УДК 681.3.07

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ, СОЗДАННОЙ НА ОСНОВЕ СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Асташев В.Б., Шипулин П.М.,
Научный руководитель – канд. физ.-мат. наук, доцент Кучеров М.М.
Сибирский федеральный университет
Институт космических и информационных технологий

В современном мире мы постоянно сталкиваемся с различными информационными системами. Каждая информационная система имеет свои характеристики, свое назначение, своих создателей и свою степень защиты. Но какие бы замки не защищали эту систему, всегда найдется уязвимость, которая сможет стать критической. Споры по поводу того, приводит ли свободное программное обеспечение к большей или меньшей безопасности, длятся уже много лет. Трудно выбрать ту или иную позицию, поскольку это программное обеспечение предоставляет большие преимущества по безопасности как защитнику системы, так и злоумышленнику. К счастью, технология по укреплению безопасности для систем со свободно распространяемым программным обеспечением может помочь защитнику системы в укреплении ее безопасности.

На самом деле, тяжело дать точное определение слова «защищена» по отношению к информационной системе. Именно поэтому оценка защищенности имеет, в основном, условный характер. Большинство современных систем, используемых в различных структурах, имеют сторонних, по отношению к организации, разработчиков. Это первое и одно из самых важных замечаний. Перед тем, как внедрять такую систему, следует рассмотреть ее работу с целью выявления «закладок» программного кода, созданных разработчиками, которые смогут выдавать хранимую информацию. Следует также рассматривать возможность кражи информации так называемыми «инсайдерами». Не стоит забывать о возможности взлома системы через внешние интерфейсы.

Если невозможно создать абсолютно защищенную систему, как же тогда обрабатывать и хранить информацию? Большие компании, такие как ОАО «РЖД», разрабатывают системы, отвечающие собственным требованиям. Подобные системы используются только на рабочих станциях, которые не имеют выхода в Интернет и публичные сети. Информация, которая проходит через почтовые ящики работников, просматривается на предмет невыдачи корпоративной тайны специальными работниками. За каждым работником скрытые элементы системы ведут пристальную «слежку», собираемая ими информация хранится длительное время в специальных хранилищах. Открытые интерфейсы имеют строго ограниченную форму допуска к служебной информации, а также подключения к другим местам хранения данных. Каждый бит особо важной информации имеет несколько копий, хранящихся в разных частях предприятия. Система постоянно претерпевает модернизации, улучшающие уровень ее безопасности, уровень ее надежности.

Но как быть, если невозможно разграничить доступ компьютеров информационной системы к публичным сетям? В этом случае приходится использовать специальные программы типа Firewall. Они достаточно защищают систему от доступа к ее узлам извне, препятствуют выдаче конфиденциальной информации. Но, к сожалению, и они не могут противостоять проникновению через скрытые от пользователей «люки» или ошибки этой программы. В таких случаях приходится прибегать к другому виду программ – Honeypot (рис. 1).

За столь безобидным названием скрываются весьма мощные средства предотвращения вторжений. В то время как злоумышленник, пытаясь идти по пути наименьшего сопротивления, сканирует открытые порты компьютера-приманки, система начинает «бить тревогу», сообщая о наличии злоумышленника, его способах воздействия на систему. В зависимости от самой программы Honeypot на этом этапе защиты можно выбрать тот набор базовых действий, которые будет предпринимать система при обнаружении вторжения: она может начать выдачу ложных данных, может отключить хранилища данных, может просто поддаваться взлому. Но и эти действия имеют предел.

Именно с этого момента начинается поле нашей деятельности. Сама работа заключается в составлении различных комбинаций «защищенной», на первый взгляд, системы, а затем проведения атак на уровне сетевого программного обеспечения с использованием различных алгоритмов. Последующий анализ комбинации шагов, приводящих к сбоям в работе системы, позволяет совершенствовать свои знания как в разработке системы с использованием широкодоступного набора программ, часть которых является свободно распространяемыми, так и получать представление о трудоемкости тех действий, которые необходимо проделать злоумышленнику для достижения своих целей.

