Научная статья
Original article
УДК 004.424

БЕЗОПАСНОСТЬ БАЗЫ ДАННЫХ

DATABASE SECURITY

Казарян Каторина Камоевна студент специалитета, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kazaryan_katorina@mail.ru

Kazaryan Katorina Kamoevna specialty student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kazaryan_katorina@mail.ru

Аннотация: Безопасность баз данных включает ряд мер, используемых для защиты систем управления базами данных от злонамеренных кибератак и незаконного использования. Программы безопасности баз данных предназначены для защиты не только данных в базе данных, но и самой системы управления данными и каждого приложения, которое обращается к ней, от неправильного использования, повреждения и вторжения. Цель работы: организация безопасности баз данных

Abstract. Database security includes a number of measures used to protect database management systems from malicious cyber attacks and illegal use. Database security software is designed to protect not only the data in the database, but also the data management system itself and every application that accesses it from misuse, damage, and intrusion.

Ключевые слова: кибератака, базы данных, безопасность баз данных

Keywords. cyberattack, databases, database security

Безопасность базы данных включает инструменты, процессы и методологии, которые обеспечивают безопасность в среде базы данных.

Угрозы безопасности базы данных

Многие уязвимости программного обеспечения , неправильная конфигурация или схемы неправильного использования или небрежности могут привести к нарушениям. Вот ряд наиболее известных причин и типов киберугроз безопасности баз данных .

Внутренние угрозы

Внутренняя угроза - это угроза безопасности из одного из следующих трех источников, каждый из которых имеет привилегированные средства доступа к базе данных:

- Злонамеренный инсайдер со злым умыслом
- Неосторожный человек в организации, который подвергает базу данных атаке из-за неосторожных действий.
- Посторонний, который получает учетные данные с помощью социальной инженерии или других методов или получает доступ к учетным данным базы данных.

Внутренняя угроза - одна из наиболее типичных причин нарушений безопасности базы данных, и она часто возникает из-за того, что многим сотрудникам предоставлен привилегированный доступ.

Человеческая ошибка

Слабые пароли, совместное использование паролей, случайное стирание или повреждение данных и другое нежелательное поведение пользователей по-прежнему являются причиной почти половины зарегистрированных утечек данных .

Использование уязвимостей программного обеспечения баз данных

Злоумышленники постоянно пытаются изолировать и нацелить уязвимости в программном обеспечении, а программное обеспечение для

управления базами данных является очень ценной целью. Новые уязвимости обнаруживаются ежедневно, и все платформы управления базами данных с открытым исходным кодом и поставщики коммерческого программного обеспечения для баз данных регулярно выпускают исправления безопасности. Однако, если вы не используете эти исправления быстро, ваша база данных может подвергнуться атаке.

Даже если вы вовремя примените исправления, всегда существует риск атак нулевого дня , когда злоумышленники обнаруживают уязвимость, но она еще не была обнаружена и исправлена поставщиком базы данных.

Атаки внедрения SQL / NoSQL

Угроза, специфичная для базы данных, заключается в использовании в запросах к базе данных произвольных строк атаки, отличных от SQL и SQL. Обычно это запросы, созданные как расширение форм веб-приложений или полученные через HTTP-запросы. Любая система баз данных уязвима для этих атак, если разработчики не придерживаются методов безопасного кодирования и если организация не проводит регулярное тестирование уязвимостей.

Атаки переполнения буфера

Переполнение буфера происходит, когда процесс пытается записать большой объем данных в блок памяти фиксированной длины, превышающий допустимый размер. Злоумышленники могут использовать избыточные данные, хранящиеся в соседних адресах памяти, в качестве отправной точки для запуска атак.

Отказ в обслуживании (DoS / DDoS) атаки

При атаке типа «отказ в обслуживании» (DoS) киберпреступник перегружает целевую службу - в данном случае сервер базы данных - с помощью большого количества поддельных запросов. В результате сервер не может выполнять настоящие запросы от реальных пользователей и часто дает сбой или становится нестабильным.

При распределенной атаке типа «отказ в обслуживании» (DDoS) фальшивый трафик генерируется большим количеством компьютеров, участвующих в ботнете, контролируемом злоумышленником. Это создает очень большие объемы трафика, который трудно остановить без хорошо масштабируемой защитной архитектуры. Облачные службы защиты от DDoS - атак могут динамически масштабироваться для защиты от очень крупных DDoS-атак .

