Защита баз данных

Повестка дня

- Реалии сегодняшнего дня…
  - Источники атак
  - Уязвимости СУБД
- Что делать? Кто поможет?
  - DbProtect – новое предлагаемое решение
  - Решаемые задачи
  - Схема внедрения
  - Функционал
  - Поддерживаемые СУБД
  - Поставка
  - Лицензирование
- Резюме

Реалии сегодняшнего дня…

Источники атак

Увеличивается количество сфокусированных атак:

- ✓ непосредственно на приложения - 75%!
- ✓ рост количества внутренних атак - 80+%!

Внешние угрозы

- хакеры, черви…

Внутренние пользователи

- ✓ операторы БД
- ✓ аналитики
- ✓ администраторы

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

Что делать? Кто поможет?

Предлагаемое решение

DbProtect

Интегрированное решение для обеспечения защиты СУБД со встроенной системой централизованного управления производства компании Application Security (США).

Решаемые задачи

Задачи, которые решает **DbProtect**

обнаружение
сканирование
и оценка
уязвимостей

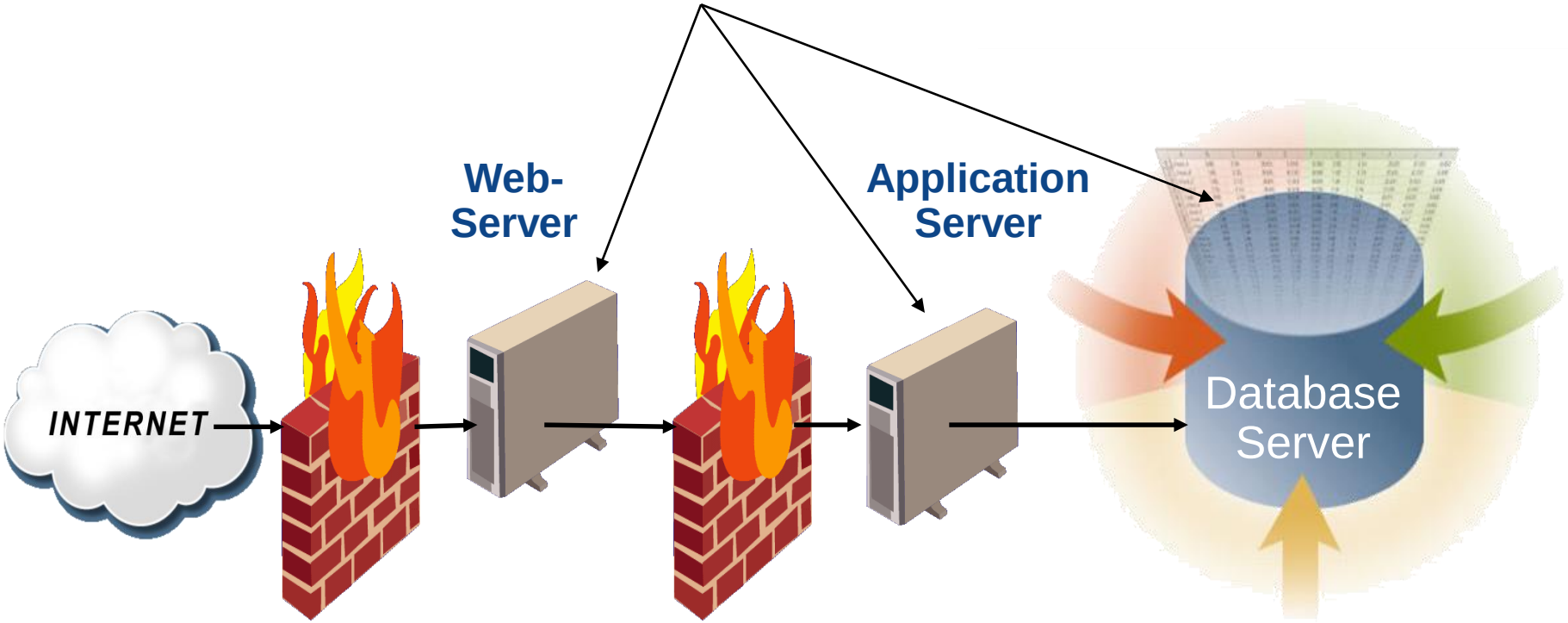
тестирование на
проникновения
(Penetration
Testing)

мониторинг
активности в
режиме реального
времени

анализ
защищённости

Схема внедрения

AppDetective™



Функционал DbProtect (1)

AppDetective™

сканер безопасности

Функции:

- инвентаризация сети
- оценка защищенности от внешних вторжений и злоупотреблений внутренних пользователей
- тестирование на проникновение
- создание детальных отчетов и выдача рекомендаций
- сбор информации с установленных в сети сканеров при помощи единой консоли управления дистанционно

Функционал DbProtect (2)

AppDetective™

Достоинства:

- дистанционное сканирование СУБД - не требует установки на них агентов
- проведение аудита защищённости не только самой БД, но и приложения, с помощью которого пользователь взаимодействует с этой базой
- возможность одновременного анализа нескольких СУБД
- наиболее полный анализ защищенности БД - > 1 000 проверок и тестов
- классификация всех уязвимостей по приоритетности
- встроенная гибкая подсистема создания отчётов – оперативная подготовка отчётов для руководства
- выдача рекомендаций

Функционал DbProtect (3)

DbProtect

аудит безопасности

Возможности:

- мониторинг в **режиме реального времени**:
  - действий всех пользователей и изменений системы
  - комплексных атак и угроз
- разграничение прав доступа силами администратора
- оправка оповещений о критичных событиях
- получение обновлений в режиме ASAP

Функционал DbProtect (4)

DbProtect

Характерные особенности:

- возможность создания пользовательских сигнатур и правил
- возможность контролировать обращения (запросы типа select, insert и т.п.) к отдельным полям таблицы
- агенты DbProtect могут устанавливаться как на сервер БД, так и в сети (host & network sensors)
- управление всеми агентами DbProtect осуществляется через консоль встроенной системы централизованного управления

Функционал DbProtect (5)

DbProtect

Достоинства:

- встроенная система централизованного управления
- масштабируемая архитектура
- обнаружение атак, использующих уязвимости web-приложений, взаимодействующих с СУБД
- настраиваемая система оповещения о событиях безопасности

Поддерживаемые СУБД

DbProtect

AppDetective™

- ✓ Oracle Database
- ✓ Microsoft SQL Server
- ✓ IBM DB2
- ✓ IBM DB2 on Mainframe
- ✓ Sybase ASE
- ✓ Lotus Domino Notes

Поставка

DbProtect поставляется в 2 вариантах:

- ✓ полнофункциональный – DbProtect
- ✓ сканер безопасности – DbProtect AppDetective

Лицензирование

DbProtect лицензируется по количеству защищаемых баз данных. Для Oracle – по SID.

Лицензия – ежегодная подписка, включающая:

- ✓ лицензию на использование продукта
- ✓ получение обновлений
- ✓ стандартную техническую поддержку (5x12)
- ✓ систему централизованного управления
- ✓ пользовательский интерфейс
- ✓ возможность разграничения прав доступа по ролям и ответственности
- ✓ "движок" сканирования
- ✓ ПО сенсора

Резюме

- ✓ грамотная инсталляция со сменой всех паролей и блокировкой ненужных служебных учётных записей
- ✓ своевременная установка патчей и обновлений
- ✓ **аудит и анализ приложений!!!!!**
- ✓ **мониторинг…….**

Спасибо за внимание!