CENTRO DE
CIBERSEGURIDAD
INDUSTRIAL

Euskadin Zibersegurtasun Industrialak duen egoerari buruzko azterketa

BASQUE
CYBERSECURITY
CENTRE

2018ko edizioa

ZIBERSEGURTASUN INDUSTRIALAREN ZENTROA

Zibersegurtasun Industrialaren Zentroa (Centro de Ciberseguridad Industrial, CCI) irabazi asmorik gabeko erakunde independentea da. Bere eginkizuna Zibersegurtasun Industriala sustatzea eta hobetzen laguntzea da testuinguru berezi batean, non fabrikazioaren edo energiaren sektoreetako erakundeek eginkizun kritikoa duten gaurko gizartearen eraikuntzarako, ongizate estatuaren euskarri modura.

CCIk erronka horri aurre egiten dio hainbat jarduera garatuz: ikerkuntzak eta analisiak burutzea, iritzia sortzea, azterketak eta tresnak prestatzea eta argitaratzea, eta informazioaren eta ezagutzaren trukea, Ziberespazioan prozesu eta azpiegitura industrialak integratzearen ondorioz sortzen diren arriskuei –eta beren kudeaketari– dagokienez, bai teknologien, beren prozesu eta praktikak barne, eta bai norbanakoen eraginari buruz.

CCI da, gaur egun, Zibersegurtasun Industrialak eragiten dien, kezkatzen dituen edo horretan diharduten entitateen –pribatuak nahiz publikoak– eta profesionalen ekosistema eta topagunea. Era berean, esperientzien trukaketarako eta arlo honetan murgilduta dauden sektoreen dinamizaziorako erreferentzia da gaztelaniaz dihardutenentzat.

ISBN: 978-84-947727-1-9
Lehenengo edizioa: 2018ko urria

Maiquez, 18 · 28009 MADRID
+34 910 910 751
info@CCI-es.org
www.CCI-es.org
blog.CCI-es.org
@info_CCI
www.linkedin.com/in/centrociberseguridadindustrial/

BASQUE CYBERSECURITY CENTRE

ZIBERSEGURTASUN EUSKAL ZENTROA (BASQUE CYBERSECURITY CENTRE, aurrerantzean BCSC) Eusko Jaurlaritzako Ekonomiaren Garapen eta Azpiegitura Sailaren mendekoa den ERALDAKETA LEHIAKORRERAKO SOZIETATEA SAn (aurrerantzean SPRI Taldea) kokatzen den ekimena da. BCSC Euskadin zibersegurtasuna eta herritarren, enpresen eta erakunde publikoen konfiantza digitala garatzeko erreferentziazko entitatea da, batez ere eskualde honetako ekonomiaren sektore estrategikoentzat.

BCSC euskal gizartean zibersegurtasunaren kultura areagotzeko Eusko Jaurlaritzak duen tresna da eta zerbitzu espezializatuen eskaintzaile eta eskatzaileen arteko topagunea izatera iritsi nahi du. Horrekin berrikuntzarako aukera sortu eta enpresen arteko lehiakortasuna sustatuko luke, eta herritarrek jarduera digital seguruago bat izateko ohiturak gara ditzaten ahalbidetuko litzateke.

Bere helburuak lortzeko, zehar ekimen baten modura definitzen da BCSC, bere sorreratik bertatik Eusko Jaurlaritzako lau sail inplikatzen dituena: lehen aipatutako Garapen eta Azpiegitura Saila, Segurtasun Saila, Gobernantza Publiko eta Autogobernu Saila eta Hezkuntza Saila.

Zentroaren jardueren artean ikerkuntza proiektuak, ekintzailetza ekimenak eta estatu nahiz nazioarte mailako beste eragile eskudun batzuekiko lankidetza koordinatuak daude. Izan ere, elkarlan estuan dihardu bere Batzorde Iraunkorreko kide diren Zientzia Teknologia eta Berrikuntzaren Euskal Sareko eragileekin.

Hortaz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera sustatzea eta erreferentzia izango den sektore profesionala sor dadin ahalbidetzea. Testuinguru horretan eragile osagarrien artean lankidetza proiektuak gara daitezen sustatzen du berrikuntza teknologikoaren alorrean, ikerkuntzarenean, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorrean.

BCSCk hainbat zerbitzu ematen ditu Gertakarien aurreko Erantzun Talde modura (aurrerantzean CSIRT, bere ingelesezko siglengatik: “Computer Security Incident Response Team”). Era berean, Euskal Autonomia Erkidegoaren eremuan lanean dihardu bere gaitasuna areagotzeko mehatxu berriak garaiz antzematen eta horiei buruzko alertak ematen, informazioaren segurtasun arloko gertakarien erantzun eta analisian, eta euskal gizartearen beharrei erantzuteko prebentzio neurrien diseinuan.

Arabako Parke Teknologikoa
+34 945 010 059
info@bcsc.eus
www.basquecybersecurity.eus
@basquecscentre
www.linkedin.com/company/basque-cybersecurity-centre/

egileak

Susana Asensio

Javier Diéguez

Edorta Echave

Asier Martínez

José Valiente

aurkibidea

00.
SARRERA 6
Azterketaren deskribapena 8
Aztertutako sektoreak 8
Esker onak 8

01.
ZIBERSEGURTASUN INDUSTRIALAREN ANTOLAKUNTZA 11
Zibersegurtasun industrialari dagokion ardura 13
Trebakuntza maila zibersegurtasun industrialean 15

02.
ZIBERSEGURTASUN INDUSTRIALAREN KUDEAKETA 17
Arriskuen ebaluazioa 19
Segurtasun gertakarien kudeaketa 19
Zibersegurtasun industrialeko ekimenen planifikazioa 20

03.
ZIBERSEGURTASUN INDUSTRIALAREN ALDERDI TEKNIKOAK 21
Sareen konexioa 23
Urruneko sarbideak 23
Arau eta ereduen erabilera 25
Zibersegurtasun industrialari buruzko neurriak 25

04.
ZIBERSEGURTASUN INDUSTRIALAREN MERKATUA 27
Zibersegurtasun industrialeko jarduera berrien aurreikuspena 29
Proiektu berrietarako baldintzak 30
Zibersegurtasun industrialeko proiektuen kontratazioa 31
Ziurtagiri profesionalak 32

05.
ONDORIOAK 34

06.
GLOSARIOA 35

AHOLKUA: Logotipoen gainean klika egiterakoan indizera itzultzen zara.
Hiperesteka batera joan ondoren atzera vueltatzeko Alt+ ezkerreko gezia.

