Контроль действий привилегированных пользователей

Суховей Андрей

Ведущий инженер центра информационной безопасности R-Plus

Who is mister PU?

Привилегированные пользователи (Privileged Users) — это все сотрудники в организации, обладающие расширенными правами доступа к ее информационным системам. Они могут быть как внутренними системными администраторами, так и внешними поставщиками услуг, ответственными за удаленное управление или обслуживание ИТ-систем.

R PLUS

Цифры

- 42% системных администраторов хотя бы раз использовали служебное положение для несанкционированного доступа к конфиденциальным данным в своей организации.
- 74% из них признались, что могут с лёгкостью обойти меры безопасности, предпринятые в организации для защиты информации.
- В 30% случаев количество привилегированных учётных записей вовсе неизвестно, а в подавляющем большинстве компаний оценка этого количества ошибочна на порядок.

RPLUS

Зачем нам это нужно?

- У организации нет полного и актуального списка всех привилегированных учетных записей, которые существуют в ее сети.
- Факты предоставления привилегированных учетных записей конкретным лицам документально не оформляются.
- Выяснить, кто, когда и с какой целью обращался под привилегированными учетными записями к ИТ-ресурсам организации, не представляется возможным.
- Организация не может проверить, насколько сложны, уникальны и как часто меняются пароли привилегированных учетных записей, можно ли считать их надежными.
- У организации нет полного списка паролей привилегированных учетных записей, хранящихся в приложениях, и нет возможности узнать, какие штатные и внештатные сотрудники могут получить с их помощью доступ к конфиденциальной информации.

Как итог:

- Несанкционированные изменения конфигурации серверов целевых систем, либо изменения сделанные неквалифицированным персоналом могут привести к остановке целевых систем с прерыванием бизнес-процессов.

R PLUS

Методология решения

- Контроль доступа к привилегированным учетным записям (включая управление паролями);
- Мониторинг активности (предполагающий аудит действий пользователя);
- Управление привилегиями (в т. ч. ручное управление доступом);
- Аутентификация приложений;

