Penetrační testy praktikami sociálního inženýrství

AEC

Pomůžeme vám vytvořit povědomí a snížit riziko vniknutí

Lidský faktor je kvůli nedostatečnému vzdělávání primárním bezpečnostním rizikem pro data a informace napříč všemi společnostmi. Vzdělávání uživatelů rizika úniků dat výrazně snižuje.

Při testech sociálním inženýrstvím vám vzdělávací plán přizpůsobíme na míru. Provedeme test zahrnující shromažďování informací, vishing, phishing, spear-phishing nebo fyzické vniknutí. Výsledky prezentujeme ve zprávě, která identifikuje úroveň povědomí o vašich uživatelích a zranitelností vaší organizace. Představíme vám konkrétní opatření, která byste měli přijmout a která jsou přizpůsobena tak, aby se zvýšila vaše ochrana před hrozbami – či už interními nebo externími.

www.aec.cz

Penetrační testy praktikami sociálního inženýrství

Phishing jako služba – provádíme formou e-mailových penetračních testů jednorázově nebo ve formě kontinuální kampaně. Cílem phishingové kampaně je prověření aktuálního stavu zabezpečení společnosti a vzdělání zaměstnanců simulovaným phishingovým útokem.

Vishing jako služba – představuje telefonické penetrační testy, které stejně jako při phishingu provádíme jednorázovou nebo kontinuální formou. Samotný test je simulací reálného telefonického útoku. Při podvodném telefonátu se útočník snaží získat informace nebo uživatele přesvědčuje k akci, která může narušit bezpečnost vaší organizace.

Penetrační test praktikami sociálního inženýrství – je komplexní služba, která může zahrnovat kombinaci phishingu, vishingu a fyzické infiltrace, ve které se náš tým sociálních inženýrů pokouší o průnik do chráněných prostor organizace. Služba pomáhá odhalit náchylnosti k útokům vedenými praktikami sociálního inženýrství.

KnowBe4 – je největší světová integrovaná platforma pro školení zaměstnanců v oblasti bezpečnosti. Nabízí simulované útoky phishingu, vishingu nebo zjištění reakce zaměstnanců na neznámé USB zařízení. Kromě možnosti simulací útoků nabízí platforma také videa vzdělávacího charakteru na témata phishing, bezpečnostní povědomí, hesla, mailová bezpečnost, malware a jiné.

Penetrační testy praktikami sociálního inženýrství

Phishing

představuje jeden z nejznámějších útoků pomocí sociálního inženýrství a jedná se o samotný akt rozposlání potenciálně škodlivých e-mailů, které se tváří, že pocházejí z důvěryhodných zdrojů. Cíle phishingu lze rozdělit takto:

- doručení škodlivých dat, která poskytují přístup vzdáleným útočníkům
- shromažďování přihlašovacích údajů
- shromažďování dalších kousků informací pro další útoky

Cílem phishingu jako služby je vzdělávání zaměstnanců pomocí simulace útoku. Rozesíláme e-mail, který detekuje chování uživatele hned po jeho doručení. Výsledkem jsou statistiky, které ukazují, v jaké míře jsou zaměstnanci náchylní k vektoru útoku phishingu a kde bude potřebné další vzdělávání. Výstupem jsou dva reporty, první průběžný, který informuje o provedených akcích uživatelů a rovněž obsahuje všechny měřené metriky. Druhý formální obsahuje popis scénáře, získaných dat, popis chování uživatelů, doporučení a poměření s předchozími kampaněmi.

Vishing

je možné definovat jako telefonický phishing. Během podvodného telefonátu používá útočník metody sociálního inženýrství, aby donutil oběť sdílet informace a vykonat určitou akci.

- sdílet určitou informaci
- vykonat určitou akci

Vishing jako služba má také vzdělávací charakter. Jde o telefonáty s plně řízeným lidským přístupem. Službu vykonává tým sociálních inženýrů, kteří využívají dynamické záminky k nepřetržitému získávání kritických dat od zaměstnanců. Při interním penetračním testu využíváme technologii VoIP, se kterou zaměňujeme ID volajícího za důvěryhodný zdroj, při externím testu pak přicházejí hovory z telefonních čísel mimo organizaci. Scénáře hovorů upravujeme na míru a jednotlivé hovory z edukačních důvodů nahráváme. Výstupem je formální zpráva, která obsahuje detailní popis scénářů, měřené metriky, akce uživatelů, poměření s předchozími kampaněmi a doporučení.

Penetrační test z pohledu sociálního inženýrství

V tomto komplexním testu využíváme phishing, vishing a fyzickou infiltraci. Na začátku testu společnost určí svoje kritická aktiva. Náš tým sociálních inženýrů pak vykoná průzkum informací napříč internetem i darknetem, přičemž důraz klademe na kritická aktiva společnosti. Na základě získaných informací vypracujeme potenciální scénáře útoku. Následuje samotné provedení penetračního testu, který ověří existující proces nebo politiku v návaznosti na definovaná aktiva. Výstupem je detailní zpráva s popisem scénářů, popis chování uživatelů a doporučení.

KnowBe4

přináší uživatelsky přívětivé prostředí, které vám umožní provádět simulované phishingové útoky. Obsahuje tisíce šablon s neomezeným použitím a také největší knihovnu školení o povědomí o bezpečnosti, včetně interaktivních modulů, videí, her, plakátů a zpravodajů. KnowBe4 vám umožní provádět automatizované tréninkové kampaně s naplánovanými upomínkovými e-maily. Výsledné zprávy jsou pak tvořeny z phishingových testů a školení.

Více na specializovaném webu .....
www.socialing.cz

Naše přednosti

- Patříme mezi zavedené české security firmy, na trhu úspěšně působíme již déle než 30 let.
- Máme více než 10 let zkušeností v oblasti sociálního inženýrství.
- Náš tým tvoří specialisté se zkušenostmi ze stovek dílčích projektů.
- Jsme držiteli certifikací eMAPT, CISSP, OSCP, OSCE, CEH a celé řady dalších.
- Provozujeme vlastní hackerskou laboratoř na výzkum v řadě oblastí, zabývajících se bezpečností různých řešení.
- Naslouchámе klientům a přizpůsobujeme testy jejich potřebám a časovým možnostem.
- Sledujeme moderní trendy v oblasti sociálního inženýrství.
- Při testování klademe důraz na individuální potřeby organizace.

Praha – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283