#PAYMENTSECURITY

Актуальные векторы атак на платежную инфраструктуру и способы их митигации

Артем Чувикин

Эксперт по техническому сопровождению ключевых клиентов · NGENIX

5–6 августа 2026

Докладчик

Артем Чувикин

Эксперт по техническому сопровождению ключевых клиентов · NGENIX

Работаю с ключевыми заказчиками облачных сервисов защиты от киберугроз, помогаю крупному бизнесу бороться с DDoS, ботами, взломами.

EMAIL

a.chuvikin@ngenix.net

01

РАЗДЕЛ 01

Ландшафт веб-атак

Проблематика

01	**Бюджетное давление**	Хакеры удешевляют стоимость атак из-за ИИ, а бюджет на защиту сокращается
02	**Эволюция веб-угроз**	Все новые и актуальные угрозы для веба релевантны для платежных систем
03	**Сложность архитектуры**	Бизнес-логика платежных систем дает возможности для точечных атак
04	**Узкое горлышко**	Платежные системы – цель для злоумышленников из-за своей роли

Доступность под угрозой

Доступность платежной инфраструктуры = доступность всего приложения

Сложная бизнес-логика предполагает, что вывод из строя одного компонента экосистемы означает, что весь сервис становится недоступным для конечного пользователя

Угрозы растут и усложняются

Платежная инфраструктура – привлекательная цель для злоумышленников

- Финансовый сектор и платежные сервисы принимают на себя **до трети** всех сетевых атак.
- Доля целенаправленных атак на алгоритмы искусственного интеллекта в банках и платежных шлюзах достигает **5–10%.**
- **До 64%** успешных атак на финансовые организации сопровождаются утечками конфиденциальных пользовательских записей
- Общая длительность DDoS увеличилась **в 2,3 раза.**

