Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 8 (147)/2005

Эксплуатация защищенных информационных систем

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Эксплуатация защищенных информационных систем

Наталья Баталова,
консультант отдела продвижения и маркетинга
Борис Симис,
начальник отдела сопровождения систем безопасности

СОДЕРЖАНИЕ

Введение 3
Состояние и тенденции рынка сервисных услуг ИТ и безопасности 3
Ситуация в компаниях, где система защиты внедрена и работает 4
- Специфика эксплуатации защищенных ИТ-систем 5
- Эволюция ИТ-инфраструктуры и безопасность 5
- Кадры 6
- В результате 10

Как эксплуатировать? 11
- Общий состав работ на этапе эксплуатации 11
- Кому поручить? 11
- Что нужно знать при выборе сервисных услуг 12

Виды сервисных услуг для защищенных ИТ-систем 13
Техническая поддержка средств и систем защиты 14
Анализ и контроль защищенности ресурсов 15
Аутсорсинг в области безопасности 17
- Потребность в услугах внешних сервисных компаний 17
- Барьеры и страхи 18
- Аутсорсинг: виды и уровни услуг 19
- Подготовительные мероприятия по передаче функций ИБ на аутсорсинг 20
- Выгоды аутсорсинга 20

Центр компетенции по вопросам информационной безопасности 21
Поставщики сервисных услуг 22
- Выбор сервисной компании 22
- Регламентация отношений с сервисной компанией 23

Средства и услуги в области защиты информации, предлагаемые компанией «Инфосистемы Джет» 24

Введение

Многолетняя история компании «Инфосистемы Джет» как системного интегратора и интегратора в области безопасности не просто отражает ситуацию на российском рынке, но, как показывает анализ продаж ИТ-продуктов и услуг, позволяет прогнозировать проявление и развитие тех или иных тенденций. Мы стараемся соответствовать ситуации, которая складывается на российских предприятиях, в том числе у наших заказчиков, эксплуатирующих и развивающих свои информационные системы.

Данная статья представляет собой обзор основных тенденций на отечественном и мировом рынках услуг в области информационных технологий и информационной безопасностии и содержит анализ современных потребностей компаний-заказчиков ИТ-продуктов и услуг. Статья адресована главным образом руководителям и специалистам тех компаний, в которых уже установлены и работают средства и системы информационной безопасности и защиты ресурсов. Цель авторов — помочь этим компаниям раскрыть нюансы, связанные с эксплуатацией защищенных информационных систем, и существующие в этой области проблемы, а также правильно сориентироваться на рынке сервисных услуг в области информационной безопасности.

Состояние и тенденции рынка сервисных услуг ИТ и безопасности

Согласно проводимым в России и в мире исследованиям, положение на рынке информационной безопасности сегодня схоже с ситуацией на рынке информационных технологий 4—5 лет назад. Это объясняется тем, что, во-первых, рынок продуктов и услуг в области безопасности является частью общего ИТ-рынка, а во-вторых, некоторое «отставание» образовалось из-за того, что большинство компаний сначала занимаются автоматизацией своей деятельности, а уж затем — защитой ресурсов.

Основная тенденция в области информационных технологий, наблюдающаяся последние несколько лет, связана с тем, что все больше компаний завершают процесс построения информационных систем и переходят к этапу их эксплуатации. Это означает быстрый рост потребностей в сервисных услугах — технической поддержке и обслуживании ИТ-компонентов. Эти потребности далеко не всегда могут быть удовлетворены полностью и на достаточно профессиональном уровне.

Рынку информационной безопасности в ближайшие несколько лет будут свойственны те же тенденции, которые наблюдались в сфере ИТ: происходит постепенное смещение от поставок средств и систем защиты информации в сторону сервисных услуг. Все больше заказчиков проходят этап разработки и внедрения средств и систем защиты, и у них возникает необходимость в технической поддержке и обслуживании внедренных решений.

В чем именно заключается это обслуживание, кто должен его оказывать в том или ином случае, будет рассказано далее. Прежде проанализируем, в каких условиях происходит эксплуатация защищенных информационных систем.

С одной стороны, компании все активнее оснащают ИТ-системы средствами защиты. Рост объема продаж этих средств в мире составляет в каждом классе не менее 10%: рынок виртуальных частных сетей (VPN) и межсетевых экранов вырос на 13%, а продажи сравнительно новых средств защиты (например, систем контекстного анализа) растут еще быстрее.

В России рынок средств и систем защиты развивается очень динамично: в последние два года он растет примерно на 50% ежегодно (по оценке РБК: 2003 г. — более $50 млн, 2004 г. — около $100 млн, 2005 г. — около $140 млн). Казалось бы, информационные ресурсы становятся все более защищенными по мере оснащения ИТ-систем соответствующими средствами. Но при этом в течение 2003 г. около 40% компаний понесли различные виды ущерба в связи с проблемами в системе защиты, а в 2004 г. таких компаний стало уже более 80%! Число успешных попыток несанкционированного доступа и атак неуклонно растет. Например, количество случаев кражи или утечки конфиденциальных данных за последний год увеличилось более чем вдвое.

Ущерб от этих и других инцидентов безопасности становится все ощутимее: по наблюде-

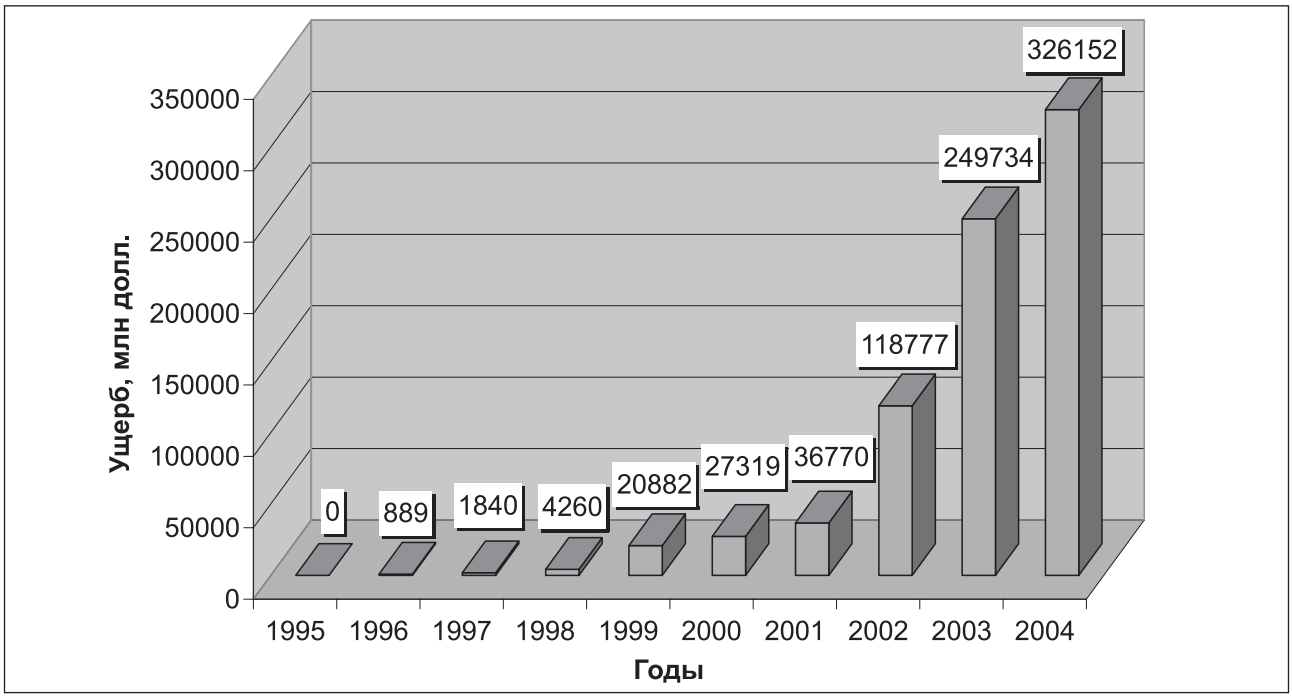

Рис. 1. Совокупный мировой ущерб от компьютерных атак. Источник: mi2g, 2004 г.

ниям компании mi2g, предоставленным CNews, начиная с 1995 г. ежегодный рост экономического ущерба никогда не был ниже 30%, а зачастую превышал 100%.

Среди компаний, которые НЕ пострадали от проблем с безопасностью, достаточно защищенными и готовыми к отражению атак оказалось чуть больше трети (38%). И это происходит в тот период, когда рынок средств и систем защиты растет уверенными темпами год от года, все больше компаний внедряют системы защиты, которые, в свою очередь, становятся все более совершенными и комплексными.

О чем это говорит? Во-первых, о некоторых особенностях, присущих именно сфере информационной безопасности (в ИТ, например, увеличение инвестиций в автоматизацию обычно гарантирует снижение затрат на ведение бизнеса, а в области безопасности это возможно только при выполнении определенных условий). Во-вторых, закупка и инсталляция средств защиты не решает полностью проблему безопасности ресурсов компании. Необходимо не просто «выставить заслон» от возможных посягательств на ресурсы (пусть даже хорошо спроектированный и грамотно установленный), а постоянно прилагать усилия для того, чтобы он сохранял надежность и с течением времени.

Конечно, положение на рынке в целом и выводы, к которым приводит анализ статистических данных, могут не очень волновать конкретную компанию, поскольку у нее есть собственные проблемы и особенности. Поэтому обратимся к ситуации в организациях, эксплуатирующих защищенные информационные системы, чтобы понять, в чем именно состоит специфика обеспечения безопасности ресурсов, и что должна делать компания, чтобы ее система защиты действительно работала.

Ситуация в компаниях, где система защиты внедрена и работает

Сегодня уже всем ясно, насколько важна защита информационных ресурсов. Многие также понимают, что система информационной безопасности — это не просто защита от прямых материальных потерь, но и конкурентные преимущества, репутация на рынке и более высокая степень доверия со стороны клиентов и партнеров. Поэтому на данный момент финансовые вложения в защиту своих ресурсов в том или

ином объеме сделаны практически во всех компаниях: отдельные средства или комплексные системы безопасности установлены в каждой ИТ-системе.

Основная задача на этапе эксплуатации системы — это поддержание достигнутого уровня безопасности. Данное требование является таким же жестким, как и требование обеспечения отказоустойчивости ИТ-компонентов и непрерывности работы ИС в целом. Эксплуатация информационных систем, оснащенных современными средствами защиты — довольно сложная и специфичная задача.

Специфика эксплуатации защищенных ИТ-систем

Основная особенность эксплуатации средств и систем безопасности (в отличие от других ИТ-компонентов) заключается в том, что информационная система, которая сегодня надежно защищена, завтра может оказаться уязвимой, причем владелец не обязательно будет знать об этом.

Серверный комплекс может надежно работать несколько лет, не требуя внесения изменений в его конфигурацию. При этом его неработоспособность (например, поломка процессора) станет очевидной сразу. В то же время система защиты, не учитывающая появление новых угроз безопасности или неправильно эксплуатируемая, через несколько месяцев утрачивает адекватность и становится уязвимой. Причем владелец заметит это лишь тогда, когда наступят последствия хакерской атаки, проникновения вируса, халатных действий пользователей и других инцидентов безопасности. Тому есть несколько объективных причин глобального характера.

