



G - Pentest E

Externé penetračné testovanie

Crash-testy nezávislých inštitúcií sú vynikajúcim prostriedkom hodnotenia automobilov. Na ich základe si môžete povedať, že váš automobil je skutočne bezpečný.

**A čo môžete povedať o vašom informačnom systéme?
Ako dopadol v testovaní bezpečnosti?
Kedy bol testovaný?**



GORDIAS
IT • SECURITY

G - Pentest E

Externé penetračné testovanie bezpečnosti IS

Vo veľkej väčšine súčasných firiem je obvykle používaný celý komplex rôznych operačných systémov a aplikácií. Do podnikových procesov sú integrované aj služby internetu. Softvérové prostredie je teda veľmi komplikované a mnohvrstvé.

Pri komerčnom i voľne šíriteľnom softvéri je dôležité si uvedomiť, že **každý týždeň sa objaví niekoľko nových bezpečnostných chýb v štandardne používaných a populárnych softvérových produktoch**. Zneužitie týchto chýb predstavuje vážne narušenie bezpečnosti, pretože jeho dôsledkom je únik, strata či zmena údajov, strata dostupnosti služieb alebo kontroly nad službami.

Prieniky z internetu, narušenie dostupnosti služieb či infiltračia sú dnes vážnou hrozbou. Je potrebné periodicky prehodnocovať dostatočnosť, konzistentnosť a vhodnosť použitých bezpečnostných opatrení. Mechanizmom, ktorý prakticky overí účinnosť ochranných prvkov, je externé penetračné testovanie.

Najčastejšie bezpečnostné problémy, ktorých pôvod súvisí s používaním internetu, sa týkajú:

- najrozšírenejších operačných systémov - všetkých verzií operačných systémov firmy Microsoft a variantov systému UNIX (komerčných i voľne šíriteľných),
- štandardne používaného programového vybavenia poskytujúceho služby cez Internet - WWW servery, prehliadače a programy doručujúce elektronickú poštu,
- počítačových vírusov, červov a iného šíriaceho sa zlomyseľného kódu.

Útočníci sú stále v strehu

Sledujú verejné i uzavreté zdroje informácií, takže už v priebehu niekoľkých hodín po zverejnení chyby sa internetom šíri vlna pokusov o jej zneužitie. Bezpečnostné opatrenia na minimalizáciu prieniku je **preto potrebné realizovať** bezprostredne po zverejnení chyby. Navyše je nutné priebežne testovať, či je úroveň opatrení dostatočná.

Vaše problémy vie vyriešiť spoločnosť GORDIAS

Ponúka vám pravidelné testovanie vašich počítačov, aktívnych sieťových prvkov, operačných systémov a aplikácií formou simulovaného útoku.

GORDIAS monitoruje špecializované oznamy a diskusie o bezpečnosti, hlásenia o útokoch, „hackerské“ fóra ako aj ďalšie informačné zdroje. O novej chybe v programoch, ktoré používate, budete informovaní okamžite. A navyše môže byť odolnosť vášho systému hneď otestovaná.

Realizácia externého penetračného testovania

Penetračné testovanie je tvorené súborom simulovaných útokov cez internet. Jeho cieľom je overiť dostatočnosť a účinnosť existujúcich bezpečnostných opatrení. Testovanie je vykonávané kombináciou špecializovaných softvérových nástrojov a interaktívnych pokusov o prienik. Penetračné testovanie je nedeštruktívne.

Výsledkom penetračného testovania je záverečná správa, ktorá:

- dokumentuje vykonané bezpečnostné testy,
- podrobne vysvetľuje testy, ak ich výsledok bol pozitívny (odhalili sa zneužiteľné chyby),
- klasifikuje výsledky pozitívnych testov podľa ich významu,
- odporučí postup odstránenia zistených bezpečnostných nedostatkov.

Informácie o bezpečnostných chybách sa objavujú prakticky nepretržite a situácia v tejto oblasti sa dynamicky mení. Z tohto dôvodu je vhodné vykonávať penetračné testovanie periodicky (napríklad raz za 6 mesiacov).

GORDIAS vám ponúka trvalé sledovanie stavu bezpečnosti. Uskutočňuje sa na základe zoznamu komponentov, operačných systémov a aplikácií, ktoré sú u vás využívané.

Dôverujete bezpečnosti vášho informačného systému? Dajte si ho teda otestovať, veď anekdota hovorí, že kontrola je najvyššia forma dôvery...

