Открытые сети: "за" и "против"

Игорь Кадощук, технический директор ОАО "ЭЛВИС+"
Сетевой журнал №12.2000
Не "закрытие" технологий защитит бизнес, а другая технология и профессионалы, ею владеющие!

История человечества учит (если она кого-то все же чему-либо учит), что каждый раз, создавая новые возможности, мы создаем и новые угрозы, зависимости и опасности. Примеров тому масса, не стоит перечислять. Как ни горько, как ни обидно, но, при всем нашем восхищении, восхвалении и преклонении, с Сетью (как иногда запросто называют Интернет) та же история! В самом деле, особо восторженные и эмоциональные журналисты называют Интернет самым грандиозным творением человечества и спорят только о том, считать ли его принадлежностью XX или уже XXI века. И тому есть причины. Раскрывающиеся перспективы кажутся практически безграничными: от кардинальной трансформации буквально через несколько лет бизнес-структур и мирового рынка (пример тому -- Forrester Research) до не менее кардинального изменения интимной частной сферы, скажем, способа любить друг друга (думаю, ссылки не нужны?).

Вместе с тем опасности, которые подстерегают беспечных пользователей в Сети, оказываются не менее безграничны: от тривиального воровства с частных банковских счетов до возможности полного паралича и даже разрушения очень хорошо построенного бизнеса!

Зачем бизнесу открытые сети?

Если попытаться перечислить все главные причины восторгов по поводу открытых сетей вообще и Интернета в частности, то список не будет слишком уж длинным. Достаточно всего нескольких удачных свойств, чтобы создать богатейшие возможности. Например, генетический код, алфавит, натуральный ряд чисел, звукоряд - все они состоят из немногих элементов, а какие результаты (!). То же и в данном случае. Итак, думаю, что первыми и важнейшими параметрами для бизнеса (в силу его имманентной сущности) будут стоять дешевизна и доступность, глобальность и множественность (иногда уникальность) сервисов: от почты - до аренды приложений, электронной коммерции и электронного же бизнеса (зачатки тех самых революционных преобразований мировой экономики).

Даже если бы главные причины этим и исчерпывались- этого было бы более чем достаточно! Спрашивается, какого рожна ему (бизнесу) еще хотелось бы, когда Интернет задешево пролезает по вездесущему IP к каждому потенциальному клиенту, причем позволяет протащить на себе не только весь маркетинговый мусор, но и возможность обсудить сделку, заключить (или отвергнуть) ее, расплатиться за покупку. А сколько денег приходилось тратить раньше на каждый визит и беседу с клиентом!?

Покупатель же идет на это, потому что все вышеперечисленное он может совершать (при желании) в тапочках, халате (или без) и абсолютно не вставая с дивана! И все это невзирая на неоднократные предупреждения истории про «бесплатные сыры». Давайте попробуем поискать скрытые пружины Интернет-мышеловки.

Технологические причины открытости

В чем же глубинные причины опасностей, возникающих в открытых сетях Интернета? Причин много, и вряд ли нам удастся разобраться во всех. Поэтому попробуем рассмотреть хотя бы наиболее очевидные.

