

Espediente-zk.: 2022019

Kontratazioaren xedea: Basque CyberSecurity Centre-rako “*Pentesting*” zerbitzua

Dokumentua: Baldintza tekniko partikularren agiria

Edukia

1. TESTUINGURUA.....	3
2. KONTRATAZIOAREN XEDEA.....	3
3. ZERBITZUAREN DESKRIBAPENA	3
4. IRISMENA.....	4
5. ZERBITZUAREN EZAUGARRIAK	4
5.1. Metodologia	4
5.2. Plangintza	5
5.3. Entregagarriak	5
5.4. Lantaldea	6
6. ZERBITZUA EMATEKO BALDINTZAK	6

1. TESTUINGURUA

BASQUE CYBERSECURITY CENTRE (aurrerantzean, “**BCSC**”) Agencia Vasca De Desarrollo Empresarial - Enpresen Garapenerako Euskal Agentziaren (aurrerantzean, “**SPRI**”) barruan kokatzen den ekimena da. SPRI Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren mendeko zuzenbide pribatuko erakunde publikoa da.

BCSC, SPRIko unitate gisa, erreferentzia-erakundea da Euskadiko herritarren, enpresen eta erakunde publikoen zibersegurtasuna eta konfiantza digitala garatzeko, bereziki eskualdeko ekonomiaren sektore estrategikoentzat.

BCSC Eusko Jaurlaritzaren tresna bat da, euskal gizartean zibersegurtasunaren kultura goragoko maila batean jartzea helburu duena, eta zerbitzu espezializatuen eskaintzaileen eta eskatzaileen arteko topaleku bihurtu nahi du, horrela berrikuntzarako aukera bat sortuz, enpresen lehiakortasuna indartuz eta herritarrek jarduera digital seguruago baterako ohiturak garatzea erraztuz.

Bere helburuak lortzeko, BCSCk zeharkako ekimen gisa definitzen du bere burua, eta hasieratik Eusko Jaurlaritzako lau sail inplikatzeko ditu: lehen aipatutako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Saila; Segurtasun Saila; Gobernantza Publiko eta Autogobernu Saila; eta Hezkuntza Saila. Jarduerak biltzen ditu ikerketa-proiektuak, ekintzailetzako ekimenak eta estatu- eta nazioarte-mailan eragile eskudun batzuekin koordinatutako lankidetzak. Izan ere, lankidetzak estuan lan egiten da Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko eragileekin, BCSCko Batzorde Iraunkorreko kide baitira.

BCSCren egitekoa da, beraz, euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa-jarduera dinamizatzea eta erreferentzia izango den sektore profesional bat sortzea ahalbidetzea. Testuinguru horretan, eragile osagarrien arteko lankidetzak-proiektuak exekutatzea bultzatzen da, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren eremuetan.

BCSCk zenbait zerbitzu eskaintzen ditu Gorabeheren Erantzuteko Lantalde gisa (aurrerantzean, CSIRT: “Computer Security Incident Response Team” ingelesezko siglak), eta Euskal Autonomia Erkidegoaren esparruan lan egiten du mehatxu berriak detektatzeko eta garaiz ohartarazteko gaitasuna handitzen, informazioaren segurtasun-gorabeheren erantzuna eta analisia egiten, eta euskal gizartearen beharrei erantzuteko prebentzio-neurriak diseinatzeko.

2. KONTRATAZIOAREN XEDEA

Espedientearen xedea da Pentesting zerbitzu bat kontratatzea BCSCren IKT azpiegiturako ahultasunak eta akatsak identifikatzeko. Era berean, arrisku horiek ezabatzeko edo arintzeko neurri egokiak proposatu beharko dira.

3. ZERBITZUAREN DESKRIBAPENA

Atal honetan, kontratuaren xedea osatzen duten eta esleipendunak eskaini beharko dituen ezaugarri teknikoak deskribatzen dira, eta behean azaltzen den zerrenda ez da kontratatutako zerbitzuaren ezaugarrien zerrenda zehatz bat, baizik eta BCSCk eskatutako jarduera orokorrak (egin beharreko gutxienezko zereginen alderdiak eta espero diren emaitzak estaliz).

Eskakizun horiek gutxienez hartu behar dira (kontraktorik adierazi ezean), eta lizitatzailerak eskakizunak handitu ahal izango dituzte beren eskaintzetan.

Lizitatzailerak proiektuaren emaitzarik onena ziurtatzeko lagunduko duten ezagutzak, metodologiak, tresnak eta giza lantaldea aurkeztu eta deskribatu beharko ditu.

Esleipenduna behartuta egongo da sekretua gordetzera eta zerbitzua emateko erabiltzen dituen langileei gordetzeraz lanak garatzeagatik ezagutzen duten informazio osoari dagokionez, eta

ezin izango dute beren buruentzat edo beste pertsona edo erakunde batentzat erabili.

