PRESKRIPZIO TEKNIKO PARTIKULARREN AGIRIA, ZIUR FUNDAZIORAKO GIPUZKOAKO IoT SEKTOREKO PRODUKTU INDUSTRIALEN DISEINUAREN ZIBERSEGURTASUNAREN EREMUKO EBALUAZIO ZERBITZUARENA (Esp.: ZIUR2024-015)

I. ZERBITZUAREN XEDEA ETA IRISMENA

ZIUR Fundazioak proiektu honekin ekimen bat garatu nahi du etorkizunean produktu industrial ziberseguruak egiaztatzeko. Horretarako, ZIUR Fundazioak *metodologia* bat definitu du, aukera ematen duena *produktu industrialak ebaluatzeko eta egiaztatzeko* IEC 62443 arauaren arabera, haren segurtasun betekizunei eta segurtasun mailei jarraituz.

Metodologia diseinatzeko, honako alderdi gako hauek hartu dira kontuan:

- *Eskariari balioa ematea*, eskaintzak produktuak egiaztatzea sustatzeko.
- *Metodologia fidagarri* bat izatea, lurraldeko ekosistema barnean hartzen duen *ebaluazio kolaboratibo*ko sistema bat sustatuko duena.
- *Ziur Fundazioa* txertatze horren *pieza gako gisa kokatzea*.

Lizitazio honen **xedea** da produktu industrialen zibersegurtasunaren alorreko ebaluazio zerbitzu bat lortzea, zehazki, IoT sektorean. Ebaluazio hori preskripzio teknikoen agiri honetan definituko diren gaitasun teknikoak eta giza gaitasunak dituen laborategi ebaluatzaile batek egin behar du, ZIUR Fundazioak definitutako metodologiari jarraituz, zeina enpresa lizitatzaileen esku jarriko baitu, lizitaziorako proposamena aurkezteko epearen lehen hamar egunetan berariaz eskatuz gero.

ZIUR beste proiektu bat egiten ari da, ZIUR2024-018 lizitazioari lotua, ZIUR Fundazioak definitutako metodologia, IEC 62443 arauan oinarritutakoa, IoT sektorearen beharretara egokitzeko , CRA Legea oinarritzat harturik. Metodologia hori ezarritakoan, enpresa adjudikaziodunari eskuragarri utziko zaio.

Honako hauek dira proiektuaren **helburuak:**

- IoT sektoreko produktu industrial aztertuen zibersegurtasunaren betetze maila eta heldutasuna identifikatzea.
- Lurraldeko enpresa sareko produktu industrialak ebaluatzeko gaitasunak identifikatzea.
- IoT sektoreari laguntzea merkatuak eskatuko dizkion zibersegurtasunaren arloko beharrak eta sor daitezkeen arauzko betekizunak ezagutzen.

Proiektuaren emaitza moduan, Gipuzkoako enpresa industrialek honako **onura** hauek izango dituzte:

- Gaitasun zientifiko eta teknologikoak eta industriakoak lerrokatzea
- Gure enpresa sarearen lehiakortasuna indartzea
- Urratsak egitea Gipuzkoa zibersegurtasun industrialaren eta produktu industrialaren ebaluazioaren erreferentzia bihur dadin

Irismena

Zerbitzuaren barruan sartzen da **IoT sektoreko bi enpresatako bi produktu industrialen segurtasuna ebaluatzea**, eta honako fase hauek aurreikusi dira:

1. ZIUR2024-018 lizitazioko enpresa adjudikaziodunarekin biltzea eta ebaluazioaren metodologiaren egokitzapena, IoT sektorera doitzekoa.
2. Enpresa ebaluatuentzako ebaluaziorako eta bidelaguntzarako prestatzeko aurreko zerbitzua
3. Ebaluazio egoeraren dokumentazioa
4. Produktuaren eragiketa parametroak adostea
5. Egin beharreko probak hautatzea eta ebaluazioen diseinua
6. Aurreko puntuetan egindako probetan lortutako emaitzen analisia eta diseinua hobetzeko proposamena
7. Enpresa bakoitzarentzako laguntzarako zerbitzu teknikoa, konpontze planean proposatutako hobekuntzak egiten laguntzeko

