**POSTA ELEKTRONIKOARI EGINDAKO *PHISING* ERASOEN SIMULAZIO ERAKO IRTENBIDE BATEN KUDEATUTAKO ZERBITZURAKO BALDINTZA TEKNIKOEN PLEGUA ZIUR FUNDAZIORAKO (2023-026 ESPEDIENTEA)**

## I. ZERBITZUAREN HELBURUA ETA IRISMENA

Kontratuaren xedea da Ziur fundazioari emateko beharrezko laguntza teknikoa prestatzea 3 kanpaina burutzeko. Horietan posta elektronikora azken erabiltzaileei egindako *phising* erako erasoen simulazioaren kudeatutako zerbitzu bat gauzatuko da eta, ondoren, prestakuntza arloko edukia sortuko da. Baldintza Teknikoen Plegu honetan zehaztutako baldintzetan gauzatuko da. Baldintza horien bidez erakundeetako erabiltzaileen kontzientziazioari dagokionez egungo egoera ebalua daiteke, posta elektronikoari egindako *Spear Phising* erako erasoen egoera baten aurrean. Modu horretan, honakoak lortzeko beharrezkoak diren datuak lortu ahal izate aldera:

- Gipuzkoako enpresetan posta elektronikoan oinarritutako mehatxuen aurrean erabiltzaileen kontzientziazio/ezagutza eta sentiberatasun mailaren ikuspegi orokor bat eskuratzea,
- erabiltzaileentzat formatu ezberdinen inguruko prestakuntza arloko edukia sortzea, eraso-simulazioen gainean eskuratutako emaitzen arabera,
- phising erako mehatxuen aurrean erabiltzaileen kontzientziazio/ezagutza maila alderatzea, prestakuntza jaso aurretik eta ondoren,
- enpresetan zibersegurtasunaren kultura bat sortzea bultzatzea, jardun onenak aztura bilaka daitezen, uneko iradokizunetatik harago.

Eman beharreko zerbitzuaren izaera kontuan izanik, 72222300-0 CPV kodea, Informazioaren teknologiaren zerbitzuak izenekoa, esleitzea proposatzen da, kontratuko zerbitzuen artean hau adierazgarriena izateagatik.

## II. ZERBITZUAREN DESKRIBAPENA

Kontratuaren xede den jarduera garatu ahal izateko, esleipendunaren eginbeharrak hauek dira:

a) *Phising* erasoaren aurrean erantzuteko gaitasunaren ebaluazio bat egin eta erabiltzaileen segurtasuna eta betetze-jarrera modu integralean ebaluatzeko aukera ematen dion zibersegurtasunean kontzientziatzeko tresna bat erabilgarri izatea; kanpainak zein prestakuntza-edukiak diseinatu eta hedatzeko gaitasunarekin.

   Azken enpresan aplikatiboa eta hartako osagai guztiak hedatzeko beharrezkoak diren hardware eta software lizentzia guztiak lizitatzailearen kontura izango dira.

b) ZIUR Fundazioak izendatzen dituen pertsonak tresnaren erabileran prestatzea.
c) Zerbitzuan jasotako 2 kanpainak garatzea, bakoitza 6 hilabeteko iraupenarekin, ZIUR Fundazioak hautatutako enpresekin lotuta. Aipatu fundazioa izango da enpresak identifikatu eta hautatuko

dituena, eta kanpaina bakoitzean gutxienez 8 enpresak parte hartuko dute, esleipendunak egindako proposameneko baldintzetan parte-hartzaile kopurua areagotzearen kalterik gabe.

Horretarako, abian jartzeko lanetan kanpaina bakoitzean, eta horietan parte hartuko duten enpresa bakoitzean, zerbitzua abiarazteko beharrezkoa den oro jasoko da.

