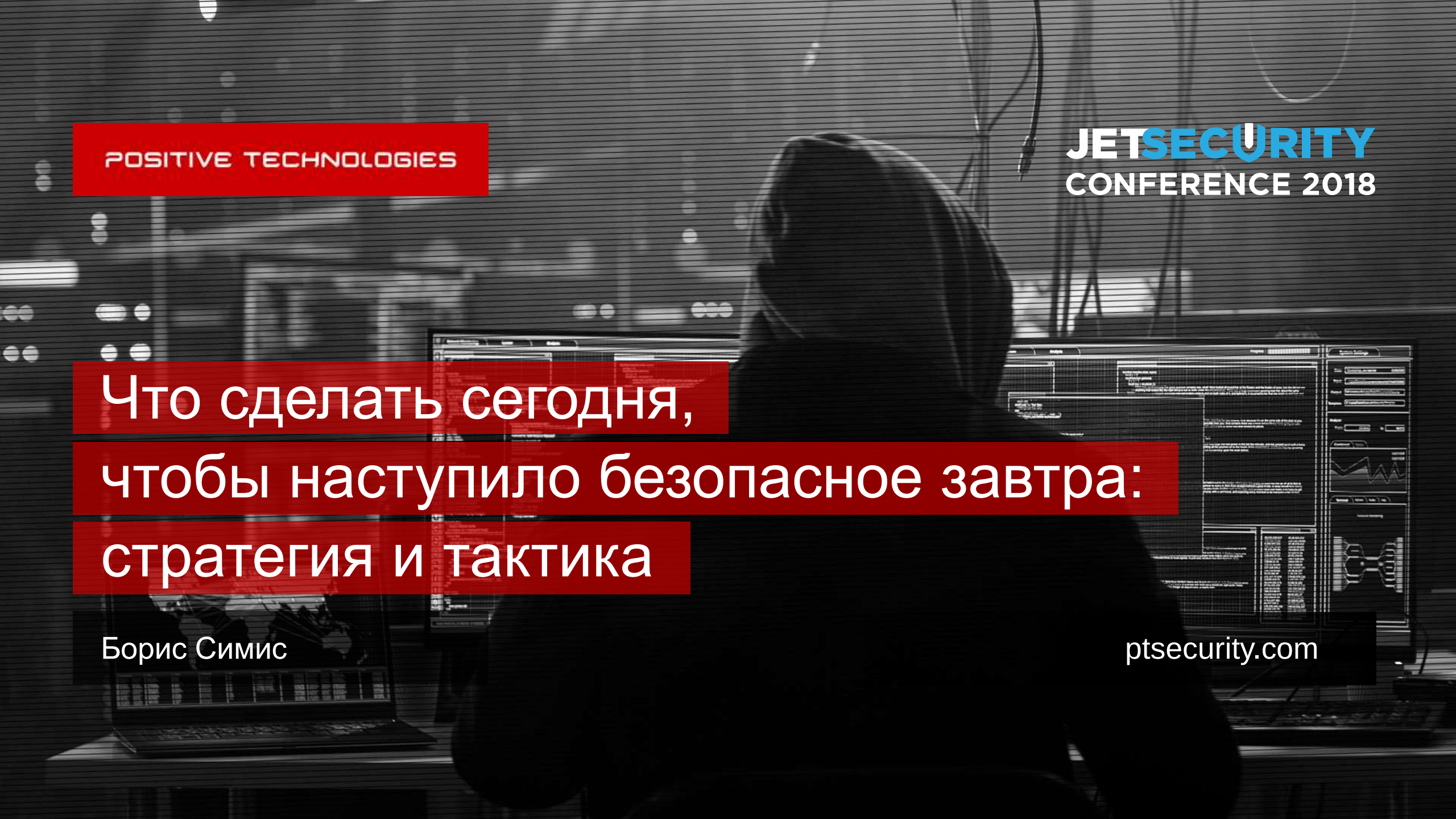
JETSECURITY
CONFERENCE 2018

IX ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ

31 мая, 2018
Radisson Resort, Zavidovo



POSITIVE TECHNOLOGIES

JETSECURITY
CONFERENCE 2018

Что сделать сегодня, чтобы наступило безопасное завтра: стратегия и тактика

Борис Симис

ptsecurity.com

Кто все эти люди и что они делают?

