Практическая работа №2

Виды угроз. Характер и виды происхождения угроз.

Виды угроз

Угрозы возникают из противоречий экономических интересов различных элементов, взаимодействующих как внутри, так и вне социально-экономической системы -- в том числе и в информационной сфере. Они и определяют содержание и направления деятельности по обеспечению общей и информационной безопасности. Следует отметить, что анализ проблем экономической безопасности необходимо проводить, учитывая взаимосвязи экономических противоречий, угроз и потерь, к которым может приводить реализация угроз.

Угрозы можно классифицировать по нескольким критериям:

* по важнейшим составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых направлены угрозы в первую очередь;
* по компонентам информационных систем и технологий (данные, программно-аппаратные комплексы, сети, поддерживающая инфраструктура), на которые угрозы непосредственно нацелены;
* по способу осуществления (случайные или преднамеренные действия, события техногенного или природного масштаба);
* по локализации источника угроз (вне или внутри информационной технологии или системы).

Основные нарушения:

* физической целостности (уничтожение, разрушение элементов);
* логической целостности (разрушение логических связей);
* содержания (изменение блоков информации, внешнее навязывание ложной информации);
* конфиденциальности (разрушение защиты, уменьшение степени защищенности информации);
* прав собственности на информацию (несанкционированное копирование, использование).

Три наиболее выраженные угрозы:

* подверженность физическому искажению или уничтожению информации;
* возможность несанкционированной (случайной или злоумышленной) модификации информации;
* опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

Существует несколько типов атак: атаки, основанные на ошибках реализации программного обеспечения (срыв стека, использование конвейера); атаки, основанные на неправильной конфигурации сервера и атаки, основанные на уязвимости сетевых протоколов (внедрение ложного DNS, перехват трафика).

Даже при условии отсутствия ошибок реализации правильно настроенный почтовый сервер может быть атакован, если не предпринять особых мер предосторожности, о которых осведомлен далеко не каждый администратор.

Ниже представлен перечень некоторых атак, которым подвержены сегодня организации, использующие почтовые e-mail-системы:

* трояны;
* фишинг организаций;
* Backscatter - bounce-сообщения;
* Email Bombing - почтовая бомбардировка;
* Denial of Email Service (DoES) -отказ почтовой службы;
* эксплуатация (эксплойты) открытых релеев

Простой взгляд на Web-сайты большинства компаний может дать атакующему злоумышленнику список e-mail-адресов для реализации, например, фишинг-атаки, рассылки вредоносного вложения или ссылки на хакерский сайт, после посещения которого на компьютеры пользователей незаметно будет установлено программное обеспечение, ворующее их пароли к корпоративным ресурсам или другую не менее ценную персональную информацию.

Характер происхождения угроз

Угрозы безопасности информации в современных системах ее обработки определяются умышленными (преднамеренные угрозы) и естественными (непреднамеренные угрозы разрушающими и искажающими воздействиями внешней среды, надежностью функционирование средств обработки информации, а также преднамеренным корыстным воздействием несанкционированных пользователей, целью которых является хищение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации. При этом под умышленными или преднамеренными понимаются такие угрозы, которые обуславливаются злоумышленными действиями людей. Случайными или естественными являются угрозы, не зависящие от воли людей. Классификация угроз:

1. Умышленные факторы:

1) хищение носителей информации;

2) подключение к каналам связи;

3) перехват электромагнитных излучений (ЭМИ);

4) несанкционированный доступ;

5) разглашение информации;

6) копирование данных.

2. Естественные факторы:

1) несчастные случаи (пожары, аварии, взрывы);

2) стихийные бедствия (ураганы, наводнения, землетрясения);

3) ошибки в процессе обработки информации (ошибки пользователя, оператора, сбои аппаратуры).

