

PENETRAČNÍ TESTY

I nejspolehlivější bezpečnostní systém je pouze teoretickou obranou proti útokům, dokud není vyzkoušen v praxi. Samozřejmě nemá smysl čekat na skutečný útok, ideální je řízená zkouška robustnosti a spolehlivosti bezpečnostních opatření, kterými firma chrání citlivá data.

Simulovaný útok

Naši specialisté prověří nejen bezpečnostní řešení implementované naší společností, ale i ochranné prvky, které již klient používá. Penetrační test spočívá v útoku, samozřejmě v souladu s pokyny klienta. Cílem testu je zjištění, jak je firemní prostředí chráněno proti krádeži dat, jak je zajištěna integrita firemního informačního systému a zda správně pracují systémy zajišťující dostupnost či odepření služeb.

Interní penetrační testy

Jednou z možností otestování bezpečnosti je simulovaný útok z vnitřního prostředí. Naši specialisté tak na sebe berou roli narušitele, který se s nekalými úmysly připojuje do informačního systému přímo z prostředí firmy. Interní penetrační test lze provést dvěma způsoby. První představuje situaci se znalostí prostředí (simuluje například situaci, kdy se zaměstnanec snaží získat data, ke kterým běžně nemá přístup). Druhou variantou je útok bez znalosti prostředí, tedy simulace typové situace, kdy se o útok pokusí cizí osoba, která ovšem má přístup k vnitřní síti nebo použije vzdálený přístup.

Externí penetrační testy

Externí penetrační testy jsou zaměřeny na prověření stupně zabezpečení prvků a služeb dostupných z vnějšího prostředí, z internetu. Testy jsou zaměřené hlavně na oblast bezpečného připojení k internetu a ověřují správnou konfiguraci nabízených služeb. Cílem externích testů je důkladná prověrka bezpečnostního nastavení a ověření zranitelnosti nástrojů staršími i novějšími druhy elektronických útoků.

Vyhodnocení a návrh opatření

Všechny provedené penetrační testy je samozřejmě nutné řádně vyhodnotit. Naši specialisté vypracují detailní dokumenty o výsledcích testů. Zároveň navrhnou vhodné úpravy, které odstraní nedostatky odhalené penetračními testy. Díky znalosti kompletního portfolia bezpečnostních produktů navrhujeme ucelená řešení, která zapadnou do celkové firemní strategie klienta. Jsme navíc připraveni pro klienta připravit návrh celé bezpečnostní strategie a postarat se o její implementaci.

VÝHODY

Jediná spolehlivá metoda ověření bezpečnosti

- bezpečná simulace útoku
- analýza výsledků a zjištěných nedostatků
- návrh vylepšení bezpečnostní infrastruktury
- možnost vypracování nové bezpečnostní strategie a její implementace

Ověření všech složek informačního systému

- ověření důvěrnosti
- ověření integrity
- ověření dostupnosti

Ucelené a spolehlivé testy

- interní testy
- externí testy
- test bezpečnosti síťového protokolu
- test bezpečnosti vzdáleného přístupu

Ověření všech složek

- norma BS ISO/IEC 17799:2005

