Применение модели Zero Trust в корпоративной коммуникации

Перефразируя слова главной героини из культового советского фильма “Москва слезам не верит”, получившего Оскар в 1981 году, представленная статья в первую очередь ориентирована на корпоративных юристов и будет менее интересна внешним консультантам. Однако и им могут быть полезны рассмотренные в статье идеи.

Введение

Модель Zero Trust, изначально разработанная как концепция кибербезопасности, базируется на принципе «никогда не доверяй, всегда проверяй». Первоначально эта модель предназначалась для защиты корпоративных сетей от несанкционированного доступа. Основываясь на ней, я предлагаю адаптировать модель Zero Trust для внутренней коммуникации в компаниях. В современном взаимосвязанном мире внутренняя переписка и коммуникация уязвимы к раскрытию через судебные процессы, утечку данных в результате хакерских атак или недоброжелательные действия уволенных сотрудников. Учитывая эти риски, я рекомендую топ-менеджерам компаний и юридическим службам внедрять принципы Zero Trust для защиты репутации компании и интересов всех её заинтересованных сторон. В данной статье рассматривается модель Zero Trust и её применение к офисной коммуникации.

Понимание модели Zero Trust

Основные принципы модели Zero Trust

Модель Zero Trust ставит под сомнение традиционную концепцию защиты корпоративных сетей, которая основывается на создании безопасного периметра вокруг внутренней сети. Вместо этого Zero Trust использует подход, ориентированный на ресурсы, где каждый запрос на доступ проходит аутентификацию и авторизацию независимо от его происхождения. Эта модель

включает следующие ключевые элементы:

1. **Защита ресурсов вместо защиты периметра**:
   Фокус на защите критически важных ресурсов, таких как конфиденциальные данные и инфраструктурные компоненты, а не на устранении всех уязвимостей в сети.
2. **Микросегментация**:
   Разделение корпоративной среды на небольшие узлы с уникальными политиками безопасности и контролем доступа. Это ограничивает распространение угроз и усиливает защиту конкретных ресурсов.
3. **Принцип минимальных привилегий**:
   Доступ предоставляется только в рамках задач, что минимизирует ущерб от скомпрометированных учетных данных.
4. **Аутентификация**:
   Каждый пользователь, устройство и приложение должны проходить проверку при любом запросе на доступ, рассматривая каждый запрос как потенциальную угрозу.
5. **Полный контроль и мониторинг**:
   Необходим постоянный мониторинг устройств, приложений и взаимодействий для выявления аномалий и предотвращения угроз.

Преимущества модели Zero Trust

Реализация Zero Trust усиливает защиту от утечек данных, упрощает адаптацию к изменениям в компании и обеспечивает надежную безопасность как в физической (on-premise), так и в облачной среде (cloud-based).

Расширение модели Zero Trust на корпоративную коммуникацию

Уязвимости внутренней коммуникации

Внутренняя коммуникация часто воспринимается как безопасный и внутренний процесс, в рамках которого сотрудники могут свободно обсуждать вопросы, которые, возможно, не полностью соответствуют требованиям применимого законодательства, исходя из предположения, что эта информация останется внутренней и никогда не станет достоянием общественности. Однако это заблуждение, учитывая как минимум следующие риски:

- **Судебные процессы**: внутренняя переписка может быть использована в качестве доказательств в суде, что приведет к раскрытию переписки.
- **Кибератаки**: утечка данных может произойти через взлом коммуникационных систем , нанося вред репутации компании.
- **Недоброжелательные сотрудники**: уволенные сотрудники могут использовать внутреннюю переписку для нанесения ущерба компании.

Применение принципов Zero Trust к коммуникации

Для минимизации этих рисков рекомендуется внедрить стратегию, основанную на принципах Zero Trust:

1. **Формирование осведомленности и ответственности**:
   Обучение сотрудников осознанию рисков раскрытия информации способствует созданию культуры осмотрительности в переписке.
2. **Ограничение доступа к конфиденциальной информации**:
   Доступ предоставляется только тем, кто непосредственно вовлечён в процесс, что снижает риск утечек.
3. **Аутентификация и шифрование сообщений**:
   Использование защищённых платформ связи с шифрованием и строгой проверкой идентификации.
4. **Мониторинг и аудит каналов связи**:
   Применение инструментов для анализа коммуникации позволяет своевременно выявлять угрозы.
5. **Разработка чётких политик**:
   Создание и внедрение правил, регулирующих обсуждение конфиденциальных тем.

Роль руководства в формировании культуры Zero Trust

Топ-менеджмент компаний играет ключевую роль в внедрении принципов Zero Trust. Привитие понимания того, что любая переписка может быть раскрыта, помогает сотрудникам формировать профессиональный подход к коммуникации.

Заключение

Помните «Денискины рассказы» советского писателя Виктора Драгунского? Все тайное становится явным! Вести коммуникацию нужно так, как будто она в любой момент времени может оказаться на столе прокурора.

В целом, модель Zero Trust предлагает инновационный подход к обеспечению безопасности корпоративной коммуникации. Считая каждую внутреннюю переписку потенциально уязвимой, компании могут снизить риски утечек данных и укрепить защиту своих интересов.
Внедрение Zero Trust в коммуникацию — это не только технический, но и стратегический вызов. Оно обеспечивает готовность организаций к непредвиденным ситуациям и защищает их репутацию в мире, где прозрачность становится новой нормой.

* * *

Этот материал предназначен для общей информации и не является юридической консультацией. Если вы хотите узнать больше о теме этой статьи или о практике нашей фирмы в области корпоративного права, свяжитесь с нами по адресу info@danilovpartners.ru.