Информационная безопасность предприятия с PCI DSS. Жизнь до и после

2016 г.

Wildberries — один из крупнейших интернет-магазинов России

Более
4 тыс.
брендов
на сайте

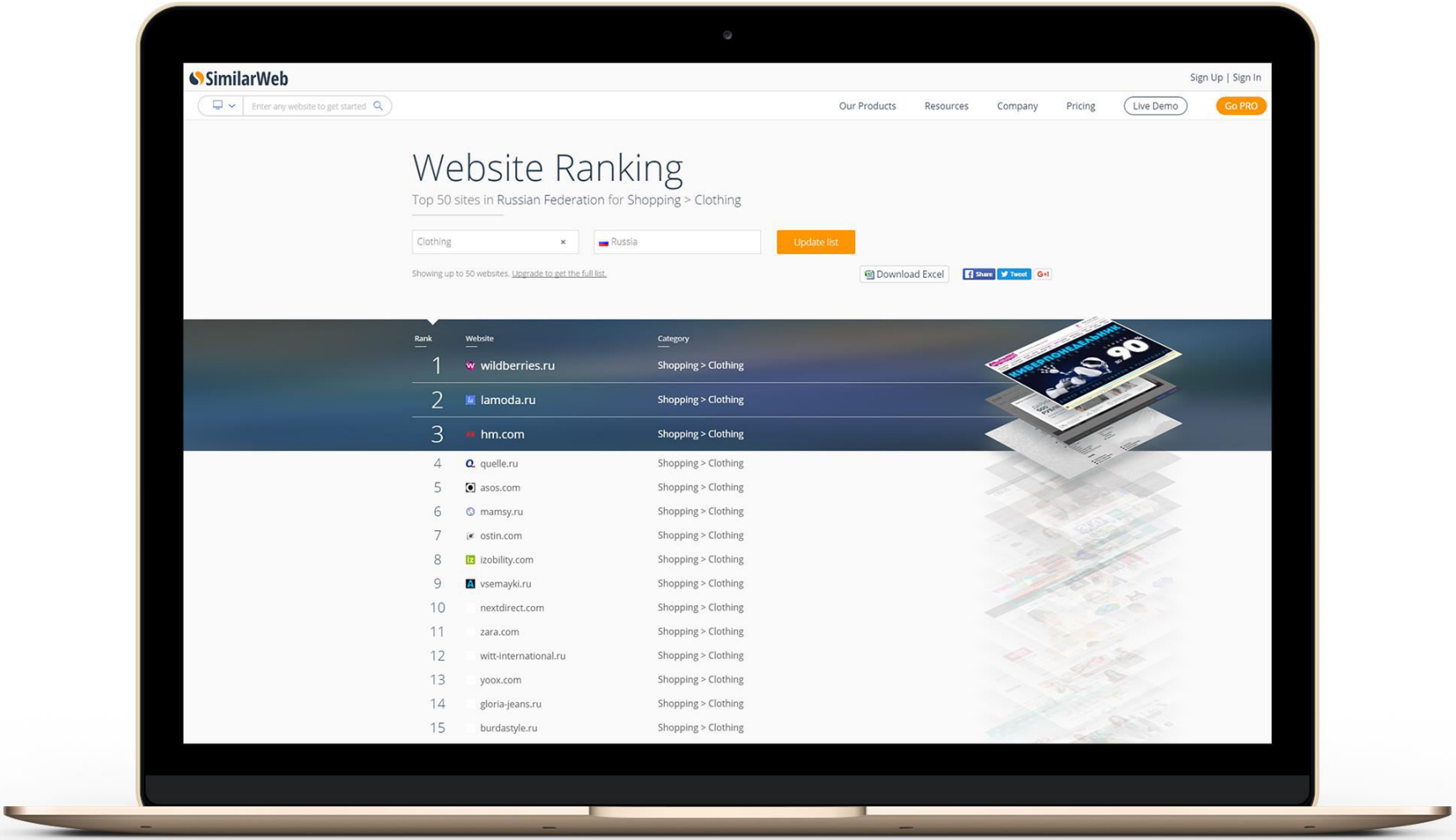
Более
100 тыс.
заказов
в день

Более
1 млн.
посетителей
в день

Более
8 млн.
товаров
на складе

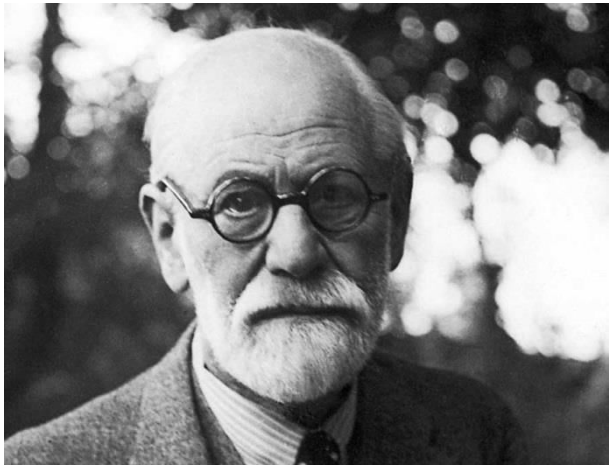
2. Наши клиенты

3. Самый посещаемый интернет-магазин России*



* Согласно международному online-сервису исследования интернет-трафика Similar Web: www.goo.gl/cqzEpf

4. Бывает же такое



Для того, что бы люди относились к процедурам серьёзно – надо брать деньги за услуги. Большие деньги!

Враги ИБ:

1. Проблема финансового обоснования ИБ
2. Хаотичные задачи со сроками ВЧЕРА
3. Некогда учится ИБ – у нас куча задач!
4. Зачем нам ИБ конференции – все есть в интернете!
5. Какое анализ кода? Срочно готовьте релиз!
6. Общая ответственность
7. Вражда команд
8. У нас ДОС атака – что мне делать

5. Обязательная проработка планов реагирования на инциденты ИБ

Действия дежурного:

ДО

1. Найти человека который знает у кого спросить
2. Найти контакты знающего сотрудника
3. Дозвониться
4. Рассказать суть происшествия
5. Повесить трубку с чувством выполненного долга

ПОСЛЕ

1. Создать инцидент в системе – кто, что, где и как?
