МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине
«Технологии обеспечения информационной безопасности»
для студентов направления подготовки
10.04.01 Информационная безопасность

Практическое занятие №1. Основные классы атак в сетях на базе TCP/IP

1. Цель занятия

1. Изучить построение технических каналов утечки информации в корпоративной сети.
2. Отработать навыки анализа технических каналов утечки информации в корпоративной сети.

2. Подготовка к занятию

1. Изучить теоретический материал лекций №1-№2.
2. Ознакомиться с заданием на лабораторную работу.

3. Теоретическая часть

Каждый технический *канал утечки информации* (ТКУИ) характеризуется показателями, которые позволяют оценить риск утечки информации. К таким показателям относятся: пропускная способность ТКУИ; длина ТКУИ; относительная информативность ТКУИ.

Пропускная способность канала определяется как $C = \Delta F \cdot \log_2\left(1 - \frac{M_c}{M_n}\right)$, бит/с

где: ΔF – ширина полосы пропускания канала, Гц; M_c, M_n – мощность сигнала и помехи в Дб или Вт

Как видно пропускная способность канала зависит от ширины пропускания и соотношения сигнал/шум. Различают узкополосные и широкополосные каналы, а также каналы с низкой и высокой энергетикой передаваемого сигнала.

Наибольшую пропускную способность имеет оптический канал, наименьшую – акустический. Например, ΔF для телефонного канала 3,1 кГц, телевизионного канала до 8МГц. Если канал составной, например, акустико-оптический или акустико-радиоэлектронный, то пропускная способность канала определяется по наименьшему значению.

Длина ТКУИ оценивается расстоянием от источника сигнала до приѐмника при условии обеспечения качественного приѐма.

Длина в общем случае зависит от показателей составных элементов канала, а также от мощности сигнала в среде распространения,*технических характеристик* приѐмной аппаратуры, помех в канале и т.д.

Чем больше длина ТКУИ, тем более вероятно успешное действие злоумышленника по перехвату информации, т.к. возможна организация нескольких несанкционированных точек подключения или перехвата.

Рассмотренные показатели не учитывают ценность передаваемой информации.Т.к. неизбежны потери вследствие, например, действия помех в несанкционированно организованном ТКУИ, ценность информации может быть существенно ниже исходной.

Однако при накоплении информации можно повысить еѐ ценность и восстановить потери, но здесь может сыграть роль фактор старения информации во времени. Немаловажное значение имеет и время функционирования канала при передачи информации и возможность еѐ перехвата именно в это время.

Различают следующие каналы: постоянные, эпизодические, случайные, которые, в свою очередь могут быть открытыми, технически закрытыми и шифрованными. Наиболее трудно-организуемыми являются ТКУИ случайные с техническим закрытием или шифрованием.

Многообразие технических каналов утечки информации представляют определѐнный выбор путей, способов и средств несанкционированного добывания информации.

Анализируя ТКУИ можно сделать выводы:

1. Утечка информации с возможностью ее дальнейшего анализа возможна по всем техническим каналам.

2. Наиболее уязвимым по видовым демаскирующим признакам является оптический канал, т.к. на расстоянии с помощью соответствующих технических средств возможен перехват информации, например, с помощью специальной фотосъѐмки.

Основным каналом получения сигнальных демаскирующих признаков является радиоэлектронный канал, весьма существенным является и вещественный.

3. Чем большую пропускную способность и длину имеет ТКУИ, тем он опаснее для владельца информации.

4. Пропускная способность, длина и относительная информативность ТКУИ зависит от характеристик его элементов: источника, среды и приемника.

Для наиболее полного восстановления информации со стороны злоумышленников используется комплексирование каналов

ИИ – источник информации; ЦА – центр анализа.

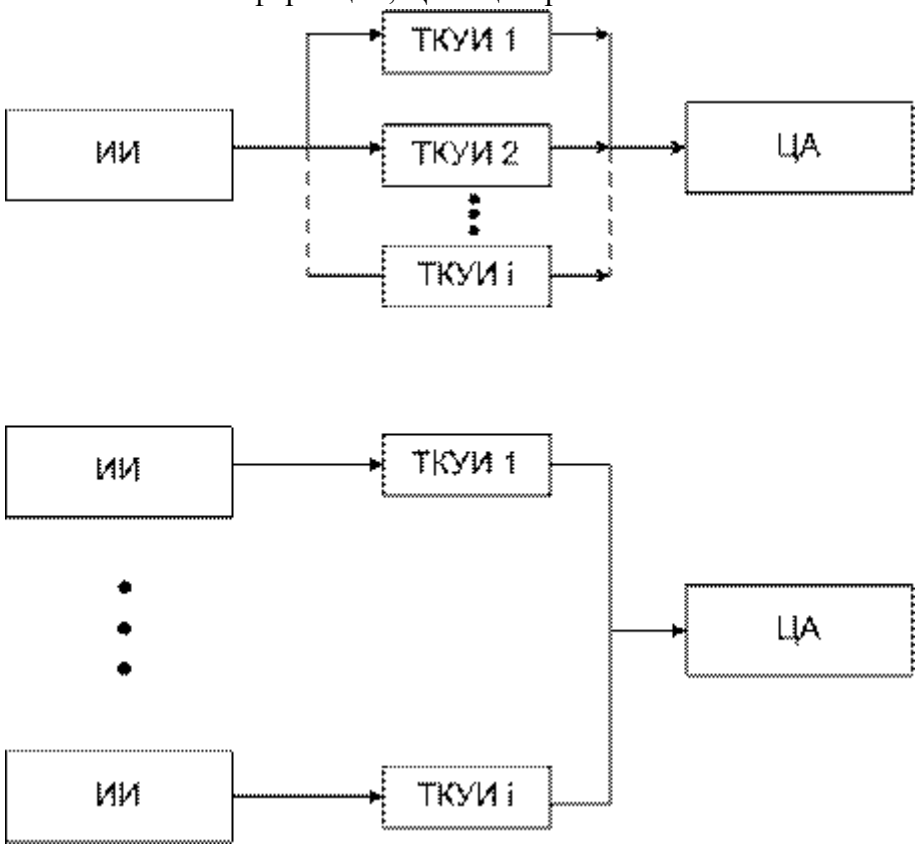

Рисунок 1 – Комплексирование технических каналов утечки информации

В верхней части рисунка 1 одна и та же информация попадает к злоумышленнику через разные ТКУИ. Так как вероятность воздействия помех на одинаковые элементы передаваемой информации в разных каналах мала, увеличивается достоверность суммарной информации, извлекаемой в дальнейшем злоумышленником. Пример: речь людей в помещении может быть подслушана через дверь, снята с помощью направленного микрофона или извлечена из опасных побочных сигналов.

Если злоумышленник не может быть уверен в достоверности источника, он может получить одну и ту же информацию из разных источников, как показано в нижней части рисунка 1.

В данной лекции мы ознакомились с понятием информационного сигнала и его основными характеристиками с точки зрения физики и математики. Знание физических

основ передачи информации необходимо для понимания того, как могут быть реализованы технические каналы утечки информации.

Когда говорят об информационной безопасности, то чаще всего подразумевают защиту информационных ресурсов от НСД, рассмотренную нами в предыдущих лекциях. Тем не менее, есть и "другая сторона медали". Как бы хорошо ни была защищена ваша корпоративная сеть с помощью криптографии, *антивирусов*, *межсетевых экранов* и т.п., всегда существует возможность утечки информации через технические каналы утечки информации. Следует заметить, что техническая разведка требует достаточно высокой квалификации от злоумышленника, но, тем не менее, современное развитие техники и общая тенденция ее удешевления приводят к тому, что воспользоваться техническим каналом утечки информации иногда может быть проще, чем взломать корпоративную сеть.

Вопросы и задания:

Базовый уровень:

1. Типы технических каналов утечки информации.
2. Средства для нахождения каналов утечки информации.

Повышенный уровень:

3. Опишите полный анализ нахождения каналов утечки информации.

Список литературы, рекомендуемый к использованию по данной теме

1. Основная литература:

1. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012.

2. Дополнительная литература:

1. Обеспечение информационной безопасности машиностроительных предприятий. Учебник для вузов./ Под ред. П.П. Мельникова. – М.: Сатурн-С, 2006.

2. Галатенко В.А. Стандарты информационной безопасности. Курс лекций / Под ред. акад. РАН Бетелина. – М.: Интернет-университет информационных технологий, 2006.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А. – Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.

Лабораторная работа №2. Вредоносные программы и их классификация. Антивирусы

1. Цель занятия

1. Изучить угрозы несанкционированного доступа к информации.
2. Изучить основные классы атак в сетях на базе TCP/IP.

2. Подготовка к занятию

1. Изучить теоретический материал лекций №3-№4.
2. Ознакомиться с заданием на лабораторную работу.
3. Ответить на контрольные вопросы.

3. Теоретическая часть

Согласно ГОСТ Р 50922-96 "Защита информации. Основные термины и определения" несанкционированный доступ (НСД) к информации – деятельность,

направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Заинтересованным лицом в данном случае может выступать:

–государство;

–юридическое лицо;

–группа физических лиц или одно физическое лицо;

общественная организация.

Проблеме защиты информации от НСД посвящен ряд руководящих документов ФСТЭК (соответственно, бывш.Гостехкомиссии). Определение НСД там более узкое, чем в ГОСТе.

Несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС).

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем. Несмотря на это, действие внедренной программной закладки ("червя" и т.п.), результатом которого стало попадание защищаемой информации к злоумышленнику, также можно рассматривать как факт НСД.

К основным угрозам НСД можно отнести следующее:

–угрозы проникновения в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

–угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;

–угрозы внедрения вредоносных программ (программно-математического воздействия).

Кроме этого, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрениявредоносных программ могут создаваться условия для НСД в операционную среду компьютера.

В общем случае, комплекс программно - технических средств и организационных мер по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

–управления доступом;

–регистрации и учета;

–криптографической;

обеспечения целостности.

Источником угрозы НСД может быть нарушитель, носитель с вредоносной программой или аппаратная закладка. Модель нарушителя – абстрактное (формализованное или неформализованное) описание нарушителя.

При разработке модели нарушителя определяются следующие предположения:

–категория лиц, к которой относится нарушитель;

–мотивы нарушителя;

–цели нарушителя;

–квалификация и техническая оснащенность нарушителя;

–возможные действия нарушителя;

–время действия (постоянно, в определенные интервалы).

Выделяют две категории нарушителей по отношению к АС – внутренние и внешние. Внешними нарушителями могут быть:

−разведывательные службы государств;

−криминальные структуры;

−конкуренты;

−недобросовестные партнеры;

−внешние субъекты (физические лица).

Злоумышленник – это нарушитель, намеренно идущий на нарушение.

Внешний нарушитель может осуществлять НСД следующими способами:

1. через автоматизированные рабочие места, подключенные к сетям общего пользования или сетям международного обмена (например, Интернет);
2. с помощью программного воздействия на защищаемую информацию (программные закладки, вирусы и др.);
3. через элементы автоматизированной системы, которые побывали за пределами контролируемой зоны (например, съемные носители информации);

Внутренними нарушителями могут быть следующие категории лиц:

−пользователи АС;

−персонал АС;

−сотрудники службы безопасности;

−руководители различных уровней.

По уровню знаний нарушителей можно классифицировать следующим образом:

−знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;

−обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;

−обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;

−знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

−применяющий только агентурные методы получения сведений;

−применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);

−использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;

−применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

− в процессе функционирования АС (во время работы компонентов системы);

в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);

− как в процессе функционирования АС, так и в период неактивности компонентов системы.

По месту действия:

−без доступа на контролируемую территорию организации;

– с контролируемой территории без доступа в здания и сооружения;
– внутри помещений, но без доступа к техническим средствам АС;
– с рабочих мест конечных пользователей (операторов) АС;
– с доступом в зону данных (серверов баз данных, архивов и т.п.);
– с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться следующие ограничения и предположения о характере действий возможных нарушителей:

– работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;

– нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников.

Модель нарушителей может иметь разную степень детализации.

Содержательная модель нарушителей отражает систему принятых руководством объекта защиты взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия.

Сценарии воздействия нарушителей определяют классифицированные типы совершаемых нарушителями акций с конкретизацией алгоритмов и этапов, а также способов действия на каждом этапе.

Математическая модель воздействия нарушителей представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, параметрически характеризующих результаты действий, и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами объекта и системы охраны. Именно этот вид модели используется для количественных оценок уязвимости объекта и эффективности охраны.

Вопросы и задания:

Базовый уровень:

1. Что такое TCP/IP?
2. Основные угрозы несанкционированного доступа к информации?
3. Основные классы атак в сетях на базе TCP/IP.

Повышенный уровень:

4. Обнаружение и устранение несанкционированного доступа к информации.

Список литературы, рекомендуемый к использованию по данной теме

1. Основная литература:

1. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012.

