Данный материал является фрагментом электронного учебника
по информационной безопасности и может обновляться.
При цитировании рекомендуется использовать ссылку:

Амелин Р. В. Информационная безопасность. Конспект лекций // Амелин Р.В. Лаборатория преподавателя [Электронный ресурс]. URL: rv-lab.ru (2017).

Введение

Под ***информационной безопасностью*** понимают состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений (в том числе владельцам и пользователям информации).

Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности. Существует также одноименная учебная (научная) дисциплина – отрасль информационных технологий, занимающаяся изучением (разработкой) средств, методов и моделей защиты информации.

Самая распространенная модель информационной безопасности базируется на обеспечении трех свойств информации: конфиденциальность, целостность и доступность.

Конфиденциальность – состояние информации, при котором ознакомиться с ней может только строго ограниченный круг лиц, имеющих на это право. Если доступ к информации получает неуполномоченное лицо, происходит утрата конфиденциальности.

Используются и другие определения конфиденциальности:

- Конфиденциальность – обеспечение доступа к информации только авторизованным пользователям (ГОСТ 17799-2005[1]);
- Конфиденциальность – обязательное для исполнения требование к лицу, получившему доступ к информации, не допускать ее распространения без согласия владельца или законного основания;
- Конфиденциальность – необходимость предотвращения утечки информации.

Для некоторых типов информации конфиденциальность является наиболее важным свойством. Это государственная тайна, служебная тайна (медицинские и страховые записи, материалы следствия, налоговые данные), коммерческая тайна (данные стратегических исследований, спецификации новых изделий), персональные данные (сведения о клиентах банка, кредиторах, партнерах), интимная переписка.

Целостность – такое состояние информации, при котором изменения в нее вносят только уполномоченные лица. Целостность теряется, когда в результате сбоев или действий злоумышленника данные искажаются. Обеспечение целостности с точки зрения информационной безопасности – это решение двух самостоятельных задач:

1) Собственно предотвращение искажения данных. В основном включает методы защиты от естественных и непредумышленных угроз: обеспечение отказоустойчивости (зеркалирование оборудования, например, с мощью RAID-массивов) и обеспечение безопасного восстановления (резервное копирование и т.д.), антивирусная защита.

2) Обнаружение искажений. Получатель сообщения должен точно знать, дошло ли оно до него в том виде, в котором было отправлено. Эта задача решается, в основном, криптографическими методами.

[1] ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

Другие определения целостности:

- Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право (Рекомендации по стандартизации Р 50.1.056-2005[2]).
- Целостность информации – условия, при которых информация хранится, передается и принимается без изменений.

Целостность особенно важна для данных, связанных с функционированием объектов критических инфраструктур (например, управления воздушным движением, энергоснабжения и т. д.), финансовых данных, CRM и ERP-системах.

Показателен пример, когда злоумышленник вторгся в компьютерную систему исследовательской лаборатории ядерной физики в Швейцарии и изменил один знак в значении числа «пи», в результате чего из-за ошибок в расчетах был сорван важный эксперимент, а организация понесла миллионные убытки[3].

Доступность – состояние информации, при котором субъекты, имеющие право доступа к ней, могут беспрепятственно осуществлять этот доступ. Уничтожение или блокирование информации (в результате ошибки или преднамеренного действия) приводит к потере доступности.

Другие определения доступности:

- Доступность информации – возможность за приемлемое время выполнить ту или иную операцию над данными или получить нужную информацию.

Доступность считается наиболее важным из трех рассмотренных свойств. Информационные системы создаются для того, чтобы оказывать информационные услуги. Если информация недоступна, предоставление таких услуг становится невозможным. Информационная система выведена из строя.

Особенно важна доступность для систем, ориентированных на массовое обслуживание клиентов (системы продажи железнодорожных билетов, распространения обновлений программного обеспечения, банковские услуги).

Ситуацию, когда уполномоченный пользователь не может получить доступ к определенным услугам (чаще всего сетевым), называют *отказом в обслуживании* (DoS – Demand of Service).

Нарушение доступности информации при помощи DoS-атаки хорошо иллюстрирует один нашумевший случай – *дело балаковских хакеров*.

Дело балаковских хакеров

Балаковские хакеры шантажировали английских букмекеров.

Букмекер – организация (реже один человек), чья работа состоит в предложении пари на исходы спортивных состязаний (иногда других событий). Букмекер принимает

[2] Рекомендации по стандартизации «Техническая защита информации. Основные термины и определения» (Р 50.1.056-2005)

[3] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография — М.: Норма, 2004. С. 21.

деньги (ставки) по установленным им коэффициентами и выплачивает выигрыши [www.bukmekerskiekontory.ru].

Англия – наиболее крупная историческая и административная часть Соединенного Королевства Великобритании и Северной Ирландии, официально страна в его составе, занимающая юго-восточную часть большого острова Великобритания. Население Англии составляет 83 % от общего числа населения Великобритании. [wikipedia.org]

Хакер – высокопрофессиональный программист, склонный к нетривиальным решениям, искушённый в тонкостях компьютерных систем, способный принести большую пользу или вред [ru.wiktionary.org].