15,9%

DDoS- атак в 2025 году пришлось на банки и платежные системы

02

РАЗДЕЛ 02

Актуальные типы атак на веб и API: DDoS

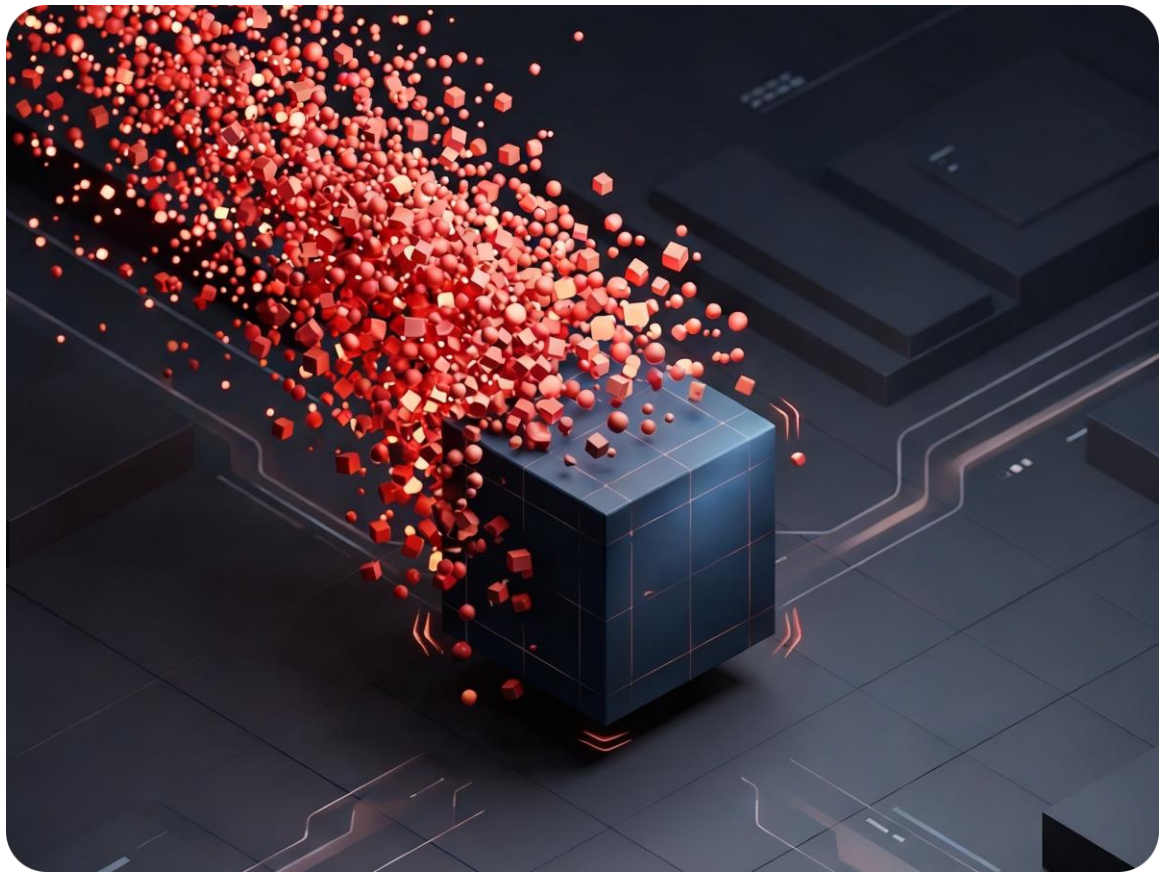
DDoS никуда не делся

- L3/L4 DDoS: атаки на инфраструктуру, TCP/UDP flood
- L7 DDoS: давление на «тяжелые ручки» OAT-015 Denial of Service, перебор uri или сканирование, обращение, медленные запросы HTTP flood
- DDoS на вспомогательные сервисы: DDoS на DNS
- Финансовый сектор – в топ-3 по DDoS-атакам

x3

рост отраженных финансовым сектором DDoS-атак за квартал (2024 vs 2025)

Burst-атаки



Burst-атаки – очень быстрые атаки, основанные на исчерпании ресурса

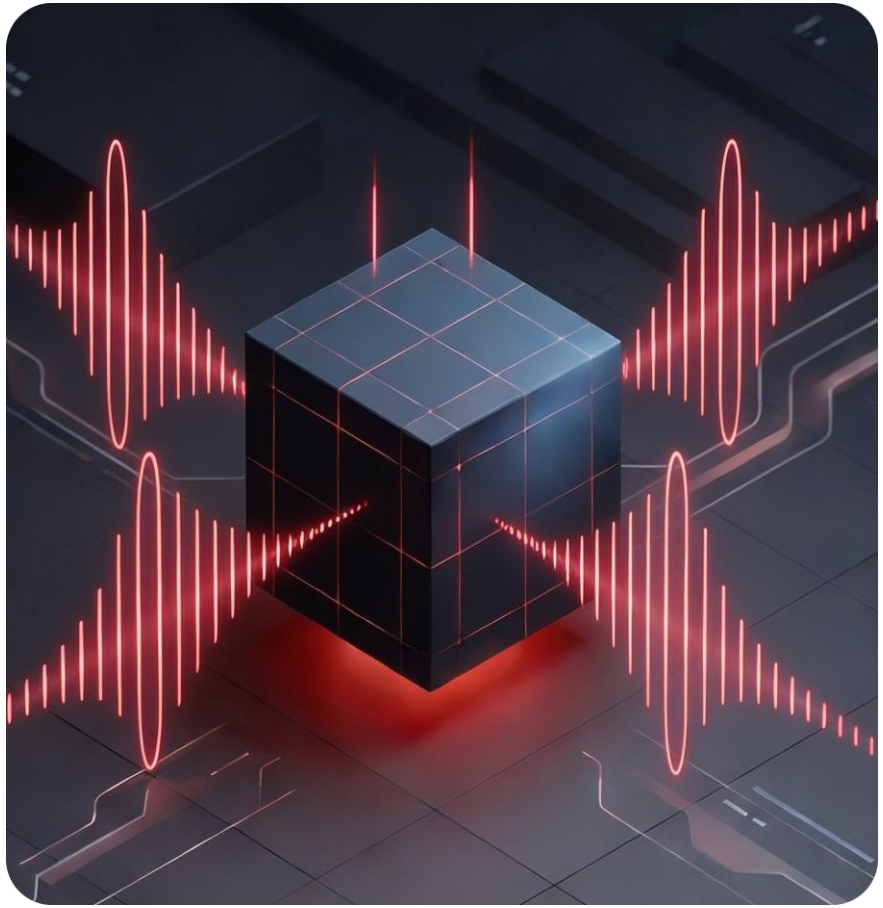
Цель:

- Исчерпание CPU
- Истощение потоков
- Переполнение connection pull

Почему сложно детектировать и отражать:

- Быстрая атака > сервисы защиты, основанные на анализе статистических метрик и порогов, слишком инертны
- Нельзя агрессивно использовать Rate Limiting > риск «уронить» легитимных пользователей
- Атака распределенная (ботнеты, разные IP и т.д.)

