Пентест ДБО: насколько хорош ваш антифрод?

Тимур Юнусов

Руководитель отдела

анализа защищенности банковских систем

POSITIVE TECHNOLOGIES

ptsecurity.com

Обо мне

POSITIVE TECHNOLOGIES

- Анализ защищенности приложений с 2009
- Анализ защищенности банковских систем с 2012
- Только практическая безопасность

- …Из года в год одна и та же история
- Новые направления: автоматизация безопасности банковских систем: ДБО, ATM, POS, антифрод

http://uk.linkedin.com/in/tyunusov

Антифрод системы

POSITIVE TECHNOLOGIES

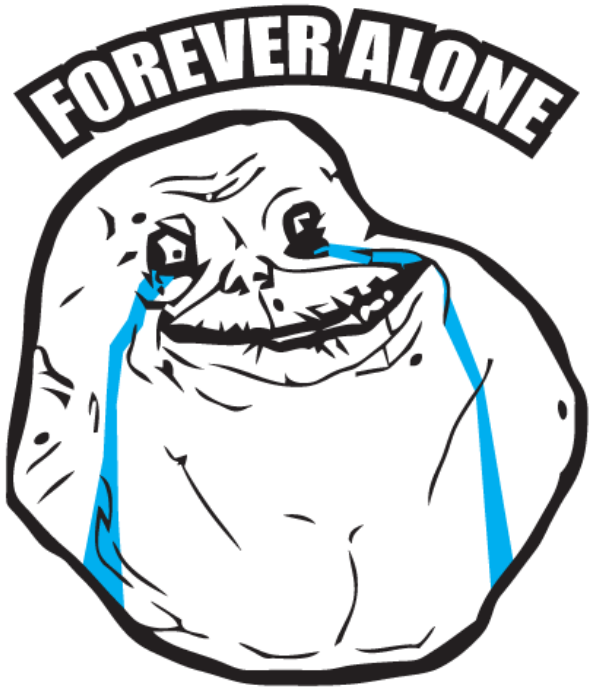
- Часто делаются на основе SIEM
- В 90% случаев уходят на ручную валидацию
- Настроены для защиты от хищений у клиентов
- Ошибки 2 рода – недопустимы

Антифрод системы НЕ РАБОТАЮТ

POSITIVE TECHNOLOGIES

- 3 звонка за последние 5 лет из банка

- Когда дебет с кредитом не сходятся
- Или когда карту уже перевыпустили(



Антифрод кейс

- Bot-Trek
  - Еще нужно правильно настроить
  - Заточен под атаки на клиентов
- HTML5, AJAX, etc

Чеклист

POSITIVE TECHNOLOGIES

- Аутентификация
- Авторизация
- 2FA
- Бизнес-процессы
- Атаки на клиентов
- Пентест

Аутентификация

POSITIVE TECHNOLOGIES

- Брутфорс учетных данных
  - Ввод 2 паролей из 3 и новый запрос
  - Запросы с разных IP
  - Авторазблокировка

- Брутфорс PAN/CVV/EXP DATE

Аутентификация

POSITIVE TECHNOLOGIES

- Регистрация по PAN/кодовому слову/etc
  - Регистрация по PAN
  - Восстановление пароля по PAN/EXP DATE

Аутентификация

POSITIVE TECHNOLOGIES

- Сторонние каналы (боты, авторизация по FB, etc)
  - Telegram API – не панацея
  - В OAuth есть очень много недостатков
  - Нужно подключать отдельный источник в антифрод

Аутентификация

POSITIVE TECHNOLOGIES

- Брутфорс 2фа – «Угнать за 120 секунд»
  - ОТП 4 символа
  - 120 секунд время жизни
  - Сколько угодно транзакций в этом окне
- Мобильный банк – мой любимый

- Брутфорс 2фа – «Угнать за 120 секунд»
  - ОТП 4 символа
  - 120 секунд время жизни
  - Сколько угодно транзакций в этом окне
  - 1000 транзакций за 30 секунд
  - 3000 попыток за 90 секунд
  - ~30%

