sPACE

sPACE PAM

Сценарии использования PAM

ООО «Вэб Контрол ДК»

О компании «Вэб Контрол ДК»

- ✓ Российский разработчик системы управления доступом привилегированных пользователей sPACE PAM
- ✓ 15-летний опыт работы с решениями мировых лидеров — разработчиков ПО
- ✓ Дистрибьютор решений сетевой и информационной безопасности, а также решений в области безопасной разработки
- ✓ Собственная команда разработки и служба технической поддержки

Проблема

sPACE

Проблема:

Риск компрометации привилегированных учетных данных и неконтролируемый административный доступ к ИТ-инфраструктуре и критическим данным Компании

Последствия:

- Блокировка или вывод из строя ИТ-инфраструктуры
- Потеря или компрометация чувствительных данных
- Утечка конфиденциальной информации и персональных данных
- Финансовые и репутационные потери

Рост числа киберугроз в 2024

Рост числа APT-групп, атакующих цели в России*	Рост количества DDoS-атак как по количеству, так и по числу задействованных в ботнетах устройств*	Значительный рост числа атак на российские компании, с использованием шифровальщиков*
В 2 раза	**Минимум на 50%**	

Прогнозируется расширение фишинговых атак на многофакторную аутентификацию (MFA): атакующие будут искать способы обхода этой защиты, используя фишинговые схемы для получения доступа к защищённым системам и аккаунтам*

Большинство значимых кибератак являются осуществляются с использованием скомпрометированных привилегированных учетных данных

* Источник — Киберугрозы в России и СНГ. Аналитика и прогнозы 2024/25. Исследование компании F6

Последствия кибератак (лето 2025)

sPACE

«Аэрофлот» (Июль 2025)

Значительный материальный ущерб.
Заведено уголовное дело.

Винлаб (Июль 2025)

Акции Novabev Group на Московской бирже упали на 5,5%. Ущерб включает также прямые потери из-за простоя.

12storeez (Июнь 2025)

Хакеры зашифровали часть данных в 1С и требовали выкуп в 20 млн. руб. Магазины не работали 2 дня. Ущерб включает прямые потери из-за простоя.

Сеть аптек «Столички» (Июль 2025)

Ущерб включает прямые потери из-за простоя, а также возможные штрафы и компенсации в случае утечки персональных и медицинских данных

KNP Logistics (Великобритания) июль 2025

Уничтожена 158-летняя британская компания.
Без работы осталось 730 человек.
Группировка Akira проникла в систему транспортной компании, угадав учётные данные одного из работников. После этого злоумышленники зашифровали все корпоративные данные и потребовали выкуп в размере £5 миллионов. KNP не смогла заплатить такую сумму и была вынуждена объявить о банкротстве.

Типовые сценарии кибератак

sPACE

✓ **Атака через корпоративный сегмент**

Атаки с проникновением злоумышленников через корпоративный сегмент сети передачи данных посредством фишинга или социальной инженерии

✓ **Атака через удаленные рабочие места**

Компрометация рабочих мест работников компании или подрядчиков, имеющих удаленный доступ в технологический сегмент

✓ **Атака через цепочку поставок**

Компрометация одного из участников цепочки поставок:

- производителей ПО
- подрядчиков, обслуживающих компоненты ИТ-инфраструктуры

Кто в зоне внимания?

sPACE

Основной фокус:

Привилегированные пользователи, имеющие административные права на управление ИТ-ресурсами компании и доступ к чувствительной информации и персональным данным:

- ИТ-администраторы — сотрудники компании
- Внешние подрядчики
- Бизнес-пользователи компании, работающие с чувствительными данными

Решение

sPACE PAM – система для автоматизации подключения и обеспечения безопасного и контролируемого доступа привилегированных пользователей к управлению ИТ-инфраструктурой и критическими данными

Безопасное использование привилегированных учетных данных

- Хранение в зашифрованном виде
- Ротация в соответствии с заданными параметрами
- Обновление на целевых системах

Подключение и автоматизация доступа

- Безопасный трек подключения пользователей

(Гранулирование доступа, минимизация привилегий, использование доверенных инструментов, запуск сессий в защищенной среде)

- Различные сценарии доступа
- Гибкий механизм запроса и согласования доступа

Контроль действий пользователей

- Фиксация действий пользователей

(Формирование журнала сеансов, запись экрана, лога нажатий клавиатуры и мыши, отслеживание метаданных сеансов)

- Он-лайн мониторинг сессий
- Контроль запрещенных команд
- Аудит завершенных сессий