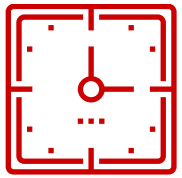
Статистика, полученная опытным путем

POSITIVE TECHNOLOGIES

Расследования VS Анализ защищенности

50% крупных организаций в 2017 году столкнулись с APT-атаками

9 из 10 случаев во время аудитов детектируется активность той или иной группировки



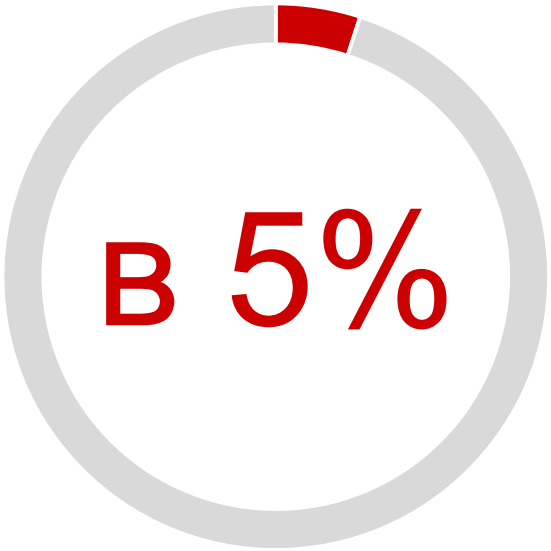
3 года в среднем киберпреступники присутствуют в захваченных информационных системах

100% получен полный контроль над ресурсами от лица внутреннего нарушителя

68% преодолен сетевой периметр извне с использованием социальной инженерии и атак на беспроводные сети

Есть ли кто-то на страже?

POSITIVE TECHNOLOGIES



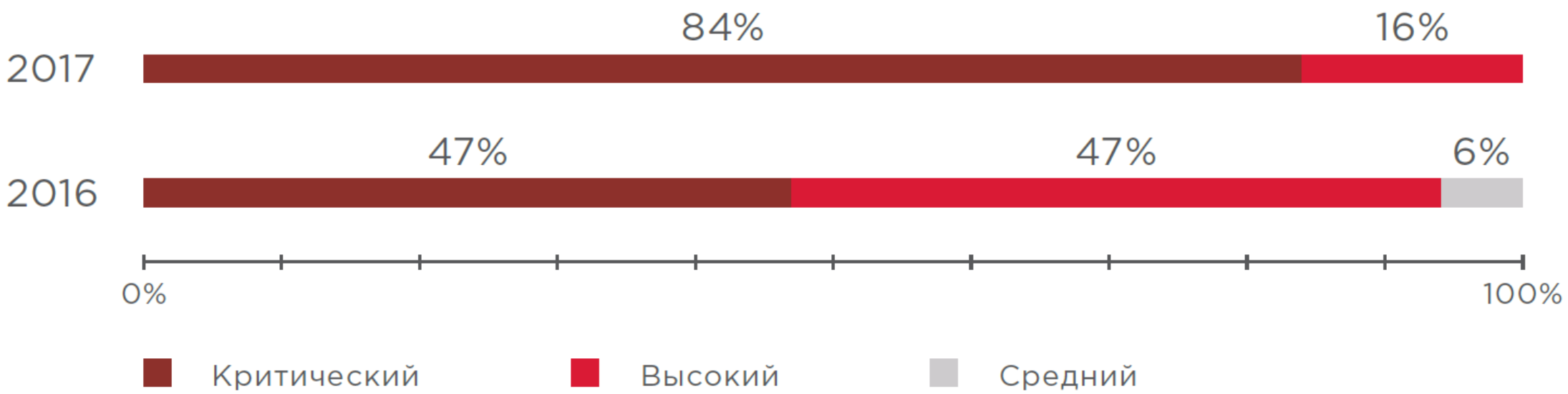
случаев наша активность
по тестированию компании
на безопасность была замечена

