СБЕРБАНК
Всегда рядом

Защита привилегированных учетных записей, опыт внедрения в ДБ АО «Сбербанк», «подводные камни».

Мусабек Садыков
Главный специалист Отдела информационной безопасности
Департамент безопасности и защиты информации

«**Предприятия** должны обеспокоиться теми **рисками**, которые могут вызвать **системные администраторы**, включая аварии, кражи данных и прочие возможные негативные их действия. Процесс **снижения рисков** должен начаться заранее, **до принятия на работу** системного администратора, а также на протяжении всей его работы».

Gartner®

Кто они Администраторы?

СБЕРБАНК
Всегда рядом

В каждой компании есть «Звезды» имеющие привилегированный доступ в информационную систему компании.

Атаки на корпоративный сегмент

СБЕРБАНК
Всегда рядом

Любое дело начинается с **разведки**. **Цель** ясна — **стать администратором домена**, но по пути к этой цели надо выявить критичные точки

Как было до внедрения системы?

1. Авторизация администраторов ИС происходила по логину и паролю.

2. Работа с привилегированной учетной записью в 4 четыре руки.

3. Периодическое ручное изменение пароля от привилегированной учетной записи.

4. Контроль действии администраторов проводился в момент проведения работ администратором.

5. Не ограниченный сетевой доступ до серверов ИС Банка.

Затраты на изменение пароля для всех серверов банка: 48 часов

После внедрения…

1. **Прозрачный контроль за действиями привилегированных пользователей**.

2. **Защита паролей от административных учетных записей.**

Все пароли от административных учетных записей меняются системой автоматически. Администраторам ИС Банка не известны пароли от привилегированных учетных записей, тем самым существенно снижается риск похищения злоумышленниками паролей администраторов.

3. **Высвобождение человечских ресурсов в связи с автоматизацией процесса по контролю за действиями администраторов.**

В 2014 году произошла утечка из банка JPMorgan. Атака хакеров началась с кражи паролей привилегированных учетных записей. В результате атаки, хакеры получили доступ к 90 серверам Банка и произвели кражу информацию о 76 миллионах клиентов.

После внедрения…

4. Соответствие требованиям в стандарта PCI DSS.
Обязательное требование по двухфакторной авторизации административных учетных записей.

5. Снижение инцидентов ИБ со стороны действии администраторов.
Ранее зачастую тяжело было определить кто именно и какие действия производил в момент инцидента и конкретные администраторы не могли перед своим руководством доказать свои вину или невиновность.

6. Отчуждение вводимых команд в SIEM

Какие риски покрывает система

СБЕРБАНК
Всегда рядом

- Снижения числа неконтролируемых действий со стороны администраторов ИС (своевременность обнаружения и обеспечение необходимого времени реакции на инциденты).

- Минимизация риска в получении злоумышленниками административных привилегий для совершения нерегламентированных действий.

Какие информационные ресурсы контролируются системой?

СБЕРБАНК
Всегда рядом

- Сервера с ОС Unix\Linux, Windows.
- СУБД
- Сетевые коммутаторы и межсетевые экраны
- Консоли администрирование: WEB.
- Прикладное приложение.

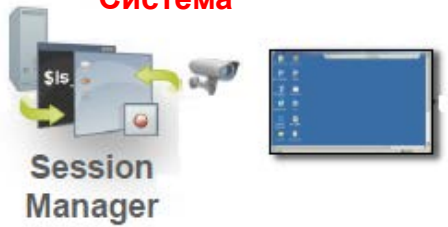
Более **400** контролируемых привилегированных учетных записей.

Инфраструктура системы

СБЕРБАНК
Всегда рядом

Администратор

Система



Информационные ресурсы

О сроках внедрения …

СБЕРБАНК
Всегда рядом

↙ Отсутсвие желания администраторов.

↖ Мотивация со стороны подразделение безопасности.

↖ 1-2 дня внедрение системы.

↖ 1 месяц заведение привилегированных учетных записей.

СБЕРБАНК
Всегда рядом

Вопросы?