соответственно ограниченном объеме). Функции определения конфигурации сети, администрирования и аудита, типичные для сетевых операционных систем, являются строго контролируемыми и выполняются централизовано.

Таким образом, выполненный анализ показывает существенное упрощение протоколов и связей между ними в сетях повышенной безопасности по сравнению с обычными сетями, но в то же время усложнение самих процедур связи. Топология же сети повышенной безопасности должна отличаться от топологии традиционных сетей.

Литература: 1. Кейлингерт П. Элементы операционных систем, 1985. 2. Медведовский И. Д. и др. Атака на Internet, 1999.

УДК 004.056.5

НАБЛЮДАЕМОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Денис Кудин
Общество с ограниченной ответственностью «АННА»
Запорожский государственный технический университет

Анотація: **У цій статті розглядається необхідність реалізації властивостей спостерігання обчислювальних систем у програмах захисту від персонала й основні вимоги до методів і технологій, забезпечующим цю властивість.**
Summary: **The necessity of computer systems accountability implementation in personnel security programs and general requirements to accountability technologies are discussed in this article.**
Ключевые слова: **обчислювальна система, автоматизована система, спостерігання, захист від персоналу, регістрація.**

I Введение

Защита от персонала – это большая проблема, которой в настоящее время уделяется огромное внимание во всем мире. В Украине она стоит особенно остро, так как отсутствие специализированных технических средств и программного обеспечения, а также некомпетентность ответственных лиц, создают благоприятную почву для развития различных форм промышленного и коммерческого шпионажа [1].

В программах защиты от персонала (Personnel Security Programs) используется два основных подхода. Первый связан с разработкой правил безопасного использования компьютеров при работе в сети, разграничением доступа к информации и т.д., а также разработкой физических мер защиты (охрана помещений, применение систем наблюдения и т.д.). Второй подход связан с определением состава программного (программно-аппаратного) обеспечения, которое используется администратором безопасности вычислительной системы для обеспечения ее *наблюдаемости* – свойства вычислительной системы, позволяющего фиксировать деятельность пользователей и процессов, использование пассивных объектов, а также однозначно устанавливать идентификаторы причастных к определенным событиям пользователей и процессов с целью предотвращения нарушения политики безопасности и/или обеспечения ответственности за определенные действия [2]. Именно это свойство, в зависимости от качества его реализации, позволяет в той или иной мере контролировать соблюдение сотрудниками предприятия установленных правил безопасной работы на компьютерах.

Однако многие предприятия Украины часто ограничиваются какой-либо одной мерой защиты, например, покупкой дорогостоящего межсетевого экрана, работающего на границе внутренней корпоративной сети и внешней глобальной сети Internet. При этом предполагается, что все компьютеры, объединенные в сеть, имеют выход в Internet через этот межсетевой экран. Между тем, крупнейшие корпорации мира ежегодно увольняют сотни сотрудников за то, что те приносят свои модемы и подключаются к внешней сети через телефонные линии со своих рабочих мест. Если произошла утечка критичной информации, то администратор безопасности, не имея дополнительных программных средств, практически не в состоянии выявить злоумышленника и определить, к какому компьютеру, в какое время был несанкционированно подключен модем, и какая именно информация была скомпрометирована. С этой точки зрения, межсетевые экраны не могут обеспечить надежную защиту от персонала.

Другой пример – некоторые сотрудники банков могут за определенную плату совершать незаконную деятельность, предоставляя заинтересованным лицам сведения о финансовых операциях любых клиентов банка. Эти сведения могут передаваться заинтересованному лицу как по сети, так и в виде распечатки, сделанной на локальном принтере. Во втором случае никакие средства сетевого контроля не в состоянии выявить нарушение.

Для решения этих и многих других проблем, связанных с защитой от персонала, необходимо применять программные или программно-аппаратные средства, реализующие свойство наблюдаемости вычислительных систем, что позволяет:

- определить (локализовать) все случаи попыток несанкционированного доступа к конфиденциальной информации с точным указанием времени и сетевого рабочего места, с которого такая попытка осуществлялась.
- определить факты несанкционированной установки программного обеспечения;
- проконтролировать возможность использования персональных компьютеров в нерабочее время и выявить цель такого использования;
- определить все случаи несанкционированного использования модемов в локальной сети путем анализа фактов запуска несанкционированно установленных специализированных приложений;
- определить все случаи набора на клавиатуре критичных слов и словосочетаний, подготовки каких-либо критичных документов, передача которых третьим лицам приведет к материальному ущербу;
- определить факты нецелевого использования персональных компьютеров и т.д.

В настоящее время в Украине существует всего один программно-аппаратный комплекс, попадающий в данную категорию – это система безопасности «СОВА» разработки запорожского ООО «АННА».