Kanpaina bakoitzeko beste hilabete bat luzatzea aurreikusi behar da, kasuren batean enpresaren baten kanpaina luzatu beharko balitz ere, langileen opor-agendara edo langileen lan-egoera handietara egokitzeko

ZIUR Fundazioa, zerbitzua emate aldera, aipatu enpresekin harremanetan ipiniko da, ZIUR Fundazioaren eta parte hartzen duen enpresa bakoitzaren arteko harremana juridikoa izango delarik (edozein kasutan). Zentzu horretan, dagozkion lankidetza-hitzarmenak formalizatuko dira Fundazioaren eta parte hartzen duten enpresen artean. Hitzarmen horien bidez, kontratuaren xedea betetze aldera, beharrezkoak diren enpresako bitartekoetarako sarbidea izatea ahalbidetuko da.

d) Kanpaina bakoitzean eta enpresa bakoitzarekin jarduera hauek burutzea:

- Aztergai den enpresa bakoitzean teknologia hedatzea
- Enpresa parte-hartzaile bakoitzeko langileekin batera, proiektuaren arduradun bat definitzea, enpresakoa, proiektuaren barne-jarraipenaz arduratuko dena, zerbitzuaren koordinazioa hobetzeko helburuarekin.
- Posta elektronikoen bidalketa zehaztu, modelatu eta pertsonalizatzea *phising* kanpaina bat simulatuz, horiek abiatzen diren aldi bakoitzeko Orokorrak enpresa guztietara Negozioaren premia, inguruabar edo arriskuen arabera pertsonalizatuak.
  - Orokorrak enpresa guztietara
  - Negozioaren premia, inguruabar edo arriskuen arabera pertsonalizatuak.
- Gaikuntza arloko prestakuntzako eduki interaktiboak zehaztu eta modelatzea enpresetako langileak lanlekuan zibersegurtasunarekin lotutako mehatxuen inguruan hezteko.
  - Orokorrak enpresa guztietara
  - Negozioaren premia, inguruabar edo arriskuen arabera pertsonalizatuak.
- Hautatutako erabiltzaile guztientzat posta elektroniko bidezko eraso simulatuen (*phising*) lehen abiaraztea.
  - Emaitzen analisia.
  - Erabiltzaileentzako prestakuntza arloko edukia eratzea.
  - Erabiltzaile indibidualen errendimenduari buruzko laburpenak sortzea, sail bakoitzeko, kanpaina bakoitzeko, enpresa bakoitzeko, etab.
  - Bilera enpresa bakoitzarekin, *phishing*-aren lehen simulazioaren emaitzak aurkezteko, enpresaren barneko arduradunarekin online prestakuntza koordinatzeko.
- Enpresetako erabiltzaileen prestakuntzarekin lotutako bigarren saio/txanda bat sortzea, erabiltzaileen gaikuntza indartzeko. Kasu honetan hornitzailearen, enpresaren eta ZIUR Fundazioko langileen artean gaia eta prestakuntza-euskarria hautatuko dira.

  - Fase honetan aldizkako harremana mantendu beharko da, inplikatu guztiek batera definituko dena, informazioa izan dezaten beren enpresako langile bakoitzak prestakuntza plana betetzeari eta hari laguntzeari buruz.
- Hautatutako erabiltzaile guztientzat posta elektroniko bidezko eraso simulatuen (*phising*) bigarren abiaraztea
  - Emaitzen analisia.
  - Erabiltzaileentzako prestakuntza arloko edukia eratzea.
  - Erabiltzaile indibidualen errendimenduari buruzko laburpenak sortzea, sail bakoitzeko, kanpaina bakoitzeko, enpresa bakoitzeko, etab.

e) Emaitzen analisia
- Kanpaina bakoitzean, eraso ezberdinak abiarazten diren bakoitzean, esleipendunak emaitzen analisi bat egin eta horiek balioetsi beharko ditu. Txosten horiek parte hartzen duten enpresei eta ZIUR fundazioko langileei helaraziko zaizkie.
- Enpresa parte-hartzaile bakoitzarentzat amaierako txosten bat sortzea. Bertan, esleipendunak emaitzen analisia eta horien balorazioa egin beharko ditu. Txosten horiek enpresa parte-hartzaileei eta ZIUReko langileei helaraziko zaizkie, eta, gutxienez, honako atal hauek jaso beharko dituzte:
  - Lehen eta azken erasoen simulazioaren artean egon den eboluzioa, kontzientziazio maila hobetzeari dagokionez.
  - Zerbitzua gauzatzeari buruz izan den edozein gertakari garrantzitsuren xehetasuna.
  - Eskainitako prestakuntzan langileek izan duten parte-hartzeari buruzko datuak.
  - "Hobekuntza-proposamena", enpresako langileek lortutako emaitzak ikusita.

