6. *Браиловский Н.Н., Марковский А.Р., Хорошко В.А., Чирков Д.В.* Оценка времени задержки пакетов в каналах передачи данных борт-земля-борт // Зб. наук. праць ІПМЕ НАН України "Моделювання та інформаційні технології", 1999.-Вип. 2.-С.95-100.

7. *Кудинов В.А., Пархуць Л.Т., Плус Д.В., Хорошко В.А.* Оценка эффективности алгоритмов коммутации пакетов сообщений в распределенной информационной сети // Захист інформації.-2004.-Спец. випуск.-С.36-40.

8. *Месарович М., Такахара Я.* Общая теория систем: математические основы.-М.: Мир, 1978.-312 с.

9. *Браіловський М.М., Олешко Т.І., Хорошко В.О.* Проектування інформаційних мереж.-Матеріали 5-ої МНТК "АВІА-2003", Київ.-С.125-128.

10. *Прим Р.* Кратчайшие связывающие сети и некоторые обобщения // Кибернетический сборник: Вып.2.-М.: Изд-во иностр. лит., 1961.-С.95-107.

11. *Кудінов В.А., Хорошко В.О.* Корпоративна мережа ОВС України та моделі її захисту від порушників безпеки // Захист інформації.-2004.-№1.-С.26-36.

12. *Ковалева Ю.Е., Олешко Т.И., Хорошко В.А.* Проектирование корпоративных вычислительных сетей // Захист інформації.-2003.-№2.-С.4-14.

13. *Моржов С.В., Хорошко В.А.* Применение сетей Петри для моделирования параллельных процессов // Проблемы управления и информатики.-2004.-№2.-С.86-94.

Поступила 27.10.2004г.

УДК 004.056.52 (045)

Сорокопуд С.А.,Мудрова Л.В., Ширяев С.В.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

В настоящее время невозможно оставить незамеченным влияние на все сферы человеческой деятельности стремительного развития информационных технологий, наиболее перспективным направлением применения которых является бизнес. Появившиеся технологические возможности облегчают информационный обмен, повышают эффективность производственных процессов, способствуют расширению деловых операций. Повышают эффективность бизнеса корпоративные информационные системы путем качественного и оперативного управления бизнес-процессами. Целью построения системы защиты корпоративной сети предприятия является установление баланса между стоимостью системы защиты и возможными убытками, который сопровождается снижением количества уязвимостей, уменьшением риска и сохранением ресурсов. Изначально необходимо определить угрозы, которым может подвергнуться корпоративная сеть предприятия.

Возможности общесистемного и прикладного программного или аппаратного обеспечения часто используются злоумышленником для осуществления соответствующей атаки. Основные атаки:

использование чужого идентификатора;
несанкционированный доступ к электронной почте;
несанкционированный доступ к программному обеспечению www;
внедрение вредоносного программного обеспечения;
злоупотребление системными ресурсами;
отказ от авторства;
отказ в обслуживании;
ошибки при маршрутизации;

снижение эффективности работы сети;
атаки на уровне TCP (Transport Control Protocol);
анализ сетевого трафика;
атаки на межсетевые экраны и системы обнаружения атак;
атаки на VPN (Virtual Private Network);
промышленный шпионаж;
уволенные или недовольные сотрудники, имеющие права доступа к конфиденциальной информации;
низкая квалификация кадров;
халатность кадров.

Угроза «использование чужого идентификатора», то есть подмена доверенного лица или субъекта корпоративной сети реализуется злоумышленником передачей по каналам связи сообщений от имени санкционированного объекта или субъекта данной сети с целью идентификации. Эта атака является активной с нарушением конфиденциальности и целостности информации. Может быть внутрисегментной и межсегментной, с обратной связью с атакующим объектом или без нее. Осуществляется на канальном, сетевом, транспортном уровнях модели OSI. При установленном виртуальном соединении злоумышленник с целью ведения сеанса работы с объектом системы от имени доверенного субъекта присваивает права последнего путем передачи пакетов обмена с атакующего объекта на цель атаки от имени доверенного субъекта взаимодействия. Атака без установленного виртуального соединения подразумевает передачу служебных сообщений от имени сетевых управляющих устройств.

