Внешнее тестирование front-end уязвимостей в сфере перс. данных. **68% компаний никогда не проверяли** свой front-end комплаенс *

* согласно опросу Comply в апреле-мае 2022 г.

Comply.Privacy: Pentest

Собственная методология на базе:

- 100+ проведенных аудитов
- 10+ проверок Роскомнадзора
- своей библиотеки уязвимостей и bugbounty@Comply

Зачем нужен privacy-pentest?

- Выявляет privacy-уязвимости, которые могут эксплуатироваться 3-ми лицами извне
- Устраняет наиболее критичные риски, которые несут немедленный негативный эффект для компании
- Дает максимально объективную комплексную оценку безопасности внешнего privacy-периметра компании
- Обнаруживает отсутствие процессов privacy-комплаенса или недостатки контролей в таких процессах

Традиционный аудит: **100%** рисков	• Проверки Роскомнадзора, но (i) в этом году все проверки отменены, (ii) риски из проверок не носят немедленный эффект, т.к. 6 месяцев на устранение	• Однократные штрафы по КоАП • Запрет обработки ПД
Privacy pentest : **95%** рисков	Источники • Дистанционный контроль Роскомнадзора • Клиенты и бывшие клиенты • Privacy-экстремисты • Ассоциации (коллективные иски) • Конкуренты • Запросы Роскомнадзора	Риски • Кратное применение штрафов КоАП • Утрата лояльности клиентов и инвесторов • Повышенное внимание регуляторов • Необходимость сбора новых согласий • Блокировка сайтов и приложений • Коллективные иски

В сравнении с традиционным аудитом в сфере персональных данных (ПД) privacy-pentest гораздо эффективнее и не создает дополнительной проектной нагрузки на компанию.

В сравнении с privacy-pentest стоимость и сроки выполнения аудита в сфере ПД во много раз выше, хотя аудит дополнительно исключает только риски из проверок Роскомнадзора.

Методология проверки

Этап **#1**
комплексное выявление уязвимостей

- Найдем все точки / каналы поступления запросов, вкл. сайты, формы, приложения, колл-центры и т.д.
- Пройдем все сценарии Customer Journey (CJM), вкл. регистрацию, подписку, заказ и т.д.
- Отработаем все типы запросов субъектов и возможные векторы атаки 3-х лиц
- Проанализируем процедуры реагирования
- Проверим весь front-end комплаенс, вкл. политики, уведомления, баннеры, механику принятия условий

→ **Отчет** о front-end privacy-уязвимостях и **рекомендации** по устранению

Этап **#2**
устранение «под ключ» [опционально]

- Интервью ответственных работников за исполнение запросов в каждом сервисе/точке контакта с субъектом
- Согласование предлагаемого дизайна DSR-процесса с владельцами
- Согласование уточнений в документы и рекомендаций по CJM
- Подготовка front-end документов, а также внутреннего регламента, вкл. SLA по каждому типу запроса, формат ответа, критичность и сроки реагирования, роли вовлеченных работников и случаи эскалации, контрольные точки
- Внедрение процесса и контролей вкл. тренинги

→ Превентивно **внедрена система защиты** front-end периметра от возможных рисков

Учтем фреймворки 152-ФЗ и GDPR, если применим

Тест проводится по модели black-box, что позволяет:

- получить максимально объективную информацию о состоянии процессов компании и
- выполнить проект полностью автономно с минимальным вовлечением работников компании

Возможны иные форматы: white- / grey-box, offline и т.д.

Стоимость Этапа #1 – от 50 000 до 150 000 (НДС не применяется) вкл. тест по всем каналам коммуникации с вашим ключевым клиентом *

Сроки ~ 1-3 недели

Стоимость Этапа #2 [опционально] – в зависимости от объема выявленных уязвимостей, зрелости и сложности процессов

* Стоимость может отличаться, если у компании много сервисов, имеющих различный CJM
** Платные подписки и курьерские расходы согласуются заранее и не включены в стоимость

Артем Дмитриев
Управляющий партнер

artem.dmitriev@comply.ru
t.me/artydmitriev
+7 (961) 806 27-76

Comply.
comply.ru
info@comply.ru
t.me/comply_ru

Общество с ограниченной ответственностью «Комплаенс Офис» | ОГРН 1207800126742 | ИНН 7811751473