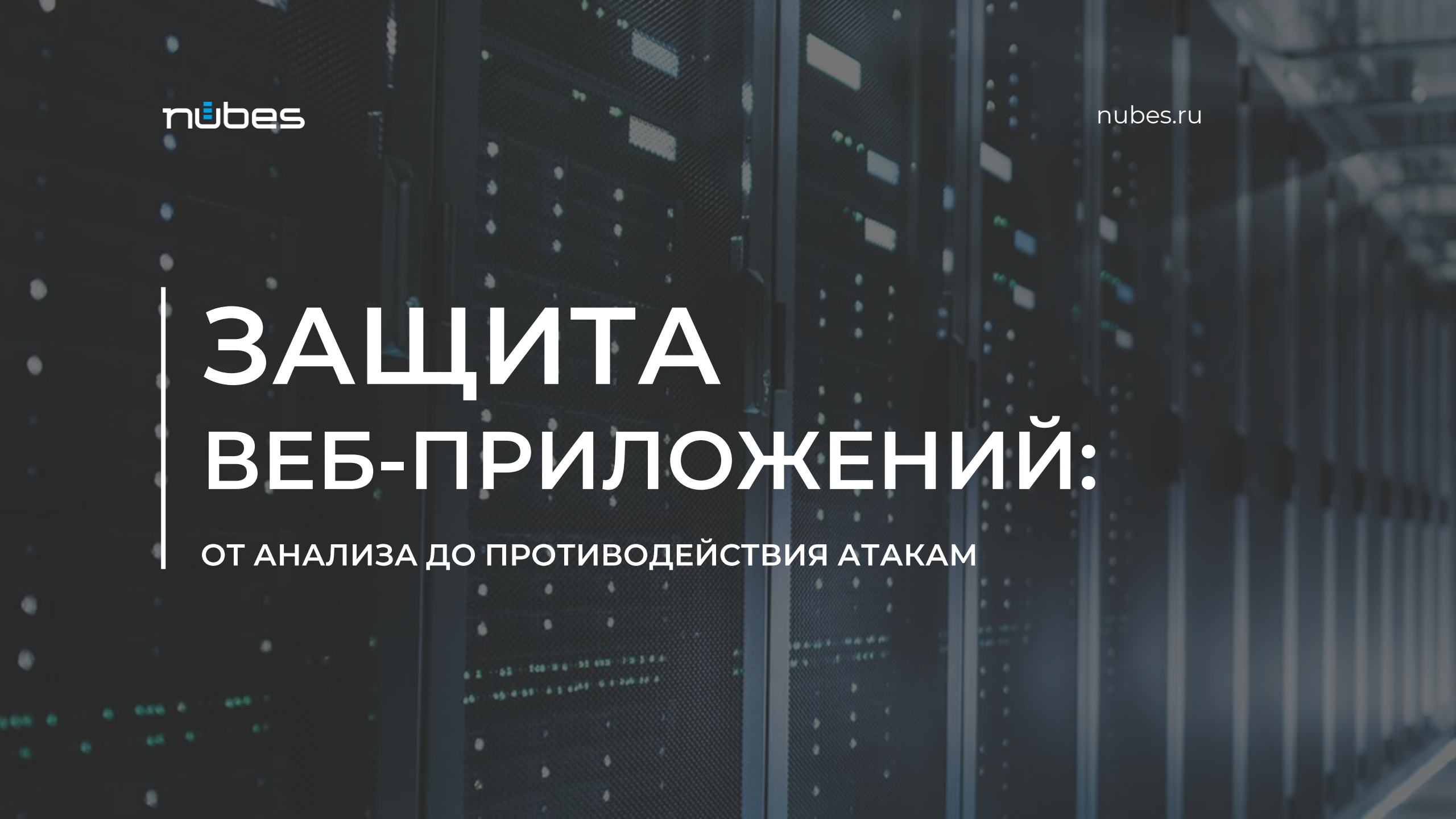


nubes

nubes.ru

ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ:

ОТ АНАЛИЗА ДО ПРОТИВОДЕЙСТВИЯ АТАКАМ

ПРЕЖДЕ ЧЕМ НАЧНЕМ

- Задавайте вопросы в чат.
  Ответим на них в конце выступления.
- Если нет звука или картинки,
  попробуйте перезайти в другом браузере.
- Презентацию и запись вышлем
  на почту всем участникам.