Атака «несанкционированный доступ к электронной почте» реализуется несанкционированным использованием SMTP-серверов или перехватом электронной почты. Первый вариант становится возможным при некорректной настройке программ – серверов SMTP. Второй вариант может быть достигнут атакующим объектом в результате выполнения одного из следующих действий: чтение разделов жесткого диска на нижнем уровне; модификация конфигурационных файлов SMTP-серверов или POP-сервера; взлом паролей доступа к почтовым ресурсам.

Атака «несанкционированный доступ к программному обеспечению www», то есть нештатное использование программ-броузеров HTML-страниц www и/или использование программ, которые расширяют возможности броузеров, может быть реализована интерпретаторами языка Postscript; нецензурными изображениями; паразитным сетевым трафиком; несанкционированным использованием броузеров Java; непрямым воздействием на объекты; несанкционированным доступом посредством броузера; переполнением буфера с разрушением области кодов; использованием люков в интерфейсе CGI. Рассмотрим подробнее каждый из методов реализации. Поскольку Postscript поддерживает команды создания, удаления, копирования, переименование файла, Postscript-файлы могут перезаписывать ключевые файлы системы. С помощью Postscript возможно несанкционированное внедрение программного продукта. А также организация несанкционированной передачи данных, созданием Postscript-программы, интегрированной в печатаемом или отображаемом на экране файле, которая передает информацию с атакуемого объекта с запущенным броузером на атакующий объект через порт 80. Отвлечение сотрудников от своих обязанностей происходит с помощью нецензурных изображений. Реализация последних атакующим объектом может происходить путем интеграции в текстовые документы нецензурных изображений в Postscript-файлах; путем навязывания нецензурных изображений в GIF-файлах, которые, как известно, отображаются сразу после загрузки; путем подмены документов сервера нецензурными изображениями. Паразитный сетевой трафик атакующая сторона реализовывает с помощью HTML-документов, которые содержат предложение торговли; дезинформации за счет помещения соответствующих документов и подмены ссылок на серверы, которые содержат подтверждение данной информации; развлекательных серверов и сетевых игр; загрузки из сети исполняемых

программ; создания бесконечных циклов загрузки документов, используя особенность протокола HTTP. Несанкционированное использование броузеров Java подразумевает внедрение программ, выполняющих несанкционированные действия; внедрение вирусов; передачу в сеть данных атакуемого объекта; перенаправление маршрута передачи запросов таким образом, чтобы они проходили через атакующий объект; загрузку канала передачи данных бесполезным трафиком; перенаправление всего сетевого трафика таким образом, чтобы он проходит через атакующий объект; подмену внутренних потоков данных передачей информации через внешние машины; сбор статистики об использовании систем; проверку текущих задач пользователя; перехват номеров кредитных карточек. При помощи непрямого воздействия на подсознание объекта по средствам www у объекта появляется склонность к покупкам или продаже вещей, материальных средств, также легко узнать его распорядок дня путем проведения опросов, анкетирования. Несанкционированный доступ по средствам броузера подразумевает реализацию таких атак, как подделка исходящего адреса электронной почты; выведение из строя броузера с помощью аномально длинного URL; рассылка нецензурных материалов через глобальные списки рассылки. Использование люков в интерфейсе CGI позволяет атакующему объекту получить список пользователя сервера; получить личные ключи; перехватить номера кредитных карточек; сформировать подложные заказы; саботировать процесс прохождения заказов.

Под атакой «внедрение вредоносного программного обеспечения» подразумевается внедрение программ типа «троянский конь», которые незаметно для пользователя выполняют множество функций (перехват ввода с клавиатуры и кража паролей, удаленное управление узлом и т. д.), мобильного кода, вирусов. При помощи мобильных кодов, точнее апплетов Java, управляющих элементов ActiveX или сценариев JavaScript, атакующий объект может модифицировать информацию как при передачи ее по сети, так и в процессе обработки и хранения ее на атакуемом объекте; нарушить конфиденциальность информации; нарушить работоспособность компьютера; несанкционированно использовать ресурсы компьютера и т. д.

