UserGate

Ландшафт угроз для веб-приложений в эпоху цифрового суверенитета. Итоги 2025 года

Абрамович Виталий

Менеджер по развитию UserGate WAF

Для “Сетевая безопасность 2025”
25.11.2025

UserGate

750+ человек
в команде, и мы растем

70% штата
занимаются разработкой

7 продуктов: WAF +
NGFW, DCFW, LogAn, SIEM, Client, MC

uWAF

2025 запуск
коммерческой версии
UserGate WAF

Реальный опыт
Широкий ландшафт эксплуатирующих
заказчиков и партнёров, более 100 пилотов

ОСНОВНЫЕ ДРАЙВЕРЫ ЦИФРОВОГО СУВЕРЕНИТЕТА В 2025 ГОДУ

01

Фрагментация интернета:

Появление национальной цифровой инфраструктуры и ужесточение регуляторики: *законы ФЗ-152, ФЗ-406, требования к КИИ*

02

Локализация ИТ-инфраструктуры:

Массовое использование отечественных решений.
Массовый переход на 1С-Битрикс и отечественные CMS

03

Геополитика как мотиватор:

Рост активности кибергрупп. Их цель — не прибыль, а дестабилизация и шпионаж. “BlackCocaine”, целевые атаки на госсектор

ЦЕЛИ И ЛАНДШАФТ УГРОЗ ДЛЯ ВЕБ-ПРИЛОЖЕНИЙ В 2025 ГОДУ

UserGate

01 Шпионаж 68%

02 Финансовое обогащение 20%

03 Кибертерроризм 8%

01 ДДоС, ДоС, брутфорс

02 Эксплуатация известных уязвимостей

03 Уязвимые и устаревшие КОМПОНЕНТЫ ПО

04 Небезопасные конфигурации

Последствия

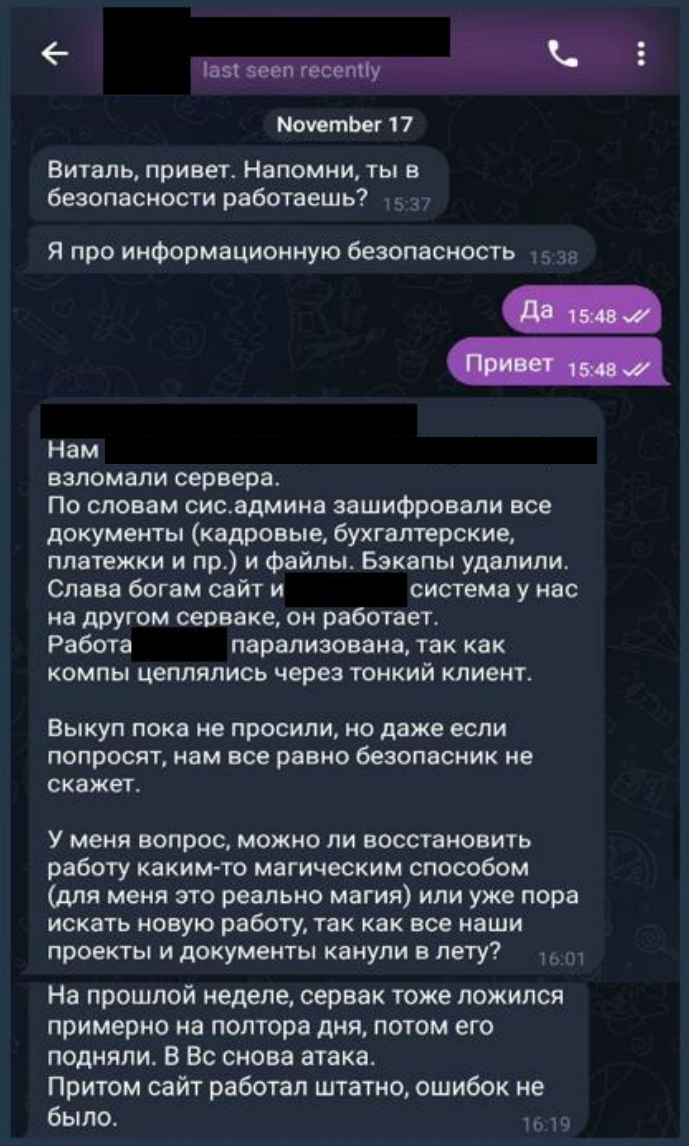
01 Утечка конфиденциальной информации – в 52% атак

