

# Основные проблемы безопасности корпоративных СУБД

**Александр Поляков,**

руководитель направления аудита ИБ, Digital Security,

руководитель исследовательской лаборатории DSecRG

## Закон о персональных данных (ПД)

- Обязывает обеспечивать защиту ПД
- СУБД — место хранения ПД
- Обеспечение безопасности СУБД — ключ к защите данных в независимости от законов или стандартов
- Появление законов и стандартов вынуждает обратить пристальное внимание на технические аспекты защиты СУБД

## Места хранения ПД

- ПД в большинстве случаев хранятся в СУБД и в различных ERP-системах
- Наиболее распространенные СУБД:
  - Oracle (используется как backend для таких ERP, как Oracle EBS, SAP R/3 и прочие)
  - MsSQL (используется как backend для таких ERP, как Microsoft dynamics, 1С и прочие)
- Другие СУБД также используются для хранения ПД, но в меньшей степени, хотя имеют аналогичные проблемы

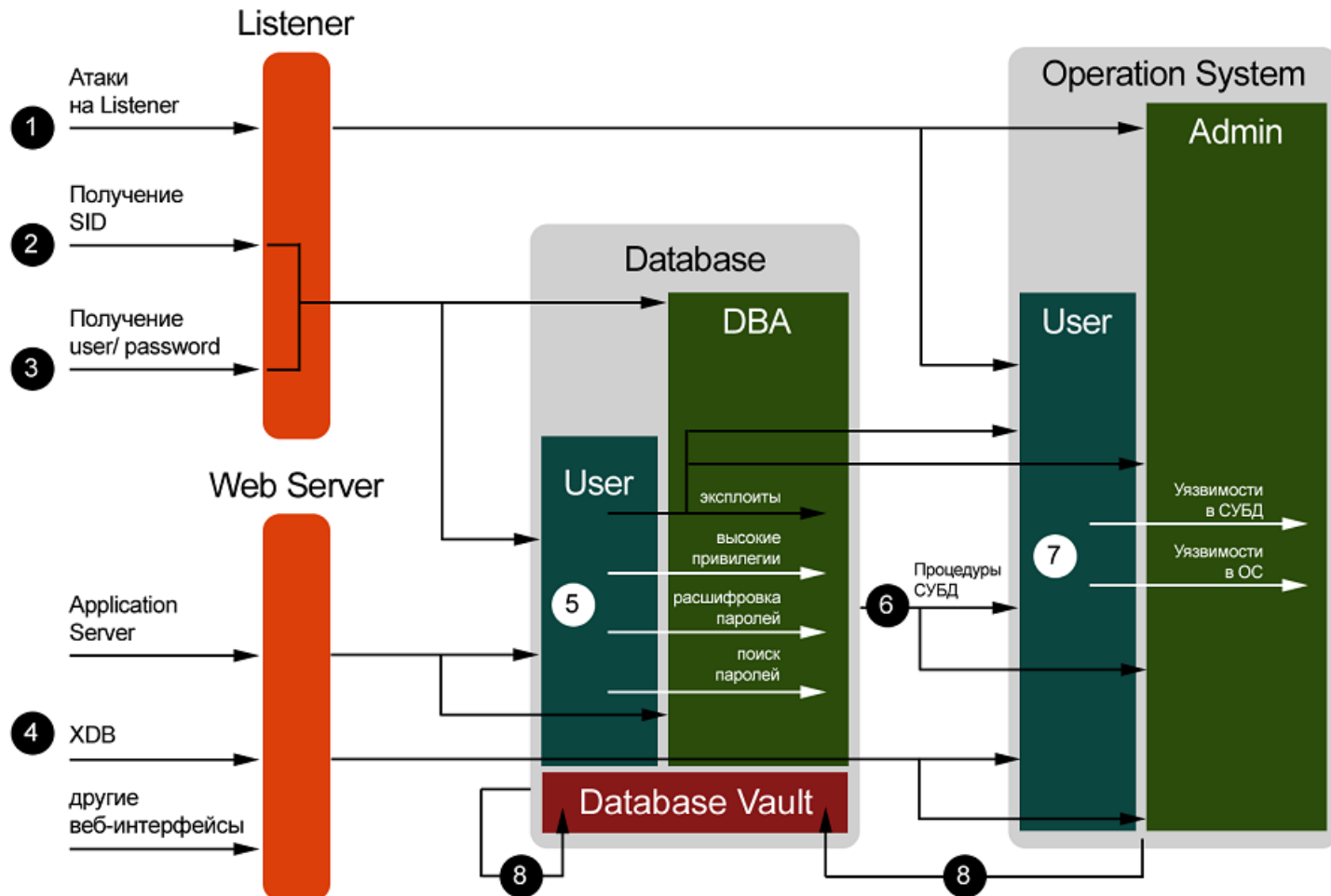
## Уязвимости СУБД

1. Существует множество классов уязвимостей на различных уровнях построения систем, позволяющих получить доступ к данным
2. **Каждый из этих классов периодически пополняется различными новыми атаками**

### Пример:

Одна из наиболее **ОПАСНЫХ** уязвимостей — **возможность получения административного доступа в ОС** и, как следствие, **из него в СУБД**, имея непривилегированную учетную запись в **Oracle и MsSQL** и прочих популярных СУБД

## Основные атаки на Oracle



## Пример

- Подключение со стандартной учетной записью DBSNMP/DBSNMP
- Обращение к ложному SMB серверу из СУБД
- Получение хэша учетной записи пользователя, от которого запущена СУБД
- Расшифровка хэша или атака SMB Relay