00.

Sarrera

00.

AZTERKETAREN DESKRIBAPENA
AZTERTUTAKO SEKTOREAK
ESKER ONAK

AZTERKETAREN DESKRIBAPENA

Azterketa hau elkarrekin egin dute Zibersegurtasun Industrialaren Zentroak (CCI) eta Zibersegurtasun Euskal Zentroak (BCSC, siglak ingelesetik hartzen dituenez gero).

Bere prestakuntzarako euskal enpresa industrialetako profesionalei inkestak egin zaizkie, zibersegurtasunaren ondoko arloei buruz:

Arloa	Helburua	Galdera kop.
Antolakuntza	Euskal Industrian Zibersegurtasun Industrialari dagokionez dauden antolakuntza egitura ezberdinak aztertzea	4
Kudeaketa	Arriskuaren ebaluazio maila identifikatzea, bai eta zibersegurtasun industrialaren arloko ekimenen planifikazioa eta gertakarien kudeaketa ere	3
Alderdi teknikoak	Euskal Industrian automatizazio eta kontrol teknologietarako sarbidean eta horien erabilpenean dauden babes neurriak aztertzea	6
Merkatua	Euskal Industrian zibersegurtasun arloko proiektuak burutzeko eta konponbideak ezartzeko motibazioak identifikatzea	7

Horretarako, inkestak egin diren sektore bakoitzeko lagin adierazgarri bat hartu da. Lankidetza epea zabalik egon da 2018ko otsailetik ekainera bitartean, eta guztira **90 enpresa industrialek** hartu dute parte.

Egindako azterketaren emaitzak aurkezten ditu dokumentu honek eta interpretazio bat ere eskaintzen du, berau erredaktatu dutenen eta berrikuspen prozesuan parte hartu dutenen ezagutzan eta esperientzian oinarrituta. Irakurlearen irizpidearen baitan uzten dugu bakoitzak bere ondorioak ateratzea.

Azterketa honetan ez da argitaratuko inolako bezero, proiektu, informazio tekniko edo finantzarioaren xehetasunik. Bertan soilik datu kuantitatibo kontsolidatuak agertzen dira eta, beraz, ez dago inolako mehatxurik parte hartu duten erakundeen konfidentzialtasunerako.

AZTERTUTAKO SEKTOREAK

Azterketarako inkestatutakoak gure eskualdean gehien hazten ari diren eta euskal ekonomian pisurik handiena duten sektoreetako erakundeetako ordezkariak dira. Horregatik, multzorik handiena fabrikazioak, ingeniaritzak eta sektore elektrikoak osatzen dute, eta ondoren “beste” sektore batzuek –zehaztu gabe–. Era berean, informazioaren teknologien sektoreak eta multisektore industrialak ere parte hartze nabarmena izan dute. Parte hartu duten beste sektore batzuk industria kimikoa, garraioa, eraikuntza, gasa eta petrolioa eta ikerkuntza dira, besteak beste.

ESKER ONAK

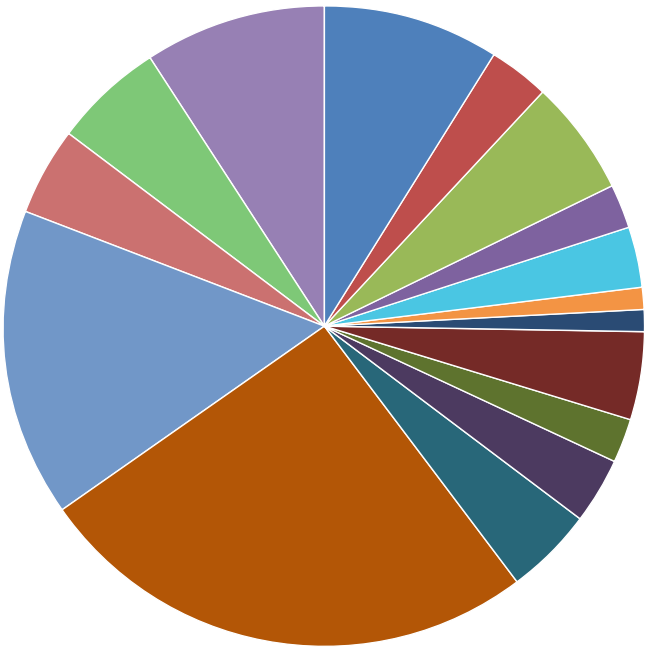
Zibersegurtasun Industrialaren Zentroak (CCI) eta Zibersegurtasun Euskal Zentroak (BCSC) aipamen berezia eta esker ona adierazi nahi diete inkestaren galdetegiaren zabalkundean lagundu duten entitateei:

Segurtasun Adituen Euskal Elkartea (SAE)

- **Industria alorreko 9 kluster**
  Energía - http://www.clusterenergia.com
  FEAF - http://www.feaf.es
  MAFEX - https://www.mafex.es
  MLC-ITS - http://www.mlcluster.com
  PAPEL - http://www.clusterpapel.com
  SIDEREX - https://www.siderex.es
  SIFE - http://www.forjas.org
  UNIPORT - http://www.uniportbilbao.es
  ERAIKUNE - http://www.eraikune.com/

- **Industria alorrekoak ez diren 2 kluster**
  GAIA - http://www.gaia.es
  EIKEN - https://eikencluster.com