организаций
имели для этого
технические средства

JETSECURITY
CONFERENCE 2018

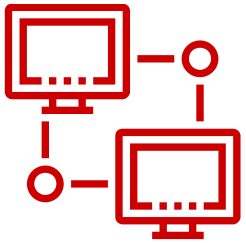
Уровень уязвимостей

POSITIVE TECHNOLOGIES



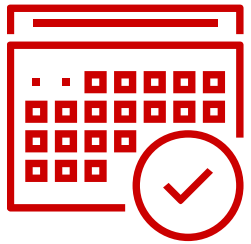
Доля систем по максимальному уровню опасности уязвимостей

Год прошел, а WannaCry все еще «жив»



в 60%

корпоративных систем обнаружена уязвимость MS17-010, которая используется в атаке шифровальщика WannaCry и NotPetya



3–5 дней

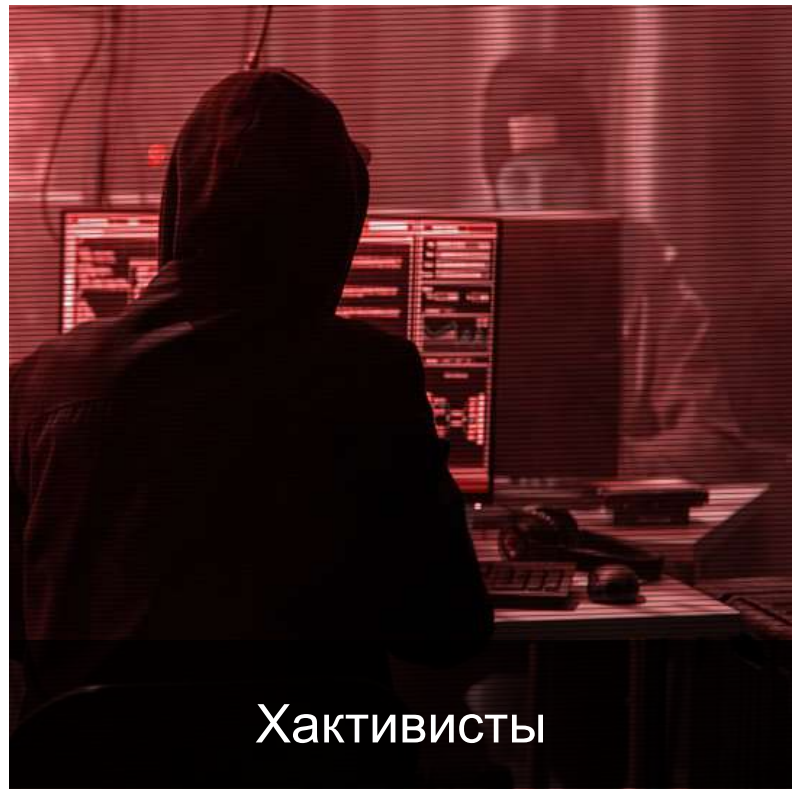
нужно для того, чтобы новый эксплойт начал активно использоваться для атак

Захватчик: кто он и что ему нужно?

POSITIVE TECHNOLOGIES

Промышленный шпионаж

State-sponsored group



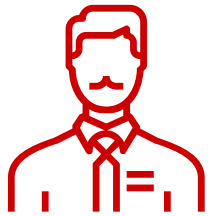
Хактивисты

… или просто захватить сеть.

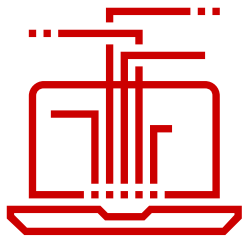
Любую. Чтобы было.