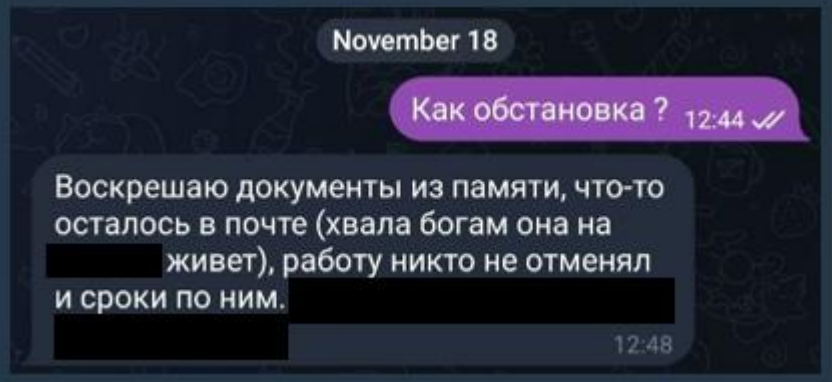
02 Нарушение основной деятельности – в 45% атак

03 Использование ресурсов организации для проведения атак – в 9% атак

04 Прямые финансовые потери – в 4% атак

РЕАЛЬНА ЛИ УГРОЗА?





Fasana, производитель бумажных салфеток из Германии, не вынесла хакерского удара и объявила о банкротстве после масштабной кибератаки 19 мая, которая парализовала ее системы и привела к потере около 2 млн евро за две недели простоя. В результате инцидента были остановлены производство, выплата зарплат и обработка заказов на сумму свыше 250 000 евро.

АКТУАЛЬНОСТЬ ОБНОВЛЁННОГО СПИСКА OWASP TOP 10 ДЛЯ РОССИИ И СНГ

2017	2021	2025
1. Инъекции	1. Нарушение контроля доступа	1. Нарушение контроля доступа
2. Недочеты системы аутентификации	2. Сбои криптографии	2. Ошибки конфигурации
3. Раскрытие чувствительных данных	3. Инъекции	3. Ошибки в цепочке поставок ПО
4. Внешние сущности XML (XXE)	4. Небезопасный дизайн	4. Сбои криптографии
5. Нарушение контроля доступа	5. Ошибки конфигурации	5. Инъекции
6. Ошибки конфигурации	6. Уязвимые и устаревшие компоненты	6. Небезопасный дизайн
7. Межсетевой скриптинг	7. Ошибки идентификации и аутентификации	7. Ошибки аутентификации
8. Небезопасная десериализация	8. Нарушения целостности взаимодействия ПО и данных	8. Нарушения целостности взаимодействия ПО и данных
9. Использование компонентов с известными уязвимостями	9. Ошибки ведения журнала и мониторинга безопасности	9. Ошибки ведения журнала и отправки уведомлений безопасности
10. Недостаточное ведение журнала и мониторинга безопасности	10. Подделка межсерверных запросов	10. Некорректная обработка исключений

1 УГРОЗА: СЛОЖНАЯ ИНФРАСТРУКТУРА, ОТСУТСТВИЕ КАДРОВ

Отсутствие ИБ специалистов

- Отсутствие штатного ИБ специалиста !!!
- Менее 25% государственных учреждений, организаций среднего и малого бизнеса и используют WAF для защиты своих веб-сервисов
- Закладки в инфраструктуре

26.05.2023 была проведена массовый дефэйс веб-серверов национального сегмента РФ сети интернет. В качестве цели атаки выступала CMS Bitrix. В ходе расследование было установлено, что массовые взломы были проведены загодя, в начиная с 2022 года через известные уязвимости, включая CVE-2022-27228. Злоумышленником был установлен бэкдор, позволяющий создавать произвольные файлы и вызывать команды ОС. 26 мая в районе 14:00 бэкдору была дана команда на замену главной страницы сайта.