Во-первых, сложность информационных систем возрастает, и это неизменно вызывает рост числа уязвимостей в ИТ-компонентах и средствах защиты. Эти уязвимости активно используются злоумышленниками для проведения различных видов атак, организации сбоев в работе критических приложений, сетей передачи данных и в предоставлении сервисов, а также в кражах конфиденциальных данных и в других подобных действиях.

Во-вторых, появляются новые угрозы безопасности, вирусы, способы атак. Методы и инструменты проведения атак постоянно совершенствуются, скорость их распространения стремительно растет (корпоративную систему можно вывести из строя за несколько секунд), а последствия иногда оказываются катастрофическими для бизнеса.

Есть также ряд особенностей, которые могут быть в той или иной степени присущи конкретной компании и конкретной информационной системе. Например, в больших и сложных информационных системах набор применяемых решений по защите бывает достаточно широк. Используются средства защиты разных производителей, взаимосвязи между этими средствами в рамках комплексной системы безопасности довольно сложны. Кроме того, механизмы работы современных средств защиты становятся все сложнее, применяются все более тонкие методы обнаружения атак, фильтрации трафика и реализации других защитных функций (например, контекстный анализ).

Таким образом, для реального контроля безопасности ресурсов нужна целостная картина работы множества сложных взаимосвязанных средств — задача непростая как с точки зрения техники, так и для персонала, ответственного за эксплуатацию такой системы.

Еще одна проблема, особенно актуальная для обслуживания и поддержки комплексных систем безопасности, — производители постоянно выпускают новые версии продуктов, содержащие улучшения, изменения, вводящие новый функционал и программные коррекции, исправляющие ошибки. И нужно постоянно проводить мониторинг выпуска этих изменений и устанавливать их в своей системе. Не секрет, что многие уязвимости, которые использовались для осуществления атак на корпоративные системы, на момент атаки были уже обнаружены и известны производителям средств защиты или атакуемых ИТ-компонентов. Эти уязвимости можно было устранить за несколько недель или месяцев до атаки, просто установив соответствующую заплатку (патч).

Чтобы уследить за всеми нововведениями, необходимо постоянно их отслеживать и проводить мониторинг такого рода событий. Если же этим не заниматься, то система безопасности довольно быстро перестанет выполнять свои задачи.

Эволюция ИТ-инфраструктуры и безопасность

Определенные особенности характерны и для эксплуатации защищенных ИТ-систем, в состав и структуру которых вносятся изменения. Как показывает опыт, информационная система, обеспечивающая работу достаточно большой

организации, практически никогда не бывает статичной. Расширение, добавление новых компонентов и прочие изменения — естественный и непрекращающийся процесс, поскольку ИТ-системы работают в тесной связи с основными процессами деятельности, которые меняются. Появляются новые информационные сервисы, активно внедряются новые информационные технологии, на определенном этапе возникает необходимость оптимизировать систему. Как следствие, решения по обеспечению информационной безопасности корпоративных ресурсов, принятые в процессе проектирования, быстро утрачивают соответствие той системе, ресурсы которой они призваны защищать.

Например, рост объема информации, добавление новых сегментов, увеличение количества рабочих мест снижают эффективность механизмов и процедур защиты, и для сохранения требуемого уровня защищенности ресурсов требуется масштабирование и самой системы обеспечения безопасности.

Расширение возможностей ИТ-системы — добавление новых информационных сервисов и внедрение новых технологий (например, Wi-Fi) — приводит к появлению дополнительных рисков и уязвимостей в защите. Чтобы эти риски нейтрализовать, необходимо незамедлительно учесть все специфичные для новой технологии аспекты защиты информации. Поэтому в изменяющихся информационных системах важно не просто внедрить адекватные механизмы защиты, но и поддерживать заданный уровень безопасности в процессе эксплуатации. А для этого необходимо не только поддерживать работоспособность средств защиты, но и проводить разовые или периодические работы по контролю уровня защищенности ресурсов (см. раздел «Анализ и контроль защищенности ресурсов»), что позволяет гарантировать этот уровень даже в условиях внесения изменений в информационную систему.

Кадры

Современные угрозы безопасности в принципе преодолимы, уязвимости — устранимы, и в целом задача обеспечения защиты ресурсов выполнима даже в тех сложных условиях, описанных выше, нужно только грамотно эксплуатировать и поддерживать систему безопасности. Это подразумевает проведение целого комплекса непрерывных и периодических работ, таких как техническая поддержка средств защиты, мониторинг и анализ событий безопасности, происходящих в системе, периодический контроль защищенности ресурсов, преодоление нештатных ситуаций и ликвидация последствий.

Для выполнения названных работ, во-первых, требуется соответствующее техническое и программное обеспечение, а во-вторых, нужен персонал необходимой численности, квалификации и имеющий достаточный опыт. Современные технологии безопасности действительно довольно эффективны и хороши, но они все равно не заменят человека, его мышление и опыт, особенно в преодолении критических проблем в системе защиты корпоративных ресурсов.

Многие фирмы и предприятия, в основном крупные, имеют собственные отделы, службы или даже целые управления по обеспечению информационной безопасности. На сегодня в большинстве крупных компаний есть назначенные руководители служб безопасности, несущие ответственность за защиту корпоративных ресурсов. Некоторые организации практически не привлекают внешние специализированные компании на этапе эксплуатации систем защиты, поскольку считают, что расходы на содержание собственного штата специалистов меньше, чем существующие риски для защищаемых ИТ-систем. Иногда это может соответствовать действительности, но только при выполнении целого ряда условий.

Интересный факт: половина компаний, пострадавших в 2004 г. из-за проблем в системе защиты своих ресурсов (а таких в мире по разным оценкам насчитывается до 80%!), полагали, что достаточно хорошо оснащены средствами защиты и имеют квалифицированный во всех необходимых областях персонал. Однако заметим, что в компаниях, которые в течение последнего года не пострадали (или не понесли ощутимого ущерба) от брешей в системе защиты, количество сотрудников, занимающихся данной задачей, составляет примерно 10% штата ИТ-специалистов, и это достаточно хорошее соотношение. Но таких компаний, к сожалению, меньшинство (в среднем, в мире не более четверти). Компьютерный парк быстро увеличивается, внедряются современные сложные средства автоматизации — системы управления производством, системы управления базами данных, системы документооборота, электронной коммерции и т.д., системы информационной безопасности, наконец. Но при этом штат обслуживающих подразделений увеличивается далеко не пропорционально сложности и объему подлежащих решению задач.

На практике эффективное решение задач эксплуатации и обслуживания систем безопасности силами собственного подразделения означает постоянное присутствие на предприятии персонала в необходимом количестве.

Кроме того, специалисты, занимающиеся поддержкой и обслуживанием систем безопасности, должны иметь высокую квалификацию в области информационной безопасности и смежных областях информационных технологий, поскольку набор используемых в большинстве компаний средств защиты довольно широк, а механизмы их работы усложняются год от года. Уровень подготовки персонала, ответственного за корректную и (главное!) эффективную работу систем защиты, всегда должен соответствовать таким условиям работы. То есть необходимо обеспечить сотрудникам возможность проходить специализированное обучение по всему набору средств и систем защиты. В больших и сложных информационных системах выполнение этого условия также требует серьезных затрат.

Существенное значение имеет опыт работы специалистов, особенно в части преодоления нештатных ситуаций. Чем чаще они сталкиваются с нештатными ситуациями, тем более адекватны и точны будут их действия по локализации и устранению сбоев и решению других возможных проблем, тем меньше вероятность для компании понести ущерб. Такой персонал, естественно, требует соответствующего уровня оплаты труда, что для многих предприятий является непростым условием.

Обслуживание комплексных систем безопасности невозможно и без должной степени автоматизации администраторских и других эксплуатационных функций. Это означает наличие соответствующего технического и программного обеспечения для администраторов безопасности и их руководителей (начальников отделов и служб): сканеров, средств мониторинга и управления безопасностью, корреляции событий, анализа защищенности ИТ-компонентов, средств получения статистики и генерации отчетов — еще одна затратная статья.

Тем не менее, даже при выполнении всех перечисленных условий сотрудники, ответственные за защиту корпоративных ресурсов, сталкиваются с множеством проблем.

Типичные проблемы для администраторов безопасности

Самая очевидная и часто встречающаяся проблема для администраторов — постоянный поток множества (тысяч или десятков тысяч) сообщений от обслуживаемых ими средств защиты и смежных ИТ-компонентов: сетевых устройств, имеющих встроенные функции защиты, межсетевых экранов, систем контроля содержимого, обнаружения атак и других. Все эти сообщения так или иначе связаны с проблемами безопасности, хотя подавляющее большинство, строго говоря, не являются критичными и не свидетельствуют о реальных атаках и других критичных событиях. Однако среди них есть малая часть событий, которые в самом деле могут нанести ущерб ресурсам защищаемой сети и требуют немедленной реакции. Администратору в таких условиях работы необходимо решать две задачи: правильно трактовать события, выделяя только те, которые действительно требуют внимания, и правильно и быстро реагировать на действительно критичные сообщения.

Очевидно, что даже при использовании средств автоматизации администраторских функций (анализа и корреляции событий от множества средств защиты) обслуживающему персоналу сложно ориентироваться в таком потоке событий, поэтому существует реальный риск отреагировать на пустое или ложное сообщение и пропустить другое, критичное и влекущее за собой тяжелые последствия.

Помимо этой проблемы, персонал службы безопасности сталкивается еще с одной: для повышения уровня понимания событий, происходящих в системе, необходимо углубляться в ИТ-специфику, однако тогда у этих сотрудников не остается времени и возможностей на анализ и другие работы, имеющие специфику именно безопасности.

Есть и другой вариант — передать ИТ-службам все вопросы, касающиеся функционирования ИТ-компонентов средств защиты. Например, система обнаружения атак сообщает о попытке взлома сервера СУБД Oracle по протоколу SQL*Net. Чтобы понять серьезность этой атаки, администратору безопасности нужно разбираться в тонкостях работы сервера Oracle на уровне администратора СУБД. И таких событий из области сетевых технологий и сетевого оборудования, веб- и других приложений, доменов Windows и Novell и других областей могут быть сотни.

Получается, что служба безопасности должна либо иметь специалистов, разбирающихся во всех областях информационных технологий, способных объективно интерпретировать события (например, аудита), либо переложить эту функцию на ИТ-службу, у которой много и своих забот.

Типичные проблемы для начальников отделов и служб безопасности

Основная задача руководителей отделов и служб безопасности — обеспечение стабильного уровня защиты информационных ресурсов компании при любых условиях. Подавляющее большинство (86% в мире) руководителей таких отделов и служб отвечают за безопасность компании и отчитываются непосредственно перед высшим руководством.

Очевидно, что начальнику службы безопасности нужны эффективные средства получения информации об уровне защищенности системы в целом на настоящий момент, а также средства контроля этого уровня в динамике. В большинстве случаев бывает трудно получить такую информацию от собственных сотрудников — нужны, как минимум, специальные технические средства анализа защищенности ресурсов и методики оценки уровня защищенности, а также время. Кроме того, полученная информация не будет объективной при проведении оценки собственными сотрудниками, а не внешними компаниями-экспертами.

