

Sociální inženýrství

Praktickým testem zvýšíme vašim zaměstnancům povědomí o možných bezpečnostních rizicích a zároveň snížíme pravděpodobnost infiltrace útočníků do vaší organizace.

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.

KnowBe4

Největší světová integrovaná platforma pro školení zaměstnanců v oblasti bezpečnosti, to je KnowBe4. **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 test praktikami sociálního inženýrství

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 slabá místa při útocích** vedenými praktikami sociálního inženýrství.



Phishing

Phishing představuje jeden z nejznámějších útoků pomocí sociálního inženýrství a jedná se o samotný akt rozeslání potenciálně škodlivých e-mailů, které se tváří, že pocházejí z důvěryhodných zdrojů. Cíle phishingu dělíme na:

- doručení škodlivých dat, která poskytují přístup vzdáleným útočnickům,
- 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 a kde bude potřebné další vzdělávání.

Výstupem jsou dva reporty – průběžný a formální. Průběžný informuje o provedených akcích uživatelů a rovněž obsahuje všechny měřené metriky. Formální obsahuje popis scénáře, získaných dat, popis chování uživatelů, doporučení a poměření s předchozími kampaněmi.

Vishing

Vishing je jako telefonický phishing. Jde o telefonáty s plně řízeným lidským přístupem. Službu vykonáváme v týmu sociálních inženýrů, kde využíváme 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.

KnowBe4

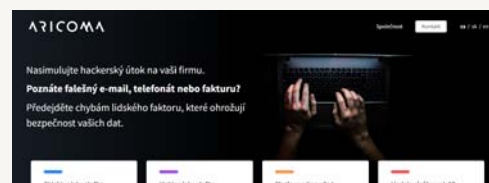
KnowBe4 přináší uživatelsky přívětivé prostředí, které vám umožní provádět simulované phishingové útoky. Obsahuje tisíce šablon s neomezeným použitím a také největší knihovnu školení z oblasti kybernetické bezpečnosti, včetně interaktivních modulů, videí, her, plakátů a zpravodajů.

KnowBe4 vám umožní provádět automatizované tréninkové kampaně s naplánovanými upomínkovými e-maily. Výsledné zprávy jsou pak tvořeny z phishingových testů a školení.

Přínosy

- Prověříme bezpečnostní povědomí členů vaší organizace.
- Odhalíme slabá místa, která vám nahlásíme.
- Po dokončení testu snížíte pravděpodobnost úniku svých dat.
- 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.

Více informací najdete na webu www.socialing.cz



Penetrační test z pohledu sociálního inženýrství

V tomto komplexním testu využíváme phishing, vishing a fyzickou infiltraci. Na začátku testu určíte svá kritická aktiva. Náš tým sociálních inženýrů pak vykoná průzkum informací napříč internetem i darknetem, při kterém klademe důraz na takto určená kritická aktiva.

Na základě získaných informací vypracujeme potenciální scénáře útoku. Následně provedeme penetrační test, který ověří existující proces nebo politiku v návaznosti na definovaná aktiva. Obdržíte poté detailní zprávu s popisem scénářů, popisem chování uživatelů a doporučení.