Enpresaren sectorea



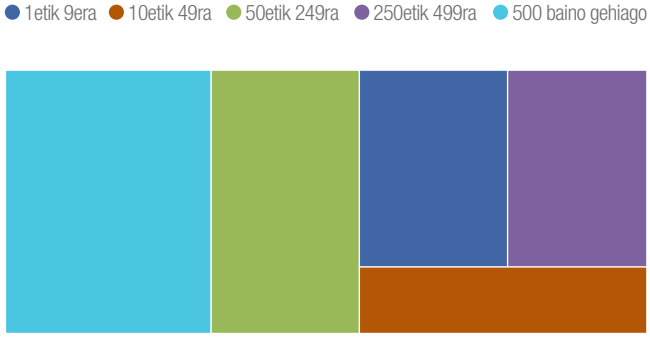
- Elektrikoa **9%**
- Gasa eta petrolioa **3%**
- Informazio teknologiak **6%**
- Osasuna **2%**
- Ikerkuntza instalazioak **3%**
- Elikadura **1%**
- Industria Nuklearra **1%**
- Industria Kimikoa **4%**
- Industria Farmazeutikoa **2%**
- Administrazio publikoa **3%**
- Garraioa (aireportuak, portuak, trenbideak, trafikoa...) **4%**
- Fabrikazioa **26%**
- Ingeniaritza **16%**
- Eraikuntza **4%**
- Industria multisektorea **6%**
- Ura **9%**

1. grafikoa – Azterketan ordezkatuta dauden sektoreak.

Azterketak sektore ugariren babesa izan du, nazio mailan nahiz nazioartean presentzia geografikoa duen ekosistema global bateko kide diren enpresak dituztenak.

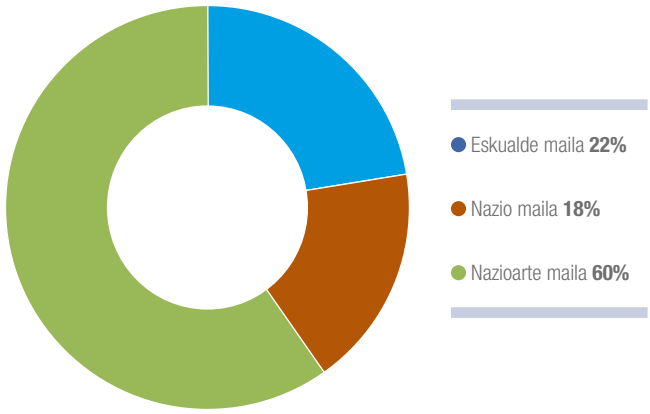
Aniztasun hori kontuan izanik, eskuratutako datuek ikuspegi zabala eta oso zehatza ematen dute Zibersegurtasun Industrialaren arloan azken urte hauetan egin diren aurrerakuntzei buruz. Eta ez soilik sektore jakin baten kasuan, bere sareen babesari dagokionez kezka handiagoa edo txikiagoa izan dezakeena, baizik eta euskal sare industrial osoari buruz.

Langile kopurua



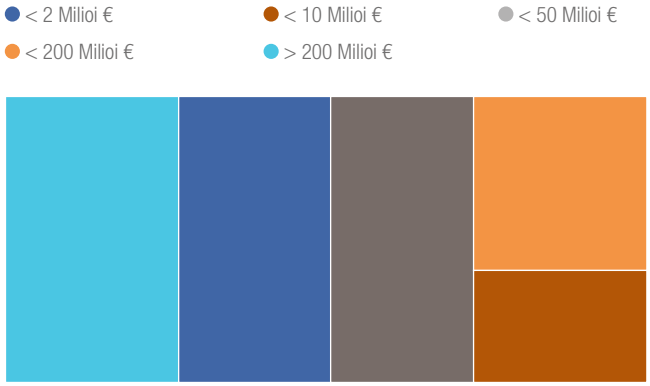
2. grafikoa – Langile kopurua.

Zabalkunde geografikoa



3. grafikoa – Zabalkunde geografikoa.

Fakturazio globala



4. grafikoa – Fakturazio globala.

Langile kopuruari eta fakturazio globalari dagokionez lortutako datuetan oinarrituz, aztertutako enpresen zati esanguratsu bat euskal enpresa handiei dagokiela ondoriozta daiteke. Baieztapen hori berretsi egiten da enpresen %60k nazioarteko presentzia duela ikustean.

Enpresa mota horiek (enpresa handiak, alegia, ETEak ez direnak) aktiboenak izaten dira normalean beren azpiegiturak babesteari dagokionez, bai euren borondate hutsagatik, bai kontzientziatze maila handiagoa dutelako jasaten duten arrisku mailagatik, bai baliabideak izateagatik, edo bai partzuergo mailan planak garatzearen ondorioz barne arauak betetzeagatik.

Bestalde, inkestatutako enpresen artean eskualdeko azpiegitura kritikoak daude. Horregatik, eta aztertutako euskal industriak handiak direla dioen lehen aipatu den datuagatik, txosten honek adierazkortasun berezia duela esan daiteke.

01.

Zibersegurtasun Industrialaren antolakuntza

01.

