Вопросы построения безопасной информационной системы

Качлишвили Т.Т.
Технический Университет Грузии, 0160, пр. Костава 77, Тбилиси, Грузия

Анотация
Защита данных в сетях становится одной из самых открытых проблем. В статье рассматриваются вопросы построения безопасной информационной системы, сформулированы базовые принципы информационной безопасности, задачей которых является обеспечение целостности данных, защита от сбоев, ведущих к потере информации или ее уничтожения. Повсеместное распространение сетевых технологий и усложнение информационной инфраструктуры ведут к увеличению числа потенциально уязвимых мест, вследствие чего хакерские атаки превратились в реальную угрозу. Информация стала востребованным товаром, в связи с чем информационная безопасность признается как одна из первостепенных проблем.

Ключевые слова
Средства защиты, антивирусная защита, комфиденциальность информации, информационная безопасность.

«Кто владеет информацией, тот владеет миром». Действительно, информация – один из важнейших активов государственного управления и современного бизнеса. И этот актив нуждается в защите. О том, от чего и как надо защищать корпоративную информацию, какие подходы к информационной безопасности позволяют предотвратить не только опасности сегодняшнего дня, но и спрогнозировать угрозы дня завтрашнего.

Информационная безопасность, являясь неотъемлемой частью любой информационной системы, проходит те же этапы развития, что и информационные технологии в целом. Все начиналось с персональных компьютеров, на которых работал один человек, в крайнем случае – несколько. Вопросы безопасности решались довольно просто – достаточно было обеспечить антивирусную защиту и разграничить доступ криптографическими средствами. Тогда на рынке информационной безопасности были представлены только вендоры.

Затем появились локальные сети, которые вызвали к жизни новые понятия: транспортная среда, сетевое ПО, программное обеспечение коллективного доступа. А вслед за ними появились новые угрозы –со стороны соседей по сети. В ответ на эти изменения появились такие средства защиты как системы аутентификации, системы администрирования, WLAN, которые позволяли решить вопросы информационной безопасности в соответствии с требованиями того времени.

И вот, наконец, пришло время глобальных сетей. Теперь «враги»-профессионалы могут нанести значительный ущерб безопасности практически из любой точки земного шара. Этот этап ознаменовался появлением системных интеграторов, которые перешли к формированию систем. Изменились и механизмы обеспечения информационной безопасности: появились межсетевые экраны, системы PKI, системы обнаружения вторжений. Речь пошла о комплексном подходе к информационной безопасности, когда все элементы системы безопасности взаимодействуют между собой.

Сегодня с учетом постоянного растущего уровня информатизации и постоянно увеличивающегося количества угроз, обеспечить информационную безопасность на достаточно высоком уровне только с помощью комплексного подхода уже невозможно. Нельзя обеспечить безопасность системы, не обеспечивая безопасность компонентов, из которых она состоит. Недостаточно выставить охрану, нужно еще задействовать механизмы безопасности самих объектов. Поэтому многие крупные производители ПО всерьез

приступили к разработке инструментов обеспечения безопасности своих продуктов. Раньше внутренние механизмы собственной безопасности программных продуктов практически отсутствовали. Сейчас они становятся неотъемлемой частью любого программного продукта. Причем эти механизмы могут быть задействованы на том уровне, который нужен пользователю. Он может вообще не пользоваться встроенным механизмом безопасности, может задействовать его частично, обеспечивая необходимые ему функции защиты информации. Но если такого механизма в продукте нет, то обеспечить его безопасность только внешними средствами становится невозможно. Именно поэтому сейчас к построению систем информационной безопасности нужно подходить уже даже не комплексно, а системно. В этом случае, с одной стороны, информационная безопасность будет представлять собой включение в работу встроенных механизмов защиты в программных и технических компонентах информационной системы. С другой стороны, внешнюю защитную оболочку будет создавать комплексная система информационной безопасности При таком подходе система информационной безопасности становится двухуровневой. Верхний уровень обеспечивает комплексная система защиты, а нижний – собственные встроенные механизмы безопасности продуктов и технических средств. Обойти внешнюю защиту можно, внутреннюю – гораздо сложнее. Таким образом, до тех пор, пока не будет решен вопрос о встраивании механизма безопасности в продукты, мы по-настоящему защищенную систему не получим.

