Методы организации безопасности в операционных системах.

Мазуркевич Анастасия Дмитриевна

Содержание

Список иллюстраций

Список таблиц

Введение

Современные операционные системы (ОС) играют ключевую роль в функционировании компьютерных систем и обеспечении выполнения различных приложений. Однако с ростом числа киберугроз и увеличением объемов обрабатываемых данных, вопросы безопасности становятся особенно актуальными. Методы организации безопасности в операционных системах направлены на защиту информации, предотвращение несанкционированного доступа и обеспечение целостности данных. В данной работе рассматриваются основные подходы и технологии, используемые для обеспечения безопасности в ОС, такие как контроль доступа, шифрование данных, а также механизмы аутентификации и авторизации пользователей. Анализ этих методов позволит лучше понять, как современные операционные системы справляются с вызовами, связанными с безопасностью, и какие меры необходимо принимать для защиты информации в условиях постоянно меняющейся угрозы.

Аутентификация и авторизация

Аутентификация — проверка пользователя, котора подтверждает его личность при доступе к сайту, приложениям, аккаунтам в социальных сетях. Она необходима, чтобы убедиться, что пользователь имеет права на доступ к учётной записи в системе, на сайтах или в программе.

Основные методы аутентификации:

- пароли это пожалуй самый частый метод, который используют практически все, но он не самый безопасный и надежный так как есть угроза подбора паролей и вследствии утери доступа к аккаунту.
- биометрия или биометрические данные становятся все популярнее с каждым днём, такой метод основан на распозновании сетчатки глаза, отпечатков пальцев и других индувидуальных характеристик человека. -цифровые сертификаты(токенная), для этого используют флешки и другие физические носители, плюс этого метода в том что доступ открывается только если у тебя есть носитель -многофакторная - использование комбинации двух и более способов аутентификации, такой способ в разы повышает безопасность -данные пользователя такие как номер телефона

Авторизация - предоставление доступа после аутентификации, это подтверждение что конкретный пользователь находится на ресурсе и действия исходят от него, она направлена больше на предоставление доступа к различным действиям

Шифрование данных

Шифрование данных - преобразование данных (для их защиты) так, чтобы их значения понимали только конкретные пользователи. Так же есть обратное шифрование - дешифрование

Задачи шифрования: - конфеденциальность данных - целостность данных - неотслеживаемость данных

Основные типы шифрования:

- Симметричное шифрование Для кодировки и расшифровки информации используется один и тот же ключ. Такой способ достаточно уязвим с точки зрения безопасности данных, поэтому он чаще применяется не для передачи, а для хранения информации.
- Ассиметрическое шифрование Для кодирования и дешифровки используются разные ключи. При этом ключ, который нужен для разгадывания кода, — закрытый, то есть им владеет только нужный получатель. Такой вид шифрования информации считается более надёжным.
- Гибридное шифрование Сочетает преимущества обоих подходов: асимметричное используется для обмена симметричным ключом, а затем для работы с данными применяется более быстрый симметричный алгоритм.
- Хэш-функция Особенность этого вида шифрования в том, что он не имеет обратной силы, то есть хеш-функцию невозможно раскодировать. Исходные данные можно преобразовать миллион раз, и результат всегда будет одинаковый.

Однако, если внести изменение в первоначальную информацию, изменится и хеш-функция.

Шифрование должно быть достаточно сложным, чтобы его было трудно обойти.

Защита от вредоносного ПО

Вредоносное программное обеспечение (вирусы, трояны, шпионские программы) представляет собой серьезную угрозу для безопасности ОС.