Вредоносное ПО

Вредоносное ПО - это программное обеспечение, предназначенное для использования уязвимостей или причинения вреда базе данных. Вредоносное ПО может проникать через любое оконечное устройство, подключенное к сети базы данных. Защита от вредоносных программ важна для любой конечной точки, но особенно на серверах баз данных из-за их высокой ценности и чувствительности.

Развивающаяся ИТ-среда

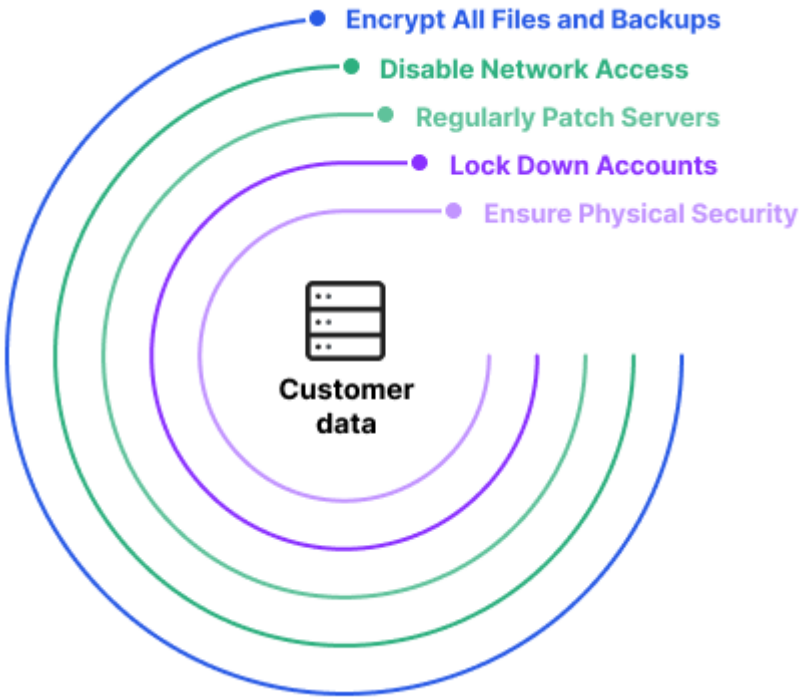
Развитие ИТ-среды делает базы данных более уязвимыми для угроз. Вот тенденции, которые могут привести к новым типам атак на базы данных или могут потребовать новых защитных мер:

- **Растущие объемы данных** - хранение, сбор и обработка данных экспоненциально растут почти во всех организациях. Любые методы или инструменты защиты данных должны обладать высокой степенью масштабируемости, чтобы соответствовать требованиям отдаленного и ближайшего будущего.
- **Распределенная инфраструктура** - сетевые среды становятся все сложнее, особенно по мере того, как предприятия переносят рабочие нагрузки в гибридное облако или мультиоблачные архитектуры, что затрудняет развертывание, управление и выбор решений безопасности.
- **Все более жесткие нормативные требования** - мировая среда соблюдения нормативных требований усложняется, поэтому выполнение всех требований становится все более сложной задачей.

- **Нехватка навыков кибербезопасности** - существует глобальная нехватка квалифицированных профессионалов в области кибербезопасности , и организациям трудно выполнять роли в сфере безопасности. Это может затруднить защиту критически важной инфраструктуры, включая базы данных.

Как вы можете защитить свой сервер базы данных?

Сервер базы данных - это физическая или виртуальная машина, на которой работает база данных. Защита сервера базы данных, также известная как «усиление защиты», - это процесс, который включает в себя физическую безопасность, безопасность сети и безопасную конфигурацию операционной системы.



Обеспечение физической безопасности базы данных

Воздержитесь от совместного использования сервера для веб-приложений и приложений баз данных, если ваша база данных содержит конфиденциальные данные . Хотя было бы дешевле и проще разместить ваш сайт и базу данных вместе у хостинг-провайдера, вы передаете безопасность своих данных в чьи-то руки.

Если вы полагаетесь на службу веб-хостинга для управления своей базой данных, вы должны убедиться, что это компания с надежной репутацией в области безопасности. Лучше держаться подальше от бесплатных услуг хостинга из-за возможного отсутствия безопасности.

Если вы управляете своей базой данных в локальном центре обработки данных, имейте в виду, что ваш центр обработки данных также подвержен атакам со стороны внешних или внутренних угроз. Убедитесь, что у вас есть меры физической безопасности, включая замки, камеры и персонал службы безопасности на вашем физическом объекте. Любой доступ к физическим серверам должен регистрироваться и предоставляться только авторизованным лицам.

