3. Средства и методы обеспечения целостности информации. Средства и методы обеспечения конфиденциальности информации

Процесс осуществления атаки на АС включает три этапа. Первый этап, подготовительный, заключается в поиске предпосылок для осуществления той или иной атаки. На этом этапе ищутся уязвимости, использование которых приводит к реализации атаки, т. е. ко второму этапу. На третьем этапе атака завершается, «заметаются» следы и т. д. При этом первый и третий этапы сами по себе могут являться атаками.

Обнаруживать, блокировать и предотвращать атаки можно несколькими путями. Первый способ, и самый распространённый, – это обнаружение уже реализуемых атак. Данный способ функционирует на втором этапе осуществления атаки. Этот способ применяется в «классических» системах обнаружения атак:

- серверах аутентификации;
- системах разграничения доступа;
- межсетевых экранах и т. п.

Основным недостатком средств данного класса является то, что атаки могут быть реализованы повторно. Они также повторно обнаруживаются и блокируются. И так далее, до бесконечности.

Второй путь – предотвратить атаки ещё до их реализации. Осуществляется это путём поиска уязвимостей, которые могут быть использованы для реализации атаки.

И наконец, третий путь – обнаружение уже совершённых атак и предотвращение их повторного осуществления.

Таким образом, системы обнаружения атак могут быть классифицированы по этапам осуществления атаки:

1. Системы, функционирующие на первом этапе осуществления атаки и позволяющие обнаружить уязвимости информационной системы, используемые нарушителем для реализации атаки. Средства этой категории называются системами анализа защищенности (security assessment systems) или сканерами безопасности (security scanners).

Системы анализа защищённости проводят всесторонние исследования систем с целью обнаружения уязвимостей. Результаты, полученные от средств анализа защищённости, представляют «мгновенный снимок» состояния защиты системы в данный момент времени. Несмотря на то что эти системы не могут обнаруживать атаку в процессе её развития, они могут определить возможность реализации атак.

Эти системы реализуют две стратегии:

Первая стратегия – пассивная, реализуемая на уровне операционной системы, СУБД и приложений, при которой осуществляется анализ конфигурационных файлов и системного реестра на наличие неправильных параметров, файлов паролей на наличие легко угадываемых паролей, а также других системных объектов на нарушения политики безопасности.

Вторая стратегия – активная, осуществляется в большинстве случаев на сетевом уровне. Она заключается в воспроизведении наиболее распространенных сценариев атак и анализе реакции системы на эти сценарии.

2. Системы, функционирующие на втором этапе осуществления атаки и позволяющие обнаружить атаки в процессе их реализации, т.е. в режиме реального (или близкого к реальному) времени. Именно эти средства и принято считать системами обнаружения атак в классическом понимании. Помимо этого, в последнее время выделяется новый класс средств обнаружения атак – обманные системы.

Обнаружение атак реализуется посредством анализа или журналов регистрации операционной системы и прикладного программного обеспечения, или сетевого трафика в реальном времени. Компоненты обнаружения атак, размещенные на узлах или сегментах сети, оценивают различные действия, в том числе и использующие известные уязвимости, сравнивая контролируемое пространство (сетевой трафик или журналы регистрации) с известными шаблонами (сигнатурами) несанкционированных действий.

Обманные системы могут использовать следующие методы: сокрытие, камуфляж и дезинформацию. Ярким примером использования первого метода является сокрытие сетевой топологии при помощи межсетевого экрана. Примером камуфляжа можно назвать использование Unix-подобного графического интерфейса в системе, функционирующей под управлением операционной системы Windows NT. Если злоумышленник случайно увидел такой интерфейс, то он будет пытаться реализовать атаки, характерные для ОС Unix, а не для ОС Windows NT. Это существенно увеличит время, необходимое для «успешной» реализации атаки. И наконец, в качестве примера дезинформации можно назвать использование заголовков, которые бы давали понять злоумышленнику, что атакуемая им система уязвима.

Системы, реализующие камуфляж и дезинформацию, эмулируют те или иные известные уязвимости, которых в реальности не существует.

Использование таких систем приводит к следующему:

• Увеличение числа выполняемых нарушителем операций и действий. Так как невозможно заранее определить, является ли обнаруженная нарушителем уязвимость истинной или нет, злоумышленнику приходится выполнять много дополнительных действий, чтобы выяснить это. И даже дополнительные действия не всегда помогают. Например, попытка запустить программу подбора паролей на сфальсифицированный и несуществующий в реальности файл приведёт к бесполезной трате времени без какого-либо видимого результата. Нападающий будет думать, что он не смог подобрать пароли, в то время как на самом деле программа «взлома» была просто обманута.

• Получение возможности отследить нападающих. За тот период времени, когда нападающие пытаются проверить все обнаруженные уязвимости, в том числе и фиктивные, администраторы безопасности могут проследить весь путь до нарушителя или нарушителей и предпринять соответствующие меры.

3. Системы, функционирующие на третьем этапе осуществления атаки и позволяющие обнаружить уже совершённые атаки. Эти системы делятся на два класса – системы контроля целостности, обнаруживающие изменения контролируемых ресурсов, и системы анализа журналов регистрации.

Системы контроля целостности работают по замкнутому циклу, обрабатывая файлы, системные объекты и атрибуты системных объектов с целью получения контрольных сумм; затем они сравнивают их с предыдущими контрольными суммами, отыскивая изменения. Когда изменение обнаружено, система посылает сообщение администратору, фиксируя вероятное время изменения.

