КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

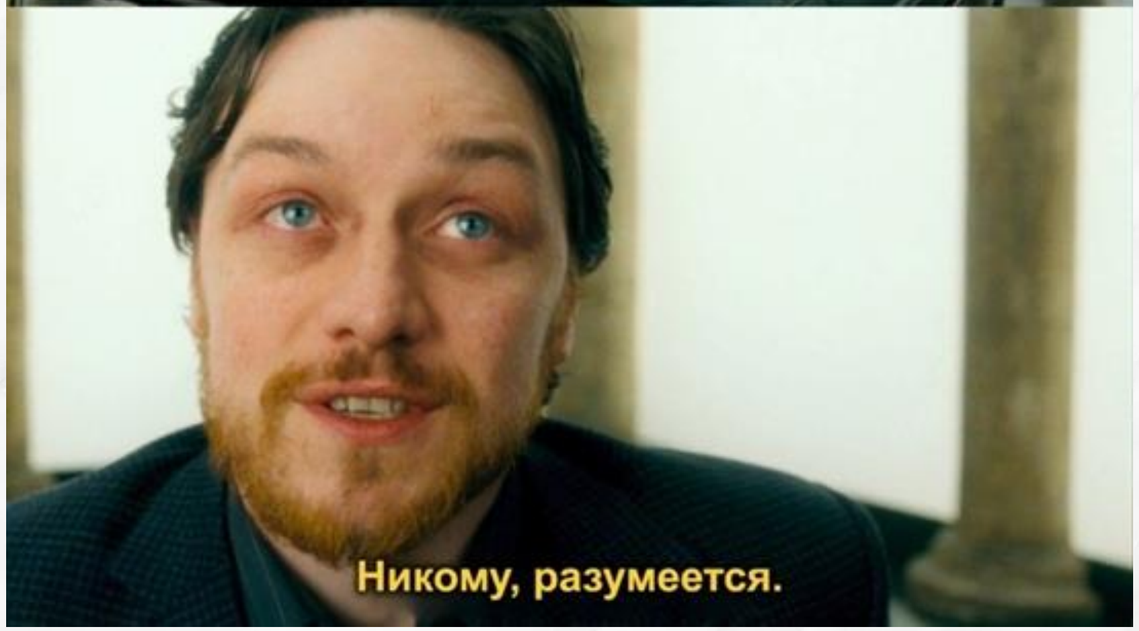
Zerotrust минимальными усилиями.

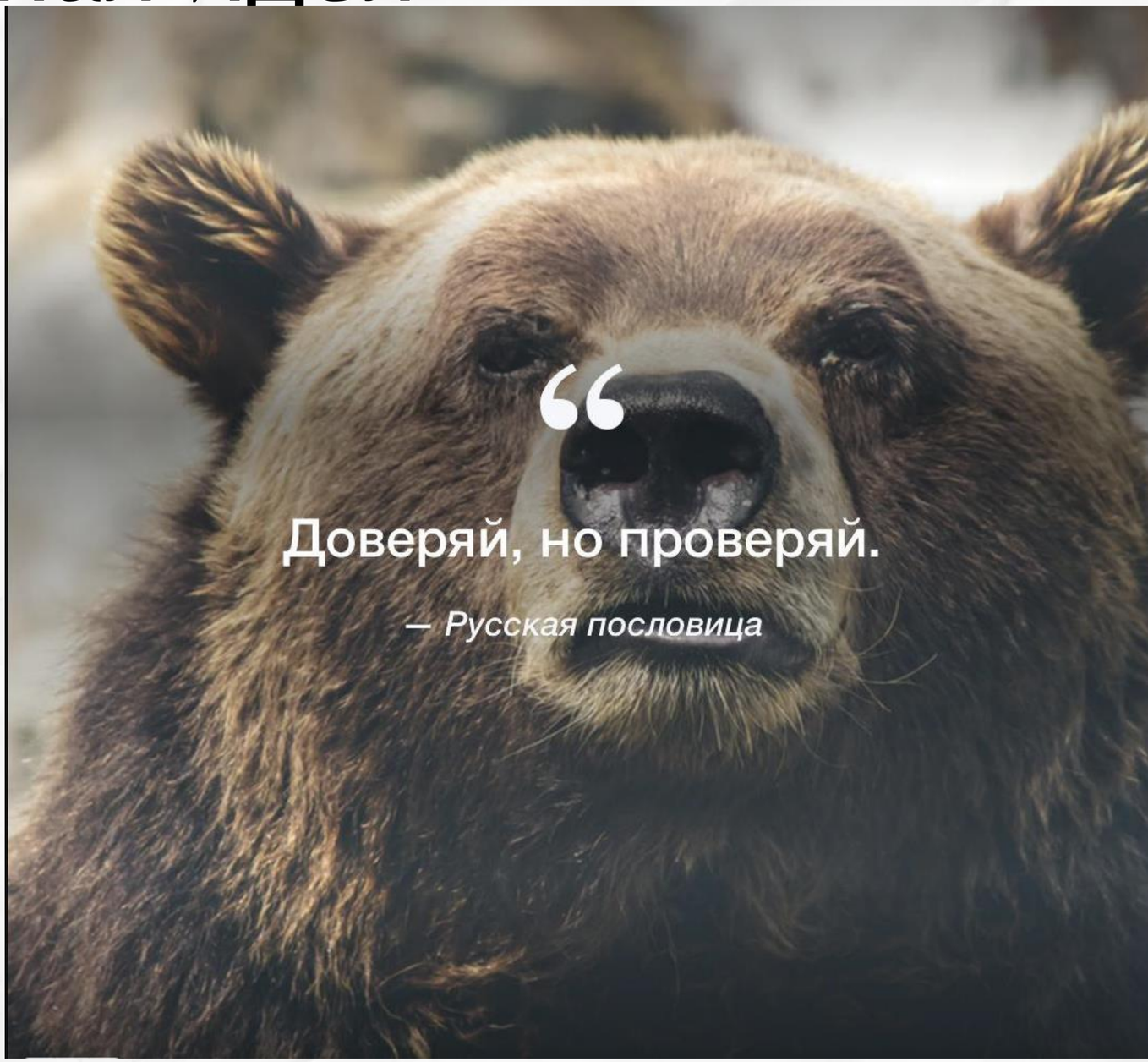
Бочкарев Антон «Третья Сторона»