Таким образом, возможность создания информационной системы состоящей, по большей части, из свободно распространяемых программ, и отвечающей заданным требованиям безопасности можно считать реальной. И здесь как раз подходит достаточно известный алгоритм разработки. Вначале следует определить, что мы будем обрабатывать и хранить. Отталкиваясь от этого, нужно изучить неформальную модель нарушителя этой системы. Исходя из полученной информации, необходимо получить ответы на вопросы: «Что будем защищать?» и «От кого будем защищать?». Далее следует выбор программного обеспечения, который определяется по наилучшему соотношению затраты/качество.

На следующем шаге требуется определить место хранения информации, а также частоту и способ ее резервного копирования. Затем необходимо определить уровни доступа к работе с этой информацией, на основании чего составляется политика безопасности. На этом этапе можно рассмотреть проблему кражи информации внутри системы и определиться с установкой программ «слежения» за пользователями. Необходимо приобрести антивирусные программы, предоставляющие требуемый уровень защиты.

Пройдя вышеописанные шаги, мы уже способны обеспечить некоторый уровень информационной безопасности системы, то есть конфиденциальность, целостность и доступность. Для настольных и распределенных информационных систем, не требующих выхода в публичные сети и не хранящих информацию, составляющую государственную тайну, такой уровень защиты можно считать достаточным, при условии, что пользователям будет запрещено устанавливать программы и работать со своими носителями информации.

Если необходимо получать доступ к внешним сетям, то здесь обязательна установка не только Firewall, но и компьютеров-приманок – Honeypot. Но без необходимой проверки начинать работу преждевременно. Следует применить расширенный набор атак, исследующих уязвимости каждого элемента системы. На основании найденных уязвимостей, следует настраивать защиту таким образом, чтобы при каждой попытке злоумышленника использовать эти «проходы», система незамедлительно оповещала администратора об атаке, а сам администратор четко знал порядок своих действий. Таким образом, мы получим защищенную информационную систему, создание которой не потребовало значительных затрат.

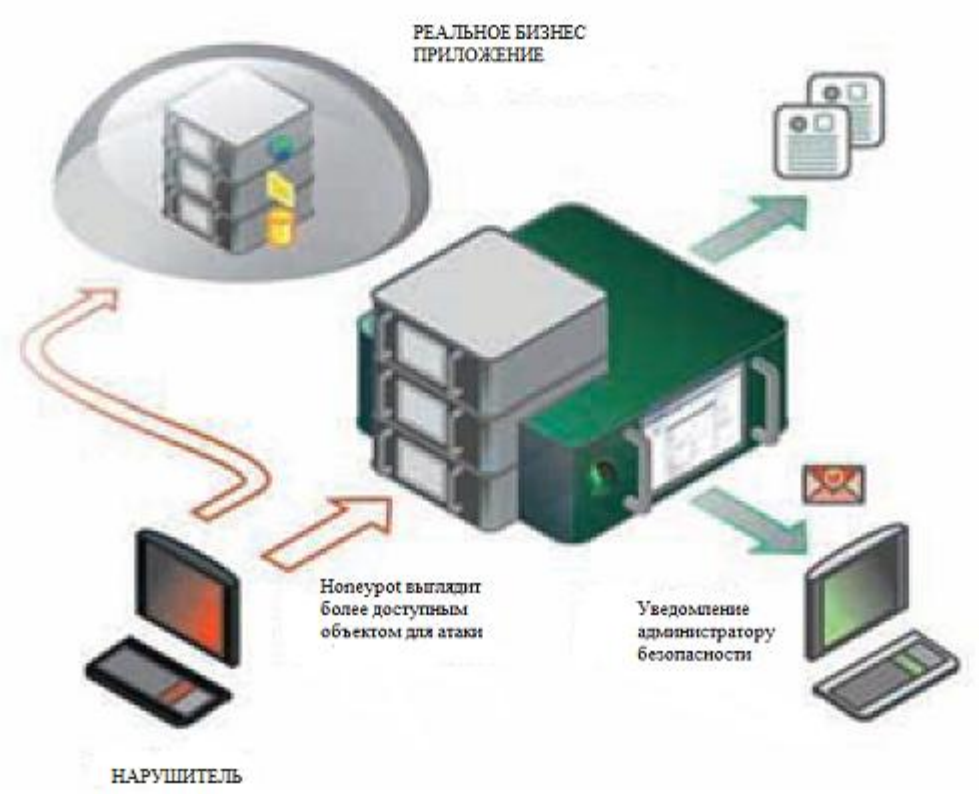

Рис.1. Honeypot – эмуляция сервера с установленной СУБД