GIPUZKOAKO INDUSTRIAK ICS INGURUNEAN DUEN ZIBERSEGURTASUN ARLOKO HELDUTASUNAREN DIAGNOSTIKOA EGITEKO ZERBITZUA ARAUTZEN DUTEN BALDINTZA TEKNIKO PARTIKULARREN AGIRIA (ZIUR2022027 ESP)

I.- ZERBITZUAREN XEDEA ETA IRISMENA

ZIUR Fundazioari 3 kanpaina aurrera eramateko behar duen laguntza teknikoa ematea du xede kontratuak. Kanpaina horietan, ICS (Industrial Control Systems) inguruneen segurtasuna ebaluatuko da hainbat sektore industrialetako enpresetan, lizitazioko Baldintza Tekniko Partikularren Agiriko baldintzak kontuan hartuta. Modu horretan, sektore industrial desberdinetako enpresek zibersegurtasunaren arloan duten egungo heldutasun maila ebaluatu nahi da, eta datuak lortu nahi dira, helburu hauek lortzeko:

- Egungo babes-sistemen heldutasun mailari buruzko ikuspegi orokorra izateko, zehazki, Gipuzkoako enpresen ingurune produktibo eta industrialetan.
- Sistema industrialetan aplikatutako segurtasun-sistemei buruz ikertzeko.
- Gipuzkoako industrian −instalazio industrialen OT nahiaz IT arloan− zabaldutako gailuen zaurgarritasun nagusiak identifikatzeko.
- Eraso errealen aurrean erantzuteko prozesuak eta teknologiak nola zabalduta eta konfiguratuta dauden egiaztatzeko, eraso horiek gertatu aurretik.
- Gipuzkoako enpresa industrialetan gehien erabiltzen diren gailuen zerrenda bat egiteko, eta, hala, ZIURen etorkizuneko ekintzak bideratzeko.

II.- ZERBITZUAREN DESKRIBAPENA

Kontratuak xede duen jarduera aurrera emateko, honako baldintza hauek bete beharko ditu esleipendunak:

a) ZIUR Fundazioak autodiagnostikorako tresna bat du. Web atari honen bitartez eskura daiteke: https://diagnostikoa.ziur.eus. Esleipendunak garatu egin behar du egungo tresna, irismen orokorrekoa baita, eta Gipuzkoako ETE industrialetara bideratutako zibersegurtasun arloko autodiagnostirako ICS tresna aurreratu bat sortu behar du.

b) Ingurune industrial baten zaurgarritasunak aztertzeko gaitasuna duen eta baldintza teknikoen agiri honetako IV. atalean adierazitako baldintza teknikoak betetzen dituen tresna izan behar du, gutxienez, esleipendunak, eta proiektuak helburu dituen kanpainetan parte hartzen duten enpresa guztietan erabiltzeko aukera izan behar du.
   Aztertutako enpresetan fabrikatzaile baten edo batzuen zunda/k zabaltzeko, *black box* modalitatea erabili beharko du esleipendunak, eta, haren bidez, datuak bildu beharko dira honako helburu hauetarako:
   - Inbentario pasiboa aurkitzeko
   - Zaurgarritasunaren azterketa pasiboa egiteko
   - Trafiko zirkulatzailearen azterketa egiteko
   - Kanpo-esposizioaren azterketa egiteko
   - Arkitekturaren azterketa egiteko

- GAP azterketa egiteko IEC 62443-3-3 arauaren arabera
- Hobetzeko gomendioak proposatzeko, aurreko puntuetan egindako aurkikuntzetan oinarrituz

Lizitatzaileak jarri beharko ditu aplikatiboa eta haren osagai guztiak amaierako enpresan zabaltzeko behar diren hardware eta software lizentzia guztiak.

c) Tresnaren/tresnen erabilerari buruzko prestakuntza eman behar dio Ziur Fundazioko teknikarien taldeari.

d) Zerbitzuan jasotzen diren 3 kanpainak eraman behar dira aurrera −4 hilabeteko iraupenekoa bakoitza− ZIUR Fundazioak aukeratutako enpresetan. ZIUR Fundazioak identifikatu eta aukeratuko ditu enpresak, eta kanpaina bakoitzeko 6 enpresek hartu beharko dute parte gutxienez, hargatik eragotzi gabe esleipendunak partaide kopuru handiagoa proposatzeko duen aukera.

   Horretarako, martxan jartzeko lanak zehaztean, kanpaina bakoitzean zerbitzua abian jartzeko eta kanpaina bakoitzean jasotako enpresa bakoitzerako behar den guztia jaso beharko da.

