Министерство образования Республики Беларусь
Учреждение образования
«Брестский государственный технический университет»
Кафедра интеллектуальных информационных технологий

РЕФЕРАТ

По дисциплине

«Современные методы защиты компьютерных систем»

Выполнил:
Студент 4 курса
Группы ИИ-21
Корнейчук А.И.

Брест 2024

1. **SSOC: Single Sign-On with Context**

   В современном цифровом мире, где большое количество приложений и сервисов требует безопасной аутентификации, концепция Single Sign-On (SSO) играет важную роль. SSOC (Single Sign-On with Context) представляет собой усовершенствованный подход к технологии SSO, который добавляет контекстуальные элементы для повышения уровня безопасности и удобства пользователей.

   Основные принципы работы SSOC

   SSOC позволяет пользователю получить доступ ко всем связанным системам и приложениям с помощью одной пары аутентификационных данных (логина и пароля). Однако, в отличие от традиционного SSO, SSOC учитывает дополнительные параметры для аутентификации, такие как:

   - Геолокация пользователя;
   - Тип и состояние устройства, с которого осуществляется вход;
   - Время доступа;
   - Поведенческие факторы, например скорость набора текста.

   Эти дополнительные параметры формируют "контекст" пользователя, который помогает системе принимать решения о предоставлении или ограничении доступа. Например, если пользователь пытается войти в систему с нового устройства или из необычного местоположения, система может запросить дополнительную проверку (например, одноразовый пароль).

   Роль криптографии в SSOC

   Криптографические методы занимают центральное место в реализации SSOC, обеспечивая конфиденциальность и защиту данных. Основные аспекты криптографической защиты в SSOC включают:

   - **Шифрование данных:** Все данные, передаваемые между клиентом и сервером, шифруются с использованием протоколов TLS (Transport Layer Security);
   - **Электронные подписи:** Используются для проверки подлинности данных и предотвращения их модификации;
   - **Хранение аутентификационных данных:** Пароли и токены хранятся в зашифрованном виде, что предотвращает их утечку.

   Протоколы, такие как OAuth 2.0 и OpenID Connect, активно применяются в SSOC-системах, обеспечивая безопасную передачу токенов доступа.

   Преимущества использования SSOC

   1. **Увеличение уровня безопасности.** Контекстуальная аутентификация снижает риск несанкционированного доступа, так как для завершения входа могут потребоваться дополнительные факторы.
   2. **Удобство для пользователей.** Один вход в систему устраняет необходимость запоминать множество паролей.
   3. **Снижение нагрузки на администраторов.** Автоматическое управление доступом упрощает администрирование и мониторинг.
   4. **Гибкость настройки.** Возможность учитывать множество параметров для аутентификации позволяет настроить систему под конкретные требования компании.

   Уязвимости и вызовы

   Несмотря на все преимущества, SSOC имеет свои риски:

   - **Атаки на токены доступа.** Если токен украден, злоумышленник может получить доступ к системам;
   - **Фишинг.** Мошенники могут попытаться обманом заставить пользователя предоставить свои данные;

- **Сложность внедрения.** Настройка контекстуальных факторов требует больших ресурсов и опыта.

Для минимизации этих рисков важно применять современные методы защиты, такие как многофакторная аутентификация (MFA), регулярные обновления систем безопасности и обучение пользователей основам кибербезопасности.

Заключение

SSOC представляет собой значительный шаг вперёд в области аутентификации, объединяя удобство Single Sign-On и высокую степень защиты благодаря учёту контекста. Внедрение этой технологии позволяет компаниям не только улучшить пользовательский опыт, но и существенно снизить риски, связанные с угрозами кибербезопасности. Однако для достижения максимального эффекта требуется тщательное проектирование и соблюдение лучших практик в области криптографической защиты.

2. **FW и NGFW: Основы и отличия**

Сетевые брандмауэры (Firewall, FW) и их усовершенствованные версии, межсетевые экраны нового поколения (Next-Generation Firewall, NGFW), являются ключевыми элементами обеспечения информационной безопасности. Эти технологии обеспечивают защиту от несанкционированного доступа, предотвращают атаки и фильтруют сетевой трафик.