ОТСЛЕЖИВАЕТЕ ЛИ ВЫ АТАКИ НА СВОИ ВЕБ-ПРИЛОЖЕНИЯ?

nübes

Александр Быков

руководитель направления сервисов защиты Nubes

- **5 лет** в ИБ;
- **Руководил созданием ИБ-сервисов** по защите веб-приложений в крупнейшем облачном провайдере;
- **Большой опыт по защите** высоконагруженных приложений от комплексных атак (WAF, IDM, AntiDDoS, сканеры уязвимостей);
- **Сертифицированный ИБ-инженер** Check Point, Fortinet, Safenet, PT.

nübes

NUBES

ОБЛАКА. ИБ. ДАТА-ЦЕНТРЫ

ИБ-сервисы по модели подписки:

- WAF
- NGFW
- AntiDDoS
- MFA

Защищенное облако NGcloud:

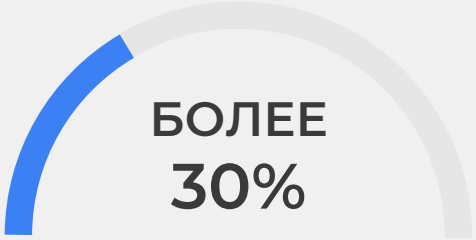
- аттестат 152-ФЗ (УЗ-1)
- встроенная защита DDoS
- регулярное сканирование
- поддержка GPU

Дата-центр Tier III:

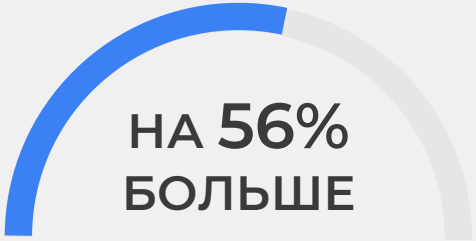
собственная площадка в Москве

nübes

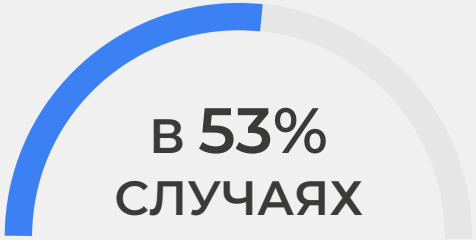
КАК АТАКУЮТ ВЕБ-ПРИЛОЖЕНИЯ: 2022



от общего количества киберинцидентов – это атаки через веб-приложения



число успешных атак



инциденты приводили к прерыванию бизнес-процессов

Самые популярные методы атак:

- межсайтовый скриптинг (или XSS)
- SQL-инъекции
- Брутфорс
- DDoS

Источник: Positive Technologies, 2023

nubes

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ВЕБ-ПРИЛОЖЕНИЯ

определяем объекты защиты

оцениваем риски (уязвимости)

купируем риски

ШАГ 1.

ОПРЕДЕЛЯЕМ, ЧТО ЗАЩИЩАЕМ

nübes

nübes

ОПРЕДЕЛЯЕМ, ЧТО ЗАЩИЩАЕМ

СОСТАВЛЯЕМ КАРТУ ДОМЕНОВ

DNSdumpster, Amass
SubGPT (AI)

ИЗУЧАЕМ ИСТОРИЮ DNS

dnshistory, wayback machine

ПРОВЕРЯЕМ НА СПАМ И MALWARE

DNSBL-списки, VirusTotal

ИЩЕМ ДВОЙНИКОВ (ФИШИНГ)

DNStwister, IDN checker

ИЩЕМ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ В КОДЕ

GIT, Google

ИЩЕМ «ЛЕВЫЕ» TLS СЕРТИФИКАТЫ

crt.sh

БОЛЬШЕ ИНСТРУМЕНТОВ ТУТ

ШАГ 2.

ОЦЕНИВАЕМ РИСКИ И ИЩЕМ УЯЗВИМОСТИ

nübes

nübes

ШАГ 2.

ОЦЕНИВАЕМ РИСКИ И ИЩЕМ УЯЗВИМОСТИ

01 Оцениваем важность найденных приложений: делим на категории по критичности

02 Сканируем инфраструктуру: закрываем “лишние” публикации

03 Сканируем приложение (DAST)

04 Сканируем код (SAST)

nübes

ШАГ 2.

ОЦЕНИВАЕМ РИСКИ (УЯЗВИМОСТИ)

01

Узнаем, какие уязвимости известны всем

Инструменты: Shodan и Censys

02

Сканируем инфраструктуру:

Open-source: nmap, OpenVAS, Nebula (AI)
Коммерческие: Vulners, Xspider, Сканер-ВС, MaxPatrol 8,

03

Сканируем WEB:

Open-source: ZAP, Nuclei, Nikto, Nebula (AI), DirBuster
Коммерческие: Burp Suite

04

Сканируем код на уязвимости

Open-source: GitHub Advanced Security, OWASP ASST, OWASP Code Crawler, OWASP WAP, SourceGPT (AI)

ШАГ 3.

