ZIBERERASOEN SIMULAZIO ERAKO IRTENBIDE BATEKO ZERBITZU KUDEATURAKO BALDINTZA TEKNIKO PARTIKULARREN PLEGUA ZIUR FUNDAZIOARENTZAT (ESPEDIENTEA 2021009)

I.- ZERBITZUAREN HELBURUA ETA IRISMENA

Kontratuaren xedea Ziur fundazioari 3 kanpaina burutzeko beharrezkoa den laguntza teknikoa ematea da. Kanpaina horietan zibererasoen simulazio erako zerbitzu kudeatu bat gauzatuko da (Breach & Attack Simulations – BAS – ingelesez) Baldintza Teknikoen Plegu honetan zehaztutako baldintzetan. Horien bidez erasoen eszenario edo bektore multzo jakin baten aurrean egun dagoen arriskuzko egoera ebaluatu daiteke, eta hurrengo ekintzetarako beharrezkoak diren datuak eskuratu daitezke:

- Gipuzkoako enpresetan dauden babes-sistemen heldutasun-mailaren gaineko ikuspegi orokor bat eskuratzea,
- pertsona, prozesu eta teknologiek egiazko erasoetan agertzen diren portaeretan modu eraginkorrean zer-nola erantzungo luketen erakustea, horiek gertatu aurretik,
- eraso jakin bat hauteman, blokeatu edota ohartarazi ez zuen segurtasun-kontrol zehatz bat identifikatzea,
- industria-sistemetan txertatutako segurtasun-neurri ezberdinen inguruan ikertzea,

II.- ZERBITZUAREN DESKRIBAPENA

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

a) Kanpainak diseinatu, hedatu eta modu automatizatuan monitorizatzeko gaitasuna duen tresna bat (BAS – Breach & Attack Simulation) erabilgarri izatea, proiektuan parte hartzeko hautatutako industria enpresa ezberdinetan aurkeztu eta hedatu beharko duena.

   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) ZIUR Fundazioak hautatutako enpresetan hurrengo eraso bektoreekin lotutako simulazioak egitea.
   - Helbide elektronikoa
   - Sarea (albokako mugimenduak)
   - Endpoint segurtasuna

d) Zerbitzuan jasotako 3 kanpainak garatzea, bakoitza 4 hilabeteko iraupenarekin, ZIUR Fundazioak hautatutako enpresekin lotuta. Aipatu fundazioa izango da enpresak identifikatu eta hautatuko dituena, eta kanpaina bakoitzean gutxienez 5 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.

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.

e) Kanpaina bakoitzean eta enpresa bakoitzarekin jarduera hauek burutzea:
- Aztergai den enpresa bakoitzean teknologia hedatzea
- Erasoen eszenarioak modelatzea:
  - Orokorrak enpresa guztietara
  - Negozioaren premia, inguruabar edo arriskuen arabera pertsonalizatuak.
- Enpresetan testatzeko irtenbidea hedatzea (eragile kopurua eta mota eszenario ereduek baldintzatuta egongo da). Eragile hauek izango dira:
  - Enpresako sarearen zona espezifikoetan hedatutako Makina Birtualak. –
  - Testatzeko enpresako endpoint maketetan instalatutako eragileak, softwarean oinarrituak eta enpresako sarean kokatuak.
  - Aukeran halakoak izan daitezke:
  - Testatzeko enpresako endpoint maketetan instalatutako eragileak, softwarean oinarrituak eta hornitzailearen sarean kokatuak. -
- Erasoen eszenarioen lehen abiaraztea.
  - Emaitzen analisia.
  - Hobekuntzarako txosten eta planak, ekintza zehatzen proposamenekin
- Hobekuntzako planak aplikatzen diren bitartean kontsultak eta zalantzak artatzea
- Bigarren abiarazeta
  - Emaitzen analisia.
  - Hobekuntzarako txosten eta planak, ekintza zehatzen proposamenekin