2. Дополнительная литература:

1. Обеспечение информационной безопасности машиностроительных предприятий. Учебник для вузов./ Под ред. П.П. Мельникова. – М.: Сатурн-С, 2006.

2. Галатенко В.А. Стандарты информационной безопасности. Курс лекций / Под ред. акад. РАН Бетелина. – М.: Интернет-университет информационных технологий, 2006.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А. – Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.

Практическое занятие №3. Система обнаружения вторжений

1. Цель занятия

Изучить реализацию модели безопасности криптографических модулей FIPS140-2.

2. Подготовка к занятию

1. Изучить теоретический материал лекций №4-№5.
2. Ознакомиться с заданием на лабораторную работу.

3. Теоретическая часть

В федеральном стандарте США FIPS 140-2 "Требования безопасности для криптографических модулей" под криптографическим модулем понимается набор аппаратных и/или программных (в том числе встроенных) компонентов, реализующих утвержденныефункции безопасности (включая криптографические алгоритмы, генерацию и распределение криптографических ключей,аутентификацию) и заключенных в пределах явно определенного, непрерывного периметра .

В стандарте FIPS 140-2 рассматриваются криптографические модули, предназначенные для защиты информации ограниченного доступа, не являющейся секретной, т. е. речь идет о промышленных изделиях, представляющих интерес для основной массы организаций. Наличие подобного модуля - необходимое условие обеспечения защищенности сколько-нибудь развитой информационной системы, однако, чтобы выполнять предназначенную ему роль, сам модуль также нуждается в защите, как собственными средствами, так и средствами окружения (например, операционной системы).

Согласно стандарту, перед криптографическим модулем ставятся следующие высокоуровневые функциональные цели безопасности:

– применение и безопасная реализация утвержденных функций безопасности для защиты информации ограниченного доступа ;

– обеспечение защиты модуля от несанкционированного использования и нештатных методов эксплуатации;

– предотвращение несанкционированного раскрытия содержимого модуля (криптографических ключей и других данных, критичных для безопасности);

– предотвращение несанкционированной и необнаруживаемой модификации модуля и криптографических алгоритмов, в том числе несанкционированной модификации, подмены, вставки и удаления криптографических ключей и других данных, критичных для безопасности;

– обеспечение отображения (индикации) режима работы (состояния) модуля ;

обеспечение доверия тому, что модуль функционирует должным образом при работе в утвержденном режиме;

– обнаружение ошибок в функционировании модуля и предотвращение компрометации информации ограниченного доступа и данных модуля, критичных для безопасности вследствие подобных ошибок.

Из перечисленных целей вытекают требования безопасности, относящиеся к этапам проектирования и реализации модуля и разделенные в стандарте на одиннадцать групп:

–спецификация криптографического модуля;

требования к портам и интерфейсам модуля;

−роли, сервисы и аутентификации;
−конечно-автоматная модель;
−физическая безопасность;
−эксплуатационное окружение;
−управление криптографическими ключами;
−электромагнитная совместимость;
−самотестирование;
−доверие проектированию;
−сдерживание прочих атак.

Спецификация модуля включает определение криптографического периметра, реализуемых функций и режимов, описание модуля, его аппаратных и программных компонентов, а также документированную политику безопасности.

Среди портов и интерфейсов модуля должны быть выделены обязательные и дополнительные. Следует специфицировать всеинтерфейсы, а также все маршруты входных и выходных данных. Кроме того, порты для незащищенных параметров, критичных для безопасности, должны быть логически отделены от других портов.

Среди ролей и сервисов необходимо провести логическое разделение на обязательные и дополнительные, обеспечить персональную или ролевую аутентификацию.

Модель в виде конечного автомата должна описывать деление на обязательные и дополнительные состояния.

Меры физической самозащиты модуля включают замки, защитные кожухи, сохраняющие свидетельства вторжений пломбы, средства оперативного выявления и реагирования на попытки вторжений, меры по противодействию атакам, основанным на использовании нештатных внешних условий.

Ядром допустимого эксплуатационного окружения должна служить операционная система, удовлетворяющая требованиям утвержденного профиля защиты, обеспечивающая произвольное управление доступом, протоколирование и аудит, доверенные маршруты. Кроме того, следует применять утвержденные методы контроля целостности и построить модель политики безопасности.

В число поддерживаемых механизмов управления ключами должны входить генерация случайных чисел, распределение ввод/вывод, хранение и обнуление ключей.

На требованиях электромагнитной совместимости мы останавливаться не будем.

При включении питания и при выполнении определенных условий необходимо выполнение тестов криптографических алгоритмов,контроль целостности программного обеспечения, проверки критичных функций.

Меры доверия проектированию должны включать конфигурационное управление, процедуры безопасной установки, генерации ираспространения. Следует подготовить функциональную спецификацию, при реализации использовать язык высокого уровня, продемонстрировать соответствие проекта и политики, снабдить пользователей соответствующими руководствами.

Наконец, предусматриваются меры по сдерживанию атак, для которых пока нет стандартизованных требований.

Стандартом FIPS 140-2 предусмотрено четыре уровня защищенности криптографических модулей, что позволяет экономически целесообразным образом защищать данные разной степени критичности (регистрационные журналы, счета на миллионы долларов или данные, от которых зависит жизнь людей) в разных условиях (строго охраняемая территория, офис, неконтролируемыйобъект).

К первому (самому слабому) уровню применяется минимальный набор требований безопасности, которым удовлетворяет, например, шифрующая плата для персонального компьютера. Программные компоненты соответствующих модулей могут выполняться на универсальных вычислительных системах с несертифицированной ОС.

На втором уровне требуются:

ролевая аутентификация;

– замки на съемных оболочках и дверцах, защитные покрытия и пломбы, сохраняющие свидетельства вторжений;

– использование ОС, сертифицированных на соответствие определенным профилям защиты на основе "Общих критериев" с оценочным уровнем доверия не ниже второго.

К третьему уровню предъявляются следующие дополнительные требования:

– отделение портов и интерфейсов, применяемых для нешифрованного ввода/вывода криптографических ключей и других данных, критичных для безопасности;

– персональная аутентификация с проверкой допустимости принятия определенных ролей;

– наличие средств оперативного выявления и реагирования на попытки вторжений (к примеру, микросхемы, обеспечивающие обнуление критичных данных модуля при попытке вскрыть корпус);

– использование ОС, сертифицированных на соответствие определенным профилям защиты с оценочным уровнем доверия не ниже третьего и поддержкой доверенного маршрута.

Четвертый уровень самый сильный. Его требования предусматривают полный спектр мер физической защиты, включая меры по противодействию атакам, берущим на вооружение нештатные внешние условия (электрические или температурные). Операционная система должна соответствовать оценочному уровню доверия не ниже четвертого.

Далее будут детально рассмотрены наиболее содержательные группы требований. Здесь же обратим внимание на параллель с профилем защиты для смарт-карт, общность целого ряда целей, предположений и требований безопасности для криптографических модулей и смарт-карт (что, разумеется, вполне естественно). На наш взгляд, сравнительный анализ этого профиля и стандарта FIPS140-2 позволяет в полной мере оценить достоинства "Общих критериев" и ассоциированных спецификаций, высокую степень их полноты и систематичности. Конечно, "Общие критерии" можно критиковать, их нужно развивать и совершенствовать, но перевод стандарта FIPS 140-2 на рельсы "Общих критериев", несомненно, повысил бы его качество.

Вопросы и задания:

Базовый уровень:

1. Выполнить настройку криптографического модуля.
2. Опишите технические характеристики криптографического модуля FIPS140-2.

Повышенный уровень:

3. Реализовать модель безопасности криптографических модулей.

Список литературы, рекомендуемый к использованию по данной теме

1. Основная литература:

1. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012.

2. Дополнительная литература:

1. Обеспечение информационной безопасности машиностроительных предприятий. Учебник для вузов./ Под ред. П.П. Мельникова. – М.: Сатурн-С, 2006.

2. Галатенко В.А. Стандарты информационной безопасности. Курс лекций / Под ред. акад. РАН Бетелина. – М.: Интернет-университет информационных технологий, 2006.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и

Шелупанова А.А. – Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.

Практическое занятие №4. Оценка профилей защиты и заданий по безопасности

1. Цель занятия

1. Изучить теоретический материал.

2. Получить практические навыки ограничения вещания в корпоративной сети с веб-сервисами.

2. Подготовка к занятию

1. Изучить теоретический материал лекции №6.

2. Ознакомиться с заданием на лабораторную работу.

3. Теоретическая часть

Полное название рассматриваемой спецификации (точнее, проекта спецификации) - "Дополнение к Руководству по информационной безопасности предприятия: Как выбирать поставщика Интернет-услуг". Далее, для краткости, мы будем называть ее "Дополнением к Руководству" или просто Дополнением. Напомним, что "Руководство по информационной безопасности предприятия" было рассмотрено нами ранее. При изложении Дополнения мы опираемся на публикацию.

"Дополнение к Руководству" призвано помочь в выработке политики и процедур безопасности в организациях, информационные системы которых подключены к Internet, а также служить дляпотребителей контрольным перечнем при обсуждении вопросов информационной безопасности с поставщиками Internet-услуг. В данном документе выделено три типа потребителей:

- потребители коммуникационных услуг;
- потребители услуг по размещению ресурсов;
- потребители, разместившиеся там же, где и поставщики услуг.

Еще одна цель Дополнения состоит в том, чтобы, информируя поставщиков Internet-услуг об ожиданиях общественности, побудить их принять упреждающие меры, сделав безопасность одним из приоритетных направлений развития.

Поставщик Internet-услуг определяется как организация, обеспечивающая для других подключение к Internet, а также иные Internet-услуги, в том числе размещение Web-серверов, поставкуинформационного наполнения, услуги электронной почты и т.д.

Вероятно, для многих привычнее называть такого поставщика Internet-провайдером; мы не стали этого делать, поскольку тогда, по соображениям концептуальной целостности, потребителяпришлось бы именовать Internet-консьюмером, а этот термин пока не прижился.

Роль поставщика Internet-услуг в реагировании на нарушения безопасности

Мы уже обсуждали тему реагирования на нарушения информационной безопасности и взаимодействие групп реагирования с опекаемым сообществом. Затронута она и в Дополнении.

Независимо от того, есть ли у поставщика Internet-услуг группа реагирования, он должен определить и довести до потребителей порядок передачи и обработки докладов о нарушениях, а также документировать собственные возможности по реагированию.

У некоторых поставщиков есть группы реагирования на нарушения информационной безопасности, однако даже в этом случае помощь часто предоставляется в качестве дополнительно оплачиваемой услуги, а группа включает в зону своей ответственности только тех, кто специально на нее подписался.

Если группы реагирования нет, поставщику следует определить, какую роль он возьмет на себя (если возьмет вообще) при реагировании на нарушение, и существует ли

группа, ответственность которой распространяется на потребителя, чтобы направлять ей доклады о нарушениях.

Поставщику Internet-услуг следует иметь специальные почтовые ящики: SECURITY - для сообщений о нарушениях безопасности, ABUSE - для сообщений о ненадлежащем поведении и NOC - для сообщений о проблемах в сетевой инфраструктуре.

Когда происходит нарушение информационной безопасности, затрагивающее инфраструктуру поставщика, необходимо немедленно сообщить потребителям такие сведения:

- кто координирует реакцию на нарушение;
- какая уязвимость использована атакующим;
- как нарушение сказалось на предоставляемых услугах;
- что делается для реагирования на нарушение;
- могут ли быть скомпрометированы данные потребителей;
- какие действия предпринимаются для устранения выявленной уязвимости;
- предполагаемый график реагирования, если он может быть составлен.

Если имеет место нарушение, направленное на какого-либо потребителя услуг подключения, поставщик Internet-услуг должен проинформировать его об атаке и, по возможности, оказать помощь в следующем:

- проследить видимый источник атаки и попытаться определить достоверность каждого шага на этом маршруте. Если исходный адрес подделан, поставщик может определить точку в своей сети, через которую поступает поток данных злоумышленника;
- получить контактную информацию источника атаки;

собрать и защитить свидетельства нарушения, предохраняя их от уничтожения или непреднамеренного разглашения.

В случае продолжения нарушения поставщик Internet-услуг, по запросу потребителя, может оказать помощь путем протоколирования с целью дальнейшей диагностики проблемы или посредством фильтрации определенных видов трафика.

Если окажется, что источником нарушения информационной безопасности является кто-то из потребителей, поставщик может помочь администраторам источника и цели атаки, вступив с нарушителем в контакт и переслав ему контактную информацию для связи с пострадавшими.

К поставщику могут также обратиться за помощью в случае атак, которые проходят через его сеть, но используют поддельные исходные адреса. Поддержка возможна в предоставлении сетевой регистрационной информации, генерируемой маршрутизаторами, чтобы найти точку, в которой поток данных с поддельными адресами вошел в сеть поставщика. При прослеживании источникаподобных атак требуется координация усилий со смежными поставщиками.

