УДК 621.391(075.8)

Трещев Иван Андреевич
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Заведующий кафедрой «Информационная безопасность автоматизированных систем»
Кандидат технических наук
E-Mail: kalkt@yandex.ru

Вильдяйкин Геннадий Федорович
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Кафедра «Информационная безопасность автоматизированных систем»
Кандидат технических наук, доцент
E-Mail: kalkt@yandex.ru

Ядыменко Константин Алексеевич
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Кафедра «Информационная безопасность автоматизированных систем»
Аспирант
E-Mail: kalkt@yandex.ru

О подходе к анализу защищенности корпоративных информационных систем

Аннотация. В данной работе рассмотрены основные способы тестирования корпоративных информационных систем на наличие уязвимостей и предложен новый подход, основанный на виртуализации IT-инфраструктуры предприятия для контроля защищенности от угроз безопасности. Предложенный подход может быть полезен при анализе обеспечения информационной безопасности на объектах, где не существует возможности анализа реальных ЭВМ.

Ключевые слова: информационная безопасность; корпоративные информационные системы.

Введение

Информационные сети предприятий принято называть корпоративными. Необходимые документы в электронном виде могут передаваться от одного сотрудника к другому за несколько секунд, также каждый сотрудник может получить необходимую ему информацию из единой базы данных максимально быстро. Все это делает работу предприятий более эффективной. Корпоративные сети могут иметь подключение к информационным сетям связи общего пользования (Интернет).

Широкое использование информационных технологий делает вполне закономерной и весьма актуальной проблему защиты информации, или иначе, проблему обеспечения информационной безопасности. Под типовой корпоративной сетью передачи данных в работе понимается распределенные ЛВС предприятия с подключением к информационным сетям связи общего пользования или без такого подключения.

Целью данной работы является моделирование типовой корпоративной сети в виртуальной среде для оценки по требованиям обеспечения безопасности информации.

Информационная безопасность предприятия – это защищенность информации, которой располагает предприятие (производит, передает или получает) от НСД, разрушения, модификации, раскрытия и задержек при поступлении. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода [1].

Для создания надежной подсистемы обеспечения информационной безопасности на предварительном этапе необходимо:

- выработать политику информационной безопасности;
- провести анализ рисков (т.е. определить вероятность реализации угроз);
- составить план мер по обеспечению информационной безопасности;
- составить план действий в чрезвычайных ситуациях;
- выбрать программные, технические и программно-технические средства обеспечения информационной безопасности.

Применяемые средства и механизмы защиты информации зависят от конфиденциальности данных. Конфиденциальность данных – это статус, предоставленный данным и определяющий требуемую степень их защиты. К конфиденциальным данным можно отнести: личную информацию пользователей, учетные данные (имена и пароли), данные о разработках и различные внутренние документы, бухгалтерские сведения. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы. Для остальных субъектов системы эта информация должна быть неизвестной [2].

Для того чтобы обеспечить эффективную защиту информации в АС, необходимо в первую очередь рассмотреть и проанализировать все факторы, представляющие угрозу безопасности информации.

Угрозы безопасности информации – это совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа (НСД) к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при обработке информации в информационной системе.

Угрозы могут воздействовать на информацию непосредственно или опосредственно через другие компоненты АС (программно-технические средства, обслуживающий персонал, пользователей).

При создании информационной инфраструктуры корпоративной АС на базе современных компьютерных сетей неизбежно возникает вопрос о защищенности этой инфраструктуры от угроз безопасности информации.

Защищенность является одним из важнейших показателей эффективности функционирования АС, наряду с такими показателями как надежность, отказоустойчивость, производительность и т. п.

Под защищенностью АС будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации [1].

В Российской Федерации при анализе защищенности АС принято руководствоваться основными руководящими документами, устанавливающими требования безопасности для АС на основе их классовой принадлежности. Если в системе обрабатываются дополнительно персональные данные, то требования к АС расширяются.

