PG BootCamp Russia 2024 Kazan

PGBootCamp.ru

Как быстро и эффективно защитить своего слона? Оценка безопасности вашего Postgres

Артем Сергиенко, руководитель отдела ТП «Тантор Лабс»

tantor

Первый шаг к защите вашего слона. Осознание

- Зачем нужна безопасность СУБД?

Первый шаг к защите вашего слона. Осознание

- Зачем нужна безопасность СУБД?
- Хранение критических (sensitive) данных

Первый шаг к защите вашего слона. Осознание

- Зачем нужна безопасность СУБД?
- Хранение критических (sensitive) данных
- Угрозы (человек) и уязвимости (в коде) СУБД

Первый шаг к защите вашего слона. Осознание

- Зачем нужна безопасность СУБД?
- Хранение критических (sensitive) данных
- Угрозы (человек) и уязвимости (в коде) СУБД
- Непрерывность обслуживания вашего бизнеса (кейс СДЭК ;))

Второй шаг к защите вашего слона. Планируем

- Цель аудита безопасности

Второй шаг к защите вашего слона. Планируем

- Цель аудита безопасности
- Выявление уязвимостей

Второй шаг к защите вашего слона. Планируем

- Цель аудита безопасности
- Выявление уязвимостей
- Рекомендации и меры, которые мы хотим предпринять

Второй шаг к защите вашего слона. Планируем

- Цель аудита безопасности
- Выявление уязвимостей
- Рекомендации и меры, которые мы хотим предпринять
- Предотвращение будущих инцидентов

Третий шаг к защите вашего слона. **Выбираем**

- Ручной аудит*

** сомнительно, но окей :)*

Третий шаг к защите вашего слона. Выбираем

- Ручной аудит
- Автоматизированные инструменты проверки

Третий шаг к защите вашего слона. Выбираем

- Ручной аудит
- Автоматизированные инструменты проверки
- Стандарты проверки (CIS Benchmark for PostgreSQL 15/16*)

150 страниц рекомендаций и проверок безопасной настройки

** https://www.cisecurity.org/benchmark/postgresql*

Четвертый шаг к защите вашего слона. Выбираем

› Проверка расширений

timescale/pgspot

```
> pgspot --ignore PS017 <<<"CREATE TABLE IF NOT EXISTS foo();"
PS012: Unsafe table creation: foo
Errors: 1 Warnings: 0 Unknown: 0
```

** атаки на основе search_path*
** создание небезопасного объекта CREATE OR REPLACE*

*https://github.com/timescale/pgspot

Четвертый шаг к защите вашего слона. Выбираем

timescale/pgspot

```
> pgspot --ignore PS017 <<<"CREATE TABLE IF NOT EXISTS foo();"
PS012: Unsafe table creation: foo
Errors: 1 Warnings: 0 Unknown: 0
```

Посканируем?
nmap, OpenSCAP, SQLMap, Metasploit...

```
  nmap --script pgsql-brute -p 5432 <target-ip>
  5432/tcp open  pgsql
| pgsql-brute:
|   root:<empty> => Valid credentials
|_  test:test => Valid credentials
```

Пятый шаг к защите вашего слона. Запоминаем

- И не забудем все запомнить!
- До, после и вовремя аудита. Желательно в письменном виде..

- Pgaudit

- PgBadger

Предпоследний шаг. **Защищаем**

- Детальная конфигурация аутентификации и авторизации клиентов*

**никаких host all all 0.0.0.0*
LDAP/RADIUS – хорошо. RBAC – идеально.
MD5 → SCRAM-SHA-256

Предпоследний шаг. **Защищаем**

- Детальная конфигурация аутентификации и авторизации клиентов
- Защита клиентских подключений*

** hostssl и точка! Никаких открытых соединений без сертификатов*

Предпоследний шаг. **Защищаем**

- Детальная конфигурация аутентификации и авторизации клиентов
- Защита клиентских подключений
- Минимизация прав*

** Никаких персональных GRANT ALL PRIVILEGES. В идеале RLS и CREATE POLICY*

Предпоследний шаг. **Защищаем**

- Детальная конфигурация аутентификации и авторизации
- Защита клиентских подключений
- Минимизация прав
- Многофакторная аутентификация. 2FA/MFA*

** редко, сложно, трудновыполнимо*

Предпоследний шаг. **Защищаем**

- Детальная конфигурация аутентификации и авторизации
- Защита клиентских подключений
- Минимизация прав
- Многофакторная аутентификация
- Шифрование, мониторинг и журналирование событий безопасности*

**pgcrypto, LUKS, etc...*

Последний шаг к защите слона. Проверяем

- Pgdsat
- PostgreSQL Database Security Assessment Tool - утилита, проверяющая порядка 80-ти параметров безопасности кластера PostgreSQL, в том числе все рекомендации CIS PostgreSQL Benchmarks

```
# pgdsat -U postgres -h IP -d postgres -o report.html*
```

*https://github.com/HexaCluster/pgdsat

*https://www.darold.net/sample_pgdsat/report.html

Самый последий шаг. **Финализируем**

› Регулярные аудиты СУБД и мониторинг событий безопасности*

** один раз и на всю жизнь*

Самый последий шаг. **Финализируем**

- Регулярные аудиты СУБД и мониторинг событий безопасности
- Документирование результатов*

** плохих и хороших. Делаем работу над ошибками и едем дальше.*

Самый последий шаг. **Финализируем**

- Регулярные аудиты СУБД и мониторинг событий безопасности
- Документирование результатов
- Регулярность обновлений СУБД*

** регулярность != раз в год. Смотрим рассылку CVE и планируем.*

Самый последий шаг. **Финализируем**

- Регулярные аудиты СУБД и мониторинг событий безопасности
- Документирование результатов
- Регулярность обновлений СУБД
- Планирование ваших действий*

** на случай очень плохих событий. В идеале планируем детально и письменно.*

Самый последий шаг. **Финализируем**

- Регулярные аудиты СУБД и мониторинг событий безопасности
- Документирование результатов
- Регулярность обновлений СУБД
- Планирование ваших действий
- Постоянное улучшение безопасности (hardening)*

** все, что мы успели обсудить в этом докладе :)*

Спасибо за внимание!

Артем Сергиенко, «Тантор Лабс»

tantor