Shortwave-атаки



#PAYMENTSECURITY

Shortwave-атаки – атаки короткими импульсами с паузами, вызывающие состояние, при котором система обрабатывает запросы параллельно, но не успевает обновить общее состояние

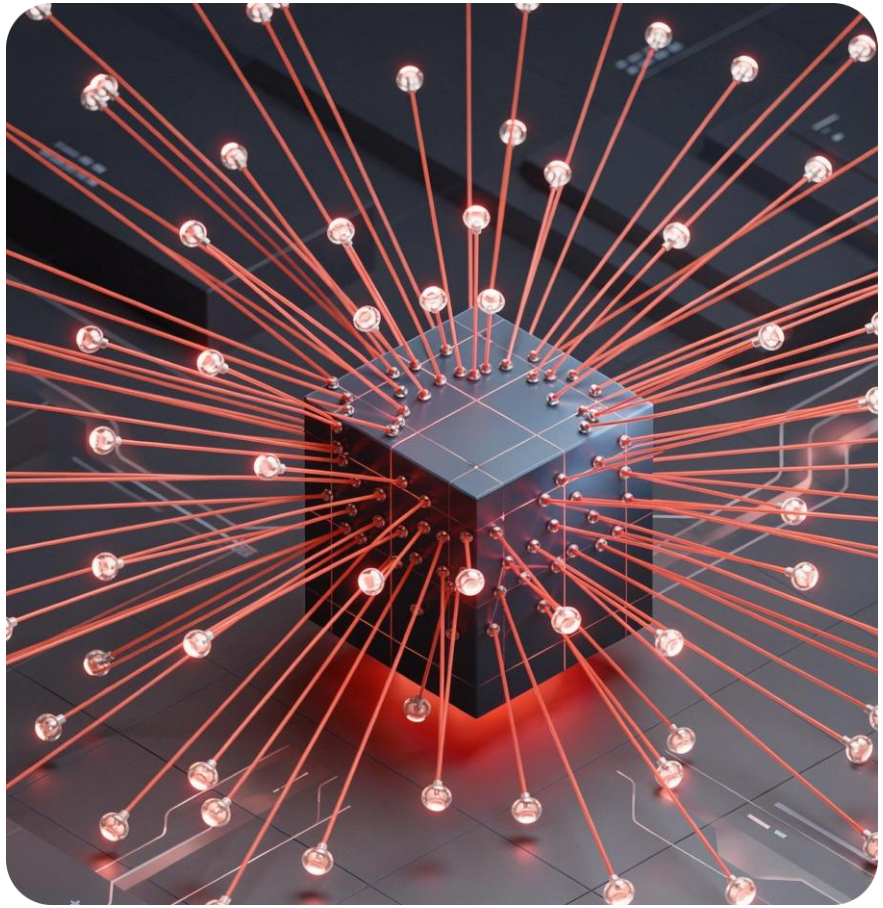
Цель:

- Race conditions
- Обход лимитов
- Timing-анализ

Почему сложно детектировать и отражать:

- Каждый отдельный запрос «чист»
- Нет явного превышения лимитов
- Нет сигнатуры атаки
- Данные систем защиты об rps, ошибках, сигнатуры ничего не дают
- WAF и API gateway вне контекста. Для них два одинаковых запроса подряд – не аномалия

Carpet bombing-атаки



«Ковровые бомбардировки» – распределенная атака, где играет роль не размер аномалии, а количество атакуемых эндпойнтов

Цель:

- Создание распределенной нелегитимной нагрузки
- Разведка устойчивости системы

Почему сложно детектировать и отражать:

- Нет одного «плохого» эндпойнта
- Нет пиков нагрузки
- Каждый запрос выглядит легитимным
- Rate limiting не срабатывает (разные URL)
- WAF не срабатывает (нет сигнатуры)
- Мониторинг не срабатывает (не аномального пика)

Классические методы неэффективны

Burst

Ломает нагрузкой

Shortwave

Ломает временем

Carpet Bombing

Ломает распределением

03

РАЗДЕЛ 03

Актуальные типы атак на веб и API: боты

Боты атакуют: угрозы по OWASP

1. OAT – 001 Carding
2. OAT – 010 Card Cracking
3. OAT – 012 Cashing Out
4. OAT – 021 Denial of Inventory
5. OAT – 005 Scalping
6. OAT – 007 Credential Cracking
7. OAT – 008 Credential Stuffing
8. OAT – 020 Account Aggregation
9. OAT – 019 Account Creation