Подключение к PAM
Сценарии применения 1#6

Сценарий 1: Единая точка входа

Сценарий 2: МФА для подключения к любым целевым системам

Основные возможности:

- Сокращение количества правил на межсетевых экранах
- Аутентификация пользователей при подключении к любым целевым системам
- Сокращение инструментов МФА
- Администрирование и контроль доступа всех пользователей в одной точке

Подключение к целевым системам
Сценарии применения 2#6

Сценарий 3: Безопасное и контролируемое подключение пользователей

Сценарий 4: Автоматизация подключения пользователей

Основные возможности:

- Протоколонезависимость, подключение к любым целевым системам
- Безопасный трек подключения
- Автоматизация подключения

  Запуск сессий одним кликом мыши с использованием доверенных инструментов, запускаемых в защищенной среде с автоматической подстановкой привилегированных учетных данных

- Подключение любых категорий пользователей (в т.ч. бизнес-пользователей)

  Простота подключения, отсутствие необходимости подключения

Управление привилегиями
Сценарии применения 3#6

Сценарий 5: Гранулирование доступа и минимизация предоставляемых привилегий

Сценарий 6: Контроль использования привилегий

Основные возможности:

- Удобное назначение привилегий с помощью встроенного механизма Нарядов-допусков

  Различные варианты запроса и согласования Нарядов-допусков: централизованное назначение и/или децентрализованное при котором пользователи могут запросить разрешение, а владельцы целевых систем его согласовать

- Возможность гранулирования доступа до уровня задачи в целевой системе
- Автоматический контроль использования привилегий в рамках действующих Нарядов-допусков

  Контроль сроков и графиков использования Нарядов-допусков, разрешенных для доступа целевых систем, привилегированных учетных записей и инструментов администрирования

- Возможность реализации широкого спектра сценариев подключения

Запись действий пользователей
Сценарии применения 4#6

Сценарий 7: Контроль действий пользователей

Сценарий 8: Аудит завершенных сессий

Основные возможности:

- Запись сеансов и фиксация действий пользователей

  Запись экранов, логов нажатия клавиатуры и мыши, метаданных сеансов

- Автоматический контроль действий пользователей в рамках списка запрещенных команд

  Контроль вводимых команд с возможностью блокировки пользовательского ввода или принудительного завершения сессии или отправки сообщений сотрудникам ИБ

- Онлайн мониторинг сессий

  Скрытое подключение к сессиям с возможностью блокировки пользовательского ввода или принудительного завершения сессий

- Быстрый поиск причин инцидентов

Безопасное использование ПУЗ
Сценарии применения 5#6

Сценарий 9: Автоматическая подстановка ПУЗ при подключении к целевым системам

Сценарий 10: Обеспечение жизненного цикла ПУЗ

Основные возможности:

- Исключение риска компрометации ПУЗ

  Пользователи не знают ПУЗ и не могут их скомпрометировать

- Хранение ПУЗ в sPACE PAM в зашифрованном виде
- Автоматическая ротация ПУЗ и обновление на целевых системах

  Для каждой ПУЗ может быть задан свой режим ротации: до сеанса, после сеанса, по расписанию, по ручной команде, без ротации

- Безопасное использование ПУЗ с их автоматической подстановкой при подключении к целевым системам

Взаимодействие с другими решениями
Сценарии применения 6#6

Сценарий 11: Интеграция взаимодействия sPACE PAM с другими решениями

Основные возможности:

- Интеграция взаимодействия по REST API

  Например, интеграция с Тикет-системой или ServiceDesk

- Выгрузка событий по протоколу Syslog и/или в XLS формате для анализа сторонними системами

  Например, интеграция с SIEM

- Отправка информации о событиях системы в почтовые сервисы

Основные преимущества sPACE PAM

- ✓ Протоколонезависимость и возможность подключения к любым целевым системам
- ✓ Минимизация привилегий и гранулирование доступа до уровня задачи в конкретной целевой системе
- ✓ Безопасный трек подключения пользователей к целевым системам
- ✓ Гибкая архитектура, кластеризация компонентов, широкие возможности вертикального и горизонтального масштабирования
- ✓ Простота работы с системой, возможность подключения к целевым системам любых категорий пользователей, включая бизнес-пользователей
- ✓ Нетребовательность к инфраструктуре, низкая стоимость масштабирования

sPACE

Запросить проведение демонстрации и провести пилотное тестирование:

Система управления доступом привилегированных пользователей sPACE PAM

Разработчик: ООО "Вэб Контрол ДК"

info@web-control.ru

www.web-control.ru

тел.: +7 495 925 7794