- Новые отечественные решения – идёт процесс перехода, пользуются несколькими решениями

Низкая квалификация специалистов

Низкая осведомлённость актуальной проблематикой, отсутствие постоянного обучения
Использование генеративный low-code

2 УГРОЗА: ОТСУТСТВИЕ ЗАЩИТЫ МОДУЛЕЙ СОБСТВЕННОЙ РАЗРАБОТКИ

UserGate

Общий рынок

	CMS	Проектов	Доля
#1	WordPress	566 100 +31 700	43.81% -0.92%
#2	1C-Bitrix	173 000 +13 700	13.39% +0.05%
#3	Joomla	123 100 -17 400	9.53% -2.23%
#4	CMS.S3	39 500 +39 500	3.06% new
#5	OpenCart	39 000 +0	3.02% -0.25%
#6	Tilda	35 500 +19 800	2.75% +1.43%

2 УГРОЗА: ОТСУТСТВИЕ ЗАЩИТЫ МОДУЛЕЙ СОБСТВЕННОЙ РАЗРАБОТКИ

UserGate

Коммерческий рейтинг

Место	CMS / Платформа	Доля	Ключевые риски в 2025
1	**1С-Битрикс**	>50%	**Атаки на цепочку поставок** (CMS, CRM, и т.д), уязвимости в ядре, целевой DDoS (*Bitrix24DoS*), концентрация рисков.
2	**WordPress**	До 25%	**Массовые автоматизированные атаки**, уязвимости в плагинах
3	**Drupal / Joomla!**	~5-10%	Меньше целевых атак, но выше сложность поддержки и безопасной настройки.

Исследование на GitHub (jhonnybonny/Bitrix24DoS) демонстрирует уязвимость, позволяющую провести эффективную DoS-атаку "малой кровью", исчерпав ресурсы сервера.

3 УГРОЗА: ПОВЫШЕННЫЙ УРОВЕНЬ ВНИМАНИЯ К ДОМЕНУ .RU

70%

Вредоносного трафика автоматизированно
В 2023 – до 50%

L4 -> L7

Эволюция DDoS-атак

x1,7

Вырос уровень бот активности Q3 2024->Q3 2025

4 УГРОЗА: НЕДОСТАТОЧНОЕ ВНИМАНИЕ К **DEVSECOPS**

Отсутствие специализированных HTTP-заголовков

Кликджекинг

Разработка без учёта информационной безопасности

Нарушение контроля доступа через автоматизированные средства, эксплуатация бизнес логики

Отсутствие понимания технологического стека веб-приложений

Эксплуатация древних CWE

Эпоха цифрового суверенитета не сделала нас безопаснее по умолчанию. Она смешала киберугрозы с геополитикой, создав более сложные вызовы. Победа останется за теми, кто научится управлять рисками не только своего кода, но и всей своей цифровой инфраструктуры.

А ДЕЛАТЬ ТО ЧТО?

01 **Технические меры:** Внедрить WAF, который компенсирует "дыры" в коде и конфигурации.

02 **Процессные меры:** Внедрить DevSecOps, проводить регулярный аудит и пентесты.

03 **Кадровые меры:** Обучать команды, нанимать специалистов.

UserGate

Абрамович Виталий

Менеджер по развитию UserGate WAF

Спасибо за внимание!
А теперь ваши вопросы!