МЕТОДИЧЕСКИЕ ОСНОВЫ СОВРЕМЕННОЙ НФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Булатова С., Христодуло А.Д.

Уфимский государственный авиационный технический университет

Аннотация: в статье описаны методические основы современной информационной безопасности, рассмотрены такие важные понятия, как угрозы, их виды и способы реализации, ценности и меры безопасности по отношению к информации. Описаны и объяснены такие механизмы защиты информационных систем, как идентификация и аутентификация, а именно доказательства знаниями, владением и имуществом.

Ключевые слова: информационная безопасность, угрозы, политика безопасности, идентификация и аутентификация.

В последние годы правительства и военные организации разных стран широко применяют локальную и глобальную сети интернет с целью продвижения в IT-сфере. При этом, большинство организаций уверены, что их внутренняя система может быть атакована, в результате чего ценная информация будет скомпрометирована. Эффективные меры по обеспечению безопасности заключаются, прежде всего в том, чтобы детально изучить и понять проблему безопасности и факторы, которые делают информацию в сетевой среде уязвимой для атаки. Наиболее распространенными мотивами в совершении компьютерных преступлений выступают деньги, месть, терроризм, распознавание информации и даже любопытство. В связи с этим, информационные системы (ИС) могут быть атакованы как посторонними людьми, проникающими в компьютерную систему, так и членами организации, которые имеют право пользоваться всеми ресурсами компании, но злоупотребляют своей авторизацией. Атакующий может действовать двумя способами: 1) срыв ИС какой-либо организации (активная атака), 2) получение доступа к ее конфиденциальной информации (пассивная атака). Несмотря на то, что прямого ущерба во время пассивной атаки не возникает, любая утечка информации может иметь радикальные последствия для организации. Другими словами, термин «безопасность» можно определить

как «защита ИС от непреднамеренного доступа». Безопасность ИС распространяется на защиту всех её компонентов: данные, программное обеспечение, аппаратные средства и сети. Соответственно, комплексные меры по обеспечению безопасности включают в себя как политику, так и механизмы безопасности [1]. Факторами, влияющими на политику безопасности, являются деятельность всей организации, оценка риска, уровень необходимой безопасности, экономическая эффективность, обязанности по обеспечению безопасности персонала и отчетной документации, а также социальные факторы.

Базовые понятия информационной безопасности

Информационная безопасность включает в себя четыре ключевые задачи:

Конфиденциальность: Уверенность в том, что информация не обнаружена или не предоставлена посторонним лицам.

Целостность: Данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение.

Доступность: Обеспечение авторизированным пользователям доступа к информации и ее ресурсам.

Законное использование: Уверенность в том, что авторизированные пользователи не используют информацию незаконным способом .

Активы – это ценные ресурсы организации, которые должны быть защищены. Потеря активов ведет к значительному ущербу компании. В некоторых случаях потерянный актив не может быть заменен, в частности, в случае престижности фирмы или конфиденциальности исследований. В качестве примеров категорий активов могут выступать пользователи, данные, приложения, серверы, сети, документация, престиж и репутация компании.

Угрозы

Угрозами называются действия, производимые какими-либо лицами или

событиями, которые несут вред активу. Потеря актива вызвана реализацией угрозы, которая, в свою очередь, приводится в действие через среду уязвимости. Угрозы исходят из среды организации, поэтому они не могут быть полностью под контролем компании. Рассмотрим четыре основных вида угроз:

Утечка информации: Информация раскрыта неавторизированным пользователям, что приводит к угрозе секретности.

Нарушение ценности: Разрушение, изменение или создание поддельных данных, что приводит к несовместимости данных.

Отказ в обслуживании: Использование законных прав активов для полного или частичного срыва трафика.

Незаконное использование: Эксплуатация привилегий законными пользователями.

Описанные угрозы, могут быть реализованы следующими способами:

Нарушение авторизации: Лицо, авторизированное для использования ресурсов, использует эти ресурсы несанкционированно.

Путем передачи управления: Выявление недостатков системы или слабых сторон защиты для приобретения несанкционированных привилегий.

Подслушивание: Утечка информации происходит путем «мониторинга»
канала связи.

Перехватывание: Извлечение информации с радиочастот или электромагнитного оборудования.

Вредоносные программы: Программы, написанные специально для того, чтобы наносить вред другим программам.

«Маскарад»: Лицо или целая организация, выдающие себя за других.

Анализ трафика: Утечка информации путем отслеживания схемы движений трафика.

Отрицание: Лицо, принимающее участие в обмене информацией, отказывается передавать свою часть информации.

Истощение ресурсов: Использование ресурсов таким образом, чтобы сделать их недоступными для других, что, в конечном итоге, приводит к отказу в обслуживании.

Социальная инженерия: Одурачивание пользователя в целях раскрытия его пароля, в частности подглядывание из-за плеча, подслушивание разговоров так же выполняются в рамках социальной инженерии.

Уязвимость – это недостаток или отсутствие мер защиты. В отличие от угроз, уязвимость иногда существует вне организации. Уязвимость можно подразделить на: политику безопасности, процедуры, администрирование, реализацию и безразличие [2]. Меры защиты – механизмы или, процедуры, которые защищают активы компании от угроз.

