Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 11 (162)/2006

Управление рисками: обзор употребительных подходов

Часть I

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Управление рисками: обзор употребительных подходов

В данном выпуске бюллетеня предлагается обзор, подготовленный по материалам учебного курса «Основы информационной безопасности» доктора физ.-мат. наук, заведующего сектором в отделе информационной безопасности НИИ системных исследований РАН В.А. Галатенко с любезного согласия автора. По мнению редакции, этот материал представляет большой интерес, поскольку вопросы анализа рисков в сфере информационных технологий в настоящее время особенно актуальны.

СОДЕРЖАНИЕ

Введение

Информационная безопасность (ИБ) должна достигаться экономически оправданными мерами. В данной статье представлена методика, позволяющая сопоставить возможные потери от нарушений ИБ со стоимостью защитных средств и выбрать направления, на которых целесообразно сконцентрировать основные ресурсы.

Тема «Управление рисками» рассматривается на административном уровне ИБ, поскольку только руководство организации может выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Вообще говоря, управление рисками, равно как и выработка собственной политики безопасности, нужны только для тех организаций, информационные системы (ИС) которых и/или обрабатываемые данные можно считать нестандартными.

Типовую организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно, с формальной точки зрения, в свете российского законодательства в области информационной безопасности). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество документов, во втором — достаточно определиться лишь с несколькими параметрами.

Основные понятия

Адекватная безопасность — уровень безопасности, соразмерный с риском и величиной ущерба от потери, ненадлежащего использования, модификации или несанкционированного доступа к информации.

Базовый уровень безопасности — минимальный набор регуляторов безопасности, необходимый для защиты информационной системы, определяемый из потребностей ИС в обеспечении доступности, конфиденциальности и целостности.

Калиброванная (регулируемая, настраиваемая, повышаемая) *безопасность* — система безопасности, обеспечивающая несколько уровней защиты (низкий, умеренный, высокий) в зависимости от угроз, рисков, доступных технологий, поддерживающих сервисов, времени, кадровых и экономических ресурсов.

Компрометация — раскрытие информации неавторизованным лицам или нарушение политики безопасности организации, способное повлечь за собой умышленное или неумышленное несанкционированное раскрытие, модификацию, разрушение и/или потерю информации.

Нарушение информационной безопасности — нарушение или угроза неминуемого нарушения политики информационной безопасности, правил добропорядочного поведения или стандартных правил информационной безопасности.

Уровень (степень) критичности ИС — параметр, характеризующий последствия некорректного поведения информационной системы. Чем серьезнее прямое или косвенное воздействие некорректного поведения, тем выше уровень критичности ИС.

Система, критичная для выполнения миссии организации (критичная система) — телекоммуникационная или информационная система, передающая, обрабатывающая и/или хранящая информацию, потеря, ненадлежащее использование и/или несанкционированный доступ к которой могут негативно воздействовать на миссию организации.

Окружение (среда) — совокупность внешних процедур, условий и объектов, воздействующих на разработку, эксплуатацию и сопровождение информационной системы.

Воздействие (влияние) — величина (размер) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы.

Анализ воздействия на производственную деятельность — анализ потребностей информационной системы и ассоциированных с ней процессов и зависимостей, используемый для спецификации требований к непрерывности функционирования и приоритетов восстановления ИС после серьезных аварий.

Контрмеры — действия, устройства, процедуры, технологии или другие меры, уменьшающие уязвимость информационной системы. Синонимом служит термин *«регуляторы безопасности»*.

Лечение — действие по исправлению уязвимости или устранению угрозы. Тремя возможными типами лечения являются:

- установка корректирующих «заплат»;
- регулировка конфигурационных параметров;
- устранение уязвимых программных приложений.

План лечения — план осуществления лечения одной или нескольких угроз и/или уязвимостей, которым подвержена информационная система организации. В плане обычно рассматривается несколько возможных способов устранения угроз и уязвимостей и определяются приоритеты по осуществлению лечения.

Риск — уровень воздействия на производственную деятельность организации (включая миссию, функции, образ, репутацию), ее активы (ресурсы) и персонал, являющегося следствием эксплуатации информационной системы и зависящего от потенциального воздействия угрозы и вероятности ее осуществления (реализации).