Пример:

Угрозы, связанные с сервером, содержащим бухгалтерский отчет крупной компании:

Серверы меньше подвержены атакам, поскольку они, как правило, работают в контролируемых условиях, обслуживаются квалифицированными администраторами и обладают одним или несколькими уровнями защиты. Сервер отчетов является сервером без сохранения состояния, который хранит содержимое и данные приложений во внешнем хранилище. Одна из самых больших угроз для установки сервера отчетов — несанкционированный доступ и вмешательство в базу данных и файлы конфигурации сервера отчетов. Менее очевидная, но столь же важная угроза определяется способом создания отчетов и кругом лиц, которым предоставлено разрешение на публикацию содержимого на сервере отчетов. Определения отчета — сборки, которые запускаются на компьютере сервера с полным уровнем доверия. Определения отчетов могут содержать другие пользовательские сборки, которые также выполняются на сервере. Если отчет или пользовательская сборка содержит вредоносный код, этот код будет выполняться на компьютере сервера отчетов с учетными данными пользователя, запросившего отчет. Причиной других неявных угроз может быть структура отчета, в которой непреднамеренно раскрываются конфиденциальные данные. Например, если сотрудник запускает отчет, в котором в качестве параметра используется идентификатор сотрудника, то он не должен иметь возможности видеть сведения о другом сотруднике, вставляя произвольные идентификаторы в URL-адрес отчета. Наконец, учитывайте методы распространения отчетов в организации. Можно настроить сервер отчетов, чтобы уменьшить возможность доставки отчетов вне организации. Можно также использовать разрешения файловой системы и разрешения сервера отчетов, чтобы только авторизованные пользователи могли открыть отчет.

В следующей таблице описаны угрозы и меры по снижению уязвимости.

Таблица 1

|  |  |  |
| --- | --- | --- |
| Компонент или операция | Угроза | Меры по снижению уязвимости |
| Параметры конфигурации, хранящиеся в файле Web.config и файлах конфигурации приложения на компьютере сервера отчетов. | Злоумышленник может получить доступ к компьютеру, обнаружить незашифрованный или незащищенный файл конфигурации и внести изменения в этот файл. | Назначьте разрешения для файла. По умолчанию разрешения предоставляются группам безопасности служб Службы Reporting Services, созданным в процессе установки. |
| Веб-служба сервера отчетов обрабатывает запросы по требованию, переданные через соединения TCP/IP. | Злоумышленник может запустить атаку типа «запрет в обслуживании», которая принимает следующие формы.  На целевой сервер направляются множественные запросы без проверки подлинности.  Неполные запросы направляются на целевой сервер, но никогда не завершаются.  Запросы чрезмерно велики; злоумышленник начинает запрос, а затем посылает большой объем данных на сервер. | Сервер отчетов удаляет все запросы без проверки подлинности в течение двух минут, что может уменьшить последствия атаки типа «запрет в обслуживании». Двухминутный интервал имеет фиксированную длительность, его нельзя уменьшить.  Если атака основана на операциях передачи данных на сервер отчетов, можно уменьшить значение элементаmax Request Lengthв файле Machine.config. По умолчанию устанавливаемая платформой ASP.NET верхняя граница для объема передаваемых на сервер файлов составляет 4 МБ. Обратите внимание, что уменьшение значенияmax Request Length должно быть временной мерой. Необходимо вернуть прежнее значение, если передача больших файлов (например, моделей) выполняется часто. Дополнительные сведения о настройке параметра max Request Lengthв установке служб Reporting Services см. в разделе. [Максимальные размеры отчетов и моментальных снимков](http://msdn.microsoft.com/ru-ru/library/ms156002(v=sql.105).aspx). |
| Службы Службы Reporting Services поддерживают расширяемую архитектуру, которая позволяет развертывать сторонние модули обработки данных, модули доставки и модули подготовки отчетов. Также можно развертывать пользовательские конструкторы запросов. Модули должны выполняться с полным уровнем доверия. | Злоумышленник может вставить вредный код в пользовательский модуль. | Развертывайте модули только от доверенных пользователей и организаций. |

Практическая часть:

Для своего варианта представить угрозы и меры по снижению уязвимости.