Основы работы Firewall (FW)

Firewall — это система, которая контролирует входящий и исходящий трафик в сети на основе заданных правил. Основные функции FW:

- **Фильтрация пакетов:** Анализ каждого сетевого пакета на предмет соответствия заданным правилам;
- **Контроль доступа:** Ограничение или разрешение соединений на основе IP-адресов, портов и протоколов;
- **Сетевой адресный перевод (NAT):** Маскировка внутренних IP-адресов для повышения безопасности.

Типичные FW работают на уровне сетевой модели OSI (уровни 3 и 4), анализируя заголовки пакетов без глубокого изучения их содержимого.

NGFW: Межсетевые экраны нового поколения

NGFW значительно расширяют функциональность традиционных FW, интегрируя современные технологии защиты. Основные отличия и возможности NGFW:

1. **Глубокий анализ пакетов (DPI):** NGFW исследует содержимое пакетов, а не только заголовки, что позволяет обнаруживать сложные угрозы, такие как вредоносный код и скрытые атаки.
2. **Идентификация приложений:** Вместо контроля только портов и протоколов NGFW анализирует поведение приложений, что помогает различать легитимный и вредоносный трафик.
3. **Интеграция IPS:** Встроенная система предотвращения вторжений (Intrusion Prevention System, IPS) позволяет NGFW блокировать известные уязвимости и атаки в реальном времени.
4. **Контроль пользователей:** NGFW используют механизмы аутентификации для управления доступом на уровне пользователей и групп.

5. **Шифрование и деформация трафика:** NGFW способны анализировать зашифрованный трафик с использованием SSL/TLS-декрипции.

Преимущества NGFW

- **Улучшенная защита от современных угроз.** NGFW защищает от атак типа APT (Advanced Persistent Threats) и Zero-Day.
- **Объединение функций.** NGFW совмещает возможности FW, IPS и других решений в одном устройстве.
- **Повышенная производительность.** Благодаря оптимизации процессов NGFW обрабатывает большой объём данных без значительного влияния на производительность сети.

Примеры использования FW и NGFW

1. **Малый бизнес.** Firewall обеспечивает базовую защиту сети от внешних атак и фильтрацию трафика.
2. **Крупные предприятия.** NGFW используется для глубокого анализа трафика, предотвращения сложных атак и централизованного управления безопасностью.
3. **Облачные среды.** NGFW поддерживают защиту виртуальных и облачных инфраструктур, включая гибридные решения.

Ограничения и вызовы

- **Стоимость.** NGFW дороже традиционных FW как в плане начальной покупки, так и обслуживания.
- **Сложность настройки.** Установка и управление NGFW требуют высокой квалификации специалистов.
- **Обработка шифрованного трафика.** Анализ зашифрованных данных может снижать производительность.

3. IDS/IPS: Системы обнаружения и предотвращения вторжений

Системы IDS (Intrusion Detection System) и IPS (Intrusion Prevention System) являются важными компонентами обеспечения информационной безопасности, позволяя выявлять и предотвращать угрозы в компьютерных сетях. Они работают в тандеме, обеспечивая защиту от сетевых атак, вредоносной активности и несанкционированного доступа.

IDS: Система обнаружения вторжений

IDS — это технология, которая мониторит сетевой трафик и анализирует его с целью обнаружения подозрительных или вредоносных действий. Основные функции IDS:

- **Пассивное выявление угроз:** IDS фиксирует потенциально опасные события и уведомляет администратора системы;
- **Анализ на основе сигнатур:** Сравнение трафика с базой данных известных угроз (сигнатур);
- **Аномальный анализ:** Обнаружение нетипичного поведения в сети на основе заранее заданных шаблонов.

IPS: Система предотвращения вторжений

IPS — это активная защита, которая не только выявляет, но и блокирует вредоносную активность в режиме реального времени. Основные функции IPS:

- **Блокировка угроз:** Автоматическое предотвращение подозрительных действий, таких как блокировка IP-адресов или сброс соединений;
- **Фильтрация трафика:** Анализ и удаление пакетов, содержащих вредоносный код;
- **Реакция на инциденты:** IPS может настраиваться для выполнения специфических действий при обнаружении угрозы.

Основные различия между IDS и IPS

- **Действия:** IDS обнаруживает угрозы и уведомляет администратора, в то время как IPS принимает меры для их предотвращения.
- **Размещение в сети:** IDS работает параллельно с сетевым трафиком, не вмешиваясь в его передачу, а IPS устанавливается "инлайн" и активно фильтрует трафик.
- **Цель использования:** IDS фокусируется на мониторинге и сборе информации, IPS направлена на немедленное реагирование.

