Защищенная открытость

Игорь Кадощук, технический директор ОАО ЭЛВИС+
Сетевой журнал №9.2000

Основные проблемы современных систем электронного бизнеса.

Слова «электронная коммерция» и e-business сегодня, похоже, стали даже более популярными, чем в начале 60-х годов были «русские в космосе». Во всяком случае, анекдоты на тему e.com сочиняются с не меньшей энергией, хотя русские имеют к этому гораздо меньшее отношение, чем к космосу.
Вместе с тем, по всеобщему мнению, электронная коммерция - явление далеко не новое, и начало оно берет в тех же 60-х годах. В течение всех этих лет бизнес пользовался системами электронного обмена данными (Electronic Data Interchange) для размещения заказов и их оплаты поставщикам. Однако при этом не использовались сети общего доступа - их просто не было.
Что же сегодня имеют в виду, когда говорят об электронной коммерции, e-Commerce, iCommerce, и т.д.? Эксперты определяют электронную коммерцию как торговлю товарами и услугами, при которой окончательный заказ размещается через Интернет. Другими словами, электронная коммерция - это заключение сделок в электронной форме, а Интернет-торговля - только оплата покупок через Интернет, то есть незначительная часть той же электронной коммерции. Таким образом, хотя электронную коммерцию часто путают с Интернет-торговлей, первое из этих понятий - более широкое.
Основными моделями глобальной электронной коммерции являются торговые отношения между бизнесами (B2B - business-to-business) и между бизнесом и покупателем (B2C - business-to-customer), так же как электронное (EDI) размещение заказов через Интернет.
Откуда такая популярность? Это ведь не космос и не разгадка генома человека, а вполне заурядный процесс обмена коммерческой информацией, реквизитами и некоторыми подтверждениями. Неужели причиной сегодняшнего бума является обычная человеческая лень - пресловутый двигатель прогресса, и человечество просто устало ходить по магазинам? Впрочем, перспективы этого рынка впечатляют.
Объем мирового оборота электронной коммерции через Интернет в 2003 году, по прогнозам Forrester Tech., будет составлять от $1.8 триллиона до $3.2 триллиона. Верхняя граница этого диапазона достигается за счет всеобщего стремления сделать процесс покупки и продажи через Интернет простым, безопасным и повсеместно доступным. Медленное признание со стороны бизнеса и непримиримость со стороны государств и правительств могут серьезно препятствовать развитию электронной коммерции. В этом случае мировой оборот достигнет нижней из указанных отметок.
Оба прогнозных сценария оценки включают рынки между бизнесами (B2B), между покупателем и бизнесом (B2C) и электронное (EDI) согласование и размещение заказов через Интернет, но исключают величину объема чисто финансовых транзакций.
Таким образом, двигателем прогресса в данном случае является извечное стремление человечества делать дорогое дешевым, сложное - простым, недоступное - всеобщим, и все это желательно «не вставая с дивана»; а проще говоря, все та же самая человеческая лень и скупость.
Однако обратим внимание на то, что же нам мешает. Ключевыми словами здесь будут «безопасность», «медленное признание со стороны бизнеса» и «непримиримость со стороны государств и правительств». Попробуем разобраться, чего же опасаются правительства, бизнес и покупатель, что их беспокоит, и на что они надеются? На первый взгляд, все, как всегда: правительствам нужны налоги (то есть точные данные о том, кто сколько продал и купил), покупатели боятся случайной, а тем более предварительно организованной пропажи денег (необходимы точные данные о том, где в какой момент они находятся, и о правах доступа к ним), бизнесам нужны покупатели (точные данные о том, где они находятся и что они предпочитают), и они тоже опасаются краж, поскольку бизнесы, как правило, одновременно являются и продавцами, и покупателями.
Таким образом, всем нужны точные данные по самым разным поводам, а значит, нужны эффективные механизмы их получения, безопасного хранения и обмена. Следовательно,

большинство проблем электронной коммерции и бизнеса сегодня лежит в области информационной безопасности, и именно проблемы безопасности являются самым серьезным препятствием на пути электронной коммерции и бизнеса.