Zerbitzuari lotutako kostu guztiak adjudikaziodunaren kontura izango dira, zerbitzutik eratorritako garraioari eta joan-etorriei lotutakoak barne, esaterako:

- Bi enpresa parte-hartzaileetako langileen laborategi ebaluatzailerako joan-etorriak. Bi enpresa parte-hartzaileak Gipuzkoan egongo dira kokatuta.
- Aztertu beharreko makinak bi enpresa parte-hartzaileetatik laborategi ebaluatzailera garraiatzea.

II. ZERBITZUAREN DESKRIBAPENA

Apartatu honetan deskribatzen dira kontratuaren xedea osatzen duten ezaugarri teknikoak, adjudikaziodunak eman beharrekoak. Dena den, jarraian datorren zerrendak ez ditu jasotzen kontratatutako zerbitzuaren ezaugarri guzti-guztiak, baizik eta ZIUR Fundazioak eskatutako jarduera orokorrak, egin beharreko zereginak eta espero diren emaitzak.

Adjudikaziodunak bere eskaintzan proiektuan emaitzarik onena lortzen duela bermatzeko erabiliko dituen ezagutza, metodologiak, tresnak eta giza taldea aurkeztu eta deskribatu beharko du, ezaugarrien taulan eta klausula administratibo partikularren agiriko klausuletan jasotako moduan.

Zerbitzuan hainbat eragilek parte hartzea aurreikusi da:

- **Fabrikatzailea – enpresa parte-hartzailea (adjudikaziodunaz besteko eragilea) -** Ebaluazio prozesua hasteko, fabrikatzaileak produktuaren ziurtagiria eskatzen du, eta horretarako behar den dokumentazioa ematen. ZIUR Fundazioko langileek hautatuko dituzte prozesuan parte hartuko duten bi fabrikatzaileak. IEC 62443 arauari jarraituz, sakon aztertuko dira produktuaren ezaugarriak eta haren berezitasunak.
- **Laborategi ebaluatzailea (adjudikazioduna) -** Zehaztutako entseguak egiten dira, dagozkion kontrolak betetzen direla egiaztatzeko, laborategi independente batean.

Erreferentzia esparruari eta ebaluazio metodologiari dagokienez, ZIUR Fundazioak aurretik beste proiektu bat egina du, zeinean, ZIUR Fundazioak garatutako eta IEC 63443 4-1 eta 62443 4-2 arauetan oinarritutako erreferentzia-, ebaluazio- eta testatze-framework batetik abiatuta, framework hori egokitzen ari den proiektu honetarako araudi aplikagarrira, hau da, EU-MDR eta 2017/745 arauetara. Framework hori lizitatzaileen esku jarriko da, aurretik ziur@ziur.es helbide elektronikoan eskatuta, proposamena egiteko erreferentzia gisa erabiltzeko. Lehen aipatutako egokitzapenaren emaitza eskura edukitakoan, proiektu honen enpresa adjudikaziodunarekin partekatuko da.

Ebaluazio hori hainbat eremutan egiten da: orokorretatik hasi, non erabilera industrialeko protokoloak ebaluatzen diren (OPC-UA, Profinet, Modbus eta abar), eta produktu industrial baten eremu zehatzagoetara arte, besteak beste, fabrikatzaileak berak garatutako aplikazioetara. Bereizketa hori egiteak aukera ematen du proba orokorretarako dagoeneko badauden test tresnak erabiltzeko, eta fabrikatzailearen aplikazioaren ebaluazioaren emaitza, aldiz, probetako teknikarien ezagutzaren eta esperientziaren araberakoa izango da.

Ebaluazioa egiteko behar diren hardware eta software lizentzia guztiak adjudikaziodunaren kargura izango dira.

