Лекция 12. Безопасность баз данных

Цель лекции: познакомиться с видами СУБД, с защитой базы данных, с уязвимостями СУБД; рассмотреть атаки на повышение привилегий

План лекции:

1. Виды СУБД
2. Защита базы данных
3. Уязвимости СУБД
4. Безопасность систем баз данных

«Безопасность баз данных» (англ. Database security) относится к использованию широкого спектра средств защиты информации для защиты баз данных (потенциально включая данные, приложения баз данных или хранимые функции, системы баз данных, серверы баз данных и связанные с ними сетевые ссылки) против компрометации их конфиденциальности, целостности и доступности. Он включает в себя различные типы или категории контроля, такие как технические, процедурные / административные и физические.

Росс Андерсон часто говорил, что по своей природе большие базы данных никогда не будут свободны от злоупотреблений в результате нарушений безопасности; Если большая система предназначена для облегчения доступа, она становится небезопасной; Если сделана водонепроницаемая, становится невозможно использовать. Это иногда называют «Правилом Андерсона».

Виды СУБД:

- Корпоративные
- Специализированные
- Встраиваемые
- Защищенные

Защита базы данных относится к коллективным мерам безопасности. Они направлены на предотвращение несанкционированного доступа к информации путем кибератак.

Защита систем баз данных – это технологический термин, который включает в себя множество процессов, инструментов и методологий, обеспечивающих безопасность. Наиболее эффективные меры предотвращения несанкционированного доступа к информации:

- разделение баз данных и веб-серверов;
- шифрование сохраненных файлов и резервных копий;
- регулярное обновление используемого программного обеспечения до последних версий;

- осуществлять контроль безопасности.

Многие уровни и типы управления информационной безопасностью подходят для баз данных, в том числе:

- Контроль доступа
- Базы данных аудита
- Аутентификация
- Шифрование
- Целостность данных
- Резервные копии
- Безопасность приложений
- Защита базы данных с использованием статистического метода

Уязвимости СУБД

- **система авторизации:**
  - неверное разграничение прав доступа, определение полномочий и ролей
  - несоответствие настроек удалённого доступа к БД
- **система контроля целостности**
  - “троянцы” в хранимых процедурах
  - неустановленные обновления СУБД
  - неправильная настройка БД
  - переполнение буфера
- **система аутентификации**
  - “плохие пароли”
  - несоответствующие настройки системы аутентификации

Безопасность систем баз данных

Нарушение целостности данных может быть вызвано рядом причин:

- сбои оборудования, физические воздействия или стихийные бедствия;
- ошибки санкционированных пользователей или умышленные действия несанкционированных пользователей;
- программные ошибки СУБД или ОС;
- ошибки в прикладных программах;
- совместное выполнение конфликтных запросов пользователей и др.

Управление привилегиями

- GRANT привилегия [ON объект] TO субъект [WITH GRANT OPTION]
- REVOKE привилегия [ON объект] FROM субъект

- GRANT привилегия [ON объект] TO PUBLIC
- REVOKE привилегия [ON объект] FROM PUBLIC
- SELECT — привилегия на выборку данных; INSERT — привилегия на добавление данных; DELETE — привилегия на удаление данных; UPDATE — привилегия на обновление данных;
- ALTER — изменение физической/логической структуры базовой таблицы
- INDEX — создание/удаление индексов на столбцы базовой таблицы;
- ALL — все возможные действия над таблицей.

Решения по защите БД

- многофакторная аутентификация (подтверждения прав доступа к аккаунту).
- Многофакторная аутентификация — это технология контроля доступа в несколько этапов: помимо ввода логина и пароля к аккаунту, пользователь вводит код подтверждения, полученный в SMS-сообщении (one time password — OTP), проходит голосовую верификацию или использует токен.
- разграничение доступа.
- шифрование данных.
- резервирование данных.
- аудит доступа к данным.
- тестирование нагрузки, оптимизация запросов, индексирование.
- мониторинг трафика и защита базы данных от нежелательной активности.
- применение RAID-массивов.

Избирательные политики безопасности

Объект доступа (диск, каталог, файл, системная служба, средства обработки и передачи информации) — любой элемент системы, доступ к которому может быть произвольно ограничен.