Угрозы автоматизированных атак

Атаки на учетные записи

OAT – 007
Credential Cracking

OAT – 008
Credential Stuffing

OAT – 020
Account Aggregation

OAT – 019
Account Creation

Атаки на товары

OAT – 021
Denial of Inventory

OAT – 005
Scalping

Атаки на ДДК

OAT – 001
Carding

OAT – 010
Card Cracking

OAT – 012
Cashing Out

#PAYMENTSECURITY

«

Рассмотрим некоторые автоматизированные атаки

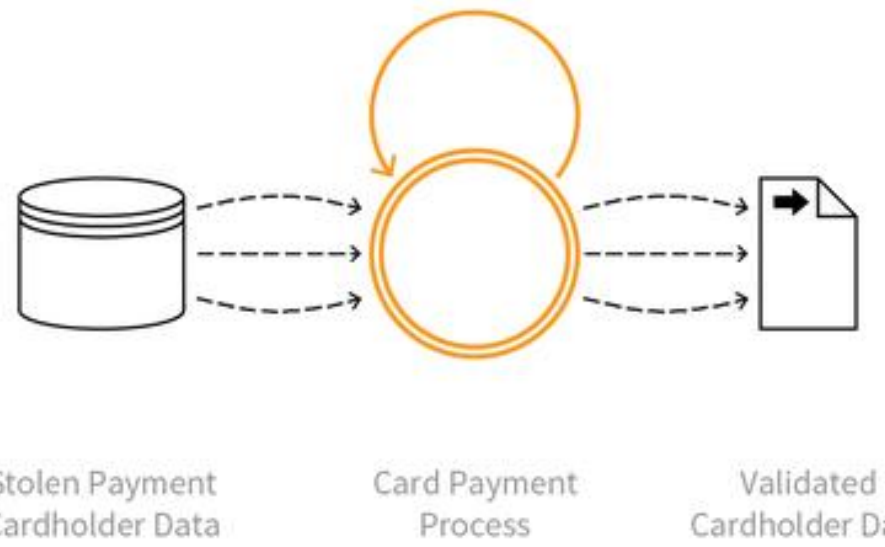
Carding (OAT – 001)

Card Cracking (OAT – 010)

Scalping (OAT – 005)

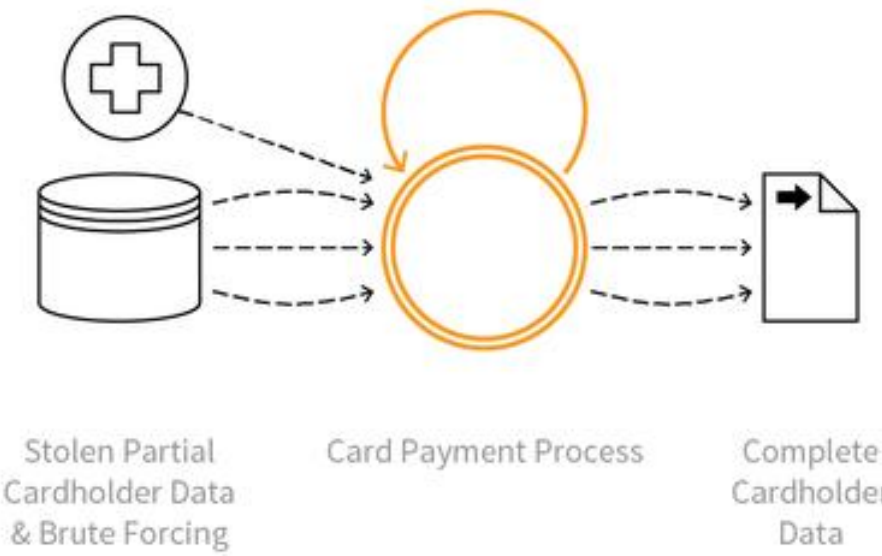
Кардинг

Списки полных данных кредитных и/или дебетовых карт проверяются на соответствие платежным процессам продавца для выявления действительных данных карты. Качество украденных данных часто неизвестно, и кардинг используется для выявления качественных данных, представляющих большую ценность. Данные владельца платежной карты могли быть украдены из другого приложения, другого платежного канала или приобретены на криминальном рынке.