Цели вредоносного ПО:

- похитить данные
- вывести из строя системы и сервисы
- собрать информацию о действиях пользователей
- заблокировать доступ к данным на устройстве

Основные виды:

- Вирусы. Это вредоносный код, который способен к самостоятельному воспроизведению в другом приложении, документе или в устройстве хранения данных.
- Бэкдоры. Приложение, которое способно обойти процедуру аутентификации в компьютере или устройстве и получить доступ к системе, к приложению, к базе данных, что даёт возможность удалённого управления системой.
- Вымогатели и шифровальщики. Это вредоносная программа, которая блокирует доступ пользователей к компьютерным системам и файлам, предоставляя злоумышленникам контроль над любой персональной информацией, хранящейся на устройствах жертв.
- Шпионское ПО. Это вредоносные программы, которые отслеживают и собирают ценные данные о пользователе или предприятии и отправляет их злоумышленникам.

- Трояны. Разновидность вредоносной программы, проникающей в компьютер под видом легитимного программного обеспечения.
- Загрузчики. Это вредоносный код, цель которого соединиться с удалённым сервером злоумышленника и начать загрузку, а потом и установку вредоносной программы.
- Рекламное ПО. Это программы, которые отображают рекламу на экране компьютера или смартфона в виде всплывающих окон на рабочем столе или на веб-сайтах.
- Боты. Это программы, цель которых выполнять определённые операции в автоматическом режиме.
- Майнеры. Это вредоносная программа, основной целью которой является добыча криптовалюты с использованием ресурсов компьютера жертвы.

Для защиты от вредоносных программ рекомендуют:

- Регулярно обновлять операционную систему. Новые версии ПО содержат исправления для уязвимостей, через которые хакеры могут проникнуть в систему.
- Использовать антивирусные программы. Они сканируют систему на наличие потенциальных угроз, устраняют их и предотвращают повторное появление.
- Быть осторожным при открытии подозрительных ссылок на электронной почте, скачивании файлов, посещении веб-сайтов сомнительного происхождения. Избегать скачивания файлов из непроверенных источников.
- Использовать сложные пароли. Рекомендуется создавать пароли, содержащие буквы, цифры и специальные символы, а также регулярно их изменять.
- Включить брандмауэр. Он поможет защитить компьютер от несанкционированного доступа и сетевых атак.
- Работать под правами пользователя, а не администратора, чтобы ограничить возможность вирусам повредить систему.
- Регулярно проводить резервное копирование данных. Это позволит восстановить информацию в случае атаки.

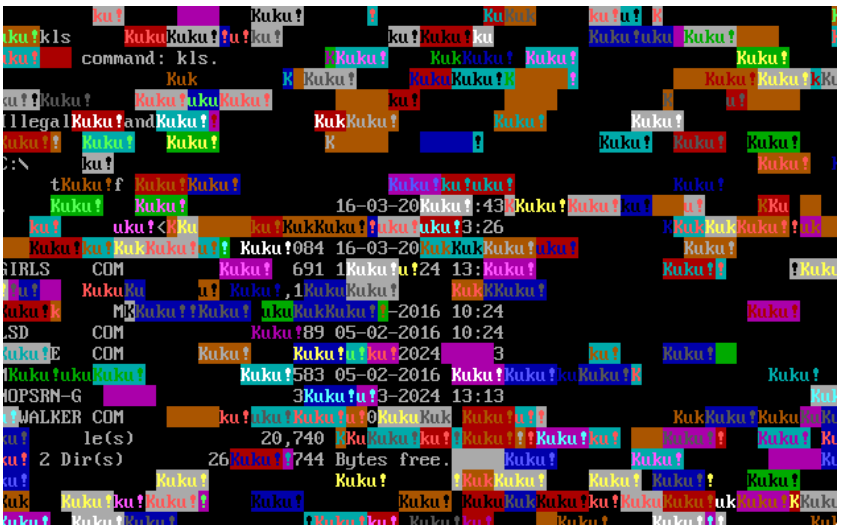

Рис. 1: Вирус

Пример вируса Kuku, источник https://ru.wikipedia.org/

Мониторинг безопасности

Мониторинг системы позволяет выявлять подозрительную активность и реагировать на инциденты безопасности.