Поставщики электронной торговли

Электронная коммерция объединяет множество различных функций. В простейшем виде цель электронной коммерции можно определить как изменение способов ведения бизнеса через технологии. Это может быть настолько же просто, насколько просто установить информационную связь между бизнесом и потребителем, между бизнесом и поставщиками, между поставщиками и производителями. Электронная коммерция использует новые технологии для изменения способов организации контакта покупателей и продавцов, методов представления, обсуждения и изменения заказа, продажи товаров и услуг, а также процесса осуществления платежей.

Таблица 1.

Компания	**Оборот** (млн. USD)	**Год основания**
Поставщики программного обеспечения и услуг		
Microsoft	19,747	1975
Oracle	9,063	1977
Intuit	848	1983
Network Associates	785	1992
Cambridge Tech. Partners	628	1991
TMP Worldwide	585	1967
USWeb/CKS	375	1995
Citrix Systems	323	1989
Macromedia	167	1992
Network Solutions	142	1979
Concentric Network	110	1991
Exodus Communications	108	1992
BroadVision	71	1993
Inktomi	71	1996
Security First Technologies	44	1995
Razorfish	36	1995
Поставщики технического обеспечения		
IBM	87,448	1911
Lucent Technologies	38,303	1995
Intel	28,194	1968
Dell Computer	21,670	1984
Cisco Systems	12,154	1984

Sun Microsystems	11,726	1982
EMC	4,459	1979
Qualcomm	3,937	1981
Network Appliance	335	1992
Broadcom	335	1991
Juniper Networks	31	1992

Это действительно замечательный бизнес! Тут, кажется, есть повод, и для популярности, и для ажиотажа. В конце концов, если объем электронной коммерции достигнет такой величины, как почти 10% мирового торгового оборота в 2004 году, то эти, пусть и электронные, магазины должен кто-то построить! И поставщики инфраструктуры стараются изо всех сил, создавая всевозможные необходимые компоненты!
Примерами полных наборов программных продуктов для организации торговой цепочки являются такие продукты, как Net.Commerce компании IBM, Internet Commerce Server 1.1 (или ICS) корпорации Oracle, Site Server корпорации Microsoft, Domino.Merchant 2.0, корпорации Lotus Development, i.Sell компании Informix, eStore компании PeopleSoft, Business-to-Business Procurement Release 2.0 компании SAP AG, CommerceXpert корпорации Netscape Communications, LiveCommerce фирмы OpenMarket, и другие продукты. Рынок таких программ довольно разнообразен. Здесь уместно будет сказать только то, что подобные "готовые магазины" дополняются заказными программными системам повышенной гибкости в использовании, с широкими возможностями удовлетворения специфических требований компаний и высоким уровнем интеграции с бизнес процессами. В то же время, "готовые магазины", как правило, гораздо дешевле заказного программного обеспечения.

Беззащитность электронного бизнеса

В целом поставщики программного обеспечения осознают проблему безопасности и, декларируя «абсолютную безопасность» использования собственных программных средств, встраивают в состав своих комплексов некоторые механизмы информационной защиты: например, обеспечивающие идентификацию, туннелирование и шифрование конфиденциальных данных. Несмотря на это, мы постоянно слышим о взломах торговых систем и электронных магазинов, о краже таких конфиденциальных данных, как номера кредитных карт, причем кражах массовых - речь обычно идет о тысячах и десятках тысяч номеров, если не больше! И это только данные, попадающие в открытые средства информации.
Таблица 2.