Card Cracking

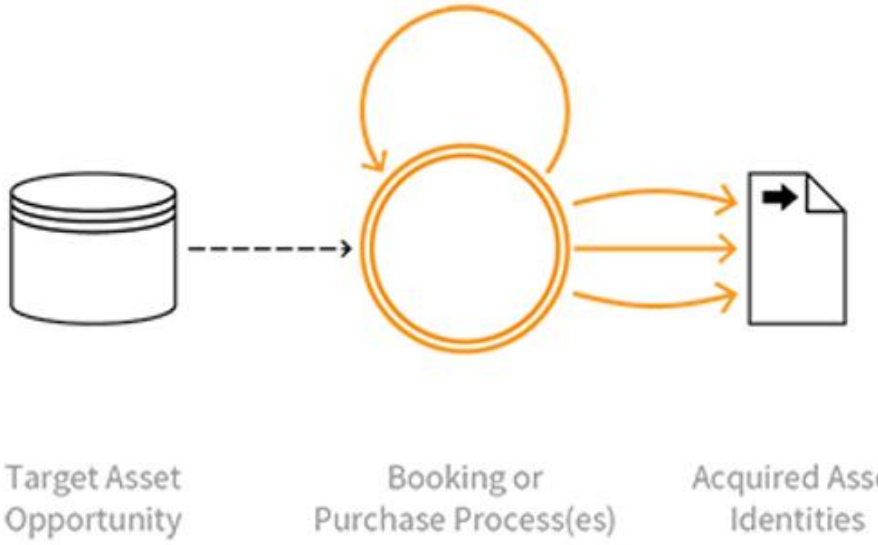
Card Cracking — это атака методом перебора (brute force) на процессы обработки платёжных карт в приложениях. Цель атаки — выявить недостающие данные: дату начала действия карты, срок её действия и код безопасности (CSC). Код безопасности может называться по-разному: CVN2, CVC, CV2 или CID.