Риски, связанные с информационными технологиями — общее воздействие на производственную деятельность с учетом:

- вероятности того, что определенный источник угроз использует или активизирует определенную уязвимость информационной системы;
- результирующего воздействия, если угроза будет реализована. Риски, связанные с информационными технологиями, являются следствием законодательной ответственности или производственных потерь вследствие:
  - несанкционированного (злоумышленного, незлоумышленного, случайного) доступа к информации;

- незлоумышленных ошибок и/или упущений;
- разрушения ИС в результате стихийных бедствий или техногенных катастроф;
- неспособности проявлять должную аккуратность и старательность при реализации и/или эксплуатации ИС.

Остаточный риск — остающийся, потенциальный риск после применения всех контрмер. С каждой угрозой ассоциирован свой остаточный риск.

Совокупный (суммарный, полный) риск — возможность осуществления вредоносного события при отсутствии мер по нейтрализации рисков.

Анализ рисков — процесс идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительных контрмер, ослабляющих (уменьшающих) это воздействие. *Анализ рисков* является частью управления рисками и синонимом термина *«оценка рисков»*, он включает в себя анализ угроз и уязвимостей.

Управление рисками — процесс, включающий оценку рисков, анализ экономической эффективности, выбор, реализацию и оценку контрмер, а также формальное санкционирование ввода системы в эксплуатацию. В процессе управления рисками принимаются во внимание и анализируются эффективность действий и законодательные ограничения.

Нейтрализация (уменьшение, ослабление) рисков — определение приоритетов, оценка и реализация контрмер, должным образом уменьшающих риски.

Терпимость по отношению к риску — уровень риска, который считается допустимым для достижения желаемого результата.

Санкционирование безопасной эксплуатации — официальное решение, принимаемое руководством организации, санкционирующее ввод информационной системы в эксплуатацию и явным образом объявляющее допустимыми риски, оставшиеся после реализации согласованного набора регуляторов безопасности.

Категория безопасности — характеристика информации и/или информационной системы, основанная на оценке потенциального воздействия потери доступности, конфиденциальности и/или целостности этой информации и/или информационной системы на производственную деятельность организации, ее активы и/или персонал.

Уровень защищенности — иерархический показатель степени чувствительности по отношению к определенной угрозе.

Требования безопасности — требования к информационной системе, являющиеся следствием действующего законодательства, миссии и потребностей организации.

Наиболее распространенные угрозы

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для выбора наиболее экономичных средств обеспечения безопасности.

Основные определения и критерии классификации угроз

Угроза — это потенциальная возможность определенным образом нарушить информационную безопасность. Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, — злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Чаще всего угроза возникает из-за уязвимостей в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении). Промежуток времени от момента, когда появляется возможность использовать уязвимость, и до того, когда она ликвидируется, называется окном опасности, ассоциированным с данной уязвимостью. Пока существует окно опасности, возможны успешные атаки на информационную систему.

Если речь идет об ошибках в ПО, то окно опасности образуется с появлением средств использования ошибки и ликвидируется при наложении «заплат», ее исправляющих. Для боль-

шинства уязвимостей окно опасности существует довольно долго (несколько дней, иногда — недели). За это время должны произойти следующие события:

- появляется информация о средствах использования уязвимости;
- выпускаются соответствующие «заплаты»;
- «заплаты» устанавливаются в защищаемой информационной системе.

Новые уязвимости и средства их использования появляются постоянно. Это означает, что, во-первых, почти всегда существуют окна опасности, и во-вторых, отслеживание таких окон должно производиться непрерывно, а выпуск и наложение «заплат» — как можно более оперативно.

Отметим, что некоторые угрозы нельзя назвать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы происходит по причине зависимости аппаратного обеспечения информационных систем от электропитания.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы. Существует много мифов в информационных технологиях о возможных угрозах и уязвимостях (вспомним хотя бы пресловутую «Проблему-2000»). Незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Отметим, что само понятие «угроза» в разных ситуациях трактуется по-разному. Например, для подчеркнуто открытой организации может просто не существовать угроз конфиденциальности, так как вся информация считается общедоступной. И все же в большинстве случаев нелегальный доступ считается серьезной опасностью.

Рассмотрим отношение к угрозам с точки зрения типичной (по нашему мнению) организации. Их можно классифицировать по нескольким критериям:

- аспект информационной безопасности (доступность, целостность, конфиденциальность), против которого они (угрозы) направлены в первую очередь;
- компонент информационных систем, на который угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- способ осуществления угроз (случайные/преднамеренные действия природного/техногенного характера);
- расположение источника угроз (внутри/вне рассматриваемой ИС).