Поскольку ответственность за сохранение состояния защищенности информационных ресурсов компании полностью лежит на руководстве службы безопасности, именно оно должно организовать и обеспечить выполнение работ по поддержанию корпоративной системы безопасности в состоянии, соответствующем современным условиям. К таким работам относятся мониторинг новых угроз безопасности и видов атак, появляющихся достаточно часто, отслеживание узявимостей в используемом программном и аппаратном обеспечении (не только системы защиты, но и всей информационной системы). Результатом этих работ должно быть своевременное внесение соответствующих изменений в настройки средств и систем защиты и ИТ-компонентов или дополнение/модернизация системы защиты в соответствии с новыми условиями ее эксплуатации, а также изменение проектной и эксплуатационной документации на систему. Данная задача сама по себе является сложной и трудоемкой, иногда — неподъемной для существующей службы безопасности. Но в любом случае руководитель этой службы должен организовать выполнение необходимых работ (возможно, с привлечением внешней специализированной компании) и, как результат, получить четкую картину безопасности.

Еще одна сложная проблема для ответственных за безопасность лиц — поддержка уровня защищенности ресурсов информационных систем, подвергающаяся изменениям (см. главу «Эволюция ИТ-инфраструктуры и безопасность»). Те или иные изменения вносятся в структуру и состав практически каждой защищаемой ИТ-системы, и если в одних случаях они не очень существенны с точки зрения безопасности и практически не требуют изменений в систему защиты, то в других могут потребовать ее полной модернизации.

Во многих компаниях, особенно крупных и динамично развивающихся (например, у операторов сотовой связи), руководителям служб безопасности каждую неделю (если не чаще) попадают на стол проекты по развитию и модернизации ИТ-инфраструктуры, направленные на развитие бизнеса, — освоение новых рынков, предоставление новых услуг и т.д. И все эти проекты, содержащие предложения по добавлению новых сегментов, подключению новых офисов и филиалов, внедрению новых, более современных технологий, приложений и т.д., — требуют экспертизы с точки зрения информационной безопасности, во всех проектах должны быть соответствующие требования, которые впоследствии будут выражены в адекватном изменении корпоративной системы защиты.

Повторим, что экспертиза ИТ-проектов с точки зрения безопасности является трудоемкой и требует высокой квалификации специалистов, и задача внедрения необходимых изменений также требует материальных и человеческих ресурсов.

Проблемы для руководства компании

Результатом усилий руководителей отделов и служб безопасности должна быть работающая информационная система, ресурсы которой надежно защищены в соответствии с существующими на данный момент условиями. Это, конечно, подразумевает определенное финансирование работ. Как известно, бюджет на информационную безопасность должен составлять 10% от ИТ-бюджета. Почти в половине компаний в мире он составляет около 3%, у трети фирм — в пределах 4—6%, и только десятая часть компаний выделяет примерно 10% стоимости ИТ-системы на защиту ее ресурсов.

Для того чтобы выделять (или не выделять) средства на закупку тех или иных программно-технических средств и проведение определенных мероприятий по защите, руководство компании должно понимать, каким образом это отразится на уровне безопасности ИТ-системы и бизнеса компании в целом. Насколько корпоративные ресурсы защищены (или уязвимы) в

данный момент и как эта ситуация меняется во времени? В чем реальная причина существующих проблем в защите (недостаточность используемых средств и систем безопасности, халатность персонала, невозможность заставить службу ИТ внести необходимые корректировки в настройки, потому что для них задача безопасности стоит на последнем месте и т.д.)?

Сегодня примерно треть компаний вообще не выполняют такого рода анализ и не проводят контроль уровня защищенности своих ресурсов. Часто необходимые средства на информационную безопасность не выделяются, а работы не проводятся до тех пор, пока «гром не грянет» (такие ситуации бывают на руку компаниям, специализирующимся в этой области), и только в одной трети фирм в мире должный контроль проводится на регулярной основе.

Статистика также показывает, что отчеты руководству о состоянии информационной безопасности компании, существующих рисках и инцидентах предоставляются недостаточно качественно, полно и часто. Чуть более трети компаний составляют отчеты о состоянии безопасности ежеквартально или даже раз в полгода, еще треть не делают этого вовсе или, в лучшем случае, готовят некие специальные отчеты по особым случаям. Руководству компании (в отличие от администраторов безопасности и руководителей соответствующих отделов и служб) нужен короткий и внятный отчет-обоснование, для чего ему вкладывать средства в безопасность ресурсов, или отчет-оценка эффективности инвестиций в защиту корпоративных ресурсов.

Зачастую (даже при наличии соответствующих средств получения статистики и генерации отчетов о состоянии безопасности ресурсов) сотрудникам и руководителям отделов и служб безопасности сложно собрать подробные технические отчеты и преобразовать их в аргументированное обоснование затрат. Здесь есть и технические сложности, и проблемы выбора действительно необходимых мер и средств защиты, адекватных по стоимости и другим критериям. Отчасти по этой причине руководство может не осознавать уязвимости своего бизнеса и его зависимости от надежной и безопасной работы информационной системы.

Проблемы взаимодействия подразделений

Очевидно, что обеспечение и контроль защищенности ресурсов информационной системы — общая задача руководителей служб ИТ и безопасности. В некоторых ситуациях сотрудникам службы безопасности нужно контролировать работу службы ИТ. Это, например, уже упоминавшиеся задачи развития ИТ-инфраструктуры, которые требуют не только соответствующих средств и мер защиты, но часто и внесения изменений собственно в ИТ-проекты (настройки ИТ-компонентов, схемы их подключения и т.д.), если такие изменения продиктованы соображениями безопасности. Существуют также и повседневные, более «мелкие» задачи, требующие согласованного взаимодействия нескольких служб (ИТ-подразделения, службы информационной безопасности, службы охраны, HR-подразделения и т.д.). Например, прием на работу нового сотрудника, выделение ему рабочего места, предоставление полномочий доступа и т.д.

По нашему наблюдению, взаимодействие служб ИТ и безопасности не всегда достаточно эффективно для решения поставленных задач. Надо отметить нечетко очерченное разделение сфер ответственности и обязанностей между всеми участниками процесса обеспечения информационной безопасности, существует «конфликт интересов» между этими службами (в службе ИТ задачи информационной безопасности часто имеют низкий приоритет). В комплексе с вышеназванными кадровыми и другими проблемами все это вызывает сложности с реальным контролем защищенности эксплуатируемой системы, с адекватным реагированием на нештатные ситуации и т.д.

Пользователи

Эту категорию сотрудников полезно рассмотреть, поскольку именно они занимаются эксплуатацией защищенных рабочих мест и используют защищенные информационные и иные ресурсы компании. В связи с этим дисциплина и грамотность пользователей имеет большое значение для обеспечения информационной безопасности предприятия. В то же время пользователи на предприятиях часто считают, что защита информации не входит в их обязанности и является навязанной функцией. Последнее время в условиях быстрого роста автоматизации деятельности предприятий средний уровень знаний, навыков и профессионализма пользователей часто отстает. А это означает, что небрежность действий сотрудника может иметь весьма серьезные последствия — от нарушения работы его собственной рабочей станции до блокирования критичных для компании подсистем и сервисов (например, систем электронной почты или веб-сервисов). Тем самым все усилия предприятия по построению корпоративной системы защиты будут сведены на нет.

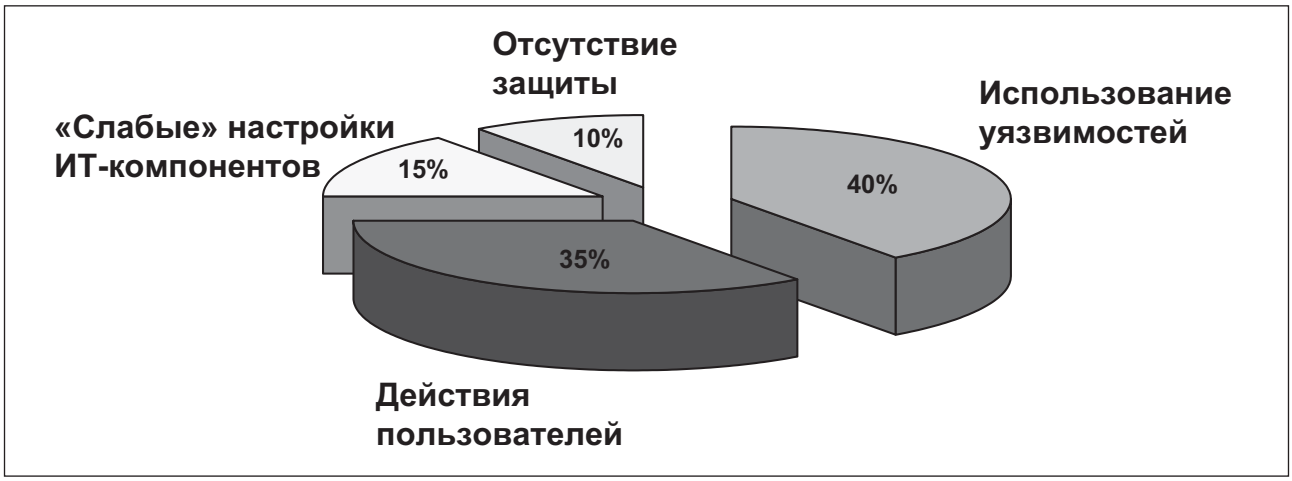

Рис. 2. Причины нарушений в работе защищенных ИС, март 2005 г.

Предоставление или ограничение прав доступа — еще одна проблема на многих предприятиях: пользователи обращаются к администраторам с просьбой предоставить доступ к ресурсам (внутренним или внешним), которые им на самом деле не нужны (по крайней мере, в рабочее время), или предоставить им расширенные (административные) права в какой-либо системе (своей рабочей станции), чтобы иметь возможность самостоятельно устанавливать и настраивать «нужное» им программное обеспечение. Администратор может отказать, если имеет соответствующие инструкции, но бывают ситуации, когда довольно высокая должность сотрудника, обратившегося с просьбой о расширении своих прав, или дружба с ним не позволяют этого сделать. В случае недостаточной квалификации и дисциплины такого сотрудника негативные последствия могут быть весьма ощутимыми.

Масштаб бедствия окажется еще больше, если внутренний сотрудник будет преднамеренно выполнять определенные действия против собственной компании, поскольку законный пользователь имеет для этого массу возможностей и способов, в том числе простых для использования и не требующих от него особой квалификации или знаний.

Статистика показывает, что в 2004 г. основные источники проблем с безопасностью (а отмечены они у 80% компаний) были внешние, а в течение первого полугодия 2005 г. у большинства фирм, пострадавших от брешей в системах защиты (всего за шесть месяцев пострадали уже около 30% компаний), источники были именно внутри компании. По некоторым оценкам, сегодня на долю внутренних сотрудников приходится свыше 70% всех нарушений в системах безопасности. Доля финансовых потерь от внутренних источников также продолжает стремительно увеличиваться с каждым годом.

Как видно из диаграммы (Рис. 2), треть всех проблем в защите составляют неумышленные (халатные) действия. Среди остальных инцидентов, связанных с использованием существующих уязвимостей в компонентах информационных систем и «слабых» настроек ИТ-компонентов, есть атаки, совершаемые внутренними злоумышленниками (именно такие атаки наиболее опасны). Это подтверждает, что сейчас защита информационных ресурсов и технологий от недобросовестного или просто халатного легального пользователя стала очень важной, причем по сравнению с уже известными и хорошо освоенными областями информационной безопасности, она требует особого подхода и применения специальных программно-технических средств. Решение этой задачи обязательно должно быть включено в комплекс работ, проводимых на предприятии в процессе эксплуатации защищенных информационных систем.