Кроме того, не оставляйте резервные копии базы данных в общедоступных местах, таких как временные разделы, веб-папки или незащищенные сегменты облачного хранилища.

Блокировать учетные записи и привилегии

Рассмотрим сервер базы данных Oracle. После установки базы данных помощник по настройке базы данных Oracle (DBCA) автоматически истекает и блокирует большинство учетных записей пользователей базы данных по умолчанию.

Если вы установите базу данных Oracle вручную, этого не произойдет, и привилегированные учетные записи по умолчанию не будут заблокированы или истекли. По умолчанию их пароль остается таким же, как и имя пользователя. Злоумышленник попытается использовать эти учетные данные первыми для подключения к базе данных.

Очень важно убедиться, что каждая привилегированная учетная запись на сервере базы данных настроена с надежным уникальным паролем. Если учетные записи не нужны, срок их действия должен быть истек и заблокирован.

Для остальных учетных записей доступ должен быть ограничен до необходимого минимума. Каждая учетная запись должна иметь доступ только

к таблицам и операциям (например, SELECT или INSERT), которые требуются пользователю. Избегайте создания учетных записей пользователей с доступом к каждой таблице в базе данных.

Регулярно обновляйте серверы баз данных

Убедитесь, что исправления остаются актуальными. Эффективное управление исправлениями базы данных - критически важный метод обеспечения безопасности, поскольку злоумышленники активно ищут новые недостатки безопасности в базах данных, а новые вирусы и вредоносные программы появляются ежедневно.

Своевременное развертывание последних версий пакетов обновления базы данных, критических исправлений безопасности и накопительных обновлений повысит стабильность производительности базы данных.

Отключить доступ к общедоступной сети

Организации хранят свои приложения в базах данных. В большинстве реальных сценариев конечному пользователю не требуется прямой доступ к базе данных. Таким образом, вам следует заблокировать весь доступ к серверам баз данных из общедоступной сети, если вы не являетесь хостинг-провайдером. В идеале организация должна настроить серверы шлюза (туннели VPN или SSH) для удаленных администраторов.

Зашифровать все файлы и резервные копии

Независимо от того, насколько надежна ваша защита, всегда есть вероятность того, что хакер может проникнуть в вашу систему. Однако злоумышленники - не единственная угроза безопасности вашей базы данных. Ваши сотрудники также могут представлять опасность для вашего бизнеса. Всегда существует вероятность того, что злонамеренный или неосторожный инсайдер получит доступ к файлу, к которому у него нет разрешения.

Шифрование ваших данных делает их нечитаемыми как для злоумышленников, так и для сотрудников. Без ключа шифрования они не могут получить к нему доступ, это обеспечивает последнюю линию защиты от

нежелательных вторжений . Шифруйте важные файлы приложений, файлы данных и резервные копии, чтобы неавторизованные пользователи не могли прочитать ваши важные данные.

Рекомендации по обеспечению безопасности баз данных

Вот несколько рекомендаций, которые вы можете использовать для повышения безопасности конфиденциальных баз данных.

Активное управление паролями и доступом пользователей

Если у вас большая организация, вы должны подумать об автоматизации управления доступом с помощью управления паролями или программного обеспечения для управления доступом. Это предоставит разрешенным пользователям кратковременный пароль с правами, которые им нужны каждый раз, когда им нужно получить доступ к базе данных.

Он также отслеживает действия, выполненные в течение этого периода времени, и не дает администраторам обмениваться паролями. Хотя администраторы могут посчитать, что обмен паролями удобен, однако это делает эффективную подотчетность и безопасность базы данных практически невозможными.

Кроме того, рекомендуются следующие меры безопасности:

- Необходимо применять надежные пароли
- Хэши паролей должны быть солеными и храниться в зашифрованном виде.
- Учетные записи должны быть заблокированы после нескольких попыток входа в систему.
- Учетные записи необходимо регулярно проверять и деактивировать, если сотрудники переходят на другие должности, покидают компанию или больше не требуют того же уровня доступа.

Проверьте безопасность своей базы данных

После того, как вы создали инфраструктуру безопасности вашей базы данных, вы должны протестировать ее на наличие реальной угрозы. Аудит или выполнение тестов на проникновение в вашу собственную базу данных

поможет вам понять мышление киберпреступника и выявить любые уязвимости, которые вы могли упустить.

