и аутентификация пользователей сетевых объектов;
- централизованное управление политикой корпоративной сетевой безопасности.

Преимущества использования VPN-продуктов:

- независимость от криптографии. Возможность подключения модулей криптографии от третьих производителей, благодаря чему их можно использовать в любой стране мира в соответствии с принятыми национальными стандартами;
- масштабируемость продуктов, которая позволяет подобрать оптимальное по стоимости и надежности решение с возможностью постепенного наращивания мощности системы защиты;
- наличие открытых интерфейсов для интеграции с другими программными системами и бизнес-приложениями;
- гибкость установки и настройки, позволяющая внедрить систему безопасности, не меняя сетевой конфигурации корпоративной сети;

- экономичность. При использовании VPN-продуктов не требуются специальные каналы для передачи конфиденциальной информации: защита допускает передачу конфиденциальной информации по любым каналам, поддерживающим протоколы TCP/IP;
- поддержка международных стандартов. Совместимость продуктов с продуктами RSA, Baltimore, Entrust, VeriSign, SSH, Siemens, Microsoft и др.

Защита от вирусов и «троянских коней»

Одним из элементов комплексной системы информационной безопасности является антивирусная защита. Антивирусное программное обеспечение должно устанавливаться на основных путях проникновения и распространения вирусов, шлюзовых и коммуникационных серверах, серверах баз данных, файловых, почтовых и информационных серверах и рабочих станциях. Используя антивирусные средства, необходимо учитывать, что защищенный трафик не может быть проконтролирован этими средствами. Поэтому антивирусные средства должны устанавливаться в узлах, на которых информация хранится, обрабатывается и передается в открытом виде.

К примеру, получили распространение продукты лидеров мирового рынка антивирусных комплексов защиты: многоплатформный пакет программ McAfee Total Virus Defense компании McAfee и система антивирусной безопасности «Антивирус Касперского» (AVP) компании «Лаборатория Касперского». Будучи установленными на межсетевой экран, их продукты позволяют обнаруживать вирусы в передаваемых файлах и вложениях писем, проверять архивированные файлы, отслеживать в реальном времени изменения всех записываемых и читаемых файлов, проверять входящий/исходящий трафик. В этих программных продуктах используют сканирующие и резидентные модули, осуществляют автоматическую установку и обновление версий и баз данных по вирусам, а также поддерживают удаленное администрирование и оповещение в случае выявления вирусов.

Технологии токенов

Электронные токены (смарт-карты, touch-memory, ключи для USB-портов и т. п.) являются средством повышения надежности защиты данных на основе гарантированной идентификации пользователя. Токены являются так называемыми "контейнерами" для хранения персональных данных пользователя системы. Основное преимущество электронного токена заключается в том, что персональная информация всегда находится на носителе (смарт-карте, ключе и т. д.) и предъявляется только во время доступа к системе или компьютеру. В качестве компонентов комплексного решения по информационной безопасности могут использоваться, например, токены компаний Aladdin и Gemplus.

Защита информации на файловом уровне

Технологии защиты информации на файловом уровне позволяют скрыть конфиденциальную информацию пользователя на жестком диске компьютера или на сетевых дискетах путем кодирования содержимого файлов, каталогов, дисков с помощью мощных криптоалгоритмов. Доступ к информации осуществляется посредством ключа, который может вводиться с клавиатуры, храниться и предоставляться со смарт-карты, HASP- или USB-ключей и прочих токенов. Помимо вышеперечисленных функций предлагаемые нами средства позволяют мгновенно "уничтожить" информацию при подаче сигнала "тревога" и при "входе под принуждением", а также блокировать компьютер на время перерывов в работе.

В качестве компонентов комплексного предложения на российском рынке получают распространение, к примеру, такие продукты компании Aladdin, как система защиты конфиденциальной информации на персональных компьютерах - Secret Disk и система защиты корпоративной информации на серверах Secret Disk Server.

Технологии обнаружения атак (Intrusion Detection)

Постоянные перемены в сети (появление новых рабочих станций, серверов, сетевых устройств, реконфигурация программных средств и т. п.) могут привести к появлению новых уязвимых мест, угроз и возможностей для атак как на информационные ресурсы, так и на систему защиты. В связи с этим особенно важно своевременное их выявление и внесение изменений в соответствующие настройки информационного комплекса и его подсистем, и в том числе в подсистему защиты. Это означает, что рабочее место администратора системы должно быть укомплектовано специализированными программными средствами обследования сетей и выявления уязвимых мест (наличия "дыр") для проведения атак изнутри и снаружи, а также комплексной оценки степени защищенности от нарушителей.

