Penetračné testy praktikami sociálneho inžinierstva

ÚVOD

Najzraniteľnejším činiteľom v organizácii je spravidla jej zamestnanec. Môže byť predmetom záujmu útočníkov snažiacich sa o kompromitáciu alebo získanie osobného prospechu na úkor napadnutej organizácie, jej partnerov alebo zákazníkov. Ako eliminovať riziká spojené so zneužitím dôvery alebo chýb v správaní zamestnanca? Základným predpokladom je vytvorenie interných pravidiel pre zamestnancov a budovanie bezpečnostného povedomia. Súčasťou dobrej praxe v každej oblasti riadenia je aj efektívna kontrola zavedených opatrení. Najúčinnejším spôsobom preverenia bezpečnostného povedomia zamestnancov, znalosti interných predpisov a ich dodržiavania v bežnej praxi je simulácia potenciálnych útokov – realizácia penetračných testov praktikami sociálneho inžinierstva.

CIEĽ

Otestovať a vyhodnotiť správanie zamestnancov v rôznych situáciách a preveriť súlad ich správania s internými pravidlami a dobrou praxou v oblasti informačnej bezpečnosti.

POPIS

Penetračné testovanie praktikami sociálneho inžinierstva je pokusom o riadenú kompromitáciu informačných aktív testovanej organizácie pomocou komunikačných zručností, technických prostriedkov a komunikačných kanálov.

Konanie zamestnancov môže byť preverené v rôznych oblastiach správania:

- e-mailová komunikácia,
- telefonická komunikácia,
- faxová komunikácia,
- narábanie s prenosnými médiami,
- fyzický vstup do priestorov,
- dodržiavanie pravidiel skartácie a likvidácie informácií, prípadne v iných.

Testovanie využíva rôzne faktory ovplyvňujúce ľudské správanie - podriadenie sa autoritám, plnenie požiadaviek na základe sympatií, pod vplyvom stresujúcich faktorov, plnenie požiadaviek podporené logickým zdôvodnením alebo ďalšie.

Kľúčovým predpokladom úspešného testu je realizácia vhodných scenárov, ktoré odrážajú špecifiká, požiadavky a potreby testovanej organizácie. Testovacie scenáre sú preto vždy pripravované na mieru konkrétnej organizácie.

Testovanie sa môže uskutočniť pri rôznom rozsahu informácií, ktoré testovaný subjekt vopred sprístupní. Testy môžu simulovať rôzne druhy útokov, napr. útočníka dobre oboznámeného s interným fungovaním organizácie, útočníka mimo organizácie bez znalostí, dodávateľa alebo bývalého zamestnanca s čiastočnými znalosťami, súčasného zamestnanca s istou úrovňou fyzického a logického prístupu a pod.

VÝSTUPY

Výstupom je správa o výsledkoch a priebehu testovania. Súčasťou správy je aj návrh nápravných opatrení zameraných na odstránenie zistených nedostatkov.

METÓDA

ESET používa vlastnú metodiku, ktorá vychádza z dobrej praxe a skúseností tímu špecialistov v oblasti informačnej bezpečnosti.

Testovacie praktiky nie sú deštruktívne a získané informácie sú chránené dohodou o mlčanlivosti medzi testovanou organizáciou a ESETom.

VIAC INFORMÁCIÍ

www.eset.sk/services
services@eset.sk

O ESET Services: Spoločnosť ESET, založená v roku 1992, je svetovým výrobcom bezpečnostného softvéru pre domácich i firemných zákazníkov. Rozširovanie portfólia služieb vyústilo v roku 2008 do akvizície Šetrnet, českej spoločnosti s dlhoročnými skúsenosťami v oblasti IT a bezpečnosti. V roku 2009 bola vytvorená divízia ESET Services, ktorá poskytuje produkty manažovanej bezpečnosti a konzulting pre malých a stredných podnikateľov (SMB) a pre veľkých firemných (Enterprise) zákazníkov. Výhradné zameranie sa na služby informačnej bezpečnosti sleduje poskytnutie maximálnej pridanej hodnoty v tejto oblasti. Zázemie ESET, globálne uznávaného dodávateľa bezpečnostných riešení a dôraz na odbornosť pracovníkov ESET Services je garantom kvality poskytovaných služieb.