Московский физико-технический институт (Государственный Университет)
Кафедра Радиотехники

Эссе по курсу «Защита информации»

на тему «Организационная защита, атаки и методы защиты»

студента 116 группы Седельникова М.В.

Москва, 2005г.

Содержание

Введение

В нашем XXI веке компьютеры развиваются семимильными шагами. В свете столь бурного развития компьютеров и компьютерных технологий, компьютер является незаменимым помощником и дома, и на работе. Если ранее позволить себе компьютер было роскошью, то теперь компьютер стоит почти в каждом доме.

В век компьютерной эры развиваются и корпоративные информационные системы. Не отстают в развитии и домашние компьютерные сети. Компьютер и средства взаимосвязи между ними становятся настолько привычными и обыденными для большинства людей, что уже и перестаешь заботиться о компьютерной безопасности. Предпосылками этому является халатность и надежда на проведение, на то, что основные вопросы компьютерной безопасности уже решены. Также уровень компьютерной грамотности в среднем в России все ещё остается достаточно низким, это помогает большинству компьютерных преступлений оставаться безнаказанными.

Если проанализировать материалы средств массовой информации и провести опросы населения, то можно получить примерно следующие результаты. В средствах массовой информации существует довольно много материалов об успешно проведенных хакерских операциях. Хакер является неким «кумиром» для подрастающей компьютерной молодежи. Неким гуру компьютера, который все может, а доказательством проявления крутости является взлом.

С другой же стороны, редко где можно найти описание или материалы про раскрытие компьютерных преступлений. Не ведется также агитационной работы по оповещению подрастающего поколения о последствиях творимых ими действий, а так же методах наказания.

Все выше сказанное делает занятие хакерством неким романтическим и можно сказать в какой-то сфере героическим занятием в поисках приключений.

Если посмотреть на эту проблему с другой стороны баррикады, а именно со стороны защиты компьютерной информации, то можно наблюдать следующую тенденцию. В связи с растущим количеством компьютеных сетей, проблемой их поддержания является лишь выборочные знания обслуживающего персонала. То есть ко всему прочему не квалифицированный персонал.

Рассмотрим основные функции безопасности информации, а также методы защиты этой информации. В соответствии с [1] основными функциями защиты информации являются:

- Конфиденциальность
- Целостность
- Доступность
- Наблюдаемость
- Обеспечение гарантии

На основании данных функций можно сформулировать направления основных атак, направленных на информацию. Как пример, получения доступа к конфиденциальной информации, изменение информации, являющейся недоступной для изменения никем, кроме администраторов данного ресурса и так далее.

В своей основе все атаки предполагают получения доступа до информации (чтения, записи, редактирования). Ради чего совершаются атаки? Возможны различные варианты. Можно провести классификацию данных атак:

- Атаки, совершающиеся ради развлечения. В основе данных атак может лежать как совершенствования мастерства, так и доказательство собственной «крутости», как и говорилось выше.
- Атаки, материальные цели которых являются основными. Сюда включаются также и атаки совершенные хакерами на заказ. В основе данных атак может

лежать и разведка конкурентов и изменение внутренней информации конкурентной фирмы, а также разнообразное похищение номеров кредиток и другой личной конфиденциальной информации.

- И последним, самым интересным видом атак являются атаки, заказанные хакерам на собственные информационные системы для проверки надежности систем от взлома. Данные взломы являются вполне законными и на данный момент уже существуют фирмы, осуществляющие подобные услуги. Но краеугольным камнем в данном случае является боязнь заказчика перед реальным взломом после проведения «обследования» системы безопасности. Обходным путем является заказ подобных услуг одновременно в нескольких фирмах, и информирование их об идущей между ними конкуренции.

Второй тип атак является наиболее существенным, наиболее подготовленным и содержащим в себе разнообразные способы подхода к атаке.

Осталось теперь понять, что в себя включает атака и насколько она опасна. Развитие компьютерных технологий привело к буму информации, и кроме всего прочего человечество сосредоточилось на совершенствовании программной защиты информации, совершенно позабыв про остальные аспекты защиты. И именно под взломом программного обеспечения понимается атака, что на самом деле не является верным!

Рассмотрим различные виды защиты, исходя из набора объектов, работу которых в своих корыстных целях может изменить злоумышленник, таким образом приблизившись к достижению своей цели – взлому.