В качестве первого шага рекомендуют информационное обследование системы, желательно совмещенное с ИТ-аудитом и бизнес-аудитом. В результате будут определены те угрозы и риски, от которых компании необходимо защищаться. Дать универсальный рецепт для всех организаций и предприятий невозможно – единого, стандартного перечня угроз просто не существует. До определенного периода под безопасностью, в основном, подразумевалось сохранение конфиденциальности информации, а о других аспектах, таких как сохранение целостности и доступности никто не вспоминал.

Базовый уровень обеспечения информационной безопасности, который подразумевает обязательное наличие определенных средств защиты. Так, например, вирусы представляют опасность для любой информационной системы, поэтому средства антивирусной защиты должны быть всегда. При создании любой информационной системы существует внутренняя политика обеспечения безопасности, заключающаяся хотя бы в разграничении доступа к ресурсам. Наличие различных прав у разных категорий пользователей вызывает необходимость контроля за реализацией этих прав. Следовательно, обязательно должны быть решены вопросы аутентификации и наличия механизма администрирования системы. Логично предположить, что если в компании существуют правила и система администрирования, надо ввести некоторый мониторинг процесса функционирования системы, чтобы иметь возможность фиксировать «следы» действий как легальных пользователей, так и нелегальных.

Для обеспечения реализации внутренних правил и регламентов безопасности можно ограничиться мониторингом системы, а с точки зрения внешних воздействий надо постараться поставить барьер для защиты от несанкционированных действий извне. Для этого используется межсетевой экран (firewall), определяющий права внешних пользователей и процессов по отношению к внутренним. Это практически обязательный набор, который присутствует во всех достаточно сложных информационных системах. А дальше начинается другой уровень, который регулирует наличие и пропорции тех или иных механизмов защиты.

Для правильного построения системы защиты информации нужно пройти этап анализа и оценки рисков. Этот этап позволяет понять уровень адекватности между средствами защиты, которые используются в компании, и реальными угрозами. У любой компании есть ряд бизнес-процессов, часть из которых поддерживается информационной инфраструктурой. Для бизнес-процессов существуют угрозы, некоторые из которых могут реализоваться через информационную систему. В первую очередь, надо уделять внимание тем угрозам

информационной системе, которые представляют опасность для бизнеса, а не для самой системы как таковой. Аналогичный подход должен быть и для обеспечения безопасности процессов управления. В результате анализа может оказаться, что проще, например, обеспечивать целостность информации не путем внедрения электронной цифровой подписи, а с помощью системы резервирования. А с вирусами эффективнее бороться не путем внедрения сетевой антивирусной системы, а путем наведения элементарного порядка и разработки регламентов работы пользователей. Самое главное четко осознавать – для чего создается комплекс мер по информационной безопасности. Считается, что если «увешать» систему целым ворохом средств информационной безопасности, то она станет неуязвимой. Но это глубокое заблуждение. Можно сколько угодно защищать систему внешними устройствами, и тем не менее оказаться под ударом по вине собственных сотрудников: как свидетельствует, официальная статистика, около восьмидесяти процентов всех инцидентов происходит по вине легальных пользователей. Причем эти удары далеко не всегда вызваны злым умыслом, зачастую это случается из-за рассеянности пользователей, из-за случайности, незнания правил работы с системой. В каждой компании найдется немало сотрудников, у которых бумажка с паролем доступа в систему, наклеена на монитор…

