

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Тестове за проникване в Wi-Fi мрежи

Проверяваме кой може да се свърже с безжичната ви мрежа, на какво се доверяват устройствата и до кои системи получават достъп. Получавате доклад с доказателства, приоритетни корекции и включен повторен тест в договорения обхват.

ПОДХОДЯЩО ЗА	Корпоративни и гост мрежи, лични устройства и IoT; преместване на офис или промени в инфраструктурата
ПОЛУЧАВАТЕ	Констатации за безжичната мрежа, доказани пътища за достъп, насоки за корекции и потвърждение от повторния тест
ОБХВАЩА	Безжичен достъп, удостоверяване и сегментация

Безжичният сигнал не бива да отваря път към вътрешните ви системи.

Границата на безжичната мрежа не свършва на рецепцията. Посетител, устройство в съседно помещение или компрометиран служебен лаптоп може да е достатъчно близо, за да взаимодейства с нея. Силното шифроване е само част от защитата: важни са удостоверяването, настройките на устройствата и достъпът, предоставен след свързване.

Тестваме договорените безжични мрежи и защитните граници около тях. Проверяваме как се удостоверяват потребителите и устройствата, дали клиентите разпознават доверената мрежа и дали гост или неуправлявано устройство може да достигне корпоративни услуги. Доказваме достъпните пътища с разрешени акаунти и контролирани тестови данни.

Какво може да включва обхватът

- Договорени обекти, SSID, точки за достъп и Wi-Fi профили на устройствата
- Настройки на WPA2/WPA3-Personal и управление на споделените ключове
- WPA2/WPA3-Enterprise, 802.1X, EAP и проверка на сървърния сертификат
- Гост мрежи, портали за достъп и изолация между клиентските устройства
- Сегментация между корпоративни, гост, BYOD и IoT мрежи
- Изрично разрешени сценарии с неоторизирани точки за достъп и имитация на мрежа
- Достъп до договорени вътрешни услуги след свързване към мрежата
- Проверка на безжичния мониторинг и сигнализирането, ако са в обхвата

Как протича

- Уточняваме обектите и обхвата — Договаряме обекти, SSID, идентификатори на точките за достъп, устройства, тестови акаунти, разрешени техники и условия за спиране.
- Картографираме и преглеждаме — Наблюдаваме разрешената безжична среда и преглеждаме съответните настройки на точките за достъп, контролерите и устройствата.
- Проверяваме достъпа и изолацията — Тестваме удостоверяването и доверието на клиентите, след което проверяваме какво достига всяка договорена роля. Активните сценарии се изпълняват само в разрешените времеви прозорци.
- Доклад и повторен тест — Обясняваме констатациите, подкрепяме промените по приоритет и проверяваме договорените поправки. Радиотестовите може да изискват повторно посещение на място.

Какво получавате

- Резюме за ръководството — Въздействието върху бизнеса и най-важните пропуски в достъпа или изолацията.
- Технически доказателства — Засегнати мрежи, предпоставки, наблюдавано поведение и възпроизводими доказателства с контролирани тестови данни.
- План за отстраняване — Приоритетни промени в удостоверяването, клиентските профили, сегментацията и мониторинга.
- Включен повторен тест — Проверка на съобщените поправки в обхвата, при условията за достъп и в 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/wireless-penetration-testing.