- Программная защита. Далее под этим понимается взлом программного обеспечения.
- Организационная защита, которая в свою очередь подразделяется на
  - Физическую защиту помещения
  - Человеческий фактор

Отсюда несложно заключить, что наиболее эффективными атаками являются те, которые реализуются с различных фронтов. Человечество же подвергается самообману, и большинство совершенствует только программную защиту информации. Этот аспект защиты информации очень широко представлен, включает в себя много поднаправлений. В данной же работе будет рассматриваться другой, а именно организационный аспект защиты информации.

Организационная защита

Рассматривая какой-либо объект и оценивая его безопасность, можно сказать, что объект защищен настолько хорошо, насколько хорошо защищена и/или спрятана слабая сторона. Использование мощного сервера с новейшим программным обеспечением, «дыр» в котором не знает ещё не один хакер, является совершенно бессмысленным, в случае если ключи от серверной комнаты имеются у «бабы Нюры», которая должна навести там порядок. В данном примере продемонстрирована несостоятельность физической защищенности помещения, которая вместе с составляющей психологического воздействия на человека может быть основой доступа к информации.

Из всего выше сказанного можно сделать вывод о необходимости комплексного подхода к построению систем защиты информации. Основным принципом при построении комплексной системы защиты информации должен служить принцип таксономичности (одного уровня защищенности) различных аспектов зашиты.

Физическая защита помещения

Под физической защитой понимается защита сервера и прямого, физического доступа до информации, серверов, компьютеров и другого оборудования внутренней сети организации.

Основным моментом физической защиты является доступность в помещение, в котором находится оборудование, способное помочь проникнуть в сеть. Для защиты от прямого доступа к оборудованию применяются стандартные методы защиты имущества. А именно, установление соответствующий системы безопасности, включающей в себя сигнализацию, квалифицированную охрану, имеющую доступ только до внешнего периметра комнат. То есть не имеющая прямого доступа к оборудованию, которое охраняет.

Помещение, в котором хранится основное серверное оборудование, должно также обладать соответствующими стенами и потолком. Помещение с отсутствием окон является идеальным, поскольку окно является слабым место, а основной идеей является исключение слабых мест нашей защиты. Кроме того, желательно, чтобы стены комнаты не являлись стенами здания, то есть до них не было прямого доступа с улицы. Расположение помещения внутри здания также является важной частью защиты. Расположение комнаты в стороне от основного «гуляющего» потока людей является неочевидным, но вполне действенным приемом. Так каждый человек, находящийся в данной части здания уже привлекает внимание и бросается в глаза.

Доступ в данное помещение осуществляется, конечно же, через дверь, она должна быть единственной, в том понимании, что через нее должен осуществляться единственный доступ в комнату. Дверь должна быть надежно укреплена, рассчитана на преднамеренные попытки взлома, а с другой стороны являться неприметной для злоумышленника, существенно не отличаясь от остальных дверей.

В случае надежной охраны самой комнаты, так что не имеется возможности прямого проникновения внутрь, у злоумышленника остается ещё два способа. Первым является прямой взлом программного обеспечения, этот путь в данной работе не рассматривается. Вторым способом является воздействие через электрическую сеть. Отключение электричества может быть направлено на нарушение работоспособности оборудования, сбоев в нем, в результате чего получения доступа к информации. Установление автономного питания серверов, в том числе и использование источников бесперебойного питания, обеспечивает защиту на время отсутствия электропитания.

При данных видах атак чаще всего ведется борьба за целостности информации, поэтому ещё одним методом защиты целостности информации, на случай взлома, является создание архивной копии. Частота создания архивной копии определяется важностью и объемами поступления новой информации. Но в любом случае, методы защиты архивной копии должны не уступать методам защиты основного источника информации.

Оговоренные ранее методы защиты помещений по большинству относятся к защите серверных комнат, в которые доступ должен быть полностью закрыт. Но существуют ещё и компьютерные сети, принадлежащие организациям, с множеством компьютеров, защиту которых такой же степени организовать сложно, да и является лишним мероприятием. Поэтому для защиты рабочих компьютерных мест сотрудников используются немного другие способы защиты.

Первым делом необходимо препятствовать проникновению посторонних лиц на территорию компании без необходимости. В случае нахождения постороннего человека на территории организации, следует обращать внимание на его действия и противостоять несанкционированному использованию рабочих компьютеров. Методом противодействия

может служить сопровождение человека от вахты до того места, куда он направляется и обратно.

Также следует опасаться стажеров и людей, приходящих на собеседование в компанию. Если злоумышленник не имеет непосредственного доступа до компьютера, он может попросить служащего организации открыть его резюме, находящееся на дискете, флешке и присланное по почте. При этом внутрь открываемого документа может быть зашит и троян, и вирус, или и то и другое. Поэтому для изучения резюме желательно использовать специальный компьютер, не подключенный к сети.

