Помимо базовой функциональности, традиционной для продуктов данного класса, система обладает следующими возможностями:

• является событийно-ориентированной;

• имеет механизм уведомлений по электронной почте по ключевым событиям в момент их возникновения;

• поддерживает управление проектами между географически удаленными офисами;

• интегрирована с MS Project, обеспечивая при этом возможность детализации плановой информации;

• позволяет жестко разграничить права доступа участников проекта в зависимости от стадии проекта;

• имеет встроенные средства переноса накопленной информации по проектам в формат любого средства управления проектами, используемого в компании.

Для обеспечения сотрудников компании, участвующих в управлении программами работ и проектами необходимой нормативно-методической документацией в удобной для использования форме, создан сайт НМО, представляющий собой набор HTML-файлов, содержащих описание: фаз и процессов управления программой работ/проектом, входящих в процесс работ и в каждую работу задач; ролей, выполняющих задачи; документов, формируемых при выполнении процессов управления (для основных документов в состав сайта включены их шаблоны в формате .DOC).

При этом в описание каждой из задач включена следующая информация: назначение задачи, состав входных/выходных документов, ссылка на роль, выполняющую задачу, ссылка на принадлежность задачи к работе – процессу, описание методики ее выполнения.

Заключение

Представленная в данной статье система управления программами работ и ИТ-проектами разработана и реализована по заказу крупной российской нефтяной компании, однако специфика нефтяной отрасли существенно не повлияла на ключевые методологические и проектные решения.

Внедрение системы обеспечило:

• переход к проектному управлению в компании на основе внедрения комплекса средств управления программами работ и ИТ-проектами;

• проведение единой технической политики в области сокращения совокупных затрат на реализацию проектов;

• возможность управления инвестициями в ИТ на уровне бизнес-задач компании (инвестиционный портфель – программа работ – проект);

• повышение уровня управляемости работами в области ИТ;

• наличие оперативной аналитической отчетности и накопления опыта по проектам;

• возможность управлять большим числом проектов ограниченным числом менеджеров;

• ведение проектных работ на современном организационно-техническом уровне с использованием новейших технологий;

• основу для оценки возврата на инвестиции в ИТ.

Калянов Георгий Николаевич *– проф., д-р техн. наук, зав. лабораторией Института проблем управления им. В.А. Трапезникова РАН,*
Позин Борис Аронович *– д-р техн. наук, технический директор ЗАО "ЕС-Лизинг".*
Контактный телефон (095) 311-22-18. E-mail: Kalyanov@mail.ru; Bpozin@ec-leasing.ru

Проблемы ИТ-безопасности в промышленном масштабе

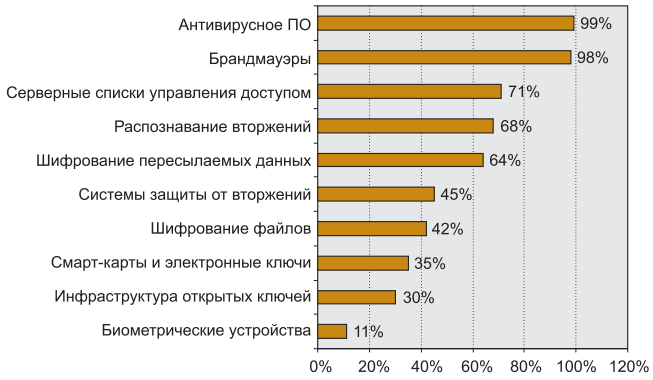
А.В. Доля ("Лаборатории Касперского")

Информационные технологии сегодня стали неотъемлемой частью бизнес-процессов. Internet и электронная почта позволяют организовать эффективные коммуникации между распределенными офисами крупных компаний, наладить взаимодействие с заказчиками и обеспечить быстрый обмен информацией между сотрудниками внутри одного офиса. ПК помогают автоматизировать многие рутинные процессы и с каждым днем берут на себя все больше и больше функций. Однако инфраструктура компании находится под постоянным давлением со стороны внешних угроз ИТ-безопасности. Проанализированы возможные внешние угрозы ИТ-безопасности промышленных предприятий и организаций, указаны способы борьбы с ними.

