Тип работы: Курсовая работа

Предмет: Информационные системы и процессы

Введение

Стремительное развитие информационных и коммуникационных связано с необходимостью обмена большими массивами информации. Современное общество всецело зависит от информационных систем различного рода - от крупных информационных порталов банков и государственных служб до небольших прикладных систем, используемых в организациях. Большинство государственных услуг переводится в электронную форму, растет доля онлайн платежей, проводимых через банковские информационные системы. Таким образом, информационные ресурсы в настоящее время представляют собой высокоценный актив, обеспечение сохранности которого является залогом успешности функционирования организаций различного рода деятельности. Потери информации с высокой вероятностью могут приводить к простоям в работе сотрудников организаций, что приводит к прямым убыткам, связанным с потерями в клиентской базе, просрочкам в исполнении заказов и подготовке документов и др. В качестве объектов обрабатываемой информации выступают: финансовые данные, элементы коммерческой тайны, объекты, охраняемые законодательством об авторском праве, а также данные о личной жизни и состоянии здоровья людей. Утечки информации, содержащей коммерческую тайну, могут выступать в качестве причины прямых убытков, вплоть до возникновения угрозы функционированию предприятия. Известен ряд прецедентов, когда из-за утечек персональных данных злоумышленники получали возможность совершения неправомерных действий (получать кредиты, снятие наличных средств в банкоматах, кража денежных средств с счетов, находящихся в электронных кошельках). Таким образом, задача обеспечения защиты информации на сегодняшний день имеет особую актуальность.
Цель работы заключается в анализе технологий обеспечения безопасности сетевых ресурсов.
Задачи работы:
- проведение анализа теоретических аспектов функционирования систем информационной безопасности;
- проведение анализа типов сетевых атак на информационные ресурсы предприятий;
- анализ основных задач обеспечения защиты информации в компьютерных сетях;
- анализ защищенности серверных и сетевых ресурсов с использованием Deerfield VisNetic Firewall.
Объект исследования: информационные ресурсы предприятий.
Предмет исследования: технологии обеспечения защиты информации в компьютерных сетях.

1 Теоретическая часть

Сетевые атаки представляют собой попытки воздействия на удаленные компьютеры с использованием программных средств. Как правило, к основным целям сетевых атак относятся попытки нарушения системы конфиденциальности данных, провоцирование утечек информации. Также, проведение сетевых атак может осуществляться в целях получения доступа к сетевым ресурсам удаленных систем [4].
Существует несколько принципов классификации сетевых атак.
Первый вид классификации - по принципу воздействия. Пассивные сетевые атаки, как правило, связаны с задачей получения конфиденциальных сведений с удаленных систем. К таким атакам, например, можно

отнести попытки чтения ящиков электронной почты абонентов, например, через попытки подбора паролей. Меры защиты в данном случае могут быть связаны с соблюдением требований к конфиденциальности паролей, к их сложности и периодичности смены. Также защита может обеспечиваться путем блокировки аккаунта после определенного числа неуспешных попыток авторизации.
Активные сетевые атаки кроме попыток чтения данных предполагают также и их модификацию. Одним из наиболее значимых различий между указанными типами атак является сложность обнаружения пассивного вмешательства в систему, в то время как признаки осуществления активных атак, достаточно просто обнаруживаются [4].
Кроме того, классификация сетевых атак может проводиться в зависимости от поставленных атакующей стороной задач. К основным задачам относятся, как правило, нарушение работы удаленных систем, получение несанкционированного доступа к данным, проведение скрытого изменения данных, хранящихся в системе.
Ряд сетевых атак может быть связан с отправкой большого количества запросов на удаленные системы, в результате которых нарушается их работоспособность.
В настоящее время проводится разработка и совершенствование методов защиты от сетевых атак, однако полноценной гарантии от проведения успешной атаки ни один из методов дать не может. Дело в том, что любая статичная система защиты имеет недостатки, и задача защиты от всех сетевых атак является невозможной. Что же касается динамических методов защиты, к которым относится применение статистических, экспертных систем, модулей защиты, использующих нечеткую логику и нейронные сети, то они также имеют ряд недостатков, поскольку основаны преимущественно на анализе подозрительных действий и сравнении их с известными методами сетевых атак. Следовательно, перед неизвестными типами атак большинство систем защиты пасует, начиная отражение вторжения слишком поздно. Тем не менее, современные защитные системы позволяют настолько осложнить злоумышленнику доступ к данным, что рациональнее бывает поискать другую жертву.
Современные технологии сетевых атак обладают достаточно широкими возможностями, к которым можно отнести:
- возможность несанкционированного входа в сеть при проведении избирательных комиссий вплоть до модификации результатов выборов;
- возможность взлома сетей аэронавигации, что может приводить к авиакатастрофам;
- возможность модификации сетей энергоснабжения, коммунальных систем и др.;
- возможность взлома учетных записей в платежных системах, что может приводить к утечкам денежных средств с банковских счетов или электронных кошельков.
Таким образом, любая современная информационная система должна обладать системой защиты от сетевых атак, исключающей возможности утечки и модификации данных. Если данная система связана с технологиями жизнеобеспечения, то необходимо проведение сертификации системы на предмет защиты от внешних уязвимостей.
Так, основными методами защиты от сетевых атак являются:
- шифрование каналов связи;
- использование систем комплексной защиты информации;
- использование ПО для защиты от сетевых атак;
- проведение оптимальных настроек защиты средствами сетевой операционной системы.
Компоненты защиты информации от сетевых атак включают в себя:
- организационную составляющую (издание ряда нормативных документов, регламентирующих вопросы защиты информации, обучение пользователей технологиям защиты от сетевых атак, распознаванию их признаков, действиям при обнаружении признаков атаки);
- программную составляющую в части установки и настройки специального программного обеспечения для защиты от сетевых атак с возможностью централизованного управления системой;
- инженерно-техническую составляющую в целях предотвращения физического проникновения злоумышленников на объекты, а также предотвращения утечек сетевой информации по каналам различной физической природы.
Построение архитектуры защиты от сетевых атак должно производиться в соответствии с утвержденными стандартами и соответствующей моделью угроз и моделью нарушителя. Класс защищенности системы, в соответствии с которым проектируется архитектура защиты информации, присваивается по результатам аудита системы защиты информации, который проводится сторонними сертифицированными организациями, либо специалистами самой организации, имеющими соответствующие компетенции.