4. IRISMENA

Enpresa lizitatzailerak zehaztu beharko du intrusio-proben xede izan daitezkeen aktiboen gehieneko kopurua; **irismen** hori ezingo da izan honako hau baino txikiagoa:

- 60 zerbitzari
- 15 kanpoko IP
- 2 SSID

5. ZERBITZUAREN EZAUGARRIAK

5.1. Metodologia

Enpresa lizitatzailerak sartzeko **metodologia** egokienak planteatu beharko ditu, industriaren zein jardunbide egokietan oinarritzen den adierazi beharko du, eta honako alderdi hauek jasoko ditu: auditoretza-arlo bakoitzaren irismena, auditatu beharreko alderdiak, nola egin behar den, zer emaitza sortzea espero den eta egileek esparru bakoitzerako zer gaitasun profesional dituzten.

Proposamenen, gutxienez, honako ebaluazio-mota hauek egin beharko dira:

- Eraso-azaleraren analisi osoa adierazitako kanpoko IPetatik abiatuta.
- Sarean Internetetik sartzeari buruzko intrusio-testa.
- Barne-sareko kutxa gris motako segurtasun-auditoretza teknika, gutxienez maila hauek aurreikusten dituenak:
 - Sarea:
 - Sistemei buruzko informazioa lortzea sareak eskaneatuz. Zerbitzuak identifikatzea (TCP edo UDP portu irekietatik), baita sistemak ere (paketeen edukiagatik).
 - Babes perimetraleko gailuak (routerrak, suebakiak, etab.) sakontasunez aztertzea.
 - Sistema eragilea (SO) eta plataforma:
 - Intrusio-saiakeren, kalteberatasunen ustiapenaren edo makinaren arteko alboko mugimenduak egitearen aurrean identifikatutako sistemen erresistentzia-gaitasuna aztertzea.
 - Taldeak, rolak eta politikak:
 - Erabiltzaile-profil desberdinetarako taldeen, rolen eta politiken konfigurazioa egiaztatzea.
- WiFi sareen segurtasun-auditorea, gutxienez alderdi hauek kontuan hartuta:
 - Sarearen barruan erabiltzen diren SSIDak aurkitzea.
 - Hari gabeko sarera sartzeko erabilitako sarbide-puntuak identifikatzea.
 - WLAN analisi bat egitea baimendu gabeko hari gabeko sareen bila.
 - Gonbidatuen haririk gabeko saretik haririk gabeko sare korporatiboa hausteko gaitasuna aztertzea.

- Erabiltzaile gisa eskuragarri dagoen wifi azpiegituraren konfigurazioa aztertzea.
- Onboarding web ataria aztertzea.
- Seinalearen bulegotik haragoko sakabanatze-mailaren ebaluazioa.

Ez dira onartuko soilik tresna automatikoekin egindako erasoak; nolanahi ere, laguntza-tresna gisa erabili ahal izango dira, baldin eta hurrengo 5.3 atalean adierazitako txosten teknikoan jasota badago eta emaitzak aipatutako txosten teknikoaren eranskin gisa ematen badira.

5.2. Plangintza

Enpresa lizitatzailerak **lan-plan** baten proposamena egin beharko du, zerbitzuaren mugari garrantzitsuenak eta bakoitzaren datak adierazita, baita jarduerak gauzatzean aplikatuko litzatekeen exekuzio/eragiketen fluxua ere.

5.3. Entregagarriak

Enpresa lizitatzailerak **entregagarriak** zehaztu beharko ditu, haietako bakoitzak jasoko duenaren gutxi gorabeherako azalpena eta egitura adierazita.

Gutxienez entregagarri hauek eskatzen dira:

- Auditoretza-plana; bertan, gutxienez, egin beharreko probak, denbora-antolaketa eta balizko inpaktuak zehaztuko dira.
- Txosten exekutiboa, txosten teknikoaren informazio garrantzitsuena biltzen duena, goi-aginteei eskalatzeko.
- Txosten teknikoa, arlo, sistema edo sistema-talde analogo bakoitzerako zehaztuta:
 - Auditoriaren helburua, ikuskatutakoa identifikatuz.
 - Prozesu metodologikoa eta aplikatutako tresnak.
 - Egindako proben tipologia eta egitura.
 - Erabilitako proben historikoa, erabilitako TTPei erreferentzia eginez.
 - Identifikatutako urritasunen / kalteberatasunen identifikazio unibokoa
 - Aurkikuntzen arrisku-sailkapena erreferentzia-markoaren arabera, eta lehentasunak proposatzea, jarduerak konpondu bitartean lortutako testuinguruan oinarrituta.
 - Lortutako irizpenen oinarri diren datuak, egitateak eta oharrak.
 - Identifikatutako arriskuak ezabatzeko edo arintzeko beharrezkoak diren neurri zuzentzaile edo osagarriak xehatzen dituen ekintza-plana.
 - Ebidentziak eta adibideak, segurtasun-arrisku handia edo kritikoa dakarten probetarako, BCSCko langileek modu autonomoan erreproduzitu ahal izan ditzaten.