ОБО МНЕ

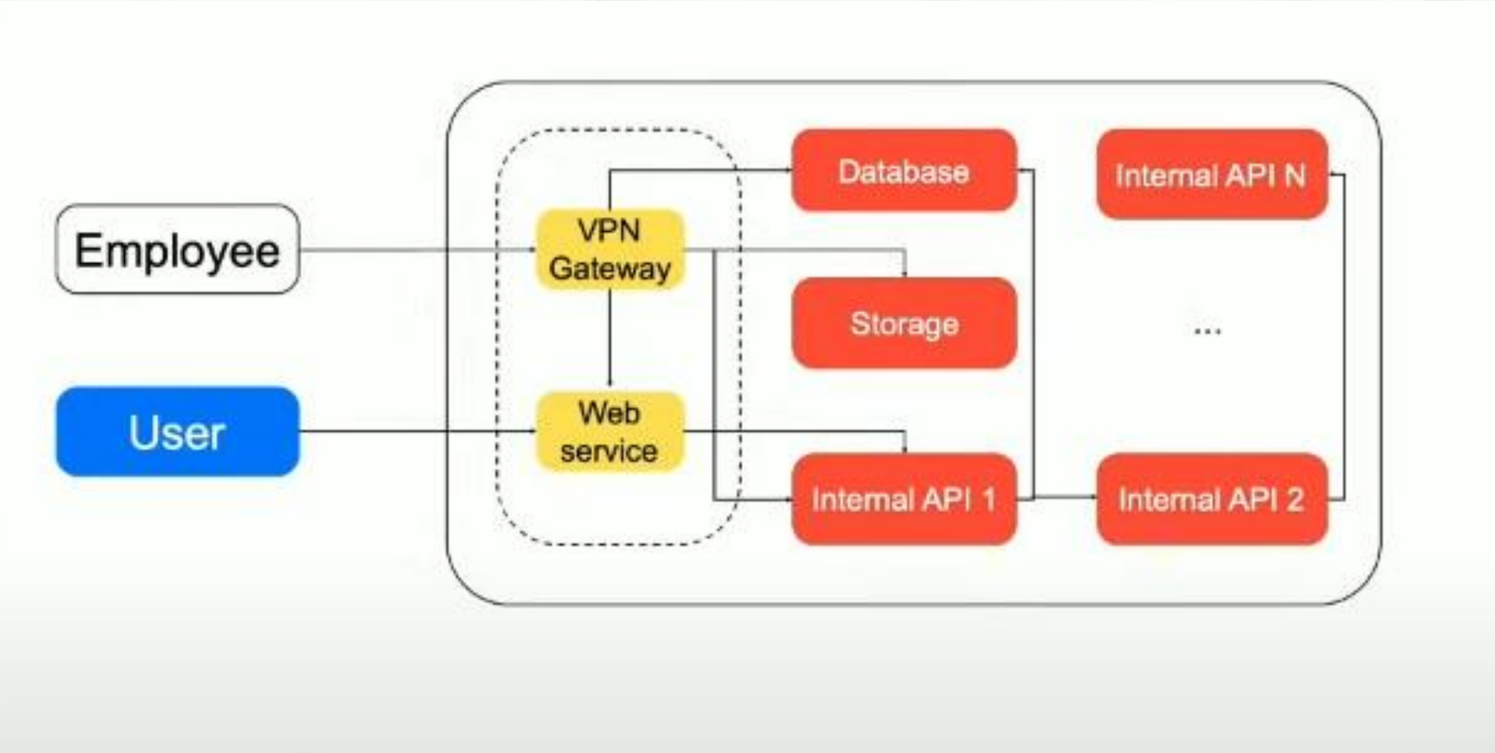
- 9 лет в атакующей безопасности.
- Ex JetInfosystems, Ex Bi.Zone, Ex Red Team Сибур.
- Спикер IT/ИБ конференций.
- Финалист CTF, участник «the Standoff».
- Популяризатор Информационной Безопасности.
- Сооснователь ИБ-стартапа «Третья сторона» 3side.org