Чтобы убедиться, что тест является всеобъемлющим, привлеките к тестированию безопасности этических хакеров или признанные службы тестирования на проникновение . Тестеры на проникновение предоставляют подробные отчеты со списком уязвимостей базы данных, и важно быстро исследовать и исправить эти уязвимости. Выполняйте тест на проникновение в критически важной системе баз данных не реже одного раза в год.

Используйте мониторинг базы данных в реальном времени

Постоянное сканирование базы данных на предмет попыток взлома повышает вашу безопасность и позволяет быстро реагировать на возможные атаки.

В частности, мониторинг целостности файлов (FIM) может помочь вам регистрировать все действия, выполняемые на сервере базы данных, и предупреждать вас о потенциальных нарушениях. Когда FIM обнаруживает изменение в важных файлах базы данных, убедитесь, что группы безопасности предупреждены и могут расследовать угрозу и реагировать на нее.

Используйте брандмауэры веб-приложений и баз данных

Для защиты сервера базы данных от угроз безопасности базы данных следует использовать брандмауэр. По умолчанию брандмауэр не разрешает доступ к трафику. Он также должен остановить вашу базу данных от запуска исходящих подключений, если для этого нет особой причины.

Помимо защиты базы данных с помощью брандмауэра, вы должны развернуть брандмауэр веб-приложений (WAF). Это связано с тем, что атаки, нацеленные на веб-приложения, в том числе SQL-инъекции , могут использоваться для получения незаконного доступа к вашим базам данных.

Брандмауэр базы данных не остановит большинство атак на веб-приложения, поскольку традиционные брандмауэры работают на сетевом уровне, а уровни веб-приложений работают на уровне приложений (уровень 7 модели OSI). WAF работает на уровне 7 и может обнаруживать

вредоносный трафик веб-приложений, например атаки SQL-инъекций, и блокировать его до того, как он может нанести вред вашей базе данных.

Литература

1. Толковый словарь по вычислительной технике. – М.: Издательский отдел "Русская редакция" ТОО "Channel trading Ltd", 2005.
2. Материалы сайта "Сервер информационных технологий". WEB: www.citforum.ru.
3. Хомоненко А. Базы данных: Учеб. Для вузов. – 2-е изд. – СПб., 2000.
4. Фёдорова А., Елманова Н. Базы данных для всех. –М.: Компьютер пресс , 2001.
5. Глушаков С.В., Ломотько. Базы данных (2001 год издания). – М.: АСТ, 2001.
6. Карпова Т. Базы данных: модели, разработка, реализация, 2001.
7. Когаловский М.Р. Энциклопедия технологий баз данных. –М.: Финансы и статистика, 2002.
8. Конноли Т., Бегг Л., Страчан А. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. – 2-е изд. – Вильямс, 2000.
9. Ханенко В.Н. Информационные системы. – СПб.: Питер, 2001
10. Корнеев В.В., Гареев А.Ф. и др. Базы данных. Интеллектуальная обработка информации. М.: Изд. С.В. Молгачева, 2001.
11. Ребекка М. Райордан Основы реляционных баз данных, 2001.

References

1. Explanatory dictionary of computer technology. - M.: Publishing department "Russian edition" LLP "Channel trading Ltd", 2005.
2. Materials of the site "Information Technology Server". WEB: www.citforum.ru
3. Homonenko A. Databases: Proc. For universities. - 2nd ed. - St. Petersburg, 2000.
4. Fedorova A., Elmanova N. Databases for everyone. –M.: Computer press, 2001.

5. Glushakov S.V., Lomotko. Databases (2001 edition). – M.: AST, 2001.
6. Karpova T. Databases: models, development, implementation, 2001.
7. Kogalovsky M.R. Database Technology Encyclopedia. –M.: Finance and statistics, 2002.
8. Connolly T., Begg L., Strachan A. Databases. Design, implementation and support. Theory and practice. - 2nd ed. - Williams, 2000.
9. Khanenko V.N. Information Systems. - St. Petersburg: Peter, 2001
10. Korneev V.V., Gareev A.F. and other databases. Intelligent information processing. M.: Ed. S.V. Molgacheva, 2001.
11. Rebecca M. Riordan Fundamentals of Relational Databases, 2001.

© Казарян К.К., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Казарян К.К. БЕЗОПАСНОСТЬ БАЗЫ ДАННЫХ // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.