Политика безопасности

Политика безопасности – свод правил, установленный организацией и применяемый ко всем действиям, связанным с безопасностью. Существуют различные уровни политики безопасности, такие как: политика менеджмента, оперативная политика и процессуальная политика. Авторизация – это фундаментальная часть политики безопасности, которая назначает каждому лицу свои исполнительные роли и выполняется с помощью механизмов контроля доступа. Механизмы и процедуры обеспечения безопасности, являющиеся основными гарантиями безопасности, называются службами безопасности .

Атака – это реализация угрозы. В широком смысле, атакующие или злоумышленники – это хакеры, шпионы, и профессиональные преступники. Инструменты, преимущественно используемые злоумышленниками, это в основном физические атаки, обмен информацией, команды пользователям, программы и выкачивание данных. Злоумышленники могут действовать различными способами, в зависимости от уязвимости данных, например, сканирование, обман, кража, чтение, копирование, изменение данных. Как правило, целью атаки являются аккаунт, данные, сетевые компоненты и сети.

Идентификация и аутентификация

Идентификация и аутентификация – это один из наиболее исследованных на сегодняшний день механизмов защиты ИС от незаконного проникновения в них неавторизированных пользователей. Идентификация – это способ, с помощью которого пользователь получает утвержденную подлинность, самой распространенной формой идентификации является ID пользователя. Аутентификация– это средство установления заявленного идентификационного номера, то есть проверка подлинности пользователя. Процесс входа в систему как раз и включает в себя эти две задачи [3]. Существует три способа аутентифицировать пользователя: доказательство знаниями, доказательство владением и доказательство имуществом.

Доказательства знаниями. Пароли

Пароль может быть связан с каждым пользователем или с целой организацией. Пароли - это обмен информацией между пользователем и системой. Чтобы получить доступ к системе, пользователь обязан ввести свой ID и пароль. Система аутентифицирует пользователя в том случае, если введенный пароль совпадает с тем, который сохранен в системе. Существует несколько способов сохранения пароля в системе.

Чёткие пароли: Система сохраняет текстовые пароли в файл, который защищен от прочтения другими пользователями. Однако, это не обеспечивает достаточную защиту от администратора системы. Место хранения файлов с паролями в резервных средствах массовой информации так же создает риск безопасности.

Зашифрованные пароли: Функция паролей заключается в том, что они сохраняются, а не стираются. Когда пользователь вводит пароль, компьютер, используя функцию паролей, сравнивает его с тем, который сохранен в ИС.

Угрозы паролям

Повторение: Злоумышленник записывает пароль, когда он передается в чистом виде по линии связи. Записанный пароль впоследствии используется в личных целях.

Атака с применением грубой силы: Злоумышленник пробует все возможные пароли, с целью отгадать правильный пароль. Успешность атаки зависит от доступного количества попыток и времени, отведенного для каждой попытки.

Отгадывание пароля: Злоумышленник отгадывает пароль, используя имена членов семьи пользователя, либо имена собственные.

Словарные атаки: Злоумышленник пытается сопоставить пароль со словарными словами. В отличие от стандартных словарей, on-line словари специализируются на словах из фильмов или песен. Данная атака чаще всего не работает в случае угадывания пароля какого-либо определенного пользователя, однако она способна взломать слабый пароль и получить доступ к системе.

Чтобы запретить использование слабых, ненадежных паролей, на пароли накладываются следующие правила:

1) минимальная длина пароля, доступные символы, верхний регистр, числа – четко определены;

2) временные рамки старения пароля указаны для того, чтобы обеспечить его изменение;

3) сайт может использовать реактивную стратегию проверки паролей, где программа по взлому паролей периодически запускается, чтобы обнаружить слабые пароли;

4) сайт так же может использовать проактивную стратегию проверки пароля, где система проверяет доступные пароли во время регистрации, если пароль ненадежный, он отклоняется.

Доказательство владением

Пользователь предоставляет какой-либо физический знак, который система воспринимает как принадлежность пользователя, например, банковская карта. Чтобы идентифицировать пользователя, вместе с физическим знаком часто используются PIN-коды. Для предотвращения

атаки PIN-кода, автомат конфискует карту, запирая ее, и деактивирует ее в случае трёх неудачных попыток введения PIN-кода.

Доказательство имуществом

Биометрические технологии опираются на измерение легкодоступных и уникальных характеристик пользователя, таких как отпечатки пальцев, голос, сетчатка глаза, геометрия лица и линии на ладонях. Когда системе требуется распознать пользователя, она получает биометрические измерения пользователя, а затем сравнивает с теми, которые сохранены в базе данных.

Таким образом, эффективные механизмы безопасности требуют глубокого понимания строения сетей, проблем безопасности, факторов, которые делают сеть ценной для атаки, администрирование сетевой безопасности, а также осведомленность о безопасности.

Список использованных источников

1. C Ptleeger, Security in Computing, Prentice-Hall, 1997.
2. E Turban, E Mclean & J Etherbe, Information Technology Making connections for strategic Advantage, John Wiley & sons, Inc, New York, 1999.
3. J Linn, Practical Authentication for Distributed Computing, Security and Privacy Symposium, *IEEE CS Press,* 1990.

METHODICAL BASICS OF MODERN INFORMATION SECURITY

Bulatova S., Khristodulo A.

Russia, Ufa State Aviation Technical University

Abstract: In this article methodical basics of modern information security are described, such important terms such as threats, vulnerabilities and safeguards were discussed. The identification and authentication schemes namely, proof by knowledge, proof by possession and proof by property were explained.

Keywords: Information Security, Threats, Political Security, Identification, Authentication.