Захист інформації

УДК 681.32

А.А. Ващеня[1], Э.В. Лысенко[2]

[1] *Харьковский национальный университет радиоэлектроники, Харьков*
[2] *Харьковский национальный университет городского хозяйства им. А.Н. Бекетова, Харьков*

АНАЛИЗ МОДЕЛЕЙ ИНСАЙДЕРСКИХ УГРОЗ В СОЦИАЛЬНО-ТЕХНИЧЕСКИХ СИСТЕМАХ

В данной статье проведен обзор четырех основных моделей управления доступом. Рассмотрены принципы функционирования каждой модели. Также проведен краткий анализ возможных инсайдерских угроз. Представлено возможное разбиение основных сценариев на конкретные угрозы.

Ключевые слова: *разграничение доступа, модель управления доступом, сценарии угроз, инсайдер.*

Введение

Анализ литературы [2, 4] указывает на то, что на данный момент инсайдерские угрозы являются серьезной проблемой в сфере обеспечения безопасности. Так, например, исследование компании InfoWatch показывает, что в первом полугодии 2015 года в мире зарегистрировано 723 случая утечки конфиденциальной информации, и в 58% случаев виновными в утечке информации оказались сотрудники компаний. А в 1% случаев – даже высшие руководители организаций [4]. Важно понимать, что при нынешней доступности информации инсайдером может стать любой сотрудник. Поэтому в компаниях необходимо реализовывать разграничение доступа сотрудников к критической информации.

Цель статьи – ознакомительный обзор основных моделей управления доступом, а также рассмотрение основных сценариев инсайдерских угроз.

Основная часть

Инсайдерские угрозы реализуются за счет уязвимостей системы защиты информации. Данные уязвимости определяются не только пробелами в системе безопасности и политики, но и в организации управления доступом к ресурсам. Это вызвано тем, что инсайдер имеет авторизованные права доступа в системе. Поэтому рассмотрим анализ базовых моделей вправления доступом и инсайдерских угроз независимо друг от друга.

Базовые модели управления доступом

Для создания системы контроля доступа изначально необходимо определить множества субъектов и объектов доступа. Разграничение доступа проявляется в том, что для доступа к конкретному объекту у субъекта должны быть соответствующие полномочия. Существует несколько формальных моделей управления доступом.

1. Мандатное управление доступом. В рамках данной модели каждый объект и субъект в системе должны быть однозначно идентифицированы. Каждому объекту в зависимости от его ценности присваивается уровень конфиденциальности. Аналогичным образом каждому субъекту присваивается уровень доступа. Таким образом, происходит разграничения доступа, при котором субъекты с более низким уровнем доступа не могут использовать объекты с более высоким уровнем конфиденциальности. Доступ полностью определяется политикой безопасности системы, и обычно пользователь не может устанавливать более свободный доступ к его ресурсам, чем тот, который дан администратором. Применение мандатной политики безопасности предотвращает утечку информации от объектов с высоким уровнем доступа к субъектам с низким уровнем доступа [1].

2. Модель Белла-ЛаПадулы. Модель основана на мандатной модели управления доступом. В классической модели Белла-ЛаПадулы анализируются условия [3], при которых невозможно создание информационных потоков от субъектов с более высоким уровнем доступа к субъектам с более низким уровнем доступа. Первое условие: субъект может читать информацию из объекта только в том случае, если уровень доступа субъекта преобладает над уровнем конфиденциальности объекта. Второе условие: субъект может записывать информацию в объект только в том случае, если уровень конфиденциальности объекта превышает уровень доступа субъекта.

3. Избирательное или же дискреционное управление доступом [1]. Являет собой управление доступом субъектов к объектам на основе матрицы доступа, в которой строки соответствуют субъектам, а столбцы – объектам. Для каждой пары «субъект – объект» задается явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.).

4. Управление доступом на основе ролей. Основная идея реализуемого в данной модели подхода состоит в том, что понятие «субъект» заменяется двумя новыми понятиями [3]: пользователь – человек, работающий в системе; роль – совокупность

полномочий, необходимых для тех или иных действий в системе. Каждому пользователю в зависимости от его должности назначается список доступных ролей. В свою очередь, для каждой роли указывается ограниченный набор полномочий при доступе к объектам системы.

Применение подхода разграничения доступа уменьшает вероятность инсайдерской угрозы, так как определяющим фактором для действий инсайдера является круг его возможностей для нанесения ущерба. Но полностью исключить такую угрозу нельзя, так как всегда есть вероятность того, что инсайдером окажется сотрудник с достаточным уровнем доступа для реализации широкого спектра угроз.

Анализ инсайдерских угроз

Рассмотрим наиболее распространенные сценарии угроз [2].

1. Угроза утечки конфиденциальной информации: когда важная для организации информация покидает корпоративный периметр и оказывается в руках тех, у кого нет прав на ее использование.

2. Обход средств защиты: когда инсайдеры знают, какие именно средства защиты установлены в организации, они намеренно буду пытаться обмануть систему защиты. По сути это подсценарий первого сценария. Его выделяют в отдельный сценарий из-за того, что, если инсайдер в силу служебного положения знаком с системами защиты организации, то уровень угрозы от него возрастает на порядок.

