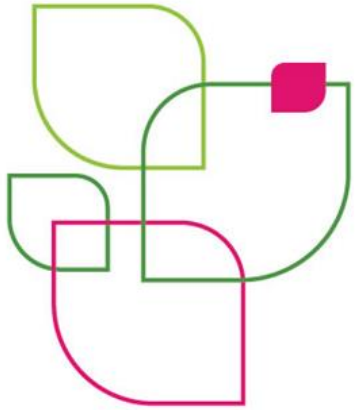
Ренессанс Кредит

Привилегированные учётные записи

Управление, способы контроля



Дмитрий Стуров
Москва, 2014

Привилегированные учётные записи

Ренессанс Кредит

Категории:

1. Общие учетные записи
   - Unix root
   - Windows Administrator
   - DB admins (Oracle SYS)
2. Учётные записи приложений (Application-to-Application)
3. Личные учётные записи администраторов

Привилегированные учётные записи

Ренессанс Кредит

Особенности привилегированных учётных записей:

1. Неограниченный доступ
2. Общий, коллективный доступ к паролям
3. Анонимность
4. Широкая распространённость
5. Статичность, несменяемость

Привилегированные учётные записи

Ренессанс Кредит

Проблемы управления:

1. Прозрачность, ответственность, аудит
2. Управление паролями
3. Жизненный цикл
4. Контроль доступа

Ренессанс Кредит

ОБЩИЕ УЧЁТНЫЕ ЗАПИСИ

управление паролями

#

Got root?

Управление паролями общих записей

Ренессанс Кредит

Задачи системы:

1. Устранение статичных, широко известных паролей
2. Доступ только для конкретных пользователей
3. Маскировка пароля, сокрытие от администратора
4. Контроль доступа
5. Интеграция с системами сильной аутентификации
6. Аудит

Система сама не должна быть уязвимой либо служить точкой отказа

Управление паролями общих записей

Ренессанс Кредит

Применяемые механизмы:

1. Защищённое хранение паролей (шифрование, изолирование, строгая аутентификация и контроль доступа)
2. Выдача паролей (авторизация ➔ выдача пароля ➔ использование ➔ смена)
3. Инициация сессий (rdp, ssh, telnet)
4. Смена паролей (периодическая, по требованию, после выдачи п.2)
5. Верификация паролей (после смены, периодическая)
6. Автоматическая инвентаризация через сканирование инфраструктуры
7. Аудит действий, отчёты

Ренессанс Кредит

УЧЁТНЫЕ ЗАПИСИ ПРИЛОЖЕНИЙ

управление паролями

#

Application-to-Application

Управление паролями A2A записей

Ренессанс Кредит

Особенности A2A паролей:

1. Указываются в скриптах в открытом виде
2. Скрипты раскиданы по многим серверам, хранилищам кодов, средам
3. Доступны практически всем участникам процесса разработки, тестирования
4. Пароли никогда не меняются
5. Неиспользуемые A2A записи не удаляются

Управление паролями A2A записей

Ренессанс Кредит

Применяемые механизмы:

(в дополнение к уже перечисленным)

1. Интерфейс для взаимодействия с системами (web сервис, библиотеки, API и пр.)
2. Дополнительная аутентификация вызываемого сервиса (IP, сертификаты и пр.)
3. Автоматическая инвентаризация внутри скриптов (файлы, хранилища кода)

Ренессанс Кредит

УЧЁТНЫЕ ЗАПИСИ АДМИНИСТРАТОРОВ

управление

#

Super User

Управление УЗ администраторов

Ренессанс Кредит

Применяемые механизмы:

1. Sudo/RunAs
2. Делегирование прав
3. Централизованное управление политиками
4. Фильтрация команд
5. Проксирование сессий

Ренессанс Кредит

МОНИТОРИНГ

#

Log

Мониторинг действий

Ренессанс Кредит

Применяемые механизмы:

1. Подключение к сессиям, запись
2. Нажатые клавиши
3. Аналитика
4. Уведомления

Ренессанс Кредит

Спасибо за внимание