Троян И.В. Эффективные методы разбиения и изоляции метаданных для повышения безопасности// Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 1(51) с. 172–175

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.736

ЭФФЕКТИВНЫЕ МЕТОДЫ РАЗБИЕНИЯ И ИЗОЛЯЦИИ МЕТАДАННЫХ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ

Троян И.В.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: it.bonch@gmail.com

Метаданные часто являются ценным источником информации для злоумышленников, поскольку они могут содержать ключевую информацию о пользователях, приложениях и системах. Статья описывает подходы к разбиению и изоляции метаданных, такие как минимизация их сбора, применение принципа наименьших привилегий и использование специальных хранилищ для предотвращения несанкционированного доступа. Эти методы помогают значительно повысить уровень безопасности данных и защитить конфиденциальную информацию.

Ключевые слова: Метаданные, разбиение, изоляция, безопасность данных, принцип наименьших привилегий, защита информации, хранилище метаданных.

EFFECTIVE METHODS FOR PARTITIONING AND ISOLATING METADATA TO ENHANCE SECURITY

Troyan I.V.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: it.bonch@gmail.com

Metadata is often a valuable information source for attackers, as it can contain critical insights about users, applications, and systems. This article outlines approaches to partitioning and isolating metadata, such as minimizing its collection, applying the principle of least privilege, and using dedicated storage solutions to prevent unauthorized access. These methods significantly improve data security and safeguard sensitive information.

Keywords: Metadata, partitioning, isolation, data security, principle of least privilege, information protection, metadata storage.

Введение

Метаданные, представляющие собой данные о данных, играют важную роль в современных системах. Они содержат информацию о структурах баз данных, логах событий, сессиях пользователей и многом другом. Несмотря на их полезность, метаданные представляют значительный риск для безопасности. Злоумышленники часто используют их для анализа инфраструктуры, выявления уязвимых мест и выполнения целенаправленных атак. Например, метаданные логов могут содержать ключевую информацию о работе приложений или сети, включая IP-адреса, идентификаторы пользователей и временные метки.

В условиях увеличивающегося числа атак, связанных с утечкой данных, важно разработать и внедрить стратегии по защите метаданных. Одним из наиболее эффективных

методов является разбиение и изоляция метаданных. Это подразумевает их разделение на независимые сегменты с ограничением доступа к каждому из них, а также изоляцию в специализированных хранилищах. Подход позволяет минимизировать ущерб в случае успешной атаки и снизить вероятность компрометации всей системы.

Эффективные методы разбиения и изоляции метаданных для повышения безопасности

Разбиение и изоляция метаданных — это фундаментальные методы, направленные на минимизацию рисков, связанных с их утечкой или несанкционированным доступом. Первый шаг в этом процессе — минимизация объёма собираемых метаданных. Организации часто собирают больше информации, чем необходимо для выполнения бизнес-задач, что увеличивает риск её компрометации. Например, в логах веб-приложений могут сохраняться конфиденциальные данные пользователей, которые не требуются для мониторинга или отладки. Оптимизация процессов сбора данных, включая использование инструментов фильтрации и маскирования, помогает исключить хранение избыточной информации[1].

Далее, метаданные должны быть разделены на логически независимые сегменты. Например, данные о пользователях и данные об их активности в системе могут храниться в разных хранилищах, чтобы ограничить последствия в случае утечки. Разделение данных также должно учитывать их уровень критичности. Высокочувствительные данные, такие как персональные данные или информация о платежах, должны быть строго отделены от менее критичных данных. Это позволяет применить к различным сегментам разные уровни защиты, включая использование более сложных механизмов шифрования и усиленных политик доступа для особо важных данных[2].

Изоляция метаданных предполагает использование физических или логических методов защиты. Например, критически важные метаданные могут храниться в изолированных сегментах облачной инфраструктуры, доступ к которым осуществляется через строго контролируемые API-интерфейсы. Локальные хранилища метаданных могут быть защищены дополнительными уровнями аутентификации и авторизации. Применение технологии виртуализации также может быть эффективным решением: виртуальные машины или контейнеры могут использоваться для хранения и обработки метаданных, обеспечивая их логическую изоляцию[3].

Ещё одним важным аспектом является управление доступом к метаданным. Принцип наименьших привилегий (Least Privilege) требует, чтобы пользователи и приложения имели доступ только к тем данным, которые необходимы для выполнения их задач. Например, разработчики могут иметь доступ к логам только тех компонентов системы, которые они поддерживают, в то время как доступ к логам всего приложения может быть ограничен только для системных администраторов[4].

Для повышения безопасности также рекомендуется использовать механизмы шифрования. Даже если злоумышленник получит доступ к метаданным, их зашифрованное состояние затруднит их использование. Современные методы шифрования, такие как AES или RSA, могут быть интегрированы в процесс хранения и передачи метаданных, обеспечивая их защиту на всех этапах жизненного цикла.

Важным элементом является аудит и мониторинг доступа к метаданным. Логирование всех операций, связанных с чтением, изменением или удалением метаданных, позволяет

выявить подозрительные активности и своевременно реагировать на инциденты. Инструменты анализа логов с применением технологий машинного обучения могут помочь обнаруживать аномалии и предотвращать угрозы[5].

Наконец, сегментация сети, в которой работают приложения, использующие метаданные, также играет важную роль. Изоляция сетевых сегментов позволяет предотвратить распространение угроз в случае успешной атаки. Например, если злоумышленник получит доступ к одному сегменту, строгая сегментация ограничит его возможность проникнуть в другие части системы.

Заключение

Эффективные методы разбиения и изоляции метаданных являются важной частью современной стратегии обеспечения безопасности. В условиях увеличивающегося числа кибератак, направленных на компрометацию данных, эти подходы позволяют минимизировать потенциальные риски и обеспечить защиту конфиденциальной информации.

Разделение данных на логически независимые сегменты, их изоляция в специализированных хранилищах, шифрование и строгий контроль доступа помогают снизить вероятность утечек и защитить критически важные ресурсы. Применение принципа наименьших привилегий и использование сегментации сети дополняют комплексный подход к защите метаданных.

Организации, стремящиеся повысить уровень безопасности своих систем, должны интегрировать описанные методы в свои стратегии защиты данных. Это не только укрепит их защиту от киберугроз, но и поможет обеспечить соблюдение регуляторных требований и защиту репутации.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей. – 2018.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks. – 2018.

2. Minyaev A. A. Method for evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
3. Lesnova E. M., Pestov I. E. Development of a method of error detection and correction for a distributed information network based on big data //Regional informatics and information security. – 2018. – pp. 236-240.
4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
5. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Actual problems of infotelecommunications in science and education. - 2021. – pp. 409-414.