Осуществить атаку «отказ от авторства» можно передачей на атакуемый объект бесконечного числа анонимных запросов на подключение от имени других объектов, числом на несколько порядков меньше пропускной способности канала («мини-шторм») или передачей с одного адреса столько запросов на атакуемый объект, сколько позволит трафик («шторм»). Данная атака является активной с целью нарушения работоспособности системы. Может быть единонаправленной межсегментной, внутрисегментной на канальном, сетевом, транспортном уровнях модели OSI.

Атаки на отказ могут классифицироваться следующим образом: сетевые DOS-атаки; распределенные сетевые DOS-атаки. В результате осуществления атаки первого класса блокируется соединение хоста жертвы. Объектами данных атак являются любой основной сетевой сервис атакуемой системы, который отвечает за обработку входящего и исходящего трафика прикладных сервисов и программ; маршрутизатор; канал связи «атакуемый объект – маршрутизатор». Нарушается целостность и адекватность одного из объектов. Распределенные сетевые DOS-атаки отличаются от сетевых DOS-атак тем, что инициаторов атаки может быть несколько, также в атаку может быть вовлечено большое количество топологических промежуточных хостов.

Угроза «ошибки при маршрутизации» реализуется внедрением в корпоративную сеть ложного объекта. Первый способ – путем навязывания ложного маршрута – это фактически посылка по сети служебной информации протоколами управления сетью (RIP (Routing Internet Protocol), OSPF (Open Shortest Path First), ICMP (Internet Control Message Protocol), SNMP (Simple Network Management Protocol)) от имени сетевых управляющих устройств с целью изменения таблиц маршрутизации. Это активная атака, преследующая цель либо нарушить конфиденциальность информации или ресурсов системы, либо работоспособность системы. Может осуществляться в одном сегменте или межсегментно с обратной связью или без нее на канальном, сетевом, транспортном уровнях модели OSI. Второй способ – путем

использования недостатков алгоритмов удаленного поиска. Осуществляется перехватом поискового запроса и последующей передачей ложного ответа с данными адресации на атакующий объект или периодической передачей на атакуемый объект подготовленного заранее ложного ответа без перехвата поискового запроса. Данная атака является активной и преследует цель нарушения конфиденциальности и целостности информации. Может быть внутрисегментной или межсегментной с обратной связью на канальном, сетевом, транспортном уровнях модели OSI. Контроль потока информации между объектами дает возможность атакующему объекту проводить селекцию потока информации и сохранять ее на ложном объекте корпоративной сети, модифицировать передаваемые данные, передаваемый код, внедрением разрушающих программных средств или изменением логики работы исполняемого файла, подменять информацию.

Атака «снижение эффективности работы сети» основывается на особенностях протоколов TCP и IP. Она реализуется атакующим объектом путем выведения из строя серверов сети Интернет, использования особенностей маршрутизации пакетов TCP/IP, создания скрытых каналов передачи данных, деградации пропускной способности каналов передачи данных. Вывести из строя сервера сети Интернет можно перегрузкой серверов незавершенными процессами установки соединений, превышением временных ограничений на открытие TCP - соединений, переполнением системного журнала, пересылкой файлов, которые приводят к краху программ-броузеров, использованием некорректного кода сетевых программ. Использовать особенности маршрутизации пакетов TCP/IP атакующий объект может с целью подмены URL-адресов для перенаправления запросов или записи всех транзакций конечного пользователя с целью заочного изучения. Создание скрытых каналов передачи данных подразумевает передачу программ, создающих скрытый канал обмена сквозь firewall через порт 80. Деградация пропускной способности каналов передачи данных подразумевает передачу бессмысленных огромных файлов по низкоскоростным каналам.

Атаки на TCP могут быть пассивными и активными. Пассивные атаки сводятся к наблюдению за доступными данными и сессиями. Реализация активных атак может осуществляться перехватом и модификацией сетевого потока, попытками выдать себя за другую систему или лишить работоспособности атакуемый объект. Основное в активных атаках -- это возможность формировать произвольные IP-пакеты.

