SKEN ZRANITEĽNOSTÍ

Ak Vaša spoločnosť ešte nebola podrobená penetračným testom, sken je dobrým štartovacím bodom na zlepšenie bezpečnosti Vašich aktív v infraštruktúre.

Sken býva vykonávaný automatizovanými nástrojmi, ktoré zozbierajú informácie o vašich komponentoch infraštruktúry a porovnajú ich s databázami známych zraniteľností. Tieto zraniteľnosti sa počas testu nezneužívajú.

Pravidelné vykonávanie skenov je jedným z odporúčaných opatrení vedúcim ku kontinuálnej bezpečnosti.

Po ukončení skenu obdržíte prehľadný report zraniteľností spolu s odhadom technického rizika. Pre každú identifikovanú zraniteľnosť obdržíte konkrétne opatrenie, ktoré je nutné aplikovať na odstránenie problému.

Test vykonaný z externého prostredia sa sústreďuje na všetky systémy a aplikácie dostupné z internetu, pričom sa overuje či sú dostatočne zabezpečené proti preniknutiu do vnútornej siete Vašej organizácie.

Bezpečnosť vnútorných systémov by nemala byť zanedbávaná a test vykonaný z interného prostredia je rovnako dôležitý ako test vonkajšieho prostredia (z internetu). Sken vnútorného prostredia identifikuje a klasifikuje zraniteľnosti interných aktív vašej organizácie.

Cena bezpečnostného skenu infraštruktúry záleží od počtu skenovaných zariadení a periodicity vykonávania služby.

Výhody oproti penetračnému testovaniu:

- Lacnejšie
- Kratšie čakanie na výsledky (sken trvá obvykle kratšie ako štandardný penetračný test)
- Výsledky sú dostupné okamžite po skončení testov

Nevýhody oproti penetračnému testovaniu:

- Odhalí len známe zraniteľnosti
- Viac náchylné na nesprávne (false-positive) identifikované zraniteľnosti
- Nie je možné overiť či momentálne implementované ochranné mechanizmy dokážu zabrániť exploitácií
- Nie je možné overiť skutočné technické riziko, keďže neprebehne pokus o zneužitie nájdených zraniteľností (exploitácia)