Подходы к информационной безопасности госсектора и бизнес-сектора отличаются. Общепринятым стандартом считается подход к информационной безопасности как к обеспечению конфиденциальности, целостности и доступности данных. Когда мы говорим о защите государственной тайны, все силы сосредотачиваем на сохранении конфиденциальности информации. А когда компания, которая по роду своей деятельности предоставляет информацию широкому кругу пользователей, заинтересована чтобы эта информация была доступна 24 часа в сутки и 7 дней в неделю, а заботы о конфиденциальности информации для такой компании не столь актуальны. Компании, бизнес которых существенным образом зависит от электронных транзакций – интернет-магазины, информационно-маркетинговые центры, основной упор могут сделать на обеспечении доступности информации, а банки, операторы мобильной связи – на ее целостности. Словом, разность подходов к информационной безопасности зависит от бизнес-приоритетов компаний и организаций. Однако на государственном уровне должны быть сформулированы критерии, которые позволяли бы компаниям и госорганам оценивать результаты своей деятельности по защите информации. Отсутствие государственного регулирования в области информационной безопасности, с одной стороны, хорошо, потому что не ограничивает возможность компаний для самостоятельного развития подходов к информационной безопасности. С другой стороны достаточно остро чувствуется нехватка документов, которые позволили бы компании действовать согласно стандартов и рекомендации, чтобы избежать многочисленных ошибок.

Специалист в области информационной безопасности должен, прежде всего, предлагать безопасные решения, то есть строить безопасные системы, а не системы безопасности. Информационная безопасность должно закладывается при проектировании любой информационной системы – будь то портал, сайт или ERP-система. Наличие высококвалифицированных специалистов делает выполнение этих задач вполне реальным. Воспользоваться заложенным механизмом или создать что-то альтернативное – право заказчика, но механизм обеспечения информационной безопасности изначально должен быть заложен в самом ИТ-решении.

До последнего времени понимание проблематики информационной безопасности не поднималось выше ИТ-уровня. Это была просто определенная расходная статья. К сожалению, лица, которые принимают решения, часто до конца не понимают реальной взаимосвязи между угрозами информационной безопасности и угрозами для бизнес-процессов. И именно по этой причине, даже когда компания серьезно настроена на создание системы информационной безопасности, специалистам заказчика оказывается сложно сформулировать правильные вопросы, ответы на которые необходимы для создания безопасного решения.

Рассмотрим задачу обеспечения информационной безопасности (ИБ) с точки зрения высшего руководства компании и руководителя ИТ-подразделения (или руководителя выделенного подразделения, отвечающего за обеспечение информационной безопасности).

Каковы общие требования к состоянию защищенности информационной системы (ИС) у топ-менеджеров компании и у руководителей бизнес-подразделений? Можно привести примеры таких требований:

- обеспечение конфиденциальности финансовой информации, личной почтовой переписки, информации о проектах и/или заказчиках;
- обеспечение непрерывности ведения бизнеса;
- выполнения обязательств перед клиентами;
- выполнение требований законодательства.

И все эти требования желательно выполнить при минимальных затратах.

Соотнесение бизнес-рисков и рисков технологических позволяет добиться взаимопонимания между высшим руководством компании и руководителями ИБ, что в итоге ведет к оптимизации и прозрачности затрат на обеспечение информационной безопасности.

Риск — это возможность того, что через уязвимые места ИС будет реализована угроза информационной безопасности и произойдет потеря или повреждение активов (ресурсов). Анализ и управление рисками — это процесс идентификации уязвимых мест и угроз в отношении ресурсов ИС и выработка контрмер для снижения рисков до приемлемого уровня, с учетом ценности ресурсов для организации.

Обеспечение ИБ требует финансовых вложений. При этом возврат инвестиций от таких вложений не всегда очевиден. Проведение аналитической работы, позволяющей сопоставить бизнес-риски с рисками технологическими, выявить критичные ресурсы в ИС, угрозы нарушения ИБ, оценить последствия от реализации угроз для деятельности организации, иными словами — проведение анализа рисков может стать обоснованием финансовых вложений в обеспечение информационной безопасности.

