СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Никитин П.В., Капелькина А.В., Фархшатов И.В.

В настоящее время проблемы защиты информации являются приоритетными направлением. Под защитой информации понимается защита от угроз, исходящих от источников программного характер, которые воздействуют на уязвимости, характерные как для рядового пользователя, так и для локальных сетей компании, с целью защиты персональных данных. Ситуация усугубляется тем обстоятельством, что информационные технологии все больше проникают в нашу жизнь, тем самым защита персональных данных является первоначальной задачей любой организации либо рядового пользователя. В данной статье рассматриваются семь самых распространенных сетевых атак и способы защиты с ними, такие как: анализ сетевого трафика, сканирование сети, угроза выявления пароля, подмена доверенного объекта, навязывание ложного маршрута, внедрение ложного объекта сети и отказ в обслуживании. Показано, что для осуществления эффективной политики информационной безопасности, необходимо проводить комплексный подход во избежание внешнего проникновения. Преднамеренные действия в области защиты информации могут предотвратить возможность сетевых атак. Уникальность данной статьи заключается в том, что были рассмотрены самые распространенные сетевые атаки и предложены комплексные меры по их предотвращению.

Ключевые слова: защита информации, информационная безопасность, сетевые атаки, методология информационных угроз

THE MODERN PROBLEMS OF PERSONAL INFORMATION SECURITY

Nikitin P.V., Kapelkina A.V., Farkshatov I.V.

Nowadays the problem of information security is a priority. Under the protection of information refers to protection against threats from the nature of the sources of software that affect the vulnerability, typical for the average user, and for the company's local area network, in order to protect personal data. The situation is aggravated by the fact that information technology is increasingly introducing our lives, that's way the protection of personal data is the initial task of any organization or an ordinary user. This article focuses on the seven most common network attacks and ways to protect them, such as: network traffic analysis, network scanning, threat of revealing the password, the substitution of the trusted object, the imposition of a false route, the introduction of a false network entity and denial of service. It has been shown that effective information security policy, it is necessary to carry out a comprehensive approach to prevent outside intrusion. Deliberate actions in the field of information security can prevent network attacks. The uniqueness of this article lies in the fact that they were considered the most common network attacks and proposed wide measures to prevent them.

Keywords: information security, network attacks, methodology of information threats

Современное общество дошло до такого уровня, когда некоторые формальные границы, существовавшие ранее, начинают исчезать. В настоящее время, когда люди добровольно публикуют информацию о себе в различных аккаунтах, множество программ считывают действия пользователей, шпионские программы автоматически отправляют информацию о пользователе без его согласия, необходимо задумываться о защите своих данных. Все отмеченные процессы, во многом имеют серьезные последствия, как для рядового пользователя, так и организаций в целом, которые в них участвуют.

Исследования ведущих компаний постоянно подтверждают озабоченность бизнеса проблемами ИТ-безопасности внутри компаний. Проблема защиты конфиденциальных данных занимает лидерство по ИТ-проблемам. Можно уверенно утверждать, что проблема

защиты конфиденциальных данных приобретает наибольшее значение, чем хакерские и вирусные атаки.

Под информационной безопасностью будем понимать защиту от перечня угроз безопасности персональных данных, исходящих от источников, имеющих программный характер и воздействующих на уязвимости, характерные как для рядового пользователя, так и для локальных сетей компании, в конечном итоге реализующих угрозы информационной безопасности [4].

На практике наиболее реализуемыми атаками можно назвать следующие:

1) Анализ сетевого трафика. Данную угрозу используют для получения идентификатора и пароля пользователя с помощью «прослушивания сети». Программа-анализатор перехватывает пакеты по сети и, если протокол передает открытую аутенфикационную информацию, легко получить доступ к учетной записи пользователя.

Одним из наиболее эффективных методов защиты системы от данного типа атаки является запрет на использование основных прикладных протоколов удаленного доступа TELNET и FTP, которые не предусматривают криптозащиту передаваемых по сети идентификаторов и аутентификаторов. Атака становится бессмысленной при использовании стойких криптографических алгоритмов защиты IP-потока.

2) Сканирование сети. В результате угрозы собирают информацию о топологии сети, открытых портах и др. Эта угроза проводится в форме DNS-запросов, эхо-тестирования адресов[2]. В результате эхо-тестирования можно получить список хостов работающих в данной среде. Далее сканируют порты и затем составляют список услуг, которые поддерживают хосты. В итоге, злоумышленник проводит анализ характеристик приложений, работающих на хостах, и получает информацию для взлома системы.

Избежать полностью данной атаки невозможно. Один из способов борьбы с данной атакой — использование систем обнаружения вторжений (IDS), которые оповестят администратора о ведущейся сетевой разведке.

3) Угроза выявления пароля. Данная атака реализуется с помощью простого перебора значений, перебора специальных программ, перехвата пароля с помощью программ-анализаторов сетевого трафика и многих других методов.