Типы нарушения систем информационной безопасности	% зафиксированных инцидентов	% связанных потерь
Внешний несанкционированный доступ к корпоративной сети	44%	25%
Отказ в обслуживании	32%	28%
Подмена данных при передаче	17%	18%
Активное прослушивание	2%	1%
Внутренний несанкционированный доступ к сети	97%	62%
Внутренний несанкционированный доступ к информации	55%	32%

Для того чтобы разобраться в необходимости и достаточности механизмов информационной безопасности, встраиваемых поставщиками в специализированное программное обеспечение электронной торговли, следует более подробно рассмотреть весь спектр задач информационной безопасности.
Потенциальные опасности электронной торговли

В процессе функционирования систем электронной торговли возникает значительное число потенциальных опасностей, например:
Ответственность за безопасность при использовании сетей общего доступа, как правило, перекладывается на пользователя. Интернет не принадлежит никому, и потому никто не несет ответственности за управление, администрирование и безопасность в целом. Каналы доступа в Интернет могут дать возможность доступа к информационным ресурсам торговой организации извне.
Неосторожное использование коммуникативных программ, в том числе на основе HTTP-протокола, может привести к проникновению «троянских коней» - специальных программ, нарушающих работоспособность и/или искажающих данные вашей информационной системы. Наибольшее распространение этого типа программ получили вирусы.
Сети общего доступа часто используются специфически квалифицированными специалистами для проникновения незамеченными в системы безопасности информационных систем.
Частое использование электронной почты может помочь злоумышленникам скомпрометировать имена пользователей торгующей организации. Специальные широко доступные в Сети программы могут быть использованы для поиска слабых мест в системах хранения пользовательских данных (имена, пароли, PIN-коды, и т.д.) информационной системы.
Интернет дает возможность пересылать конфиденциальную информацию практически в любую точку мира, однако если она недостаточно защищена, она может быть перехвачена, скопирована, искажена, прочитана любыми внешними пользователями - злоумышленниками, конкурентами, спецслужбами, просто любопытствующими.
Так, например, пересылая недостаточно защищенное платежное поручение либо номера кредитных карточек, необходимо помнить, что пересылка идет не через частную/собственную сеть, и значительное число внешних пользователей имеет потенциальную возможность манипулировать вашим сообщением. Кроме того, ваше сообщение может быть подменено: существуют методы отправки сообщений пользователем А так, как будто оно отправлено пользователем В.
Сети общего пользования предоставляют своим клиентам много ценных служб. Многие люди полагаются на эти службы в своей работе, так как они позволяют им эффективно решать свои задачи. Когда эти службы недоступны в нужный момент, производительность падает. Сеть может стать неработоспособной из-за специального пакета, чрезмерного количества вполне легальных пакетов, искажений при передаче или по причине неисправности компонента сети. Вирус может снизить производительность или остановить систему ЭЛКОМ. Подобного рода случаи называются «отказом в обслуживании» и представляют очень серьезную угрозу для электронной коммерции.
Интернет предоставляет доступ к ресурсам и услугам, которые могут сделать труд персонала организации менее производительным, если внешняя активность персонала соответствующим образом не отслеживается и не корректируется.
Защита информационных потоков организации защищена настолько, насколько защищенным является самое слабое место в информационной системе организации.
Безопасность обеспечивается целым набором методов и средств, и является одним из важнейших элементов систем электронной торговли. Без должной защиты электронная торговля фактически невозможна.
Объем потенциальных продаж в области электронной коммерции ограничивается страхом, который испытывают покупатели, продавцы и финансовые институты, обеспокоенные вопросами безопасности в Интернете. Этот страх основан в частности, на следующем: отсутствие гарантии конфиденциальности - кто-то может перехватить передачу ваших данных и попытаться найти ценную информацию, (например, номер вашей кредитной карточки, дату поставки товара (и адрес); недостаточный уровень проверки участников операции - без проверки участников транзакции одна из сторон может устроить «маскарад», который будет иметь для другой стороны весьма серьезные последствия. Например, покупатель, посещая сайт, не уверен, что представленная на нем компания именно та, за кого она себя выдает; может случиться также, что покупатель передаст номер своей кредиткой карточки (при использовании ее как средства платежа) лицу, которое не обладает достаточным уровнем полномочий; у продавца нет возможности проверить, что покупатель, сделавший заказ, является законным обладателем кредитной карточки; банк-эмитент кредитной карты может захотеть проверить продавца, от которого поступило требование на выполнение платежа; наконец, нет гарантии целостности данных: даже если отправитель данных может быть

идентифицирован, то третья сторона, возможно, изменит данные во время их передачи. Следовательно, необходим способ предотвращения вмешательства или метод определения модификации данных.
Еще одна проблема возникает как результат того, что многие компании занимаются разработкой программного обеспечения именно для электронной коммерции. Это означает, что все участники торговых операций должны иметь одни и те же приложения, что практически неосуществимо. Следовательно, необходим способ обеспечения взаимодействия между приложениями различных разработчиков и интегрированного механизма управления безопасности!