В качестве основного критерия мы будем использовать первый (аспект ИБ), привлекая при необходимости остальные.

Наиболее распространенные угрозы доступности

Самыми частыми и опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки являются непосредственными угрозами (неправильно введенные данные или ошибка в программе, вызвавшие крах системы), иногда они создают уязвимости, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь — следствие непреднамеренных ошибок. Пожары и наводнения можно считать пустяками по сравнению с безграмотностью и неорганизованностью.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками — это максимальная автоматизация и строгий контроль за правильностью совершаемых действий.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новое и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой, так как нет соответствующей подготовки (недостаток общей компьютерной грамотности и культуры, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);

- невозможность работать с системой из-за отсутствия технической поддержки (неполнота документации, невозможность получения справочной информации и т.п.).

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание выполнения обслуживающим персоналом и/или пользователями своих обязанностей (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые обиженные сотрудники — нынешние и бывшие. Как правило, их действиями руководит желание нанести вред организации-обидчику, например: повредить оборудование; встроить логическую «бомбу», которая со временем разрушит программы и/или данные; удалить данные и т.д. Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны вредить весьма эффективно. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия — пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и аналогичных «злоумышленников» (среди которых самый опасный — низкое качество электропитания и его перебои) приходится 13% потерь, нанесенных информационным системам.

Примеры угроз доступности

Угрозы доступности могут выглядеть грубо — как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение, как правило, происходит по естественным причинам (чаще всего из-за грозы). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, поэтому не редки случаи выгорания оборудования.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом — с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную угрозу следует признать экзотической и, следовательно, надуманной. Действительно опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы. Автору довелось быть свидетелем прорыва трубы отопления, в результате чего системный блок компьютера (это была рабочая станция производства Sun Microsystems) оказался заполненным кипятком. Справедливости ради стоит отметить, что когда кипяток вылили, а компьютер просушили, он возобновил нормальную работу, однако лучше такие опыты не ставить...

Летом в сильную жару, когда они больше всего нужны, норовят сломаться кондиционеры, установленные в серверных залах, набитых критически важным и дорогостоящим оборудованием. В результате весьма чувствительный ущерб наносится и репутации, и кошельку организации.

Теоретически все (или почти все) знают, что периодически необходимо производить резервное копирование данных. Однако, даже если такое копирование осуществляется на практике, резервные носители зачастую хранятся небрежно, не обеспечивая их элементарной сохранности, защиты от вредного влияния окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Перейдем теперь к угрозам доступности. Речь пойдет о программных атаках на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное использование ресурсов (полосы пропускания сетей, вычислительных возможностей процессоров или оперативной

памяти). По расположению источника угрозы такое потребление подразделяется на локальное и удаленное. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов — атака, получившая наименование «SYN-наводнение». Ее идея состоит в попытке переполнить таблицу «полуоткрытых» TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака, по меньшей мере, затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к атаке «Papa Smurf» уязвимы сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты «съедают» полосу пропускания (сеть как бы самовозбуждается).

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме — как скоординированные распределенные атаки, когда на сервер с множества разных адресов в максимально возможном темпе направляются вполне легальные запросы на соединение и/или обслуживание. Начало «моды» на подобные атаки можно отнести к февралю 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее, владельцы и пользователи систем). Отметим, что если имеет место архитектурный просчет, нарушающий баланс между пропускной способностью сети и производительностью сервера, то защититься от распределенных атак на доступность крайне трудно.

Для выведения систем из штатного режима эксплуатации могут использоваться программные и аппаратные ошибки. Например, известная ошибка в процессоре Pentium I дает возможность локальному пользователю путем выполнения определенной команды «завесить» компьютер, так что помогает только аппаратный RESET.

Программа «Teardrop» удаленно «завешивает» компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

Вредоносное программное обеспечение

Одним из опаснейших видов атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Мы выделим следующие грани вредоносного ПО:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Часть, осуществляющую вредоносную функцию, будем называть «бомбой». Вообще говоря, спектр вредоносных функций неограничен, поскольку «бомба», как и любая другая программа, может характеризоваться сколь угодно сложной логикой, но обычно «бомбы» предназначаются для:

- внедрения другого вредоносного ПО;
- получения контроля над атакуемой системой;
- агрессивного потребления ресурсов;
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

- вирусы — код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- «черви» — код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по информационной системе и их выполнение (для активизации вируса требуется запуск зараженной программы).