Преимущества и недостатки IDS и IPS

IDS:

- Преимущества:
  - Глубокий анализ сетевого трафика;
  - Уведомления о возможных угрозах для дальнейшего изучения.
- Недостатки:
  - Не предотвращает угрозы самостоятельно;
  - Возможны ложные срабатывания.

IPS:

- Преимущества:
  - Активная защита сети;
  - Уменьшение риска успешных атак.
- Недостатки:
  - Требует мощных ресурсов для обработки трафика;
  - Возможны ошибки, приводящие к блокировке легитимного трафика.

Примеры использования IDS и IPS

1. **Обнаружение и предотвращение атак:** IDS может фиксировать сканирование портов, а IPS — блокировать попытки эксплуатации уязвимостей.
2. **Защита от DDoS:** IPS способен ограничивать вредоносный трафик в случае распределённой атаки.
3. **Анализ и реагирование:** IDS позволяет создавать отчёты для последующего анализа, IPS обеспечивает автоматическое реагирование.

4. NTA: Анализ сетевого трафика

Network Traffic Analysis (NTA) — это процесс мониторинга и анализа сетевого трафика для выявления угроз, аномалий и несанкционированной активности. Эта технология помогает обеспечить безопасность сети, предоставляя детальную информацию о её состоянии и активности.

Что такое NTA?

NTA представляет собой методику, которая фокусируется на сборе и анализе данных сетевого трафика. **Основная цель NTA** — обнаружение подозрительных действий и обеспечение видимости сетевых процессов. Примеры данных, анализируемых в рамках NTA:

- Источники и получатели трафика;
- Объёмы передаваемых данных;
- Используемые протоколы и порты;
- События и временные метки сетевой активности.

Основные возможности NTA

1. **Обнаружение угроз:** NTA выявляет аномалии, которые могут свидетельствовать о вредоносной активности, включая атаки Zero-Day и скрытые угрозы.
2. **Мониторинг трафика в реальном времени:** Технология позволяет отслеживать сетевые соединения в текущий момент, предоставляя данные для немедленного реагирования.
3. **Анализ поведения:** На основе шаблонов поведения NTA идентифицирует отклонения от нормы, что может указывать на кибератаки или утечки данных.
4. **Поддержка зашифрованного трафика:** Современные системы NTA могут анализировать зашифрованный трафик без его расшифровки, используя метаданные.

Как работает NTA?

1. **Сбор данных:** Инструменты NTA собирают данные из различных источников, включая сетевые устройства (маршрутизаторы, коммутаторы) и сетевые зеркала (SPAN или TAP).
2. **Обработка данных:** Полученные данные проходят обработку, где фильтруются и структурируются для дальнейшего анализа.
3. **Анализ и выявление угроз:** Используются методы машинного обучения и поведенческой аналитики для обнаружения подозрительных паттернов в сетевом трафике.
4. **Уведомления и отчёты:** При обнаружении угроз система генерирует уведомления и предоставляет отчёты для дальнейших действий.

Преимущества NTA

- **Глубокая видимость сети:** NTA предоставляет полное представление о движении данных в сети, включая скрытые сегменты.
- **Обнаружение сложных атак:** Технология помогает выявлять угрозы, которые сложно обнаружить традиционными методами, такими как IDS/IPS.
- **Интеграция с SIEM:** Данные из NTA могут использоваться для централизованного анализа и корреляции событий.
- **Поддержка гибридных сред**: NTA адаптируется для работы как в локальных, так и в облачных инфраструктурах.

Ограничения NTA

- **Большие объёмы данных:** Анализ трафика в масштабных сетях требует значительных вычислительных ресурсов.
- **Сложность настройки:** Эффективность NTA зависит от правильной конфигурации системы и точной настройки аналитических правил.
- **Ложные срабатывания:** Возможны ситуации, когда система идентифицирует нормальный трафик как потенциальную угрозу.

Примеры применения NTA

1. **Выявление утечек данных:** Анализ аномалий помогает обнаруживать попытки передачи конфиденциальной информации за пределы сети.
2. **Противодействие скрытым атакам:** NTA идентифицирует вредоносную активность, маскирующуюся под легитимный трафик.
3. **Мониторинг IoT-устройств:** Технология используется для отслеживания активности устройств интернета вещей, защищая их от взлома.