Как обычно, «наши недостатки суть продолженияенаших достоинств»: дешевизна, доступность, глобальность и разнообразие сервисов оборачиваются огромным количеством иногда просто любопытных, а иногда и по-своему заинтересованных пользователей. При этом спектр их интересов и степень вооруженности разнообразными спецсредствами настолько широк, насколько это вообще возможно (и даже невозможно) себе представить! Образ информационной войны вполне реален, и в ней участвуют, в том числе, наиболее подготовленные и самые профессиональные воины, отряды и армии мира. И только потому, что не слышно выстрелов, мало кто знает, что Они уже и здесь...
Однако, прежде чем мы перейдем к «фронтовым сводкам», несколько слов о более глубинных причинах. Очевидно, что Интернет, как глобальная открытая система, строился по законам открытых систем. И это естественно, на то они и законы, хотя им нет и десяти лет! А законы гласят - мобильность и совместимость программ, данных и пользователей (да простят меня классики за свободу слога)!
А это, в свою очередь, означает всеобщую согласованность открытых протоколов, интерфейсов, типовую функциональность и пр. Причем согласованность действительно всеобщую, т. е. общественную, значительного количества именно общественных организаций, ведущих процессы согласования, включая ISO - Международную организацию по стандартизации.
Ведь «открытость» есть степень, по сути, известности и согласованности архитектуры, интерфейсов и модулей (Open Systems Joint Task Force - OS JTF). Здесь под «архитектурой» подразумевается «общая структура сущности и ее компонентов, а также взаимосвязи компонент»ов. Открытая архитектура основана на функциональной модульности и распределенности, опирающейся на «правильным» образом формируемые интерфейсы и протоколы.
Модульная система строится как структура «разъемов», позволяющих заменять отдельные модули, как только это необходимо, а также по мере реализации собственных возможностей. Конкретные разъемы определены по Форме, Функциям, Фазам и Интерфейсам (ФЗИ - OS JTF) , что строго соблюдается на системном уровне архитектуры.
Открытая система - чистый случай модульности, управляемой потребностями архитектуры, при этом архитектура и интерфейсы правильным образом определены и поддерживаются публичным процессом согласования, основанным на консенсусе. В частности, они (интерфейсы и коммуникационные протоколы) могут оказаться стандартами достаточно высокого общественного уровня, либо стандартами де-факто.
Таким образом, «все всё знают» и, более того, «все всё должны знать» - очевидное противоречие открытости и защищенности! И если бы только одно это противоречие, это бы еще пол беды! Но трудностей и помимо него хватает!

Объективные трудности

За прошедшие годы область, именуемая «информационной безопасностью», накопила колоссальное количество самых разнообразных элементов, самим своим многообразием порождающих реальные трудности для «сознательных» пользователей, понимающих необходимость и ценность защиты информационной ресурсов и пытающихся разобраться: а о чем, собственно, речь?
Сделаем беглый обзор, ни в коем случае не претендуя на полноту, а лишь с целью проиллюстрировать многообразие. Ведь это жизнь, и «все меняется еще до того, как мы доберемся до конца этой фразы»!
Итак, с чем же сталкивается «сознательный» пользователь сегодня. Накоплено значительное число разнообразных теорий и технологий, протоколов, криптоалгоритмов и пр. Вперемешку с ними - редко переводимые и расхожие "buzzwords" - VPN, firewall, intrusion detection, single sign-on, APIs... Но это только начало; далее процедуры - аудит, управление, сертификация, политика

безопасности… А затем всевозможные модели и схемы - PKI, DCE… Не забудьте собственно многообразие компонентов открытой среды - коммуникации, платформы, промежуточные слои и, в частности, масштабирование и мобильность приложений: от больших ЭВМ (mainframe) до персональных систем и прочее, что придает «открывающемуся ландшафту нескучный характер». Однако и это пока только цветочки.
Как мы уже заметили, «это - жизнь» и мы находимся в потоке, в водовороте живых изменений - все преобразуется и довольно быстро, как говорят, меняется прямо на глазах: уязвимые места, угрозы атак и сами атаки, опасности - потеря целостности, конфиденциальности данных, нелегальные вторжения. Пользователи - это, как правило, люди, и утеря ключей для них обычное житейское дело, даже если это ключи шифрования. Да и как тут не утерять, когда приходится иметь дело с чрезмерным количеством ключевых слов - чуть не каждая программа, сайт, Web-узел требует своего пароля.
Поставщики и производители средств информационной безопасности тоже «стараются»: уважаемый «сознательный» пользователь часто сталкивается с невозможностью использования политики безопасности в своей информационной системе. Производители создают продукты «без политики», продукты с разными политиками - и, как результат для пользователя, централизация средств информационной безопасности, увы, недостижима! Все это приводит, помимо прочего, к эскалации цены безопасности. Наконец, для разных программно-аппаратных сред, системного окружения и реализаций требуются различные продукты информационной защиты. Производители иногда не думают о защите инвестиций клиентов.
Но и пользователи не отстают (правильно будет сказать, что современный бизнес этого требует, а пользователи - выразители его воли, не более). Достаточно ознакомиться с примерными перечнями требований, которые они предъявляют к системам информационной безопасности.
Требования к технологиям: построение по согласованным (национальным, международным) стандартам; масштабируемость относительно организационной и технологической структуры; адаптивность к трансформации бизнес-процессов и методов их защиты.
Требования к функциям:

- обеспечение защищенных сегментированных сетей для локальных и удаленных пользователей;
- разграничение прав доступа и фильтрация приложений и данных;
- идентификация пользователей по индивидуальным смарт-картам;
- маркировка информации и разграничение доступа по уровням конфиденциальности;
- администрирование пользователей и информационных сервисов;
- протоколирование действий пользователей и пр.

Продолжать можно долго, но думаю, вполне достаточно, чтобы даже не понять, а почувствовать (!) обратное влияние всех перечисленных проблем на бизнес-процессы. Они зачастую приводят к параличу инициатив, особенно в электронном бизнесе, как наиболее зависимом от проблем в информационных средах.

Результат - информационная война

Уже давным-давно все знают, что «бизнес - это война». Если, перефразируя классика, мы станем утверждать, что информационная война есть продолжение бизнеса другими средствами, то не слишком оторвемся от действительности. Мы совсем от нее не оторвемся!

Как говорили древние, «если хочешь мира, готовься к войне. Искусство войны жизненно важно для государства. Это вопрос жизни и смерти, дорога и к безопасности, и к гибели. Поэтому ни при каких обстоятельствах не пренебрегайте этим...»

Глядя на периодически публикуемые журналами, новостными и информационными агентствами и официальными государственными службами безопасности перечни компьютерных атак и потерь, размышляя над «сводками с полей сражений», видишь, что война уже в самом разгаре! Еще бы, если верить директору ФБР Луису Фри («В наше время верить нельзя никому! Мне... можно». А кому же верить, если не ФБР?), то число находящихся в производстве дел, связанных с незаконным вторжением в информационные системы, возросло в 1999 году в 2.11 раза по сравнению с 1998-м. Согласно опубликованному пятому ежегодному отчету «Исследования компьютерных преступлений и безопасности» («Computer Crime and Security Survey»), в 1999 году потери частных и государственных структур США от вторжений в их информационные сети составили $265 млн. (другие источники содержат цифры во много раз большие!). Причем нападения различного рода были отмечены в 90% (!) отзывов более чем 600 компаний и организаций. При этом 51% респондентов не смогли оценить собственные финансовые потери и только 31% были в состоянии смогли предоставить соответствующие данные. Компании часто не открывают данные об атаках и потерях еще и потому, что это может пагубно сказаться на их репутации и устойчивости бизнеса в целом!

По данным специального доклада Белого Дома 2000 года, подготовленного администрацией президента США, «National Plan for Information Systems Protection. Version 1.0», более 72% компаний, фирм, корпораций, государственных и общественных организаций США обнаружили рост угрозы безопасности их данных в течение последних двух лет. Основными причинами финансовых потерь, связанных с недостаточной информационной безопасностью, являлись: компьютерные вирусы (76%), атаки изнутри (62%), атаки извне (25%), ошибки из-за невнимательности (70%) и индустриальный шпионаж (10%).

Кроме того, следует принять во внимание следующее обстоятельство. Согласно сведениям того же ФБР, в открытую печать попадают сведения только о 0,7% всех реально проведенных атак, т. е. примерно каждая сто сороковая! Вот как появляется эта оценка. Приблизительно 65% попыток несанкционированных вторжений оказываются успешными, и практически все они (96%) остаются незамеченными. Из четырех процентов зафиксированных успешных атак в открытую печать попадают сведения только об одной четверти (27%). Таким образом, общественность узнает только о 0,7% от общего количества атак, а именно о зарегистрированных и успешно проведенных несанкционированных вторжениях!