f) Zerbitzuaren azken emaitza: kanpaina guztiak garatu ostean azken txosten bat taxutuko da, testatutako enpresetan erabiltzaileek segurtasun arloan kontzientziazioari dagokionez hasierako eta amaierako egoera ebaluatu eta alderatzekoa. Txosten horretan ZIUR Fundazioak aztertzeko garrantzitsutzat jotzen dituen alderdiak jasoko dira, baina horietakoren bat izan daiteke.
- Erabiltzaileen zibersegurtasun arloko kontzientziazio-mailaren abiapuntua edo hasierako egoera.
- Hasierako egoera horren analisi alderatzaile eta anonimoa enpresa guztietan erabiltzekoak diren kasuen artean. Analisi horretan, gainera, negozio eta sektore motaren araberako alderaketa bat jaso daiteke, betiere, konfidentzialtasuna mantendu badaiteke edo negozioek beren baimena ematen badute.
- Erabiltzaileek zibersegurtasun arloan kanpainaren amaieran zuten eta azken kanpainaren ostean duten kontzientziazio-maila.
- Azken egoera horren analisi alderatzaile eta anonimoa.
- Enpresa bakoitzeko hobekuntzen bilakaerazko analisia.

## III. METODOLOGIA

Enpresa esleipendunak ZIUR Fundazioak garatzekoak diren lanen gaineko ikuskapen eta kontrolerako funtzioak gauzatzea ahalbidetu beharko du, jasotzen dituen ohar eta gomendioak zehatz-mehatz betez.

ZIUR Fundazioak lanen garapen eta jarraipena errazte aldera, zerbitzuko premien arabera, enpresa esleipenduna deitu dezake beharrezkotzat jotzen dituen dokumentu guztiak aurkeztu ditzan eta zerbitzua behar bezala garatzeko egokitzat jotzen dituen laneko edo informaziorako bilkura guztietara joan dadin, bileretara presentziazko moduan zein modu telematikoan bertaratzeko aukera izanik, esleipendunak nahieran.

Edozein kasutan, ZIUR Fundazioaren eskuetan geratuko da jarraipena egiteko modua (bilkurak, aktak, txostenak, etab.) aldatzeko aukera beharrezkotzat jotzen baldin badu.

Kontratista honen barnean garatutako dokumentu eta ekintzak ZIUR fundazioaren identitate korporatiboko eskuliburua betez egingo dira.

Kontratuaren egikaritze materiala hurrengo faseak betez egingo da:

1. fasea. Aurretiko lanak eta tresnaren hedapen eta konfigurazioa.

2. fasea. 1. kanpainaren garapen, egikaritze eta ebaluazioa.

3. fasea. 2. kanpainaren garapen, egikaritze eta ebaluazioa, eta azken ebaluazioa

Lehendabiziko fasea egikaritzeko ZIUR Fundazioko zuzendariak, zerbitzuaren lehendabiziko hilabetean, kanpaina bakoitzean bete asmo diren helburuetako Proiektuaren arduraduna ezagutaraziko du, parte hartzen duten enpresen zerrendarekin batera. Aldi berean, zerbitzua emateko garatzeko esku-hartzeen kronograma onartuko du enpresaren proposamena eta esleipendunak ZIUR Fundazioak tresna erabiltzeko izendatzen dituen pertsonekin partekatzeko prestakuntza-planaren plangintza eta edukia kontuan izanik.

Horien garapenean, eta kanpaina bakoitza hasi aurretik, aldeek garatzeko ekintzak zehaztuko dituzte xehetasunez.

Kanpaina bakoitzaren amaieran zerbitzuaren atzera begirako analisi bat, lau hilabetean behingoa, egingo da, ZIUR fundazioak aurrez zehaztutako helburuen betetze-maila eta lan-metodologiaren egokitasuna ebaluatuz, eta azken kanpaina amaitu ondotik, era berean, zerbitzuaren eta eskuratutako emaitzen balioespen orokor bat egingo da.