Атака «анализ сетевого трафика» заключается в прослушивании канала связи. Анализ сетевого трафика – пассивное воздействие. Если данная атака осуществляется без обратной связи, то нарушается конфиденциальность информации внутри одного сегмента сети на канальном уровне модели OSI. Перехватывая и анализируя пакеты обмена на канальном уровне атакующий объект получить однозначное соответствие событий, которые происходят в системе, и команд, которые пересылают друг другу ее объекты, в момент появления этих событий. Также атакующий объект удаленно получает несанкционированный доступ к информации, обмениваемой двумя сетевыми абонентами между собой.

Атаки на межсетевые экраны можно классифицировать так: атаки вследствие неправильной конфигурации межсетевого экрана; атаки в обход межсетевого экрана; атаки через туннели, возникшие вследствие свойств многих сетевых протоколов, в межсетевом экране; атаки из доверенных узлов и сетей; атаки путем подмены адреса источника, то есть скрытие реального адреса атакующего объекта; атаки на сам межсетевой экран; атаки на подсистему аутентификации межсетевого экрана. Атаки на системы обнаружения атак: ослепление датчика путем высокой загрузки сети; отказ в обслуживании – это атаки на перегрузку или на отказ; простые и сложные уклонения, вводящие в заблуждение системы обнаружения атак.

Атаки на VPN можно классифицировать следующим образом: атаки на криптографические алгоритмы (DES, TripleDES, RSA, AES, ГОСТ 28147-89); атаки на криптографические ключи; атаки на датчики случайных чисел; атаки на протоколы VPN; атаки на протоколы аутентификации; атаки на реализацию; атаки на оборудование VPN; атаки на операционные системы; атаки на пользователей. Необходимо помнить, что

причинами появления возможности осуществления вышеперечисленных атак являются неправильная реализация и неправильная эксплуатация средств VPN.

Организационные методы играют значительную роль в процессе обеспечения безопасности корпоративной сети предприятия. Под организационными методами защиты информации подразумевается регламентация деятельности предприятия и взаимосвязь исполнителей на нормативно-правовой основе. Организационная защита обеспечивается благодаря сформированной комплексной системе организационно-распорядительных документов относительно защиты информации корпоративной сети предприятия.

Однако перед тем, как подходить непосредственно к созданию нормативно-правовой основы обеспечения информационной безопасности, Вам будет необходимо исследовать информационную структуру предприятия, в состав которой входят не только информационные потоки и используемые сетевые протоколы, но и топология сети, ее сетевое оборудование и программное обеспечение. На основе исследования строится схема информационной структуры предприятия с четкой градацией сегментов и потоков требующих и не требующих защиты. И только теперь, когда Вы точно знаете, что нужно защищать и почему именно это должно быть защищено, разрабатывается концепция защиты информации.

Концепция защиты информации – это систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности. Данный документ должен включать в себя общее описание объекта защиты; цели создания системы защиты и ее задания; правовое обеспечение вопросов защиты информации; модель возможных угроз информационной безопасности и пути их реализации; направления обеспечения безопасности корпоративной сети предприятия; принципы, методы, средства построения системы защиты, которые не влияют с отрицательной стороны на информационную среду и экономически обоснованы; требования класса защищенности корпоративной сети.

Следующим шагом по организационному обеспечению информационной безопасности после создания концепции защиты информации является разработка комплекта нормативно-методических документов, содержание которых вкратце изложено ниже.

В плане защиты от несанкционированного доступа к информации и в процесс функционирования корпоративной сети необходимо рассмотреть цели, задания системы защиты и пути их достижения; требования по проведению работ относительно защиты информации; описание использованных методов и средств защиты информации и требований предоставленных ними; разделение ответственности за реализацию защиты информации.

Положение про категоризацию ресурсов должно раскрывать цели введения категоризации ресурсов; критерии категоризации ресурсов по степени защищенности; пример формуляра компьютерной системы и функциональных задач, которые она решает, для отчетности необходимой степени защищенности.

Документ «Порядок обращения к информации, подлежащей защите» должен четко определить виды информационных ресурсов, подлежащих защите; вопросы отчетности, хранения и уничтожения документов и носителей с конфиденциальной информацией; порядок передачи конфиденциальной информации третьим лицам; ответственность за нарушение вышеуказанного в данном пункте; форму договора о соблюдении порядка обращения к информации, подлежащей защите.