   ZIUR Fundazioa harremanetan jarriko da zerbitzuaren prestazioa egingo den enpresekin. Ziur Fundazioaren eta enpresa partaide bakoitzaren arteko harreman hori juridikoa izango da kasu guztietan. Horretarako, dagozkion lankidetza-hitzarmenak formalizatuko dira Fundazioaren eta enpresa partaideen artean. Hitzarmen horien bidez, enpresako baliabideetarako sarbidea ahalbidetuko da, kontratuaren xedea bete ahal izateko.

e) Kanpaina bakoitzean eta enpresa bakoitzarekin honako jarduera hauek egin beharko ditu esleipendunak:
   - Aztertutako enpresa bakoitzean ICS autodiagnostikoa egiten lagundu.
   - Aztertutako enpresa bakoitzean teknologia/k zabaldu, eskura izanez konektatutako sare industrialak nahiz sarera konektatuta gabeko OT zelulekin konektatuta ez dauden sare industrialak. Ereduzko agertokien arabera zehaztuko da zunda kopurua eta mota. Honelakoak izango dira zundak:
     - Enpresako sare industrialaren eremu zehatzetan −enpresa industrial bakoitzak aukeratuko du− zabaldutako makina birtualak edo zunda fisikoak.
     - Beharrezkoa izanez gero, enpresari laguntza eman beharko zaio bere sarea presta dezan (konfigurazio mailan), eta, hala, zundek ondo funtziona dezaten.

f) Emaitzen azterketa

   - Kanpainaren erdian (tresna/k zabaldu eta handik 2 hilabetera) eta enpresa bakoitzeko, emaitzen hasierako analisia eta balorazioa egin beharko du esleipendunak.
   - Kanpaina bakoitzaren amaieran, esleipendunak txosten indibidualizatu bat egin beharko du parte hartzen duen enpresa bakoitzeko. Txosten horretan jaso beharko dira enpresari buruzko informazio garrantzitsuena, OT segurtasun arloko heldutasun maila (IEC 62443), zaurgarritasunen zerrenda, aktiboen inbentarioa, arkitekturaren analisia, hobetzeko gomendioak, egindako aurkikuntza nagusiak…

g) Entregagaiak:

Entregagaien zerrendaren barruan, kanpaina bakoitzean parte hartzen duen enpresa bakoitzari buruzko txosten hauek aurkeztu beharko dira, gutxienez:

1. Irtenbidearen/irtenbideen zabalkuntzari buruzko txostena: tresna/k zabaltzeko arkitekturaren deskribapena, sare monitorizatuak eta eskura dauden sarbideak. Arkitektura hori parte hartzen duen enpresa bakoitzarekin adostuko da, eta haiek proposatutako aldaketetara moldatu beharko da proposamena.
2. Kanpaina bakoitzari buruzko txosten orokorra, kanpainaren amaieran, mehatxu eta zaurgarritasun garrantzitsuenei buruzko informazioa jasotzen duena. Azterketak helburu duen azken txostenean erabiliko den informazioa partzialki jasotzen duen atzera begirako azterketa bat izango litzateke.
3. Kanpaina bakoitzaren amaieran, esleipendunak txosten indibidualizatu bat egin beharko du parte hartzen duen enpresa bakoitzeko. Txosten horretan jaso beharko dira enpresari buruzko informazio garrantzitsuena, OT segurtasun arloko heldutasun maila (IEC 62443), zaurgarritasunen zerrenda, aktiboen inbentarioa, arkitekturaren analisia, hobetzeko gomendioak, egindako aurkikuntza nagusiak….
4. Proiektuaren amaieran, kanpaina guztietan bildutako informazioaren azterketa bateratua egingo da, **Gipuzkoako industriak ICS inguruneetan duen zibersegurtasun arloko heldutasun mailari buruzko diagnostikoaren azken azterketa egiteko**. Txosten hori da azterketaren emaitza nagusia, eta, gutxienez, atal hauek izan behar ditu:
    a. Kanpainen garapena
    b. Aztertutako sektoreak
    c. Enpresen heldutasuna vs IEC62443-3-3
    d. Zaurgarritasunen identifikazioa eta horiek kudeatzeko modua
    e. Aktibo nagusien zerrenda
    f. Detektatutako arkitekturen tipologia
    g. Zaurgarritasunak kudeatzeko irtenbideen azterketa
        i. Eragindako sektorearen arabera
        ii. Enpresen tamainaren arabera
    h. Gomendio edo hobetu beharreko alderdi orokorrak, egindako aurkikuntzak kontuan hartuta.
    i. …

III.- METODOLOGIA

ZIUR Fundazioak lanak ikuskatzeko eta kontrolatzeko bete beharreko funtzioak eraman beharko ditu aurrera enpresa esleipendunak, eta, horretarako, zorrotz bete beharko ditu jasotako ohar eta gomendio guztiak.

Lanen bilakaeraren eta segimenduaren berri izateko, Ziur Fundazioak aukera izango du −zerbitzuaren beharren arabera− zerbitzua aurrera eramateko beharrezko jotako behar adina dokumentu aurkez ditzan

eta beharrezko jotako lan- edo informazio-bileretara joan dadin eskatzeko enpresa esleipendunari (presentzialki eta/edo telematikoki egin ahal izango du esleipendunak).

Edonola ere, segimendua egiteko modua (bilerak, aktak, txostenak…) aldatu ahal izango du ZIUR Fundazioak, baldin eta beharrezkoa dela iruditzen bazaio.

Kontratu honen barruan egindako dokumentuak eta aurrera eramandako ekintzak Ziur Fundazioaren nortasun korporatiboaren eskuliburuaren arabera eraman beharko dira aurrera.

