УДК 377

Автор: Дубаев Исмаил Магомедович

Преподаватель

ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова»

Россия, г. Грозный

Соавтор: Базаева Айна Алиевна

Магистрантка, 2 курс, группа ЗБИН-22М

ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова»

Россия, г. Грозный

АДМИНИСТРИРОВАНИЕ БЕЗОПАСНОСТИ ЛОКАЛЬНЫХ СЕТЕЙ

Аннотация.

Статья посвящена разработке предложений по повышению защищённости информации, циркулирующей в локальных вычислительных сетях. Рассматриваются классификация каналов утечки и угроз безопасности информации, а также существующие способы защиты информации от несанкционированного доступа. Разработан программно-аппаратный комплекс удалённого контроля несанкционированного доступа к автоматизированному рабочему месту. Представлена общая структура предлагаемой системы контроля защиты информации, обрабатываемой в сетевых хранилищах данных от несанкционированного доступа.

Ключевые слова: локальные вычислительные сети, несанкционированный доступ, программно-аппаратный комплекс, сетевые хранилища данных.

Author: Dubaev Ismail Magomedovich

Teacher

Grozny State Petroleum Technical University named after academician M.D. Millionshchikova"

Russia, Grozny

Co-author: Bazaeva Aina Alievna

Undergraduate, 2nd year, ZBIN-22M group

Grozny State Petroleum Technical University named after academician M.D. Millionshchikova"

Russia, Grozny

ADMINISTRATION OF LOCAL AREA NETWORK SECURITY

Annotation.

The article is devoted to the development of proposals to improve the security of information circulating in local area networks. The classification of information leakage channels and threats to information security, as well as existing ways to protect information from unauthorized access, are considered. A software and hardware complex for remote control of unauthorized access to an automated workplace has been developed. The general structure of the proposed control system for the protection of information processed in network data warehouses from unauthorized access is presented.[1]

***Keywords*: local area networks, unauthorized access, hardware and software complex, network data warehouses.**

Локальные вычислительные сети (ЛВС) играют ключевую роль в поддержании потока информации и обеспечении связи в современном мире. Они позволяют пользователям делиться данными, ресурсами, такими как принтеры и файлы, и предоставляют платформу для коллективной работы, что особенно важно в бизнес-средах и образовательных учреждениях.

[1]Рузметов А. А., Рустамов О. А., Худайбегенов Т. А., Хужаев О. К. Администрирование безопасности локальных сетей на примере Ургенческого филиала ТУИТ. Universum: технические науки, 2021.

Преимущества ЛВС включают:

Эффективность общения: Ускоряет процесс обмена информацией между пользователями.

Централизованное управление: Упрощает администрирование сети и управление ресурсами.

Совместное использование ресурсов: Позволяет множеству пользователей использовать общие устройства и приложения.

Гибкость: ЛВС можно масштабировать и адаптировать к изменяющимся потребностям организации.

Безопасность: Возможность внедрения политик безопасности для защиты данных и ресурсов.

Тем не менее, существуют и вызовы, связанные с ЛВС:

Защита данных: Необходимо обеспечить защиту от внешних и внутренних угроз.

Обслуживание: Требуется регулярное техническое обслуживание и обновление оборудования и программного обеспечения.

Масштабируемость: По мере роста организации может потребоваться расширение сетевой инфраструктуры.

ЛВС продолжают развиваться, включая новые технологии, такие как беспроводные сети, облачные вычисления и интернет вещей (IoT), которые дополнительно усиливают их значимость в цифровой эпохе.

В современном мире, где количество и сложность киберугроз постоянно растет, администрирование безопасности локальных сетей становится критически важным аспектом для любой организации. Это не только защищает ценные данные, но и является основой для непрерывной работы бизнеса и сохранения доверия клиентов и партнеров.

Основные аспекты эффективного администрирования безопасности ЛВС включают:

Политики безопасности: Разработка и внедрение строгих политик безопасности, которые регулируют доступ к сети и ее ресурсам.