Задачи информационной безопасности Internet

Для поиска решений этих проблем был создан независимый консорциум - Internet Security Task Force (ISTF) - общественная организация, состоящая из представителей и экспертов компаний-поставщиков средств информационной безопасности, электронных бизнесов и провайдеров Интернет-инфраструктуры. Среди членов консорциума - такие лидеры рынка поставщиков электронной инфраструктуры, как Cisco Systems, eToys, Sabre, Travelocity, Verio и CA. Консорциум был создан специально для разработки технических, организационных и операционных руководств по безопасности Интернет, нацеленных на предотвращение атак хакеров.
Консорциум ISTF выделяет двенадцать областей информационной безопасности, на которых в первую очередь должны сконцентрировать свое внимание создатели электронного бизнеса, чтобы обеспечить его работоспособность. Список, в частности, включает следующие пункты:

- аутентификация (механизм объективного подтверждения идентифицирующей информации);
- право на частную, персональную информацию;
- определение событий безопасности (Security Events);
- защита корпоративного периметра;
- определение атак;
- контроль за потенциально опасным содержимым (Malicious Content);
- контроль доступа;
- администрирование;
- реакция на события (Incident Response).

Рекомендации ISTF предназначены для существующих или вновь образуемых компаний электронной коммерции и бизнеса. Рекомендации помогают определить потенциальные бреши и дыры в их компьютерных сетях, которые, если не обратить на них должного внимания, могут использоваться взломщиками-хакерами. Это может привести к атакам на систему электронной коммерции, потрясениям и даже к потенциальному крушению электронного бизнеса! Консорциум ISTF настоятельно рекомендует воспользоваться его наработками еще до начала организации электронной коммерции и бизнеса.

Начальный набор рекомендаций включает обстоятельства, часто незаметные, но легко обнаруживаемые в большинстве систем, развертываемых сегодня в Интернете. Среди них, в частности, требование не использовать значения, задаваемые «по умолчанию» во время установки и настройки приложений, поскольку это ведет к тому, что:

- установленные по умолчанию имена пользователей и пароли становятся широко известными;
- отсутствует защита от несанкционированного вторжения хакеров во внутреннюю и внешнюю сеть;

- отсутствует возможность организации аудита после проведения изменений в среде электронного бизнеса таких, например, как установка новых приложений и компьютеров;
- как правило, мы имеем дело с непрофессиональным и слабым администрированием, приводящим к неполному уничтожению устаревших имен пользователей и пр.

В случае с электронным бизнесом информационная безопасность и защита являются критичными для непрерывности бизнеса как такового. Безопасность больше не является дополнительным свойством: ведь даже 97-процентная надежность системы означает, что за год для бизнеса будут потеряны 293 часа!

Ценность электронной коммерции и бизнеса создается установлением контакта и интеграцией бизнес процессов, информации и людей. Наиболее успешные электронные бизнесы учитывают природу децентрализации Интернет. При изменении условий и появлении новых возможностей новая функциональность должна быть доступна через Web для любого сколь угодно удаленного пользователя. И если структура электронного бизнеса основана на стандартах, такой переворот может быть осуществлен за одну ночь: решающее преимущество в мире, где быстрый «съедает» большого!

Что является камнем преткновения для информационной безопасности? Как ни странно, в этой роли выступают некоторые основополагающие принципы электронной коммерции.