Обычно вирусы распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. «Черви», напротив, ориентированы в первую очередь на сетевые «путешествия».

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, «черви» «съедают» полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных «бомб».

Вредоносный код, обладающий внешним представлением в виде функционально полезной программы, называется троянским. Например, некогда «нормальная» программа, будучи пораженной вирусом, становится троянской. Порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Отметим, что данные нами определения и приведенная классификация вредоносного ПО отличаются от общепринятых. Например, в ГОСТ Р 51275-99 «Защита информации. Объект

информатизации. Факторы, воздействующие на информацию. Общие положения» содержится следующее определение:

«Программный вирус — исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах».

На наш взгляд, подобное определение неудачно, поскольку в нем смешаны функциональные и транспортные аспекты.

Окно опасности для вредоносного ПО появляется с выпуском новой разновидности «бомб», вирусов и/или «червей» и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых «заплат».

Вероятно, по какой-то традиции, из всего вредоносного ПО наибольшее внимание общественности приходится на долю вирусов. Однако до марта 1999 года с полным правом можно было утверждать, что несмотря на экспоненциальный рост числа известных вирусов, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил компьютерной гигиены сводит риск заражения практически к нулю. Там где работают, а не играют, число зараженных компьютеров составляет лишь доли процента.

В марте 1999 года, с появлением вируса Melissa, ситуация кардинальным образом изменилась. Melissa — это макровирус для файлов MS-Word, распространяющийся посредством электронной почты в присоединенных файлах. Когда такой (зараженный) присоединенный файл открывают, он рассылает свои копии по первым 50 адресам из адресной книги Microsoft Outlook. В результате почтовые серверы подвергаются атаке на доступность.

В данном случае отметим два момента.

- Пассивные объекты уходят в прошлое; так называемое активное содержимое становится нормой. Файлы, которые по всем признакам должны были бы относиться к данным (например, документы в форматах MS-Word или Postscript, тексты почтовых сообщений), способны содержать интерпретируемые компоненты, которые могут запускаться неявным образом, при открытии файла. Как и всякое в целом прогрессивное явление, такое «повышение активности данных» имеет свои оборотные стороны (в рассматриваемом случае — отставание в разработке механизмов безопасности и ошибки в их реализации). Еще не скоро рядовые пользователи научатся применять интерпретируемые компоненты «в мирных целях» (или хотя бы узнают об их существовании), а перед злоумышленниками открылось по существу неограниченное поле деятельности. Как ни банально это звучит, но если для стрельбы по воробьям устанавливают пушку, то пострадает стреляющий.
- Интеграция разных сервисов, наличие среди них сетевых, всеобщая связность многократно увеличивают потенциал для атак на доступность, облегчают распространение вредоносного ПО (вирус Melissa — классический тому пример). Образно говоря, многие информационные системы, если не принять защитных мер, оказываются «в одной лодке» (точнее — в одном корабле без переборок), так что достаточно одной небольшой казалось бы «пробоины», чтобы «лодка» стала стремительно тонуть, заливаемая бурным, все усиливающимся потоком.

Как это часто бывает, Melissa дала толчок к быстрому появлению на свет целой серии вирусов, «червей» и их комбинаций: Explorer.zip (июнь 1999), Bubble Boy (ноябрь 1999), ILOVEYOU (май 2000) и т.д. и т.п. Не то чтобы от них был особенно большой ущерб, но общественный резонанс, как это свойственно вирусам, они вызвали немалый.

Активное содержимое, помимо интерпретируемых компонентов документов и других файлов данных, имеет еще одно популярное обличье — так называемые мобильные агенты. Это программы, которые загружаются на другие компьютеры и там выполняются. Наиболее известные примеры мобильных агентов — Java-аплеты, загружаемые на пользовательский компьютер и интерпретируемые Интернет-навигаторами. Оказалось, что разработать для них модель безопасности, оставляющую достаточное количество возможностей для полезных действий, не так-то просто; еще сложнее безошибочно реализовать такую модель. В августе 1999 года стали известны недочеты в реализации технологий ActiveX и Java в рамках Microsoft Internet Explorer, которые давали возможность размещать на Web-серверах вредоносные аплеты, позволяющие получать полный контроль над системой-визитером.

