

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Тестове за проникване в десктоп приложения

Тестваме приложението, което потребителите инсталират, данните, които съхранява, и услугите, на които се доверява. Получавате възпроизводими доказателства, приоритетни корекции и включен повторен тест в предварително договорен обхват.

ПОДХОДЯЩО ЗА	Корпоративен десктоп софтуер, клиентски приложения и проверка преди нова версия
ПОЛУЧАВАТЕ	Резюме за ръководството, технически констатации, насоки за корекции и потвърждение от повторния тест
ОБХВАЩА	Десктоп клиенти, инсталатори и API

Приложението работи на машина извън вашия контрол.

Нападателят разполага с бинарните файлове, конфигурацията и работещото десктоп приложение. Скрит бутон, шифрована локална настройка или забранено меню не заменят проверката на права на сървъра. Изследваме кои защити остават ефективни, когато клиентът бъде анализиран, променен или стартиран от обикновен потребител.

Проследяваме границите на доверие около приложението: локални файлове и данни за достъп, привилегирвани услуги, комуникация между процеси, инсталиране и обновяване и сървърния API. Свързваме слабостите само в договорения обхват и доказваме въздействието с контролирани тестови данни.

Какво може да включва обхватът

- Windows приложения, включително .NET и приложения с нативен код
- Electron и други десктоп клиенти, изградени с уеб технологии
- Java клиенти; версии за macOS и Linux по договорка
- Локални бази данни, конфигурация, логове, кеш и данни за достъп
- Инсталатори, пакети за обновяване, подписи и зареждане на библиотеки
- Привилегирвани услуги и комуникация между процеси (IPC)
- Удостоверяване, сесии, контрол на достъпа и сървърни API
- Целеви обратен инженеринг и тестове на входни данни, когато са приложими

Как протича

- Уточняваме обхвата — Договаряме версиите, операционните системи, ролите, тестовите акаунти, API и началната позиция на тестера.
- Анализираме приложението — Преглеждаме пакета, локалното съхранение и поведението при изпълнение; картографираме привилегированите компоненти и мрежовата комуникация.
- Проверяваме защитите — Тестваме клиентските проверки, локалните права, доверието при обновяване и сървърния контрол на достъпа с възпроизводими доказателства.
- Доклад, обсъждане и повторен тест — Обсъждаме констатациите с инженерите ви, подреждаме корекциите по приоритет и проверяваме договорените поправки.

Какво получавате

- Резюме за ръководството — Въздействието върху бизнеса и решенията, които ръководството трябва да вземе.
- Технически доказателства — Засегнати версии, предпоставки, стъпки за възпроизвеждане и контролирано доказателство за въздействието.
- Практически корекции — Насоки за отстраняване на първопричината, подредени по риск и възможност за експлоатация.
- Включен повторен тест — Проверка на съобщените поправки в обхвата и срока, договорени в офертата.

Старши тестери. Доказателства за всяка констатация. Включен повторен тест. Минимум пет дни тестване. Обхват и примерни доклади — pxlsec.com/bg/services/desktop-application-penetration-testing.