Основная идея





Что мы привыкли видеть?



Zerotrust: «Нет доверенной сети, в каждом сегменте уже есть скомпрометированный хост»

Сроки

- К этой модели идут **годами**.
- Даже Google и Яндекс ее строили много лет. Откладывать старт можно бесконечно.
- Но с каждым пройденным этапом уровень вашей защищенности будет повышаться.
- Совершенно не нужно внедрять это одномоментно во всей компании.

Этап 0. Точка старта

- Определите критичные для бизнеса сегменты.
- Определите наиболее вероятно скомпрометированные сегменты.

Именно в таком порядке и в этих сегментах вам и нужно внедрять Zerotrust в первую очередь.

И лишь потом, во всех остальных. Точно также с точки зрения групп пользователей.

Возможно своими силами? Да.
Бюджет на аутсорс этапа? Минимальный.

Этап 1. Инвентаризация и identity

- Избавиться от «shadow it», ведь как мы может то, о чем не знаем?
- Облака инвентаризуются автоматически.
- Инвентаризация доступов, сведение к белому списку и наименьшим привилегиям.

На инвентаризованные хосты устанавливаем железо-зависимые средства идентификации.

Самый простой способ - сертификаты в hardware storage.

Не идентифицированные устройства – не имеют доступа к сети.

Возможно своими силами? Да.
Бюджет на аутсорс этапа? Минимальный.

Этап 2. Сильная аутентификация

- Singe Sign ON (SSO) – обязательное требование для Zerotrust сегмента.
- Многофакторная аутентификация (MFA).
- Короткие сессии, в зависимости от важности сервиса.

Что дает SSO?

- Пользователь привыкает вводить пароль только там.
- Управляем политикой доступа в одном месте.
- Упрощаем блокировку и отзыв доступов.

Что важно для MFA?

- Удобство.
- Без передачи пользователю «резервных данных».

Возможно своими силами? Да, но не всегда рентабельно.
Бюджет на аутсорс этапа? Средний, стоит передать на аутсорс.

Этап 3. Менеджмент секретов

Идеальные секреты:

- Короткоживущие.
- Легко ротируемые.
- Легко детектируемые.

Токены – специального формата.

Вместо паролей – сертификаты.

Возможно своими силами? Да.
Бюджет на аутсорс этапа? Низкий, можно передать на аутсорс.

Этап 4. Зашита конечных устройств

Compliance устройств:

- Средства защиты (от AB до DLP).
- Контроль обновлений.
- Шифрование.
- Постоянный мониторинг.

Доступ только с контролируемых устройств, ведь если вы не контролируете устройство, как вы можете ему доверять?

Возможно своими силами? Да, со значительным противодействием.
Бюджет на аутсорс этапа? Средний.

Этап 5. Вводим дополнительные атрибуты контроля

Принимаем решение о дополнительных проверках/ограничениях/блокировках, исходя из дополнительных атрибутов.

Например, используя Identity Aware Proxy, оцениваем:

- Тип устройства, геолокацию IP, время подключения.
- Проверяем на аномалии в запросах, действиях.

Возможно своими силами? Сложно.
Бюджет на аутсорс этапа? Средний.