Сложность приложений. Логически "разгружая" клиентскую рабочую станцию, упрощая и унифицируя пользовательский интерфейс, мы все более усложняем приложения на сервере, а также процесс их разработки и окружающую среду эксплуатации. Интегрируя среду разработки и эксплуатации, мы можем радикально упростить разработку и эксплуатацию новых приложений.

Интеграция с существующими приложениями или другими системами. Как показывает статистика, каждая большая организация, фирма, корпорация поддерживает в среднем шесть операционных сред и более 150 различных приложений на рабочих станциях пользователей.

Идеальное решение состоит в том, чтобы расположенные на сервере и/или клиентских станциях технологии в мире электронного бизнеса были как можно более широко основаны на стандартах и стандартных решениях. Единственное, что можно гарантировать в этом мире: завтра все будет по-другому!

Возможности готовых решений

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

- коммуникационные протоколы,
- средства криптографии,
- механизмы авторизации и аутентификации,
- средства контроля доступа к рабочим местам сети и из сетей общего пользования,
- антивирусные комплексы,
- программы обнаружения атак и аудита,
- средства централизованного управления контролем доступа пользователей, а также безопасного обмена пакетами данных и сообщениями любых приложений по открытым IP-сетям.

Графически основные компоненты системы безопасности в электронной торговле, согласно классификации «рубежей обороны» Hurwitz Group, выглядят следующим образом:

Детальный анализ прикладных решений электронной коммерции, поставляемых различными производителями, показывает, что эти приложения реализуют только часть необходимых функций защиты и безопасности (вопреки смелым декларациям и всевозможным заверениям, что те или иные системы «абсолютно» безопасны и используют самые лучшие средства шифрования).

В этих системах, как правило, реализуются: функции защищенных коммуникаций с использованием специальных протоколов; функции контроля целостности данных, аутентификации и авторизации доступа пользователей в торговую систему; и реже функции обеспечения конфиденциальности пересылаемых данных. Однако ни одна из прикладных систем не может контролировать целостность сети и всей информационной системы; защищать систему от неавторизованного вторжения из внутренней сети; а также защищать систему от неавторизованного вторжения из сетей общего пользования.

Как правило, прикладные решения электронной коммерции:

- не интегрированы с системами контроля доступа пользователей к своим рабочим местам;
- ни одна из них не защищена от «троянских коней» и вирусов других типов;
- кроме того, процессы обнаружения несанкционированного доступа и аудита также реализуются внешними по отношению к торговой системе механизмами.

Итак, можно сделать вывод, что ни одно из прикладных решений в области электронной коммерции не обеспечивает интегрированной комплексной управляемой системы информационной защиты, а также что все они подвержены значительным рискам потерь, искажений, компрометации информации и пр.

Согласно рекомендациям ISTF и классификации «рубежей обороны» Hurwitz Group, первым и важнейшим этапом разработки системы информационной безопасности электронной торговли и бизнеса будут механизмы управления доступом к сетям общего пользования и доступом из них, а также механизмы безопасных коммуникаций, реализуемые межсетевыми экранами и продуктами частных защищенных виртуальных сетей (VPN). Сопровождая их средствами интеграции и управления всей ключевой информацией системы защиты (PKI - инфраструктура открытых ключей), мы получаем сравнительно целостную, централизованно управляемую систему информационной безопасности.

Следующий рубеж включает в себя интегрируемые в общую структуру средства контроля доступа пользователей в систему вместе с системой однократного входа и авторизации (Single Sign On).

Антивирусная защита, средства аудита и обнаружения атак по существу завершают создание интегрированной целостной системы безопасности, если речь не идет о

работе с конфиденциальными данными. В этом случае потребуются также средства криптографической защиты данных и электронно-цифровой подписи.

Только некоторые их этих механизмов встраиваются поставщиками в готовые приложения электронной коммерции и бизнеса. Остальную и главную работу по созданию информационной защиты и безопасности электронной коммерции и бизнеса должны взять на себя именно специалисты по информационной безопасности - системные интеграторы в этой области. Без их участия ваша информационная защита всегда будет иметь потенциальные прорехи.