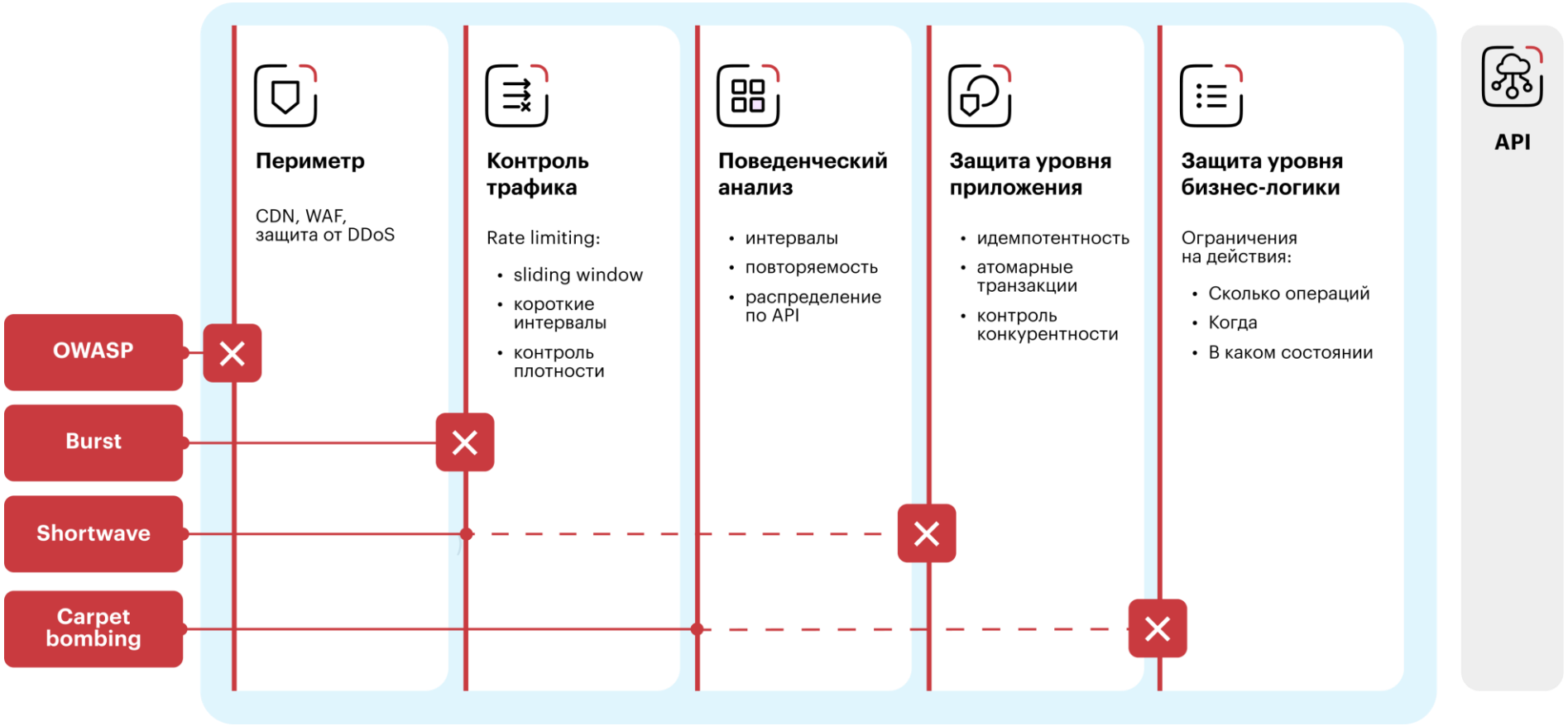
Скальпинг

Кейс с покупкой билетов на концерт Oasis

Наиболее известен скальпинг в сфере продажи билетов, когда купленные билеты перепродаются с выгодой для спекулянтов. Это также может привести к своего рода отказу в обслуживании пользователей, поскольку товары или услуги быстро становятся недоступными.



