



ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ



ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

ПЕНЕТРЕЙШЪН ТЕСТОВЕ



Сдружение Клъстер Айтос

Какво представляват тестовете за пробив?


Тестовете за пробив имитират реални заплахи към системи, приложения и данни, които могат да бъдат предизвикани от външни хакери, злонамерени служители, кибер-престъпни организации. Това е контролиран, оторизиран процес, който се провежда според изискванията на клиента и без да навреди по никакъв начин на изпитваните системи. Похватите и техниките, които използваме, позволяват откриването на уязвими звена в системите. Подлагаме тези точки на тест, след което обобщаваме резултатите и ви предоставяме доклад с включени препоръки и решения за отстраняването им.

Оценка на информационната сигурност

- Идентифициране и оценка на уязвимости
- Идентифициране на уязвимостите, които не са открити при автоматично сканиране (vulnerability scanning)
- Оценка на последиците и загубите в случай на успешна атака
- Проверка на реалната ефективност на мрежовата защита чрез изпълнението на по-чести, по-сложни и комплексни тестове, можете по-ефективно да предвидите рисковете за сигурността и да се предпазите от неоторизиран достъп до критични системи и ценна информация.

Защо да предприемете такъв тест?

- За оценка на нивото на защита на вашите мрежи, приложения, данни, системи и потребители
 - За защита на активите и репутацията на компанията чрез избягване на финансовите загуби и лошата реклама
 - За да разберете и оцените кои са критичните и уязвими места за организацията, кои са по-незначителни, както и да разграничите открити фалшиви положителни резултати (false positives).
 - За аргументация на нуждата от бюджет, свързан със сигурността пред висшето ръководство на компанията;
 - За по-ефективни и ефикасни методи за отстраняване на открити уязвимости и съответно повишаване на сигурността на системите в организацията;
 - За адресиране на основни изисквания, свързани с регулации и стандарти като ISO 27001, PCI-DSS, GDPR. По този начин се предотвратява налагането на високи санкции в случай на несъответствие.
- Пробивите в сигурността могат да доведат до преки финансови загуби, да



повлияят негативно на репутацията на организацията, да намалят доверието на клиентите както и до други негативни последици за компанията. Тестовите за пробив на информационни системи, които предлагаме, могат да бъдат приложени както като индивидуална поръчка, така и като част от стратегия за регулярно тестване на сигурността, продиктувана от необходимостта за покриване на изисквания по регулации и стандарти като ISO 27001, PCI-DSS, GDPR. Ние ще извършим бърза и качествена оценка на способността ви да защитите своите мрежи, приложения, данни, системи и потребители от недоброжелателни хакери.

www.eufunds.bg

Проект № BG16RFOP002-2.009-0043 „Развитие на капацитета и интернационализацията на продуктите на Клъстер Айтос /ITOS/“ финансиран от Оперативна програм „Иновации и конкурентоспособност“, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.