- Мобильный банк – мой любимый
  - /auth?step=1&login=&password=
  - /auth?step=2&password=OTP

- Брутфорс 2фа – «Угнать за 120 секунд»
  - ОТП 4 символа
  - 120 секунд время жизни
  - Сколько угодно транзакций в этом окне
  - 1000 транзакций за 30 секунд
  - 3000 попыток за 90 секунд
  - ~30%

- Мобильный банк – мой любимый
  - /auth?step=1&login=&password=
  - /auth?step=2&password=OTP
  - **/auth?step=2&login=&password**

Решение

POSITIVE TECHNOLOGIES

- Скоринг попыток одинаковых действий с фейлом
- Временная блокировка по всем каналам
- Цель – учетка, а не сессия (логаут всех текущих сессий)
- Подключение всех событий в источники – регистрация идентификация авторизация и т.д.
- Модели машинного обучения

Авторизация

POSITIVE TECHNOLOGIES

- Шаблоны в мобильном банке – вечная боль

```
POST /pay HTTP/1.1
Host: bank

{"amount":100,"templateId":"393141","accountFrom":“xxxx81039xxxx028","
methodName":"createPayment"}
```

Решение

POSITIVE TECHNOLOGIES

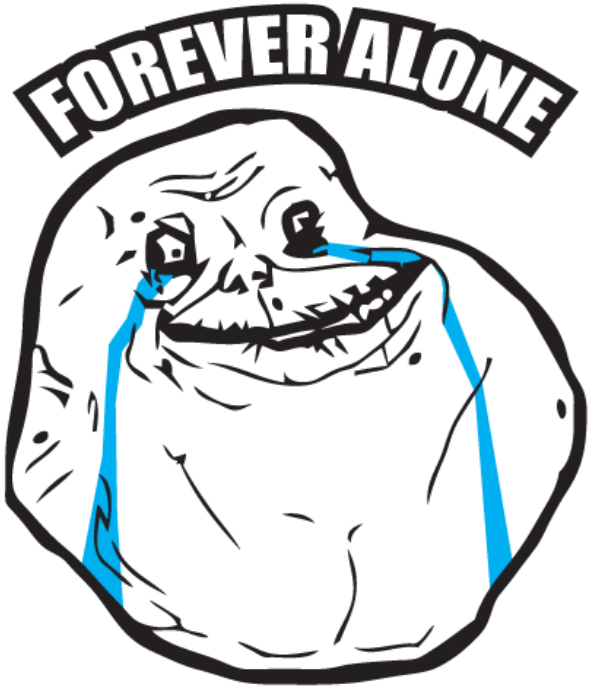
- Прописать все ACL
  - WAF с доступом в backend
  - DBF
- Нарушение ACL – блок.
- ACL в антифроде

Решение

- Правильно настраивать «умные машины»

- Limits
- Округление

- 3 звонка за последние 5 лет из банка
- Перевели $0.1 100 раз? Ну и ладно



Решение

POSITIVE TECHNOLOGIES

- Ручные действия не исключают автоматические
- Детект «аномалий». За профилированием будущее.

Атаки на клиентов

POSITIVE TECHNOLOGIES

- XSS
  - Информативность смс страдает
- CSRF
- ClickJacking
- Контроль последовательности событий
- Контроль автоматических действий
  - CARD2CARD