R PLUS

Варианты архитектуры

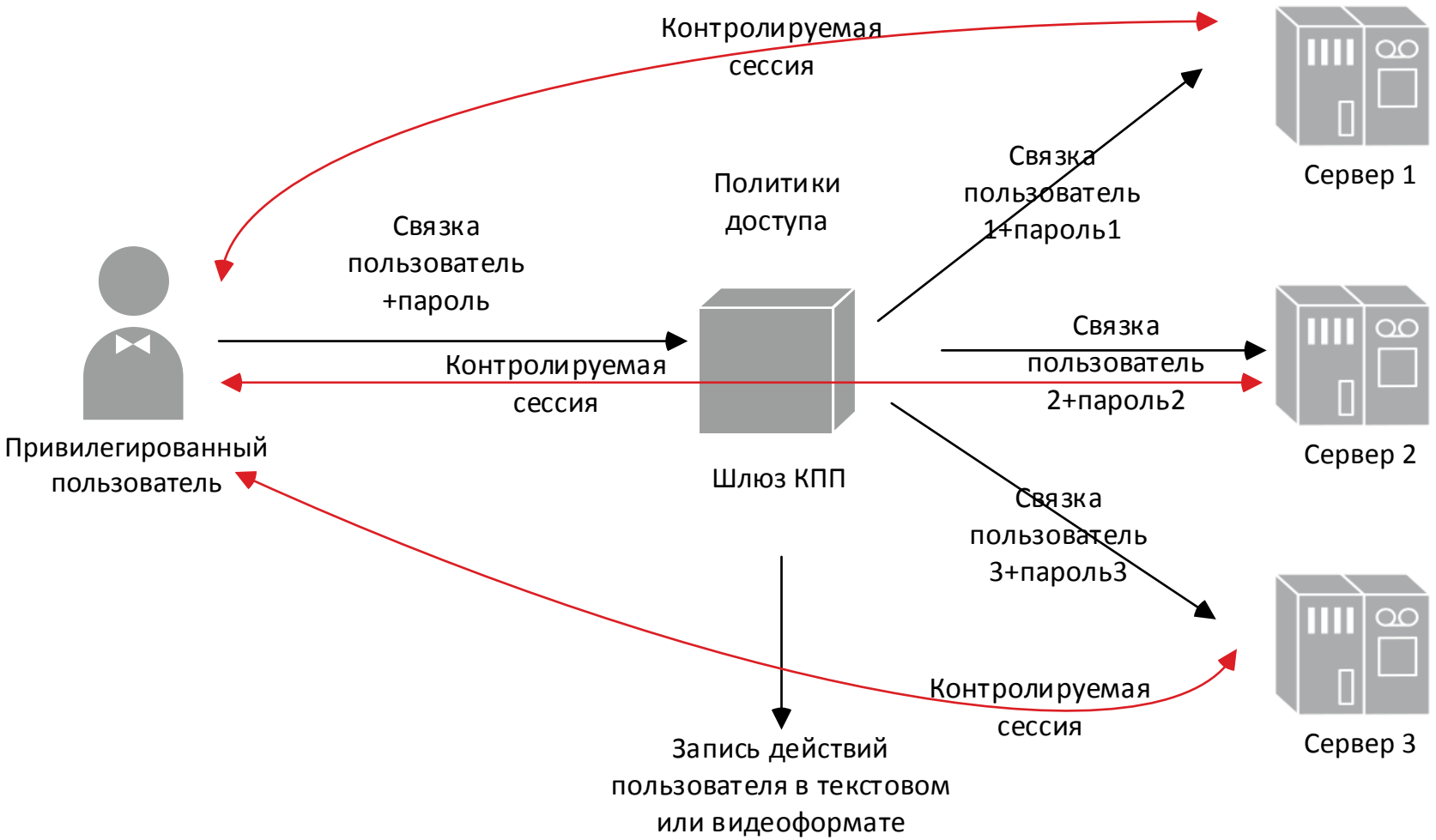
ПАК — **Хост**

- Appliance\virtual machine
- Контроль серверов
- Контроль администраторов инфраструктуры и бизнес-приложений
- Безопасное хранение паролей
- Легко администрируется (меньше OPEX)
- Видеоархив за 4 мес

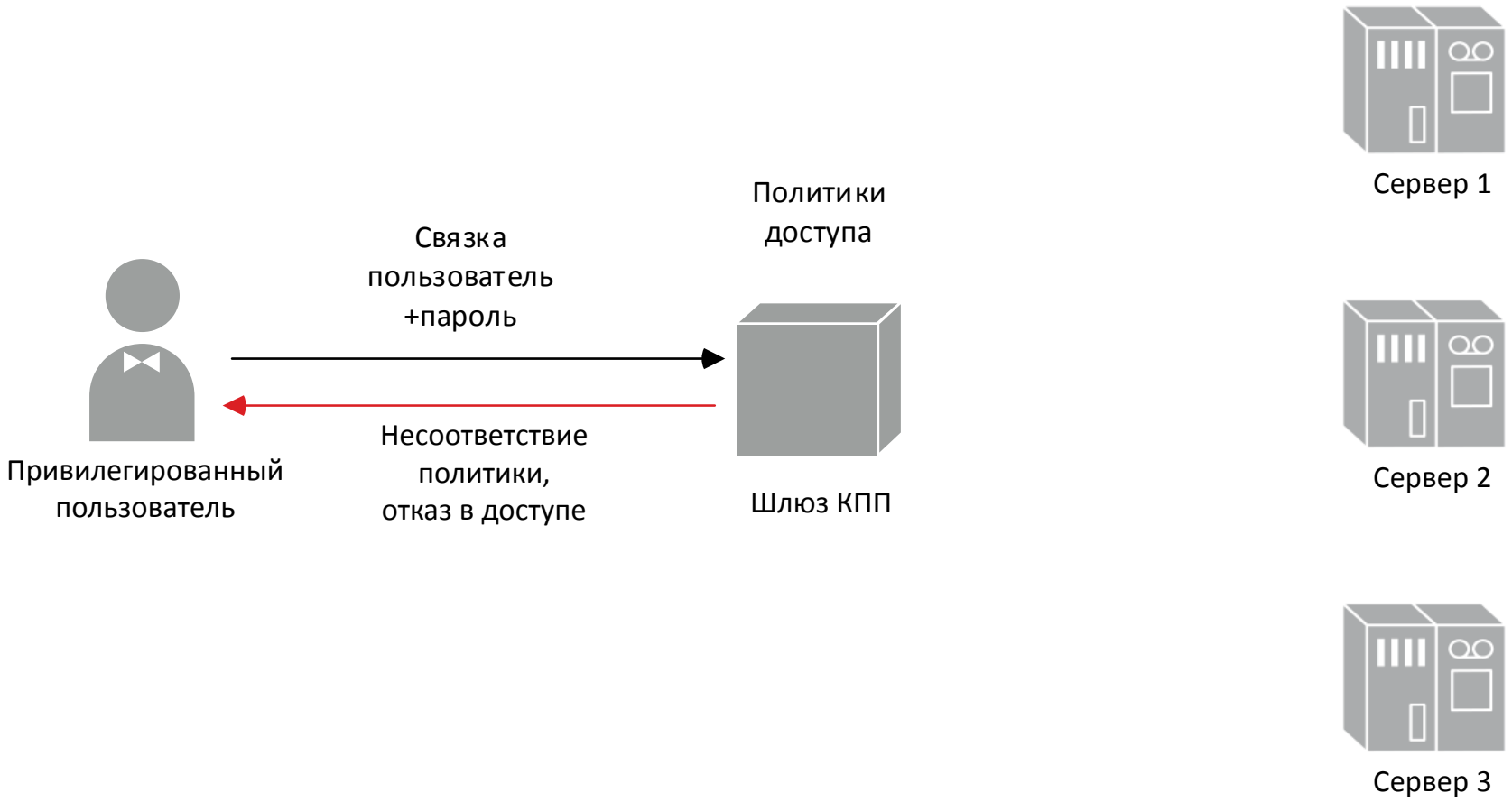
- Установка на каждом ПК
- Контроль рабочих мест
- Контроль временных работников, трейдеров и операторов call-center
- Безопасное хранение паролей
- Лицензии дешевле (меньше CAPEX)
- Видеоархив за 2 года