Для внедрения «бомб» часто используются ошибки типа «переполнения буфера», когда

программа, работая с областью памяти, выходит за допустимые границы и записывает в нужные злоумышленнику места нужное ему содержимое. Так действовал еще в 1988 году знаменитый «червь Морриса»; в июне 1999 года нашли способ использовать аналогичный метод по отношению к Microsoft Internet Information Server (IIS), чтобы получить контроль над Web-сервером. Окно опасности охватило сразу около полутора миллионов серверных систем...

Не забыты современными злоумышленниками и «старые, но недобрые» троянские программы. Например, «троянцы» Back Orifice и Netbus позволяют получить контроль над пользовательскими системами с различными вариантами MS-Windows. Актуальной и весьма опасной угрозой является внедрение руткитов (набор файлов, устанавливаемых в системе с целью изменения ее стандартной функциональности вредоносным и скрытным образом), ботов (программа, автоматически выполняющая некоторую миссию; группа компьютеров, на которой функционируют однотипные боты, называется ботсетью), потайных ходов (вредоносная программа, слушающая команды на определенных TCP-или UDP-портах) и шпионского программного обеспечения (вредоносное ПО, нацеленное на компрометацию конфиденциальных данных пользователя.

Таким образом, вредоносное ПО может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности. К рассмотрению соответствующих угроз мы и переходим.

Основные угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) располагаются кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен суммарный ущерб в размере 882 миллионов долларов. Можно предположить, что подлинный ущерб был гораздо больше, поскольку многие организации по понятным причинам скрывают такие инциденты. Не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

В большинстве расследованных случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Целесообразно провести различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (являющийся, как правило, штатным сотрудником) может:

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, порой — служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) возбудила судебный иск против президента корпорации, обвиняя его в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее боссом президенту. Содержание письма для нас сейчас не важно; важно время отправки.

Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что он (босс) в указанное время разговаривал по мобильному телефону, находясь за рулем автомобиля вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние «файл против файла». Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль своего босса, поскольку ей было поручено его регулярное изменение), и иск был отвергнут...

(Теоретически существует возможность, что оба фигурировавших на суде файла были подлинными, корректными с точки зрения их целостности, а письмо отправили пакетными средствами, однако, на наш взгляд, это было бы очень странное для вице-президента действие.)

Помимо прочих, из приведенного случая можно сделать вывод не только об угрозах нарушения целостности, но и об опасности слепо доверять компьютерную информацию. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя. Отметим, что последняя угроза актуальна даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность.

Еще один урок: угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить «неотказуемость», то компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы по отношению к нарушению целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного ПО — пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на два класса — предметную и служебную. Служебная информация (такая, например, как пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато несанкционированным доступом ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются (многоразовые) пароли или иная конфиденциальная информация, то можно быть уверенным, что она будет храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на своем рабочем столе или попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности — частой) смене только ухудшают положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двумтрем легко запоминаемым (и столь же легко угадываемым) паролям.

Описанный класс уязвимостей можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую и не может быть обеспечена) необходимая защита. Угроза же состоит в том, что кто-то не откажется взять секреты, которые сами просятся в руки. Помимо паролей в головах и записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает вполне возможной реализацию угрозы перехвата данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея тут одна — осуществить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной угрозой являются... выставки, на которые многие организации, недолго думая, отправляют оборудование из производственной сети, со всеми хранящимися на этих носителях данными. Остаются прежними пароли, при удаленном доступе они по-прежнему передаются в открытом виде. Это плохо даже в пределах защищенной сети организации; в объединенной же сети выставки это слишком суровое испытание честности всех участников.

Еще один пример изменения, о котором часто забывают, — хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах, и получить доступ к ним могут многие.

Перехват данных — очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, установить их, например, на кабельную сеть может даже уборщица, так что эту угрозу нужно принимать во внимание не только по отношению к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие, как «маскарад» — выполнение действий под видом лица, обладающего полномочиями для доступа к дан-

ным (см., например, статью Айрэ Винклера «Задание: шпионаж» в Jet Info, № 18, 1996г.).

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример — злоумышленные действия при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные угрозы, на долю которых приходится львиная доля ущерба, наносимого субъектам информационных отношений.

Основные этапы управления рисками

Общие положения

Использование информационных систем связано с определенной совокупностью рисков. Когда риск (возможный ущерб) неприемлемо велик, необходимо принять экономически оправданные защитные меры. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения размер риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимости), а также величины возможного ущерба.