Поставщикам Internet-услуг следует иметь правила и процедуры, касающиеся разделения информации о нарушении безопасности со своими потребителями, с другими поставщиками илигруппами реагирования, с правоохранительными органами, средствами массовой информации и общественностью. Понадобятся средства для организации доверенного канала с целью передачи подобной информации.

Меры по защите Internet-сообщества

Поставщики Internet-услуг играют критически важную роль в повышении безопасности Internet.

Каждому из них следует иметь политику добропорядочного пользования, с учетом которой составляется контракт с потребителем. В политике определяются права потребителей на те или иные действия в разных частях сети и на разных системах.

Во многих странах есть законы о защите данных. В ситуациях, когда они применимы, поставщики должны проанализировать характер поступающих к ним персональных данных и, если нужно, принять меры, препятствующие их противозаконному использованию. Учитывая глобальный характер Internet, поставщикам

Internet-услуг, действующим в странах, где таких законов нет, необходимо хотя бы ознакомиться с идеей защиты данных.

Важно, чтобы штат поставщика постоянно помнил о проблемах информационной безопасности, с пониманием подходил к их решению, умел должным образом применять средства повышения безопасности. К числу наиболее значимых принадлежат вопросы использования доверенных каналов для передачи конфиденциальной информации, управления аутентификационными данными и т.д.

Поставщики Internet-услуг ответственны за такое управление сетевой инфраструктурой Internet, чтобы обеспечивалась устойчивость к появлению уязвимостей, а атакующие не могли легко организовать плацдарм для последующих атак.

Ключевой элемент сетевой инфраструктуры - маршрутизаторы. К сожалению, они не только сами по себе являются притягательными целями атак на безопасность, но и представляют собой отличный плацдарм для организации нападений на другие цели.

Многие маршрутизаторы позволяют злоумышленникам совершать опасные действия, например:

- "прослушивать" транзитные потоки данных;

манипулировать таблицами маршрутизации для перенаправления потоков данных;

- изменять состояние интерфейсов с целью нарушения обслуживания;

вызывать "трепыхание" маршрутных таблиц, чреватое отказом в обслуживании для крупных частей Internet;

- создавать пакеты с поддельными адресами и любым желаемым набором флагов;
- порождать штормы ICMP-пакетов, устраивать другие атаки на доступность;
- отправлять потоки данных в "черную дыру";

скрывать обращения по внешним адресам, что облегчается недостаточным протоколированием в маршрутизаторах.

Доступ к маршрутизаторам следует основывать на одноразовых паролях или еще более сильных средствах и ограничивать в максимально возможной степени. Обращения к маршрутизатору - протоколировать, привлекая ресурсы других систем.

Сеансы взаимодействия с маршрутизаторами подлежат шифровке для предотвращения краж сеансов или данных и для недопущения атак, основанных на воспроизведении трафика.

На маршрутизаторы нельзя возлагать выполнение мелких услуг, которые нередко включены по умолчанию.

Поставщики Internet-услуг должны быть столь же бдительными при конфигурировании всех видов сетевого оборудования, по возможности ограничивая доступ к сетевому оборудованию, предоставляя его только уполномоченным сетевым администраторам.

Конфигурационную информацию маршрутизаторов и коммутаторов следует сопровождать на файловом сервере.

Производители предлагают много сетевых устройств - от недорогих маршрутизаторов до принтеров, - принимающих соединения по протоколу telnet без запроса пароля. Если в сети поставщика Internet-услуг есть такое оборудование, доступ к нему следует ограничить. Кроме того, потребителям необходимо рекомендовать блокировать доступ к подобным устройствам из внешних сетей. Крайне нежелательно использовать протокол telnet для управления компонентами сети.

Центр управления сетью (ЦУС) является критически важной частью инфраструктуры поставщика Internet-услуг, поэтому его работу следует строить с соблюдением должных мер безопасности.

ЦУС располагает административным контролем над конфигурационными данными сетевого оборудования и обязан ограничить доступ к такой информации.

Как правило, ЦУС выполняет функции мониторинга сети, периодически опрашивая множество сетевых устройств. Помимо простого опроса, для взаимодействия с сетевыми устройствами ЦУС может использовать управляющий протокол, в частности SNMP. Обычно с его помощью выясняют значения различных переменных, например, число пакетов, принятых через определенный интерфейс. Однако протокол может применяться и для установки переменных, возможно, с далеко идущими последствиями (к примеру, переконфигурирование устройства). В любом случае, в SNMPv1 присутствует только тривиальная аутентификация. По возможности, к SNMP следует прибегать только как к средству получения информации от удаленных устройств, трактуя ее как конфиденциальную.

Еще одно применение протокола SNMP состоит в уведомлении управляющей станции о возникновении исключительных ситуаций. Такую информацию также необходимо считать конфиденциальной и проявить осторожность, чтобы SNMP-сообщения сами по себе не вылились в атаку на доступность.

В плане физической защиты наибольший интерес представляет ситуация, когда оборудование потребителей располагается на площадке поставщика Internet-услуг. В идеале каждый потребительдолжен получить полностью закрытую, запирающуюся "клетку", т. е. небольшое помещение со стенами и проемами для прокладки множества кабелей, а также со стойками для монтажа оборудования. Потребители проходят туда в сопровождении сотрудника поставщика (либо получают ключи только от своей комнаты).

Выделение отдельных комнат, однако, может оказаться слишком накладным, поэтому многие поставщики идут на компромисс, собирая "чужое" оборудование в одном машинном зале и тщательно контролируя все, что в нем происходит. К сожалению, этого может оказаться недостаточно, чтобы избежать таких недоразумений, как нечаянное отключение оборудования другогопотребителя. Вместо единого открытого пространства следует разделить зал перегородками и предоставлять каждому потребителю отдельное помещение с запирающейся дверью.

Вблизи чужого оборудования никого нельзя оставлять без присмотра. Такое оборудование запрещается трогать, фотографировать или исследовать.

Надо помнить также о безопасности на втором уровне семиуровневой модели, запрещая разделение физического сегмента сети между оборудованием потребителя и компьютерами, принадлежащими другим потребителям или поставщику Internet-услуг. Нередки случаи, когда злоумышленники пользуются уязвимостями или незашифрованными удаленными входами в оборудование потребителя, получают контроль над этими устройствами, переводят его в режим прослушивания сегмента локальной сети, потенциально нарушая тем самым конфиденциальность или безопасность других устройств в этом сегменте.

Вопросы безопасности чрезвычайно важны и тогда, когда компоненты сетевой инфраструктуры поставщика Internet-услуг размещены вне его территории (например, у партнера или в удаленной точке присутствия). Такие компоненты нередко являются жизненно важными с точки зрения топологии сети и, в то же время, могут стать объектом атаки или пострадать от несчастного случая. Для ограничения физического доступа оборудование в идеальном случае следует размещать в полностью закрытых, запирающихся комнатах или "клетках". Если на чужой площади хранятся запчасти, их также следует защищать от кражи, порчи или встраивания "жучков". По возможности необходимо использовать системы безопасности и замки, открывающиеся персональными картами. Удаленные компоненты нужно периодически проверять на предмет встраивания постороннего оборудования, которое может использоваться для прослушивания сетевых соединений. Как и на других площадках, компьютеры не следует подключать к транзитным сегментам или допускать подсоединение к сети неиспользуемых физических интерфейсов.

Маршрутизация, фильтрация и ограничение вещания

Способность поставщика Internet-услуг направлять потоки данных к правильному конечному пункту зависит от правил маршрутизации, заданных в виде маршрутных таблиц. Поставщики должны убедиться, что находящаяся в их ведении маршрутная информация может быть изменена только после надежной аутентификации и что права на внесение изменений должным образом ограничены.

В граничных маршрутизаторах следует аутентифицировать соседей в рамках протокола BGP.

При выборе протоколов внутренней маршрутизации нельзя забывать о безопасности. В случае изменения маршрутов необходимо обратиться к наивысшему уровню аутентификации, поддерживаемому протоколом внутренней маршрутизации.

Нередко атакующие скрывают следы, подделывая исходные адреса. Чтобы отвлечь внимание от своей системы, в качестве исходного они выбирают адрес невинной удаленной системы. Кроме того, поддельные исходные адреса часто встречаются в атаках, основанных на использовании отношения доверия между узлами сети.

Чтобы уменьшить область распространения подобных атак, поставщики Internet-услуг должны применять входную фильтрацию потоков данных, т. е. фильтрацию в направлении от периферийной системы (потребитель) к Internet (см.). Во всех граничных маршрутизаторах, к которым подключены потребители, следует сразу отфильтровывать идущие от них сетевые пакеты и имеющие исходные адреса, отличные от выделенных данным потребителям.

Дополнительной мерой защиты потребителей от атак, основанных на подделке исходных адресов, является выходная фильтрация - от сети Internet к периферийной системе (см.). Во всех граничных маршрутизаторах, к которым подключены потребители, следует сразу отфильтровывать потоки данных, идущие к потребителю и имеющие исходные адреса из выделенного ему пространства.

Иногда возникают ситуации, когда фильтрация оказывается невозможной. Например, большой агрегирующий маршрутизатор не выдерживает дополнительной нагрузки, вызванной применением пакетных фильтров. Кроме того, входная фильтрация способна привести к трудностям для мобильных пользователей. Следовательно, хотя данный метод для борьбы с подделкой адресов настоятельно рекомендуется, им не всегда удается воспользоваться.

В тех редких случаях, когда фильтрация на стыке потребителя и поставщика Internet-услуг невозможна, следует рекомендовать потребителю организовать фильтрацию внутри его сети.

Злоумышленники могут прибегнуть к избыточным изменениям маршрутной информации как к средству увеличения загрузки, на базе которого развивается атака на доступность. По меньшей мере это приведет к деградации производительности. Поставщикам Internet-услуг следует отфильтровывать поступающие объявления о маршрутах, игнорируя, например, маршруты к адресам для частных объединений сетей, избегая фиктивных маршрутов и реализуя политику расщепления и агрегирования маршрутов.

Поставщики Internet-услуг должны применять методы, уменьшающие риск нарастания нагрузки на маршрутизаторы в других частях сети. Следует отфильтровывать "кустарные" маршруты, настойчивое агрегирование и расщепление маршрутов.

Протокол IP поддерживает направленное вещание (посылку) через сеть пакетов, которые в определенной подсети станут широковещательными. Практической пользы от такой возможности немного, зато на ней основываются несколько различных видов атак (в первую очередь, это атаки на доступность, использующие эффект размножения широковещательных пакетов). Следовательно, маршрутизаторы, подключенные к вещательной среде, не следует конфигурировать так, чтобы было возможным непосредственное вещание на эту среду.

Защита системной инфраструктуры

То, как поставщик услуг управляет своими системами, критически важно для безопасности и надежного функционирования сети. Нарушения в работе систем могут в лучшем случае привести к снижению производительности или функциональности, но способны также вызвать потерю данных или сделать возможным перехват сетевого трафика (не исключена и последующая атакаметодом "нелегального посредника").

В общедоступном месте, например, на Web-сервере поставщика услуг, следует опубликовать его политику по отношению к защите персональных данных, обеспечению аутентичности, подотчетности, наложению защитных заплат, поддержке доступности, реагированию на доклады о нарушениях.

Предоставление разных услуг следует возлагать на разные системы. Кроме выгод от облегчения системного администрирования можно сослаться на многократно проверенный факт, что при таком подходе гораздо проще построить защищенную систему.

Все услуги выиграют от организации надежной защиты на сетевом уровне средствами IPsec.

Доступ ко всем системам поставщика, выполняющим критически важные функции (среди которых - почта, телеконференции и размещение Web-серверов), следует ограничить, разрешая его только администраторам соответствующих услуг, предоставлять после надежной аутентификации и осуществлять по доверенному каналу. Доступными из внешних сетей должны быть только те порты, на которых ожидают подключения уже востребованные услуги.

Если распространение и обновление программного обеспечения производится с помощью автоматизированных средств, им выделяется доверенный канал. Целостность ПО необходимо гарантировать путем вычисления и распространения вместе с ПО криптографических контрольных сумм.

Регистрационная информация должна быть доступна на чтение только системному администратору.

Если поставщик услуг ведет учет работы потребителей, то системы, обеспечивающие этот учет, изолируются от остальной части сети.

Нельзя подключать системы к транзитным сегментам.

Резервное копирование может являться слабым звеном в системной безопасности, если защита резервных носителей не налажена должным образом. При копировании по сети следует пользоваться доверенным каналом. Если в процессе резервного копирования данные помещаются на промежуточные диски, то доступ к этим дискам ограничивается в максимально возможной степени.

Отслужившие срок носители должны уничтожаться, а не выбрасываться.

Пользователей систем и услуг необходимо информировать о том, что сохраняется на резервных копиях, а что нет.

Доменная система имен (DNS) играет критически важную роль в повседневной деятельности миллионов пользователей Internet. Поставщикам услуг при администрировании DNS-серверов следует обратить внимание на следующие аспекты:

- мониторинг: обязательный контроль доступности DNS (способности отвечать на запросы);
- синхронизация часов: синхронизация установленного на серверах времени с помощью протокола NTP с аутентификацией.