R PLUS

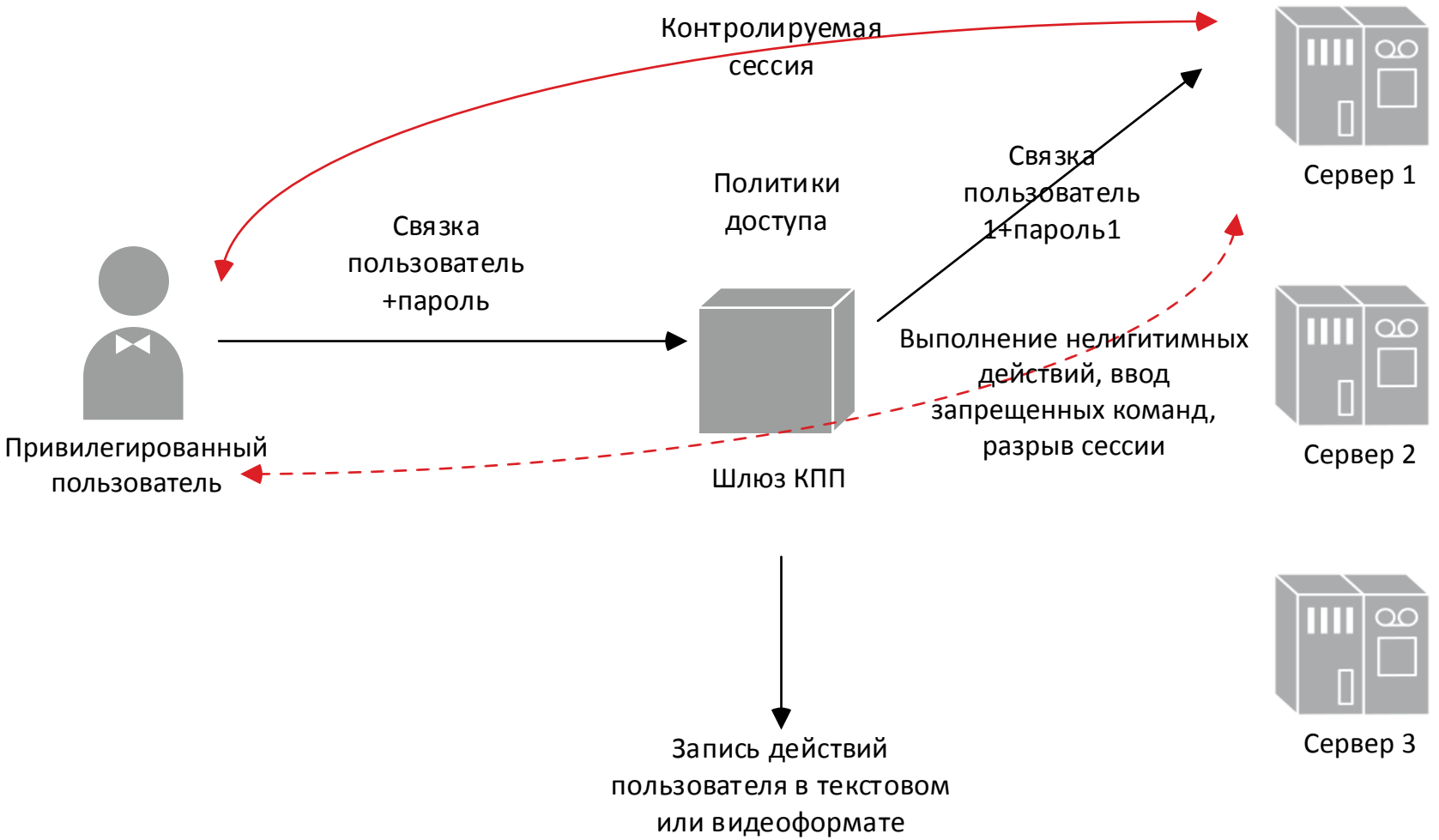
Как это работает?