Таким образом, суть работы по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры по уменьшению этого размера и затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- (пере)оценку (измерение) рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);
- уменьшение риска (например, за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно подразделить на следующие этапы:

(1) выбор анализируемых объектов и уровня детализации их рассмотрения;
(2) выбор методики оценки рисков;
(3) идентификация активов;
(4) анализ угроз и их последствий, определение уязвимостей в защите;
(5) оценка рисков;
(6) выбор защитных мер;
(7) реализация и проверка выбранных мер;
(8) оценка остаточного риска.

Этапы (6) и (7) относятся к выбору защитных средств (нейтрализации рисков), остальные — к оценке рисков.

Уже перечисление этапов показывает, что управление рисками — процесс циклический. По существу, последний этап — это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС. Тогда эффект оказывается наибольшим, а затраты — минимальными. Можно выделить пять основных этапов жизненного цикла ИС:

- инициация;
- закупка (разработка);
- установка;
- эксплуатация;
- выведение из эксплуатации.

Кратко опишем, что может дать управление рисками на каждом из перечисленных этапов.

На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности.

На этапе закупки (разработки) выявленные риски способны помочь при выборе архи-

тектурных решений, играющих ключевую роль в обеспечении безопасности.

На этапе установки выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию.

На этапе эксплуатации управление рисками должно сопровождать все существенные изменения в системе.

При выведении системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

Подготовительные этапы управления рисками

Первые три этапа процесса управления рисками можно считать подготовительными. Их суть состоит в следующем.

Выбор анализируемых объектов и уровня детализации их рассмотрения — первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако, если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приблизительностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

По многим причинам целесообразно создать карту информационной системы организации. Для управления рисками подобная карта особенно важна, поскольку она наглядно показывает, какие сервисы выбраны для анализа, а какими было решено пренебречь. Если ИС меняется, а карта поддерживается в актуальном состоянии, то при переоценке рисков сразу станет ясно, какие новые или существенно изменившиеся сервисы нуждаются в рассмотрении.

Вообще говоря, уязвимым является каждый компонент информационной системы — от куска сетевого кабеля, который могут прогрызть мыши, до базы данных, которая может быть разрушена из-за неумелых действий администратора. Как правило, в сферу анализа невозможно включить каждый винтик и каждый байт. Приходится останавливаться на некотором уровне детализации, отдавая себе отчет в приблизительности оценки. Для новых систем предпочтителен детальный анализ; старая система, подвергшаяся небольшим модификациям, может быть проанализирована более поверхностно.

Очень важно выбрать разумную методику оценки рисков. Целью оценки является получение ответов на следующие вопросы:

- приемлемы ли существующие риски?
- какие из неприемлемых рисков в первую очередь нуждаются в уменьшении?
- какие защитные средства экономически целесообразно использовать для уменьшения неприемлемых рисков?

Следовательно, оценка рисков должна быть количественной, допускающей сопоставление с заранее выбранными границами допустимости и расходами на реализацию новых регуляторов безопасности. Управление рисками — типичная оптимизационная задача, и существует довольно много программных продуктов, способных помочь в ее решении (иногда подобные продукты просто прилагаются к книгам по информационной безопасности). Принципиальная трудность, однако, состоит в неточности исходных данных. Можно, конечно, попытаться получить для всех анализируемых величин денежное выражение, высчитать все с точностью до копейки, но большого смысла в этом нет. Практичнее пользоваться условными единицами. В простейшем и вполне допустимом случае можно пользоваться трехбалльной шкалой. Далее будет продемонстрировано, как это делается.

При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации. Отправной точкой здесь является представление о миссии организации, то есть о видимых основных направлениях деятельности, которые желательно (или необходимо) сохранить в любом случае. Выражаясь объектно-ориентированным языком, следует в первую очередь описать внешний интерфейс организации, рассматриваемой как абстрактный объект.

Одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее (структуры) использования. Эти сведения целесообразно нанести на карту ИС в качестве граней соответствующих объектов.

Информационной основой любой сколько-нибудь крупной организации является сеть, по-

этому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование (мосты, маршрутизаторы и т.п.).

К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), другое базовое и прикладное программное обеспечение, инструментальные средства, средства управления сетью и отдельными системами. Важно зафиксировать, где (в каких узлах сети) хранится программное обеспечение и из каких узлов используется.

Третьим видом информационных активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и категориям критичности, выявить места их хранения и обработки, способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности.

Управление рисками — процесс далеко не линейный. Практически все его этапы связаны между собой, и по завершении почти любого из них может выявиться необходимость возврата к предыдущему. Так, при идентификации активов может появиться понимание, что выбранные границы анализа следует расширить, а степень детализации — увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны.