По оценкам североамериканских компаний USA Today и Avantgarde рабочая станция под управлением Windows XP, подключенная к Internet, в течение одного часа подвергается 341 атаке вредоносных кодов. Первая же атака легко достигнет успеха, если ПК не защищен соответствующим антивирусным средством. Эксперты подсчитали, что незащищенный специальным ПО компьютер уже через 4 минуты своей работы в сети Internet превращается в марионетку в руках злоумышленников: начинает рассылать вирусы и спам.

Крупные компании уже давно осознали выгоду использования информационных технологий и те опасности, которыми это чревато. Последнее исследование ФБР показало, что 99% представителей бизнеса используют антивирусные средства, 98% – межсетевые экраны, более 50% применяют и другие распространенные технологии (рисунок).

Однако компании по-прежнему несут убытки в связи с инцидентами ИТ-безопасности, а также испытывают трудности с эксплуатацией уже имеющихся средств. Например, организация CERT зарегистрировала в 2003 г. в 1,7 раз больше инцидентов, чем в 2002 г.. По сведениям Computer Economics, прошедший 2004 г. с точки зрения ИТ-безопасности стал худ-



шим из всех предыдущих: убытки от вирусных атак выросли с 13 до 17,8 млрд. долл. США, появились вредоносные коды для мобильных устройств (карманных компьютеров и мобильных телефонов), использующихся в корпоративной среде.

Институт компьютерных преступлений США и ФБР провели исследование "2004 CSI/FBI Computer Crime and Security Survey", в ходе которого были опрошены 494 американские компании и организации. Результаты опроса показали, что за 2004 г. 47% респондентов зафиксировали 1...5 инцидентов в сфере информационной безопасности, наибольший ущерб компаниям нанесли вредоносные коды (55 млн. долл. США), атаки типа "отказ в обслуживании" (26 млн. долл. США) и кража конфиденциальных данных (11,5 млн. долл. США).

Вирусные атаки не случайно являются самой опасной угрозой сегодняшнего дня. Последствия успешной вирусной атаки могут быть самыми разнообразными: недееспособные узлы корпоративной сети, уничтожение или похищение конфиденциальной информации, слежка и удаленное управление инфраструктурой компании со стороны злоумышленника и т.д. В последнее время вирусы используются для организации атак типа отказ в обслуживании и кражи важных данных. Именно поэтому симбиоз этих трех атак постоянно занимает первые строчки в списке наиболее опасных угроз.

Получается, что, с одной стороны, компании используют современные технологии для обеспечения ИТ-безопасности, а с другой – по-прежнему несут убытки вследствие инцидентов в этой сфере. Такое положение дел вызвано тем, что за прошедшие годы акцент в построении корпоративной системы ИТ-безопасности сместился от простейшего внедрения самих средств ИТ-безопасности к построению комплексных систем, характеризующихся всесторонней управляемостью и высокой степенью интеграции в общую ИТ-инфраструктуру компании.

Проблемы индустрии

Одна из основных проблем современной индустрии состоит в том, что система ИТ-безопасности на многих предприятиях состоит из отдельных разрозненных компонентов. Каждый такой компонент обычно имеет собственного разработчика и поставщика, специализированные средства управления и обновления.

Такая ситуация обусловлена тем, что при внедрении средств ИТ-безопасности компании пытались сэкономить на стоимости начального решения и, следовательно, формировали свою будущую систему ИТ-безопасности на основе отдельных продуктов от разных производителей. Таким образом, ИТ-инфраструктура крупного и среднего современного предприятия порой может включать антивирусные модули одного поставщика для защиты рабочих станций, другого – для защиты почтовых шлюзов, а третьего – для защиты файловых и Web-серверов.

Такой подход часто позволяет сэкономить на стоимости начального решения. Более того, у администратора системы ИТ-безопасности может возникнуть уверенность, что каждая внешняя угроза выявлена и локально обезврежена (собственными средствами). Тем не менее, это лишь иллюзия. Во-первых, такое разнородное решение позволяет сэкономить лишь на начальном этапе, а в долгосрочной перспективе оборачивается дополнительными трудозатратами на внедрение, поддержку и управление. Во-вторых, при построении такой системы некоторые узлы ИТ-инфраструктуры могут остаться просто неучтенными, хотя бы на время. В-третьих, такую систему очень сложно обновлять и модернизировать.