В сети могут использоваться специальные средства анализа защищенности, которые позволяют оперативно проверить десятки и сотни территориально разнесенных узлов сети. При этом они не только выявляют большинство угроз и уязвимых мест информационной системы, но и предлагают администратору безопасности рекомендации по их устранению. В числе таких средств, к примеру, можно назвать наиболее мощные среди обширной номенклатуры коммерческих пакетов продукты компании Internet Security Systems семейство SAFEsuite: Internet Scanner и System Security Scanner, а также продукты компании Cisco - систему обнаружения несанкционированного доступа NetRanger и сканер уязвимости системы безопасности NetSonar.

Пакет Internet Scanner предназначен для определения уязвимых мест в средствах защиты Web-серверов, межсетевых экранов (Firewall), серверов и рабочих станций, работающих под управлением ОС Windows NT, SunOS, Solaris, LUnix, HP UX, Windows 95 и т. п. Принцип работы Internet Scanner основан на моделировании известных методов, используемых для несанкционированного проникновения в компьютерные сети, что напоминает принцип работы многих антивирусных программ. База данных, содержащая информацию о вариантах взлома сети, содержит сведения более чем о 140 методах. Результатом работы программ, входящих в систему Internet Scanner, является отчет о найденных уязвимых местах

анализируемого модуля сети. По требованию администратора в отчет включается перечень мер, необходимых для повышения уровня защищенности системы. Interranet Scanner применяется для тестирования любого устройства, имеющего IP-адрес (рабочая станция, сервер, интеллектуальный принтер и т. п.), и определения тех настроек, которые могут быть использованы злоумышленником для взлома сети.

Система System Security Scanner предназначена для контроля надежности отдельных компьютеров, хостов, работающих под управлением ОС Unix или Windows NT. Она проверяет права доступа одного или нескольких пользователей к системным или прикладным файлам. При этом фиксируется наличие вирусов, настройки ОС, целостность файлов и паролей, признаки взлома анализируемого компьютера и т. п. Характерной особенностью этой системы является возможность устранения выявленных недостатков.

Система обнаружения несанкционированного доступа NetRanger предназначена для облегчения использования и масштабирования сети, а также для обеспечения производительности и надежности, необходимых для работы сети масштаба предприятия. Являясь компонентом продуктов системы безопасности компании Cisco, NetRanger может работать со стороны как Интернета, так и интрасети предприятия. Система NetRanger состоит из двух компонентов: высокоскоростного сетевого детектора, анализирующего содержание и контекст каждого из проходящих сетевых пакетов с целью обнаружения попыток несанкционированного доступа, и управляющей консоли. При попытке атаки в режиме реального времени детекторы NetRanger Sensor посылают предупреждения на управляющую консоль NetRanger Director. Механизм выявления атаки основан на обширном списке сигнатур и поэтому позволяет обнаружить широкий набор атак по содержанию и контексту сетевых пакетов.

Устройства NetRanger Sensor используются в нескольких сетевых сегментах с разной скоростью и типами интерфейсов, включая Token Ring, Fast Ethernet и FDDI. Сигнатуры NetRanger Sensor можно централизованно обновлять с управляющей консоли NetRanger Director. Одна управляющая консоль способна управлять десятками детекторов. Консоли NetRanger Directory объединяются в связанную структуру для управления неограниченным количеством детекторов NetRanger Sensor. В свою очередь, детекторы могут передавать предупреждения об атаках сразу нескольким консолям, используя уникальный отказоустойчивый протокол. Кроме того, информацию об атаках можно экспортировать в реляционную базу данных для последующего анализа.

Сканер уязвимости системы безопасности NetSonar обеспечивает всесторонний анализ системы на предметбезопасности, выполняет подробное отображение сети и составляет электронную опись устройств в сети. Как активное приложение в наборе средств системы безопасности сети, NetSonar обладает всеми средствами уведомления конечного пользователя, консультантов по безопасности и администраторов о внутренней уязвимости сети, позволяя, таким образом, эффективно решать потенциальные проблемы безопасности.

Автоматически обнаруживая новые узлы и сервисы, NetSonar позволяет собирать информацию о всех сетевых устройствах, находящихся в исследуемой сети, таких как WWW- и почтовые серверы, межсетевые экраны, а также маршрутизаторы, серверы удаленного доступа и т. д. Эта функция позволяет пользователям

составить представление о полной архитектуре устройств в сети и активизированных сервисов путем опроса сетевых устройств по протоколу SNMP. С помощью инновационных технологий управления данными и представлением информации легко определить уязвимые места исследуемой сети и составить подробный отчет о возможных проблемах. Уникальная запатентованная компанией Cisco база данных и используемые методы отображения информации допускает получение результатов сканирования в любых представлениях и с любым уровнем детализации.