Как это работает?



Как это работает?



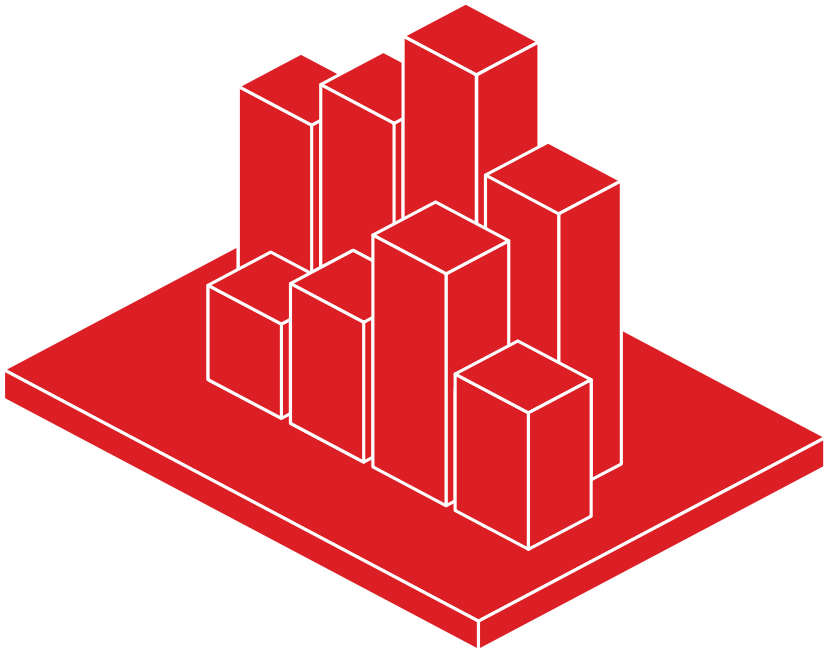
Поддерживаемые протоколы

Система поддерживает следующие протоколы:

- SSH;
- Web (HTTP, HTTPS);
- Radmin;
- VNC;
- RDP;
- TELNET;
- HPiLO;
- VSphere (vmware);
- AS400;
- SQL+;
- OS390.

Варианты применения

- “Кадровая текучка” ИТ и ИБ специалистов;
- Сопровождение инфраструктуры внешним подрядчиком;
- Отсутствие “доказательной базы”



Достигаемые результаты

- Централизованный контроль за привилегированными учетными записями;
- Хранение и управление паролями привилегированных пользователей (достигается независимость от атак используемых встроенные учётные записи ОС и приложений);
- Возможность аудита пользовательских сессий и построение отчётов;
- Интеграция с SIEM;
- Оповещения в режиме реального времени (mail & logs)
- Наличие “доказательной базы”, содержащей детальную информацию о пользовательских сессиях для проведения служебных расследований.

R PLUS

Уже внедрено: ведущие компании в мире и России

Производство | Телеком&ИТ | Банки | Госсектор | ТЭК

PSA PEUGEOT CITROËN

orange

УРАЛСИБ

ФСТ РОССИИ

TOTAL

ArcelorMittal

FABRIKANT.RU
СДЕЛАНО В РОССИИ

ВТБ24

EDF

Pfizer

МТС

Raiffeisen BANK

ГАЗПРОМ НЕФТЬ

Трубная Металлургическая Компания

Билайн

UniCredit Bank

Федеральное казначейство

МОЭК

РОСНАНО

R PLUS

Возможности R-Plus

Вендоры

WALLIX
TRACE, AUDIT & TRUST

CYBERARK

observe it
People audit

Опыт

Федеральное
казначейство

R PLUS

Контактная информация

123022, г. Москва, ул. Рочдельская, д. 15, к. 16а

Т. +7 495 640-6010

www.r-style.com