Английские букмекеры принимают ставки посредством своих интернет-сайтов. Те самые балаковские хакеры устраивали распределенные DoS-атаки на эти сайты. В результате сайты падали, пользователи не могли зайти сделать ставки, английские букмекеры несли убытки.

Распределенная DoS-атака (DDoS-атака) заключается в том, что атакуемый сервер начинает получать огромное количество запросов (десятки тысяч в секунду), которые не успевает обработать – и в результате совсем выходит из строя после переполнения всех возможных буферов, либо перестает обрабатывать запросы обычных пользователей (они просто теряются в этом потоке).

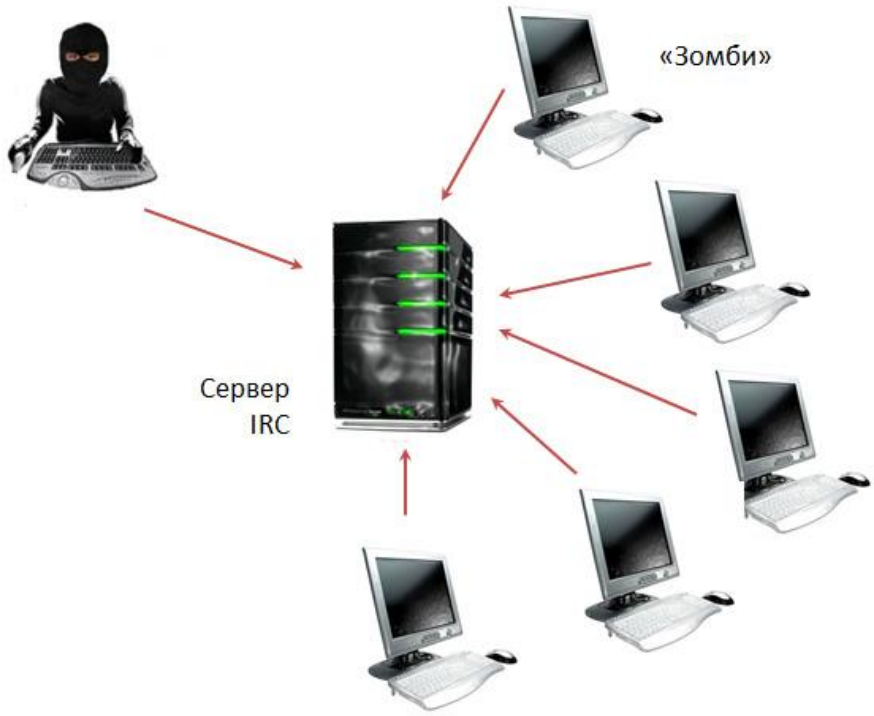

Рис. 0.1. Структура ботнета

Чтобы такая атака стала реальной (одновременные запросы со ста тысяч компьютеров), нужно создать вирус, который заразит эти сто тысяч компьютеров, но вирус не простой, а управляемый. Зараженный компьютер периодически подключается к специальному управляющему серверу (см. рис. 0.1**Ошибка! Источник ссылки не найден.**) и получает от него указания о том, какие сайты следует бомбить. Множество компьютеров, зараженных таким управляемым вирусом, называют *зомби-сетью* или *ботнетом*.

В общем случае ботнет – это сеть компьютеров («зомби» или «ботов»), зараженных специализированным вирусом, посредством которого злоумышленники получают частичное управление этими компьютерами, используя их ресурсы в своих целях.

Основные команды, которые умеют исполнять боты, это *update* (обновление бота или установка на зараженный компьютер дополнительных вредоносных программ), *flood* (собственно DDoS-атака: направление множества одновременных запросов от всех зараженных компьютеров по указанному адресу), *proxy* (использование зараженного компьютера в качестве прокси-сервера – т.е., работа в сети от его имени). К опциональным возможностям относятся рассылка спама, «накрутка» посетителей сайта или счетчика голосования, показ всплывающей рекламы и т.д.

Имея в своем распоряжении рабочий ботнет, балаковские хакеры направляли английским букмекерским конторам письма примерно следующего содержания: «В указанный день на компанию будет совершена DDoS-атака, длительность которой будет зависеть от ее руководства. Если отправитель письма не получит 15000 долларов, атака будет продолжаться до полного банкротства компании»[4]. Убытки, которые несли компании (прежде чем уступить требованиям вымогателей) значительно превышали запрашиваемые суммы.

Кроме трех перечисленных свойств дополнительно выделяют еще два свойства, важных для информационной безопасности: аутентичность и апеллируемость.

Аутентичность – возможность достоверно установить автора сообщения.

Апеллируемость – возможность доказать, что автором является именно данный человек и никто другой.

Как учебная и научная дисциплина информационная безопасность исследует природу перечисленных свойств информации, изучает угрозы этим свойствам, а также методы и средства противодействия таким угрозам (защита информации).

Как прикладная дисциплина информационная безопасность занимается обеспечением этих ключевых свойств, в частности, путем разработки защищенных информационных систем.

[4] Подробнее см. В. Н. Черкасов. Дело «Балаковских» хакеров. Факты и размышления // «Информационная безопасность регионов». – № 6—8.