КСБ-СОФТ АЙТИБАСТИОН

Удаленный доступ к критической инфраструктуре: как совместить удобство и безопасность

Спикеры:

- **Шляпкин Максим –** руководитель отдела защиты объектов КИИ и АСУ ТП, КСБ-СОФТ
- **Барановский Иван** - руководитель группы поддержки продаж/пресейл, АйТи Бастион

Модератор:

- **Ильин Александр –** руководитель регионального направления, КСБ-СОФТ

«КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Телеграм-канал
«Мнение интегратора»

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

80+
регионов внедрения

4000+
реализованных проектов

Портфолио КСБ-СОФТ

КОМПАНИЯ
АЙТИ БАСТИОН

АЙТИБАСТИОН

2014

ОСНОВАНИЕ КОМПАНИИ
10 лет на российском рынке информационной безопасности

300+

ПАРТНЕРОВ-ИНТЕГРАТОРОВ
Интеграции с компаниями, позволяющие выполнить квалифицированную помощь в реализации защиты инфраструктуры

250+

ЗАКАЗЧИКОВ И ПРОЕКТОВ
Присутствие во всех отраслях от нефтяных компаний до футбольных клубов, от небольших офисов до георазпределенных площадок

>70%

РАМ-РЫНКА РФ
Комплекс СКДПУНТ решение, проверенное «в боях» и доказавшее свою эффективность, надежность и качество

Обменивайтесь
сообщениями
во вкладке «Чат»

Запись вебинара
направим Всем
участникам на указанный
при регистрации e-mail

Задавайте вопросы
во вкладке «Вопросы»

Телеграм-канал
«Мнение интегратора»

ПЛАН ВЕБИНАРА

- Что такое удалённый доступ? На сколько он актуален для субъектов КИИ?
- Как эффективно отслеживать действия пользователей и противостоять основным угрозам при удалённом доступе?
- С помощью каких решений можно организовать безопасный удалённый доступ к ЗОКИИ?
- И многое другое

Наградим авторов 3 лучших вопросов фирменным мерчем!

УДАЛЕННЫЙ ДОСТУП. ОПРЕДЕЛЕНИЕ

Удаленный доступ - процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

[Методический документ ФСТЭК от 11.02.2014 «Меры защиты информации в государственных информационных системах»]

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИБ ОБЪЕКТОВ КИИ ПРИ ОРГАНИЗАЦИИ УДАЛЕННОГО ДОСТУПА СОТРУДНИКОВ СУБЪЕКТА КИИ

УДАЛЕННЫЙ ДОСТУП К ЗОКИИ РАБОТНИКОВ СУБЪЕКТА КИИ

Разработка регламента управления доступом
(блок мер УПД из 239 приказа ФСТЭК России)

Проведение инструктажа работников субъекта КИИ, осуществляющих удаленный доступ к ЗОКИИ, о правилах безопасного удаленного взаимодействия с такими объектами

Определение перечня СВТ, используемого для удаленного доступа.
Запретить использование личных СВТ

Определение перечня информации и информационных ресурсов (программ, томов, каталогов, файлов), расположенных на серверах ЗОКИИ, к которым будет предоставляться удаленный доступ

УДАЛЕННЫЙ ДОСТУП К ЗОКИИ РАБОТНИКОВ СУБЪЕКТА КИИ

Назначение минимально необходимых прав и привилегий пользователям при удаленной работе

Идентификация удаленных СВТ по физическим адресам (MAC-адресам) на серверах ЗОКИИ, к которым будет предоставляться удаленный доступ. Предоставление доступа методом "белого списка"

Исключение возможности эксплуатации удаленных СВТ посторонними лицами

Выделение в отдельный домен работников, управление которым должно осуществляться с серверов субъекта КИИ, и присвоение каждому удаленному СВТ сетевого (доменного) имени

УДАЛЕННЫЙ ДОСТУП К ЗОКИИ РАБОТНИКОВ СУБЪЕКТА КИИ

Обеспечение двухфакторной аутентификации работников удаленных СВТ, при этом один из факторов обеспечивается устройством, отделенным от ЗОКИИ, к которому осуществляется доступ

Организация защищенного доступа с удаленного СВТ к серверам ЗОКИИ с применением средств криптографической защиты информации (VPN-клиент)

Применение на удаленных СВТ средств антивирусной защиты информации, обеспечение актуальности баз данных признаков вредоносных компьютерных программ (вирусов) на удаленных СВТ путём их ежедневного обновления

УДАЛЕННЫЙ ДОСТУП К ЗОКИИ РАБОТНИКОВ СУБЪЕКТА КИИ

Исключение возможности установки работником ПО на удаленное СВТ, кроме ПО, установка и эксплуатация которого определена служебной необходимостью, реализуемое штатными средствами ОС удаленного СВТ или СЗИ от НСД

Обеспечение мониторинга безопасности ЗОКИИ, в том числе ведения журналов регистрации действий работников удаленных СВТ и их анализа. Оперативное реагирование и принятие мер защиты информации при возникновении компьютерных инцидентов

Блокирование сеанса удаленного доступа пользователя при неактивности более установленного субъектом КИИ времени

РЕКОМЕНДАЦИИ ПО МИНИМИЗАЦИИ ВОЗМОЖНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ РАБОТЕ С ПОДРЯДЧИКАМИ

УДАЛЕННЫЙ ДОСТУП ПОДРЯДЧИКОВ К ЗОКИИ

Удаленный сетевой доступ должен осуществляться с применением средств шифрования, при этом обмен ключами шифрования необходимо осуществлять по алгоритмам, исключающим их раскрытие сторонним лицам

Использовать принцип наименьших привилегий для учетных записей инженеров подрядных организаций