При проведении анализа рисков выполняются следующие основные работы.

Инвентаризация и классификация ресурсов (активов). Составляется перечень всех ресурсов в ИС и определяется их значимость в качественном или количественном виде.

Построение модели угроз и модели потенциального злоумышленника. На этом этапе составляется перечень угроз, проводится их формализованное описание, описание источников этих угроз (потенциального злоумышленника) и механизмов реализации. От того, какая будет принята модель угроз и злоумышленника, зависит очень многое и, в первую очередь, стоимость системы защиты. Действительно, разница в построении и затратах на систему ИБ очевидна, если в качестве потенциального злоумышленника принимается 1) внешняя персона, не имеющая какой-либо определенной мотивации на несанкционированные действия, но способная использовать общедоступный инструментарий для реализации атак, и 2) конкурирующая организация, заинтересованная в экономическом шпионаже. Строить же систему защиты, ориентируясь на все возможные угрозы, бессмысленно как с технологической, так и с финансовой точки зрения.

Идентификация уязвимых мест в ИС. Ориентируясь на выбранную модель угроз и потенциального злоумышленника, осуществляется идентификация и описание уязвимостей, существующих в ИС. Необходимо понимать, наличие какой уязвимости связанно с реализацией определенной угрозы, так как эта взаимосвязь будет использоваться на двух последующих этапах анализа рисков.

Оценка последствий от реализации угроз. Этап, результаты которого должны стать основой для технологического и финансового обоснования системы защиты. Проводится оценка влияния нарушений, связанных с работой ИС и вызванных реализацией угроз, на деятельность организации (Business Impact Analysis). То есть проводится анализ сценариев “если, то”, позволяющий получить представление о том, насколько сильна зависимость деятельности организации от функционирования ИС. Результатами этапа является перечень

рисков и их качественная или количественная оценка. На рисунке приведена графическая зависимость между основными понятиями, используемыми при проведении анализа рисков.

Формирование требований по обеспечению ИБ. Зная уязвимые места, угрозы, имея представление о последствиях реализации угроз, приступают к формированию требований к системе обеспечения информационной безопасности. Данные требования должны впоследствии стать основой при составлении технического задания на построение СОИБ. Выполнение требований по информационной безопасности, сформулированных на этом этапе, должно снизить риски нарушения ИБ до приемлемого уровня.

Уже упоминалось: для того чтобы результаты анализа рисков были объективными и охватывали интересы по защите информации всей организации, необходимо активное совместное участие представителей бизнес- и технологических подразделений на всех этапах анализа рисков. Очень часто анализ рисков нарушения ИБ понимается как сугубо технологическая задача, и это является одной из причин того, что результаты такого анализа не удовлетворяют лиц, ответственных за принятие решений.

При проведении инвентаризации и классификации ресурсов ИС оценку их значимости для организации необходимо давать на основании разностороннего анализа со стороны владельцев и потребителей ресурса. Для разных категорий ресурсов (информационных, сервисных, программно-аппаратных, людских) их значимость может определяться исходя из различных критериев. Например, если за работоспособность Интернета отвечает отдел системного администрирования, для которого критичное время простоя этого сервиса составляет 48 ч, то для отдела, использующего Интернет для выполнения ежедневных производственных задач, допустимое время простоя данного сервиса может быть существенно меньше. Также необходимо учитывать взаимосвязь между ресурсами. Если для сервиса электронной почты, реализуемого, в том числе, с использованием сервиса Интернет, предъявляются более строгие требования, это должно найти отражение и для всех ресурсов, связанных с сервисом электронной почты. Формирование единой шкалы ценностей ресурсов ИС, которая может зависеть от уровня конфиденциальности информационного ресурса, максимального допустимого времени простоя, затрат на получение ресурса и т. д. и которая принимается всеми заинтересованными подразделениями, является основной задачей этапа инвентаризации и классификации ресурсов.

