ЗАЩИТА ДАННЫХ

7 апреля 2025 года
Москва, Холидей Инн Сокольники

ЗАЩИТА ДАННЫХ

Компрометация веб-приложения

Сафонов Лука

Технический директор Weblock, ГК «Гарда»

ЗАЩИТА ДАННЫХ

Компрометация веб-приложений становится одной из основных угроз информационной безопасности.

Анализ инцидентов помогает выявить уязвимости и улучшить защиту систем.

Анализ журналов веб-сервера

Журналы веб-сервера содержат ключевую информацию о подозрительной активности (например, необычные запросы, ошибки доступа).

Примеры аномалий:

- Множественные запросы к служебным файлам, конфигурациям.
- Неудачные попытки входа с разных IP-адресов.
- Подозрительные параметры в URL (например, SQL-инъекции или XSS).

Анализ журналов веб-сервера

Топ-10 IP-адресов с наибольшим количеством запросов:

```
awk '{print $1}' access.log | sort | uniq -c | sort -nr | head -n 10
```

Построение автоэнкодера для анализа журналов веб-сервера с использованием Keras и TensorFlow: обработка данных, создание модели автоэнкодера, обучение модели и её использование для анализа аномалий.

Выявление "точек входа"

Точки входа — это уязвимые места приложения, через которые злоумышленники могут получить доступ.

Основные типы точек входа:

- Уязвимые формы ввода данных (например, поисковые строки, формы регистрации).
- Неправильно настроенные права доступа к файлам и директориям.
- Использование устаревших библиотек или фреймворков.

Поиск артефактов компрометации

Артефакты — это следы, оставленные злоумышленниками после атаки.

Примеры артефактов:

- Неизвестные файлы или скрипты в директориях приложения.
- Изменение прав доступа к файлам или их содержимого.
- Логи с подозрительными командами.

Устранение последствий

Немедленно отключить/изолировать скомпрометированное приложение для предотвращения дальнейших атак.

Удалить все подозрительные файлы и скрипты, восстановить оригинальные версии.

Провести полную проверку системы на наличие вредоносного ПО.

Защита

Обновление компонентов.

Мониторинг.

СЗИ (WAF/WAAP/AntiDDoS/Маскирование данных).

ЗАЩИТА ДАННЫХ

Благодарю за внимание!