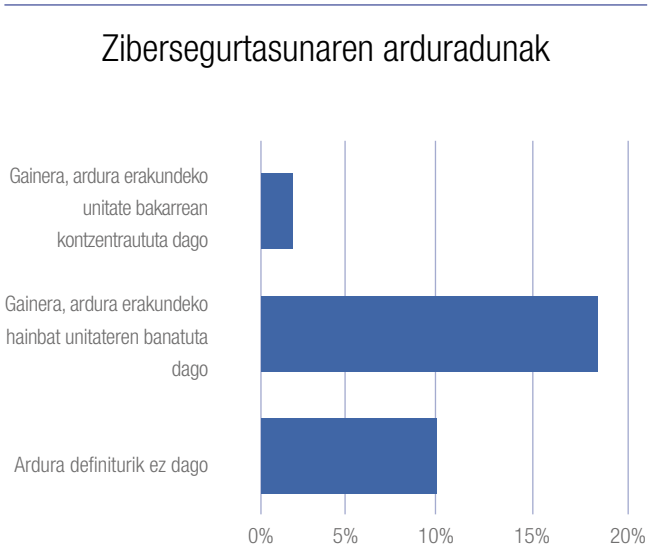
ZIBERSEGURTASUN INDUSTRIALARI DAGOKION ARDURA
TREBAKUNTZA MAILA ZIBERSEGURTASUN INDUSTRIALEAN

Atal honetan kontuan hartu beharra dago aztertutako enpresen antolakuntza egitura ezberdina dela. Hori dela eta, Zibersegurtasun Industrialari dagokionez, arduren, inplikazioen eta gaitasunen esleipenak ere aldakuntzak izan ditzake.

ZIBERSEGURTASUN INDUSTRIALARI DAGOKION ARDURA

Zure erakundean nork edo nortzuk daukate Zibersegurtasunaren arloan automatizazio sistemak eta kontrol industriala babesteko ardura?

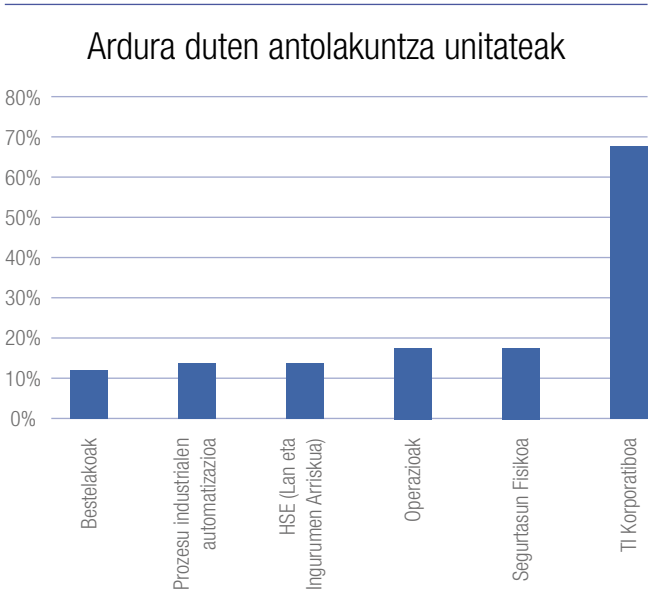
Zibersegurtasunaren arloan ardura finkatuta daukatenen artean, datuek baieztatzen dute joera berdina dutela guztiek ardura hori antolakuntza unitate ezberdinen artean banatzeko. Inkestatutako entitateen artean, oso gutxik kontzentratzen dute konpromiso hori sail bakar batean. Nolanahi ere, daturik kezkagarriena da oraindik badaudela erakundeak errealitate horri aurre egin ez diotenak eta ardura hori definitu ez dutenak. Kasu horietan zibersegurtasuna ez da arlo zehatzen bati esleitu zaion eskuduntza, eta hortaz, erakundeari ez zaizkio ematen behar dituen baliabide eta bitartekoak neurriak aurrera eraman ahal izateko.



5. grafikoa – Zibersegurtasunaren arduradunak.

Sail unitateei dagokienez, inkestatutako entitate gehienek (%70) ardura hori informazio teknologien alorrari esleitzen diote, eta hortaz, ekintza horiek ikuspegi logiko batetik antolatzen dituzte, fisiko edo prozesuei lotutako batetik baino. Hau izan daiteke arlo horiek zibersegurtasunaren arloari buruz duten kontzientziazio eta heldutasun maila handiagoagatik, eta horietatik jartzen direlako abian agertoki berriei aurre egiteko neurriak.

Gainerako arloek %10 eta %20aren arteko pisua dute. Prozesuen Automatizazio arloa nekez iristen da %10era eta datu horrek seguruenik adierazten du instrumentazio eta kontroleko arduradunek zibersegurtasunaren gaiei buruz duten kontzientzia falta beren ingurunean.

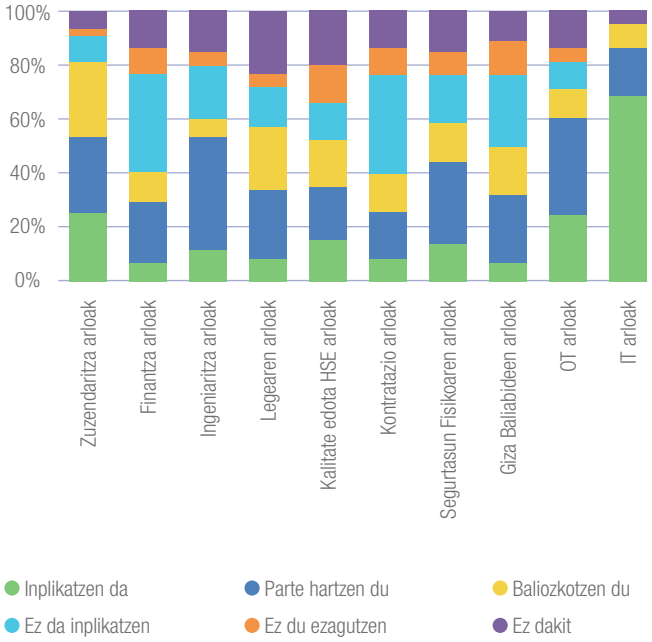


6. grafikoa – Ardura duten antolakuntza unitateak.

Nola hartzen dute parte erakundeko arlo ezberdinek zibersegurtasunaren alderdietan?

Kontrol sistemen babesean dagoen ardura mailari dagokionez, ikusten da IT arloak daukala inplikaziorik handiena alde handiz. Jarraian OT arloak (Operazio Teknologiak) eta ingeniaritza daude, izan ere, horien parte hartze eta inplikazioa txikiagoa izan arren, azpimarratzekoa da.