Оценка последствий от реализации угроз — ключевой этап анализа рисков. И здесь, с одной стороны, подразделение, отвечающее за информационную безопасность, должно четко определить, какие ресурсы ИС потенциально подвержены внешнему или внутреннему негативному воздействию и каковы могут быть результаты такого воздействия. Подразделение, отвечающее за ИБ, должно определить возможность реализации каждой угрозы на основании анализа уязвимых мест в ИС и модели потенциального злоумышленника. С другой стороны, подразделения, имеющие непосредственное отношение к бизнес-деятельности организации, должны определить результаты негативного воздействия на ресурс уже в терминах бизнеса (финансовые потери, ухудшение имиджа компании, уход текущих и потенциальных заказчиков и др.). При этом возможность реализации и оценка результатов негативного воздействия может осуществляться как по качественной шкале, так и в количественном виде.

В случае, если в организации ведется подробная статистика по инцидентам, связанным с нарушениями ИБ, то, используя ее данные и результаты количественного анализа рисков, нетрудно спрогнозировать потенциальный ущерб на определенный промежуток времени. Очевидно, что вложения в ИБ не должны превышать сумму потенциального ущерба.

Работы по анализу рисков нарушения ИБ могут проводиться как собственными силами, так и с привлечением внешних консультантов. При проведении анализа рисков собственными силами в составе рабочей группы, проводящей анализ рисков, необходим менеджер достаточно высокого уровня, который бы имел возможность согласовывать работу на уровне руководителей ИТ, ИБ и бизнес-подразделений. Отсутствие в составе рабочей

группы лица с достаточным уровнем полномочий может затруднить получение необходимой информации и снизить доверие к результатам анализа.

При проведении анализа рисков с привлечением внешнего консультанта к задаче выбора компании-консультанта нужно подходить очень тщательно и, в первую очередь, исходить из специфики деятельности вашей компании и используемых информационных технологий. У компании-консультанта должен быть штат сотрудников необходимой квалификации и опыт работы с организациями в вашей отрасли. При таком подходе к проведению работы информация об используемых технологиях ИБ будет доступна сторонней компании, и этот аспект следует учитывать при формировании договорных отношений. Из положительных моментов можно отметить то, что консультант имеет опыт работы со многими заказчиками, что поможет избежать общеизвестных ошибок и использовать только хорошо себя зарекомендовавшие решения. Консультант обладает методиками, способен выделить на работу необходимые ресурсы, что позволит повысить качество и сократить сроки проекта.

В заключение хотелось бы отметить аспект, связанный с востребованностью анализа рисков. Процесс обеспечения ИБ носит циклический характер. При этом для организаций с разным уровнем развития ИТ количество этапов в таком цикле может существенно различаться. Для некоторых организаций вполне достаточно базовых механизмов безопасности. Действительно, если небольшой компании, в которой используется электронная почта и Интернет, имеется несколько файловых серверов и небольшая бухгалтерская система, а весь ИТ-персонал — это два системных администратора, предложить работу по проведению анализа рисков, то такое предложение может не найти понимания. А дать какие-либо четкие критерии идентификации организации, для которой проведение анализа рисков целесообразно, довольно сложно. Единственное, что можно сказать уверенно: если в вашей компании существует понимание высокой зависимости вашего бизнеса от используемых информационных технологий (независимо от размера организации), то результаты анализа рисков будут интересны и помогут построить систему обеспечения ИБ, адекватную реальным угрозам, позволят оптимизировать финансовые вложения в данное направление.

Литература

1. Журналы Информационная безопасность *за 2004-2005гг.*
2. PCWeek *№14/2004.*
3. GIO №4/2004

Article received: 2006-05-11