3. Утечка конфиденциальной информации по неосторожности: когда корпоративные секреты подвергаются риску ненамеренно. Отличается от первого сценария тем, что изначально у инсайдера отсутствуют какие-либо злоумышленные намерения.

4. Нарушение авторских прав на информацию: когда злонамеренные действия касаются неправомерного использования объектов, защищенных авторским правом.

5. Мошенничество: когда инсайдер совершает определенные неправомерные действия в рамках компании.

6. Нецелевое использование информационных ресурсов компании: когда инсайдер использует информационные ресурсы компании для неправомерных действий.

7. Саботаж IT-инфраструктуры: когда своими умышленными действиями инсайдер мешает нормальному функционированию компании.

Каждому сценарию могут соответствовать несколько конкретных угроз. Каждая конкретная угроза может относится к нескольким сценариям. На основе этого составим таблицу принадлежности возможных угроз рассмотренным сценариям (табл. 1).

Выводы

Обзор моделей управления доступом показывает, что существуют разные варианты разграничения доступа. Но ни одна модель не защитит от человеческого фактора. Поэтому вероятность инсайдерской угрозы существует всегда, ведь инсайдером может стать любой сотрудник с любым набором полномочий. Рассмотренные варианты угроз показывают, что существует довольно обширный список возможностей для инсайдеров. Чтобы разработать качественную модель противодействия инсайдерам, необходимо провести классификацию инсайдеров, определить возможности каждого отдельного класса и, согласно этому, определить возможные меры и средства защиты.

Таблица 1

Таблица принадлежности возможных угроз рассмотренным сценариям

Сценарии / Конкретные угрозы	Утечка информации	Обход средств защиты	Утечка по неосторожности	Нарушение авторских прав	Мошенничество	Нецелевое польз. инф. ресурсов	Саботаж
Копирование информации на посторонние носители	+	+	+				
Утеря носителей информации			+				+
Пересылка конфиденциальных данных по незащищенному каналу	+		+				
Порча носителей конфиденциальной информации							+
Посещение посторонних сайтов						+	
Загрузка, хранение, использ. посторонних фалов на рабочем месте						+	
Передача информации на сторонние открытые ресурсы			+				+
Разглашение информации							+
Превышение должностных полномочий для доступа к информации					+		
Использование чужих идей/разработок				+			
Порча и фальсификация данных							+
Рассылка спама с корпоративной почты						+	
Подделывание документации					+		
Кража информационных носителей	+						+
Загрузка вирусов в корпоративную сеть							+
Уничтожение информации							+
Порча оборудования							+
Изменение/искажение информации					+		+
Порча имиджа компании							+
Порча оборудования							+
Организация каналов утечки информации		+					
Установка вредоносных скриптов на сайтах компании		+					+
Преобразование данных (шифрование, измен. формата, кодировки)		+					
Шифрование информации на собственном ключе				+			

Для выявления уязвимостей к инсайдерским угрозам необходимо использовать графовый подход, связывающий модель управления доступом и инсайдерские угрозы.

Список литературы

1. Девянин П.Н. Модели безопасности компьютерных систем [текст]: учебное пособие / П.Н. Девянин. – М.: Академия, 2005. – 144 с.

2. Скиба В.Ю. Руководство по защите от внутренних угроз информационной безопасности [текст] / В.Ю. Скиба, В.А. Курбатов. – СПб.: Питер, 2008. – 320 с.

3. Цирлов В.Л. Основы информационной безопасности автоматизированных систем [текст]: учебное пос. / В.Л. Цирлов. – Ростов-на-Дону: Феникс, 2008. – 253 с.

4. Исследование утечек информации за первое полугодие 2015 года [Электронный ресурс] / InfoWatch. – Режим доступа к ресурсу: http://www.infowatch.ru/analytics/reports/16340# (дата обращения 21.10.2015).

Поступила в редколлегию 28.10.2015

Рецензент: д-р техн. наук, проф И.В. Рубан, Харьковский национальный университет радиоэлектроники, Харьков.

АНАЛІЗ МОДЕЛЕЙ ІНСАЙДЕРСЬКИХ ЗАГРОЗ У СОЦІАЛЬНО-ТЕХНІЧНИХ СИСТЕМАХ

А.О. Ващеня, Е.В. Лисенко

У даній статті проведений огляд чотирьох основних моделей керування доступом. Розглянуті принципи функціонування кожної моделі. Також проведений короткий аналіз можливих інсайдерських загроз. Представлено можливе розбиття основних сценаріїв на конкретні загрози.

Ключові слова: *розмежування доступу, модель керування доступом, сценарії загроз, інсайдер.*

ANALYSIS OF MODELS OF INSIDER THREATS IN THE SOCIO-TECHNICAL SYSTEMS

A.A. Vashchenia, E.V. Lisenko

In this article we propose a review of four major models of access control. There is a description of functioning principles of each model. Also a brief analysis of possible insider threats is presented. And we propose a possible fragmentation of the basic scenarios to specific threats.

Keywords: *access control, access control model, threat scenarios, insider.*