SAGA
A NOVENTIQ Company

USLUGA SIMULACIJE PHISHING[1] KAMPANJE

Simulacija phishing kampanje, putem e-mail poruka, je proaktivni pristup koji organizacije preduzimaju kako bi ojačale svoju odbranu protiv ovakvih pretnji. Ova metodologija predstavlja simulaciju stvarnih phishing napada unutar kontrolisanog okruženja.

Ovom uslugom, organizacije mogu proceniti podložnost svojih zaposlenih prema phishing pokušajima, identifikovati ranjivosti u svojim sigurnosnim sistemima i implementirati ciljane obuke i sigurnosne mere radi efikasnog smanjenja rizika.

KARAKTERISTIKE

- **PRILAGODLJIVI SCENARIJI** Kreiraćemo prilagođene phishing scenarije kako bismo oponašali napade iz stvarnog sveta
- **SIMULACIJA PHISHING LINKOVA** Procenite ponašanje prilikom klika na link
- **TESTIRANJE RAZLIČITIH ODELJENJA/ULOGA UNUTAR ORGANIZACIJE KROZ PRILAGOĐENE SCENARIJE**
- **IZVEŠTAVANJE I ANALITIKA** Sveobuhvatno praćenje rezultata
- **POKAZATELJ SVESTI** Merenje svesti i odziva zaposlenih
- **PRUŽANJE NEPOSREDNE POVRATNE INFORMACIJE ZAPOSLENIMA KOJI SU IMALI INTERAKCIJU SA SIMULIRANIM POKUŠAJIMA PHISHINGA**
- **TESTOVE IZVODE SERTIFIKOVANI PROFESIONALCI (OSCP I CEH SERTIFIKATI)**

KLJUČNE KORISTI

- POVEĆANJE SVESTI ZAPOSLENIH O PHISHING PRETNJAMA
- IDENTIFIKOVANJE SIGURNOSNIH SLABOSTI U SISTEMIMA ZA ZAŠTITU
- SMANJIVANJE RIZIKA OD USPEŠNIH PHISHING NAPADA
- PROMOVISANJE BEZBEDNIJIH NAVIKA NA INTERNETU
- SPREČAVANJE POTENCIJALNIH FINANSIJSKIH GUBITAKA
- UVID O PONAŠANJU ZAPOSLENIH I OBLASTIMA KOJE SE MOGU UNAPREDITI

REZULTATI

- Detaljni izveštaji o rezultatima svake simulirane kampanje.
- Podaci o stopi odgovora zaposlenih, stopi kliktanja i stopi odliva podataka.
- Predlozi za poboljšanje sigurnosnih mera.
- Edukativni Video sa opisom i rezultatima testiranja kao i praktičnim preporukama.

[1] Phishing (pecanje) jest pokušaj da se dobiju osetljive informacije kao što su korisnička imena, lozinke i podaci o kreditnoj kartici, prikrivajući se kao pouzdan entitet u elektronskoj komunikaciji