Антивирусная безопасность и защита данных в ИТ компании

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Так постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации, формируются рекомендации по защите информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах.

Что же такое «защита информации от несанкционированного доступа» или информационная безопасность?

Под информационной безопасностью (информационной системы) подразумевается техника защиты информации от преднамеренного или случайного несанкционированного доступа и нанесения тем самым вреда нормальному процессу документооборота и обмена данными в системе, а также хищения, модификации и уничтожения информации.

Другими словами вопросы защиты информации и защиты информации в информационных системах решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Под фразой «угрозы безопасности информационных систем» понимаются реальные или потенциально возможные действия или события, которые способны исказить хранящиеся в информационной системе данные, уничтожить их или использовать в каких-либо целях, не предусмотренных регламентом заранее.

Первое разделение угрозы безопасности информационных систем на виды.

Если взять модель, описывающую любую управляемую информационную систему, можно предположить, что возмущающее воздействие на нее может быть случайным. Именно поэтому, рассматривая угрозы безопасности информационных систем, следует сразу выделить преднамеренные и случайные возмущающие воздействия.

Комплекс защиты информации может быть выведен из строя, например из-за дефектов аппаратных средств. Также вопросы защиты информации встают ребром благодаря неверным действиям персонала, имеющего непосредственный доступ к базам данных, что влечет за собой снижение эффективности защиты информации при любых других благоприятных условиях проведения мероприятия по защите информации. Кроме этого в программном обеспечении могут возникать непреднамеренные ошибки и другие сбои информационной системы. Все это негативно влияет на эффективность защиты информации любого вида информационной

безопасности, который существует и используется в информационных системах.

В этом разделе рассматривается умышленная угроза защиты информации, которая отличается от случайной угрозы защиты информации тем, что злоумышленник нацелен на нанесение ущерба системе и ее пользователям, и зачастую угрозы безопасности информационных систем – это не что иное, как попытки получения личной выгоды от владения конфиденциальной информацией.

Для предотвращеия утечки информации необходимо регулярное изменение паролей доступа на всех компьютерах. Однако такую операцию производить каждый раз на сотнях машин просто невозможно. Даже если сменить пароль на всех компьютерах, то после этого необходимо сообщить всем заинтересованным лицам о новых паролях. Хотя этот метод и решит проблему,он доставит множество неудобств.

Второй метод - изменение подхода к самому средству удаленного управления. Сотрудникам, работающим через программу удаленного управления, не предоставляется пароль в открытом виде. Однако, большинству программ требуется пароль в открытом виде, поэтому можно воспользоваться дополнительными разработками или другой программой удаленного администрирования. Но и в этом случае есть один очень неприятный момент - большинство программ предоставляет возможность экспортировать адресную книгу со всеми настройками в виде файла и потом загрузить ее на другом компьютере. Чтобы полностью исключить возможность проникновения необходимо в качестве профилактики регулярно менять основные пароли доступа (рисунок 1.1).