При конфигурировании почтовых серверов поставщики Internet-услуг должны руководствоваться такими положениями:

- по возможности использовать ПО с раздельными агентами приема/отправки и обработки, чтобы агент приема/отправки, взаимодействующий с удаленными почтовыми серверами, выполнялся с минимальными привилегиями;

– ограничить запуск очередей по запросу (предоставляемый для удобства потребителей, получающих почту в своем домене и не имеющих постоянного соединения), желательно средствами надежной аутентификации;

– запретить предоставлять информацию о локальных пользователях или механизмах доставки, выходящую за рамки необходимого;

– выявлять исключительные ситуации (повторяющиеся неудачи аутентификации, зацикливание почты, ненормальная длина очереди) и генерировать соответствующие доклады.

Говорят, что почтовый SMTP-сервер функционирует в режиме "открытой" системы промежуточного хранения и пересылки почты, если он допускает прием и пересылку нелокальным адресатам таких сообщений, которые были порождены нелокально. Подобные открытые системы пересылки почты нередко используются "спамерами", организующими массовую незапрошенную рассылку с сокрытием инициатора. Только в весьма специфических обстоятельствах можно оправдать решение администратора сделать систему пересылки в Internet полностью открытой.

При конфигурировании серверов телеконференций (NNTP) поставщикам Internet-услуг необходимо соблюдать следующие требования:

– использовать ПО, устойчивое к вредоносным управляющим сообщениям и к переполнению буферов;

– освободить сервер телеконференций от выполнения каких-либо иных функций; если поддерживаются входящие пакеты статей, не подавать их на вход командного интерпретатора.

Размещение Web-серверов

Многие организации передают свои Web-серверы поставщикам Internet-услуг вместе с обязанностями по эксплуатации и администрированию, исходя, главным образом, из соображений информационной безопасности.

Помимо перечисленных выше аспектов, поставщики услуг при администрировании оборудования, на котором размещены Web-серверы, должны руководствоваться такими положениями:

– разумное использование DNS. В момент подключения клиента не следует выполнять поиск его имени, поскольку это делает Web-серверы уязвимыми для атак на доступность и заметно сказывается на производительности;

– минимизация привилегий. Web-демон следует выполнять от имени пользователя и группы, специально выделенных для этой цели и имеющих минимальные привилегии. Ответственный заинформационное наполнение Web-сервера должен работать от имени другого пользователя;

– контроль DocumentRoot. Все, что располагается ниже этого каталога, надо тщательнейшим образом проконтролировать. Желательно использовать системный вызов chroot для смены корневого каталога HTTP-демона;

– контроль UserDir. На сервере нельзя регистрировать других пользователей, кроме администраторов. Если такие пользователи все-таки есть, директиве "UserDir" (в случае ее разрешения) не следует предоставлять доступ к информации пользователей - в частности, не разрешать выполнение командных процедур от имени этих пользователей;

– разбиение на виртуальные серверы. Единый сервер, на котором размещено множество серверов (виртуальных доменов), необходимо организовать так, чтобы все данные, программы и регистрационные журналы различных виртуальных серверов были отделены друг от друга и чтобы доступ к "чужой" конфигурации или данным был невозможен. Кроме того, надо исключить доступ к данным или программам на сервере одного потребителя через локатор ресурсов, в хостовой части которого указано имя сервера другого потребителя;

– управление доступом. Следует сделать возможным разграничение доступа к определенным частям сервера на основе механизмов надежной аутентификации - сертификатов или одноразовых паролей.

Программы на серверной стороне, поддерживающие CGI или какой-либо другой интерфейс, важны для гибкости web как коммуникационной среды. Однако эта гибкость достигается ценой появления угроз безопасности, а слабая программа может сделать уязвимыми все виртуальные домены на сервере. Правила, сообразно которым поставщик Internet-услуг разделяет программы на допустимые и недопустимые, является показательным аспектом всей его политики безопасности.

Поставщику следует руководствоваться такими положениями:

– политика безопасности; выработка для своих потребителей ясной методики написания безопасных программ в имеющейся среде размещения Web-серверов с обязательным описанием тех приемов программирования, при применении которых программы будут отвергаться.

– установка программ: запрет на установку собственных программ потребителей. Все программы и командные процедуры передаются поставщику для первоначальной проверки на соответствие политике безопасности. Программы устанавливаются так, чтобы только администратор сервера мог их модифицировать.

– выбор пользователя и группы процесса: программы выполняются от имени пользователя и группы, специально выбранных для этой цели и имеющих минимальные привилегии (часто используют "nobody").

– отображение в навигаторах: запрет при любых обстоятельствах на отображение программ в навигаторах. Как следствие - программы нельзя размещать под DocumentRoot.

– разделение виртуальных серверов: программы не следует делать доступными через сервер другого потребителя или для Web-мастера другого потребителя;

– обработка пользовательского ввода: не вычислять выражения в пользовательском вводе, если нет механизма изоляции небезопасных действий.

– лимитирование потребления ресурсов: ввести лимит потребляемого астрономического и процессорного времени, а также дискового пространства для всех программ.

– маршрутные имена: все маршрутные имена делать абсолютными или начинающимися с DocumentRoot. Переменную PATH устанавливает только системный администратор.

Данные, которые пишет программа серверной стороны, следует считать конфиденциальными. Чтобы сделать невозможным доступ к таким данным через навигаторы, права устанавливаются так, чтобы у Web-демона не было права на чтение этих данных.

Если через Web-сервер предоставляется доступ к базам данных, то программам, осуществляющим такой доступ, выделяются лишь те полномочия, которые абсолютно необходимы для их функционирования.

Данные, относящиеся к управлению состояниями (идентифицирующие цепочки - cookies), следует считать конфиденциальными. Требуется исключить возможность доступа к ним из навигаторов.

Регистрационная информация, генерируемая Web-демоном, должна быть весьма конфиденциальной. Для реализации этого положения понадобится:

– поставщику Internet-услуг разрешить выполнение лишь необходимых операций с регистрационной информацией - генерацию счетов и периодическую ротацию;

– регистрационную информацию хранить вне дерева с корнем в DocumentRoot, чтобы исключить возможность доступа через навигаторы;

– регистрационную информацию в первоначальном или обработанном виде передавать потребителю только по доверенному каналу.

Многие поставщики Internet-услуг предоставляют своим потребителям средства для продажи товаров или услуг через размещенные у поставщика Web-серверы. Поставщику, разместившему у себя приложения электронной коммерции, следует руководствоваться такими положениями:

– шифрование транзакций: транзакции нельзя хранить на сервере в открытом виде. Разрешается использование криптографии с открытыми ключами, так что только потребитель сможет расшифровать транзакции. Даже если транзакции передаются напрямую в финансовое учреждение или потребителю, поставщик услуг вправе сохранять у себя какую-то часть данных для обеспечения подотчетности;

– передача транзакций: передача производится по доверенному каналу, если транзакции не обрабатываются немедленно, а передаются потребителю пакетами;

– резервное копирование: в случае записи транзакций на резервные носители должна гарантироваться физическая безопасность этих носителей.

Загрузку информационного наполнения на сервер поставщика Internet-услуг следует производить по доверенному каналу.

Поставщики услуг нередко предоставляют для использования потребителями поисковые машины, средства контроля целостности ссылок и т.д. Зачастую такие средства создают весьма существенную дополнительную нагрузку, поэтому их запуск по запросу необходимо запретить, чтобы защититься от атак на доступность.

Поисковые машины надо сконфигурировать так, чтобы поиск ограничивался частями Web-сервера, доступными всем.

Результат проверки целостности ссылок следует считать конфиденциальным, а доступ к нему предоставить только лицу, управляющему информационным наполнением.

Вопросы и задания:

Базовый уровень:

1. Настройка криптографического модуля.
2. Опишите технические характеристики криптографического модуля FIPS140-2.

Повышенный уровень:

3. Реализация модели безопасности криптографических модулей.

Список литературы, рекомендуемый к использованию по данной теме

1. Основная литература:

1. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012.

2. Дополнительная литература:

1. Обеспечение информационной безопасности машиностроительных предприятий. Учебник для вузов./ Под ред. П.П. Мельникова. – М.: Сатурн-С, 2006.

2. Галатенко В.А. Стандарты информационной безопасности. Курс лекций / Под ред. акад. РАН Бетелина. – М.: Интернет-университет информационных технологий, 2006.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А. – Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.

Практическое занятие №5. Анализ защищенности. Операционные системы

1. Цель занятия

1. Изучить возможные вопросы к поставщику Internet-услуг.
2. Разобрать размещение Web-серверов.

2. Подготовка к занятию

1. Изучить теоретический материал лекции №6.
2. Ознакомиться с заданием на лабораторную работу.

3. Теоретическая часть

1. Возможные вопросы к поставщику Intemet-услуг

Передача информации и аутентификация

Поставщикам Интернет-услуг СЛЕДУЕТ иметь ясные правила и процедуры, касающиеся разделения информации о нарушении безопасности со своими потребителями, с другими поставщиками или группами реагирования, с правоохранительными органами, средствами массовой информации и общественностью.

Поставщикам Интернет-услуг СЛЕДУЕТ иметь средства для организации защищенного канала с целью передачи подобной информации. Отметим, однако, что не везде законы разрешают защищенные коммуникации.

Защита Интернет-сообщества

Поставщики Интернет-услуг играют критически важную роль в повышении безопасности Интернет. В этом и следующем разделах рассматриваются меры, которые, в случае их скоординированного и оперативного принятия поставщиками Интернет-услуг, оказали бы на сетевую безопасность существенное положительное влияние и значительно затруднили злоумышленникам сокрытие следов.

Затем мы относительно подробно рассмотрим вопросы, касающиеся специфических услуг, таких как входная фильтрация и организация открытых систем промежуточного хранения и пересылки почтовых сообщений. Согласованное решение этих вопросов поставщиками Интернет-услуг также дало бы заметный позитивный эффект.

Каждому поставщику Интернет-услуг СЛЕДУЕТ иметь политику добропорядочного пользования.

Контракт между поставщиком и потребителем Интернет-услуг следует составлять с учетом этой политики, быть может, пересматривая политику при продлении контракта. Потребителя следует заранее информировать об изменениях в политике.

В политике следует ясно определить, что потребители могут или не должны делать в разных частях сети и на разных системах, включая допустимые типы трафика.

Защита данных

Во многих странах есть законы о защите данных. В ситуациях, когда подобные законы применимы, поставщики Интернет-услуг должны проанализировать характер поступающих к ним персональных данных и, если нужно, принять меры, препятствующие противозаконному использованию данных. Учитывая глобальный характер Интернет, поставщикам Интернет-услуг, действующим в странах, где таких законов нет, следует хотя бы ознакомиться с идеей защиты данных, прочитав, например, Data Protection Act[5].

Обучение

Важно, чтобы весь штат поставщика Интернет-услуг был соответствующим образом подготовлен, то есть постоянно помнил о проблемах информационной безопасности, с пониманием подходил к их решению, умел должным образом применять средства повышения безопасности. К числу наиболее важных принадлежат вопросы использования защищенных каналов для передачи конфиденциальной информации, риска атак с применением методов морально-психологического воздействия, управления аутентификационными данными и т.д.

Сетевая инфраструктура

Поставщики Интернет-услуг ответственны за такое управление сетевой инфраструктурой Интернет, чтобы:

– обеспечивалась разумная устойчивость к появлению известных слабостей в защите;

– атакующие не могли легко и просто организовать плацдарм для последующих атак.

Маршрутизаторы

Маршрутизаторы не только сами по себе являются притягательными целями атак на безопасность, но и представляют собой отличный плацдарм для организации атак на другие цели.

Многие маршрутизаторы позволяют злоумышленникам делать опасные вещи, например:

– "прослушивать" транзитные потоки данных;

манипулировать таблицами маршрутизации для перенаправления потоков данных;

– изменять состояние интерфейсов с целью нарушения обслуживания;

вызывать "трепыхание" маршрутных таблиц, чреватое отказом в обслуживании для крупных частей Интернет;

– создавать пакеты с поддельными адресами и любым желаемым набором флагов;

– порождать штормы ICMP-пакетов, устраивать другие атаки на доступность;

отправлять потоки данных в "черную дыру" (например, организуя локальный маршрут на пустой или некорректный интерфейс или на некорректный следующий маршрутизатор, который не знает нужного маршрута и не имеет подразумеваемого маршрутизатора, или, что хуже всего, используя протокол динамической маршрутизации для афиширования маршрута с низкой стоимостью, активно втягивая тем самым трафик в черную дыру);

– скрывать обращения по внешним адресам, что облегчается недостаточным протоколированием в маршрутизаторах.

Усилению подобных угроз способствует та центральная роль, которую играют маршрутизаторы в сетевой инфраструктуре, а также нередко доступная им широкая полоса пропускания.