JETSECURITY CONFERENCE 2018

Два основных вектора атак



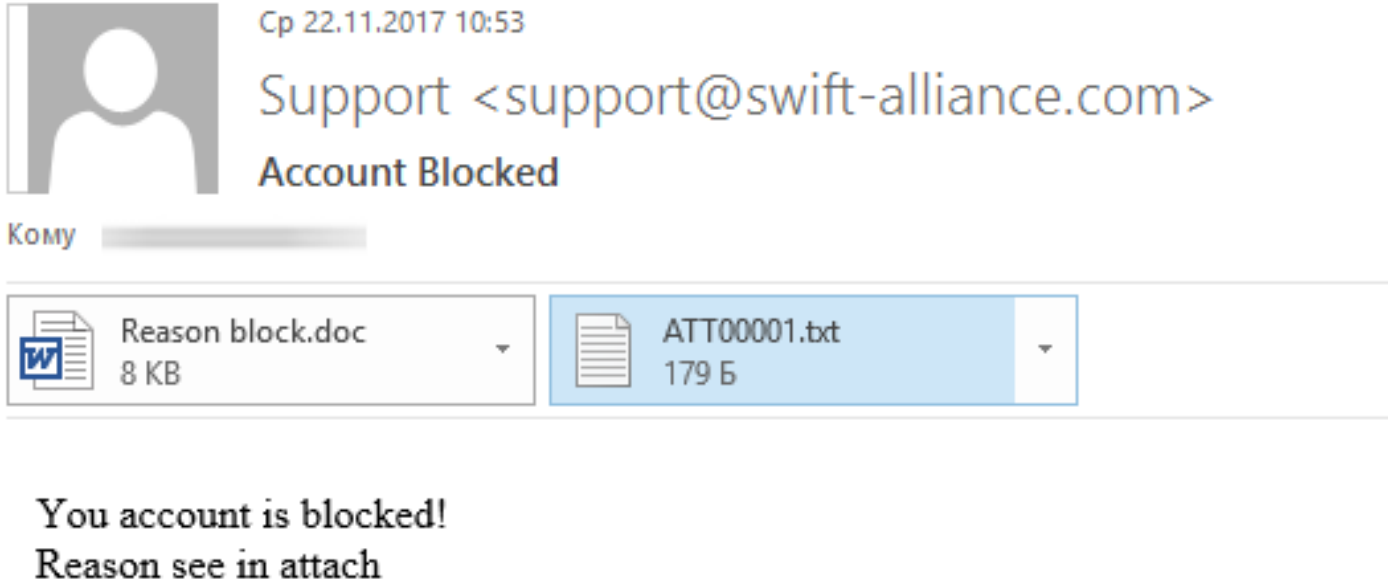
Через социальную инженерию
(письма, флэшки, ссылки)



Через взлом внешнего периметра
(web, роутеры, инфраструктура)

Взлом через социальную инженерию

POSITIVE TECHNOLOGIES

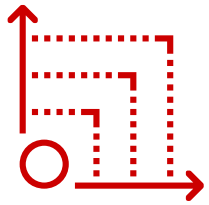


JETSECURITY CONFERENCE 2018

Атаки — сложнее, инструменты — технологичнее

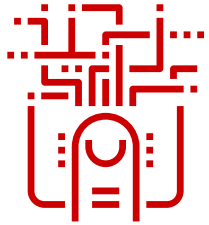
POSITIVE TECHNOLOGIES

Бесфайловые атаки



Анти-форенсика

ВПО, подписанное цифровой подписью



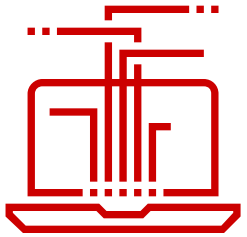
Анти-атрибуция

Уязвимости нулевого дня

Анти-анализ

… дешево и надежно для хакера

POSITIVE TECHNOLOGIES

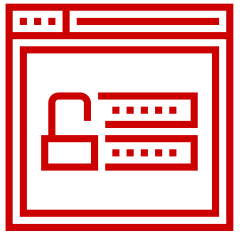


Дырявый периметр

- В 55% случаев внешний нарушитель может получить полный контроль над инфраструктурой
- Нарушителю нужно всего два шага для проникновения внутрь

Необновленное ПО

- В 91% исследованных случаев используются уязвимые версии ПО
- Возраст не установленных обновлений — 108 месяцев (9 лет!)