Физическая безопасность: Защита сетевого оборудования от несанкционированного физического доступа.[2]

Аутентификация и авторизация: Установление надежных методов аутентификации и авторизации пользователей и устройств.

Шифрование: Использование шифрования для защиты данных во время их передачи по сети.

Мониторинг сети: Непрерывный мониторинг сетевой активности для выявления подозрительных действий и потенциальных угроз.

Резервное копирование и восстановление: Регулярное создание резервных копий важных данных и разработка планов восстановления после сбоев.

Обновление и патчинг: Своевременное обновление программного обеспечения и операционных систем для устранения уязвимостей.

Обучение пользователей: Повышение осведомленности сотрудников о киберугрозах и обучение их безопасному поведению в сети.

Эти меры помогают создать многоуровневую систему защиты, которая может эффективно противостоять различным угрозам и обеспечить безопасность цифровых активов организации.

В своем исследовании мы опирались на труды:
Рузметов А. А., Рустамов О. А.,[8], Худайбегенов Т. А., Хужаев О. К.[12], Шаньгин В. Ф. [29], МуравьеваН.В. [10], Соколов А. В., Кудаева, М.М. [17], Зима В., [22].

Локальные сети сталкиваются со сложным и постоянно меняющимся ландшафтом угроз, требующим многогранного подхода к безопасности. Несанкционированный доступ остается постоянной проблемой, поскольку злоумышленники используют разнообразный арсенал методов для взлома

[2]Шаньгин В. Ф. Комплексная защита информации в корпоративных системах. Москва: ИД «ФОРУМ», ИНФРА-М, 2021.

периметра сети. Атаки с использованием грубой силы используют автоматизированные инструменты для взлома слабых учетных данных, в то время как мошенничество в области социальной инженерии использует человеческие уязвимости, чтобы обманом заставить пользователей раскрыть конфиденциальную информацию или перейти по вредоносным ссылкам. Искушенные злоумышленники также используют неисправленные уязвимости программного обеспечения, чтобы закрепиться в сети.

Вредоносное ПО, включая вирусы, черви и программы-вымогатели, представляет собой серьезную угрозу. Эти вредоносные программы могут быстро распространяться по сети, заражая устройства, повреждая данные и нарушая работу критически важных систем. Атаки программ-вымогателей, в частности, могут быть особенно разрушительными: они шифруют важные файлы и требуют непомерных выкупов за их расшифровку. Внутренние угрозы добавляют еще один уровень сложности. Недовольные сотрудники, халатные люди или лица с скомпрометированными учетными данными могут нанести значительный ущерб из-за присущих им привилегий доступа и знания внутренних систем. Кроме того, такие методы, как подслушивание и атаки «человек посередине» (MitM), могут поставить под угрозу конфиденциальность передачи конфиденциальных данных, позволяя злоумышленникам перехватывать и красть ценную информацию.

Для усиления защиты локальной сети необходим многоуровневый подход к безопасности, учитывающий различные принципы безопасности.

Внедрение надежного контроля доступа является краеугольным камнем безопасности локальной сети. Принцип минимальных привилегий требует, чтобы учетным записям пользователей предоставлялись только минимальные разрешения, необходимые для выполнения назначенных им задач. Многофакторная аутентификация (MFA) добавляет дополнительный уровень безопасности, требуя вторичного фактора проверки помимо простого имени пользователя и пароля. Этот дополнительный шаг значительно усложняет доступ к сети неавторизованным лицам, даже если они получат учетные данные

пользователя. Ограничение несанкционированного физического доступа к сетевым устройствам и реализация сегментации сети — процесса разделения сети на более мелкие изолированные сегменты — еще больше ограничивают [3]потенциальные возможности атак, ограничивая зону действия злоумышленников, если они проникают в определенный сегмент.

Системы обнаружения и предотвращения вторжений (IDS/IPS) действительно являются важными компонентами в стратегии безопасности сети. Они работают, отслеживая сетевой трафик и анализируя его на предмет признаков известных атак или аномального поведения, которое может указывать на новые или неизвестные угрозы.