Таким образом, доступ к маршрутизаторам СЛЕДУЕТ основывать на одноразовых паролях или еще более сильных средствах (таких, например, как Kerberos) и ограничивать в максимально возможной степени. Обращения к маршрутизатору следует протоколировать, привлекая ресурсы других систем.

Если маршрутизатор поддерживает различные уровни авторизации, эти уровни следует использовать для ограничения привилегированного доступа к маршрутизатору.

Сеансы взаимодействия с маршрутизаторами следует шифровать для предотвращения краж сеансов или данных и для недопущения атак, основанных на воспроизведении трафика.

На маршрутизаторы не следует возлагать выполнение мелких услуг, которые нередко включены по умолчанию. Имеются в виду bootp, chargen, daytime, discard, echo, finger и т.д.

Коммутаторы, терминальные серверы, модемы и другое сетевое оборудование

Поставщикам Интернет-услуг следует быть столь же бдительными при конфигурировании всех видов сетевого оборудования. К сожалению, многие подобные устройства, находящиеся в эксплуатации, поддерживают лишь слабые методы аутентификации, предоставляют права доступа по принципу "все или ничего" и не протоколируют почти (или совсем) ничего. В прошлом у поставщиков Интернет-услуг не оставалось улик, по которым можно было бы проследить нарушителя, после того как он

переконфигурировал коммутаторы, использовал терминальные серверы для атак на сторонние организации или выключил источники бесперебойного питания.

По возможности доступ к сетевому оборудованию следует ограничивать, предоставляя его только уполномоченным сетевым администраторам.

Оборудование, составляющее сетевую инфраструктуру, нередко не поддерживает сколько-нибудь развернутого внутреннего протоколирования, поскольку в нем нет долговременной памяти, такой как жесткие диски компьютеров. Впрочем, многие устройства поддерживают syslog или SNMP-сообщения или, по крайней мере, небольшой внутренний регистрационный журнал или отладочный режим, так что соответствующую информацию можно направить на консоль или в удаленный протокол.

Конфигурационную информацию маршрутизаторов и коммутаторов следует обязательно сопровождать на файловом сервере, чтобы возврат к прежней конфигурации мог быть выполнен легко и быстро. Разумеется, подобные резервные конфигурационные файлы следует защитить от несанкционированной передачи или злоумышленного изменения.

Анонимный telnet и другие непротоколируемые соединения

Имеется много сетевых устройств, от недорогих маршрутизаторов до принтеров, принимающих соединения по протоколу telnet без запроса пароля. Разумеется, подобные устройства, зачастую лишенные средств протоколирования, весьма популярны среди злоумышленников, желающих скрыть свои следы.

Если в сети поставщика Интернет-услуг есть такое оборудование, доступ к нему следует ограничить. Кроме того, потребителям следует рекомендовать блокировать доступ к подобным устройствам из внешних сетей.

Крайне нежелательно использовать протокол telnet для управления компонентами сети.

Центр управления сетью и сетевое администрирование

Центр управления сетью (ЦУС) является критически важной частью инфраструктуры поставщика Интернет-услуг, поэтому его работу следует строить с соблюдением должных мер безопасности.

ЦУС зачастую располагает административным контролем над конфигурационной информацией сетевого оборудования, поэтому следует проявить бдительность, ограничив доступ к такой информации. Загрузка конфигурационных файлов в сетевые устройства до сих пор нередко производится по протоколу TFTP, который не только лишен средств аутентификации и использует незащищенные коммуникации, но и требует повышенной осторожности при конфигурировании на серверной стороне.

Как правило, ЦУС выполняет функции мониторинга сети, периодически опрашивая (например, посредством SNMP-сообщения Echo) множество сетевых устройств. При определении набора опрашиваемых устройств следует помнить о критически важной роли оборудования, перечисленного в разделе 5.2.

Помимо простого опроса, ЦУС для взаимодействия с сетевыми устройствами может также использовать управляющий протокол, такой как SNMP. Обычно протокол применяется для выяснения (посредством операции get) значений различных переменных, таких как число пакетов, принятых через определенный интерфейс. Однако, протокол может применяться и для установки переменных (операция set), возможно, с далеко идущими последствиями (такими как переконфигурирование устройства). В любом случае, в протоколе SNMPv1 присутствует только тривиальная аутентификация. По возможности, SNMP следует применять только как средство чтения, получения (get) информации от удаленных устройств. Полученную информацию следует трактовать как конфиденциальную.

Еще одно применение протокола SNMP состоит в уведомлении управляющей станции о возникновении исключительных ситуаций (SNMP trap). Такую информацию

также следует считать конфиденциальной, а в ЦУСе следует проявить осторожность, чтобы подобные SNMP-сообщения сами по себе не вылились в атаку на доступность.

Физическая безопасность

Физической защите информационных систем следует уделять соответствующее внимание. Это особенно верно, если в одном месте располагается несколько систем, так что к ним имеют доступ сотрудники различных организаций с разной политикой безопасности.

Нас будут особенно интересовать три случая совместного расположения ресурсов:

– оборудование потребителей располагается на площадке поставщика Интернет-услуг;

– оборудование поставщика Интернет-услуг размещено на удаленной площадке под присмотром уполномоченного персонала;

–оборудование поставщика Интернет-услуг располагается на удаленной площадке без контроля физического доступа.

Скорее всего, потребителя может непосредственно затронуть первый случай. Если поставщик Интернет-услуг предоставляет площади для размещения оборудования потребителей, то возникает множество вопросов, связанных с доступом последних к своему оборудованию, соседствующему с системами поставщика услуг.

В идеале, каждый потребитель должен получить полностью закрытую, запирающуюся "клетку", то есть небольшую комнату со стенами и проемами для прокладки множества проводов, а также со стойками для монтажа оборудования. Потребителям предоставляется доступ в отведенное помещение в сопровождении сотрудника поставщика Интернет-услуг (либо потребитель получает ключи только от своей комнаты).

Выделение отдельных комнат, однако, может оказаться слишком накладным, так что многие поставщики Интернет-услуг идут на компромисс, собирая все "чужое" оборудование в одном машинном зале и тщательно контролируя все, что делают потребители. К сожалению, этого может оказаться недостаточно, чтобы избежать недоразумений, таких как нечаянное отключение оборудования другого потребителя. Вместо единого открытого пространства, следует разделить зал перегородками, построив для каждого потребителя отдельное помещение с запирающейся дверью.

Потребителя не следует оставлять без присмотра вблизи чужого оборудования. Такое оборудование запрещается трогать, фотографировать или исследовать.

Следует помнить также о безопасности на втором уровне семиуровневой модели, запрещая разделение физического сегмента сети между оборудованием потребителя и компьютерами, принадлежащими другим потребителям или поставщику Интернет-услуг. Нередки случаи, когда злоумышленники пользуются слабостями в защите или незашифрованными удаленными входами в оборудование потребителя, получают контроль над этими устройствами, переводят его в режим прослушивания сегмента локальной сети, потенциально нарушая тем самым конфиденциальность или безопасность других устройств в этом сегменте.

Вопросы безопасности чрезвычайно важны и тогда, когда компоненты сетевой инфраструктуры поставщика Интернет-услуг размещены вне его территории (например, у партнера или в удаленной точке присутствия). Такие компоненты нередко являются жизненно важными с точки зрения топологии сети и, в то же время, они могут стать объектом атаки или пострадать от несчастного случая. Для ограничения физического доступа оборудование в идеальном случае следует размещать в полностью закрытых, запирающихся комнатах или "клетках". Если на чужой площади хранятся запчасти, их также следует защищать от кражи, порчи или встраивания "жучков". По возможности следует использовать системы безопасности и замки, открывающиеся персональными картами. Периодически удаленные компоненты нужно проверять на предмет встраивания постороннего оборудования, которое может использоваться для прослушивания сетевых

соединений. Как и на других площадках, компьютеры не следует подключать к транзитным сегментам или допускать подсоединение к сети неиспользуемых физических интерфейсов.

Инфраструктура маршрутизации

Способность поставщика Интернет-услуг направлять потоки данных к правильному конечному пункту зависит от правил маршрутизации, заданных в виде маршрутных таблиц (см. [13]). Поставщикам Интернет-услуг следует убедиться, что находящаяся в их ведении маршрутная информация может быть изменена только после надежной аутентификации и что права на внесение изменений должным образом ограничены.

Двойную осторожность следует проявлять и при решении вопроса о том, кому больше доверять при наличии нескольких маршрутов, ведущих к цели. В прошлом злоумышленное афиширование маршрутной информации приводило к попаданию потоков данных в "черную дыру" или, что хуже, к перехвату соединений. В граничных маршрутизаторах следует аутентифицировать соседей в рамках протокола BGP.

При выборе протоколов внутренней маршрутизации поставщикам Интернет-услуг также следует помнить о безопасности. При конфигурировании не следует предполагать, что перевычисления маршрутов редки и дороги, поскольку это открывает путь для атак на доступность. При изменении маршрутов следует использовать наивысший уровень аутентификации, поддерживаемый протоколом внутренней маршрутизации.

Если от партнеров начинает поступать большое число объявлений о наличии специфических маршрутов к частям выделенного поставщику Интернет-услуг пространства адресов, следует проявлять осторожность, решая, учитывать ли эти объявления. Впрочем, с данной проблемой могут столкнуться только поставщики, допускающие фрагментацию своего пространства адресов (то есть позволяющие потребителям сохранять адреса при смене поставщика Интернет-услуг). Предполагается, что используется бесклассовая междоменная маршрутизация (CIDR).

Входная фильтрация по исходным адресам

Направление входной фильтрации –от периферийной системы (потребитель) к Интернет (рис. 1).

Нередко атакующие скрывают следы, подделывая исходные адреса. Чтобы отвлечь внимание от своей системы, они выбирают в качестве исходного адрес невинной удаленной системы или даже из пространства адресов, выделенных для частных объединений сетей [16]. Кроме того, поддельные исходные адреса часто применяются в атаках, основанных на использовании отношения доверия между узлами сети.

Чтобы уменьшить область распространения атак, основанных на подделке исходных адресов, поставщики Интернет-услуг должны делать следующее. Во всех граничных маршрутизаторах, к которым подключены потребители, следует сразу отфильтровывать потоки данных, идущие от потребителей и имеющие исходные адреса, отличные от выделенных данному потребителю. Более подробно этот вопрос освещен в спецификации [26].

Иногда возникают ситуации, когда входная фильтрация пока оказывается невозможной. Например, большой агрегирующий маршрутизатор может не выдержать дополнительную нагрузку, вызванную применением пакетных фильтров. Кроме того, подобная фильтрация способна привести к трудностям для мобильных пользователей. Следовательно, хотя использование данного метода для борьбы с подделкой адресов настоятельно рекомендуется, оно не всегда возможно.

В тех редких случаях, когда входная фильтрация на стыке потребителя и поставщика Интернет-услуг невозможна, следует рекомендовать потребителю организовать входную фильтрацию внутри его сети. Вообще, фильтрацию следует производить как можно ближе к хостам.

Выходная фильтрация по исходным адресам

Направление выходной фильтрации –от Интернет к периферийной системе (потребитель) (рис. 2).

В настоящее время в Интернет широко используется много приложений, считающих другие узлы сети надежными, основываясь исключительно на IP-адресах (например, r-команды, пришедшие из BSD). Такие приложения уязвимы по отношению к подделке IP-адресов (см. [2]). Кроме того, имеются уязвимости по отношению к злоумышленному использованию адресов, которые предполагаются локальными (например, land, см. [4]).

Чтобы усилить защиту потребителей от атак, основанных на подделке исходных адресов, поставщики Интернет-услуг должны делать следующее. Во всех граничных маршрутизаторах, к которым подключены потребители, следует сразу отфильтровывать потоки данных, идущие к потребителю и имеющие исходные адреса из пространства, выделенного этому потребителю.

Препятствия для входной фильтрации, описанные в пункте 5.7, делают невозможной и выходную фильтрацию.

Фильтрация маршрутной информации

Избыточные изменения маршрутной информации могут использоваться злоумышленником как средство увеличения загрузки, на базе которого развивается атака на доступность. Как минимум это приведет к деградации производительности.

Поставщикам Интернет-услуг следует отфильтровывать поступающие объявления о маршрутах, игнорируя, например, маршруты к адресам для частных объединений сетей, избегая фиктивных маршрутов и реализуя политику расщепления и агрегирования маршрутов.

Поставщики Интернет-услуг должны применять методы, уменьшающие риск нарастания нагрузки на маршрутизаторы в других частях сети. Следует отфильтровывать "кустарные" маршруты, настойчивое агрегирование и расщепление маршрутов. Все это снижает Ваше воздействие на других, когда Вы производите внутренние изменения, других не касающиеся.

Направленное вещание

Протокол IP поддерживает направленное вещание –посылку через сеть пакетов, которые в определенной подсети станут широковещательными. Практической пользы от такой возможности весьма немного, зато на ней основывается несколько различных видов атак (в первую очередь, это атаки на доступность, использующие эффект размножения широковещательных пакетов). Следовательно, маршрутизаторы, подключенные к вещательной среде, НЕ СЛЕДУЕТ конфигурировать так, чтобы было возможным непосредственное вещание на эту среду (см. [28]).

