Penetrační testy praktikami sociálního inženýrství

ÚVOD

Nejzranitelnějším činitelem v organizaci je z pravidla její zaměstnanec. Může být předmětem zájmu útočníků snažících se o kompromitaci nebo získání osobního prospěchu na úkor napadené organizace, jejich partnerů nebo zákazníků. Jak eliminovat rizika spojená se zneužitím důvěry a nebo chyb v chování zaměstnance? Základním předpokladem je vytvoření interních pravidel pro zaměstnance a budování bezpečnostního povědomí. Součástí dobré praxe v každé oblasti řízení je i efektivní kontrola zavedených opatření. Nejúčinějším způsobem prověření bezpečnostního povědomí zaměstnanců, znalosti interních předpisů a jejich dodržování v běžné praxi, je simulace potenciálních útoků - realizace penetračních testů praktikami sociálního inženýrství.

CÍL

Otestovat a vyhodnotit chování zaměstnanců v různých situacích a prověřit soulad jejich chování s interními pravidly a dobrou praxí v oblasti informační bezpečnosti.

POPIS

Penetrační testování praktikami sociálního inženýrství je pokusem o řízení kompromisu informačních aktivit testované organizace pomocí komunikačních zručností, technických prostředků a komunikačních kanálů.

Působení zaměstnanců může být prověřeno v různých oblastech chování:

- e-mailová komunikace
- telefonická komunikace
- faxová komunikace
- správné zacházení s přenosnými médii
- fyzický vstup do prostoru
- dodržování pravidel skartování a likvidace informací

Testování využívá různé faktory ovlivňující lidské chování - podřízení se autoritám, plnění požadavků na základě sympatií, pod vlivem stresujících faktorů, plnění požadavků podpořených logickým zdůvodněním a další. Klíčovým předpokladem úspešného testu je realizace vhodných scénářů, které odrážejí specifikace, požadavky a potřeby testované organizace. Testovací scénáře jsou proto vždy sestavované na míru konkrétní organizace. Testování se může uskutečnit při různém rozsahu informací, které testovaný subjekt předem zpřístupní. Testy mohou simulovat různé oblasti útoku, např. útočníka dobře obeznámeného s interním fungováním organizace, útočníka mimo organizaci bez znalostí, dodavatele nebo bývalého zaměstnance s částečnými znalostmi, současného zaměstnance s jistou úrovní fyzického a logického přístupu apod.

VÝSTUPY

Výstupem je zpráva o výsledcích a průběhu testování. Součástí zprávy je i návrh nápravných opatření zaměřených na odstranění zjištěných nedostatků.

METODA

ESET používá vlastní metodiku, která vychází z dobré praxe a zkušeností týmu specialistů v oblasti informační bezpečnosti.

Testovací praktiky nejsou destruktivní a získané informace jsou chráněné dohodou o mlčenlivosti mezi testovanou organizací a ESETem.