## Основные атаки на MsSQL

### 1. Получение административных прав в СУБД:

- Повышение привилегий через уязвимости (sp\_replwritetovarbin)
- Поддельные процедуры
- Поддельные триггеры
- Поиск паролей в СУБД
- Связанные сервера

### 2. Получение административных прав на сервере:

- Чтение регистра и хэшей паролей к ПО типа Radmin, VNC и прочим (xp\_regread)
- Атаки типа SMB Relay (xp\_dirtree)
- Чтение файлов ОС (bulkinsert)

## Автоматизированные атаки

- Простые утилиты для подбора паролей и проведения различных атак:
  - **piggy, oscanner, oak, oat...**
- Множество общедоступных эксплоитов:
  - **milw0rm.com, securityfocus.com, dsecrg.ru ...**
- Комплексные программы для упрощения атаки нажатием одной кнопки:
  - **Orasploit 2007** <http://orasploit.com/> (Red-Database-Security)
  - **Inguma Inguma 2007** <http://inguma.sourceforge.net/> (Joxean KoretOracle)
  - **Oracle Mixin for Metasploit 2008** <http://metasploit.com/> (CG, MC, Alexander Polyakov [DSecRG])
- Утилиты для получения доступа к СУБД через веб-уязвимости:
  - **Bsqlbf v2.4** (Defcon 2009), **Sqlmap** (Blackhat Europe 2009)
- Коммерческие сканеры безопасности:
  - **Repscan**(Red-Database-Security), **Ngssquirrel** (NGS), **Appdetective** (Appsecinc)

## Защита

**В СУБД хранятся критичные бизнес данные вне зависимости от любых законов или стандартов, требующие адекватного уровня обеспечения ИБ**

Основные направления обеспечения ИБ СУБД:

1. Контроль доступа (аутентификация, авторизация)
2. Разграничение ролей (назначение ролей, принцип наименьших привилегий)
3. Защита данных (шифрование)
4. Регулярные обновления
5. Обнаружение и предотвращение вторжений
6. Аудит событий

## Контроль доступа

1. Защита сетевых интерфейсов управления (Oracle Listener)
2. Фильтрация доступа на сетевом уровне
3. Удаление учетных записей «по умолчанию» и тестовых учетных записей
4. Внедрение парольной политики (сложность, длина, блокирование подбора)
5. Процедуры по периодической смене паролей

## Разграничение ролей

1. Назначение всем пользователям определенных ролей
2. Разграничение ролей в соответствии с их правами доступа к данным (принцип наименьших привилегий)
3. Удаление ненужных и опасных функций, доступных непривилегированному пользователю  
в Oracle: UTL\_FILE, UTL\_HTTP...  
в MsSQL: xp\_regread, xp\_dirtree...

## Шифрование

1. Обеспечить прозрачное шифрование данных
  - (Oracle TDE, SQL Server TDE 2008)
2. Безопасное управление ключами (генерация, хранения, смена)
  - Oracle Wallet/ HSM
3. Шифрование отдельных полей

## Периодические обновления

1. Наладить процесс отслеживания последних уязвимостей в программном обеспечении (подписка на рассылки)
2. Процедуры установки последних обновлений безопасности
3. Все равно нет защиты от 0-day!

## Обнаружение и предотвращение вторжений

1. Наличие 0-day уязвимостей
2. Промежуток между выпуском обновления и его установкой значительно больше 1 дня
3. Большинство атак, направленных на СУБД, не отслеживаются сетевыми IDS
4. Атаки, которые можно обнаружить, легко видоизменить и обойти механизмы обнаружения (например, шифрование эксплоитов в Metasploit)
5. Наиболее эффективное решение — специализированная IDS
6. На данный момент — это Sentrigo Hedgehog

## Если все таки сломали?

1. Сломать можно все, неязвимых систем не бывает
2. Важно знать **КТО, КОГДА** и **К ЧЕМУ** получил неавторизованный доступ

### **СЛЕДОВАТЕЛЬНО**

#### **Необходимо настроить аудит событий:**

1. Выбрать способ аудита (в Oracle — стандартный или FGA, в MsSQL — стандартный или c2)
2. Проанализировать к ЧЕМУ и КАКОЙ именно доступ будет подвергаться аудиту
3. Защитить данные аудита от неавторизованного доступа
4. Настроить централизованный удаленный сервер хранения и анализа журналов (применение дополнительных программных средств, таких как audit vault и прочих продуктов)

## Быть всегда в курсе

**1. Англоязычные ресурсы и литература по базам данных**

[petefinnigan.com](http://petefinnigan.com)

[blog.red-database-security.com](http://blog.red-database-security.com)

[oracleforensics.com](http://oracleforensics.com)

[cisecurity.org/bench\\_sqlserver.html](http://cisecurity.org/bench_sqlserver.html)

[databsesecurity.com](http://databsesecurity.com)

**2. Русскоязычные ресурсы и литература**

1. [dsecrg.ru](http://dsecrg.ru)

2. [pcidss.ru](http://pcidss.ru)

3. [securitylab.ru](http://securitylab.ru)

**3. Книга «Безопасность Oracle глазами аудитора: нападение и защита»**

Вопросы?

**Спасибо  
за внимание**

[a.polyakov@dsec.ru](mailto:a.polyakov@dsec.ru)