Txostenaren formatua BCSCren ingurunerako partikularizatu eta testuinguruan kokatu behar da, baita lortutako aurkikuntza, erabilitako metodologia eta egindako jardueretarako ere, eta ez da onartuko tresnek sortutako txosten automatikorik erabiltzea. Laguntza gisa tresna automatikoak erabili badira, txosten teknikoaren eranskin gisa entregatu behar dira txosten "gordinak".

Erakusgarri gisa, **lizitatzailleak eskatutako hiru entregagarrien adibide bat aurkeztu beharko du**, bai eta gehitu nahi den beste edozein agirirena ere, **eskaintza teknikoaren 2._eranskina gisa**.

Aurreko atalean aipatutako adibideak izan daitezke lizitatzailleek bai aurreko jardueretarako bai BCSCz bestelako bezero/erabiltzaileentzat garatu dituzten ezaugarri berdinak edo antzekoak dituzten entregagarriak, edo bestela atal honetan adierazitako entregagarrien zirriborro gisa jardungo duten txosten sistemikoak.

5.4. Lantaldea

Enpresa lizitatzailleak kontratua gauzatzeko eskuragarri dagoen **lantaldea** zehaztu beharko du, baliabide bakoitzarentzat zein profil eta rolekin lotzen den adierazita, eta baita antzeko jardueretan duen esperientzia ere, zerbitzua behar bezala ematen dela bermatzeko.

Lantaldeko kideek **gutxienez 5 urteko esperientzia** egiaztatu beharko dute, eta lanak egiteko beharrezkoak diren ezagutzak egiaztatzen dituzten ziurtagiriak izatea baloratuko da (GXPN, GWAPT, GPEN, GAWN, LPT, OSCP, OSWE, PenTest + edo antzekoak).

Lanak egiteko kontratua formalizatu ondoren sartuko den lantaldea esleipendunaren eskaintzan zehaztutakoa izango da eta, ondorioz, baloratu egin behar izango da, eta, esleipena eginez gero, adierazitako ziurtagiriak egiaztatu beharko dira balorazioa egiteko argudio gisa.

Lantaldearen ezaugarriak 1. eranskina_Lantaldea taula erabiliz justifikatuko dira, administrazio-klausulen agirian adierazitakoaren arabera.

6. ZERBITZUA EMATEKO BALDINTZAK

Jarraian, lizitatzailleak eskatu diren zerbitzuak emateko baldintzak aipatuko dira:

- Intrusio-probak egiteko ordutegia BCSCrekin adostuko da, 8:30etik 17:30era bitartean erreferentzia gisa; nolanahi ere, sistema kritikoetan inpaktua izan dezaketen proben kasuan, BCSCk, bere irizpide eskusiboan, probak lan-ordutegitik kanpo egitea eskatu ahal izango du.
- BCSCren kokalekuetako sistemetan sartzeko, BCSCtik haren azpiegituraren eta sistemen eta esleipendunaren arteko sarbidea eta komunikazioak ahalbidetzeko baliabideak emango dira, VPNa erabiliz.
- Barne-sareko kutxa grisaren probak enpresa lizitatzaillearen instalazioetatik nahiz BCSCren instalazioetatik egin ahal izango dira; bigarren aukera hautatuz gero, BCSCtik instalazioetarako sarbidea eta ingurune egokia eskainiko dira beharrezkoak diren ekipamenduak hedatzeko.
- Erabiltzaile-profil desberdinetarako taldeen, rolen eta politiken konfigurazioa egiaztatzeko, BCSCtik dagozkion kredentzialak emango dira.
- Wifi ingurune probetarako beharrezkoa izango da BCSCren instalazioetan *In-situ* egotea. Horretarako, BCSCtik instalazioetarako sarbidea eta ingurune egokia emango dira beharrezkoak diren ekipamenduak hedatzeko.
- Lizitatzailleak bere gain hartuko du proiektuaren kostuen barruan lantaldea BCSCren instalazioetara lekualdatzearen ondoriozko edozein gastu, eta ezingo du konpentsaziorik eskatu horregatik.
- Lizitatzailleak aurkeztu beharko ditu eskatu diren zerbitzuak emateko indarrean dagoen legeriak galda ditzakeen ziurtagiriak eta baimenak.