Erakundeko arlo ezberdinek nola hartzen dute parte zibersegurtasunaren gaian?



7. grafikoa – Erakundeko arloen parte hartzea.

Negozioaren arduradunak sentiberatuta daude sare industrialen Segurtasunaren arau eta arriskuekin?

Datuek erakusten dutenez, aztertutako enpresen negozio arduradunen artetik ia erdiak (%48) sentiberatuta daude 'normaltzat' jo daitekeen neurri batean sare industrialetako arau eta arriskuei dagokienez *–normaltzat jotzen da erakunde batentzat gertakari batek duen, nahita egindakoa nahiz ez, arrisku, mehatxu eta eragin nagusien ezagutza, zeinahi delarik bere sektorea–.*

Zoritxarrez, oraindik %18ak dio arrisku horiei buruzko oso sentiberatasun txikia duela. Zuzendaritzaren babes egokirik gabe, gai honetako ekimenek seguruenik ez dute izango laguntzarik erabakiak hartzerakoan ezta aurrekontu nahikorik ere instalazioen eskuragarritasunari eragingo dioten arriskuak murrizteko eta saihesteko. Testuinguru horretan, ezinbestekoa da zuzendaritzaren mailan ahalegin handiagoa egitea, erakundearen barnean negozioaren iraunkortasunak duen arriskuaz kontzientzia hartzen lagun dezan.

Zibersegurtasun Industrialaren Zentroak eta Zibersegurtasunaren Euskal Zentroak lanean dihardute xede horretan laguntzeko erakunde industrialetako zuzendaritzako kideei eta negozio arduradunei, gaur egun teknologiak negozioaren iraunkortasunerako duen garrantziari buruz, eta bere integritatearen edo eskuragarritasunaren galerak prozesuen kalitatean edo segurtasunean izan ditzakeen ondorio larriei buruz jabe daitezen. 2017an argitaratutako *"Zibersegurtasunaren onurak enpresa industrialentzat"* dokumentua[1] Zibersegurtasun Industrialaren hobekuntzaren bultzadan eta sustapenean CCIk duen konpromisoaren erakusgai bat baino ez da.

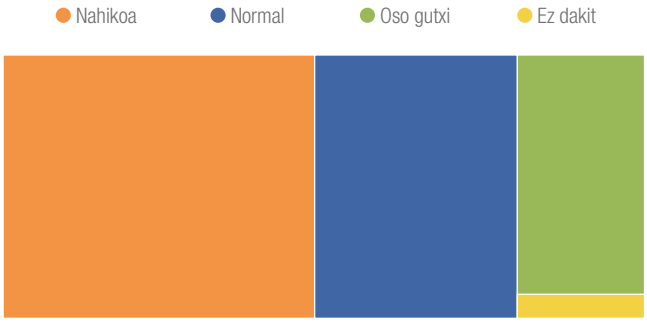
Bestalde, Zibersegurtasun Euskal Zentroak aldiro antolatzen ditu kontzientziazio jardunaldiak ingurune industrialetan xede diren entzule mota ezberdinei zuzenduta. Jardunaldi horien helburu nagusia da OT munduko enpresek zibersegurtasunaren alorrean aurre egin behar dieten arrisku ohikoenez kontzientziatzea eta enpresa horiek zibersegurtasun neurriak aplikatzea babestuago egon daitezen eta, beraz, dauden mehatxuetatik urrunago. Halaber, teknologia mota horiek ezarrita, enpresa horiek balio erantsi bat izango dute beren gaitasun lehiakorrari eusteko.

Jarduera hori Eusko Jaurlaritza aurrera eramaten ari den beste ekimen publiko mota batzuen ildo beretik doa, zibersegurtasuna areagotzeko sektore pribatuak egiten dituen ahaleginak babestea bilatzen dutenak. Horien artean prestakuntza, diru-laguntzak eta beste era batzuetako laguntzak daude eta, azken finean, azken helburua Euskadi erreferentzia modura kokatzea da zibersegurtasunaren aplikazioari dagokionez.

Azkenik, aurretik esandakoarekin aurrez aurre, horien artetik kopuru nabarmen batek (%32) sentiberatze maila aski adierazgarria dela uste du.

[1] Zibersegurtasun industrialaren eginkizun gaitzaileari buruzko ikuspegia https://www.cci-es.org/informes-y-analisis-estategicos

Negozioaren arduradunak sentiberatuta daude zibersegurtasunaren arau edo arriskuekin?



8. grafikoa – Negozioaren arduradunen sentiberatze maila.

Zenbateko horiek hobetu litzeke enpresaren hierarkia ezberdinetan kontzientziatze jarduerak areagotuko balira, bai zuzendaritza mailan eta bai erakundeko sareen eta sistemen eskuratze, balioztatze, kudeaketa eta kontrolarekin gutxieneko zerikusi bat izan lezaketen arlo guztietan.

Garrantzitsua da azpimarratzea Eusko Jaurlaritzak bultzatutako eskualde ekimenak eta *Zibersegurtasun Euskal Zentroa* (BCSC) bezalako eskualde entitateak[2] hasi direla eragiten euskal sare enpresarial askotarikoan, eta antolakuntza maila guztietan indarrez sartzea espero da, batez ere, enpresa publikoetan eta azpiegitura kritikoetan. Arriskuen kontzeptuei eta babes orokorreko neurriei buruzko sentiberatze eta prestakuntza ekintza gutxieneko hau sektore bakoitzerako bereziki diseinatu beharra dago. Horrela horietariko bakoitzak argi ikusi ahal izango ditu horiek aurrera eramatearen abantailak, enpresaren aktiboen gaineko eskuduntzei eta ardurei dagokienez.