III. BETEKIZUN TEKNIKOAK

Jarraian jasotakoak dira proba laborategiaren betekizun teknikoak.

Probak behar bezala egiteko, ZIUR Fundazioak espero duen kalitatearekin, eta prozedura baten araberako ebaluazio errepikagarria, kanpoko eragile batek egiazta dezakeena eta kostu mugatuak dituena egiteko gai izateko, beharrezkoa da ebaluazio erreminta komertzialak erabiltzea.

Kontuan hartuta zibersegurtasun industrialeko ebaluazio tresnak punta-puntakoak direla, adjudikaziodunak proposatutako laborategiak honako funtzio hauetarako nahikoa tresna beharko ditu izan. Enpresa lizitatzaileak proiekturako proposatutako tresnen ezaugarriak zehaztu beharko ditu, eta, gutxienez, honako ekipamendu hau izan beharko du:

- Web penetrazioko testatze erreminta
    - Erreminta horrek erreferentziazko esparru estandarizatu bat edo de facto esparru bat erabili beharko du testatzea egiteko, adibidez, Open Web Application Security Project (OWASP) edo antzeko bat.
- Komunikazio protokoloak testatzeko erreminta
    - Tresna horrek komunikazio protokolo orokorrak aztertu behar ditu. Analisi horren emaitzak lotuta egon beharko du zaurgarritasunen CVE (Common Vulnerabilities and Exposures) berri emateari lotuta egon beharko du.

- Komunikazio industrialeko protokoloak testatzeko erreminta
    - Erreminta horrek komunikazio baliogabeak edo komunikazio gaizki sortuak (fuzzing deritzona) testatzea estali behar du, baita trafiko handiko testatzea (zerbitzua ukatzearen probak deritzenak) eta OT protokoloetan zaurgarritasun ezagunak egiaztatzea ere.
    - Honako komunikazio protokolo hauek, gutxienez, onartu behar ditu:
        - EtherNet/IP (CIP)
        - Foundation Fieldbus (FF-HSE)
        - MMS
        - Modbus TCP/IP
        - OPC UA
        - PROFINET IO
        - DNP3
        - MMS (IEC 61850/ICCP)
        - Modbus TCP/IP
        - SES-92
        - ZigBee SE (802.15.4)

Nolanahi ere, lizitatzaileek probak egiteko proposatutako laborategiak proiektuaren helbururako gutxieneko betekizunak betetzen dituela egiaztatzeko, proposamenean jaso egin beharko da ebaluazioa egingo duen laborategia osatzen duten HW eta SW tresnen zerrenda zehatza, baita haien kokapen fisikoa ere.

Enpresa lizitatzaileak proba plan zehaztua proposatu behar du, arauaren betekizun guztiak betetzeko egingo diren proba guztiak eta proba bakoitzerako erabiliko diren tresnak zehazten dituena.

Proposamenetan, zehatz-mehatz adierazi beharko dira fase eta ataza bakoitzean egingo diren probak eta testak.

Halaber, proposamenean argi eta garbi zehaztu beharko da (adibidez, taula modura) ZIUR Fundazioak egindako ebaluazioaren frameworkaren kontrol bakoitza egiaztatzeko.

IV. METODOLOGIA ETA LANEKO PLANA

Enpresa lizitatzaileak proposamen bat egin beharko du, metodologia eta laneko plana jasotzen dituena, eta zerbitzuaren mugarriak jasotzen dituena, dagozkion data eta guzti. Halaber, entregatzekoen zerrenda zehaztu beharko da, bakoitzaren deskribapena eta gutxi gorabeherako egitura barne. Gutxieneko baldintza izango da honako aurkezteko hauek egitea:

E.1- Ebaluazio egoeraren dokumentazioa

Hasieran, produktuaren fabrikatzaileak enpresa adjudikaziodunari testatu beharreko aktiboei/gailuei buruzko informazioa bidaliko die (Device Under Test ere deituak, DUT), adibidez: kontrol normalaren funtzionamendua, salbuespeneko kontrolaren funtzionamendua eta gailuarekin jarduteko mekanismoen zerrenda. DUTak onartzen duen funtzionalitate posible ororekin konfiguratuta egon beharko du, ebaluazioak ahal beste estal dezan, eta, beraz, ahalik eta etekin handiena ateratzeko.

