Сколько стоит вас взломать?

Антон Бочкарев
CEO/Founder «Третья сторона»
3side/4security

[adb@3side.org | t.me/TG_3side]

О спикере

- 10 лет в кибербезе (Pentest, RedTeam, vCISO)
- Сооснователь стартапа «Третья сторона»
- Член Экспертного Совета Кибериспытаний
- Один из создателей методики Кибериспытаний
- Веду TG-канал «3side кибербезопасности»

[Как оценивали защищённость?

- [Сканирование на уязвимости
- [Тестирование на проникновение
- [Аудит защищенности
- [RedTeam/PurpleTeam
- [BugBounty

Сканирование на уязвимости

Недостатки:

- Низкая точность
- Нет проверки логики
- Проверяем только, что указали

Главная проблема – оценка не человеком.

Тестирование на проникновение

Недостатки:

- Нет противодействия
- Есть «послабления» от СЗИ
- Скоуп ограничен и в инфраструктуре и в методах.

Главная проблема – ограничения и «послабления».

Аудит защищенности

Недостатки:

- Что мы не знаем сами, не расскажем
- Нет практического аспекта
- Не все видно изнутри

Главная проблема – не практическая оценка.

RedTeam/PurpleTeam

Недостатки:

- От команды зависят методы
- Скоуп как правило фиксирован
- Слабая мотивация показать максимальный результат

Главная проблема – результат привязан к одной команде, к их сильным сторонам, методам и мотивации.

BugBounty

Недостатки:

- Нет глубины исследования
- Нет противодействия человека
- Сдаются отдельные баги, а не чейн атаки
- Иные проблемы организации

Главная проблема – результат привязан к одной команде, к их сильным сторонам, методам и мотивации.

Бизнес-ориентированная оценка

- Бизнес понимает, что взломать можно любую компанию
- Бизнес понимает свои недопустимые события (НС)
- Для бизнеса важно знать «А за сколько можно реализовать НС?»
- Именно для ответа на этот вопрос была написана методика Кибериспытаний!

Особенности Кибериспытаний

- Цель – показать возможность реализации Недопустимого События.
- Награда – уровня bug bounty за промежуточные успехи, и «большой куш» за НС.
- Полное противодействие Заказчика, обе стороны в равных условиях.
- Только независимое звено знает о ходе Кибериспытаний – Экспертный Совет.
- На данный момент проводится через площадку Standoff365.

Концепция «White as Black»

- Максимальное приближение к действиям злоумышленников.
- Отсутствие фиксированного скоупа.
- Карт бланш на социальную инженерию.
- Ключевое и практически единственное ограничение – УК РФ.
- Разрешено использовать «плоды труда» киберкриминала – покупать данные со стиллеров, доступы.

[Экспертный совет

- [Саморегулируемый независимый орган со сложным порогом входа.
- [Состоит из известных экспертов индустрии.
- [Проверяет условия КИ и отчеты о реализованных НС.
- [Участвует в улучшении методики КИ.
- [Защищает заказчика и исследователей от фальсификаций другой стороны.
- [Принимает решения о выплате вознаграждения.

Андрей Рогожкин

Тестирование на проникновение, Безопасность инфраструктуры, Безопасность АСУТП, OSCP, OSWE, CRTE

BI.ZONE, Информзащита

Антон Жаболенко

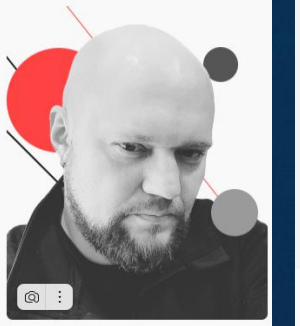
Преподаватель в МГУ и МФТИ, автор курсов по ИБ, ex. заместитель генерального директора в Wildberries, ex. директор департамента в VK, ex. Yandex

Positive Technologies, CPO

Азиз Алимов

Тестирование на проникновение, RedTeam, Безопасность приложений, CRT, CPSA, OSCP, OSCE, OSWE

Яндекс, BI.ZONE



Андрей Попов

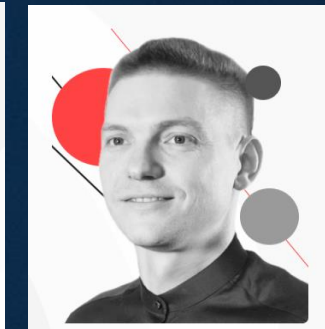
Тестирование на проникновение, RedTeam, Безопасность инфраструктуры, Безопасность беспроводной связи

SolidLab, Т-Банк, Открытие, ИнфоСистемы Джет

Антон Кузьмин

CTO

Innostage



Дмитрий Гадарь

CISO

Т-Банк

Что не делает Кибериспытание

- Не оценивает защищенность конкретного продукта/средства защиты/приложения.
- Не проверяет тестовые среды.
- Не показывает все уязвимости.

[Так для кого и что нужно?

[**Для крупных и зрелых с точки зрения кибербеза компаний – Кибериспытания.**

Так для кого и что нужно?

- **Для крупных, недостаточно зрелых с точки зрения кибербеза компаний – классические инструменты оценки защищенности.**
- **Для малых и средних предприятий, или компаний с ограниченным бюджетом:**
  - Доступные классические услуги через агрегатор «Третья сторона».
  - Комплексные и дешевые решения по кибербезопасности через 4security.
  - Релиз от 4security облачного решения по гарантированной защиты от последствий шифровальщиков – **ждите в мае**!

Спасибо за внимание!

Антон Бочкарев
CEO/Founder «Третья сторона»
3side/4security

@BY3SIDE