В результате…

Как видно из вышеизложенного, главное для предприятий, эксплуатирующих защищенные информационные системы, — владение информацией о реальном уровне безопасности (или уязвимости) корпоративных ресурсов и контроль над ним. Это означает, кроме прочего, и возможность эффективно воздействовать на этот уровень, то есть выявлять и пресекать нарушения, контролировать действия персонала (как пользователей, так и администраторов), избегать негативных последствий для бизнеса. В конечном счете, все это является серьезным

обоснованием инвестиций в корпоративную безопасность.

Однако в реальности далеко не все компании, вложившие средства в создание систем информационной безопасности, уверены, что на этапе эксплуатации их ресурсы защищены от всех существующих сегодня угроз и атак. По-прежнему не у всех руководителей есть ясная и объективная картина защищенности ресурсов и уверенность в оправданности инвестиций в корпоративную безопасность. Ведь пока в большинстве случаев становится известно только о последствиях уже произошедших нарушений, да и то лишь «ярко выраженных». Как добиться, чтобы информация о нарушениях в защите ИТ-систем, причинах этих нарушений или виновных сотрудниках была получена вовремя и в оптимальном объеме?

Как эксплуатировать?

Общий состав работ на этапе экслуатации

Эксплуатация средств и системы защиты информации должна включать целый комплекс работ, обеспечивающих необходимый уровень защищенности информационной системы. К ним относятся:

- грамотная эксплуатация системы — поддержка средств защиты в состоянии, наиболее точно соответствующем предъявляемым к системе требованиям, своевременная модификация системы и тестирование новых компонентов;
- мониторинг в режиме реального времени и анализ происходящих в системе событий, относящихся к безопасности, реагирование на критичные события;
- контроль безопасности системы — тестирование защищенности, выявление потенциальных проблем, проверка выполнения регламентов;
- преодоление нештатных ситуаций — локализация технических проблем и предотвращение/ликвидация последствий;
- мониторинг событий в области информационной безопасности на предмет появления новых уязвимостей, угроз и новых видов атак, внесение необходимых изменений в систему защиты.

Эти работы позволяют поддерживать защищаемую ИС в состоянии, соответствующем современным тенденциям и новым технологиям информационной безопасности, отслеживать выполнение корпоративной политики безопасности, предотвращать попытки вторжений в систему и других несанкционированных действий, оперативно и адекватно реагировать на нарушения в защите и другие события, существенные с точки зрения безопасности.

Кому поручить?

Существует несколько вариантов, и каждый из них имеет свои плюсы и минусы в условиях конкретной компании.

Выполнение всего комплекса работ силами собственного подразделения по информационной безопасности — задача, выполнимая далеко не для всех. Основные проблемы — нехватка и недостаточная квалификация персонала, отсутствие необходимого инструментария и методик ведения работы (например, при внештатных ситуациях), испытательных стендов и т.д. Это естественно, поскольку для большинства компаний сервис в области информационных технологий, а тем более в области безопасности, не является основным видом деятельности.

Еще одна важная проблема такого подхода — отсутствие объективной информации о своей информационной системе и происходящих в ней событиях. Независимая экспертная оценка необходима для обоснованного планирования и финансирования работ по защите или, например, при разборе сложных инцидентов в области безопасности, когда решение этой задачи собственными силами усложняется тем, что источник нарушения в защите может находиться внутри компании.

Для многих организаций оптимальным решением является делегирование части функций эксплуатации корпоративной системы, относящихся к обеспечению ее защиты, внешнему исполнителю, специализирующемуся в области информационной безопасности. Преимущества такого решения очевидны. Специализированная фирма, как правило, располагает опытным персоналом высокой квалификации, тестовыми стендами и инструментарием для проведения

работ, имеет регламенты и методики действий в экстренных ситуациях и т.д. Техническая проблема, возникшая в вашей компании, в практике специализированной сервисной фирмы наверняка уже встречалась, значит, и способ решения ей известен. Поэтому и качество работ, естественно, будет выше.

Многие компании хотели бы иметь надежную защиту своих ресурсов, которая будет работать, вообще не отвлекаясь от основного бизнеса. Руководство таких компаний предпочитает полностью поручить поддержку и контроль безопасности корпоративных ресурсов внешнему исполнителю — аутсорсеру, поскольку это бывает выгоднее, чем вкладывать деньги в развитие собственной службы безопасности. Аутсорсинг в области информационных технологий широко распространен в мире и все более активно применяется в России. Аутсорсинг в области безопасности пока не так часто встречается (как мы уже говорили, рынок информационной безопасности отстает от ИТ-рынка), но имеет хорошие перспективы. (Об этом виде услуг см. раздел «Аутсорсинг в области безопасности»).

При всех плюсах привлечения внешних исполнителей в процессе эксплуатации защищенных систем следует отметить риски, связанные с допуском внешней организации в корпоративную систему, — разглашение конфиденциальной информации, ответственность за возможные инциденты в области безопасности и другие. Поэтому при выборе внешнего исполнителя необходимо учесть имеющийся у него опыт оказания услуг в различных областях ИТ и информационной безопасности, наличие сертифицированных сервисных инженеров. Также надо обратить внимание на обеспечение юридических и технических аспектов конфиденциальности (временные пользователи и методы доступа, регистрация действий внешних сотрудников, строгая аутентификация и др.).

Соблюдение этих условий и привлечение специализированной фирмы позволяет оптимизировать расходы на поддержание безопасности информационной системы, достигнуть наиболее высокого уровня и качества поддержки и при этом сосредоточиться на основной деятельности компании.

Специализированные фирмы, в свою очередь, предлагают различные виды сервиса в области безопасности, отличающиеся набором предоставляемых услуг (от минимальной «горячей линии» до аварийных выездов в круглосуточном режиме), временными параметрами обслуживания, степенью оперативности, степенью «привязки» выполняемых работ к условиям конкретного заказчика и другими характеристиками.

Что нужно знать при выборе сервисных услуг?

Разные компании имеют существенные различия по масштабу и степени автоматизации, уровню требований к безопасности, применяемым методам защиты ресурсов и стадиям их внедрения, финансовым и человеческим возможностям и т.д. Поэтому для них востребованы и различные виды сервиса. Чтобы определить состав и параметры сервисных услуг, необходимо выяснить следующее:

1. Существует ли в компании собственная служба ИТ/безопасности (или другое подразделение, ответственное за ИБ)?
2. Обеспечена ли система защиты сервисной поддержкой? Кто ее осуществляет (производитель, собственная служба ИТ или безопасности, поставщик, никто)?
3. Достаточно ли собственных сотрудников для обслуживания системы защиты, выявления проблем и разрешения нештатных ситуаций?
4. Существуют ли в компании повышенные требования к обеспечению безопасности и надежности/отказоустойчивости работы информационной системы?
5. Происходят ли нарушения безопасности и другие события, приводящие к нежелательным последствиям? Какие именно? Как часто? Каковы последствия (ущерб)?
6. Как обслуживающий персонал узнает о нарушениях и других критических событиях безопасности? Организовано ли оповещение?
7. Удается ли начинать работы по устранению проблемных ситуаций раньше, чем наступили последствия?
8. Позволяют ли имеющиеся средства управления безопасностью выполнять автоматические/автоматизированные действия по реагированию? Используются ли эти возможности?
9. Проводится ли мониторинг безопасности ресурсов ИС? Каким образом проводится контроль и анализ событий безопасности?
10. Проводится ли оценка реального уровня защищенности ИС? Какими средствами, как часто, кем? Принимаются ли адекватные меры при обнаружении слабостей в защите?
11. Существует ли система статистики и отчетности? Доходит ли статистическая инфор-

мация до руководителей служб безопасности/ИТ? Используется ли эта информация для принятия решений по развитию/модернизации системы защиты?

Виды сервисных услуг для защищенных ИТ-систем

По вышеперечисленным характеристикам можно условно разделить компании на несколько групп, для которых востребованы соответствующие виды сервисных услуг.

Небольшим компаниям, в которых применяются средства защиты информации, необходима квалифицированная техническая поддержка этих средств. Данный вид сервиса позволит избежать проблем в процессе эксплуатации средств защиты и оперативно устранять возникающие технические неполадки.

Компаниям, в которых внедряются или уже внедрены системы защиты на базе нескольких продуктов (разных производителей), нужна техническая поддержка комплексных систем, которая помимо грамотной эксплуатации отдельных средств защиты позволит контролировать безопасность информационной системы в целом.

В компаниях различного масштаба, которые:

- хотят получить объективную информацию об уровне защищенности ресурсов на текущий момент;
- хотят контролировать уровень защищенности в течение определенного периода;
- нуждаются в оценке эффективности существующей защиты и планируют работы по ее развитию или модернизации

проводится разовый, периодический или непрерывный анализ защищенности ресурсов. Эта работа позволяет создать целостную и объективную картину, дающую представление об уровне безопасности информационной системы, полезную для планирования и финансирования работ по развитию системы защиты информации.

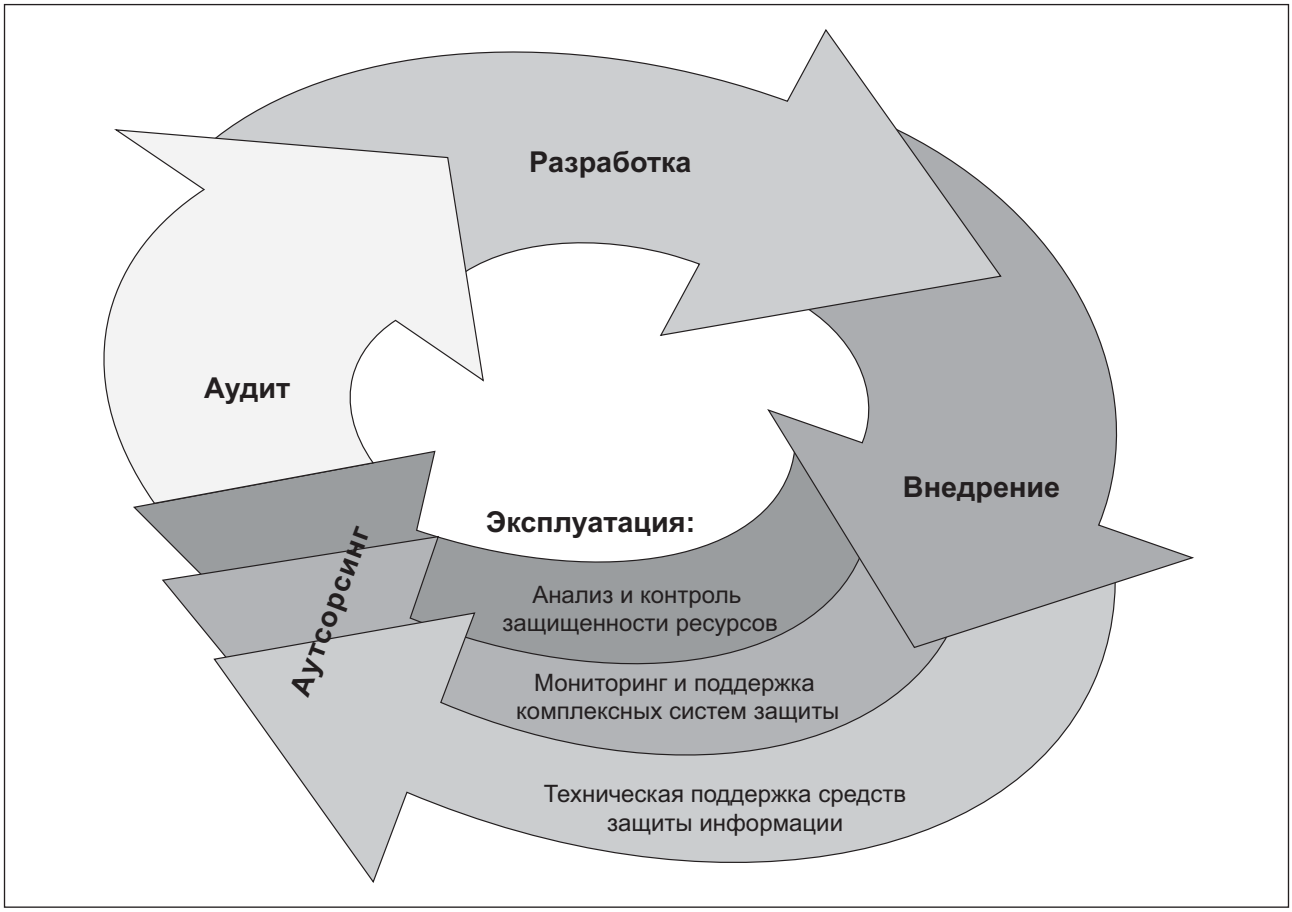

Рис. 3. Виды сервисных услуг на этапе эксплуатации систем информационной безопасности