Если приходит пакет, на который маршрутизатор ответил бы, будь пакет послан в "невещательном" режиме, маршрутизатор МОЖЕТ послать (одиночный) ответ. Если он не отвечает (либо потому, что это не нужно, либо потому, что он так сконфигурирован), он МОЖЕТ послать ICMP-ошибку. Допускается также и молчаливое игнорирование подобных пакетов. В любом случае, такие пакеты нужно считать, чтобы выявить возможные попытки злоупотребления вещанием.

Системная инфраструктура

То, как поставщик Интернет-услуг управляет своими системами, критически важно для безопасности и надежного функционирования сети.

Нарушения в работе систем могут в лучшем случае привести к снижению производительности или функциональности, но могут также вызвать потерю данных или сделать возможным перехват сетевого трафика (быть может, с последующей атакой методом "нелегального посредника").

Следует действовать по принципу "Боливар не вывезет двоих", распределяя сервисы по системам. Иными словами, предоставление разных услуг следует возлагать на разные системы. Кроме выгод от облегчения системного администрирования, можно

сослаться на многократно проверенный факт, что гораздо проще построить защищенную систему, если разные услуги (такие как почта, телеконференции или размещение Web-серверов) поддерживаются на разных системах.

Все обсуждаемые далее услуги выиграют от организации надежной защиты на сетевом уровне средствами IPsec.

Политика безопасности

Политика поставщика Интернет-услуг по отношению к защите персональных данных, обеспечению аутентичности, подотчетности, наложению защитных заплат, поддержке доступности, реагированию на доклады о нарушениях представляет интерес для потребителей. Ее следует опубликовать в общедоступном месте, например, на Web-сервере поставщика услуг.

Более детальное обсуждение политики безопасности можно найти в Руководстве по информационной безопасности предприятия.

Управление системами

Доступ ко всем системам поставщика Интернет-услуг, выполняющим критически важные функции, такие как почта, телеконференции и размещение Web-серверов, следует ограничить, предоставляя его только администраторам соответствующих услуг. Доступ следует предоставлять только после надежной аутентификации и осуществлять по шифруемому каналу. Следует делать доступными из внешних сетей только те порты, на которых ожидают подключения предоставляемые услуги.

Если поставщик услуг ведет учет работы потребителей, то системы, обеспечивающие этот учет, следует изолировать от остальной части сети.

Если распространение и обновление программного обеспечения производится с помощью автоматизированных средств, таких как rdist, им следует предоставлять защищенный канал и надежную аутентификацию, применяя, например, Secure Shell (ssh).

Системы не следует подключать к транзитным сегментам.

Если допускается применение паролей условно-постоянного действия, пользователей следует ознакомить с правилами выбора и сохранения пароля в тайне, предварительной проверки качества пароля, управления сроком годности пароля. Следует задействовать программы подбора паролей.

Резервное копирование

Нет смысла лишний раз подчеркивать важность резервного копирования. Однако, резервное копирование может являться самым слабым звеном в системной безопасности, если защита резервных носителей не налажена должным образом.

При копировании по сети следует пользоваться защищенным каналом. Если в процессе резервного копирования данные помещаются на промежуточные диски, то доступ к этим дискам следует ограничить в максимально возможной степени.

После нарушения безопасности резервные копии приобретают дополнительное значение как носители данных для анализа.

Отслужившие срок носители должны уничтожаться, а не выбрасываться.

Пользователей систем и услуг следует информировать о том, что сохраняется на резервных копиях, а что нет. Более того, если пользователю сообщили, что определенные данные не сохраняются, то их не следует копировать.

Распространение программного обеспечения

Поставщикам Интернет-услуг приходится часто распространять прикладное программное обеспечение. Целостность ПО должна гарантироваться путем вычисления и распространения вместе с ПО криптографических контрольных сумм, таких, например, как в алгоритме SHA-1 [SHA].

Доменная система имен

Доменная система имен (DNS) играет критически важную роль в повседневной деятельности миллионов пользователей Интернет. Прискорбно, что приложения зачастую слепо доверяют информации DNS, уверены в постоянной доступности DNS. Однако, до

введения протокола DNSSEC [20], в DNS явно недоставало средств защиты, а реализации содержали серьезные слабости (см. [32]).

Хотя далее и предлагаются некоторые методы повышения защищенности и надежности DNS, хочется подчеркнуть, что аутентификация, основанная на именах, внутренне небезопасна.

Администрирование DNS-сервера

В дополнение к мерам, описанным в разделе 6, поставщикам Интернет-услуг при администрировании DNS-серверов следует обратить внимание еще на несколько аспектов:

– Мониторинг. Следует контролировать доступность DNS (способность отвечать на запросы).

– Синхронизация часов. Серверам следует синхронизировать часы с помощью протокола NTP (см. [RFC1305]) с аутентификацией. Следует использовать по крайней мере два NTP-сервера.

Надежная доменная система имен

Надежный сервер в смысле DNS обладает локальным знанием DNS-зоны, поэтому для ответов на запросы по этой зоне ему не нужно обращаться к другим серверам. Потребителям следует обдумать (см. [23]), на каких вторичных DNS-серверах остановить свой выбор.

Поставщики Интернет-услуг обычно выполняют для своих потребителей роль вторичных (подчиненных) серверов, и эти серверы могут обслуживать тысячи зон. Независимо от числа зон, администраторам серверов следует ознакомиться с документом "Operational Criteria for Root Name Servers" [19] как с отправной точкой на пути обеспечения высокой доступности службы имен. В частности, следует руководствоваться такими положениями:

При обработке запросов следует запретить рекурсию.

Передачу зон следует ограничить. Помимо значительной нагрузки, вызываемой передачей зон и увеличивающей риск атак на доступность, поставщикам Интернет-услуг следует учесть, что некоторые из потребителей считают свои файлы зон конфиденциальными.

Производительность следует контролировать, отслеживая такие ключевые характеристики, как число запросов в секунду и средняя задержка.

Услуга DNS-разрешения

Как правило, поставщик Интернет-услуг предоставляет своим потребителям сервис DNS-разрешения. При этом потребители конфигурируют свои "DNS-разрешители" (клиенты) так, чтобы те обращались к серверам DNS-разрешения поставщика Интернет-услуг, которому следует руководствоваться такими положениями:

При обработке запросов следует допускать рекурсию. Это значит, что поставщик Интернет-услуг не должен использовать один и тот же сервер для сервисов разрешения и надежного DNS.

Передачу зон следует запретить. Хотя при нормальной работе зоны передавать и не придется, лучше лишний раз защититься от атак на доступность.

Производительность следует контролировать, отслеживая такие ключевые характеристики, как число запросов в секунду и средняя задержка. Кроме того, следует периодически сообщать о хостах, генерирующих наибольшее число запросов.

В программном обеспечении сервера имен не должно быть слабости, связанной с "отравлением" кэша, когда злоумышленные или ошибочные данные, полученные от удаленного сервера имен, кэшируются и становятся доступными для DNS-разрешения.

Почтовые услуги

Электронная почта стала целью ряда наиболее известных атак, а также тысяч детских шуток и шалостей.

Поставщики Интернет-услуг играют главную роль в защите общества от злоупотреблений, а также в обучении своих потребителей соответствующим методам обеспечения информационной безопасности.

Администрирование почтовых серверов

При конфигурировании почтовых серверов поставщикам Интернет-услуг следует руководствоваться такими положениями:

Выбор программного обеспечения. По возможности следует использовать ПО с раздельными агентами приема/отправки и обработки. Идея состоит в том, чтобы агент приема/отправки, взаимодействующий с удаленными почтовыми серверами, выполнялся с минимальными привилегиями.

Ограничение удаленного запуска очередей сообщений. Запуск очередей по запросу (предоставляемый для удобства потребителей, получающих почту в своем домене и не имеющих постоянного соединения) должен быть ограничен, желательно средствами надежной аутентификации. Удаленный запуск очередей сообщений реализуется разными механизмами, такими, например, как ETRN –расширение SMTP-сервиса (см. [18]).

Отключение VRFY and EXPN. Не следует предоставлять информацию о локальных пользователях или механизмах доставки, выходящую за рамки необходимого.

Синхронизация часов. Серверам следует синхронизировать часы с помощью протокола NTP (см. [11]) с аутентификацией. Следует использовать по крайней мере два NTP-сервера.

Информирование об исключительных ситуациях. Исключительные ситуации, такие как повторяющиеся неудачи аутентификации, зацикливание почты, ненормальная длина очереди, следует выявлять и генерировать соответствующие доклады.

Ограничение доступа к регистрационной информации о почте. Регистрационная информация о работе почты должна быть доступна на чтение только системному администратору.

Защищенная почта

Как отмечалось в разделе 3.4, критически важно, чтобы поставщики Интернет-услуг и, в частности, их группы реагирования на нарушения информационной безопасности, располагали средствами защищенного обмена сообщениями.

Открытые системы промежуточного хранения и пересылки почты

Говорят, что почтовый SMTP-сервер функционирует в режиме "открытой" системы промежуточного хранения и пересылки почты, если он допускает прием и пересылку нелокальным адресатам таких сообщений, которые были порождены нелокально (иными словами, адреса как отправителя, так и получателя являются нелокальными). Такие открытые системы пересылки почты нередко используются "спамерами", организующими массовую незапрошенную рассылку с сокрытием инициатора. Только в весьма специфических обстоятельствах можно оправдать решение администратора сделать систему пересылки в Интернет полностью открытой.

Способы ограничения пересылки почты хорошо документированы. Весьма прискорбно, что некоторые крупные поставщики программного обеспечения поставляют свои агенты передачи сообщений с включенной по умолчанию опцией пересылки.

Безопасность электронной почты –забота общая, но поставщикам Интернет-услуг следует быть особенно бдительными, отключая функцию открытой пересылки на администрируемых ими серверах, поскольку доступная им широкая полоса пропускания делает их серверы особенно привлекательными в качестве плацдарма спамера.

Поставщикам Интернет-услуг следует настоятельно рекомендовать своим потребителям запретить открытую пересылку на "потребительских" почтовых серверах. Ситуации, в которых разрешена организация открытой пересылки почты, следует документировать в "Политике допустимого использования" поставщика Интернет-услуг.

Представление сообщений для отправки

Чтобы облегчить проведение в жизнь политики безопасности, представлять сообщения для отправки следует через порт MAIL SUBMIT (587), как это предлагается в проводимой в настоящее время работе "Message Submission and Relay", а не через SMTP-port (25). Кроме того, представление сообщения следует аутентифицировать с помощью расширения AUTH SMTP-сервиса (в соответствии с проводимой в настоящее время работой "SMTP Service Extension for Authentication"). При таком подходе функции SMTP-порта (25) могут быть ограничены локальной доставкой.

Перечисленные меры не только защищают поставщика Интернет-услуг от превращения в плацдарм спамера, но и позволяют поддерживать подотчетность представления сообщений в ситуациях, когда потребитель рассылает спам. Далее, использование порта MAIL SUBMIT в сочетании с функцией SMTP AUTH имеет еще и то преимущество перед ограничениями по IP-адресам на представление сообщений, что оно дает потребителям дополнительную гибкость, позволяя представлять сообщения, даже если они подключились не через сеть своего обычного поставщика Интернет-услуг (например, при отправке письма с работы). Кроме того, обеспечивается большая устойчивость к подделке IP-адресов и сохраняется возможность модернизации механизмов аутентификации при появлении новых мощных средств.

Заслуживает внимания и (недокументированное) расширение XTND XMIT POP3, позволяющее клиентам отправлять почту в рамках сеанса POP3, а не по протоколу SMTP. При этом обеспечивается поддержка мобильных пользователей при отключенной функции открытой пересылки, предоставляется аутентифицированное, протоколируемое соединение.

Сервисы POP и IMAP

Поставщикам Интернет-услуг, представляющим своим потребителям доступ к почтовым ящикам по протоколам POP или IMAP, следует, как минимум, поддерживать механизмы аутентификации CRAM-MD5 [24] или APOP [17]. Следует рассмотреть возможность использования более сильной аутентификации, равно как и запрет на аутентификацию на основе передаваемых в открытом виде имен и паролей.

2. Размещения Web-серверов

Многие организации передают свои Web-серверы поставщикам Интернет-услуг вместе с обязанностями по эксплуатации и администрированию. Главную роль при принятии такого решения играют соображения информационной безопасности. Тема данного раздела –размещение Web-серверов и сопутствующие услуги. Более детальную информацию можно найти в работах [6] и [7].

Администрирование сервера с размещенными Web-серверами

Помимо аспектов, описанных в разделе 6, поставщикам Интернет-услуг при администрировании сервера с размещенными Web-серверами следует руководствоваться такими положениями:

Постоянный мониторинг. Следует контролировать доступность сервиса (способность отвечать на HTTP-запросы).