Методика анализа защищенности

Анализ защищенности АС проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите.

В настоящее время не существует каких-либо стандартизированных методик анализа защищенности АС, поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако типовую методику анализа защищенности корпоративной сети предложить все-таки возможно.

Типовая методика включает использование следующих методов [2]:

- изучение исходных данных по АС;
- оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;
- анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;
- ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры;
- сканирование внешних сетевых адресов ЛВС из сети Интернет;
- сканирование ресурсов ЛВС изнутри;
- анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную либо с использованием специализированных программных средств.

В данной работе при оценке защищенности АС по требованиям информационной безопасности используется методология – «тестирование на проникновение» (Penetration Testing). Так называется тестирование защищенности, в ходе которого используются приемы и инструменты, применяемые злоумышленниками [3]. Причем задача тестирования сводится не только к обнаружению уязвимости, которую теоретически может использовать злоумышленник, но и к эксплуатации найденной уязвимости для подтверждения ее реальной опасности.

Данный вид тестирования может использоваться при аттестации объектов информатизации. По результатам тестирования либо подтверждается отсутствие уязвимостей в АС, либо обнаруживаются уязвимости, которые необходимо устранить. С помощью такого тестирования можно определить максимальное количество уязвимостей и получить объективную оценку защищенности АС.

При анализе защищенности особо критичные серверы, например, серверы управляющие непрерывными технологическими процессами, как правило, исключаются из рамок тестирования и проверяются по проверочным листам, содержащим описание настроек безопасности [1]. Очевидно, что при этом невозможно получить полное представление о защищенности системы, в этом случае технологии виртуализации могут помочь изучить систему без влияния на процессы, протекающие в ней. Идея состоит в том, что в виртуальной среде моделируется интересующая исследователя сеть или фрагмент такой сети. Модель состоит из узлов, которые предназначены для поддержания работоспособности исследуемой системы (серверы, шлюзы и т.п.) и узлов, которые оказывают (или могут оказывать при определенных условиях) воздействие на систему. Все моделируемые узлы должны как можно более полно соответствовать их реальным прототипам. Это касается в основном ПО, т.к. для исследования уязвимостей математическое обеспечение системы имеет первостепенное значение. Чем больше программных средств установлено в системе, тем она более уязвима. Поэтому в виртуальной среде необходимо тщательно воспроизвести состав ПО исследуемой системы. Когда модель подготовлена и проверена ее работоспособность, можно приступать к исследованию защищенности. Моделирование средств обеспечения межсетевого взаимодействия, таких как коммутаторы, маршрутизаторы может быть ограничено ввиду того, что эти устройства используют в качестве ОС собственные разработки компаний-производителей данных устройств. Проверку уязвимостей этих устройств к сетевым атакам в этом случае представляется возможным проводить на реальном оборудовании с использованием различных схем подключения таких устройств к узлам сети.

Тестирование на проникновение может проводиться как изнутри сети предприятия, так и снаружи (удаленно) через каналы связи общего пользования. В первом случае атакам подвергаются внутренние узлы сети предприятия напрямую. Во втором случае атака направлена на внешние интерфейсы сети предприятия.

Методика «тестирования на проникновение» состоит из следующих этапов:

- идентификация целей;
- поиск уязвимостей;

- эксплуатация уязвимостей;
- формирование протокола (отчета) о результатах тестирования.

Рассмотрим каждый из этих этапов на примере внутреннего тестирования на проникновение, когда аудитор имеет физический доступ к корпоративной сети.

На этапе идентификации целей аудитор сканирует сеть с помощью специального сканера сети, который позволяет определить, какие узлы доступны, какие службы запущены, а также их версии. В результате специалист, проводящий тестирование, знает что скрывается в сети за определенным IP-адресом: сервер базы данных, web-сервер, контроллер домена, сервер приложений или рабочая станция.