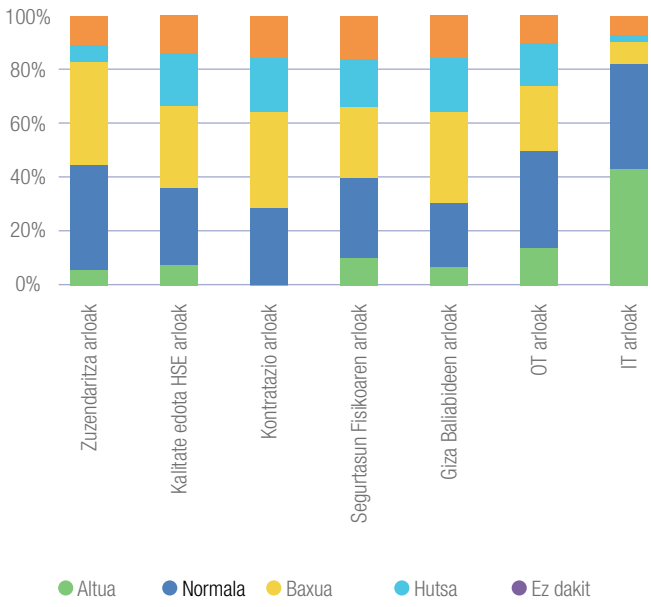
Programa hauen helburuak ardatz honetan zentratu behar lirateke: zibersegurtasunak dituen onurak prozesuen kalitate, erresilientzia eta segurtasunaren gainean. Eta hortaz, zibersegurtasunarekiko konpromisoa modu holistikoan lortu beharko litzateke erakundearen maila guztien baitan.

TREBAKUNTZA MAILA ZIBERSEGURTASUN INDUSTRIALEAN

Zein da zure erakundearen trebakuntza maila Zibersegurtasun Industrialean?

Zibersegurtasunaren alderdietan departamentuek duten parte hartze mailaren erakusgarri, hurrengo grafikoan ikus dezakegu zer harreman dagoen diziplina honetako trebakuntza mailaren eta antolakuntza unitateen artean. Zibersegurtasun Industrialaren gaian enpresek duten trebakuntza ezberdina da departamentuen arabera, noski. Enpresaren motor ekonomikoa bere ekoizpen arloa baldin bada ere –automatizazio eta kontrol teknologiak hil ala bizikoak diren arloa–, euskal enpresa industrialek trebakuntza handiagoa erakusten dute informazioaren Segurtasunarekin zuzenean lotuta dauden departamentuetan (IT), negozio prozesuen mantenuaren ardura dutenetan baino (OT).

Zein da zure erakundearen trebakuntza maila Zibersegurtasun Industrialean?



9. grafikoa – Lantaldeen trebakuntza mailaren arteko alderaketa.

[2] https://www.basquecybersecurity.eus/es/

Hortaz, negozioarekin zerikusia duten arduradunen eginkizun funtsezkoa da erresilientzia maila altua lortzea. Horrek trebakuntza berezia izatea suposatzen du ekoizpen prozesuen funtzionamendu egokia oztopa dezaketen mehatxuen edo giza akatsen aurreko babesari dagokionez.

Datu oso adierazgarria da inkestatuek uste izatea OT arloetako langileek trebakuntza maila txikia (%28) edo normala (%38) daukatela, eta soilik kudeatzaileen %12k uste du bere automatizazio ekipoa modu egokian prestatuta dagoela. Are gehiago, %14ak uste du ekipo horren trebakuntza maila hutsa dela. Ezinbestekoa da, beraz, enpresek Operazio Teknologien alderdiekin eta bere segurtasun teknologikoarekin harremana duten langileen prestakuntzan inbertitzea.

02.

Zibersegurtasun Industrialaren kudeaketa

02.

ARRISKUEN EBALUAZIOA

SEGURTASUN GERTAKARIEN KUDEAKETA

ZIBERSEGURTASUN INDUSTRIALEKO EKIMENEN PLANIFIKAZIOA

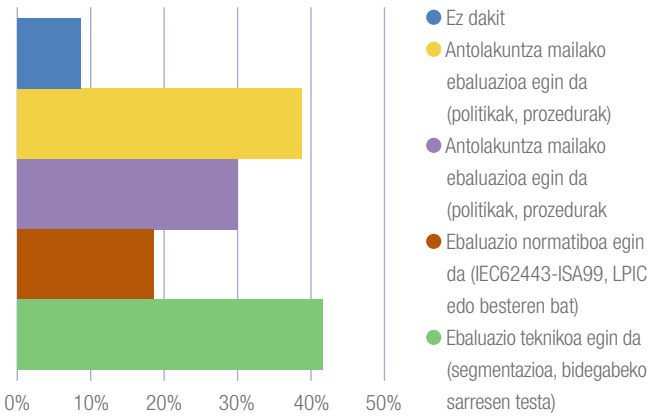
ARRISKUEN EBALUAZIOA

Zure enpresak automatizazio eta kontrol sistemek duten arrisku mailaren ebaluazioak egin ditu?

Sare industrialetako arriskuen ebaluazioa egiteari dagokionez, datuak oso kezkagarriak dira eta erakundearen prozesu industrialean operatzen duen teknologiak duen arrisku egoera erreala aztertzeko dagoen kezka txikia erakusten dute. Hain zuzen ere, %42ak onartzen du bere automatizazio eta kontrol sistemen arrisku mailaren inolako ebaluaziorik ez duela egin. Hortaz, aurre egin beharko dieten ondorioak zein diren ez jakiteaz gain, euren heldutasun egoerari buruzko informaziorik ez daukate. Beraz, nekez egin ahal izango dute behar diren baliabideen kudeaketa eta lehenespen eraginkorrik ezaugarri hauetako proiektu bat exekutatu beharrean aurkitzen direnean.

Egindako ebaluazioen artean, antolakuntza gaitasunari buruzkoa nabarmentzen da %38arekin, ezarri diren politikak eta prozedurak barne hartzen dituena, beste aldagai batzuen artean. Inkestatuen ia %38ak beste bi ebaluazio mota egin dituela adierazten du: sareei buruzko ebaluazio teknikoa, esate baterako ahultasunen eta segmentazioen azterketa eta bidegabeko sarreren testa; eta arautegiei eta hainbat arau eta estandarren betetze mailari buruzko ebaluazioa, esate baterako NERC-CIP, IEC 62443 eta Zibersegurtasun Industrialaren Kudeaketa Sistema[3]–CCIren SGCI–, besteak beste.