Господа, вы только вдумайтесь в эти цифры! Война в самом разгаре и лишь отсутствие грохота пушек и рвущихся снарядов успокаивает. Но это кажущееся спокойствие! Война не затихает ни на секунду, и «цена ошибки - поражение»! И тут действительно недалеко до паралича бизнес-инициатив!

Задачи информационной безопасности Интернета

Для поиска решений этих проблем был создан независимый консорциум Inetrnet Security Task Force (ISTF) - общественная организация, состоящая из представителей и экспертов

компаний -- поставщиков средств информационной безопасности, электронных бизнесов и Интернет-провайдеров. Среди членов консорциума - лидеры рынка поставщиков электронной инфраструктуры, такие компании, как Cisco Systems, eToys, Sabre, Travelocity, Verio и CA. Консорциум создан специально для разработки технических, организационных и операционных руководств по безопасности Интернета, нацеленных на предотвращение атак хакеров - кибер-террористов и воинов «невидимого фронта».

Консорциум ISTF выделяет двенадцать областей информационной безопасности, на которых в первую очередь должны сконцентрировать свое внимание пользователи Интернета для того, чтобы обеспечить работоспособность собственных информационных систем. Список этот, в частности, включает:

- аутентификацию (механизм объективного подтверждения идентифицирующей информации);
- право на частную, персональную информацию;
- определение событий безопасности (Security Events);
- защиту корпоративного периметра;
- определение атак;
- контроль за потенциально опасным программным кодом;
- контроль доступа;
- администрирование;
- реакцию на события (Incident Response).

Рекомендации ISTF предназначены для существующих или вновь образуемых компаний и помогают определить потенциальные бреши и дыры в их компьютерных сетях, которые, если не обратить на них должного внимания, могут быть использованы взломщиками-хакерами для атак на систему электронной коммерции. Это чревато потрясениями, вплоть до крушения электронного бизнеса! Консорциум ISTF настоятельно рекомендует воспользоваться их наработками еще до организации электронной коммерции и бизнеса.

Начальный набор рекомендаций упоминвет обстоятельства часто незаметные, но легко обнаруживаемые в большинстве систем, развертываемых сегодня в Интернете. Этот набор включает, в частности, требование не использовать значения, задаваемые «по умолчанию» во время установки и настройки приложений, так как в противном случае возможны негативные последствия:

- установленные по умолчанию имена пользователей и пароли становятся широко известны;
- 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. Надежность системы 97% означает в год потерю для бизнеса 293 часов!

Что является камнем преткновения, когда речь идет об информационной безопасности? Как ни странно, некоторые основополагающие принципы, заложенные в информационные технологии, их современное состояние и тенденции использования.

- **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.** Вот статистический факт: в большой организации, фирме, корпорации поддерживается примерно 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 информационной системе бизнеса были, и как можно шире, основаны на стандартах и стандартных решениях! В этом мире можно гарантировать только одно: завтра все будет по-другому!

Таким образом, и как бы очевидное противоречие между открытостью и защищенностью - кажущееся противоречие! Известный пример - история «закрытой» защиты GSM и «открытая» криптография. Алгоритмы защиты GSM-трафика, которые тщательно скрывались авторами как один из методов собственно защиты, были взломаны и довольно быстро. Вместе с тем человеческое сообщество открыто и гласно работает над несколькими системами шифрования (даже на уровне ISO!), так что любой желающий может узнать, как же устроены эти алгоритмы, и практически бесплатно! Но шансов взломать такой алгоритм у «любого желающего» не меньше, но и не больше, чем даже у его создателей: нет ключа - нет разгадки! Это математика, это - знание, которое, в данном случае, действительно - сила! Напрашивается аналогия с историей защиты окружающей среды. Не «закрытие» или «отмена» технологий приводит к спасению от отбросов человеческой деятельности, а другая технология и профессионалы, ею владеющие!

Спасение в войне -- это борьба. Борьба нападающих на бизнес и защищающих его от опасностей! Как в блок-бастерах - борьба плохих и хороших, темных сил и светлых, борьба Добра и Зла. Человечество всегда на том стояло и стоять будет!