Инфраструктура открытых ключей - PKI

Целостная система информационной безопасности невозможна без реальной интеграции коммуникационной и информационной систем и систем безопасности путем построения инфраструктуры открытых ключей PKI. Основные функции PKI: поддержка жизненного цикла цифровых ключей и сертификатов (в том числе их генерация, распределение, отзыв и пр.), идентификация и аутентификация пользователей, интеграция существующих приложений и всех компонентов подсистемы безопасности.

К сожалению, не каждое средство информационной защиты, даже если производитель декларирует его соответствие существующим международным стандартам (X.509, LDAP, PKCS №11, PKCS №7), определяющим функционирование системы PKI и способствующим ее взаимодействию с различными средствами защиты информации, может работать с любой системой PKI. В каждом конкретном случае необходимо проведение совместных тестовых испытаний различных средств и систем.

Интеграция коммуникационной и информационной систем и систем безопасности с построением инфраструктуры открытых ключей PKI сегодня может быть достигнута как на основе продуктов известных мировых лидеров (Entrust, Verisign, Baltimore, Microsoft, SSH, VPNC и др.), так и на основе сертифицированных продуктов российских производителей. Из отечественных продуктов по защите информации, совместимых с системами PKI всех вышеперечисленных мировых лидеров, стоит упомянуть программное средство управления VPN - сервер сертификатов «ЗАСТАВА». Сервер предназначен для хранения в виде базы данных открытых сертификатов всех пользователей VPN. Он осуществляет автоматическую раздачу сертификатов VPN-устройствам и взаимодействие с внешними PKI.

Комплексная методика проектных решений информационной безопасности

На российском рынке информационных технологий комплексные решения по защите информационных ресурсов системный интегратор вырабатывает в процессе внедрения систем сетевой информационной безопасности в различных производственных сферах и распределенных корпорациях. Комплексная методика защиты информации многими, по сути, формируется на основе проработки требований заказчика и собственного опыта внедрения системных проектов на крупных предприятиях. В настоящее время таким опытом обладают единичные

компании, имеющие лицензию Гостехкомиссии России на проведение проектных работ с решением задач по информационной безопасности.

На наш взгляд, для защиты от угроз и гарантии экономически выгодного и безопасного использования коммуникационных ресурсов необходимо решить следующие задачи:

- разработать политику информационной безопасности;
- защитить внешние каналы передачи информации, обеспечив конфиденциальность, целостность и подлинность передаваемой по ним информации;
- гарантировать возможность безопасного доступа к открытым ресурсам внешних сетей и Интернета, а также общения с пользователями этих сетей;
- защитить отдельные наиболее коммерчески значимые информационные системы независимо от используемых ими каналов передачи данных;
- предоставить защищенный удаленный доступ персонала к информационным ресурсам корпоративной сети;
- обеспечить надежное централизованное управление средствами сетевой защиты.

Комплексный пакет услуг по созданию систем информационной безопасности должен включать:

- экспертизу информационных систем на предмет соответствия требованиям безопасности;
- подготовку автоматизированных систем и объектов информатизации к аттестации на соответствие требованиям безопасности;
- анализ защищенности информационных систем и разработку политики и концепции информационной безопасности организаций;
- проектирование корпоративных систем в защищенном исполнении;
- обучение и консультирование специалистов заказчика;
- поставку (как необходимое и согласованное программное, так и техническое обеспечение!) и ввод в эксплуатацию средств защиты;
- сопровождение и техническую поддержку систем информационной безопасности;
- модернизацию и развитие систем информационной безопасности;
- консалтинг в области информационной безопасности.

Другими словами, не только функциональная полнота имеет значение, но и полный спектр услуг дает возможность получить реальную комплексную систему информационной безопасности.

Важным в комплексном проекте является процесс создания инфраструктуры открытых ключей (PKI), методически состоящий из последовательного ряда этапов, каждый из которых должен сопровождаться соответствующим документированием и проверками критериев успешности. Любой этап создания PKI дает результат в виде явно оформленного «продукта», позволяющего убедиться в законченности и общем продвижении процесса. Подробнее эти вопросы были рассмотрены в статье «Как нам организовать PKI» (см. «Сетевой журнал», № 9-2000).

В заключение отметим, что в России пока не так много компаний, предоставляющих услуги по анализу, проектированию и разработке инфраструктуры открытых ключей. И совсем плохо с компаниями, имеющими

апробированную методику построения инфраструктуры открытых ключей и соответствующий опыт!

С другой стороны, откуда может появиться такой опыт? Только из практики. Еще отметим такой статистический факт: имея дело с поставщиками и разработчиками VPN, можете быть уверены -- такой опыт у них есть! Они всё вынуждены были отрабатывать на себе, так как никакой продукт VPN не может работать без PKI! Всё - взаимосвязано!