



Готовност за тестване по DORA и NIS2

Два режима на ЕС — DORA за финансовите субекти и NIS2 за съществените и важните субекти — повишават изискванията към тестването на сигурността. Това е въведение на разбираем език за това как влияят на тестването ви и как да се подготвите. Документът е насока, а не юридически съвет.

PXLSecurity LTD. · София, България · pxlsec.com · Офанзивна сигурност от 2014 г.



НАРЪЧНИК ЗА СЪОТВЕТСТВИЕ

Готовност за тестване по DORA и NIS2

Два режима на ЕС — DORA за финансовите субекти и NIS2 за съществените и важните субекти — повишават изискванията към тестването на сигурността. Това е въведение на разбираем език за това как влияят на тестването ви и как да се подготвите.

Документът е насока, а не юридически съвет.

DORA (Акт за цифрова операционна устойчивост)

DORA се прилага за финансовите субекти в ЕС и за техните критични ИКТ доставчици. Освен широките изисквания за устойчивост, тя очаква редовно тестване на ИКТ системите — а за значимите субекти и усъвършенствано тестване за проникване, водено от заплахи (TLPT), съобразено с рамката TIBER-EU.

- Поддържайте програма за тестване, която обхваща важните ви ИКТ системи.
- Значими субекти: периодичен red teaming, воден от разузнавателна информация, срещу работещи системи.
- Включвайте разузнаване на заплахите, контролирайте риска и документирайте всичко.

NIS2 (Директива за мрежова и информационна сигурност)

NIS2 разширява обхвата на правилата на ЕС за киберсигурност към много повече „съществени“ и „важни“ субекти. Тя изисква мерки за управление на риска и средства за оценка на тяхната ефективност — което на практика означава редовна оценка на уязвимостите и тестване за проникване.

- Приемете мерки за управление на риска, съответстващи на изложеността ви.
- Тествайте и оценявайте ефективността на тези мерки.
- Бъдете готови да го докажете пред регулаторите.

Как да се подготвите

- ✓ Установете кой режим се прилага за вас и за кои системи.
- ✓ Въведете редовен ритъм на тестване, а не еднократно упражнение.
- ✓ За TLPT по DORA планирайте red teaming, воден от разузнавателна информация, с внимателен контрол на риска.
- ✓ Запазвайте отчетите от тестване и писмата от повторните тестове като доказателство.
- ✓ Работете с тестери, които могат да съотнесат констатациите към конкретните задължения.

PXLSec извършва тестването за проникване и воденият от заплахи red teaming, които тези режими изискват, с одитно готово отчитане. Пишете ни на hello@pxlsec.com или вижте pxlsec.com/bg/services/compliance-penetration-testing. Този документ е информационен и не представлява юридически съвет.

Работете с PXLSec

Независимо офанзивно тестване на сигурността от 2014 г. — тестване за проникване, red teaming и сигурна разработка, с доказателство за всяка констатация и повторен тест, който потвърждава поправката.

Заявете предложение: pxlsec.com/bg/contact · hello@pxlsec.com

PXLSecurity LTD. · бул. „Васил Левски“ 12, 1142 София, България · VAT BG203239331