KONICA MINOLTA

PENETRAČNÍ TESTY INFORMAČNÍCH SYSTÉMŮ

PRO FIRMY A INSTITUCE

Penetrační test ověřuje odolnost bezpečnostních mechanismů, procesů, případně rizikovost chování zaměstnanců simulací reálného bezpečnostního incidentu. Cílem tohoto simulovaného útoku je zjistit, do jaké míry je konkrétní informační systém odolný vůči napadení, kde jsou jeho slabá místa a jak je nejlépe odstranit.

POŽADOVANÉ VSTUPY OD ZÁKAZNÍKA

Zadání penetračního testu je velmi jednoduché. Musí obsahovat pouze níže uvedené požadavky, ostatní informace si již útočící konzultant zjišťuje sám:

a. stanovení cíle testu – získání konkrétní důvěrné informace nebo získání neoprávněného přístupu do systému, lokality apod.

b. stanovení velikosti úsilí útočníka – stanovení maximálního množství času, který testující věnuje přípravě a realizaci testu (viz varianty níže)

c. definování omezujících podmínek – např. oblasti, které testovány být nemají, protože představují riziko, dále kdy lze testovat, kdy naopak nelze apod.

VÝSTUPY SLUŽBY

- Výstupem testu je podrobná zpráva s popisem metodiky testování, dokumentace všech provedených testovacích kroků, zjištěných slabin, jejich kategorizace a návrh nezbytných protiopatření pro jejich eliminaci.
- Výsledky testu jsou vždy prezentována klientovi na společném on-line workshopu.
- Po provedeném testu jsou veškeré stopy, informace o testu a zjištěných slabinách protokolárně u testujících zničeny. Konica Minolta IT Solutions Czech neuchovává zpětně žádné informace o zjištěných slabinách.

CENA

1. Light test

Penetrační test v rozsahu testu bezpečnostních slabin perimetru internetu a web serverů. Způsob provedení je posloupnost poloautomatizovaných testů provedených z internetu. Klient získá informace o míře zabezpečení perimetru, e-mailového a webového serveru, o slabinách použitých technologií a konfiguračních chybách.

Perimetrem internetu se rozumí celá infrastruktura, která tvoří rozhraní mezi interní LAN sítí a internetem (firewall, routery, demilitarizované zóny, e-mailové servery, web servery), tedy vše, co je vidět zvenčí z internetu.

Tento test je vhodný pro menší subjekty s nepříliš sofistikovaně řešeným perimetrem internetu (klient provozuje jeden firewall, e-mail server, má jednu demilitarizovanou zónu, jeden přístupový bod, například pro home office připojení).

- **Cena testu:** 65.000 Kč bez DPH
- **Doba realizace:** 2 týdny

2. Medium test

Medium test rozšiřuje Light test o následné manuální hloubkové testování konzultantem tam, kde jsou zjištěny zranitelnosti. Součástí testu je i prověření ochrany WiFi sítí testováním na místě.

- **Cena testu:** 130.000 Kč bez DPH
- **Doba realizace:** 4 týdny

3. Heavy test

Nad rámec Medium testu jsou zde součástí i zátěžové testy, testy uživatelů formou phishingové kampaně, útoky využívající metod sociálního inženýrství s cílem získání přístupu k interním systémům, útoky vedené s cílem získání vzorku dat extrahovaných z informačních systémů.

- **Cena testu:** 290.000 CZK
- **Doba realizace:** 6 týdnů

KONICA MINOLTA

Konica Minolta IT Solutions Czech a.s., U Plynárny 1002/97, 101 00 Praha 10, its@konicaminolta.cz, www.konicaminoltaits.cz