Наиболее опасная ситуация складывается чаще всего в разгар вирусных эпидемий, когда в течение короткого промежутка времени появляются сразу несколько разновидностей вредоносных кодов. Каждый антивирусный разработчик выпускает соответствующее обновление, которое должно попасть на каждый защищенный узел ИТ-инфраструктуры. Очевидно, что каждому компоненту разнородной системы ИТ-безопасности приходится самостоятельно скачивать и устанавливать горячее обновление, что приводит не просто к повышенной загрузке каналов связи, но еще и временной недоступности некоторых сетевых ресурсов.

Вдобавок к несовершенной системе обновлений, отсутствие однородности в средствах ИТ-безопасности приводит к невозможности централизованного управления и мониторинга. Между тем в задачи администратора входит постоянное наблюдение за функционированием как самих ИТ-ресурсов компании, так и средств ИТ-безопасности. Таким образом, ИТ-специалистам очень сложно выявлять и регистрировать инциденты, составлять централизованные отчеты, контролировать параметры средств ИТ-безопасности и вообще эксплуатировать эти средства.

ИТ-инфраструктура большинства предприятий носит гетерогенный характер, который проявляется в многообразии несовместимых друг с другом ОС, стандартов, протоколов и прикладных программ, используемых в рамках одной вычислительной сети. Обычно на момент внедрения антивирусного решения информационная инфраструктура уже существует. Серверы могут находиться под управлением ОС

Microsoft Windows, Unix/Linux, *BSD или Novell Netware, а прикладное ПО, например, почтовый сервер может включать Microsoft Exchange, Sendmail, Qmail, Postfix, Exim или Lotus Notes. Эти взаимоисключающие технологии требуют специальной поддержки, реализованной в антивирусном решении. Между тем многие антивирусные разработчики вообще не покрывают, например, ОС типа Linux и FreeBSD, а те, кто выпускает соответствующие защитные модули для почтовых шлюзов на базе этих ОС, оставляют без внимания Qmail и Postfix, покрывая лишь Sendmail.

При построении системы ИТ-безопасности из разрозненных модулей сотрудникам приходится сталкиваться со всеми этими проблемами. Более того, им приходится самостоятельно решать эти проблемы, хотя соответствующего опыта порой не хватает.

Здесь сказывается отсутствие комплексности во внедряемом решении. Дело в том, что если предприятие делает ставку на всестороннее комплексное решение с самого начала, то в результате поставщик или его партнеры внедряют само решение "под ключ". Заказчику в этом случае не надо беспокоиться об анализе уже существующей ИТ-инфраструктуры, составлении политик безопасности и нормативных документов, внедрении компонентов решения и создания удобных средств централизованного управления, мониторинга и обновления. Поставщик продукта берет на себя ответственность за обучение персонала, круглосуточную техническую поддержку, консультации по мере необходимости и экстренную помощь в случае возникновения инцидента.

Насколько важны все эти сопроводительные услуги? Известная организация Computer Economics провела исследование, в ходе которого респондентам был задан вопрос о продуктах и услугах, которые им потребовались вследствие вирусной атаки. В результате оказалось, что наибольший спрос приходится именно на дополнительное ПО (25%) и консалтинговые услуги (15%). В данном случае это мероприятия, проводимые после того, как произошел инцидент и компания понесла серьезные убытки. Делая ставку на комплексное решение, предприятие с самого начала инвестирует несколько больше средств во всесторонний, но зато полностью управляемый продукт и сопроводительные услуги. Таким образом, снижаются не просто риски возникновения инцидентов, но еще и решается проблема закупки нового ПО и найма консалтинговых или аудиторских компаний. Ведь все эти продукты и услуги доступны заказчику сразу же как пользователю комплексного решения.