Существует ещё одна распространённая классификация систем обнаружения нарушения политики безопасности – по принципу реализации: host-based, т.е. обнаруживающие атаки, направленные на конкретный узел сети, и network-based, направленные на всю сеть или сегмент сети. Существуют три основных вида систем обнаружения атак на уровне узла.

4. Системы, обнаруживающие атаки на конкретные приложения.
5. Системы, обнаруживающие атаки на операционные системы.
6. Системы, обнаруживающие атаки на системы управления базами данных (СУБД).

В сетевых операционных системах вопросы защиты целостности данных решаются средствами разграничения доступа (блокировка возможности доступа, запрет на изменение, мониторинг использования файлов). К сожалению, средствами операционной системы Windows XP невозможно защитить файлы от удаления. Windows XP позволяет устанавливать атрибут файла «только для чтения», «скрытый» и делать файлы невидимыми в окне Проводника. Это может служить определённой защитой от ошибочных действий пользователя. Однако и эти файлы могут быть удалены (например, при удалении содержащей их папки).

Как сохранность данных, так и надёжная работа программного обеспечения невозможны без решения задачи их защиты от разрушающих воздействий компьютерных вирусов. Немаловажную роль при этом играет знание путей попадания вируса в

компьютерную систему и соблюдение мер предосторожности при выполнении потенциально опасных действий (или отказ от их выполнения). Вместе с тем надёжная защита от вирусов может быть обеспечена только с использованием специальных антивирусных программных средств.

Средства и методы обеспечения конфиденциальности обеспечения информации

В рамках направления защиты конфиденциальной информации необходимы: организация контроля доступа к информации, защита информации от действий нелегальных пользователей и от несанкционированного действия легальных пользователей. Если речь идёт об авторских программных системах, важным вопросом является защита данных от копирования.

Наиболее распространёнными мероприятиями защиты конфиденциальной информации являются:

- разграничение доступа к данным;
- парольная защита;
- шифрование;
- скрытие данных;
- уничтожение остаточных данных;
- защита от копирования программных систем.

Большинство сетевых операционных систем располагают развитыми средствами разграничения доступа и защиты от несанкционированного доступа (НСД). Для скрытия и шифрования данных могут использоваться специальные утилиты.

Проблема остаточных данных вызвана типичной схемой удаления файлов: запись о файле удаляется из специальной базы данных ОС – таблицы размещения файлов (FAT), а занимаемое им место на диске помечается как свободное. Таким образом, производится логическое, но не физическое удаление файла. Незащищённая конфиденциальная информация может быть прочитана из остаточных данных с помощью специальных утилит.

Уничтожение остаточных данных подразумевает возможность полного удаления файлов на физическом уровне, очистку свободного дискового пространства, включая данные из хвостовых частей последних кластеров файлов. Эти возможности должны обеспечиваться средствами защищённой операционной системы, Windows XP не выполняет подобных функций.

MS Office располагает собственными средствами защиты документов. Для документов MS Office имеются возможности: ограничить доступ к документу (парольная защита открытия документа, шифрование), установить запрет на изменение документа или его частей, скрыть часть документа (MS Excel). Кроме того, приложение MS Access позволяет установить защиту на уровне пользователя. Этот способ защиты реализует контроль доступа к объектам базы данных и подобен методам разграничения доступа, используемым в большинстве сетевых систем.

Идентификация и аутентификация – взаимосвязанные методы защиты от НСД, при их реализации часто используется криптографическое преобразование информации (шифрование).

Идентификация – это присвоение пользователям идентификатора и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация – это проверка принадлежности пользователю предъявленного им идентификатора (подтверждение или проверка подлинности).

Под безопасностью (стойкостью) системы идентификации и аутентификации понимается степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя.

Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

- индивидуального объекта заданного типа;

- знаний некоторой известной только ему и проверяющей стороне информации;

- индивидуальных биометрических характеристик.

К *первой группе* относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во *вторую группу* входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Применение методов аутентификации, основанных на измерении и сравнении с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза, сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, то такая процедура называется непосредственной аутентификацией. Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны. При этом третью сторону называют сервером аутентификации или арбитром

Уровень конфиденциальности информации является одной из самых важных категорий, принимаемых в рассмотрение при создании определённой политики безопасности.

Классификация по степени конфиденциальности – одна из основных и наиболее старых классификаций данных. Она применялась ещё задолго до появления вычислительной техники и с тех пор изменилась незначительно.

Различные классы конфиденциальной информации необходимо снабжать различными по уровню безопасности системами технических и административных мер.

При работе с информацией 1-го класса конфиденциальности рекомендуется выполнение следующих требований:

- осведомление сотрудников о закрытости данной информации;

- общее ознакомление сотрудников с основными возможными методами атак на информацию;

- ограничение физического доступа;

- полный набор документации по правилам выполнения опера-ций с данной информацией

При работе с информацией 2-го класса конфиденциальности к перечисленным выше требованиям добавляются следующие:

- расчёт рисков атак на информацию;

- поддержание списка лиц, имеющих доступ к данной информации;

- по возможности выдача подобной информации под расписку (в том числе электронную);

- автоматическая система проверки целостности системы и её средств безопасности;

- надёжные схемы физической транспортировки;

- обязательное шифрование при передаче по линиям связи;

- схема бесперебойного питания ЭВМ.

При работе с информацией 3-го класса конфиденциальности ко всем перечисленным выше требованиям добавляются следующие:

- детальный план спасения либо надежного уничтожения информации в аварийных ситуациях (пожар, наводнение, взрыв);

- защита ЭВМ либо носителей информации от повреждения водой и высокой температурой;

- криптографическая проверка целостности информации.