Одного WAF недостаточно

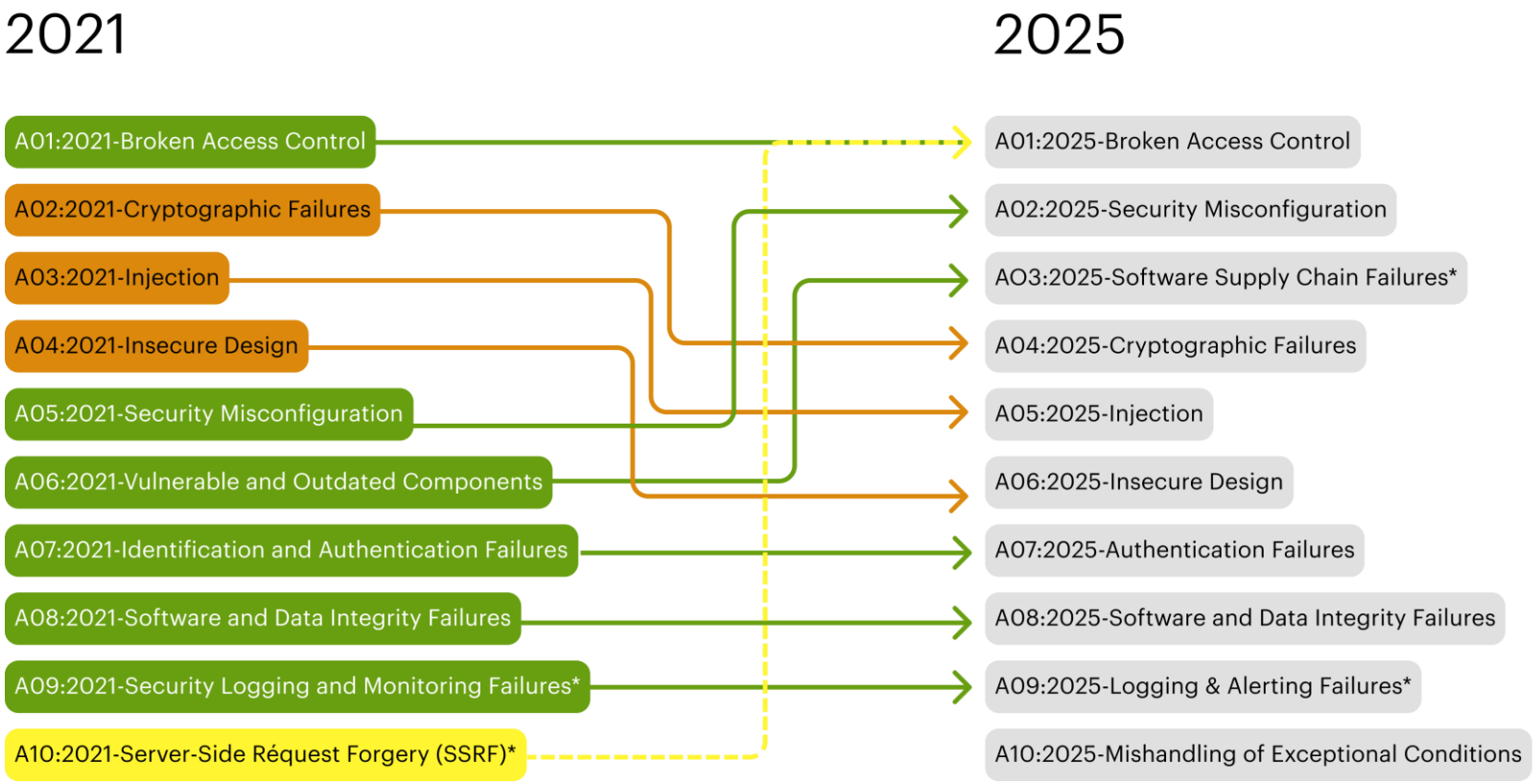


04

РАЗДЕЛ 04

Актуальные типы атак на веб и API: OWASP Top 10

Атаки, которые блокируются на WAF



05

РАЗДЕЛ 05

Актуальные типы атак: эксплуатация уязвимостей

Количество уязвимостей растет

Наиболее актуальные угрозы для финансового сектора

- Remote Code Execution (RCE) — **24%** всех атак. Злоумышленники пытаются получить полный контроль над сервером.
- Path Traversal — **25%** атак. Используется для доступа к файловой системе и как подготовка к более сложным атакам (RCE).
- XSS (Cross-Site Scripting) — составляет **25%** от всех выявленных веб-атак в целом по РФ.

4,1 млн

атак в год на 1 финансовую организацию в среднем

Тренд: выявление уязвимостей

Год	Опубликованные уязвимости CVE	Критические	Высокие
2018	17,964	2,489	7,369
2019	18,645	2,502	7,067
2020	18,941	2,510	7,5911
2021	21,469	2,397	8,359
2022	25,814	3,562	9,542
2023	30,361	3,450	9,614
2024	40,131	3,444	13,451
2025	49,458	3,579	15,868
2026*	30,550	2,906	11,187

ИИ и ландшафт уязвимостей

- ИИ помогает находить все больше уязвимостей
- ИИ снижает порог вхождения для эксплуатации сложных уязвимостей
- LLM сам стал периметром атаки (OWASP 10 LLM)
- ИИ находит реальные уязвимости: В ходе одного из экспериментов с использованием AI-агентов (Claude Code и OpenAI Codex) для анализа 11 крупных open-source веб-приложений было найдено несколько десятков реальных уязвимостей, включая 20 с высоким уровнем серьезности

06

РАЗДЕЛ 06

Подходы к построению защиты

Требования PCI DSS к публичным веб-приложениям

- Обязательное использование WAF **(Требование 6.4.2).**
- Управление скриптами платежных страниц **(Требование 6.4.3).**
- Инвентаризация собственного ПО **(Требование 6.3.2).**
- Обнаружение несанкционированных изменений **(Требование 11.6.1).**
- Приоритезация уязвимостей **(Требование 11.3.1.1).**

Подходы к защите публичных веб-приложений

Построение DIY-решения

Самостоятельная разработка ПАК/ПО, обеспечивающих защиту веб-ресурсов от DDoS-атак и ботов в составе оригинальной веб-инфраструктуры.

Равертывание On-Prem решения

Развёртывание специализированных ПАК/ПО, обеспечивающих защиту веб-ресурсов от DDoS-атак и ботов в составе оригинальной веб-инфраструктуры.

PaaS без раскрытия HTTP(S)-трафика

Облачная услуга, позволяющая анализировать поступающий поток логов с оригинальной веб-инфраструктуры и формирующая списки нежелательных источников трафика для блокировки на оригинальной веб-инфраструктуре.

PaaS с раскрытием HTTP(S)-трафика

Облачная услуга, обеспечивающая обработку, анализ и блокировку нежелательного трафика на внешней инфраструктуре сервис-провайдера и экранирующая оригинальную веб-инфраструктуру.

Построение DYI-решения

Построение DIY-решения

Самостоятельная разработка ПАК/ПО, обеспечивающих защиту веб-ресурсов от DDoS-атак и ботов в составе оригинальной веб-инфраструктуры

Капитальные затраты

₽ ₽ ₽

Разработка ПО и закупка оборудования

Операционные затраты команды на поддержку

₽ ₽ ₽

Разработка, поддержка и эксплуатация ПО и оборудования

Затраты на аттестацию / периодическую аттестацию решения в составе ИС

₽ ₽ ₽

Высокие, требуется полная переаттестация ИС

Ответственность за работоспособность решения

Владелец веб-ресурса

Нагрузка на оригинальную веб-инфраструктуру

Вся нагрузка обслуживается оригинальной веб-инфраструктурой

Масштабируемость и производительность решения

Веб-ресурс становится недоступен, если легитимная и/или нелегитимная нагрузка превысила емкость системы