Новые угрозы

Комплексность решения подразумевает безопасность не только всех узлов ИТ-инфраструктуры, но и защиту от всего спектра возможных угроз. Это становится особенно актуально, когда какая-либо новая угроза становится более опасной, чем раньше. В этом случае следует обновить не просто один из компонентов комплексной системы ИТ-безопасности (например, если появляется новый опасный сетевой червь, то необходимо обновить лишь антивирусную базу), а само решение, добавив в него соответствующий компонент. В случае, когда на предприятии используется разнородная система безопасности, сотрудникам необходимо самостоятельно проанализировать, что за новый продукт им необходим, как его внедрять и эксплуатировать. Это непростая задача, так как служащие ИТ-отделов чаще всего не обладают необходимым опытом и соответствующими знаниями. Однако при использовании комплексного решения поставщик самостоятельно разрабатывает новый модуль, помогает внедрить его в ИТ-инфраструктуру заказчика и, что не менее важно, интегрирует новую функциональность в средство централизованного управления ИТ-безопасностью.

Наиболее ярким примером внешней угрозы, которая стала значительно опаснее в последнее время, является нежелательная электронная почта или спам. Специалисты "Лаборатории Касперского" оценили долю спама в общем потоке электронной корреспонденции в более чем 70%. Такой большой поток почтового "мусора" чреват серьезными последствиями: существенным увеличением сетевого трафика, риском потери критически важной электронной корреспонденции, значительными временными и денежными потерями, риском осуществления мошенничества и психологическим дискомфортом. Вдобавок спам все чаще и чаще используется для рассылки вредоносных кодов, что значительно повышает риски заражения ИТ-инфраструктуры.

По сведениям "Лаборатории Касперского" и компании "Ашманов и партнеры" за прошедший год ущерб от спама для мировой экономики составил 20,5 млрд. долл. США, а к 2007 г. суммарные потери составят 198 млрд. долл. США. Если же рассмотреть структуру этих издержек, то ежегодный ущерб от спама в России составит 100...150 млн. долл. США. Другими словами, в расчете на одного офисного сотрудника российские компании теряют 50...200 долл. США в год.

Спам – это бизнес, который растет небывалыми темпами. Его ежегодный объем составляет 1...3 млрд. долл. США в мире и 2...3 млн. долл. США в России. Преступники, рассылающие спам, уже давно научились выявлять целевые группы получателей, поэтому в российском сегменте Internet подавляющее большинство писем является русскоязычным спамом. Вследствие этого сказывается чрезвычайно низкая эффективность фильтров нежелательной корреспонденции, поставляемых западными компаниями. В них не предусмотрены дополнительные алгоритмы для анализа сообщений на русском языке, а общие методы типа анализа формальных атрибутов письма и черные списки являются крайне неэффективными, когда используются автономно.

Комплексный подход к обеспечению ИТ-безопасности должен предполагать наличие среди компо-

нентов решения тех, что отвечают за фильтрацию спама и возможность централизованного управления этим процессом. Более того, новые компоненты комплексного решения должны быть интегрированы с уже развернутыми средствами ИТ-безопасности так, чтобы не вызывать конфликтов и потери производительности сетевых ресурсов.

Пожелания заказчика

Некоторые поставщики комплексных решений в сфере ИТ-безопасности работают со своими клиентами на равных. Это значит, что заказчики могут не только внедрить разработанные поставщиком компоненты и средства, но и попросить компанию-поставщика разработать какой-либо дополнительный модуль, специфичный для ИТ-инфраструктуры или бизнес-профиля заказчика. В этом случае требования к новому компоненту предъявляет уже не сам разработчик, исходя из собственного анализа, а клиент, который хотя бы примерно представляет, где и как он собирается эксплуатировать новый модуль. Поставщик же не только создает с нуля дополнительное решение, но и обеспечивает его интеграцию в ИТ-инфраструктуру клиента, добавляет необходимую функциональность в средство централизованного управления уже развернутого комплексного решения и оказывает сопроводительные услуги, которые могут потребоваться заказчику.