IDS (Системы обнаружения вторжений) обычно выполняют следующие функции:

Мониторинг трафика: Анализируют сетевой трафик в реальном времени.

Анализ событий: Сравнивают данные сетевого трафика с базой данных известных угроз.

Генерация предупреждений: Оповещают администраторов о потенциальных вторжениях.

IPS (Системы предотвращения вторжений), помимо обнаружения, также могут:

Блокировать трафик: Автоматически блокируют подозрительный трафик.

Исправление уязвимостей: Предотвращают эксплуатацию известных уязвимостей.

Адаптация: Обновляются для распознавания новых угроз.

Эти системы помогают обеспечить, что сеть защищена от различных видов кибератак, включая вирусы, черви, троянские программы, и могут быть настроены для предотвращения более сложных атак, таких как DDoS (распределенные отказы в обслуживании) или APT (продвинутые постоянные

[3]Основы информационной безопасности. Часть 1: Виды угроз. URL: https://habr.com/ru/ (дата обращения: 07.05.2023).

угрозы). Регулярное обновление операционных систем, приложений и встроенного программного обеспечения (ПО) на сетевых устройствах является одним из ключевых элементов стратегии кибербезопасности. Это помогает защитить системы от известных уязвимостей, которые могут быть использованы злоумышленниками для проведения атак.

Важность обновлений заключается в следующем:

Устранение уязвимостей: Обновления часто содержат патчи для уязвимостей, которые были обнаружены после выпуска предыдущей версии ПО.

Повышение стабильности: Обновления могут улучшать стабильность системы, исправляя ошибки, которые могут привести к сбоям.

Новые функции: Обновления могут включать новые функции или улучшения существующих, что может улучшить общую эффективность и удобство использования.

Соответствие стандартам: Со временем могут меняться стандарты безопасности, и обновления помогают соответствовать этим изменениям.

Для обеспечения безопасности и эффективности процесса обновления важно:

Автоматизировать процесс: Настроить автоматические обновления, где это возможно, чтобы гарантировать, что ПО всегда актуально.

Тестирование перед развертыванием: Проводить тестирование обновлений в контролируемой среде перед их развертыванием на рабочих системах.

Резервное копирование: Создавать резервные копии систем перед применением обновлений на случай, если возникнут проблемы.

Мониторинг после обновления: Отслеживать системы после обновления на предмет любых непредвиденных проблем.

Конфиденциальные данные при хранении и передаче требуют надежной защиты. Шифрование данных защищает информацию, даже если она будет перехвачена неавторизованными лицами. Шифрование делает данные нечитаемыми без соответствующего ключа дешифрования, что делает их

бесполезными для злоумышленников. Регулярное резервное копирование данных гарантирует возможность восстановления важной информации в случае кибератаки или сбоя системы. Комплексная стратегия резервного копирования [4]обычно включает репликацию данных в безопасное удаленное место, чтобы минимизировать риск потери данных в результате атак программ-вымогателей или физических катастроф.

Обучение пользователей передовым методам кибербезопасности играет жизненно важную роль в укреплении безопасности вашей сети. Программы обучения по вопросам безопасности должны вооружать пользователей знаниями и навыками, позволяющими выявлять попытки фишинга, соблюдать правила гигиены паролей и сообщать о подозрительной активности.

Передовые методы контроля доступа:

Управление доступом на основе ролей (RBAC): этот подход назначает разрешения на основе заранее определенных ролей в организации. Например, пользователь отдела маркетинга может иметь другие права доступа по сравнению с ИТ-администратором.

Управление идентификацией и доступом (IAM): IAM выходит за рамки простого контроля доступа, управляя всем жизненным циклом пользователя, включая предоставление, контроль доступа и удаление учетных записей пользователей. Такой централизованный подход упрощает управление доступом и повышает безопасность.

Безопасность порта 802.1X. Этот протокол обеспечивает аутентификацию проводных сетевых устройств перед тем, как им будет предоставлен доступ к сети. Только авторизованные устройства с правильными учетными данными могут подключаться к определенным сетевым портам.