Предприятиям, которые по различным причинам не стремятся развивать собственное эксплуатирующее подразделение по информационной безопасности, предлагается такая услуга как аутсорсинг.

Для компаний, нацеленных на выполнение большей части работ собственными силами, востребована услуга центров компетенции по вопросам информационной безопасности, которые могут давать квалифицированные консультации в этой области, ассистировать персоналу компании в выполнении особенно сложных задач, а также выступать экспертами в ситуациях, когда необходимо независимое мнение.

Техническая поддержка средств и систем защиты

Квалифицированная техническая поддержка является необходимым условием эффективной и надежной работы не только средств и систем защиты, но и всей информационной системы в целом. Некоторые услуги поддержки средств защиты оказывают сами производители: выпуск новых версий, программных коррекций (патчей), обновления используемых баз данных (антивирусных, сигнатур атак и других), а также предоставление доступа к веб- и другим ресурсам (технической документации, базе знаний и т.д.).

Эти услуги являются необходимыми, но для эффективного выполнения названными средствами своих функций необходимы также технические консультации и помощь по их обслуживанию, интеграции с другими средствами и системами, интерпретации сложных событий безопасности и т.д. Производители часто оказывают такие услуги недостаточно оперативно и качественно ввиду удаленности, разницы во времени и других причин. Получение прямых технических консультаций у производителя означает обращение в его сервисный центр по электронной почте или телефону (в случае зарубежных производителей это, как правило, звонок или электронный запрос в Европу или США на английском языке и получение ответа с поправкой на местное время производителя).

Если вопрос не критичный, то можно подождать. Но когда речь идет о сбое в работе средства защиты или о другой технической проблеме, требующей скорого решения, — сервисный центр производителя, находящийся далеко и не имеющий информации о специфике защищаемой системы, не сможет помочь достаточно оперативно (придется объяснять детали проблемы, посылать выдержки из журналов работы средства защиты и т.д.). Это связано с тем, что многие российские и зарубежные производители широко распространенных средств защиты ориентированы на предоставление сервиса клиентам не напрямую, а силами специализированных сервисных центров, обычно имеющихся в составе ведущих фирм-интеграторов. Российские представительства зарубежных производителей имеют, как правило, не более одного-двух инженеров, которые работают в основном со специалистами своих партнеров-интеграторов, помогая им в решении особо сложных технических проблем, требующих вмешательства производителя. А специализированный сервисный центр партнера — поставщика средств защиты может иметь количество инженеров, необходимое для технической поддержки всех компаний-клиентов.

Как правило, у поставщиков существует несколько уровней поддержки (Серебро, Золото, Платина или другие названия), которые отличаются набором услуг и степенью оперативности и подбираются индивидуально под требования конкретного заказчика. Услуги технической поддержки средств защиты могут включать:

- «горячую линию» — консультации по телефону и электронной почте в рабочие часы или круглосуточно;
- удаленную помощь в диагностике и устранении сбоев и других технических проблем в работе средств защиты;
- удаленное решение технических проблем специальными средствами мониторинга и управления;
- профилактические визиты для контроля функционирования средств защиты, проведения штатных модификаций, выявления потенциальных проблем;
- аварийные визиты для устранения неисправностей и ликвидации последствий нештатных ситуаций.

Такая поддержка позволит обеспечить надежную эксплуатацию средств защиты, повы-

сить эффективность их работы, значительно сократить время обнаружения, локализации и устранения технических проблем.

Услуги специализированных сервисных центров интеграторов имеют еще одно важное преимущество по сравнению с поддержкой производителей: если в компании эксплуатируется система информационной безопасности на базе продуктов разных фирм, можно приобрести поддержку всех этих средств у одного исполнителя. Тогда не придется обращаться по разным вопросам к нескольким производителям, которые будут оказывать поддержку каждого отдельного средства, а не системы в целом. Например, сообщения от разных средств защиты могут на самом деле свидетельствовать об одной и той же атаке, и для корректного решения такой проблемы необходимо знание специфики всей системы безопасности.

В организации, имеющей большое количество пользователей, офисов и каналов связи, применяется большое количество средств защиты разных производителей — межсетевые экраны, системы обнаружения атак, системы контекстного анализа трафика и другие. При этом требования к безопасности могут быть достаточно высокие (например, если это провайдер услуг или финансовая организация). Поскольку система информационной безопасности работает в комплексе, ее нужно обслуживать, учитывая особенности всех компонентов. Для этого придется обучить специалистов отдела информационной безопасности (а их даже в крупной компании бывает всего один или два!) работе со всеми средствами. Эти сотрудники должны обслуживать все используемые средства защиты, проводить мониторинг выхода патчей и своевременно их устанавливать, следить за изменениями в ИТ-системе и по мере необходимости донастраивать/менять конфигурацию системы защиты, а также быть готовыми решать срочные задачи (устранение сбоев в работе, последствий вирусных и других атак и т.д.). Оптимальный выход для такой компании — комплексная поддержка всей системы информационной безопасности силами специализированного сервисного центра. При этом операции по администрированию и управлению системой защиты могут оставаться в руках собственных немногочисленных сотрудников.

Для поддержки комплексных систем защиты, помимо грамотной эксплуатации отдельных компонентов, необходим непрерывный контроль безопасности системы в целом, сбор и анализ событий от разных средств защиты и адекватное реагирование на критичные события. Поэтому техническая поддержка комплексных систем защиты включает более широкий набор услуг, чем в случае поддержки отдельного средства:

- изучение и фиксация структуры, размещения, режимов функционирования и настроек средств защиты;
- централизованный контроль функционирования и техническая поддержка средств защиты информации, включая «горячую линию», удаленную помощь, профилактические и аварийные визиты;
- контроль происходящих событий безопасности, реагирование (при необходимости);
- время реагирования определяется степенью критичности возникающих проблем.

Специализированный сервисный центр, имеющий опыт работы с различными средствами защиты и являющийся партнером многих фирм-производителей, позволит повысить эффективность и надежность работы применяемых средств защиты.

Такая комплексная техническая поддержка обеспечивает безопасность ресурсов и надежную работу информационной системы, контроль над состоянием защиты и выполнением политики безопасности, снижает риски и ущерб от нарушений, сбоев и других критических событий.

Анализ и контроль защищенности ресурсов

Контроль уровня защищенности — очень важная часть программы информационной безопасности компании, поскольку позволяет определить степень защищенности или уязвимости ресурсов и оценить эффективность всей программы. В зависимости от конкретной цели, работы по анализу и контролю защищенности могут проводиться разово (один раз в год или полгода), периодически (раз в неделю или месяц) или непрерывно.

Разовый анализ дает объективную информацию об уровне безопасности (или уязвимости)

ресурсов информационной системы и ИТ-компонентов на текущий момент, существующих проблемах в системе защиты и их причинах. Эта информация дает возможность обоснованного планирования и финансирования работ по защите информационной системы, модернизации/развитию системы информационной безопасности, выявления и устранения брешей в защите, а также для оценки эффективности инвестиций в корпоративную безопасность.

Работы, проводимые в рамках такого анализа, должны включать:

- анализ характеристик информационной системы, существенных с точки зрения безопасности;
- анализ конфигурации ИТ-компонентов и применяемых механизмов и средств защиты;
- поиск и анализ уязвимостей компонентов ИС с помощью специализированных средств (сканеров защищенности);
- оценка защищенности ресурсов ИС;
- разработка (и реализация) рекомендаций по обеспечению требуемого уровня защищенности.

Результатом работы является подробный отчет, содержащий детальную информацию о выявленных проблемах в системе безопасности, а также предложения по устранению этих проблем (настройке существующих и применению дополнительных средств и мер защиты).

Непрерывный анализ защищенности позволяет контролировать уровень безопасности системы в течение определенного периода отслеживать нарушения безопасности, устранять их причины и минимизировать ущерб, а также поддерживать требуемый уровень безопасности в изменяющихся условиях.

Например, в крупной компании, имеющей большое количество пользователей, несколько офисов и несколько подключений к различным внешним сетям (в том числе Интернет), сложно уследить за изменениями ИТ-инфраструктуры. Система защиты внедрена и работает, средств защиты — множество, требования к надежности и безопасности информационной системы высокие. Руководство, естественно, интересует способность корпоративной системы защиты противостоять существующим на данный момент угрозам безопасности (атакам хакеров, использованию тех или иных уязвимостей в ИТ-компонентах, возможным сбоям в работе критичных приложений и т.д.).

В таких условиях сотрудникам собственной службы безопасности трудно оценить уязвимости, которым подвержена их ИТ-система в данный момент. Во-первых, специалистов может быть не так много, а этой проблемой нужно всерьез заниматься — обрабатывать обширные общие данные и отчеты от системы анализа защищенности, даже если она есть, хорошо ориентироваться в современных технологиях обеспечения безопасности и т.д. Кроме этого, важно не просто найти уязвимость в ИТ-системе, а разработать и согласовать с коллегами из ИТ-службы методы и способы ее устранения. Во-вторых, собственные сотрудники могут не иметь достаточной квалификации и опыта для проведения таких оценок (даже обучения по всем применяемым средствам защиты в таком деле недостаточно).

Оптимальный выход для таких компаний — услуга контроля защищенности ресурсов, включая периодическое сканирование с ежемесячным отчетом и оценкой уязвимостей. Состав работ при первом анализе такой же, как при проведении разовой работы. Во многих случаях при первичном анализе и сканировании уровень безопасности оценивается как неудовлетворительный, отчет содержит описание множества обнаруженных слабостей в защите, среди которых выделяются наиболее критичные, подлежащие немедленному устранению. На основании рекомендаций, содержащихся в отчете, службы безопасности и ИТ устраняют все основные и наиболее опасные уязвимости в системе.