Именно так развивались события с антивирусной проверкой трафика, проходящего через корпоративные межсетевые экраны, в ИТ-инфраструктуре Министерства Транспорта РФ. Чтобы повысить надежность и производительность антивирусной защиты, Министерство решило осуществлять антивирусную фильтрацию трафика на уровне брандмауэра Microsoft ISA Server. К этому моменту Минтранс уже являлся пользователем Kaspersky Corporate Suite, комплексного решения "Лаборатории Касперского", и обратился за помощью к поставщику, с которым уже давно и плодотворно сотрудничал. По запросу министерства "Лаборатория Касперского" разработала дополнительный компонент, который интегрируется в межсетевой экран Microsoft и защищает корпоративную сеть от вредоносных кодов. Внедрение и тестирование нового модуля в ИТ-инфраструктуре Минтранса доказало, что этот компонент комплексного решения удовлетворяет всем предъявляемым требованиям.

Таким образом, можно резюмировать, что важным преимуществом комплексного решения (помимо всесторонности, управляемости и сопроводительных услуг) является уверенность заказчика в том, что его ИТ-инфраструктура будет защищена от самых последних угроз в будущем. В рамках технической поддержки и мощного сопровождения поставщик комплексного решения поможет решить все возникающие проблемы.

На чем остановить свой выбор?

Сегодня очень сложно дать общие рекомендации по обеспечению корпоративной ИТ-безопасности и внедрению тех или иных средств. Дело в том, что у каждой компании уже существует собственная ИТ-инфраструктура, а каждый случай обладает своей бизнес-спецификой. Тем не менее, крупным и средним компаниям следует остановить свой выбор на комплексном и настраиваемом решении, которое позволит всесторонне защититься от всех современных угроз (вредоносных кодов, сетевых атак и спама), обеспечить высокую степень интеграции в уже развернутую ИТ-инфраструктуру, а также централизованные средства управления и обновления вместе с комплексом сопутствующих услуг.

При выборе поставщика необходимо руководствоваться такими параметрами, как опыт компании-кандидата в разработке и внедрении решений для данной отрасли, комплексность предлагаемого решения, поддержка и сопровождение уже внедренного продукта. Вся эта информация доступна в сети Internet и может быть предоставлена любым поставщиком по первому требованию.

Таким образом, обеспечение эффективной ИТ-безопасности зависит от правильности выбираемой стратегии. Делая ставку на комплексный и всесторонний продукт, проиграть невозможно ни сейчас, ни в будущем.

Доля Алексей Владимирович – IT-специалист "Лаборатории Касперского".
Контактные телефоны: (095) 780-33-69, 797-87-00. Http:// www.kaspersky.com

БИБЛИОТЕКА

ТЕКУЩЕЕ СОСТОЯНИЕ РЫНКА СНГ В ОБЛАСТИ ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ АВТОМАТИЗАЦИИ И РАЦИОНАЛЬНЫЙ ВЫБОР СРЕДСТВ ДЛЯ КОНКРЕТНОГО ОБЪЕКТА

Под редакцией зав. лаб. методов автоматизации производства Института Проблем Управления РАН Э.Л. Ицковича.

Объективные описания, анализ и сопоставление важнейших показателей средств отечественных и зарубежных производителей в обзорах:

Выпуск 1. "Программы связи операторов с ПТК (SCADA-программы) на рынке СНГ", Версия 8, 2004 г.;

Выпуск 2. "Микропроцессорные программно-технические комплексы (ПТК) отечественных фирм", Версия 7, 2004 г.;

Выпуск 3. "Сетевые комплексы контроллеров зарубежных фирм на рынке СНГ"", Версия 3, 2005 г.;

Выпуск 4. "Микропроцессорные распределенные системы управления на рынке СНГ", Версия 4. 2005 г.;

Выпуск 5. "Перспективные программные и технические средства автоматизации: их стандартизация, свойства, характеристики, эффективность эксплуатации", Версия 3, 2004 г.;

Конкурсный выбор средств и систем под конкретные требования:

"Методика проведения конкурса" с приложением программы "Вычисление общей ранжировки конкурсных заявок и анализ работы экспертов". Версия 2. 2004 г.

Справки по приобретению любой из перечисленных работ можно получить у Э.Л. Ицковича по тел. и факсу (095) 334-90-21, по E-mail: itskov@ipu.rssi.ru