В данной части работы рассматривались только превентивные методы защиты, направленные на нейтрализацию любых попыток взлома.

Социальный инжиниринг

Самым же слабым местом защиты на данный момент является все ещё человеческий фактор. Какими бы не были современными остальные средства защиты, наличие у нерадивого сотрудника слишком больших прав, или наличие слишком большого количества нерадивых сотрудников может очень негативно сказаться на общей информационной защите организации.

Самым эффективным и самым, пожалуй, безопасным для злоумышленника методом атаки является атака на человека. В основе подобных атак лежат психологические факторы, заложенные в каждом человеке. Самой эффективной атакой является игра на человеческих комплексах, потому как комплексы самая слабая сторона человека. Приведем один пример. Так если вспомнить детские развлечения по телефону, каждый этим в детстве занимался и прекрасно помнит следующую шутку:

Звонящий (З): Алло, здравствуйте!

Ответчик (О): Здравствуйте.

З: А почему у Вас изо рта чесноком воняет?

О (смущенно): Да что вы… А кто звонит? Что Вам нужно?

Данный пример, прекрасно показывает, что на подсознательном уровне человек первым делом реагирует на удар по его комплексу, лишь через мгновение он понимает, что злоумышленник не может знать про этот комплекс. Также все происходит и в реальной жизни, только жертва может и никогда не осознать того, что она являлась марионеткой в руках искусного кукловода.

При этом человечество обладает таким громадным количеством комплексом, что можно «ударить» практически в любое место и попасть в человеческий комплекс. С развитием же информационных технологий воздействовать на человека не показывая, и не открывая своей настоящей личности, становится все проще. Это является обратной стороной монеты развития информационных технологий.

Другим видом воздействия на человека является воздействие на его чувства. Можно влюбить в себя неопытную секретаршу и так ненароком выпытать из нее пароли или даже необходимые конфиденциальные документы. Воздействие с помощью красивой девушки на молодых людей производить ещё более просто.

В своем первоначальном понимании социальный инжиниринг понимал как раз таки воздействие на человеческую психологию. Но можно также это совмещать с уже известными человеческими недосмотрами в информационной безопасности.

Так получило свое развитие направление «копание в мусоре». По своей компьютерной безграмотности люди выкидывают в мусор все, что лежит на столе. При этом не особо задумываясь, что множество бумажек, на которых сделаны временные пометки, могут содержать ключевую информацию необходимую для взлома. Так если администраторы сети ставят условием частую смену сложных паролей, сотрудники организации начинают записывать пароли на листочках, которые после чего перекочевывают в мусорное ведро.

При социальном инжиниринге используется также следующий философский принцип, который гласит: "Не множить сущности без надобности" и называется Бритва Оккама. Данный принцип к нашей ситуации можно проинтерпретировать следующим образом. Человек домысливает развитие ситуации и собеседника, находящегося перед ним по самому простому варианту. Но данный принцип не является верным для взаимоотношений между людьми, потому как злоумышленник может преднамеренно показывать жертве совершенно другую картину, чем она есть на самом деле.

При всем выше сказанном данный способ взлома систем безопасности является самым распространенным и незаметным. Даже если жертва понимает, что её обманули, редкими являются случаи обращения к системным администраторам и службе безопасности.

«Сговор»

Наравне с остальными методами организационной защиты можно выделить атаки, совершенные в результате сговора. С другой стороны можно рассматривать данный вид взлома как подмножество социально инжиниринга, так как в сговоре все равно существует инициатор, который склоняет остальных участников сговора к взлому. Выделение в отдельную главу обусловлено тем, что обычно все участники являются сотрудниками организации.

В сговоре так же могут применяться все виды атак социального инжиниринга, рассмотрим здесь только организационную сторону предотвращения сговора.

Разделение функциональных обязанностей сотрудников началось ещё вовремя образования мануфактур. Но разделение функционала применяется для увеличения продуктивности, а разделение подразделений территориально является методом защиты от сговора. Так если у одного человека есть доступ до всевозможных информационных систем организации, появляется соблазн воспользоваться данным преимуществом.

Аналогичное явление может проявляться, когда несколько подразделений находятся в одном помещении и между сотрудниками устанавливаются тесные отношения. Это не страшно, когда организация является небольшой и имеется возможность следить за всеми потоками информации. Но в случае большой компании следует избегать такого расположения рабочих мест в офисе.