План обеспечения бесперебойной работы корпоративной сети и ее восстановления должен состоять из таких пунктов: общие положения; классификация возможных кризисных ситуаций; методы и средства обеспечения бесперебойной работы сети и восстановление ее работоспособности, и требования к ним; порядок действий и обязанности персонала относительно организации бесперебойной работы и восстановление работоспособности корпоративной сети.

Положение про отдел технической защиты информации акцентирует внимание на общих положениях; руководстве отдела; заданиях и функциях отдела; правах и обязанностях как сотрудников, так и руководства отдела.

Документ «Обязанности администратора информационной безопасности» должен определять права и обязанности по поддержке режима безопасности и ответственность за реализацию безопасности.

Памятка пользователю корпоративной сети определяет обязанности сотрудников при работе в ней и ответственность за нарушение установленных порядков.

Инструкция внесения изменений в списки пользователей раскрывает процедуру регистрации или изменения прав доступа пользователей к ресурсам корпоративной сети.

Инструкция модификации технических и программных средств описывает взаимодействие отделов предприятия относительно его защиты при модификации технических и программных средств.

Инструкция о порядке установления, хранения, использования и изменения паролей пользователей корпоративной сети раскрывает вопросы обеспечения процессов генерации, изменения и остановки действия паролей и определяет ответственность за неисполнение данной инструкции.

Положение об антивирусной защите информации в компьютерных системах включает в себя требования по покупке и установке антивирусного программного обеспечения, его порядок использования; разделение ответственности за проведение антивирусного контроля.

Инструкция по работе с ключевыми дискетами (ключами электронной цифровой подписи, шифрования) состоит из таких пунктов, как порядок создания, работы, хранения и уничтожения ключевых дискет; обязанности и ответственность сотрудников по использованию и хранению ключевой информации; форма журнала отчетности ключевых дискет; порядок действий сотрудников в случае нарушения вышеуказанного.

Правила безопасности в Интернет должны раскрыть обязанности администратора, пользователей; определить правила работы в www, ответственность за приложения, ключевые положения про виртуальные частные сети, правила применения средств контроля.

Правила безопасности электронной почты включают вопросы содержания сообщений, цели пользования электронной почтой, администрирования электронной почты, порядок использования электронной почты для обмена конфиденциальной информацией.

Технические средства защиты служат для перекрытия недостатков организационных мер. Технические средства защиты включают в себя штатные средства защиты операционных систем; антивирусное обеспечение корпоративной сети; криптографические и стенографические методы защиты информации; аппаратные и программные межсетевые экраны; системы контроля содержания; системы построения VPN; системы обнаружения атак; обманные системы; системы контроля целостности.

Штатными средствами защиты операционных систем

Встроенные средства защиты многопользовательской мультизадачной операционной системы Unix включают в себя:

многопользовательский режим со средствами защиты данных от несанкционированного доступа;

идентификация и аутентификация пользователей, подключающихся к системе (проводится по парольной схеме, определяется уникальный идентификатор пользователя и идентификатор его группы; длина пароля ограничивается 8 символами; пароль шифруется с помощью алгоритма DES);

система разграничения доступа к файлам (иерархическая файловая система (обычные, каталоги, специальные файлы), образующая единое дерево каталогов независимо от количества физических устройств, используемых для размещения файлов; файловая система принимает решение про доступ к файлу на основе индексного дескриптора, основным элементом которого является список контроля доступа к файлу, состоящий из трех полей:

владелец, группа, другие; для исполнения привилегированных заданий используется механизм установки идентификатора пользователя);

журналы регистрации событий, которые регистрируют информацию про последние удачное подключение пользователя (сохраняется в файле /usr/adm/lastlog), про активных пользователей системы (сохраняется в файле /etc/utmp), про время подключения пользователя к системе и отключения от нее (сохраняется в файле /usr/adm/wtmp), про каждую команду, которая исполнялась в системе, с указанием того, кто ее запустил и как долго пользовался ею;

сетевая защита;

криптографическая защита файлов.