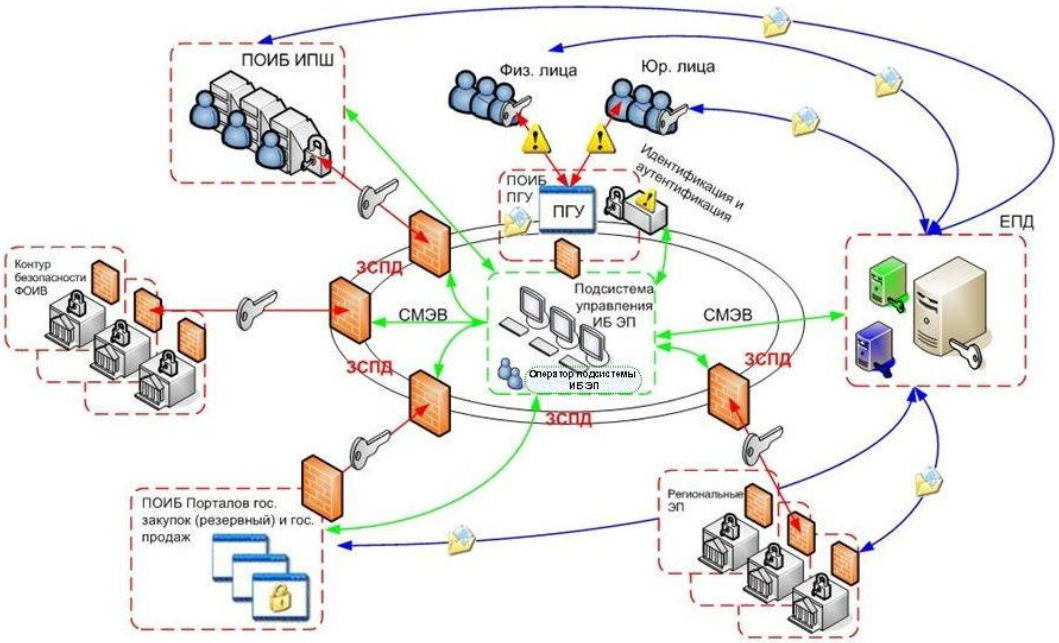

Рисунок 1.1–Схема защиты данных в Ит компании

Антивирусная безопасность

Зависимость предприятий от компьютерных и сетевых коммуникаций неуклонно возрастает. Этот факт в значительной степени увеличивает их уязвимость с точки зрения нарушения информационной защиты. Последствия вторжения вирусов различны: наносят материальный ущерб, снижают престиж предприятия, приводят к прекращению его работоспособности.

Кроме того, важно помнить, что многие виды информации сами по себе должны находиться под защитой закона. Это могут быть персональные данные клиентов, которые не хотят, чтобы их личная информация выходила за пределы компании, финансовая информация, номера кредитных карт, банковских счетов и т.п.

Пути проникновения вирусов в информационную инфраструктуру предприятия различны и зависят от типа вируса, политики безопасности предприятия и ряда внешних факторов.

Сетевые черви распространяют свои копии по локальным и глобальным сетям связи через электронную почту, программы типа icq, через файлообменные, локальные и беспроводные сети. Получить их можно в виде вложения в электронном письме, ссылки на заражённый файл, в мгновенных сообщениях. Цель подобных программ – захват удаленного компьютера и распространение на нем.

Классические компьютерные вирусы, копирующиеся на локальный диск и реагирующие на определенное действие пользователя, не используют сетевых сервисов для проникновения на другие компьютеры. Вирус передаётся через общие для разных компьютеров ресурсы — данные на дисках, дискетах, флэшках, через общие ресурсы сети, через электронные письма с заражёнными файлами.

Троянские программы под видом «полезного приложения» осуществляют несанкционированный захват и передачу данных их создателю. Они также распространяются через электронную почту.

Кроме того, в значительной степени затрудняют работу компьютера хакерские утилиты и прочие вредоносные программы — конструкторы вирусов, червей и троянов, хакерские утилиты скрытия кода от антивируса, программы-спамеры, рекламные агенты, программы-шпионы и многие другие.

Как бы ни хороша была антивирусная программа, без дополнительных мер она малоэффективна. Чтобы защита была действительно эффективной, необходимо всегда знать, откуда может прийти вирус, как с ним бороться или, по крайней мере, как его задержать, и как устранить последствия с

минимумом потерь для предприятия. Все эти меры можно реализовать при наличии трех грамотно построенных и взаимодействующих систем:

- нормативно-методическая: работает над созданием правовой базы предприятия в области защиты от вирусных угроз (политика безопасности, инструкции, регламенты, требования, должностные инструкции);

- кадровая. Предприятие должно заботиться о том, чтобы работники представляли как теоретические, так и практические аспекты антивирусной защиты. Если, не представляют – нужно научить.

- технологическая. К технике требования должны быть высокие: помимо вирусов, нужно защищаться от спама, обеспечивать обнаружение и предотвращение атак, выявление уязвимостей, сетевое экранирование, резервное копирование и подсистему управления.

Можно выделить ряд основных объектов, которые необходимо защищать от вирусов. В первую очередь это рабочие станции, различные серверы (Web-приложений, файловые серверы, серверы документооборота и т.д.), интернет-шлюзы, почтовые серверы. Качественная и бесперебойная работа предприятия зависит от уровня защищенности каждого из этих объектов. Специфика их защиты имеет свои особенности.

Важным аспектом информационной безопасности предприятия является централизованная защита рабочих станций в корпоративной сети и за ее пределами от интернет-угроз: вирусов, шпионских программ, хакерских атак и спама. Контроль всех входящих и исходящих потоков данных на компьютере (электронная почта, интернет-трафик и сетевые взаимодействия) гарантирует безопасность пользователя, где бы он ни находился — в офисе, у клиента или в командировке. Для этого оптимальным решением являются различные антивирусные и антиспамовые программы в сочетании с межсетевым экранированием. Обязательными свойствами этих программ

должны быть централизованное управление, защита и отслеживание атак в реальном времени, регистрация и протоколирование всех системных событий и сетевой активности, включая информацию об исполнителе, аутентификация и идентификация пользователей (желательно гарантированная), разграничение доступа к ресурсам рабочей станции.

Защита файловых серверов осуществляется с помощью антивирусных мониторов, способных автоматически проверять все файлы сервера, к которым идет обращение по сети. Антивирусы, предназначенные для защиты файловых серверов, выпускают все антивирусные компании.