КУПИРУЕМ РИСКИ

nübes

nubes

АТАКИ НА ВЕБ-ПРИЛОЖЕНИЯ С ТОЧКИ ЗРЕНИЯ РИСКОВ

Недоступность приложения

DDoS-атаки

Кража контента (web scraping)

атаки ботов

Компрометация приложения

эксплуатация уязвимостей

nübes

НЕДОСТУПНОСТЬ СЕРВИСА ИЗ-ЗА DDOS-АТАКИ: ЧТО МОЖНО ПРЕДПРИНЯТЬ

1. Тестирование на устойчивость к DDoS-атакам:

с помощью MHDDoS, PyDDOS

2. Настройка инфраструктуры:

- настройка Firewall
- настройка количественных правил (блокировки по количеству подключений с одного IP)
- создание черных списков

3. Инструменты:

Anti-DDOS скрипты,
Nginx-Lua-AntiDDoS

4. Подключение анти-DDoS сервисов:

- CloudFlare,
- Qrator,
- ServicePipe,
- DDoSGuard,
- Stormwall

nübes

КРАЖА КОНТЕНТА (WEB SCRAPING) С ПОМОЩЬЮ БОТОВ

Для чего используется и чем опасно?

- мониторинг цен,
  сбор контактных данных
- кража контента
  (например, карточки товаров)
- паразитная нагрузка
  на приложение

nübes

КРАЖА КОНТЕНТА (WEB SCRAPING) С ПОМОЩЬЮ БОТОВ

ЧТО МОЖНО ПРЕДПРИНЯТЬ

Защититься от ботов поможет:

- Капчи
- JS-проверки

Инструменты:

Open-source:
nginx-ultimate-bad-bot-blocker

Коммерческие:
Qrator, DDoSGuard, StormWall, CloudFlare

nübes

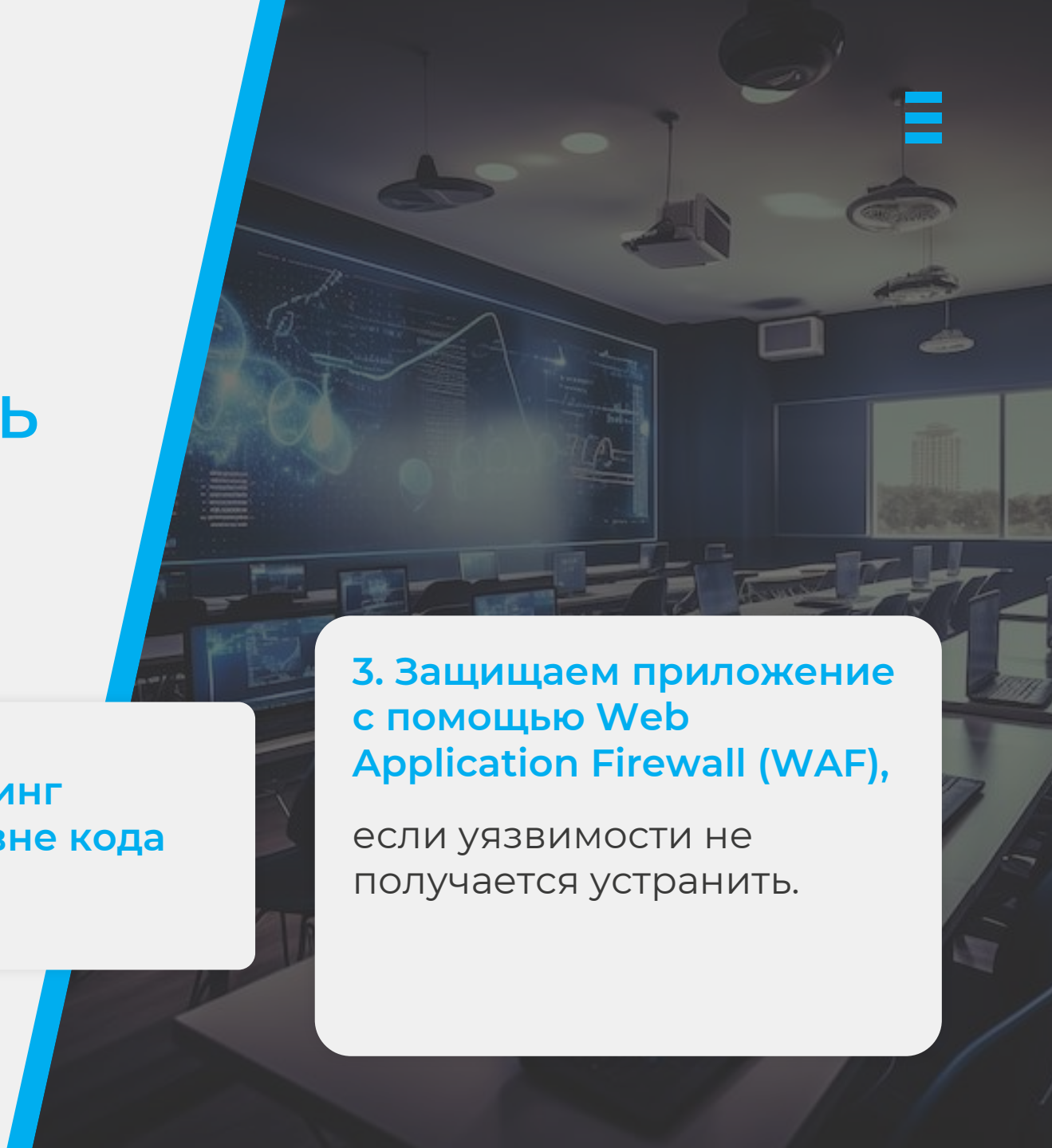
КОМПРОМЕТАЦИЯ ПРИЛОЖЕНИЯ

Чем опасно:

- публичные утечки
- взлом бизнес-логики
- кража конфиденциальной информации
- стартовая точка для взлома остальной инфраструктуры

nübes

КОМПРОМЕТАЦИЯ ПРИЛОЖЕНИЯ:
ЧТО МОЖНО ПРЕДПРИНЯТЬ



1. Безопасная публикация:

- настройка правил в firewall
- разграничение доступов
- ограничение доступа к админский консоли

2. Патчинг на уровне кода

3. Защищаем приложение с помощью Web Application Firewall (WAF),

если уязвимости не получается устранить.

nübes

ЧТО ТАКОЕ WAF?

Web Application Firewall (WAF) –
межсетевой экран для веб-приложений.

Фильтрация трафика:

- защита от известных угроз по сигнатурам (OWASP-10)
- виртуальный патчинг

Анализ трафика

nubes

WAF:

open-source и коммерческие

OPEN-SOURCE

- Modesecurity
- OWASP Coraza WAF
- Nemesida WAF Community Edition

КОММЕРЧЕСКИЕ

- Cloudflare
- PTAF
- SolidWall
- Nemesida WAF
- Вебмониторэкс (Wallarm)

ВЫВОД:

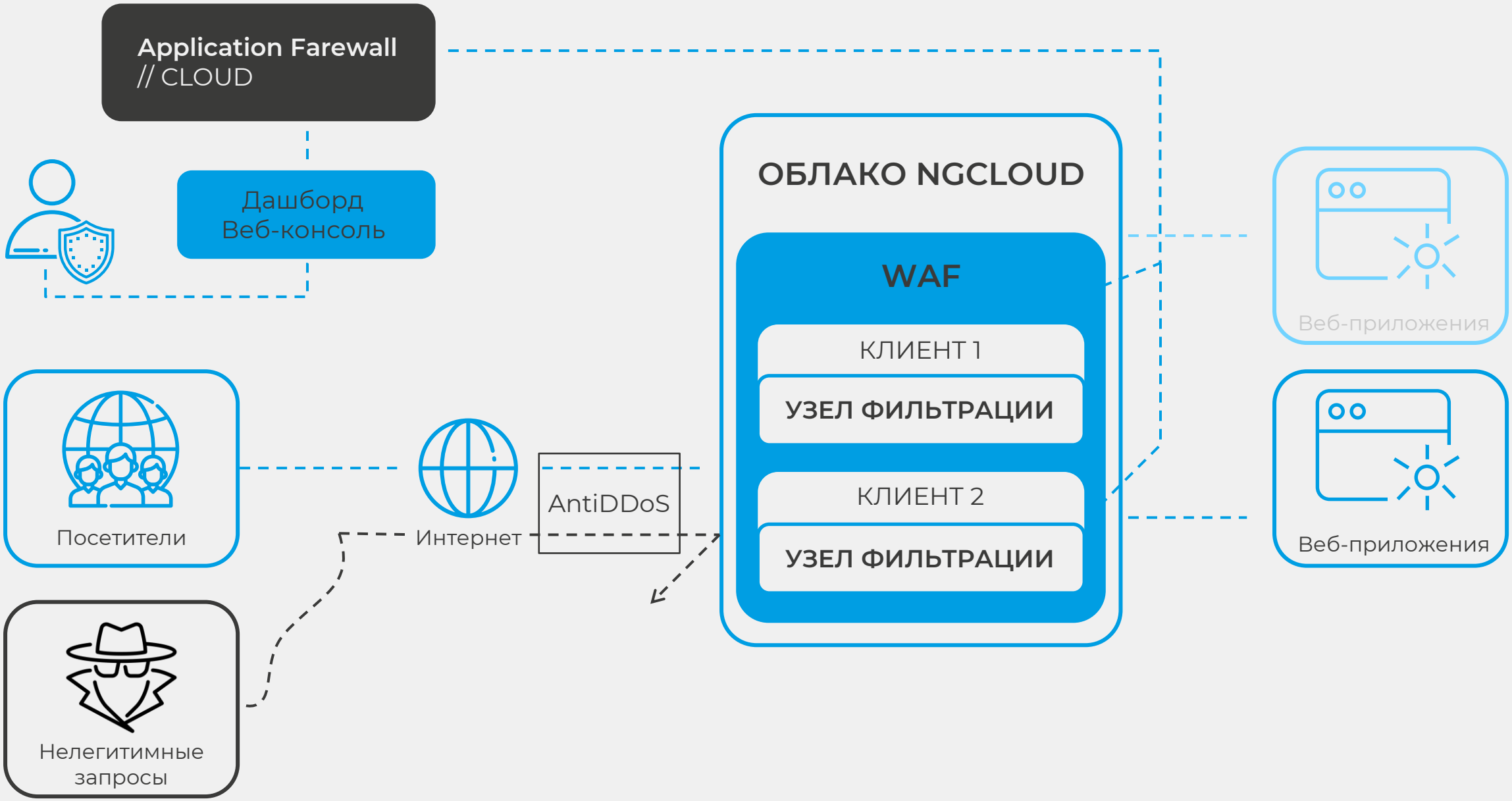
nubes

01. Защита веб-приложения требует комплексного подхода.

02. Есть возможность использовать бесплатные инструменты, но скорее всего это потребует больше временных вложений при отсутствии надежной техподдержки.

03. Даже если вы используете коммерческие инструменты, нужны время и специалисты, чтобы настраивать и управлять ими.

ЧЕМ МЫ МОЖЕМ ПОМОЧЬ В ЗАЩИТЕ ВЕБ-ПРИЛОЖЕНИЙ?


Application Farewall
// CLOUD
Дашборд
Веб-консоль
ОБЛАКО NGCLOUD
WAF
КЛИЕНТ 1
УЗЕЛ ФИЛЬТРАЦИИ
КЛИЕНТ 2
УЗЕЛ ФИЛЬТРАЦИИ
Веб-приложения
Веб-приложения
Посетители
Интернет
AntiDDoS
Нелегитимные
запросы

nubes

СЕРВИС ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ

Комплексная защита приложений и API

- от угроз owasp-10;
- от ddos-
  и целевых атак;
- сканирование
  уязвимостей.

По модели подписки

- ежемесячные платежи
- возможность
  масштабироваться
- без капитальных
  затрат

ИБ-экспертиза здесь и сейчас

- не нужно нанимать
  ИБ-специалистов,
  если их нет в штате
- вся настройка
  и обслуживание ПО
  и оборудования на
  опытных ИБ-инженерах
- круглосуточная
  техподдержка

nübes

ФИНАНСОВАЯ ОТВЕТСТВЕННОСТЬ ЗА КАЧЕСТВО В ДЕТАЛЬНОМ SLA

В соглашении об уровне обслуживания (SLA)
мы фиксируем параметры качества сервиса
выплачиваем штрафы, если не соблюдаем их.

99,95%
доступность сервиса

в течение 15 минут
реагируем на запрос

в течение 10 минут
реагируем на инцидент

24 на 7
техподдержка по почте и телефону

nübes

БЫСТРЫЙ И БЕСПЛАТНЫЙ СТАРТ

ОСТАВЬТЕ ЗАЯВКУ НА ТЕСТ-ДРАЙВ ОТ 2 НЕДЕЛЬ

Для начала работы просто предоставьте:

- список доменов, на которых опубликованы защищаемые приложения;
- сертификаты;
- ключи.

ВОПРОСЫ

nubes

КОНТАКТЫ

info@nubes.ru

1-я Стекольная улица,
дом 7, стр. 2, Москва

Telegram

Nubes.ru