Операционная система, позволяющая организовывать совместное использование данных и обмен ними в разных вычислительных средах, Novell NetWare владеет такими встроенными средствами защиты как дублирование системных таблиц FAT на НЖМД; верификация чтения после записывания и использования области HotFix; дефрагментация дискового пространства в режиме реального времени; система отслеживания трансакций; использование методов RAID; поддержка UPS; ведение отчетной информации пользователей; защита входа в систему по парольной схеме; атрибуты каталогов, файлов; маски наследования прав; защита между сетями; защита сервера; установка разрешения на загрузку модулей сервера только с каталога SYS:SYSTEM; отключение встроенной системы наладки; запрет на изменение даты и времени сервера.

Самая распространенная операционная система Windows имеет следующие встроенные средства защиты, причем в зависимости от предназначения: Home или Professional заметны весьма значительные отличия. ОС Windows, ориентированные на домашнее использование располагают такими средствами защиты, как личный вход в систему; быстрое переключение пользователей; конфиденциальность личных сведений; брандмауэр подключения к Интернету (только в ОС Windows XP); общие папки документов. А в ОС Windows, ориентированной на профессиональное использование встроенные следующие средства защиты: корпоративная безопасность; контролируемый доступ к сети; простые средства общего доступа; ограничения на пустой пароль; шифрованная файловая система; службы сертификатов; управление учетными данными; быстрое переключение пользователей; конфиденциальность личных сведений; общий доступ к Интернету; брандмауэр интернет-соединения (только в ОС Windows XP); политики ограниченного использования программ; протокол IPSec; поддержка смарт-карт; протокол Kerberos. Подробнее о средствах защиты ОС Windows XP/2000 вы сможете прочитать в статье «Реализация безопасной работы компьютеров под управлением ОС Windows XP/2000», напечатанной в №3 за 2004 год журнала «Бизнес и безопасность».

Антивирусное обеспечение корпоративной сети

На данном этапе времени существует множество таких решений. Выбирать антивирусное обеспечение непосредственно для конкретного предприятия необходимо по таким критериям, как надежность и комфортность работы; качество обнаружения вирусов, в том числе и абсолютно новых; возможность лечения зараженных объектов; существование версий антивируса под все популярные платформы и серверных вёрсий с возможностью администрирования сети; наличие режима «постоянного сканирования»; скорость роботы. Естественно здесь перечислены не все критерии выбора антивирусного обеспечения, но именно эти можно назвать основными.

Криптографические и стеганографические методы защиты информации

Криптографические методы защиты помогают нам решить целый ряд вопросов: аутентификация пользователей системы; закрытие и контроль целостности информации, которая передается каналами связи; закрытие конфиденциальной информации в корпоративной сети предприятия. Недостатки криптографических систем: низкое быстродействие алгоритмов шифрование; трудности с общим использованием зашифрованной информации; высокие требования к сохранности секретного ключа;

трудности при использовании в случае отсутствия средств защиты от несанкционированного доступа.

Для защиты от несанкционированной модификации и установления авторства электронного документа необходимо использовать электронную цифровую подпись.

При выборе криптографических средств защиты определите их соответствие таким требованиям:

читаемость зашифрованного сообщения только при наличии ключа;

число операций определения использованного ключа шифрования должно быть не меньше общего числа возможных ключей;

число операций расшифрования информации путем перебора разных ключей должно выходить за рамки возможностей вычислительной техники;

отсутствие влияния знания алгоритма шифрования на надежность защиты;

незначительное изменение ключа должно привести к существенной модификации зашифрованного сообщения;

неизменность структурных элементов шифрования;

длина зашифрованного текста и длина исходного текста должны быть равны;

простых и легко исчисляемых зависимостей между ключами не должно быть;

алгоритм должен поддерживать как программную, так аппаратную реализацию.

Компьютерная стенография подразумевает под собой скрытие факта существования секретного сообщения путем использования неточностей приборов оцифрования и чрезмерность аналогового видео- или аудиосигнала. Она позволяет решить ряд вопросов: защита конфиденциальной информации от несанкционированного доступа; преодоление систем мониторинга и управление сетевыми ресурсами; маскировка программного обеспечения; защита авторского права на некоторые виды интеллектуальной собственности.