Этап 6. Анализ кода стороннего ПО.

- Проверка на вредоносный, небезопасный код в репозиториях.
- Внедрение пайплайнов со статистическими/динамическими проверками кода, на безопасность.
- Обязательная подпись кода, в идеале «из коробки».

Возможно своими силами? Сложно.
Бюджет на аутсорс этапа? Высокий.

Этап 7. ZeroTrust Production.

- Ограничения на любые изменения в production среде.
- Система двойной проверки при внесении изменений.

Например, ежедневно сменяемый «дежурный», подтверждающий любые изменения в production среде.

Возможно своими силами? Да, со значительным противодействием.
Бюджет на аутсорс этапа? Средний.

Комментарии

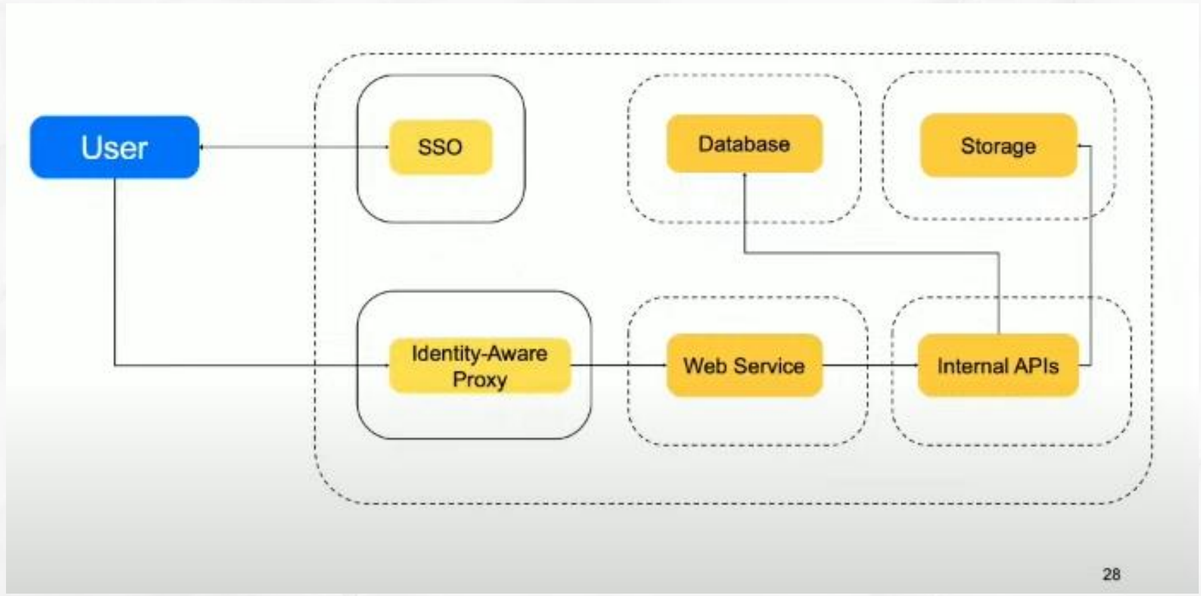
- Противодействие. Zerotrust это множество усложнений и «закручивание гаек», оно всегда вызывает противодействие, особенно привилегированных пользователей. Особенно этап контроля конечных устройств.

- Это итеративный процесс, от сегмента к сегменту, от группы пользователей к следующей группе. Старайтесь ставить себе как можно более короткие цели.

- Это не исчерпывающий список этапов. Например, создание/подключение полноценного SOC выходит за рамки доклада, но необходимо на поздних этапах. Также как и более гибкое управление доступом к данным.

Что же даст постепенное внедрение Zerotrust?

- Снижение рисков.
- Повышение уровня реагирования на инциденты.
- Упрощение расследований.
- Снижение роли человеческого фактора.



Заключение

- Вы не первые пойдете по этому пути. Используйте рекомендации тех, кто впереди.

- Практически все из этого возможно построить на открытом ПО, но это чаще всего не рентабельно. Не нужно проходить путь вендора ИБ-решений.

- Практически все из этого возможно построить своими силами, но нужна ли вам такая команда на постоянной основе? Разовый аутсорс-проект часто и дешевле, и эффективнее.

- *«Если вы думаете, что безопасность вам не нужна, подумайте еще!»* ChatGPT.

Спасибо за внимание!

Готов ответить на ваши вопросы.

Бочкарев Антон Дмитриевич
E-mail: adb@3side.org
TG: @TG_3side
3side.org