Для следующего этапа необходимо выбрать узлы, которые будут исследоваться на защищенность, и провести сканирование этих узлов на наличие уязвимостей. Основным средством тестирования на данном этапе являются сетевые сканеры, располагающие базами данных известных уязвимостей. Получив сводный перечень уязвимостей, аудитор проводит эксплуатацию части уязвимостей.

После получения доступа к какой-либо системе аудитор выполняет какие-либо действия, чтобы наглядно продемонстрировать возможные последствия осуществления подобных атак.

При анализе защищенности традиционно используются два основных метода тестирования:

- тестирование по методу «черного ящика»;
- тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рисками. Выводы о наличие уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике. Основным инструментом анализа в данном случае являются программные агенты средств анализа защищенности системного уровня.

Виртуализация ЛВС может быть полезна при оценке по требованиям обеспечения безопасности информации. Во многих случаях работы по оценке защищенности невозможно провести непосредственно на объекте. Это может быть связано с процессами, протекающими в системе, которые не могут быть приостановлены на время проведения испытаний или с другими причинами. В этом случае виртуализация инфраструктуры объекта испытаний может стать приемлемым решением, которое обеспечит безопасность проведения анализа защищенности и достаточно точную оценку уязвимостей, характерных для реального объекта исследования.

Также виртуализация может быть полезна при планировании подсистемы защиты информации реального объекта в части конфигурирования средств защиты и проверки работоспособности комплекса применяемых программных средств.

На базе платформы виртуализации VMWare ESXi развернута модель типовой корпоративной сети. Структурная схема виртуальной ЛВС представлена на рисунке 1.

Рабочие станции (АРМ) предназначены для обработки конфиденциальной информации и персональных данных.