Основные виды:

- Внутренний. Проверка инфраструктуры компании для выявления уязвимостей, которые могут привести к утечке данных и серьёзным сбоям в работе.
- Внешний. Оценка устойчивости системы к кибератакам и соответствия её решаемым задачам.
- Реактивный. Оперативный мониторинг, который предполагает реагирование на проблемы или инциденты после их возникновения. Цель — своевременно выявить и устранить неполадки.
- Мониторинг журнала. Включает анализ системных журналов для понимания поведения системы и выявления проблем. Цель — отслеживать действия, устранять неполадки и поддерживать соответствие требованиям безопасности.
- SIEM-системы. Комплексные системы, которые собирают и анализируют данные из различных источников. Они помогают обнаруживать и реагировать на угрозы в режиме реального времени.
- IDS/IPS-системы. Анализируют сетевой трафик и выявляют подозрительные активности. IDS (Intrusion Detection System) обнаруживает угрозы, а IPS (Intrusion Prevention System) не только обнаруживает, но и блокирует их.

Некоторые задачи мониторинга безопасности:

- Выявление угроз и аномалий. Анализ сетевой активности, логов и системных событий позволяет обнаруживать подозрительное поведение.
- Уведомление о событиях. Системы мониторинга генерируют оповещения при обнаружении инцидентов.
- Анализ инцидентов. Помогает выявить причину, масштаб и возможные последствия атаки.
- Отчётность и аудит. Мониторинг позволяет отслеживать соблюдение политик безопасности и подготавливать отчёты для проверок.

Политика безопасности

Политика безопасности — это набор правил и норм, определяющих, каким образом обеспечивается безопасность в организации. В этом документе также описываются основные риски и меры по их предотвращению, выявлению и нейтрализации.

Политика безопасности утверждается руководством организации и доводится до сведения всех её сотрудников, а также всех причастных сторон за пределами организации.

Задачи:

- Защита конфиденциальной информации от несанкционированного доступа, изменения или уничтожения.
- Обеспечение непрерывности работы информационных систем и сервисов компании, даже в случае кибератаки или других инцидентов.
- Соответствие требованиям законодательства в области информационной безопасности и защиты персональных данных.
- Снижение риска финансовых потерь компании из-за нарушения информационной безопасности.
- Улучшение имиджа компании как надёжного партнёра, заботящегося о безопасности данных своих клиентов и партнёров.
- Защита информационных активов компании, в том числе ограничение доступа к данным с помощью физических и технических средств.
- Проведение авторизации и аутентификации пользователей. Цель — проверка личности пользователя, предотвращение несанкционированного доступа к информации, противодействие взлому.

- Поддержание ключевых свойств информации, указывающих на её защищённость: целостности, конфиденциальности, доступности.
- Проверка степени защищённости данных. С помощью аудита и инструментов контроля исполнения политик безопасности данных можно оценить, насколько хорошо защищена информация, какие проблемы присутствуют и требуют устранения.

Как правило, корпоративная политика безопасности включает следующие составляющие:

- Определение, цели и принципы информационной безопасности в организации.
- Нормы и требования по различным направлениям обеспечения безопасности, таким как управление доступами, использование компьютерного оборудования и информационных систем, управление инцидентами безопасности и другие.
- Меры и технологии, применяемые для соблюдения установленных норм.
- Полномочия и обязанности отделов и служб в сфере безопасности, включая определение персональной ответственности назначенных лиц, а также меры реагирования в отношении пользователей, не соблюдающих или не имеющих возможности соблюдать требования политики безопасности.
- Положения, касающиеся отклонений и исключений из изложенных правил.

Заключение

Методы организации безопасности в операционных системах являются многоуровневыми и требуют комплексного подхода. Аутентификация, шифрование, защита от вредоносного ПО, мониторинг и аудит, а также разработка политик безопасности — все эти элементы играют важную роль в обеспечении защиты информации. В условиях постоянно меняющихся угроз важно постоянно обновлять и адаптировать методы безопасности, чтобы минимизировать риски и защитить данные пользователей и организаций.

Список источников

- https://ru.wikipedia.org/wiki/
- https://www.kaspersky.ru/ ::: {#refs} :::