E.2- Produktuaren eragiketa parametroak adostea

Probetako teknikariek dokumentazio hori eskura dutenean, aztertu egingo dute, eta testatze metodoen eta kontrol funtzioak monitorizatzeko irizpideen dokumentu bat proposatuko dute. Dokumentu honen parametroak probetako teknikariekin eta produktuaren fabrikatzailearekin adostuko dira.

E.3- Egin beharreko probak hautatzea eta ebaluazioen diseinua

Ebaluatu beharreko produktuaren zehaztasunak aintzat hartuta, kasu bakoitzean egin beharreko testak hautatuko dira, eta deskribatu egingo da test hori egingo den modua (eragiketa ingurua, neurketa tresnak, neurketa metodoak, emaitzen balioak eta abar).

Test horiek preskripzio teknikoen agiri honetako III. apartatuak ezarritako betekizunak bete beharko dituzte, IEC 62443 arauaren 4-1 zatiko 5. praktikari jarraituz. Test guztietan proba bat egin beharko da, gutxienez, eta gomendagarria da ahalik eta proba gehien egitea.

E.4 - Egin beharreko proben exekuzioa

Diseinua egindakoan, aipatutako ebaluazioa egingo dute proba teknikariek, laborategian.

E.5- Aurreko puntuetan egindako probetan lortutako emaitzen analisia eta diseinua hobetzeko proposamena

Behin probak egindakoan, testetan jasotako informazio guztia aztertuko da, emaitzen txostenak egiteko, eta ebaluatu beharreko enpresari eta ZIUR Fundazioari aurkeztuko zaizkie. Txosten guztiak euskaraz eta gaztelaniaz aurkeztu beharko dira.

Txosten horietan, lortutako emaitzak ikusita, produktuaren diseinuko hobekuntza proposamena jaso beharko da, zibersegurtasunaren heldutasuna hobetzekoa.

E.6- Enpresa bakoitzarentzako laguntzarako zerbitzu teknikoa, konpontze planean proposatutako hobekuntzak egiten laguntzeko.

Ebaluazioaz arduratuko den enpresa adjudikaziodunak proiektuan laguntzarako zerbitzu tekniko bat jaso beharko du, aurreko apartatuan proposatutako hobekuntzak produktuan txertatzen laguntzeko ebaluatu beharreko bi enpresetako bakoitzari.

Fase horiek izan behar ditu, gutxienez, proiektuan jasotako bi ebaluazioetako bakoitzak.

V. LANEN IKUSKAPENA ETA KONTROLA

Enpresa adjudikaziodunak erraztu egin beharko ditu ZIUR Fundazioak lanen garapenaren inguruan egin beharreko ikuskapen eta kontrol lanak, eta zorrotz-zorrotz bete beharko ditu jasotako oharrak eta gomendioak.

Nolanahi ere, ZIUR Fundazioaren iritziaren mende egongo da jarraipena egiteko modua aldatzea (bilerak, aktak, txostenak eta abar), beharrezkoa irizten badio.

Halaber, kontratua ondo garatzeko eta betetzeko beharrezkotzat jotzen diren zerbitzuak eman beharko ditu, ordain gehigarririk jasotzeko eskubiderik gabe, laneko bileretara eta informazio bileretara agertzeari dagokionez. Betebehar hori bermealdia bukatu arte mantenduko da.

María Penilla Azcuenaga
ZIUR FUNDAZIOAREN ZUZENDARI NAGUSIA

Firmado digitalmente por MARIA PENILLA AZCUENAGA
el día 05/11/2024 con certificado emitido por AC
DNIE 004