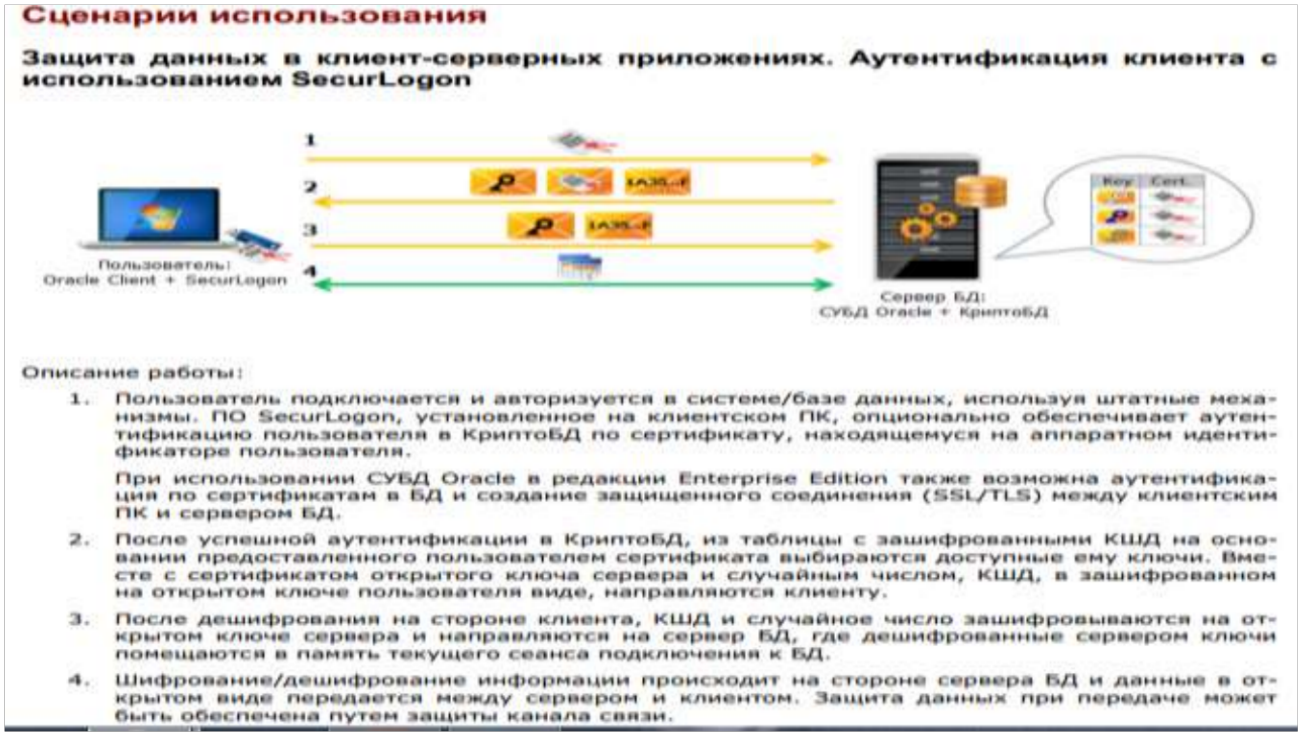
Субъект доступа (пользователь, процессы, программные средства, посредством которых осуществляется доступ к объектам) — любая сущность, способная инициировать выполнение операций над объектами.

Механизмы разграничения доступа оперируют с множествами операций, которые субъекты могут инициировать над объектами.

Для каждой пары «субъект —объект» вводится множество методов доступа и разрешенных операций, являющееся подмножеством всего множества допустимых операций.

Некоторые методы доступа для удобства использования объединяются в группы, называемые правами доступа.

Выделяют такие типы доступа субъекта к объекту как «доступ на чтение», «доступ на запись», «доступ на исполнение» и др.



Защита на уровне пользователей предполагает задание администратором БД определенных разрешений отдельным пользователям и группам пользователей на объекты: таблицы, запросы, формы, отчеты и макросы.

Причинами использования защиты на уровне пользователей являются:

- Защита приложения от повреждения из-за неумышленного изменения пользователями таблиц, запросов, форм, отчетов и макросов, от которых зависит работа приложения;
- Защита конфиденциальных сведений в БД.

Рекомендации по повышению безопасности

- Провести аудит учетных записей на наличие стандартных паролей
- Периодически просматривать учетные записи на предмет использования и периодически отключать устаревшие
- Ввести как административные, так и программные ограничения на длину и сложность пароля

Для повышения общей безопасности этих баз данных можно использовать следующие дополнительные шаги, которые выполняются в рамках сети и среды сервера:

1. Запустите сервер баз данных на компьютере, на котором установлена система Windows Server 2003. По умолчанию эта операционная система более безопасна, чем система Windows 2000 Server. Несмотря на то, что компьютер сервера Windows 2000 Server можно заблокировать, этот процесс может быть связан с затратами времени, кроме того, существует вероятность возникновения ошибок, которыми могут воспользоваться злоумышленники для получения доступа к базе данных.

2. Ограничьте физический доступ к серверу базы данных.

3. Обеспечьте, чтобы разрешения базы данных и списки разграничительного контроля доступа, имеющиеся в файлах базы данных, разрешали доступ только уполномоченному персоналу. Надежными являются разрешения по умолчанию и списки DACL, настроенные службой управления правами. Следует соблюдать осторожность при изменении любых параметров по умолчанию.

4. Не запускайте лишние службы на сервере базы данных, например службы IIS, службу очередей сообщений или службы терминалов.

5. Кроме баз данных службы управления правами, не следует запускать на сервере баз данных никакие другие базы данных.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.

2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.

3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.

4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582

5. Carl A. Sunshine. Computer Network Architectures and Protocols. — Springer Science & Business Media, 2013-06-29. — 542 с. — ISBN 978-1-4613-0809-6.

6. Database Security Best Practices. technet.microsoft.com. Дата обращения: 2 сентября 2021.