Слабые пароли

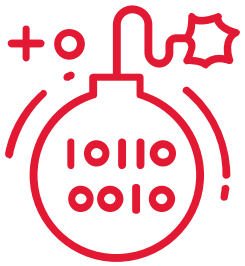
- Во всех обследованных нами системах использовались словарные пароли

Границы периметра: сканируем и видим

POSITIVE TECHNOLOGIES

23%

компаний
не знают свой
сетевой периметр



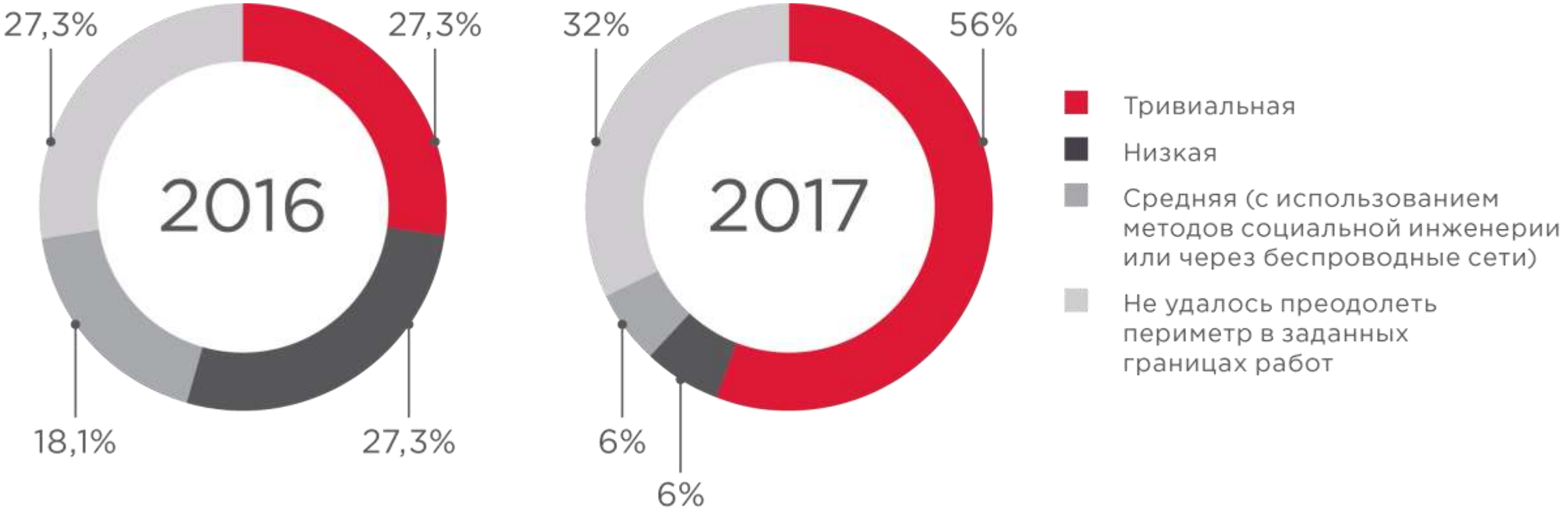
Для 6%

уязвимостей есть
общедоступный
эксплойт

наибольшее число
уязвимостей выявлено
в веб-приложениях
и службах удаленного
доступа (SSH)

Сложность преодоления

POSITIVE TECHNOLOGIES

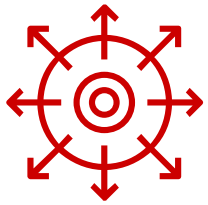


В 2017 году тривиальная сложность получения доступа к ресурсам ЛВС выросла **с 27%** до **56%** по сравнению с 2016 годом.