Kontratuaren betearazpen materiala fase hauen arabera egin beharko da:

1. fasea.- Aurretiazko lanak:

1. ICSren autodiagnostikorako *framework*a egiteko modua (IEC62443-3-3)
2. Tresna/k zabaltzeko modua.

2. fasea - 1. kanpainaren garapena, gauzatzea eta ebaluazioa.

3. fasea - 2. kanpainaren garapena, gauzatzea eta ebaluazioa.

4. fasea - 3. kanpainaren garapena, gauzatzea eta amaierako ebaluazioa.

1. fasea aurrera eramateko, zerbitzuaren lehenengo hilabetean, kanpaina bakoitzean lortu nahi diren helburuak eta parte hartuko duten enpresen zerrenda zehaztuko ditu Ziur Fundazioko zuzendariak. Halaber, zerbitzua aurrera eramateko egingo diren jardueren kronograma onartu beharko du, enpresak egindako proposamenaren eta Ziur Fundazioak tresnaren erabileran trebatzeko hautatuko pertsonei zuzendutako prestakuntza-planaren edukiaren arabera.

Kanpaina bakoitza hasi aurretik, aldeek xehe-mehe zehaztu beharko dituzte aurrera eramango dituzten ekintzak.

Kanpaina bakoitzaren amaieran, zerbitzuaren atzerabegirako azterketa egin beharko da. Azterketa horretan, Ziur Fundazioak aurrez zehazturiko helburuen betetze-maila eta lan-metodologiaren egokitasuna ebaluatu beharko dira, eta azken kanpaina amaitzean, zerbitzuaren eta lortutako emaitzen balorazio globala ere egin beharko da.

Dokumentu eta jarduera guztiak ele bitan egingo dira −euskaraz eta gaztelaniaz−, baina horrek ez du prezio edo kargu gehigarririk sortuko.

Halaber, hizkuntza, irudiak eta edukiak modu ez-sexistan eta ez-androzentrikoan erabiliko direla bermatuko duten komunikazio-politikak aplikatuko dira.

IV.- TRESNAREN/TRESNEN EZAUGARRI TEKNIKOAK

Ingurune industrialen egungo egoerari buruzko informazioa bilatzeko irtenbide teknologikoak behar dira, eta irtenbide horiek gutxieneko baldintza batzuk izan behar dituzte, kalitatezko informazioa lortzen dela bermatzeko, lortu nahi den irismena lortzen dela ziurtatzeko eta parte hartzen duten enpresen mendekotasuna eta beharrak ahalik eta txikienak izateko.

Azterketa egiteko irtenbide teknologikoek ezaugarri hauek izan behar dituzte (ezaugarri horiek irtenbide teknologiko batean edo gehiagotan bete daitezke):

- Monitorizazio pasiboko irtenbide espezifiko bat izan behar du, parte hartzen duten enpresen jardunean eraginik ez duena.
- Trafikoa "lineaz kanpo" aztertzeko gaitasuna izan behar du, sarean sortutako eta tresnara bidalitako trafikoaren kopiak aztertuz.
- Kontsulta aktiboak egiteko aukera eman behar du, beti ere, parte hartzen duen enpresak eskatuta eta aurrez oniritzia emanda.
- Parte hartzen duten enpresa batzuek ez badute *switch* kudeagarririk aztertu nahi diren sareko segmentu batzuetan. Kasu horietan, enpresa esleipendunak trafikoaren kopiak sortzeko beharrezkoa den teknologia izan beharko du, zundara birbidali ahal izateko.
- Ingurune fisikoan nahiz birtualean zabaltzeko gaitasuna
- Urruneko kontroleko zentro batekin lotura zuzena izateko aukera
- Bildutako informazioaren *offline* esportazioa (zaurgarritasunak, aktiboak, anomaliak, etab.), kontrol-gunean konexiorik ez dagoenerako.
- IT/OT eragiketa konbergenteen erabateko ikusgarritasuna.
- Eragiketa industrialei eragiten dieten mehatxuak detektatzea.
- IT eta OT aktiboak identifikatu eta arakatzea eta horien funtzionamendua eta egoera sakonki ezagutzea, baldin eta aktibo horien ikusgarritasuna lortzen bada.
- Zaurgarritasun eta mehatxu potentzialak identifikatu eta lehenestea, *exploit* bihurtu eta eragiketa industrialei eragin aurretik.
- Konfigurazio-aldaketei segimendua egitea, auditoretza-segimendua egiteko gaitasun osoarekin.
- Ez du egon behar mugarik identifikatutako zaurgarritasun edo anomalietan.
- Aginte-taulak sortzeko aukera
- Politika konfiguragarriak eta granularrak aplikatzeko aukera
- Hainbat detekzio-bitartekoren bidez aktiboak, mehatxuak eta zaurgarritasunak identifikatzeko gai izan behar dute, azterketa osatuagoa eta errealagoa izan dadin.

72724351F KOLDOBIKA PECIÑA (R: G75203067)

Digitalki sinatuta norengandik: 72724351F KOLDOBIKA PECIÑA (R: G75203067)
Data: 2022.07.01 09:34:15 +02'00'