Zure erakundean kontrol eta automatizazio sistemek duten arrisku mailaren ebaluazioak egin dira?



10. grafikoa – Kontrol sistema eta automatizazio industrialetako arriskuen azterketa

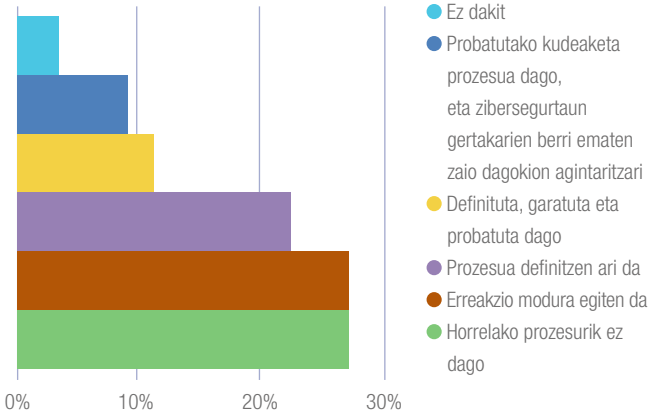
[3] https://www.cci-es.org/sgci

SEGURTASUN GERTAKARIEN KUDEAKETA

Nolakoa da Segurtasun Gertakarien Kudeaketaren prozesua zure enpresaren automatizazio sareetan?

Aztertutako enpresen artetik soilik %12ak dio Zibersegurtasun Industrialeko Gertakarien Kudeaketarako prozesu garatu bat daukala indarrean dagoena. Enpresen %27an horrelako prozesurik ez dago eta beste %27 batean erreakzio modura aplikatzen da. Bestalde, enpresen %23ak dioenez, prozesu hau definitzen ari dira, prozesu behar-beharrezkoa bestela ere, 2017an gertatu ziren eragin globaleko gertakarietan ikusi zen moduan. Wannacry, Petya eta Crashoverride bezalako malwarearen agerpenari buruz ari gara noski, hainbat sektoreri eragin ziena: automobilena, itsasokoa, energiaren zabalkundea edo petrokimikoa. Baina ez diegu gertakariei soilik begiratu behar, izaten ari diren bilakaerari baizik. Hori da, hain zuzen, instalazio industrialen segurtasun funtzionaleko safety sistemen kasua, Titón/Trisis/Hatman malwarea eragiten hasi baitzaie. Era berean, gero eta gehiagotan gertatzen da IoT gailuak erabiltzea zerbitzuaren ukapen masibo moduko erasoetarako, besteak beste.

Nolakoa da segurtasun gertakarien kudeaketaren prozesua zure erakundearen industria eremuan?



11. grafikoa – Segurtasun Industrialeko Gertakarien kudeaketa

Horregatik erakundeentzat azken urteak erabakigarriak izan dira zibersegurtasunaren alorrean, eta gertakarien kudeake-

tarako beren prozesuak probatu behar izan dira. Mundu mailako gertakarietan milaka gailu izan dira kaltetuak eta horrek erakutsi du jarduera prozedurek ezin hobeki planifikatuta egon behar dutela eta, eraginkorrak izango badira, dagokien pertsona guztien inplikazio egokia behar dutela –zuzendaritzatik hasi eta katearen azken mailaraino–.

Beharrezkoa da koordinazioa egotea kanpoko erakunde egokiekin –CERT edo CSIRT–. Hori da Zibersegurtasun Euskal Zentroaren (BCSC) kasua ere. Honek laguntza eta aholkua eskaintzen die zibersegurtasun gertakari batengatik kaltetuak izan diren erabiltzaileei, jarraitu beharreko ildoetan gidatu egiten ditu eta, beharrezkoa izanez gero, kontakturik egokienarekin harremanetan jartzen ditu. Era berean, bai nazio eta bai nazioarte mailan, arlo publiko nahiz pribatuko erakunde eta erantzun ekipo ugarirekin lan egiten da modu bateratu eta koordinatuan, zibermehatxuei erantzun bateratu eta koordinatua ematearren.

Zibersegurtasun industrialaren alderdi ezberdinei buruz esperientzien trukea egiteko ekimen desberdinek, positiboek nahiz negatiboek, komunitateari ahalbidetzen diote informazio baliagarria eskuratzea zibersegurtasunarekin zerikusia duten prozesu ezberdinak hobetzeko, eta zehazkiago, gertakarien kudeaketarako.

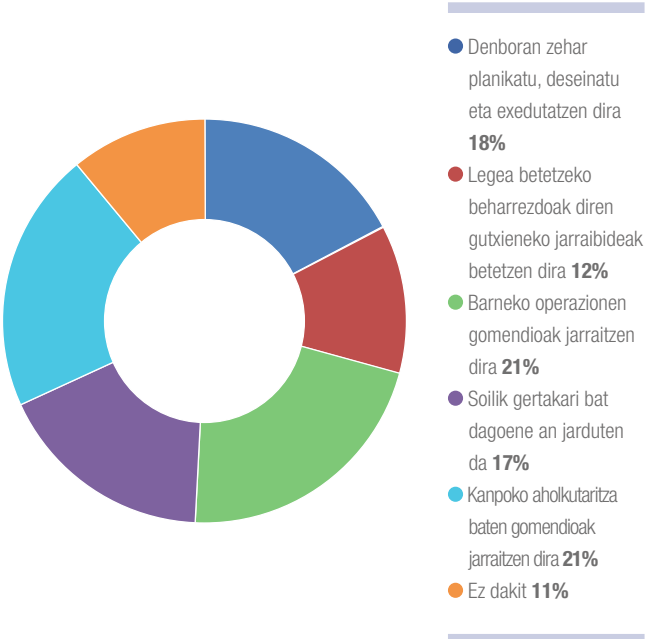
ZIBERSEGURTASUN INDUSTRIALEKO EKIMENEN PLANIFIKAZIOA

Nola planifikatu ohi dira zure enpresan Zibersegurtasun Industrialeko ekimenak?