Научиться адресно защищаться

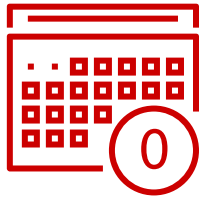
POSITIVE TECHNOLOGIES

Взлом



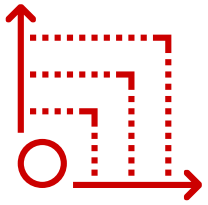
0-day,
от $100 тыс.

Известная уязвимость,
от $500 до 20 тыс.

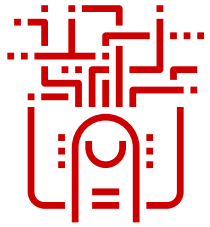


Детский сад WannaCry

Защита



Почти нет,
более $1 млн



Обновлять ПО
(ОС, офис, браузеры,
плагины) + AV

Порядок на внешнем
периметре

План действий

POSITIVE TECHNOLOGIES

По защите от взлома

Максимально усложнить атаку
и повысить ее стоимость

- Вычистив внешний периметр
- Устраняя внутри хотя бы известные уязвимости
- Проводя тренинги персонала

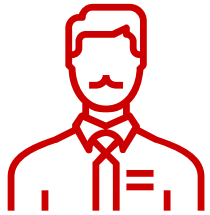
По выявлению взлома

Снизить время нахождения
злоумышленника в сети

- Обнаруживая взломанные узлы
- Проводя ретроспективный анализ
- Готовясь быть взломанным

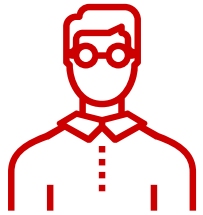
Что делать руководителю службы ИБ и инженеру?

POSITIVE TECHNOLOGIES



Руководитель службы ИБ должен

- Знать о еженедельных изменениях внешнего периметра
- Иметь регламент действий в случае взлома
- Осознавать, что узнать, что ты взломан, лучше самому
- Понимать реальную политику обновления ИТ-систем



Инженеру необходимо

- Думать, как хакер
- Постоянно образовываться (подписки, твиттеры, каналы, конференции)
- Понимать аномалии трафика, процессов

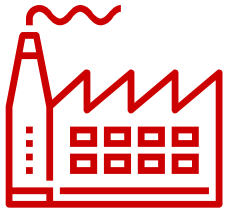
Что делать предприятиям и ведомствам?

POSITIVE TECHNOLOGIES

Предприятиям и ведомствам необходимо

- Строить SOC и выстраивать реальные процессы практической безопасности
- Регулярно проводить аудиты, пентесты, учения и тренировки
- Проводить независимую оценку уровня своей защищенности
- Полноценно расследовать инциденты, а не «гасить» симптомы
- Растить компетенции внутри компании несмотря на сложности

Что должны делать производители?



Производители должны

- Изучать техники и тактики нападающих и привносить эту экспертизу в свои продукты
- No marketing bullshit

Что делать государству?

Государству необходимо

- Популяризировать принципы реальной безопасности
- Продолжать развитие нормативной базы для средств мониторинга и защиты (песочниц, SIEM, COA/COB)
- Развивать построение системы ГосСОПКА

Не стоит прятать голову в песок

2000
Мы знаем, что нужно строить системы защиты

2010
Мы знаем, что нас могут взломать

2018
Мы знаем, что мы взломаны

2020
Не поздно ли уже интересоваться, где и кем мы взломаны?

JETSECURITY
CONFERENCE 2018

JETSECURITY
CONFERENCE 2018

Спасибо за внимание!

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