Далее в течение определенного времени (обычно — года) проводится непрерывный мониторинг новых угроз безопасности и уязвимостей в компонентах защищаемой системы, периодический поиск уязвимостей методом сканирования (например, раз в неделю) и анализ конфигурации ключевых компонентов. Периодически предоставляемый отчет содержит анализ выявленных слабостей в защите, оценку уровня их опасности и рекомендации по устранению (по мере необходимости). Периодичность определяется потребностями конкретной компании (раз в месяц, ежеквартально).

Таким образом, задача поддержания ресурсов информационной системы в защищенном состоянии решается путем слаженного взаимодействия собственных служб ИТ и безопасности, а также специализированной фирмы. Служба безопасности имеет авторитетную и независимую внешнюю организацию, которая подтверждает защищенность ресурсов системы компании. Служба ИТ получает вполне реализуемые и внятные рекомендации по устранению слабостей в настройках ИТ-компонентов, выпол-

ненные с высокой степенью подробности. Более сжатые и лаконичные отчеты о проделанной работе и текущем состоянии безопасности ресурсов представляются руководству компании.

Аутсорсинг в области безопасности

Все более широкое использование услуг внешних организаций (аутсорсинг) применительно к информационным технологиям — общемировая тенденция. Аутсорсинг в области информационной безопасности является одним из наиболее быстро развивающихся сегментов этого рынка. По прогнозам Gartner Group, в 2005 г. свыше 60% крупных компаний в мире передадут часть функций по обеспечению безопасности своих ресурсов на аутсорсинг внешним организациям. По оценкам компании IDC, в 2004 г. объем работ по аутсорсингу в области информационной безопасности показал примерно 35%-ный годовой рост.

В России повышение интереса к аутсорсингу, как и к ИТ-услугам в целом, наблюдается в последние три-четыре года. У отечественных предприятий более 50% затрат на услуги в области информационных технологий составляют расходы на поддержку аппаратного и программного обеспечения. Определить среди них долю аутсорсинга довольно сложно, по существующим оценкам это не менее 10% рынка ИТ-услуг.

Как уже отмечалось, рынок информационной безопасности, в том числе сегмент услуг, отстает от ИТ-рынка, но уже сегодня многие российские компании (как правило, имеющие практику передачи ИТ на аутсорсинг) пользуются услугами специализированных фирм-аутсорсеров. Под аутсорсингом в области безопасности понимается полная или частичная передача функций обслуживания и управления системой защиты внешнему исполнителю в течение определенного срока. При этом исполнитель должен обеспечивать заданный уровень качества выполнения этих функций (гарантированное время реакции на запрос, гарантированный период восстановления защитных функций в случае сбоев и т.д.). Работы в рамках аутсорсинга могут осуществляться как на площадке компании-заказчика, так и на стороне компании-исполнителя.

Потребность в услугах внешних сервисных компаний

Основных причин, по которым компании используют услуги сторонних специалистов в области информационной безопасности, как и в области ИТ, две.

Первая — это экономическая целесообразность, связанная со стремлением сократить расходы на обслуживание и управление системой безопасности. Эта задача для многих предприятий становится все более значимой, но при ее решении собственными силами возникают вопросы стоимости и эффективности. В идеале, нужно содержать несколько узкоспециализированных сотрудников, организовать и оборудовать для них рабочие места, периодически оплачивать их обучение и установить им высокие зарплаты. Использование же услуг сторонних специалистов позволит существенно повысить эффективность вложения средств.

В России среди тех, кто признает экономическую выгодность обращения к аутсорсингу, подавляющее большинство составляют крупные компании, предприятия с западным стилем управления или представительства иностранных фирм.

Вторая причина — квалификационная — заключается в дефиците специалистов, обладающих глубокими знаниями и практическим опытом в определенных узких областях, таких как информационная безопасность. Внешняя же фирма-исполнитель (по крайней мере, достаточно квалифицированная) имеет в своем арсенале передовые технологии и инструменты и способна предоставить высокое качество услуг (которое сложно обеспечить собственными силами). Например, в государственных структурах системы безопасности часто бывают достаточно дорогими и сложными, поскольку речь идет о закрытой информации, требующей «особого» обращения. Но при этом уровень оплаты труда не позволяет содержать специалистов высокой квалификации.

В небольших компаниях для обслуживания систем защиты не всегда целесообразно вводить новую штатную единицу. Бывают ситуации, когда функций по обеспечению защиты недостаточно, чтобы поручать их отдельному сотруднику, но в то же время слишком много, что-

бы нагружать ими существующих работников в качестве дополнения к их основной деятельности. Аутсорсинг в таких случаях позволяет приобрести на год «виртуальную половину сотрудника», который имеет достаточно высокую квалификацию и на должном качественном уровне выполнит необходимые работы.

Во многих организациях практикуется жесткое планирование расходов, например, на год. Государственные предприятия, как правило, не могут выделять незапланированные средства на обучение или подбор персонала и тому подобные вещи. Аутсорсинг позволяет стабилизировать ежегодные затраты на сервис: нужно столько и не больше.

Еще один довод в пользу аутсорсинга — существование во многих организациях текучки кадров (например, из-за невысокой зарплаты трудно удерживать квалифицированных специалистов). В таких условиях жизненно необходима эксплуатационная структура, не зависящая от конкретных людей. Аутсорсинг обеспечивает необходимый уровень сервиса независимо от болезни, отпуска или увольнения сотрудника. Грамотный поставщик сервисных услуг строит взаимоотношения с заказчиком таким образом, что сама защищаемая система и все действия в ней жестко регламентированы, поэтому ИТ-система перестает быть «черным ящиком», известным одному сотруднику, от которого зависит эффективность защиты ресурсов.

И наконец, многие компании, в которых ИТ и безопасность не являются профильным направлением деятельности, решают, что собственную инфраструктуру развивать не стоит. Передача в аутсорсинг функций поддержки систем информационной безопасности позволяет им сконцентрироваться на более важных для бизнеса задачах.

Барьеры и страхи

Основными препятствиями в обращении к ИТ-аутсорсингу являются страх потери контроля над собственными ресурсами и системами и недоверие к внешнему исполнителю. Примерно те же «барьеры» проявляются и в случае аутсорсинга в области безопасности. Одним из основных страхов для руководства предприятий является боязнь утечки или потери конфиденциальной и критически важной информации. Заказчик таких услуг, естественно, хочет быть уверен, что его внутренние ресурсы не будут доступны хакерам, конкурентам и т.д.

В качестве ответа на эти опасения приведем результаты исследований Digital Research, согласно которым в компаниях, использующих аутсорсинг, основной канал утечки информации — это действия штатных сотрудников (почти 60% случаев). Оставшиеся чуть более 40% случаев потери информации также не связаны с аутсорсером: их причиной была банальная халатность пользователей (потеря ноутбуков, документов, носителей информации и т.д.).

Кроме того, если сравнить сервис в области информационных технологий и информационной безопасности, то следует заметить: при обслуживании внешней сервисной организацией баз данных, серверов, систем резервного копирования и некоторых других ИТ-компонентов внешние сотрудники имеют непосредственный доступ к хранимой информации. Сотрудники же сервисной компании в области безопасности имеют доступ только к средствам защиты, не имея доступа к самой информации.

Основными гарантиями того, что конфиденциальная информация и критичные системы не станут более уязвимыми при переходе на аутсорсинг, являются высокая квалификация, дисциплина и ответственность компании-аутсорсера.

Высокая, как принято считать, стоимость аутсорсинга — препятствие сомнительное и устранимое методом изучения существующих на рынке сервисных предложений и оценки собственных затрат на аналогичные работы. В крупной сервисной компании, оказывающей услуги большому количеству клиентов, стоимость услуг вполне приемлема в силу того, что они оказываются массово (например, мониторинг новых угроз безопасности и уязвимостей в ИТ-компонентах проводится одним отделом для всех заказчиков, а самим заказчикам будет гораздо дороже держать такие отделы у себя). Трудность в этом вопросе скорее представляет методика расчетов экономической целесообразности аутсорсинга и оценки качества услуг.

Компании (в основном крупные) с высоким уровнем автоматизации, имеющие повышенные требования к безопасности и обеспечению непрерывности работы, считают препятствиями для перехода на аутсорсинг слабое знание сервисной компанией специфики их системы и неудовлетворительный уровень качества услуг. Эти недостатки присущи далеко не всем поставщикам сервисных услуг в области безопасности и остаются полностью на совести некоторых из них.

Ну и, конечно, имеет значение то обстоятельство, что данный сегмент рынка услуг в области безопасности в настоящее время является

самым молодым и пока недостаточно цивилизованным и зрелым. Сервисных компаний в области безопасности, способных предоставлять действительно качественные услуги, пока немного. Если выбор невелик, то у пользователя нет возможности сравнивать и в случае неудовлетворительного качества услуг сменить поставщика будет сложно. У потенциальных потребителей аутсорсинга возникает естественное недоверие к поставщикам в силу того, что большинство из них имеют непродолжительную историю работы в этом качестве и небольшой «пул» клиентов.

Тем не менее, при соблюдении определенных условий вполне реально подобрать оптимальный вариант. На российском рынке информационной безопасности достойных компаний достаточно, хороших сервисных ИТ-компаний — тоже. Остается лишь найти пересечение этих двух множеств и грамотно построить отношения с выбранным поставщиком услуг.

Аутсорсинг: виды и уровни услуг

Весь набор предлагаемых сегодня аутсорсинговых услуг можно разделить по видам (обслуживание средств и систем безопасности, аналитические задачи и т.д.) и уровням (администрирование, контроль безопасности). В трактовке компании «Инфосистемы Джет» некоторые услуги, не относящиеся в чистом виде к поддержке уровня защищенных информационных систем (экспертиза проектов, разбор сложных инцидентов безопасности и другие), оказываются в рамках центра компетенции по вопросам информационной безопасности. В комплексе эти две группы сервисных услуг позволяют решить практически любую задачу по защите ресурсов любого предприятия.

Аутсорсинг выбирается предприятием в соответствии с его нуждами и особенностями — набором применяемых решений по защите, существующей практикой эксплуатации информационной системы, имеющимися человеческими и техническими ресурсами и т.д.

Администрирование средств защиты информации

Минимальный уровень услуг, которые можно поручить внешнему исполнителю, — администрирование и обслуживание средств защиты. На аутсорсинг чаще всего передаются сложные средства обеспечения безопасности, управление которыми требует очень высокой квалификации и глубокого понимания механизмов их работы. К ним относятся системы обнаружения атак и контроля защищенности, анализа содержимого и фильтрации трафика и другие средства, требующие «тонкой» настройки, корректной трактовки генерируемых ими событий и в целом довольно большого внимания в процессе эксплуатации. Для сотрудников компании-заказчика может быть также предоставлена круглосуточная служба приема и обработки запросов, связанных с обслуживаемыми средствами защиты.

Внешняя сервисная компания может оказывать услуги по внедрению и интеграции средств защиты информации, осуществлять их круглосуточное сервисное обслуживание и техническую поддержку, проводить штатные модификации программного обеспечения, по мере необходимости корректировать их настройки, производить резервирование аппаратных компонентов оборудования. При этом разработка политик и правил работы средств защиты, а также получение отчетов от них остается в ведении службы безопасности компании-заказчика, аутсорсер обеспечивает только настройку средств защиты в соответствии с требованиями политики безопасности.