## IV. TRESNAREN BETEKIZUN TEKNIKOAK

### Kudeaketa-kontsola

Kontsolak lainoan txertatzeko modukoa izan beharko du, hura administratzeko web interfazea barneratu beharko duelarik.

Plataformatik *Spear Phising* kanpaina ezberdinen definizio, konfigurazio eta egikaritzea administratzeko aukera eman behar da. Hala erasoak simulatzeko nola erabiltzaileei zuzendutako prestakuntza eta sentsibilizazioko ekimenak kudeatzeko.

Proposatutako irtenbideak lainoan plataforma bat izateko aukera barneratu behar du, kudeaketako kontsola nagusiaren sostengu izango dena, hura administratzeko web interfazea izan beharko duena. Plataforma horrek administrariei ahalbidetu behar die:

- Erabiltzaile guztientzat, aldi berean, edo parte hartzen duen enpresatik edo ZIUR fundaziotik zehazten den lantaldeentzat, gaikuntza/sentsibilizazio esleipenak sortzea.
- Prestakuntzarekin lotutako gai eta eduki ezberdinak hautatzea, formatu ezberdinetan (ikastaro laburrak, infografiak, bideoak, etab.). Enpresa beraren barnean erabiltzaile talde ezberdinentzat gai edo formatu ezberdinak hautatzeko aukerarekin.
- Posta elektroniko bidez *phising* erasoen kanpaina abiatu eta kudeatzea.
- Langileen esleipenen amaiera monitorizatzea eta esleipenen oroitarri automatikoak helaraztea.
- Arriskuzko esparru kritikoen inguruko erabiltzaileen ezagutza sendo edo ahulenak identifikatzea.
- Denboran zeharreko ezagutzaren hobekuntza neurgarri bat agerian uzten duten txosten irakurterrazak eskuratzea.
- **Tresnan erabiltzaileek eskura duten prestakuntzaren eduki guztiak euskaraz eta gaztelaniaz egon behar du eskuragarri.**
- Segurtasun arloko haien gaikuntza eta kontzientziazioko programa guztiak lainoan oinarritutako sistema batetik administratzea, azken mehatxu zibernetikoen inguruko eduki berriekin etengabe eguneratzen dena.
- Erabiltzaileei inkestak egiteko aukera, kanpainari buruzko galderekin, prozesua berrelikatzea eta akatsak zuzentzea ahalbidetzeko informazioa eskuratzeko.

**Spear Phishing erasoen simulazioa**

Proposatutako irtenbideak posta elektronikotan oinarritutako *PHISING* eta *RANSOMWARE* erako erasoak simulatzeko aukera eman behar du, 24x7x365 oinarri batean. Behin aktibatu ostean, irtenbideak ez du segurtasun arloko operadoreen esku-hartzeren premiarik izan behar haren jarraikortasuna bermatzeko. Proposatutako irtenbideak modu automatikoan egin behar ditu gaineratutako eraso berriak.

Proposatutako irtenbideak *phising* motako erasoaren aurrean gaitasuna zehazteko modua eta segurtasuna nahiz langileek harekin betetzeko duten jarrera modu integralean ebaluatzeko modu bat barneratu behar du. Simulatutako erasoak errealistak izan behar dira eta etengabe eguneratutako mehatxuen inteligentzia sinesgarri batean oinarritu behar dira mehatxuen panorama aldakorraren aurrean egunean mantentzeko. Ebaluaziorako tresnak, esate baterako, galdetegi edo probak, liburutegi oparoa izan eta heina murrizteko funtzioekin hornituta egon behar dira, enplegatu guztiek galdera berdinak jaso eta erantzunen inguruan eztabaidatzeko aukera izango luketenean gertatuko zatekeen eran.

Ebaluaziorako tresnek, era berean, pertsonalizaziorako aukera osoak behar dituzte, parte hartzen duen enpresetako baten politika zehatzak frogatze aldera. Ebaluaziorako irtenbideek txosten sendoak gaineratu behar dituzte, kontzientziazio eta gaikuntza maila apalak agertzen dituzten arriskuzko erabiltzaileak erraz identifikatzekoak. Ebaluazioek ondorengo hezkuntzan erabiltzaileek zuzenean izena emateko aukera eman behar dute, simulazioetan eskuratutako emaitzen arabera.