Решение

POSITIVE TECHNOLOGIES

- Детект «аномалий»
- Детект автоматических действий

Внутренний нарушитель

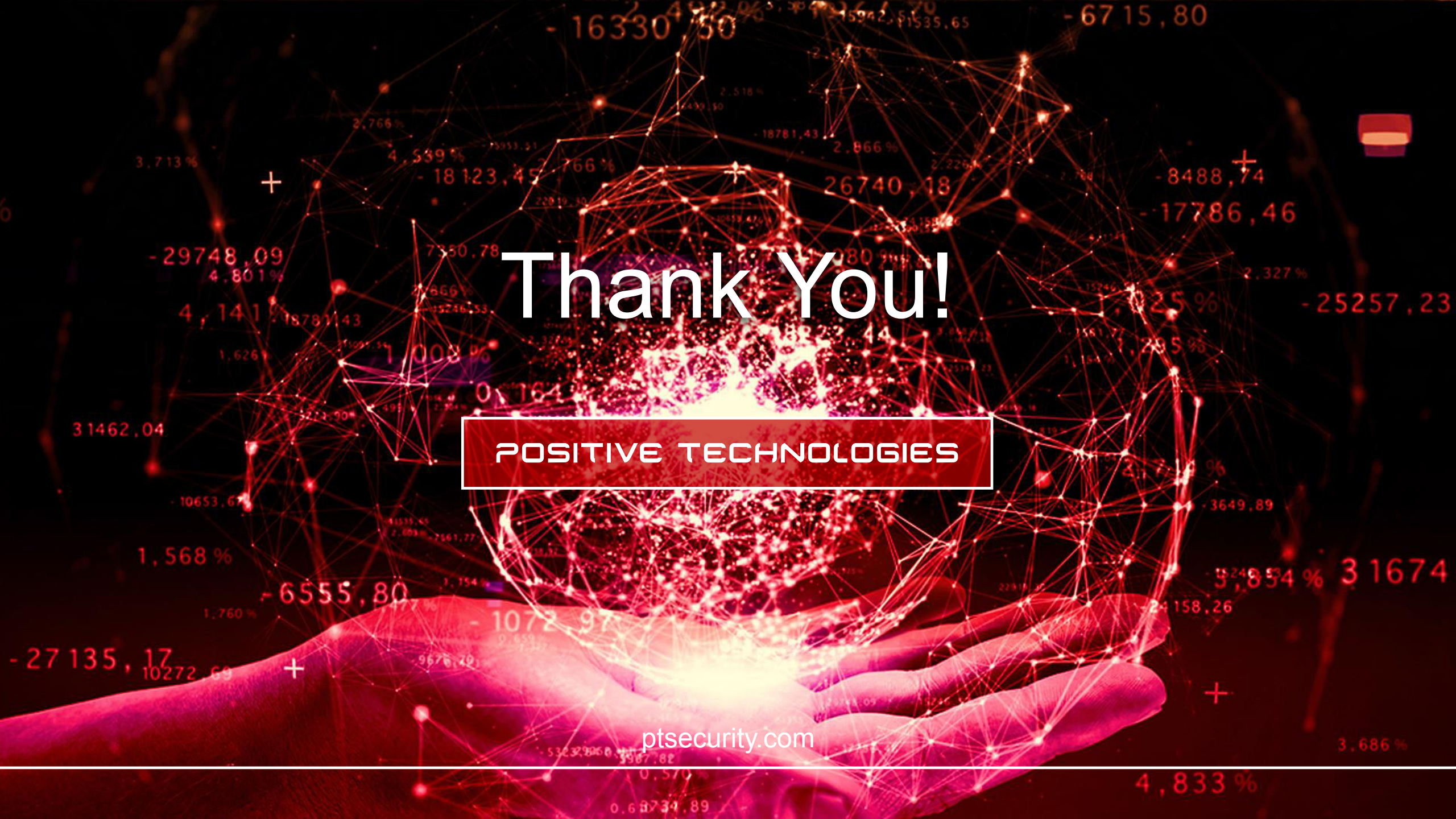
POSITIVE TECHNOLOGIES

- Доступ в СУБД
- Доступ в АБС
- Доступ в процессинг
- Доступ к ядру антифрода

Решение

POSITIVE TECHNOLOGIES

- Детект «аномалий»
- «Самозащита»
- Периметр и регулярные пентесты, социалка


Thank You!
POSITIVE TECHNOLOGIES
ptsecurity.com