f) Emaitzen analisia

- Eraso ezberdinak abiarazi ostean. Esleipendunak emaitzen analisi bat egin eta horiek balioetsi beharko ditu.
- Esleipendunak aztergai den enpresa bakoitzerako txosten indibidualizatu bat egin beharko du, abiatutako erasoen aurrerapena eta horiek ebazteko plan bat jasoz.
- Horiek ebazteko plana ez da soilik testatutako enpresan abiarazitako erasoak duen balizko inpaktu edo probabilitatearekin lotuta egongo, erasoaren konplexutasunarekin ere lotura izango du, eta esleipendunak balioetsi beharko du erabilera eta TTP kasu arrakastatsuak gauzatzen konplexuak edo errazak diren, eraso oso bat eraginkor egiteko horien arteko korrelazioa aztertzeaz batera.
- Azken kanpaina amaitzean egoeraren bilakaerari eta Eusteko gaitasunari buruzko balioespen bat barneratuko da.

g) Kanpainen azken emaitza:

Kanpaina guztiak garatu ostean azken txosten bat taxutuko da, testatutako enpresek egun segurtasunari dagokionez duten egoera ebaluatu eta alderatzekoa. Txosten horretan Ziur Fundazioak aztertzeko garrantzitsutzat jotzen dituen alderdiak jasoko dira, baina horietakoren bat izan daiteke.

- Enpresa bakoitzean gauzatutako erasoen eszenarioen aurrean segurtasun eta arrisku 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.
- Azken segurtasun eta arrisku maila, analisiaren edo plan zuzentzaileak aplikatu ostean.
- 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 hedapena.

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

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

4. fasea.- 3. kanpainaren garapen eta egikaritzea, 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

IV.1 Arkitektura

1.- **Kudeaketa-kontsola** – Kontsolak lainoan txertatzeko modukoa izan beharko du, web interfazea eta API bat barneratu beharko dituelarik.

2.- **Eragileak** – Horiek sareko puntu ezberdinetan (kanpoan edo barnean) edo endpoint mailan erasoak emulatu eta abiatzeaz arduratu beharko dira. Horiek barnean edo lainoan hedatzeko aukera izan beharko da AWS edo Azure motako cloud azpiegiturak baliozkotzeko (lainoan hedatuz gero, eragileak erasotzaile modura edo biktima modura jarduten duen aukeratu ahalko da).

3.- **Integrazioak** – Tresnak kudeaketa-kontsolaren integrazioak ahalbidetu beharko ditu, abiatutako erasoak nola eta non blokeatu edo hauteman diren ikusarazteko.

Tresnak ekoizpenaren ingurunean oso barnerakoia ez den hedapena egiteko aukera eman beharko du, beste alderdi batzuen artean, ezaugarri hauek izan beharko dituelarik:

- Sare-segmentuen artean eraso-eszenarioak ahalbidetzea makina birtualen bidez, ekoizpen-ingurunetan eragin gabe, baina simulazioaren xede den enpresako sarearen segmentazioaren eraginkortasuna testatzeko aukera izanik.
- Simulazioaren xede den enpresako maketa batean eragile bat txertatzea, hornitzaileen instalazioetan hedatzeko eta egiazko malwareak abiatzeko probak egiteko aukerarekin.
- Posta elektronikoko bektorearen analisirako, ez da eragilerik instalatu behar endpoint gunetan. Dena den, proba-kontuak sortu eta zerbitzariarekin konektatzeko metodoak baliatu beharko dira, igorpen eta harrerak egiaztatzeko.

IV.2 Betekizun teknikoak

Kudeaketa-kontsola

Proposatutako irtenbideak tokiko administrari baten nahiz lainoaren aukera ahalbidetu beharko du. Tokiko administrariak ere Interneterako konexiorik gabe eguneratzeko aukera aurreikusi beharko du, lineatik at eta operadore batek egindako eskuzko prozeduren bitartez.

Erasoaren simulazioa

Proposatutako simulazioak 24x7x365 oinarri batean erasoak simulatzeko aukera eman behar du. 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. Erasoak ez dira eten behar, plataformako administrariek hala eskatu ezean. Erasoen fluxua eguneratu egin beharko da plataformako hornitzaileak gaineratutako eraso berriekin, eskuzko interakziorik gabe.