Анализ угроз и оценка рисков

Этапы, предшествующие анализу угроз, можно считать подготовительными, поскольку, строго говоря, они впрямую не связаны с рисками. Риск появляется там, где есть угрозы.

Перечень наиболее распространенных угроз предполагается известным. К сожалению, с практической точки зрения число угроз оказывается бесконечно большим, причем далеко не все из них носят компьютерный характер. Так вполне реальной угрозой является наличие мышей и тараканов в помещениях, занимаемых организацией. Первые могут повредить кабели, вторые — вызвать короткое замыкание.

Как правило, наличие той или иной угрозы является следствием уязвимостей в защите информационной системы, которые, в свою очередь, объясняются отсутствием некоторых сервисов безопасности или недостатками в реализующих их защитных механизмах. Опасность прогрызания кабелей исходит не только от мышей, и от недостаточной прочности защитной оболочки или ее отсутствия.

Первый шаг в анализе угроз — их идентификация. Анализируемые виды угроз следует выбрать из соображений здравого смысла (оставив вне поля зрения, например, землетрясения, однако не исключая возможности захвата организации террористами), но в пределах выбранных видов провести максимально полное рассмотрение.

Целесообразно выявлять не только сами угрозы, но и источники их возникновения, это поможет в выборе дополнительных средств защиты. Например, нелегальный вход в систему может стать следствием воспроизведения начального диалога, подбора пароля или подключения к сети неавторизованного оборудования. Очевидно, для противодействия каждому из перечисленных способов нелегального входа нужны свои механизмы безопасности.

После идентификации угрозы необходимо оценить вероятность ее осуществления. Допустимо использовать при этом трехбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятность).

Кроме вероятности осуществления, важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале.

Оценивая тяжесть ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные, такие как подрыв репутации, ослабление позиций на рынке и т.п. Пусть, например, в результате дефектов в управлении доступом к бухгалтерской информации сотрудники получили возможность корректировать данные о собственной заработной плате. Следствием такого состояния дел может стать не только перерасход бюджетных или корпоративных средств, но и полное разложение коллектива, грозящее развалом организации.

Уязвимости обладают свойством притягивать к себе не только злоумышленников. Не всякий устоит перед искушением немного увеличить свою зарплату, если есть уверенность, что это сойдет в рук. Поэтому, оценивая вероятность осуществления угроз, целесообразно исходить не только из среднестатистических данных, но учитывать также специфику конкретных информационных систем. Если в подвале дома, занимаемого организацией, располагается сауна, а сам дом имеет деревянные перекрытия,

то вероятность пожара, к сожалению, оказывается существенно выше средней.

После того, как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, то есть собственно к оценке рисков. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвертый — к среднему, два последних — к высокому, после чего появляется возможность снова привести их к трехбалльной шкале. По этой шкале и следует оценивать приемлемость рисков. Правда, граничные случаи, когда вычисленная величина совпала с приемлемой, целесообразно рассматривать более тщательно из-за приближенного характера результата.

Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные защитные меры. Как правило, для ликвидации или нейтрализации уязвимости, сделавшей реальной опасную угрозу, существует несколько механизмов безопасности, отличающихся эффективностью и стоимостью. Например, если велика вероятность нелегального входа в систему, можно приказать пользователям выбирать длинные пароли (скажем, не менее восьми символов), задействовать программу генерации паролей или закупить интегрированную систему аутентификации на основе интеллектуальных карт. Если имеется вероятность умышленного повреждения сервера баз данных, что грозит серьезными последствиями, то можно врезать замок в дверь серверной комнаты или поставить около каждого сервера по охраннику.

Выбор защитных мер и последующие этапы управления рисками

Оценивая стоимость защитных мер, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, на обучение и переподготовку персонала. Эту стоимость также можно выразить по трехбалльной шкале и затем сопоставить ее с разностью между вычисленным и приемлемым риском. Если по этому показателю новое средство оказывается экономически выгодным, его можно принять к дальнейшему рассмотрению (подходящих средств, вероятно, будет несколько). Однако, если средство окажется дорогим, его не следует сразу отбрасывать, памятуя о приближенности расчетов.

Выбирая подходящий способ защиты, целесообразно учитывать возможность экранирования одним сервисом безопасности сразу нескольких прикладных сервисов. Так поступили в Массачусетском технологическом институте, защитив несколько тысяч компьютеров сервером аутентификации Kerberos.