2 Аналитическая часть
2.1 Характеристика видов угроз и моделей нарушителей

Проведем анализ основных типов угроз сетевой безопасности.
Одним из критериев классификации сетевых угроз является их происхождение, в данном случае угрозы безопасности делятся на угрозы, связанные с влиянием человеческого фактора и угрозы, связанные с особенностями работы аппаратного обеспечения.
Угрозами технического характера являются [10]:
- ошибки в работе программного обеспечения;
- проведение внешних DoS- и DDoS-атак;
- действие вредоносного программного обеспечения;
- осуществление несанкционированного съема информации;
- активность сетевых угроз.

1. IDS – Snort. О программе. [Электронный ресурс]. Режим доступа: http://www.netconfig.ru/ready/snort/
2. Сетевая защита информации. [Электронный ресурс]. Режим доступа: http://ic-dv.ru/uslugi/sredstva_doverennoj_zagruzki/
3. Сетевые атаки и их виды. [Электронный ресурс]. режим доступа: https://www.kakprosto.ru/kak-848505-chto-takoe-setevaya-ataka
4. Блинов А.М. Информационная безопасность. – СПб: СПбГУЭФ, 2011 - 96с.
5. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. – М.: Альпина Паблишерз, 2011 – 338с.
6. Стефанюк В.Л. Обеспечение физической защиты сетевых ресурсов. – М.: Наука, 2014. - 574 с.
7. Якубайтис Э.А. Информационные сети и системы: Справочная книга.- М.: Финансы и статистика, 2011. – 232с.
8. Разработка инфраструктуры сетевых служб Microsoft Windows Server 2008. Учебный курс MCSE М.: Взд-во Русская редакция, 2009.
9. Сосински Б., Дж. Московиц Дж. Windows 2008 Server за 24 часа. – М.: Издательский дом Вильямс, 2008.
11. Герасименко В.А., Малюк А.А. Основы защиты информации. – СПб.: Питер, 2010. – 320с
12. Гук М. Аппаратные средства локальных сетей. Энциклопедия. – СПб.: Питер, 2010. – 576с.
13. Иопа, Н. И. Информатика: (для технических специальностей): учебное пособие– Москва: КноРус, 2011. – 469 с.
14. Акулов, О. А., Медведев, Н. В. Информатика. Базовый курс: учебник – Москва: Омега-Л, 2010. – 557 с.
15. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия Интернет-университет информационных технологий - ИНТУИТ.ру, 2012
16. МогилевА.В.. Информатика: Учебное пособие для вузов - М.: Изд. центр "Академия", 2011
17. Партыка Т.Л. Операционные системы и оболочки. - М.: Форум, 2011
18. Под ред. проф. Н.В. Макаровой: Информатика и ИКТ. - СПб.: Питер, 2011
19. Новиков Ю. В., Кондратенко С. В. Основы локальных сетей. КуПК лекций. – СПб.:Интуит, 2012. – 360с.
20. Ташков П.А. Защита компьютера на 100%. - СПб.: Питер, 2011
21. Самоучитель Microsoft Windows XP. Все об использовании и настройках. Изд. 2-е, перераб. и доп. М. Д. Матвеев, М. В. Юдин, А.В. Куприянова. Под ред. М. В. Финкова.– СПб.: Наука и Техника, 2011. – 624 с.: ил.
22. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2011. – 256 с.