Серверы систем документооборота хранят документы в базах данных собственного формата. Существует ряд антивирусных программ, специально предназначенных для антивирусной защиты подобных систем. Они сканируют почту и файлы вложений, удаляя в реальном времени все вредоносные программы, обнаруживают макрокомандные вирусы и троянские программы в формах и макросах, в файлах сценариев и в объектах OLE. Проверка выполняется в режиме реального времени, а также по требованию.

Для защиты корпоративных Web-ресурсов (Интранет-сайта и любого приложения компании, работающего по http-протоколу) требуются специальные средства защиты при работе удаленных пользователей с Web-приложениями по криптографическому SSL-протоколу. Подсистема защиты Web-ресурсов должна обеспечивать «единую точку входа» к приложениям, интегрированный контроль доступа к корпоративным Web-ресурсам, защиту клиентских браузеров.

Основное решение — использование специальных антивирусов для шлюзов. Они реализуют первый уровень защиты на пути проникновения вирусов в сеть организации. Антивирус для шлюзов более эффективен и даже

необходим при защите крупных сетей. В малых сетях его относительная полезность в обеспечении общей безопасности несколько ниже.

Антивирус для шлюза должен:

- проверять интернет-трафик в режиме реального времени;

- отслеживать и удалять вредоносные и потенциально опасные программ из потока данных, поступающего в сеть по протоколам HTTP/FTP;

- фильтровать интернет-трафик по спискам доверенных серверов, типам объектов и группам пользователей.

Решать такую задачу можно двумя путями. Первый путь — разрабатывать с нуля систему обработки сетевых потоков, анализа пакетов, чтобы к этой системе можно было применить уже готовое антивирусное ядро и организовать проверку проходящего трафика. Этот путь требует значительных затрат на пути реализации. В то же время, существует достаточное количество решений, предназначенных исключительно для обработки трафика, анализа и маршрутизации пакетов — это брандмауэры и прокси-сервера. Поэтому второй путь состоит в интеграции антивирусного решения с брандмауэром или прокси-сервером для проверки проходящего трафика.

Электронная почта — удобное и незаменимое средство делового общения. Однако посредством электронной почты распространяется большая часть вирусов и спама, она может быть каналом утечки конфиденциальных данных.

Антивирусные мониторы неэффективны для обнаружения вирусов в почтовых сообщениях. Для этого необходимы специальные антивирусы, способные фильтровать трафик SMTP, POP3 и IMAP, исключая попадание зараженных сообщений на рабочие станции пользователей.

Для защиты почтовых серверов можно приобрести антивирусы, специально предназначенные для проверки почтового трафика, или подключить к почтовому серверу обычные антивирусы, допускающие работу в режиме командной строки[14].

Всего за несколько лет спам превратился из легкого раздражающего фактора в одну из самых серьезных угроз информационной безопасности. Непрошеные почтовые сообщения переполняют индивидуальные почтовые ящики и парализуют работу корпоративных серверов. Время, которое сотрудники вынуждены тратить на разбор и чтение спама, постоянно растет — а с ним и финансовые потери компаний.

За последние годы было изобретено немало способов борьбы со спамом. Принципиально новый подход к фильтрации спама основан на технологии «Спамтест». Ее главными компонентами являются эвристические лингвистические алгоритмы нового поколения. Новые средства фильтрации нежелательной почты дополняются уже известными механизмами, отсеивающими спам по формальным признакам. Для защиты от спама используются программы-антиспамеры, реализующие функции проверки сообщений по спискам, фильтрацию с учетом авторизации отправителя, анализ формальных признаков письма, сигнатурный анализ с использованием круглосуточно обновляемой базы лексических сигнатур, проверку с использованием методов лингвистической эвристики.

Единой стратегии защиты, пригодной для всех компаний сразу, нет и быть не может. У каждого предприятия бизнес устроен по-своему, а следовательно и риски свои — специфические. Значение имеет уровень информатизации компании. Чем больше в бизнес-процессах используются информационные технологии, тем больше их уязвимость.

Для крупных компаний, как правило, строится стратегия защиты от вирусов предполагающая активные действия ИТ-персонала, т. е. необходимо ее сопровождение силами квалифицированных специалистов.

Для малого и среднего бизнеса такой подход, к сожалению, неприменим. Дело в том, что в компаниях небольшого масштаба обычно нет выделенных ИТ-специалистов. Поэтому основными чертами антивирусной защиты в данном случае являются по возможности нулевое администрирование, универсальность внедряемого программного продукта, который защищает сразу все основные точки проникновения вредоносного кода и автоматизация всех этапов работы системы.