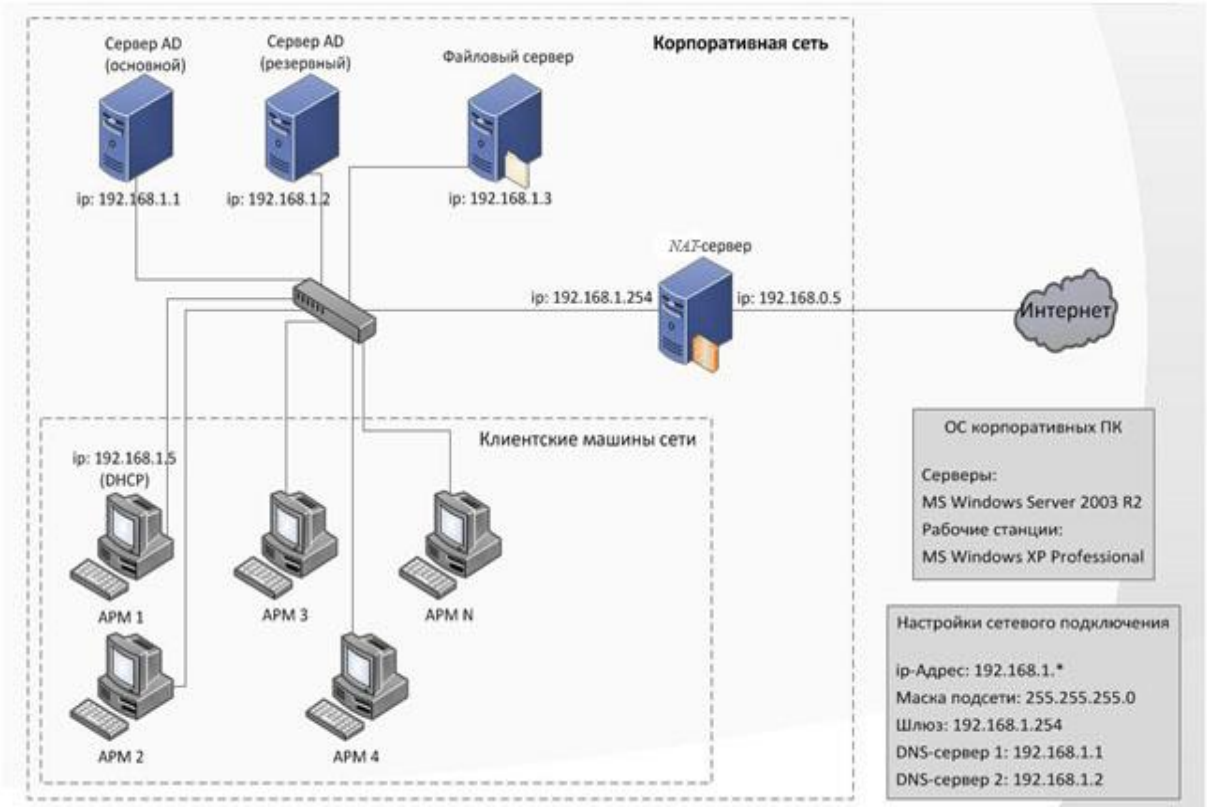

Рис. 1. *Структурная схема виртуальной ЛВС*

Файловый сервер служит накопителем персональных данных и конфиденциальной информации. Предполагается, что на рабочих станциях клиентов конфиденциальная информация не хранится. После обработки информация поступает на файловый сервер. Предполагаем, что данный подход закреплен организационно-распорядительными документами предприятия.

Основной сервер AD помимо роли AD является DNS и DHCP сервером. Резервный сервер AD дублирует основной сервер AD и предназначен для обеспечения отказоустойчивости АС при выходе из строя основного сервера. NAT-сервер – сервер, который обеспечивает клиентам сети доступ в сеть Интернет. Все сервера работают на ОС Windows Server 2003 R2 без использования стороннего ПО. Идентификатор данной локальной сети – 192.168.1.0/24. Всем клиентам сети IP-адрес выдается автоматически сервером DHCP. На всех серверах протокол TCP/IP сконфигурирован вручную, и соответствующие IP-адреса занесены в список исключений на сервере DHCP.

Заключение

Результаты данной работы могут использоваться при создании тренажера для администратора безопасности по настройке средств защиты информации, методы моделирования, основанные на виртуализации корпоративной сети, могут применяться, когда невозможно провести инструментальный контроль непосредственно на узлах физической сети в виду объективных причин (опасность нарушения работоспособности системы, управление непрерывными процессами).

ЛИТЕРАТУРА

1. Садердинов, А.А. Информационная безопасность предприятия: учеб. пособие / А.А. Садердинов, В.А. Трайнев, А.А. Федулов. – М.: Дашков и К°, 2005. – 336 с.
2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – М.: «ФОРУМ»: ИНФРА-М, 2011. – 416 с.
3. Семененко, В.А. Информационная безопасность: учеб. пособие / В.А. Семененко. – 4-е изд. – М.: МГИУ, 2010. – 277 с.

Ivan Treschev
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: kalkt@yandex.ru

Gennady Wildeisen
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: kalkt@yandex.ru

Constantine Adamenko
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: kalkt@yandex.ru

An approach to the analysis of the security of corporate information systems

Abstract. In this paper, the basic methods of testing of corporate information systems for vulnerabilities and propose a new approach based on the virtualization of IT-infrastructure for enterprise security control from security threats. The proposed approach can be useful in the analysis of information security at sites where there is no possibility of analyzing real computer.

Keywords: information security; corporate information systems.

REFERENCES

1. Saderdinov, A.A. Informacionnaja bezopasnost' predprijatija: ucheb. posobie / A.A. Saderdinov, V.A. Trajnev, A.A. Fedulov. – M.: Dashkov i Kº, 2005. – 336 s.
2. Shan'gin, V.F. Informacionnaja bezopasnost' komp'juternyh sistem i setej: ucheb. posobie / V.F. Shan'gin. – M.: «FORUM»: INFRA-M, 2011. – 416 s.
3. Semenenko, V.A. Informacionnaja bezopasnost': ucheb. posobie / V.A. Semenenko. – 4-e izd. – M.: MGIU, 2010. – 277 s.