II Технологии наблюдаемости и основные требования к ним

Рассмотрим ряд технических требований, которым должны удовлетворять программные или программно-аппаратные средства, обеспечивающие наблюдаемость автоматизированных систем (АС), т.е. организационно-технических систем, реализующих информационную технологию и объединяющих вычислительные системы, физическую среду, персонал и обрабатываемую информацию. Под вычислительной системой (ВС) подразумевается совокупность программно-аппаратных средств, предназначенных для обработки информации.

Архитектура любых сетевых программ, претендующих на переносимость и универсальность, должна базироваться на протоколах TCP/IP. Семейство протоколов TCP/IP предназначено для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины. Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи. Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети. Не требуется, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол. Таким образом, две машины, подключенные к одной подсети, могут обмениваться пакетами. Обычно, исходя из соображений безопасности, программы, реализующие наблюдаемость ВС, ограничиваются работой в подсети с заданной маской с прямой видимостью всего пространства IP-адресов.

Когда необходимо передать пакет между машинами, подключенными к разным подсетям, то машина-отправитель посылает пакет в соответствующий шлюз (шлюз подключен к подсети также как обычный узел). Оттуда пакет направляется по определенному маршруту через систему шлюзов и подсетей, пока не достигнет шлюза, подключенного к той же подсети, что и машина-получатель; там пакет направляется к получателю. Объединенная сеть обеспечивает датаграммный сервис. Проблема доставки пакетов в такой системе решается путем реализации во всех узлах и шлюзах межсетевого протокола IP. Межсетевой уровень является по существу базовым элементом во всей архитектуре протоколов, обеспечивая возможность стандартизации протоколов верхних уровней.

Программы, обеспечивающие наблюдаемость ВС, выполняются с использованием технологии «клиент-сервер». Существует одна серверная часть и ограниченное множество клиентских частей.

Клиентские части устанавливаются на рабочие станции конечных пользователей, которые могут работать под управлением различных операционных систем.

Основные функции клиентской части:

- регистрация определенных событий;
- ведение журнала регистрации;
- передача журнала регистрации на серверную часть по установленному администратором безопасности критерию.

Клиентская часть должна:

- загружаться автоматически с загрузкой операционной системы;
- быть невидимой для пользователя;

– регистрировать тексты, набираемые в графических и консольных окнах;
– регистрировать время и дату загрузки системы и имя текущего пользователя;
– регистрировать время и дату запускаемых приложений;
– регистрировать время и дату переключения между задачами;
– регистрировать адреса посещаемых узлов Internet;
– иметь возможность применения фильтров для контроля строго определенных приложений;
– иметь возможность контроля по расписанию;
– быть устойчивой к воздействию пользователя;
– передавать отчетную информацию на серверную часть невидимо для пользователя;
– использовать как можно меньше системных ресурсов, не оказывая заметного влияния на производительность системы;
– иметь возможность автоматизированной установки в локальной сети;
– не конфликтовать с антивирусным и другим программным обеспечением;
– и др.

Таким образом, клиентская часть собирает подробные сведения о том, какие действия производились пользователем на компьютере.

Для регистрации событий в операционных системах (ОС) семейства Microsoft® Windows® можно использовать драйвера уровня ядра либо механизм ловушек. *Ловушка* – это часть механизма обработки сообщений в ОС Windows, позволяющая приложению инсталлировать подпрограмму для перехвата трафика системных сообщений и обрабатывать определенные типы сообщений перед тем, как они попадут в процедуру управления окнами приложения-получателя.

ОС Windows содержит множество различных типов ловушек. Каждый из них отвечает за тот или иной аспект механизма обработки сообщений. Для каждого из этих типов система поддерживает отдельные цепочки ловушек, представляющие собой список указателей на процедуры обратного вызова. Когда происходит событие, ассоциированное с определенным типом ловушки, система передает соответствующее сообщение последовательно каждой процедуре в цепочке ловушек. Действия, которые может производить процедура ловушки, зависит от типа ловушки. Для некоторых типов ловушек процедура может только регистрировать сообщения, для других типов – изменять параметры сообщений и даже прерывать их прохождение по цепочке ловушек.

Процедура ловушки может быть глобальной, регистрируя сообщения всех потоков в системе, либо ориентированной на отдельный поток. Глобальная процедура ловушки вызывается в контексте любого приложения из модуля библиотеки динамической компоновки. Процедура, ориентированная на отдельный поток, вызывается в контексте ассоциированного потока и может располагаться как в главном исполнимом модуле, так и в модуле библиотеки динамической компоновки.