Аутсорсинг систем безопасности

Следующий уровень — передача на аутсорсинг всей системы информационной безопасности. В этом случае сервисная организация несет ответственность не просто за работоспособность и корректную конфигурацию применяемых средств защиты, а за надежный уровень защищенности ресурсов, обеспечиваемый всем комплексом средств.

Для этого помимо функций, перечисленных в предыдущем пункте, аутсорсер проводит постоянный мониторинг состояния безопасности системы (в режиме off-line или в реальном времени): анализ происходящих событий и их интерпретацию; мониторинг состояния и изменения критичных системных параметров (косвенно свидетельствующих о возможности атак и других важных событий); предпринимает меры по реагированию на события (или выдает соответствующие инструкции персоналу компании-заказчика); в случае необходимости совершает аварийный выезд для решения особо критичных проблем.

Служба безопасности компании-заказчика осуществляет контроль качества услуг, оказываемых внешней сервисной организацией, на основании журналов работы, которые ведет аутсорсер и в которых фиксирует свои действия, и предоставляемых сервисной компанией отчетов

о произошедших инцидентах безопасности, причинах, последствиях и предпринятых мерах.

Аналитические задачи

По разным причинам целесообразно передавать на аутсорсинг также аналитические задачи, требующие значительных человеческих и технических ресурсов, а также наличия у специалистов не только высокой квалификации, но и большого опыта работы. К ним относятся сбор и анализ данных о появлении новых угроз безопасности, уязвимостей и способов атак, оценка их опасности для защищаемой информационной системы и ликвидация слабостей в защите ресурсов (либо выдача рекомендаций по ликвидации персоналу).

Состав работ в принципе тот же, что в услуге «Анализ и контроль защищенности ресурсов», предоставляемой в течение определенного периода времени. Другие аналитические услуги — расследование инцидентов в области безопасности, оценка изменений в информационной системе с точки зрения информационной безопасности и т.д. — подробно описаны в главе «Центр компетенции по вопросам информационной безопасности».

Подготовительные мероприятия по передаче функций ИБ на аутсорсинг

В первую очередь руководителю любой организации стоит выяснить, при каких условиях целесообразно доверить обеспечение защиты своих ресурсов сторонней фирме и какие выгоды сулит его бизнесу использование такого сервиса. Если необходимость в услугах внешней организации очевидна, то прежде всего необходимо определить, какие именно функции, задачи и элементы защиты передать на аутсорсинг.

Учитывая, что передача систем обеспечения безопасности во внешнее обслуживание предполагает возникновение дополнительных рисков и угроз, следует провести комплекс подготовительных мероприятий, особенно в крупных компаниях со сложной организационной структурой. Часть подготовительных работ также может быть выполнена внешним исполнителем, но при руководящей функции службы безопасности и обязательном контроле с ее стороны.

Для подготовки к переводу на аутсорсинг нужно провести анализ существующей практики эксплуатации ИТ-системы и системы защиты, а также других специфических особенностей компании. Исходя из этих данных разрабатываются требования по поддержанию режима информационной безопасности и схема обеспечения безопасности в условиях внешнего сервисного обслуживания. Результатом является план организационно-технических мероприятий по вводу этой схемы в действие: этапность перевода средств и систем во внешнее обслуживание, необходимые условия и ресурсы (например, дополнительные программно-технические средства) и т.д. Важной частью разработанной схемы являются регламенты отношений с внешней организацией с точки зрения информационной безопасности, а также определение новых задач службы информационной безопасности предприятия, связанных с мониторингом и протоколированием действий внешних организаций.

Задача контроля действий внешней сервисной компании является критически важной и должна быть основной для внутренней службы безопасности. Для ее эффективного решения потребуется создать или дополнить существующую систему мониторинга. Понадобятся дополнительные средства управления компонентами системы информационной безопасности и ИТ-компонентами (сетями, серверами, прикладными системами и т.д.), фильтрации и анализа журналов регистрации событий (лог-файлов). Кроме того, необходимы средства контроля: информации, передаваемой по вычислительным сетям организации, действий системных и прикладных пользователей, методов доступа к информационным ресурсам и системам, способам аутентификации и т.д. Должен быть определен порядок эксплуатации системы мониторинга: компоненты, подлежащие контролю, частота контрольных действий, форма соответствующих отчетов, порядок хранения информации, включая лог-файлы. После этого система мониторинга передается на эксплуатацию внутренней службе безопасности предприятия.

Еще одно важное условие: при выполнении аутсорсером своих функций удаленно необходимо обеспечить безопасность и надежность всех удаленных соединений. Для этого внешняя сервисная компания должна организовать виртуальную частную сеть с компанией-заказчиком и резервирование этих защищенных каналов.

Выгоды аутсорсинга

Основные выгоды, которые получают потребители аутсорсинга (при грамотной организации работ), это оптимизация расходов на эксплуатацию систем информационной безопасности, решение кадровых проблем и повышение качества выполнения соответствующих работ.

Использование технологий аутсорсинга снижает риски нанесения ущерба компании, поскольку аутсорсер имеет большой опыт выполнения работ и все необходимые ресурсы. Высококвалифицированные специалисты узких специальностей, специальные программно-технические средства и тестовые стенды — все это работает в круглосуточном режиме. При этом система защиты ресурсов становится отчуждаемой как от сотрудника компании-заказчика, который ее обслуживает, так и от обслуживающей фирмы. Надежность и работоспособность этой системы перестает зависеть от обстоятельств у компании-заказчика.

Некоторые аналитические задачи в области безопасности — сбор и анализ информации о появлении новых угроз, «дыр» и уязвимостей, способов атак, оценка их влияния на защищенность компонентов информационной системы — сложно решать собственными силами, поскольку это требует слишком много времени, специалистов и знаний. Но они имеют существенное значение для безопасности ресурсов, система защиты должна соответствовать последним тенденциям, поэтому игнорировать их нельзя.

Передача ответственности за выполнение непрофильных функций аутсорсеру позволяет сконцентрироваться на решении основных бизнес-задач и повысить эффективность основного бизнеса.

Центр компетенции по вопросам информационной безопасности

Центр компетенции — это комплексная услуга, которая может быть полезна предприятиям разного масштаба с самыми разными условиями и требованиями по защите ресурсов. По сути, это «абонемент» с оговоренным сроком действия на получение определенного объема аналитических, консалтинговых и сервисных услуг.

В рамках центра компетенции технические специалисты внешней фирмы могут оказывать консультации, предоставлять информацию по интересующим заказчика вопросам, а также выполнять другие виды работ в области информационной безопасности и смежных областях информационных технологий.

Удобство центра компетенции состоит в том, что в любой момент можно воспользоваться нужной именно сейчас услугой. Например, получить помощь в анализе и интерпретации записей в журналах регистрации событий средств защиты или ИТ-компонентов, чтобы понять, критично ли это событие для данной информационной системы. Или привлечь квалифицированного исполнителя для выполнения срочных работ, например, внедрения нового межсетевого экрана или системы обнаружения и отражения внешних атак в течение одних выходных. В рабочие дни проводить такие работы нельзя, поскольку это нарушит работу ИТ-системы, а выполнить полное внедрение, включая настройку политик и правил, в сжатые сроки собственными силами невозможно.

Сбои в системе защиты и другие неприятные инциденты случаются, как правило, в самые неожиданные моменты — праздники, отпуска и т.д., и найти нужных специалистов внутри компании часто бывает невозможно. У сервисной компании такие специалисты присутствуют 24 часа в сутки, и можно прибегнуть к их помощи в преодолении возникшей ситуации.

Расследование сложных инцидентов безопасности часто требует быстрого привлечения специалистов в совершенно разных ИТ-областях и их взаимодействия друг с другом. Помимо сложностей с наличием таких специалистов на предприятии и сбором их в группу в нужный момент, есть и другие сложности. Например, украдены сведения из базы данных. Что могут сделать сотрудники службы безопасности? Собственными силами — немного. Нужны, как минимум, эксперты по базам данных, а возможно, еще и по другим областям. Но ситуация может осложняться тем, что источник утечки информации может находиться внутри компании. В таких случаях необходима именно независимая профессиональная экспертиза.

Специализированная сервисная компания может также представлять интересы компании-заказчика при разрешении внешних конфликтных ситуаций, вызванных нарушениями информационной безопасности.

В рамках центра компетенции проводится еще один важный пласт работ: оценка изменений ИТ-инфраструктуры (новые подключения, изменения схем функционирования, плановые дора-

ботки систем) или экспертиза ИТ-проектов с точки зрения безопасности. Например, в компании практически непрерывно идут реорганизации ИТ-структуры, связанные в основном с ее расширением и внедрением новых сервисов. В службу безопасности сплошным потоком поступают проекты о модернизации сети, почтовой системы, введении новых сервисов, модернизации баз данных, подключении филиалов — список возможных перемен может быть длинным. Ко всем этим проектам нужны требования по соблюдению норм безопасности, с чем ни одна служба безопасности в таких условиях не справится. В крупных и динамично развивающихся компаниях развитие и модернизация ИТ-систем — это практически непрерывный процесс.

Подготовка или помощь в подготовке требований по безопасности в условиях предлагаемых нововведений, участие компетентной внешней организации в совещаниях по вопросам реорганизаций и т.д. позволит не только разгрузить службу безопасности, но и помочь разработать более обоснованные и надежные меры безопасности. Внешняя фирма может привлечь всех необходимых специалистов (в том числе в других областях информационных технологий). И кроме того (позволим себе повториться), у организаций-заказчиков, работающих в одной отрасли, часто возникают похожие проблемы, свойственные, например, страховым компаниям, операторам телекоммуникаций, банкам и т.д. Специализирующейся в области безопасности компании многие проблемы, возникающие у заказчиков, чаще всего уже известны.

Поставщики сервисных услуг

Выбор сервисной компании

К сожалению, компании, специализирующиеся только на информационной безопасности, часто не имеют достаточного опыта и налаженных схем предоставления сервисных услуг. Кроме того, они обычно не имеют специалистов по смежным ИТ-областям, которые часто бывают востребованы при решении задач эксплуатации систем защиты.

Среди компаний же, работающих в области предоставления сервисных услуг в различных ИТ-областях, очень немногие являются профессиональными и в области безопасности. У большинства из них есть только небольшой отдел информационной безопасности и сравнительно недолгая история на этом рынке.

Поскольку задача эксплуатации защищенных систем носит комплексный характер, многие проблемы возникают на стыке разных областей информационных технологий, целесообразно передавать функции информационной безопасности крупным компаниям, предпочтительно интеграторам, имеющим опыт построения и обслуживания сложных ИТ-систем и систем информационной безопасности.

Существует несколько критериев выбора исполнителя работ. Первая группа определяет квалификацию сервисной компании и ее способность оказывать услуги для любых имеющихся у заказчиков средств и систем защиты. Важно, чтобы потенциальный исполнитель имел долгосрочные партнерские отношения с большим количеством поставщиков технологий и средств безопасности, широко применяемых в ИТ-системах российских предприятий, располагал штатом квалифицированных сервисных инженеров, прошедших авторизованное обучение и сертификацию у производителей.

Исполнитель должен быть технически оснащен: испытательная лаборатория, в которой эмулируются различные технические проблемы в системах защиты и отрабатываются варианты реагирования на них; специальные инструменты для анализа защищенности ИТ-компонентов и т.д.