Синхронизация часов. Серверам следует синхронизировать часы с помощью протокола NTP (см. [11]) с аутентификацией. Следует использовать по крайней мере два NTP-сервера.

Разумное использование DNS. В момент подключения клиента не следует выполнять поиск его имени, поскольку это делает Web-серверы уязвимыми для атак на доступность и заметно сказывается на производительности.

Минимизация привилегий. Web-демон следует выполнять от имени пользователя и группы, специально выделенных для этой цели и имеющих минимальные привилегии. Ответственный за информационное наполнение Web-сервера должен работать от имени другого пользователя.

Контроль DocumentRoot. Все, что располагается ниже этого каталога, следует тщательнейшим образом проконтролировать. Желательно использовать системный вызов chroot для смены корневого каталога HTTP-демона.

Контроль UserDir. На сервере не следует иметь других пользователей, кроме администраторов. Если такие пользователи все-таки есть, директиве "UserDir" (если она разрешена) не следует предоставлять доступ к информации пользователей. В частности, не следует разрешать выполнение командных процедур от имени этих пользователей.

Разбиение на виртуальные серверы. Единый сервер, на котором размещено множество серверов (виртуальных доменов), СЛЕДУЕТ организовать так, чтобы все данные, программы и регистрационные журналы различных виртуальных серверов были отделены друг от друга и чтобы доступ к "чужой" конфигурации или данным был невозможен. Кроме того, следует исключить доступ к данным или программам на сервере одного потребителя через локатор ресурсов, в хостовой части которого указано имя сервера другого потребителя.

Управление доступом. Следует сделать возможным разграничение доступа к определенным частям сервера на основе механизмов надежной аутентификации, таких как сертификаты или одноразовые пароли. Другим возможным вариантом является применение хорошо выбранных паролей в сочетании с протоколом SSL, который по крайней мере исключает передачу паролей по сети в открытом виде.

Установка заплат и сервисных дополнений. Эксплуатация Web-сервера – деятельность особо ответственная, поэтому администраторам следует быть особенно аккуратными в установке заплат и сервисных дополнений по мере их появления.

Программы на серверной стороне

Программы на серверной стороне, поддерживающие CGI или какой-либо другой интерфейс, важны для гибкости web как коммуникационной среды. Однако, эта гибкость достигается ценой появления угроз безопасности, а слабая программа может сделать уязвимыми все виртуальные домены на сервере. Политика поставщика Интернет-услуг при разделении программ на допустимые и недопустимые является показательным аспектом всей его политики безопасности.

Поставщику Интернет-услуг следует руководствоваться такими положениями:

Политика безопасности. Поставщику Интернет-услуг следует выработать для своих потребителей ясную методику написания безопасных программ в имеющейся среде размещения Web-серверов и отдельно описать приемы программирования, при применении которых программы будут отвергаться.

Установка программ. Потребителям не следует разрешать устанавливать собственные программы. Все программы и командные процедуры следует передавать поставщику Интернет-услуг для первоначальной проверки на соответствие политике безопасности. Программы СЛЕДУЕТ устанавливать так, чтобы только администратор сервера мог их модифицировать.

Выбор пользователя и группы процесса. Программы следует выполнять от имени пользователя и группы, специально выбранных для этой цели и имеющих минимальные привилегии (часто используют "nobody").

Отображение в навигаторах. Ни при каких обстоятельствах НЕ СЛЕДУЕТ допускать отображения программ в навигаторах. Следствие: программы НЕ СЛЕДУЕТ размещать под DocumentRoot.

Разделение виртуальных серверов. Программы НЕ СЛЕДУЕТ делать доступными через сервер другого потребителя или для Web-мастера другого потребителя.

Обработка пользовательского ввода. В пользовательском вводе НЕ СЛЕДУЕТ вычислять выражения, если нет механизма изоляции небезопасных действий (как, например, в Perl).

Лимитирование потребления ресурсов. Для всех программ СЛЕДУЕТ ввести лимит потребляемого астрономического и процессорного времени, а также дискового пространства.

Маршрутные имена. Все маршрутные имена СЛЕДУЕТ делать абсолютными или начинающимися с DocumentRoot. Переменную PATH следует устанавливать системному администратору.

Данные и базы данных

Данные, которые пишет программа серверной стороны, следует считать конфиденциальными. Чтобы сделать невозможным доступ к таким данным через навигаторы, права следует устанавливать так, чтобы у Web-демона не было права на чтение этих данных.

Если через Web-сервер предоставляется доступ к базам данных, то программам, осуществляющим такой доступ, следует выделить только те полномочия, которые абсолютно необходимы для их функционирования.

Данные, относящиеся к управлению состояниями (идентифицирующие цепочки – cookies), следует считать конфиденциальными. Следует исключить возможность доступа к ним из навигаторов.

Обработка регистрационной и статистической информации

Регистрационная информация, генерируемая Web-демоном, может быть полезна с точки зрения информационной безопасности, поскольку в ней содержатся сведения об операциях, выполнявшихся сервером. Чаще, однако, эту информацию используют для выставления счетов, а также для маркетингового анализа или улучшения информационного наполнения.

Регистрационную информацию следует считать весьма конфиденциальной. Для реализации этого положения:

Поставщику Интернет-услуг следует разрешить выполнение лишь необходимых операций с регистрационной информацией –генерацию счетов и периодическую ротацию.

Регистрационную информацию следует хранить вне дерева с корнем в DocumentRoot, чтобы исключить возможность доступа через навигаторы.

Регистрационную информацию в первоначальном или обработанном виде следует передавать потребителю только по защищенному каналу.

Услуги принудительной или потоковой передачи

Нередко поставщики Интернет-услуг дают своим потребителям возможность доставлять информацию с помощью протоколов, отличных от HTTP. При наличии подобных дополнительных услуг и поставщику-Интернет-услуг, и потребителям следует осознать их воздействие на информационную безопасность.

Электронная коммерция

Многие поставщики Интернет-услуг предоставляют своим потребителям средства для продажи товаров или услуг через размещенные у поставщика Web-серверы. И хотя сервер, способный обмениваться информацией с навигатором по протоколу SSL, иногда называют "защищенным", этот термин в данном случае нельзя понимать буквально. Поставщику Интернет-услуг, разместившему у себя приложения электронной коммерции, следует руководствоваться такими положениями:

Шифрование транзакций. Транзакции ни в коем случае не следует хранить на сервере в открытом виде. Может использоваться криптография с открытыми ключами, так что только потребитель сможет расшифровать транзакции. Отметим, что даже если транзакции передаются напрямую в финансовое учреждение или потребителю, поставщик Интернет-услуг может сохранять у себя какую-то часть данных для обеспечения подотчетности.

Передача транзакций. Если транзакции не обрабатываются немедленно, а передаются потребителю пакетами, то передачу следует производить по защищенному (например, средствами SSL) каналу и только после проведения надежной

аутентификации. Следует аккуратно производить ротацию транзакционных файлов, чтобы каждая транзакция выполнялась ровно один раз.

Резервное копирование. Если транзакции записываются на резервные носители, следует гарантировать физическую безопасность этих носителей.

Загрузка информационного наполнения и распределенное авторство

Загрузку информационного наполнения на сервер поставщика Интернет-услуг следует производить по защищенному каналу.

Если сервер поддерживает средства для распределенного авторства, их следует администрировать с особой осторожностью, гарантируя, что имеет место надежная аутентификация, что доступ предоставляется только к виртуальному серверу потребителя и только для лиц, управляющих информационным наполнением.

Поисковые машины и другие средства

Поставщики Интернет-услуг нередко предоставляют для использования потребителями поисковые машины, средства контроля целостности ссылок и т.д. Зачастую такие средства создают весьма существенную дополнительную нагрузку, поэтому их запуск по запросу следует запретить, чтобы защититься от атак на доступность.

Поисковые машины следует сконфигурировать так, чтобы поиск ограничивался частями Web-сервера, доступными всем. Результат проверки целостности ссылок следует считать конфиденциальным. Доступ к нему следует предоставить только лицу, управляющему информационным наполнением.

Вопросы и задания:

Базовый уровень:

1. Политика добропорядочного пользователя.
2. Оповещение об атаках.

Повышенный уровень:

3. Группа реагирования на нарушение ИБ.

Список литературы, рекомендуемый к использованию по данной теме

1. Основная литература:

1. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012.

2. Дополнительная литература:

1. Обеспечение информационной безопасности машиностроительных предприятий. Учебник для вузов./ Под ред. П.П. Мельникова. – М.: Сатурн-С, 2006.

2. Галатенко В.А. Стандарты информационной безопасности. Курс лекций / Под ред. акад. РАН Бетелина. – М.: Интернет-университет информационных технологий, 2006.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А. – Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.

Практическое занятие № 6. Анализ защищенности. СУБД
Учебные и воспитательные цели:
Изучить требования и рекомендации по защите информации.

Теоретическая часть

«Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждены приказом Гостехкомиссии России от 30.08.2002 №282.

СТР-К является нормативно-методическим документом и устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну на территории Российской Федерации.

Требования и рекомендации этого документа распространяются на защиту государственных информационных ресурсов некриптографическими методами (служебная тайна), направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и специальных воздействий на информацию в целях еѐ уничтожения, искажения и блокирования.

При проведении работ по защите негосударственных информационных ресурсов, составляющих коммерческую тайну, банковскую тайну и т.д., требования настоящего документа носят рекомендательный характер.

Документ определяет следующие вопросы защиты конфиденциальной информации:

– организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;

– состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;

– требования и рекомендации по защите речевой информации при ведении переговоров, в том числе с использованием технических средств;

– требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;

– порядок обеспечения защиты информации при эксплуатации объектов информатизации;

– особенности защиты информации при разработке и эксплуатации АС, использующих различные типы СВТ и информационные технологии;

– о порядок обеспечения защиты информации при взаимодействии абонентов с Сетями.

Защита информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в виде системы (подсистемы) защиты информации во взаимосвязи с другими мерами по защите информации. Защите подлежит речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнито-оптической и иной основе.

Объектами защиты при этом являются:

– средства и системы информатизации (СВТ, АС различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования

документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для обработки конфиденциальной информации;

– технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);

– защищаемые помещения.

Защита информации на объекте информатизации достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа, программно-технических

– воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе еѐ обработки, передачи и хранения, а также работоспособности технических средств.

При защите информации в локальных вычислительных сетях (ЛВС) конфиденциальная информация может обрабатываться только в ЛВС, расположенных в пределах контролируемой зоны.

Средства зашиты информации от НСД должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют постоянного квалифицированного контроля настроек СЗИ администратором безопасности информации. Класс защищѐнности ЛВС определяется в соответствии с требованиями действующих руководящих документов ФСТЭК России.

Для управления, контроля защищѐнности ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, должны использоваться соответствующие сертифицированные по требованиям безопасности информации средства защиты.

Вопросы и задания:

1. Что является объектом информатизации?
2. Определение СТС.
3. Обобщенная структурная схема ТКУИ, обрабатываемой СВТ.

Список литературы, рекомендуемый к использованию по данной теме

1. Основная литература:

1. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012.

2. Дополнительная литература:

1. Обеспечение информационной безопасности машиностроительных предприятий. Учебник для вузов./ Под ред. П.П. Мельникова. – М.: Сатурн-С, 2006.

2. Галатенко В.А. Стандарты информационной безопасности. Курс лекций / Под ред. акад. РАН Бетелина. – М.: Интернет-университет информационных технологий, 2006.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А. – Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.

Практическое занятие № 7. Обеспечение аутентичности
Учебные и воспитательные цели:
Изучить классификацию технических каналов утечки информации.

Теоретическая часть

Под техническими средствами приема, обработки, хранения и передачи информации (ТСПИ) понимают технические средства, непосредственно обрабатывающие конфиденциальную информацию. К таким средствам относятся: электронно-вычислительная техника, режимные АТС, системы оперативно-командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д.

При выявлении технических каналов утечки информации ТСПИ необходимо рассматривать как систему, включающую основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами), распределительные и коммутационные устройства, системы электропитания, системы заземления.

Отдельные технические средства или группа технических средств, предназначенных для обработки конфиденциальной информации, вместе с помещениями, в которых они размещаются, составляют объект ТСПИ. Под объектами ТСПИ понимают также выделенные помещения, предназначенные для проведения закрытых мероприятий.

Наряду с ТСПИ в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с ТСПИ и находящиеся в зоне электромагнитного поля, создаваемого ими. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и т.д.

В качестве канала утечки информации наибольший интерес представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ), т.е. зоны, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно разделить на электромагнитные, электрические и параметрические.

Электромагнитные каналы утечки информации

К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ЭМИ) ТСПИ:

- излучений элементов ТСПИ;
- излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;
- излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Электромагнитные излучения элементов ТСПИ. В ТСПИ носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза)

изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам ТСПИ вокруг них (в окружающем пространстве) возникает электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Электромагнитные излучения на частотах работы ВЧ генераторов ТСПИ и ВТСС. В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных ВЧ колебаний генераторов. Эти промодулированные ВЧ колебания излучаются в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ. Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи т.п.) возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения лежит в пределах рабочих частот нелинейных элементов УНЧ (например, полупроводниковых приборов, электровакуумных ламп и т.п.). Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе УНЧ в нелинейный режим работы, т.е. в режим перегрузки.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными вне контролируемой зоны.