Должен вестись учет всех изменений ИТ инфраструктуры в виде актов или протоколов о проведенных работах (в электронном или письменном виде)

Перечень учетных записей инженеров подрядной организации, которым предоставляется удаленный сетевой доступ к информационным системам, необходимо сделать поименным и согласовать обеими сторонами

УДАЛЕННЫЙ ДОСТУП ПОДРЯДЧИКОВ К ЗОКИИ

Предъявление к подрядной организации требования о том, что инженеры для удаленного доступа должны использовать АРМ, которые не используются в личных целях и к которым применяются корпоративные меры по ИБ

Парольные фразы и иные аутентификационные данные инженеров должны храниться в зашифрованном виде, а доступ к ним должен осуществляться исключительно лицами из согласованного перечня

Все парольные фразы должны соответствовать установленному в организации уровню стойкости к атакам типа «Bruteforce», срок их замены должен быть не более одного календарного месяца

Все информационные системы, к которым предоставляется удаленный сетевой доступ, должны входить в контур системы управления информационной безопасностью, принятой в организации темам, необходимо сделать поименным и согласовать обеими сторонами

УДАЛЕННЫЙ ДОСТУП ПОДРЯДЧИКОВ К ЗОКИИ

Возможность удаленного сетевого доступа должна предоставляться организации только на период проведения работ, а по их завершению доступ должен быть ограничен

Все обновления программного обеспечения, по возможности, должны первоначально испытываться в тестовой (резервной) среде, а после завершения его проверки применяться в основной инфраструктуре

При передаче подрядной организации документальных материалов, содержащих сведения о критичных компонентах информационно-телекоммуникационной сети заказчика, необходимо руководствоваться принципом минимальной достаточности

Предусмотреть в договорах на выполнение работ положения об ответственности подрядной организации в случае, если компрометация ее инфраструктуры стала причиной причинения вреда информационным системам заказчика, либо произошла утрата или разглашение каких-либо конфиденциальных материалов

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

ЕДИНАЯ ТОЧКА ДОСТУПА

Единая точка доступа в инфраструктуру (SSO). Гибкая ролевая модель доступов с возможностью интеграции в существующую инфраструктуру (LDAP, AD, Radius)

ЗАПИСЬ СОБЫТИЙ ДОСТУПА

Полная запись видео и метаданных сессий с созданием долгосрочного архива. Клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и т.д. А наличие сертификата ФСТЭК по УД-4 гарантирует неизменяемость данных для использовании их в качестве доказательно базы

УПРАВЛЕНИЕ ПАРОЛЯМИ

Управление паролями целевых учетных записей без необходимости установки агентов на целевые устройства по настраиваемым политикам

БЕЗ УСТАНОВКИ АГЕНТОВ

Подключение к ЦУ без необходимости установки агентов, что особенно важно при подключении к объектам КИИ

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

КОНТРОЛЬ ПРИЛОЖЕНИЙ И УЗ В НИХ

Подключение к конечным приложениям без предоставления полного доступа с сокрытием УЗ от приложений.

ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ

Возможность не только контролировать сессию по её результату, но и видеть все действия в режиме реального времени. А в случае необходимости - блокировать сессию пользователя, предотвращая потенциальную угрозу.

РАБОТА ПО ЗАЯВКАМ С ВОЗМОЖНОСТЬЮ ПОДТВЕРЖДЕНИЯ ДОСТУПА

Возможность предоставления доступа по запросу как в момент подключения, так и заранее. Согласование доступа возможно с добавлением одного и более подтверждающих лиц.

КОНТРОЛЬ НА СТОРОНЕ ИС

Блокировка туннелей, доступа вне разрешенных диапазонов, запрет на запуск процессов и т.д.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

ПРОФИЛИРОВАНИЕ И ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

Создание и ведение профилирования пользователей. Анализ всех действий в разрезе «пользователь-цель-действие», машинное обучение и математические модели.

ДЕТЕКТИРОВАНИЕ АНОМАЛИЙ

Предобработка, анализ и детектирование аномального поведения пользователей на основе профилирования и событий

ОТЧЕТЫ И СТАТИСТИКА

Обработка информации и её выдача в виде понятных отчетов от оперативных до сводных, в т.ч. для руководителей.

ОТКАЗОУСТОЙЧИВОСТЬ И МАСШТАБИРОВАНИЕ

Возможность построения действительно отказоустойчивых инсталляций, в т.ч. распределенных между городами и странами. Легкая возможность наращивать мощности как вертикально, так и горизонтально без привязки к территориальному расположению узлов.

МЫ ПОМОЖЕМ ВАМ ЗАЩИТИТЬ ДАННЫЕ И ВЫПОЛНИТЬ ТРЕБОВАНИЯ НПА

Компания КСБ-СОФТ оказывает полный комплекс услуг по защите объектов КИИ

Безопасность объектов КИИ

Выявление и категорирование объектов КИИ, разработка и внедрение комплексного решения по обеспечению безопасности значимых объектов КИИ, организация взаимодействия с центром ГосСОПКА, анализ уязвимостей и пентест

SOCRAT - центр мониторинга и реагирования на инциденты информационной безопасности

Мониторинг и предотвращение атак на начальных стадиях, либо выявление следов проникновения

Импортозамещение

Решение задач импортозамещения в соответствии со стратегией развития информационного общества в Российской Федерации

Оценка показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры

Выполнение работ по новой методике ФСТЭК России от 02.05.2024 г.

РАБОТАЙТЕ С НАМИ!

ЗАКАЖИТЕ ПИЛОТНЫЙ ПРОЕКТ СКДПУ НТ

8 800 3333-872

info@ksb-soft.ru

ksb-soft.ru

Телеграм-канал
«Мнение интегратора»