Эффективность решения

Высокий риск ложноположительных срабатываний

Time-to-market

Разработка и внедрение требует больших ресурсов

Развертывание onprem-решения

Равертывание On-Prem решения

Развёртывание специализированных ПАК/ПО, обеспечивающих защиту веб-ресурсов от DDoS-атак и ботов в составе оригинальной веб-инфраструктуры

Капитальные затраты

₽ ₽ ₽

Закупка специализированного оборудования

Операционные затраты команды на поддержку

₽ ₽ ₽

Поддержка и эксплуатация оборудования и ПО, за исключением обновления ПО

Затраты на аттестацию / периодическую аттестацию решения в составе ИС

₽ ₽ ₽

Высокие, требуется полная переаттестация ИС

Ответственность за работоспособность решения

Владелец веб-ресурса

Нагрузка на оригинальную веб-инфраструктуру

Вся нагрузка обслуживается оригинальной веб-инфраструктурой

Масштабируемость и производительность решения

Веб-ресурс становится недоступен, если легитимная и/или нелегитимная нагрузка превысила емкость системы

Эффективность решения

Зависит от актуальной версии ПО

Time-to-market

Нужна установка оборудования

Гибридный подход

PaaS без раскрытия HTTP(S)-трафика

Облачная услуга, позволяющая анализировать поступающий поток логов с оригинальной веб-инфраструктуры и формирующая списки нежелательных источников трафика для блокировки на оригинальной веб-инфраструктуре

Капитальные затраты

Закупка оборудования для интеграции с PaaS

Операционные затраты команды на поддержку

Поддержка и эксплуатация оборудования, ПО и облачной услуги, обеспечивающей интеграцию с PaaS

Затраты на аттестацию / периодическую аттестацию решения в составе ИС

Решение не подлежит аттестации

Ответственность за работоспособность решения

Владелец веб-ресурса + PaaS-провайдер

Нагрузка на оригинальную веб-инфраструктуру

Вся легитимная нагрузка, а также часть нелигитимной нагрузки обслуживается оригинальной веб-инфраструктурой

Масштабируемость и производительность решения

Веб-ресурс становится недоступен, если легитимная нагрузка превысила емкость системы и/или оригинальная веб-инфраструктура не смогла передать поток данных для анализа

Эффективность решения

Высокая задержка в принятии решения и ограниченность механизмов валидации

Time-to-market

Сложная интеграция с PaaS-провайдером

Облако

PaaS с раскрытием HTTP(S)-трафика

Облачная услуга, обеспечивающая обработку, анализ и блокировку нежелательного трафика на внешней инфраструктуре сервис-провайдераи экранирующая оригинальную веб-инфраструктуру

Капитальные затраты

Отсутствует

Операционные затраты команды на поддержку

Эксплуатация облачной услуги

Затраты на аттестацию / периодическую аттестацию решения в составе ИС

Аттестация в зоне ответственности PaaS-провайдера

Ответственность за работоспособность решения

PaaS-провайдер

Нагрузка на оригинальную веб-инфраструктуру

Оригинальная веб-инфраструктура обрабатывает только часть легитимной нагрузки, нелегитимная нагрузка и легитимные запросы к кэшируемым данным обрабатываются в облаке

Масштабируемость и производительность решения

Эластичное облачное решение с большим запасом емкости, автоматически масштабируемое под всплески легитимного и/или нелегитимного трафика

Эффективность решения

Анализ запроса по множеству факторов и критериев с возможностью настройки дополнительных механизмов валидации

Time-to-market

Простая интеграция через CNAME или A-запись в DNS

07

РАЗДЕЛ 07

Выводы

Современные угрозы требуют эффективных подходов

- DYI > Высокий CAPEX / OPEX, долгая адаптация к постоянному изменению ландшафта угроз
- On-prem > Высокий CAPEX, проблемы в масштабировании под пики нагрузки, «зоопарк» с серыми зонами ответственности
- Гибрид («Защита без раскрытия») > Market-ready и не требует аттестации, но с ограничениями и рисками, связанными с непредсказуемыми нагрузками
- Облако (PaaS с раскрытием трафика) > Эффективно, но должно иметь соответствующие аттестаты и четкое разграничение ответственности с провайдером.

#PAYMENTSECURITY

Важно:
аттестация провайдера не снимает ответственности за аттестацию других систем

#PAYMENTSECURITY

Вопросы?

#PAYMENTSECURITY

Спасибо за внимание!

EMAIL
a.chuvikin@ngenix.net

САЙТ
ngenix.net