Одним из видов сговора, подходящий по тому же виду атаки, является сговор с самим с собой. Сотрудник может поставить себе цель завладеть доступом до множества различных видов информации и тем самым иметь подход к информационной системе безопасности с различных сторон.

Примером такой дыры в защите информации, распространенным в организациях является «открытие» новых прав доступа и «незакрытие» старых при переходе сотрудника из одного подразделения компании в другое. Известны случаи, когда, начав свою карьеру со стажера и пройдя через множество подразделений компании, сотрудник имел доступ до информации почти всех отделов.

Методы организационной защиты

На основании перечисленных выше атак сформулируем основные методы защиты от таких атак и подобных им. Классификация атак по существенным отличиям позволяет утверждать о достаточной полноте списка:

- ✓ Следует определять слабые места в информационной системе безопасности и направлять все силы на устранение этих слабых мест.
- ✓ Определив все риски в своей защите, можно оценить стоимость этих рисков, как произведение вероятности на стоимость последствий взлома. В условиях, если

стоимость риска приблизится к стоимости взлома, то можно будет утверждать, что система защищена. Потому как взлом будет просто не интересен злоумышленнику.

- ✓ Доступность каждого члена организации лишь до необходимой ему информации. Закрытие информации не являющейся необходимой. Даже в условиях «взлома» данного сотрудника злоумышленник не получит большой пользы. А «взлом» нескольких сотрудников одновременно осуществить гораздо сложнее.
- ✓ Слаженная деятельность системных администраторов и службы безопасности. Оперативное реагирование на любые попытки взлома и парирование этих попыток.
- ✓ Отсутствие паролей к общедоступной информации, что приводит к тому, что не приходится проводить аутентификацию пользователя лишний раз, тем самым лишний раз пересылая его пароль внутри сети.
- ✓ Как известно лучшим способом защиты является нападение. Как вид защиты от любых видов атак есть запуск «утки», а именно дезинформации злоумышленника. Таким образом, хакер получает не саму информацию, а веру в нее и этого достаточно для парирования атаки. Приведем несколько видов запуска дезинформации:
  - Показ злоумышленнику неправильной информации, которую он хочет получить. Для этого организуется дублирующий сервер, который он с легкостью (но чтобы не вызвать подозрений) взламывает и получает подложенную туда «утку»
  - Показ злоумышленнику самых сильных сторон, при этом подразумевая, что они самые слабые. В этом случае, видя безосновательность своих претензий на взлом, злоумышленник отказывается от взлома
  - Самостоятельный запуск информации в сеть. Сюда может входить описание ложных дыр в заданной системе защиты, что сводится к предыдущему пункту, и другие виды запуска ложной информации.
- ✓ Запрет пользоваться ICQ всему персоналу / Осуществление контроля переписки по всем внешним источникам информации (Защита от обмена информацией, по личным амбициям)
- ✓ Разработка политики безопасности, которая доводится до всех пользователей, и непрекословно исполняется ими. Политика безопасности должна учитывать множество факторов, но и не должна быть слишком строгой. Политика безопасности может содержать следующие моменты:
  - Обучение сотрудников организации основам компьютерной грамотности;
  - Правила пользования информационными ресурсами организации;
  - Все моменты атак, в основе которых лежит социальный инжиниринг;
  - Правила установление паролей пользователей, установленный образец (что парирует риск перебора паролей, содержащие в себе имена «бывших любовниц» и т.д.) В данном случае главное, чтобы метод создания пароля не вышел за границы компании;
  - Периодичность смены паролей. Не стоит устанавливать слишком частую смену паролей. Пользователи начнут повторяться или записывать пароли, что является негативным фактором.

Перечисленные методы защиты охватывают большую часть возможного противодействия и защиты от множества атак, так как при описании атак они рассматривались по общим принципам, лежащим в основе. Но вместе с методами защиты от атак появляются все новые виды атак, каждая из которых хранит в себе что-то новое и гениальное. Быть уверенным, что информационную систему взломают нельзя быть уверенным никогда, но всегда можно снизить эту вероятность.

Литература

[1] http://bezpeka.mk.ua/articles/seminar
[2] Елена Полонская, Источник: "Компьютеры+программы", http://hackzone.stsland.ru/63.html
[3] «Секретное оружие социальной инженерии» Крис Касперски. Журнал "LAN", #09, 2002 год // Издательство "Открытые системы" (www.osp.ru) http://www.osp.ru/lan/2002/09/080.htm