Предлагаемые сервисные услуги должны быть комплексными (от минимального уровня технической поддержки до экспертизы и аутсорсинга), и гибкими, адаптируемыми к условиям конкретной компании. Например, для обслуживания организации с особо высокими требованиями к безопасности и надежности работы ИТ-системы со стороны исполнителя может потребоваться выделенный менеджер по технической поддержке, который будет обеспечивать немедленное реагирование на запросы и организацию максимально быстрого решения возникающих проблем с привлечением всех необходимых ресурсов.

Для многих компаний имеет значение наличие у исполнителя сервисных центров не только в Москве, но и в других городах — чем

больше, тем качественнее и эффективнее будет сервисное обслуживание распределенных защищенных систем.

Другая группа критериев касается опыта и репутации сервисной компании. В первую очередь важен продолжительный опыт работы поставщика на рынке и успешные примеры оказания подобных услуг, поскольку это свидетельствует об уровне качества выполняемых им работ. Поэтому при выборе поставщика сервисных услуг лучше ориентироваться на крупные и известные компании, имеющие хорошую репутацию.

Регламентация отношений с сервисной компанией

Любые приобретаемые услуги должны соответствовать заданному уровню качества. А в такой специфической области, как информационная безопасность, качество услуг имеет критически важное значение. Поэтому контракт с сервисной компанией обязательно должен максимально точно и подробно определять параметры самих услуг, параметры контроля их качества, а также ответственность исполнителя за некачественные услуги.

В договоре с внешней сервисной организацией следует особо отметить следующие моменты:

- территория и объекты обслуживания;
- время предоставления услуг (рабочие часы, круглосуточно);
- время реакции на запрос или происшествие и максимальный срок их разрешения;
- способы реакции на запрос в зависимости от типа и сложности возникшей проблемы;
- порядок и форма предоставления отчетности;
- вопросы дополнительного финансирования (например, в случае необходимости срочно ликвидировать возникшие в системе уязвимости);
- требования конфиденциальности.

Неполная или неточная формулировка по любому из этих пунктов может не только минимизировать все выгоды от использования внешних сервисных услуг, но и нанести ущерб. Например, если в контракте не указано время реагирования на запрос, исполнитель может долго «думать» над решением проблемы, о которой к нему поступила информация, а в это время вирус или другая атака, которую можно было бы остановить на ранней стадии, уже выведет из строя сервер критичных приложений. Предъявлять претензии к исполнителю за то, что он промедлил, в этом случае бесполезно.

Важно также оговорить и способы реагирования исполнителя на запросы: может быть достаточно телефонной консультации, в которой внешняя компания ассистирует администратору безопасности в корректировке правил, настроенных на сетевом устройстве или средстве защиты. В случае более сложных технических проблем поможет удаленная диагностика и решение возникшей проблемы внешним сервисным инженером (управление средствами защиты по защищенному каналу). А в критичных случаях, когда удаленная помощь оказывается неэффективной, может потребоваться аварийный выезд на площадку компании-заказчика (опять же важно, чтобы этого выезда не пришлось ждать слишком долго, а приехавшие специалисты выполнили все предусмотренные для таких случаев работы, за качество которых исполнитель несет ответственность).

Отчеты и регистрационная информация, предоставляемые внешней сервисной компанией, являются основным средством контроля ее деятельности. В каком формате, как часто и насколько подробно представлять эту информацию — обязательно должно быть оговорено в контракте.

Таким образом, грамотно составленный сервисный контракт позволит заказчику контролировать работу исполнителя по заранее согласованным критериям и в случае невыполнения или ненадлежащего качества услуг привлекать его к ответственности.

Средства и услуги в области защиты информации, предлагаемые компанией «Инфосистемы Джет»

Компания «Инфосистемы Джет» — один из ведущих системных интеграторов в России и странах СНГ, специализируется также в области информационной безопасности и является производителем собственных средств защиты информации. Штат компании составляют около 400 человек, 150 из которых — сертифицированные технические специалисты в различных областях информационных и сетевых технологий, более 40 — в области информационной безопасности и 50 менеджеров по работе с заказчиками.

Компания располагает персоналом с высоким уровнем профессиональной подготовки, прошедшим обучение в ведущих специализированных центрах и у мировых поставщиков продуктов и решений в области информационных технологий и информационной безопасности. Среди этих компаний: CheckPoint Software Technologies, Internet Security Systems, RSA Security, Symantec Corporation, Sun Microsystems, Oracle, Informix, Hitachi Data Systems, Hewlett-Packard, Nortel, Cisco Systems, Lucent Technologies и другие производители с мировым именем, а также отечественные компании, работающие в области защиты информации, — «Лаборатория Касперского», НИП «Информзащита» и другие.

Наличие высококвалифицированного инженерно-конструкторского персонала и менеджмента в сочетании с техническими и организационными возможностями компании делает ее одним из лучших партнеров в работе с крупными корпоративными клиентами.

Компания «Инфосистемы Джет» выполняет полный комплекс работ по поставке, установке, настройке и сопровождению компонентов информационных систем (сетевого оборудования, высоконадежных серверных комплексов и т.д.) и систем информационной безопасности для государственных и федеральных структур, крупных банков и финансовых организаций, промышленных предприятий, страховых компаний, операторов телекоммуникаций и других государственных и коммерческих предприятий.

Для обеспечения комплексной поддержки установленных у заказчиков масштабных информационных систем, исполняющих критичные высокоответственные задачи, и систем информационной безопасности в 1994 г. в компании образован собственный сервисный центр. Сферой его компетенции являются высокопроизводительные серверные комплексы, в том числе кластерные системы, системы хранения данных, локальные и распределенные вычислительные сети, системы управления ресурсами, системы управления базами данных банковских систем, комплексные системы информационной безопасности.

На сегодня сервисный центр компании «Инфосистемы Джет» является одним из крупнейших и наиболее профессиональных в России, имеет десятилетнюю успешную историю. Сервисный центр обеспечивает исполнение взятых обязательств по качеству обслуживания благодаря высокой квалификации сервисных инженеров во всех необходимых отраслях ИТ, наличию уникальных апробированных схем оказания сервисной поддержки для информационных систем разного масштаба — от здания до региона или целой страны.

В настоящий момент сервисный центр обслуживает (в том числе в круглосуточном режиме) более 200 заказчиков более чем в 50 городах,

оборудование и программное обеспечение заказчиков размещено на более чем 300 площадках по всей территории России и СНГ. Использование автоматизированной технологии обработки запросов на сервисное обслуживание и уникальных методик организации работы позволяет наиболее эффективным образом обеспечивать постоянную готовность решения задач любой сложности.

Сервисный центр компании «Инфосистемы Джет» предлагает заказчикам различные программы обслуживания, ориентированные на решение задач любого уровня сложности, возникающих в процессе эксплуатации информационных систем и систем информационной безопасности. Развитие нескольких технических направлений позволяет сервисному центру заниматься вопросами комплексного обслуживания систем и обеспечения рабочего взаимодействия оборудования и программного обеспечения от различных производителей. Центр располагает широким спектром программ сервисного обслуживания — от ремонта вышедшего из строя оборудования до настройки систем под специфические требования эксплуатации.

Сервисное обслуживание оборудования и программного обеспечения информационных систем и систем информационной безопасности имеет несколько уровней. Предоставляемые сервисные услуги:

- комплекс пусконаладочных работ для обеспечения индивидуальной подготовки и настройки оборудования и программного обеспечения под конкретные задачи, решаемые заказчиком; пусконаладочные работы содержат предпродажную подготовку, монтаж оборудования на площадке заказчика, подключение оборудования к локальной сети и сети электропитания, тестирование работоспособности, инсталляцию и конфигурирование операционных систем с учетом особенностей последующей эксплуатации, инсталляцию и настройку управляющего и прикладного программного обеспечения;
- предоставление единой «горячей линии»: консультации по телефону и электронной почте по вопросам администрирования и эксплуатации оборудования и программного обеспечения, предоставление информационных материалов, помощь специалистам заказчика в диагностике неисправностей и проведении восстановительных работ; время оказания консультаций устанавливается индивидуально для каждого заказчика; возможно предоставление круглосуточной (24x7) «горячей линии»;
- выезды специалистов на площадку заказчика для диагностики неисправностей и восстановления работоспособности и функциональности поддерживаемого оборудования и программного обеспечения; время визитов устанавливается индивидуально для каждого заказчика; возможно осуществление визитов в круглосуточном (24x7) режиме;
- замена неисправных элементов оборудования или временное предоставление функциональных аналогов оборудования в случае длительных ремонтов;
- гарантированное время восстановления функциональности обслуживаемой системы, устанавливаемой индивидуально в зависимости от степени критичности элементов и подсистем;
- профилактические визиты специалиста на площадку заказчика по согласованному плану-графику для контроля технического состояния оборудования и программного обеспечения, профилактического обследования поддерживаемой конфигурации, направленного на анализ производительности и корректности работы, выявление и устранение потенциальных проблем;
- предоставление новых версий программного обеспечения и кодов программных коррекций (патчей) по мере их выпуска производителем;
- мониторинг выпускаемых коррекций программного обеспечения (патчей), контроль их актуальности для поддерживаемой у заказчика конфигурации, установка рекомендованного набора программных коррекций;
- решение задач интеграционного характера для оборудования и программного обеспечения, которое находится на техническом обслуживании в сервисном центре; решение таких задач подразумевает обеспечение надежного взаимодействия оборудования и программного обеспечения от различных производителей;
- консультативное сопровождение задач интеграционного характера для оборудования и программного обеспечения, не находящегося на сервисном обслуживании, но взаимодействующим с обслуживаемым оборудованием и программным обеспечением;

- ведение персонально истории заказчика в специальном формате: журнал работ, осуществляемых в рамках сервисного обслуживания, подготовка периодических отчетов о выполненных работах;
- предоставление выделенного менеджера по технической поддержке сервисного центра для координации и выполнения работ в рамках сервисного обслуживания и привлечения всех необходимых ресурсов.

Каждая из предлагаемых сервисным центром программ обслуживания может быть адаптирована под специфические условия и режим работы заказчика.

На сегодня приоритетным направлением работы сервисного центра является повышение общей надежности обслуживаемых информационных систем и систем безопасности, сокращение количества нештатных ситуаций в эксплуатации. Ключевыми элементами программ обслуживания являются услуги профилактического и консалтингового характера, которые позволяют устранить причины вероятных сбоев до возникновения серьезных аварий в системе.

В сервисном центре компании «Инфосистемы Джет» функционирует собственный технический стенд для моделирования проблемных ситуаций, которые могут возникнуть в элементах информационной системы и системы защиты, установленных у заказчиков. Технический стенд включает серверное и сетевое оборудование, специализированное прикладное программное обеспечение (системы управления ресурсами, СУБД и т.д.), программные и программно-аппаратные средства информационной безопасности разных производителей. В распоряжении специалистов центра есть также склад оборудования и комплектующих, используемых в качестве ремонтного фонда для оборудования, находящегося на сервисном обслуживании.

Одним из направлений деятельности сервисного центра является планирование, проектирование, создание и внедрение собственной службы эксплуатации у заказчика, предназначенной для повышения качества выполнения наиболее критичных задач, возникающих при эксплуатации информационных систем и систем безопасности. При этом особое внимание уделяется формализации и внедрению процедур конфигурирования и документирования, выявления и устранения сбоев в функционировании информационной системы и системы защиты, учета текущей загруженности и планирования развития.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**