Устройства сетевой безопасности в действии:

[4]Учёный XXI века. Издание 3–2 (16) марта 2016 г. UDC 004.414.22 «Administration of complex methods of security of a LAN on the example of the Urgench branch of TUIT», T. A. Khudayberganov.
Соколов А. В., Shangin V. F. Information security in the distributed corporate networks and systems. DMK the Press, 2022.

Брандмауэры. Современные брандмауэры предлагают расширенные функции, такие как глубокая проверка пакетов, которая анализирует содержимое пакетов данных для выявления вредоносных программ или другого вредоносного контента. Их также можно настроить для реализации фильтрации на уровне приложений, ограничивая доступ к определенным приложениям или веб-сайтам.

Системы обнаружения и предотвращения вторжений (IDS/IPS). Эти системы можно настроить не только на обнаружение подозрительной активности, но и на автоматическое выполнение действий по снижению угроз. Например, IPS может автоматически блокировать вредоносный IP адрес, пытающийся воспользоваться уязвимостью сетевого устройства.

Инструменты сканирования уязвимостей существуют в различных формах, некоторые из которых ориентированы на конкретные типы уязвимостей или сетевых устройств. Группы безопасности могут расставлять приоритеты в исправлениях, исходя из серьезности уязвимости, потенциального воздействия на критические системы и простоты эксплуатации.

Инструменты управления исправлениями могут автоматизировать развертывание исправлений безопасности по сети, обеспечивая своевременные обновления и минимизируя окно уязвимости.

Тестирование на проникновение включает в себя моделирование кибератаки для выявления уязвимостей, которые могут пропустить автоматические сканеры. Такой упреждающий подход помогает

организациям обнаруживать потенциальные слабые места в своей защите до того, как ими воспользуются злоумышленники.[5]

Разработка схемы программно-аппаратного комплекса для удалённого контроля несанкционированного доступа требует тщательного планирования и включает в себя следующие компоненты:

[5]Osterlokh H. TCP/IP. Family of protocols of data transmission in networks of computers. Diasoftyup, 2021.
Зима В., Moldovyan A., Moldovyan N. Security of global network technologies. BHV-St. Petersburg, 2021.

Устройства захвата данных: К ним относятся камеры, датчики движения и другие сенсоры, которые могут обнаруживать физическое присутствие возле рабочего места.

Сетевые компоненты: Включают в себя маршрутизаторы, коммутаторы и брандмауэры для защиты данных и управления трафиком.

Серверы и хранилища данных: Обеспечивают централизованное хранение и обработку данных с устройств захвата и сетевых компонентов.

Программное обеспечение для анализа данных: Включает в себя системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), а также программное обеспечение для анализа поведения пользователей.

Интерфейс пользователя: Панель управления для мониторинга системы и реагирования на инциденты.

Механизмы шифрования: Для защиты передаваемых данных между компонентами системы.

Протоколы аутентификации и авторизации: Для контроля доступа к системе и её компонентам.

Использованные источники:

1.Рузметов А. А., Рустамов О. А., Худайбегенов Т. А., Хужаев О. К. Администрирование безопасности локальных сетей на примере Ургенческого филиала ТУИТ. Universum: технические науки, 2021.
2.Шаньгин В. Ф. Комплексная защита информации в корпоративных системах. Москва: ИД «ФОРУМ», ИНФРА-М, 2021.
3.Основы информационной безопасности. Часть 1: Виды угроз. URL: https://habr.com/ru/ (дата обращения: 07.05.2023).
4.Учёный XXI века. Издание 3–2 (16) марта 2016 г. UDC 004.414.22 «Administration of complex methods of security of a LAN on the example of the Urgench branch of TUIT», T. A. Khudayberganov.
5.Соколов А. В., Shangin V. F. Information security in the distributed corporate networks and systems. DMK the Press, 2022.
6.Osterlokh H. TCP/IP. Family of protocols of data transmission in networks of computers. Diasoftyup, 2021.
7.Зима В., Moldovyan A., Moldovyan N. Security of global network technologies. BHV-St. Petersburg, 2021.