Важным обстоятельством является совместимость нового средства со сложившейся организационной и аппаратно-программной структурой, с традициями организации. Меры безопасности, как правило, носят недружественный характер, что может отрицательно сказаться на энтузиазме сотрудников. Порой сохранение духа открытости важнее минимизации материальных потерь. Впрочем, такого рода ориентиры должны быть расставлены в политике безопасности верхнего уровня.

Можно представить ситуацию, когда для нейтрализации риска не существует эффективных и приемлемых по цене мер. Например, компания, базирующаяся в сейсмически опасной зоне, не всегда может позволить себе строительство защищенной штаб-квартиры. В таком случае приходится поднимать планку приемлемого риска и переносить центр тяжести на смягчение последствий и выработку планов восстановления после аварий, стихийных бедствий и иных происшествий. Продолжая пример с сейсмоопасностью, можно рекомендовать регулярное тиражирование данных в другой город и овладение средствами восстановления первичной базы данных.

Как и всякую иную деятельность, реализацию и проверку новых регуляторов безопасности следует предварительно распланировать. В плане необходимо учесть наличие финансовых средств, сроки обучения персонала. Нужно составить план тестирования (автономного и комплексного), если речь идет о программно-техническом механизме защиты.

Когда намеченные меры приняты, необходимо проверить их действенность, то есть убедиться в том, что остаточные риски стали приемлемыми. Если это на самом деле так, значит, все в порядке и можно спокойно намечать дату ближайшей переоценки. В противном случае придется проанализировать в срочном порядке ошибки, которые были допущены, и провести повторный сеанс управления рисками.

Ключевые роли в процессе управления рисками

Управление рисками — деятельность административного уровня информационной безопасности. Ключевые роли в этой деятельности принадлежат следующим должностным лицам.

Руководитель организации. Он несет общую ответственность за выполнение организацией возложенной на нее миссии. Он должен обеспечить, чтобы ресурсы, необходимые для выполнения миссии, были выделены и эффективно применялись. При принятии решений о выделении ресурсов руководитель должен опираться на результаты анализа рисков. Разработка и проведение в жизнь эффективной программы управления рисками, связанными с информационными технологиями, включающей их (рисков) оценку и нейтрализацию, требует поддержки высшего руководства организации.

Начальник управления (отдела) информатизации. Он отвечает за планирование, выделение средств и функционирование информационных систем организации, включая аспекты, относящиеся к информационной безопасности. Принимаемые им решения должны основываться на результатах эффективной программы управления рисками.

Владельцы систем и информации. Они отвечают за то, чтобы для защиты принадлежащих им информационных систем и данных применялись соответствующие регуляторы безопасности. Они ответственны и за изменения, вносимые в системы. Решения по планированию и санкционированию реализации контрмер и внесения изменений в ИС должны основываться на результатах эффективной программы управления рисками.

Руководители производственных отделов и отдела закупок. От них зависит экономическая эффективность процесса управления рисками, экономичность и эффективность расходования ресурсов.

Начальник отдела (управления) информационной безопасности. Он отвечает за все программы безопасности в организации, включая программу управления рисками. Он должен предложить и проводить в жизнь эффективную, структурированную методологию, помогающую идентифицировать, оценить и нейтрализовать риски, связанные с информационными технологиями. Он отчитывается перед высшим руководством организации за выполнение программы управления рисками.

Администраторы безопасности, системные и сетевые администраторы. Они отвечают за должную реализацию требований и регуляторов безопасности в подведомственных им информационных системах. При изменении систем и их окружения (появлении дополнительных сетевых соединений, изменении инфраструктуры, применении новых технологий и т.п.) они должны поддержать или применить процесс управления рисками, чтобы выявить и оценить новые потенциальные риски и реализовать необходимые контрмеры для поддержания информационной безопасности систем на требуемом уровне.

Специалисты по обучению персонала. Сотрудники организации являются пользователями ее информационной системы. Использование систем и данных в соответствии с политикой безопасности и правилами добропорядочного поведения критически важно для нейтрализации рисков и защиты ресурсов организации. Для минимизации рисков необходимо обеспечить информирование и обучение персонала по вопросам информационной безопасности. Следовательно, специалисты по обучению персонала должны понимать процесс управления рисками, чтобы разрабатывать соответствующие учебные материалы и проводить учебные курсы.

(Окончание в следующем номере)

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555