Зона, в которой возможен перехват (с помощью разведывательного приемника) побочных электромагнитных излучений и последующая расшифровка содержащейся в них информации (т.е. зона, в пределах которой отношение "информационный сигнал/помеха" превышает допустимое нормированное значение), называется (опасной) зоной 2.

Электрические каналы утечки информации

Причинами возникновения электрических каналов утечки информации могут быть:

- наводки электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;
- просачивание информационных сигналов в цепи электропитания ТСПИ;
- просачивание информационных сигналов в цепи заземления ТСПИ.

Наводки электромагнитных излучений ТСПИ возникают при излучении элементами ТСПИ (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий ТСПИ и посторонних проводников или линий ВТСС. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ТСПИ и посторонних проводников.

Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется (опасной) зоной 1.

Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антеннапредставляет собой компактное техническое средство, например телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д. К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Просачивание информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Просачивание информационных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения ТСПИ с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны (металлические оболочки) соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций и т.д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, на которую могут наводиться информационные сигналы. Кроме того, в грунте вокруг заземляющего устройства возникает электромагнитное поле, которое также является источником информации.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ТСПИ, а также к их системам электропитания и заземления. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Съем информации с использованием аппаратных закладок. В последние годы участились случаи съема информации, обрабатываемой в ТСПИ, путем установки в них электронных устройств перехвата информации –закладных устройств.

Электронные устройства перехвата информации, устанавливаемые в ТСПИ, иногда называют аппаратными закладками. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в ТСПИ иностранного производства, однако возможна их установка и в отечественных средствах.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект.

Параметрический канал утечки информации

Перехват обрабатываемой в технических средствах информации возможен также путем их “высокочастотного облучения”. При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение модулируется информационным сигналом. При съеме информации для исключения взаимного влияния

облучающего и переизлученного сигналов может использоваться их временная или частотная развязка. Например, для облучения ТСПИ могут использовать импульсные сигналы.

При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют параметрическим.

Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства.

Информация после обработки в ТСПИ может передаваться по каналам связи, где также возможен ее перехват.

В настоящее время для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи. В зависимости от вида каналов связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования.

Данный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры разведки к кабельным линиям связи.

Самый простой способ –это непосредственное параллельное подключение к линии связи. Но данный факт легко обнаруживается, так как приводит к изменению характеристик линии связи за счет падения напряжения.

Поэтому средства разведки к линии связи подключаются или через согласующее устройство, несколько снижающее падение напряжения, или через специальные устройства компенсации падения напряжения. В последнем случае аппаратура разведки и устройство компенсации падения напряжения включаются в линию связи последовательно, что существенно затрудняет обнаружение факта несанкционированного подключения к ней.

Контактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации.

Электрический канал наиболее часто используется для перехвата телефонных разговоров. При этом перехватываемая информация может непосредственно записываться на диктофон или передаваться по радиоканалу в пункт приема для ее записи и анализа. Устройства, подключаемые к телефонным линиям связи и комплексированные с устройствами передачи информации по радиоканалу, часто называют телефонными закладками.

В случае использования сигнальных устройств контроля целостности линии связи, ее активного и реактивного сопротивления факт контактного подключения к ней аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее часто используют индуктивный канал перехвата информации, не требующий контактного подключения к каналам связи. В данном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками.

Индукционные датчики используются в основном для съема информации с симметричных высокочастотных кабелей. Сигналы с датчиков усиливаются, осуществляется частотное разделение каналов, и информация, передаваемая по отдельным каналам, записывается на магнитофон или высокочастотный сигнал записывается на специальный магнитофон.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные низкочастотные усилители, снабженные магнитными антеннами.

Некоторые средства бесконтактного съема информации, передаваемой по каналам связи, могут комплексироваться с радиопередатчиками для ретрансляции в центр ее обработки.

Вопросы и задания:

1. Источники сигнала.
2. Функции передатчика.
3. Классификация технических каналов утечки информации.

Список литературы, рекомендуемый к использованию по данной теме

1. Основная литература:

1. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012.

2. Дополнительная литература:

1. Обеспечение информационной безопасности машиностроительных предприятий. Учебник для вузов./ Под ред. П.П. Мельникова. – М.: Сатурн-С, 2006.

2. Галатенко В.А. Стандарты информационной безопасности. Курс лекций / Под ред. акад. РАН Бетелина. – М.: Интернет-университет информационных технологий, 2006.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А. – Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.

Практическое занятие №3. Четырехфазная модель процесса управления информационной безопасностью

Учебные и воспитательные цели:

Изучить четырехфазную модель процесса управления информационной безопасностью.

Теоретическая часть

Мы приступаем к детальному рассмотрению четырехфазной (планирование - реализация - оценка - корректировка, ПРОК) модели процесса управления информационной безопасностью, примененной в стандарте BS 7799-2:2002.

Процесс управления имеет циклический характер; на фазе первоначального планирования осуществляется вход в цикл. В качестве первого шага должна быть определена и документирована политика безопасности организации.

Затем определяется область действия системы управления информационной безопасностью. Она может охватывать всю организацию или ее части. Следует специфицировать зависимости, интерфейсы и предположения, связанные с границей между СУИБ и ее окружением; это особенно важно, если в область действия попадает

лишь часть организации. Большую область целесообразно поделить на подобласти управления.

Ключевым элементом фазы планирования является анализ рисков. Этот вопрос детально рассмотрен в курсе "Основы информационной безопасности"; здесь мы не будем на нем останавливаться.

Результат анализа рисков - выбор регуляторов безопасности. План должен включать график и приоритеты, детальный рабочий план и распределение обязанностей по реализации этих регуляторов.

На второй фазе - фазе реализации - руководством организации выделяются необходимые ресурсы (финансовые, материальные, людские, временные), выполняется реализация и внедрение выбранных регуляторов, сотрудникам объясняют важность проблем информационной безопасности, проводятся курсы обучения и повышения квалификации. Основная цель этой фазы - ввести риски в рамки, определенные планом.

Назначение фазы оценки - проанализировать, насколько эффективно работают регуляторы и система управления информационной безопасностью в целом. Кроме того, следует принять во внимание изменения, произошедшие в организации и ее окружении, способные повлиять на результаты анализа рисков. При необходимости намечаются корректирующие действия, предпринимаемые в четвертой фазе. Коррекция должна производиться, только если выполнено по крайней мере одно из двух условий:

- выявлены внутренние противоречия в документации СУИБ;
- риски вышли за допустимые границы.

Оценка может выполняться в нескольких формах:

- регулярные (рутинные) проверки;
- проверки, вызванные появлением проблем;
- изучение опыта (положительного и отрицательного) других организаций;
- внутренний аудит СУИБ;
- инспекции, проводимые по инициативе руководства;
- анализ тенденций.

Аудит должен выполняться регулярно, не реже одного раза в год. В процессе аудита следует убедиться в следующем:

- политика безопасности соответствует производственным требованиям;
- результаты анализа рисков остаются в силе;
- документированные процедуры выполняются и достигают поставленных целей;
- технические регуляторы безопасности (например, межсетевые экраны или средства ограничения физического доступа) расположены должным образом, правильно сконфигурированы и работают в штатном режиме;
- действия, намеченные по результатам предыдущих проверок, выполнены.

Даже если недопустимых отклонений не выявлено и уровень безопасности признан удовлетворительным, целесообразно зафиксировать изменения в технологии и производственных требованиях, появление новых угроз и уязвимостей, чтобы предвидеть будущие изменения в системе управления.

Систему управления информационной безопасностью надо постоянно совершенствовать, чтобы она оставалась эффективной . Эту цель преследует четвертая фаза рассматриваемого в стандарте цикла - корректировка. Она может потребовать как относительно незначительных действий, так и возврата к фазам планирования (например, если появились новые угрозы) или реализации (если следует осуществить намеченное ранее).

При корректировке прежде всего следует устранить несоответствия следующих видов:

- отсутствие или невозможность реализации некоторых требований СУИБ;

– неспособность СУИБ обеспечить проведение в жизнь политики безопасности или обслуживать производственные цели организации.

Задача фазы оценки - выявить проблемы. На фазе корректировки необходимо докопаться до их корней и устранить первопричины несоответствий, чтобы избежать повторного появления. С этой целью могут предприниматься как реактивные, так и превентивные действия, рассчитанные на среднесрочную или долгосрочную перспективу.

Таково (в сжатом изложении) содержание двух частей стандарта BS 7799. Может показаться, что каждое из его положений самоочевидно; тем не менее, собранные вместе и систематизированные, они обладают несомненной ценностью.

Вопросы и задания:

1. Формы оценки.
2. Опишите процесс аудита.
3. Опишите процесс коррекции.

Список литературы, рекомендуемый к использованию по данной теме

1. Основная литература:

1. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012.

2. Дополнительная литература:

1. Обеспечение информационной безопасности машиностроительных предприятий. Учебник для вузов./ Под ред. П.П. Мельникова. – М.: Сатурн-С, 2006.

2. Галатенко В.А. Стандарты информационной безопасности. Курс лекций / Под ред. акад. РАН Бетелина. – М.: Интернет-университет информационных технологий, 2006.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А. – Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.

Практическое занятие № 4. Эксплуатационное окружение, управление криптографическими ключами

Учебные и воспитательные цели:

1. Изучить эксплуатационное окружение.
2. Разобрать управление криптографическими ключами.

Формируемые компетенции: ПК-2, ПК-3, ПК-11

Теоретическая часть

Эксплуатационное окружение - это совокупность необходимых для функционирования модуля средств управления аппаратными и программными компонентами. В стандарте FIPS 140-2 рассматривается несколько видов окружения:

– универсальное, с коммерческой операционной системой, управляющей как компонентами модуля, так и другими процессами и приложениями;

– ограниченное, являющееся статическим, немодифицируемым (например, виртуальная Java-машина на непрограммируемой плате для персонального компьютера);

– модифицируемое, которое может быть реконфигурировано и включать средства универсальных ОС .

Ядро универсального и модифицируемого окружения - операционная система. На первом уровне безопасности к ней предъявляются следующие требования:

– используется только однопользовательский режим, параллельная работа нескольких операторов явным образом запрещается;

– доступ процессов, внешних по отношению к модулю, к данным, критичным для безопасности, запрещается, некриптографические процессы не должны прерывать работу криптографического модуля;

– программное обеспечение модуля следует защитить от несанкционированного раскрытия и модификации;

– целостность ПО модуля контролируется утвержденными средствами.

Для второго уровня безопасности требуется использование ОС, сертифицированных на соответствие определенным профилям защиты на основе "Общих критериев" с оценочным уровнем доверия не ниже второго. Для защиты критичных данных должно применяться произвольное управление доступом с определением соответствующих ролей. Необходимо протоколирование действийкрипто-офицера.

Характерная черта третьего уровня безопасности - использование доверенного маршрута.

На четвертом уровне безопасности криптографического модуля нужна ОС с оценочным уровнем доверия не ниже четвертого.

Требования безопасного управления криптографическими ключами охватывают весь жизненный цикл критичных данных модуля. Рассматриваются следующие управляющие функции:

генерация случайных чисел;

– генерация ключей ;
– распределение ключей ;
– ввод/вывод ключей ;
– хранение ключей ;
– обнуление ключей.

Секретные ключи необходимо защищать от несанкционированного раскрытия, модификации и подмены, открытые - от модификации и подмены.

Компрометация методов генерации или распределения ключей (например, угадывание затравочного значения, инициализирующего детерминированный генератор случайных чисел) должна быть не проще определения значений ключей.

Для распределения ключей может применяться как ручная транспортировка, так и автоматические процедуры согласования ключей.

Допускается ручной (с клавиатуры) и автоматический (например, при помощи смарт-карты) ввод ключей. На двух нижних уровнях безопасности при автоматическом вводе секретные ключи должны быть зашифрованы; ручной ввод может осуществляться в открытом виде. На третьем и четвертом уровнях при ручном вводе ключей в открытом виде применяются процедуры разделения знаний.

Модуль должен ассоциировать введенный ключ (секретный или открытый) с владельцем (лицом, процессом и т.п.).

Вопросы и задания:

1. Виды окружения.
2. Требования к ОС.
3. Управляющие функции.

Список литературы, рекомендуемый к использованию по данной теме

1. Основная литература:

1. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012.

2. Дополнительная литература:

1. Обеспечение информационной безопасности машиностроительных предприятий. Учебник для вузов./ Под ред. П.П. Мельникова. – М.: Сатурн-С, 2006.

2. Галатенко В.А. Стандарты информационной безопасности. Курс лекций / Под ред. акад. РАН Бетелина. – М.: Интернет-университет информационных технологий, 2006.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А. – Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2009.