2. Определить серьезность в баллах
3. На основании серьезности выставить сроки исправления
4. Ответственные лица определены заранее.
5. Мониторинг исполнения ИБ инцидентов на “безопаснике”

Разгон не быстрый – полет долгий
Нет функционалу без планов
Смена пароля – алерт
Смена правил на оборудование

6. Обязательное обучение основам ИБ

Без развития приходит деградация. PCI DSS обязывает к повышению осведомленности

SDL:
Решение вопросов ИБ на этапе проектирования
Моделирование рисков
Планы реагирования
Явно заданные роли советников по ИБ
Статичный + Динамический анализ

Работа с сотрудниками в целом:
Каждый понедельник слайд по почте
Информация о атаках на офисы
Атака на обучение изнутри

OWASP:

Знаем/слышали
XSS
Инъекции

Не знаем!
CSRF
Управление сессиями
Слабая крипто стойкость
Функционал без проверки ролей
Прямые ссылки на объекты
Finger Print
Небезопасное перенаправление
Инфо о ошибках

График обучения (ИТ):
1 раз в 3 месяца повтор по ИБ
План на год по ИБ мероприятиям
Новеньким SDL в помощь

7. Тест, анализ и еще раз тест

С удовольствием отвечу на Ваши вопросы по теме

Ревяшко Андрей Сергеевич

Технический директор

Тел.: +7 495 775-55-05 доб. 1150
E-mail: reviashko@wildberries.ru

Вопросы?

www.wildberries.ru