Идеальным вариантом защиты от данной атаки является не использование паролей в текстовой форме. К сожалению, не все системы/устройства поддерживают одноразовые пароли или криптографическую аутентификацию.

Так что при использовании текстовых паролей старайтесь, чтобы длина пароля была не менее 8 символов. Обязательно пароль должен содержать знаки верхнего регистра, цифры и различные символы. В итоге вы получите пароли, которые будет сложно подобрать. Но тогда

мы получаем список сложных для запоминания паролей. Чаще всего это вынуждает пользователя хранить перечень паролей на бумаге либо в текстовом формате. Для решения этой задачи существуют прикладные решения, задача которых зашифровать список паролей. Таким образом, пользователю необходимо запомнить только один сложный пароль для открытия файла. Можно назвать примеры следующих программ для шифрования, существующих долгое время на рынке софта, PGP Desktop, CyberSafe, Folder Lock[3].

4) Подмена доверенного объекта. Под данной атакой понимается подмена доверенного объекта и передача сообщений от его имени по каналам связи с присвоением его прав доступа. Под доверенным лицом понимается элемент сети, легально подключенный к серверу.

5) Навязывание ложного маршрута сети. Другое название угрозы IP-спуфинг. Данная атака становится возможной из-за протоколов маршрутизации и управления сетью. Используя уязвимости протоколов, вносятся несанкционированные изменения в маршрутно-адресные таблицы[1].

Для защиты системы от данной атаки есть два варианта решения: фильтрация сообщений о маршруте, не допуская к конечному объекту, либо настройка сетевой операционной системы для игнорирования таких общений соответствующим образом

6) Внедрение ложного объекта сети. Данная атака происходит при перехвате запроса с информацией и выдаче ложного ответа, изменив таблицу маршрутизации сети. Выдавая тем самым себя за легального субъекта сети.

Чтобы ликвидировать данную угрозу необходимо устранить причину ее возможной реализации. Для этого самым несложным решением может служить создание статической таблицы в виде файла, для внесения необходимой информации об адресах. Файл необходимо установить на каждый сетевой компьютер внутри локальной сети. Из этого может следовать, что нет потребности реализации сетевой ОС процедуры удаленного поиска.

7) Отказ в обслуживании. Угроза нацелена на нарушение доступности информации для законных субъектов информационного обмена.

Защитится от данной угрозы, можно только при использовании наиболее производительных компьютеров. Большее число и частота работы процессоров, больший объем памяти процессоров способствуют повышенному уровню надежности бесперебойной работы сетевой операционной системы при обрушении потока ложных запросов на создание соединения.

Анализируя ответы студентов факультета экономики и информационной безопасности МОСИ, определили, что самой распространенной угрозой является − угроза выявления пароля. Если первые две угрозы больше характерны для крупных компаний, то чаще всего

рядовой пользователь хотя бы раз сталкивался с проблемой взлома своего профиля в социальной сети или доступа к электронной почте. Предпосылки к этому создают сами пользователи, не соблюдая элементарных правил безопасности информации в сети.

В настоящем времени средства защиты, которые применяются традиционно (антивирусы, фаерволы и т.д.) не способны полноценно защитить информационные системы организации. Чтобы эффективно противостоять современным кибератакам требуется комплексный подход, который будет сочетать в себе несколько уровней защиты с использованием различных технологий безопасности.

Чтобы защитить информационную систему организаций от внешних интернет атак можно использовать системы предотвращения вторжений на уровне хоста (HIPS). Системы отлично себя зарекомендовали и при правильной настройке дают беспрецедентный уровень защищенности.

Грамотно выстроенная политика безопасности позволяет достичь очень высокого уровня защиты. Применение совместно с HIPS других программных продуктов (антивирусного пакета и др.) позволит защитить систему организации от большинства типа вредоносного ПО, затруднит работу хакера, целью которого пробить защиту компании, сохранит интеллектуальную собственность и важные данные предприятия[5].

Защита от внутренних угроз так же требует комплексных мер. Это выражается во введении четкой организационной структуры ответственных за информационную безопасность сотрудников, контролировании документооборота, мониторинге и контроле пользователей, введении механизмов аутенфикации пользователей для доступа к информации разной степени важности.

Важно понимать, что нет ни одного продукта, способного предоставить компании «полную безопасность». Высокий уровень защиты достигается при помощи трех аспектов: сочетанием различных продуктов и услуг, соблюдением сотрудниками элементарных правил и так же грамотной политикой безопасности.

Список литературы:

1. Блинов А.М. Информационная безопасность. Санкт-Петербург, 2010. С.14-21.
2. Касперски К. Техника сетевых атак. Приемы противодействия. Солон-Р, 2001. С. 397.
3. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Санкт-Петербург, 2012. С.11-12.
4. Проскурин В.Г., Крутов С.В., Мацкевич И.В.. Защита в операционных системах. Москва, 2000. С. 10-15.

5. Министерство связи и массовых коммуникаций Российской Федерации. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли. Москва, 2010. С.8.