Аппаратные и программные межсетевые экраны

Политика доступа к сетевым сервисам и политика реализации межсетевых экранов – две главные составляющие политики сетевой безопасности предприятия. Основой для политики доступа к сетевым сервисам должен быть баланс между защитой сети предприятия от присущих ей рисков и доступом к сетевым сервисам, который необходим пользователям. Политики доступа к сервисам межсетевого экрана реализуются на основе одного из принципов: запрещая доступ из Интернет во внутреннюю сеть, разрешать доступ из внутренней сети в Интернет; разрешить ограниченный доступ во внутреннюю сеть из Интернет, но при этом обеспечить работу только отдельных систем (например, почтовых серверов). Первый принцип хотя и приносит неудобства пользователям, но делает сеть более защищенной по сравнению с сетью, политика реализации межсетевых экранов которой базируется на втором принципе.

Основные требования к межсетевым экранам следующие: решение требуемой совокупности задач обеспечения безопасности; своевременность, правильность и корректность выполнения всех предусмотренных функций защиты; наличие целенаправленной адаптации; удобство администрирования; минимальность финансовых и ресурсных затрат.

Системы контроля содержания

Системы контроля доступа имеют возможность обнаруживать спам (в некоторых системах создаются списки спамеров и сообщения из этих источников блокируются); анализировать содержания сообщения; обнаруживать подмену адреса; анализировать размеры сообщения и вложения, при этом сообщение, значение размера которого превышает значение, указанное в политике безопасности, отбрасывается или блокируется; обнаруживать вирусы и троянских коней; анализировать передаваемые файлы; анализировать вложения; анализировать скрытые HTML, а потом в зависимости от политики безопасности блокировать или разрешать их; блокировать доступ к определенным URL; анализировать содержание HTML-страниц и блокировать к ним доступ.

Однако следует помнить и о недостатках: невозможность контроля зашифрованных сообщений; трудности с заданием адресов запрещенных страниц.

Системы построения VPN

Реализацию VPN можно свести к двум основным способам: разделение трафика в канале передачи; шифрование трафика в канале передачи. Результатом осуществления технологии разделения трафика в канале передачи являются VLAN (технология виртуальных локальных сетей) или MPLS (технология виртуальных глобальных сетей). Основными задачами VLAN являются структуризация, построенных на базе коммутаторов, локальных сетей и отделение одного типа трафика от другого. Причем, несмотря на то, что кадры внутри одной VLAN передаются на порт, указанный в адресе назначения кадра, смешение данных из разных VLAN невозможно независимо от того, какой адрес канального уровня. Для построения VLAN узлы группируют по разным признакам. Например, по портам; по MAC-адресам; по номерам подсетей сетевого уровня; по меткам. В технологии MPLS для разделения трафика и образования виртуальных каналов используют метки. В отличии от технологии VLAN технологии MPLS присущ ряд недостатков: применима лишь для модели связи «сеть – сеть»; возможно прослушивание сетевого трафика; передаваемая информация доступна провайдеру, предоставляющему услуги MPLS.

Компания Check Point Software Technologies предложила четыре основных варианта построения сети VPN. Вариант «Intranet VPN» объединяет несколько филиалов предприятия, взаимодействие которых происходит по открытым каналам связи, в защищенную сеть. Вариант «Remote Access VPN» реализовывает взаимодействие между сегментом корпоративной сети и пользователем, подключающимся из дома или через notebook, к ресурсам данного сегмента корпоративной сети. Вариант «Client / Server VPN» создает защищенное взаимодействие двух узлов корпоративной сети. Вариант «Extranet VPN» для сетей, к которым подключаются сторонние пользователи.

Системы обнаружения атак

Перед тем, как переходить к рассмотрению систем обнаружения атак необходимо обратить внимание на стратегии систем анализа защищенности. Заданием пассивной стратегии является анализ на уровне операционной системы, СУБД и приложений системных объектов с точки зрения нарушения политики безопасности. Заданием активной стратегии является воспроизведение на сетевом уровне сценариев атак для анализа соответствующей реакции системы.