Arintzea

Plataformak arintzeko arau espezifikoak, behin hornitzaile espezifikoak argitaratuta, zein arau orokorrak eman behar ditu. Checkpoint, F5, Forcepoint, Cisco, Fortinet, McAfee, Palo Aalto programen segurtasuna hornitzaileen zerrendan egon behar da. Horietarako, plataformak arau espezifikoak ematen ditu sare mailan (sinadurak). Balizko positibo faltsuak ekiditeko, arau horiek hornitzaileak baliozkotu behar ditu aldez aurretik eta sistemaren erabilgarri ipini behar dira modu zuzen eta automatikoan.

Erasoen datu-basea

Irtenbideak egiazko erasoen datu-base handi bat izan behar du. Hurrengo eraso-kategorietan erabilgarri izan beharko da: Kode maltzurra; Web aplikazioetara egindako erasoak; Zaurgarritasunen ustiapena; Erasoaren eszenarioa; Datuen kanpo iragaztea.

MITRE ATT & CK

Proposatutako irtenbideak, besteak beste, MITRE ATT & CK frameworkaren teknikak mapan kokatzeko aukera eman behar du eta hartako UIan egindako teknika bakoitzaren emaitza (porrota / arrakasta) aurkeztu beharko du.

SMTP proba

Proposatutako irtenbideak aukera eman behar du smtp erako ebaluazioak egiteko hala kanpotik (kanpoko posten domeinuak) nola erakunde bereko domeinuen artean.

Arriskurik gabe

Proposatutako irtenbideak ekoizpenean diren bezeroak, sareak eta lainoak babesteko segurtasun-pilaren segurtasun-maila egiaztatzeko aukera eman behar du, arriskurik eta positibo faltsurik gabeko ikuspegi bat erabiliz. Aukera eman behar du irtenbidearen sistemen arteko erasoak egiteko (hau da, makina birtual erasotzaile / biktimak soilik erabiltzea egiazko sistema eta gailuekin zuzeneko edozein kontaktu eta, horrenbestez, eragilerik gabeko moduan, zaintzeko), eragilerik instalatu beharrik gabe eta ekoizpenean

diren sistemekin (zerbitzaria / bezeroa) elkarrekintzan aritu gabe, mitre erasoaren teknikak probatzeko aztergai den enpresak erabilitako sistema estandarra (bezeroa edo zerbitzaria) ordezkatuko duen "eredu" erako makina batean instala daitekeen eragile bat baztertuz.

Albokako mugimenduak

Albokako mugimenduen tekniken gaineko probak bezeroaren "eredu" makina batean egin behar dira (Windowseko zerbitzaria edo bezeroa) "pibote" modura erabili behar dena teknika horiek administrarian zehaztutako beste sistema batzuekin egiaztatzeko eta sareko eskaneatzeak egin gabe. Albokako mugimenduaren "xede" diren sistemak bezeroak hautatutako sistemak zango dira, eragileak instalatzea eskatuko ez dutenak.

Enpresetako segurtasunaren jarrera egiaztatzeko gaitasuna egiazko erasoen azken bertsioak simulatuz

Zero egun erako mehatxuak edo eskala handiko eraso bat abiatzeko ustiatzen diren segurtasun-arrakala zaharrak eguneroko kezka-iturri dira CISO edota CIO zuzendarientzat, bere erakundeko segurtasuna babesteko eta zuzendaritza exekutiboari bere erakundeko segurtasunaren jarreraren berri emateko ardura dutenak.

Eraso berri horiek (besteak beste, Emotet eta Ryuk) modu ezberdinetan iristen dira, posta elektronikoko fitxategi atxiki modura edo webgune legitimo edo konprometitu batean agertzen den deskargarako esteka modura. Erakundearen perimetroa zeharkatu ostean, unean-unean kalte larriak eragin ditzakete erakunde batean.

Tresnak enpresetan eraso berri horiek simulatzeko aukera eman behar digu. Horri esker, azken zibererasoen aurka enpresetako segurtasunaren postura lehenbailehen ebaluatu ahalko dugu,

72724351F KOLDOBIKA PECIÑA (R: G75203067)

Digitalki sinatuta norengandik: 72724351F KOLDOBIKA PECIÑA (R: G75203067)
Data: 2021.06.16 09:50:56 +02'00'