ОС Windows содержит следующие основные типы ловушек:
– для перехвата сообщений, посылаемых процедуре обработки окна приложения-получателя, перед либо после их обработки данной процедурой;
– для перехвата сообщений, поставленных в очередь;
– для записи входных сообщений;
– для повторного воспроизведения записанной ранее последовательности сообщений;
– для перехвата сообщений, сгенерированных каким-либо событием ввода информации в диалоговом окне;
– для перехвата сообщений, сгенерированных событием клавиатуры;
– для перехвата сообщений, сгенерированных событием мыши;
– для отладки других ловушек;
– и др.

Серверной частью управляет только администратор безопасности вычислительной системы, т.к. информация, накапливаемая в журнале регистрации, при достижении определенного объема становится критичной, т.е. ее потеря или неправильное использование (модификация, ознакомление) может нанести ущерб владельцу информации или АС, или любому другому физическому (юридическому) лицу или группе лиц. Главная функция серверной части – централизованный сбор и хранение журналов регистрации, передаваемых от клиентских частей. Под журналом регистрации понимается упорядоченная совокупность регистрационных записей, каждая из которых заносится клиентской частью по факту совершения контролируемого события.

Наибольшая проблема при разработке серверной части – обеспечить устойчивую работу системы в том случае, когда серверная часть будет обслуживать десятки тысяч клиентов. При этом необходимо следить, чтобы не возникало «утечек» памяти из-за неполного освобождения объемов динамической памяти.

Программы, реализующие свойство наблюдаемости ВС, – это очень сложные и дорогостоящие комплексы. Поэтому они должны обладать соответствующими мерами защиты от несанкционированного использования. Во-первых, применяются программные технологии защиты – проверка целостности кода и данных, шифрование данных, шифрование трафика между клиентскими и серверной частями и т.д. Во-вторых, применяются

аппаратные ключи защиты, в которые прошивается персональная информация о заказчике, максимально допустимое количество клиентов, диапазон IP-адресов и др. Характерно, что программы наблюдаемости могут применяться не только в локальной сети предприятия, но и в глобальной сети Internet, поэтому необходимо жестко задавать диапазон IP-адресов клиентов и их максимальное количество, IP-адрес сервера и маску подсети.

Для удобного анализа журналов регистрации средствами систем управления базами данных (СУБД) необходимо предусмотреть возможность автоматического преобразования журналов регистрации в DBF-формат. Это позволяет применять SQL-запросы и делать выборки по интересующим критериям.

В процессе сетевого соединения два процесса обмениваются данными. Выражением абстрактной точки сетевого соединения является *сокет*. Каждый использующийся сокет имеет тип и ассоциированный с ним процесс. Сокеты существуют внутри коммуникационных доменов. Домены – это абстракции, которые подразумевают конкретную структуру адресации и множество протоколов, которое определяет различные типы сокетов внутри домена. Программы обеспечения наблюдаемости могут использовать два типа сокетов – TCP или UDP. Потоковые сокеты, использующие транспортный протокол TCP, необходимо создавать, когда требуется гарантированная доставка данных, например, при отсылке серверной части журнала регистрации клиента. Датаграммные сокеты используют транспортный протокол UDP, который позволяет пересылать небольшие пакеты фиксированной длины без подтверждения их доставки и без установления виртуального соединения. Клиентская часть может использовать датаграммные сокеты, например, для посылки сигналов активности.

III Выводы

Наиболее эффективную защиту автоматизированной системы обеспечивает только совокупность взаимосвязанных физических, технических и организационных мер.

Перспективными направлениями развития программ наблюдаемости являются:

- разработка модулей для звукового и видео контроля вычислительных систем, резко увеличивающих информативность отчетной информации;
- разработка многоплатформенных клиентских и серверных частей;
- разработка модулей по оперативному уведомлению администратора безопасности о состоянии серверной части и о нарушениях установленной политики безопасности с использованием средств сотовой и пейджинговой связи.

Литература: 1. Анков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. – М.: Мир, 1999. – 351 с., 2. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – Киев, 1999., 3. Золотов С. Протоколы Internet – СПб.: BHV – Санкт-Петербург, 1998. – 304 с., 4. RFC 1180. TCP/IP tutorial. T.J. Socolofsky, C.J. Kale. Jan-01-1991., 5. Прокоф'єва Д.М. Підприємницьке шпигунство в системі інформаційних злочинів. // Інформаційні технології та захист інформації: Збірник наукових праць. – Запоріжжя: Юридичний ін-т МВС України, 1998. – Вип. 2., 6. Куценко В.Н., Голубєв В.О. Рекомендації по забезпеченню програмно-технічного захисту інформації в комп'ютерних мережах. // Інформаційні технології та захист інформації: Збірник наукових праць. – Запоріжжя: Юридичний ін-т МВС України, 1998. – Вип. 2., 7. Красноступ М.Д. Інформаційна безпека України: сутність та проблеми. // Інформаційні технології та захист інформації: Збірник наукових праць. – Запоріжжя: Юридичний ін-т МВС України, 1999. – Вип. 1.