Классификацию систем обнаружения атак мы проведем по уровню информационной инфраструктуры: на уровне приложений и СУБД; на уровне операционной системы; на уровне сети. Системы обнаружения атак на уровне приложений и СУБД занимаются сбором и анализом информации от конкретного приложения. Данные системы не только обнаруживают атаки, которые пропустили другие средства обеспечения безопасности, но и дают возможность понизить требования к ресурсам так, как контролируются не все приложения, а только одно из них. Примерами, могут послужить WebStalker Pro, RealSecure Server Sensor.

Системы обнаружения атак на уровне операционной системы занимаются сбором и анализом информации, которая связана с деятельностью операционной системы. Эти системы предоставляют возможность контроля доступа к информации; наблюдения аномальной деятельности пользователя по отношению к приложению; отслеживания изменения режимов работы; работы в сетевом окружении с использованием шифрования; обнаружения атак, пропущенных другими средствами обеспечения безопасности; проведения автономного анализа. Однако, не следует забывать, что атаки, которые реализуются на нижних или более высоких уровнях, не рассматриваются данными системами, также обнаружить атаки на сетевое оборудование рассматриваемые средства не могут. И неоспоримым недостатком систем обнаружения атак на уровне операционной системы является возможность пропуска атаки при неполноте данных. Примером таких систем являются RealSecure Server Sensor, Intruder Alert.

Системы обнаружения атак на уровне сети занимаются сбором и анализом информации из сетевого трафика. Данные системы обладают рядом неоспоримых достоинств: контролируют и обнаруживают атаки типа «отказ в обслуживании»; одновременно могут контролировать большое число узлов сети; обнаруживают подозрительные события; обнаруживают атаки, пропущенные другими средствами обеспечения безопасности. Недостатки также весьма существенны: не рассматривают атаки, реализованные на более высоких уровнях; не предназначены для применения в сетях с использованием канального и прикладного шифрования; зависят от сетевых протоколов. В качестве примера назовем RealSecure Network Sensor, NetProwler, RealSecure for Nokia, Cisco Secure IDS, CiscoSecure IOS Integrated Software.

Идеальным решением является комбинированный подход, в котором сочетаются характеристики сетевых сенсоров с тактическими преимуществами сенсоров системного уровня. Например, Centrax.

Обманные системы

Обманные системы производят эмуляцию уязвимостей, не существующих в реальности. Причем одни системы эмулируют сервисы и уязвимости, а другие могут эмулировать компьютеры, сегменты с виртуальными узлами под управлением разных операционных систем. Примером первых систем может послужить Deception Toolkit (DTK). Примером вторых систем является CyberCop Sting.

Системы контроля целостности

Принцип работы систем контроля целостности следующий: в замкнутом цикле обрабатываются файлы, системные объекты и их атрибуты для получения контрольных сумм, которые сравниваются с контрольными суммами, полученными в результате предыдущего цикла с целью поиска изменений. В случае если найдены изменения, то администратору безопасности посылается сообщение, в котором зафиксировано время вероятного изменения. Хэш-функции являются базой для алгоритмов проверок, по причине того, что мельчайшее изменение в исходных данных приведет к большим изменениям в результате.

В результате мы приходим к выводу, что при наличии угроз информационной безопасности, например, угрозы хищения, утраты, блокирования, уничтожения, модификации, отрицания подлинности, есть вероятность осуществления атаки. Понятие атаки включает в себя источники угроз информационной безопасности: антропогенные, техногенные, стихийные; уязвимости: объективные, субъективные, случайные и методы реализации угроз информационной безопасности: аналитические, технические, программные, социальные, организационные. Последствием реализации угроз является ущерб владельцу. С целью устранения или уменьшения вероятности реализации атаки мы применяем к корпоративной сети организационные, инженерно-технические, программно-аппаратные методы защиты. При создании системы защиты корпоративной сети предприятия необходимо учитывать разнообразие и масштаб решаемых задач, сложную распределенную структуру сети, многообразие связей, глубокую иерархичность сети, высокие требования к системам обеспечения информационной безопасности.

Поступила 30.09.2004г.