Безопасность удаленного доступа:
Практики и рекомендации

Дмитрий Середа
Директор Департамента защиты активов и информации
Телефон: +7(916)5246532

Цель и задачи

Цель данной презентации - обсудить актуальность и важность защищенного удаленного доступа для современной организации. Рассмотреть простые практики, которые дали эффект.

Актуальность темы

Дистанционный доступ предоставляет бизнесу несколько ключевых преимуществ:

1

Гибкость и мобильность

Сотрудники могут работать из любого места, что позволяет компании привлекать таланты со всего мира и увеличивает гибкость в планировании рабочего времени.

2

Экономия затрат

Компании могут сократить расходы на аренду офисных помещений и инфраструктуру, так как сотрудникам не нужно физически присутствовать в одном месте.

3

Улучшение производительности

Современные инструменты для удаленной работы позволяют сотрудникам эффективно выполнять свои задачи независимо от их местоположения.

Актуальность темы

Дистанционный доступ предоставляет бизнесу несколько ключевых преимуществ:

4

Расширение рынка

Компания может легко масштабироваться и выходить на новые рынки без необходимости открытия дополнительных офисов.

5

Поддержание непрерывности бизнеса

В случае чрезвычайных ситуаций, таких как пандемии или природные катастрофы, сотрудники могут продолжать работу из дома, что помогает избежать сбоев в работе компании.

6

Нематериальные блага для работников

Удаленная работа часто приводит к уменьшению стресса и усталости, так как меньшее количество поездок на работу позволяет сотрудникам лучше балансировать свою профессиональную и личную жизнь.

Недостатки дистанционного доступа

Проблемы с коммуникацией и командным духом 1

Без личного взаимодействия между сотрудниками может снизиться уровень доверия и командного духа.

Контроль качества работы 2

Сложно контролировать качество работы и выполнение задач, особенно когда нет возможности лично наблюдать за процессом.

Кибербезопасность 3

Удаленная работа увеличивает риски киберугроз, поскольку сотрудники используют личные устройства и сети для выполнения рабочих задач.

Недостатки дистанционного доступа

Изоляция и одиночество 4

Некоторые сотрудники могут чувствовать себя изолированными и одинокими, что негативно влияет на их психологическое состояние.

Доступ к ресурсам 5

Может возникнуть проблема с доступом к необходимым ресурсам и оборудованию , особенно если они находятся в офисе.

Поддержка IT 6

Требуются дополнительные усилия для поддержки и обучения сотрудников в использовании удаленных инструментов и платформ.

Обмен значимой информацией

Защищенные виртуальные переговорные

Вместо использования социальных сетей для общения рекомендуется использовать защищенные платформы для видеоконференций и обмена сообщениями.

Протоколирование средствами компании

Автоматическое протоколирование всех коммуникаций и действий пользователей для контроля и анализа.

Запрет использования диктофонов с ИИ

Вместо этого рекомендуется использовать гарнитуры или встроенные микрофоны на устройствах, чтобы избежать возможных утечек данных.

Политики безопасности

Политика хранения информации: все важные данные должны храниться исключительно на сервере компании, а не на локальных устройствах.

Политика разделения личных вопросов и рабочих: корпоративные устройства предназначены исключительно для рабочих целей.

Ограничение на использование сторонних сервисов для переговоров или обработки информации, например, социальных сетей или диктофонов с ИИ.

Политика использования корпоративных устройств: организация должна обеспечить, а все сотрудники должны использовать только корпоративные устройства для

Обучение сотрудников

Использование защищенных виртуальных переговорных

Вместо социальных сетей для общения.

Осознание рисков

Понимание основных угроз и уязвимостей, связанных с удаленной работой, таких как атаки методом социальной инженерии, фишинг, компрометация учетных записей и утечка данных.

Безопасное использование устройств

Обучение сотрудников правилам безопасности при использовании корпоративных устройств, включая настройку паролей, обновление ПО и антивирусных программ. Инструктаж по правильному использованию гарнитур и запрещению использования диктофонов с ИИ.

Обучение сотрудников

Избежание устаревания знаний

Регулярное обновление знаний и навыков сотрудников путем проведения тренингов и вебинаров по современным угрозам и мерам защиты.

Правильное обращение с данными

Обучение сотрудников принципам обработки и хранения конфиденциальной информации, а также правилам безопасности при передаче данных через интернет.

Социальная инженерия

Осознание методов социальной инженерии и тренировка сотрудников на распознавание и противодействие таким атакам.

Противодействие социальной инженерии

Что следует учесть?

Реалистичность сценариев

Создавайте сценарии, которые максимально приближены к реальным ситуациям, с которыми могут столкнуться сотрудники.

Мотивация

Используйте мотивы которые обычно используют мошенники.

Развитие навыков критического мышления

Включите упражнения, которые развивают навыки критического мышления и умения анализировать подозрительную информацию.

Противодействие социальной инженерии

Что следует учесть?

Доступность материалов

Обеспечьте участникам доступ к материалам тренинга, включая инструкции, примеры и шаблоны ответов на типичные фишинговые атаки.

Обратная связь

Организуйте систему обратной связи, чтобы участники могли оценить полезность и сложность упражнений, а также предложить улучшения.

Поддержка руководства

Убедитесь, что руководство поддерживает инициативу по проведению тренингов и готово инвестировать ресурсы для их организации и проведения.

Практические кейсы. Примеры

Во время пандемии на сайте, похожем на официальный сайт компании, появилось предложение записаться на посещение офиса.

Пользователям предлагалось пройти обучение по противодействию фишингу, к письму была приложена перехваченная настоящая инструкция безопасности по противодействию фишингу. Однако ссылка вела на поддельный ресурс.

Практические кейсы. Примеры

Перед праздником «8 марта» пользователям было направлено «дружеское письмо» от коллег по работе с бонусом от известного магазина косметики. Письмо было составлено так, чтобы создать ощущение близости и доброжелательности, но на самом деле оно было попыткой мошенничества. Конверсия составила 200%.

После повышения ставки Центрального банка пользователям предложили беспроцентную ссуду от организации. Однако это оказалось обманом, и пользователи, воспользовавшиеся этим предложением, стали жертвами учебной атаки.

Резюме и рекомендации

Хранить все важные данные в корпоративном облаке для упрощения доступа и управления информацией.

Следовать политике разделения личных вопросов и рабочих, используя корпоративные устройства исключительно для рабочих целей.

Проводить регулярное обучение сотрудников по вопросам безопасности, включая осознание рисков, безопасное использование устройств и противодействие социальному инжинирингу.

Организовывать систему обратной связи для оценки полезности и сложности учебных заданий.

Обеспечить поддержку руководства для внедрения инициатив по обучению и повышению квалификации сотрудников.