Zibersegurtasun Industrialeko ekimenen planifikazioari dagokionez, aipagarria da jardueren artean dagoen ezberdintasun handia. Enpresen %21ak kanpo aholkularitza baten gomendioak jarraitzen dituztela adierazten dute, beste %21 batek, aldiz, dio barneko operazioen aholkuak jarraitzen dituztela. Erakundeen %18ak ekimenak denboran zehar planifikatu, diseinatu eta exekutatzen dituzte eta %12ak aitortzen duenez, legeak ezartzen dituen gutxieneko jarraibideen egokitzapenaren testuinguruan burutzen ditu bere ekimenak. Era beran, adierazgarria da hainbat enpresak soilik jarduten dutela gertakari bat gertatzen denean (%17).

Garrantzitsua da ohartaraztea zibersegurtasunaren inbertsioa legeak baimentzen duen gutxieneko mailan soilik mantentzen badugu, gaur egun epe laburrera dauden arriskuei aurre egiteko beharrezkoa den estandarretik oso behera egongo direla gure babes mailak. Estatuen lege eta arauak beti dira geldoak, batez ere, legegileentzat konplexuak eta urrunak diren gai teknikoetan, Zibersegurtasun Industrialaren kasuan bezala. Bai teknologiak eta bai ziberdelinkuentzia abiadura handian ari dira garatzen, eta batez ere bigarren hori sofistikazio eta hobekuntza maila handiagoekin.

Nola planifikatu ohi dira zure erakundean Zibersegurtasun Industrialeko ekintzak?



12. grafikoa - Zibersegurtasun Industrialeko ekimenen planifikazioa

03.

Zibersegurtasun Industrialaren alderdi teknikoak

03.

SAREEN KONEXIOA

URRUNEKO SARBIDEAK

ARAU ETA EREDUEN ERABILERA

ZIBERSEGURTASUN INDUSTRIALARI BURUZKO NEURRIAK

SAREEN KONEXIOA

Zure enpresako automatizazio sareak segmentatuta eta babestuta daude?

Azken urteetan erakunde industrialek ikusi dute beren gailuak garatu egin direla eta, horren ondorioz, erakundea bera babesteko finkatuta zeuden egituretako asko aldatu behar izan direla. Sare arkitekturek urte luzeetan trafiko isolatua, jarraitua eta segurua jasan izan dute, baina orain aldatu egin behar dira eskaera berrietara egokitzeko: mantenu prediktiboa, logistika moldatzailea, prozesuen hobekuntza eta trazabilitate adimenduna, besteak beste. IT eta OTen arteko integrazioa behar da, eta horrek negozioaren iraunkortasuna arriskuan jar dezake baldin eta neurri egokiak abian jartzen ez badira.

Aztertutako enpresa industrialen artetik laurdena inguruk (%22) diote bere sareen artean erabateko banaketa dagoela, batez ere korporatiboa eta industrialaren artean.

Erakundean sareak segmentatuta eta babestuta daude?

13. grafikoa – Automatizazio sareen segmentazioa eta babesa.

Sare korporatiboaren eta sare industrialen artean lotura bat dagoela aitortzen duten enpresen artetik portzentajerik adierazgarrienak dio suebaki batez segmentatuta dituela (%40) edo iragazki gailu batzuen bitartez hainbat segmentazio maila dituela (%22). Nolanahi ere, enpresen ehuneko oso kezkagarri bat dago, %17 hain zuzen, sareak zuzenean loturik dituena, eta hori arrisku oso handia da segurtasun gertakarien aurrean.

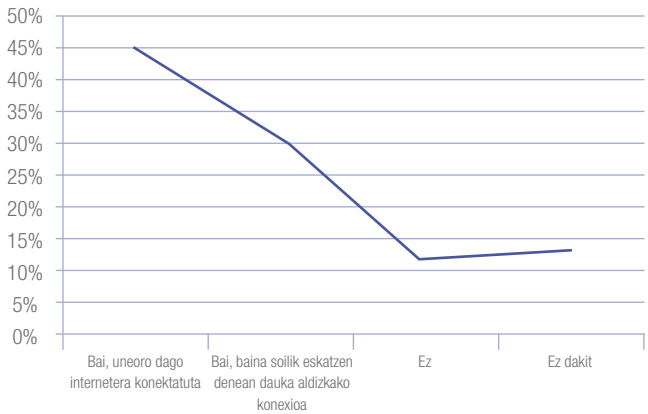
Jakina, azken enpresa multzo horren barnean egongo dira arriskuen ebaluaziorik ez dutela egin aitortzen zutenak. Horregatik, sareetako sarbidea eta beren trafikoa kontrolatzeko inolako iragazkirik gabe konektatuta izateak suposatzen duen arriskuaren pertzepzio errealik ez dute.

URRUNEKO SARBIDEAK

Internetera konektatuta dauden gailuak ditu zure sare industrialak, zeinahi direla ezarritako babes mekanismoak?

Aztertutako enpresa gehienek (%45) diote Internetera uneoro konektatuta dauden gailuak dituztela. %30era jaisten da Interneterako konexioa eskaeraren baitan soilik aktibatzen dutenen multzoa, eta %12ak dio ez daukala inolako gailurik sare irekian. Kontrol saretik kanpoko azpiegituretatik sarbidea beharrezkoa izanez gero, konexio horiek babesteko beharrezkoak diren zifratua eta autentifikazioa VPN irtenbideek eskaintzen dute. Urruneko sarbiderako software edota hardware espezializatua erabiltzea, eguneraketen mantenuari dagokion segurtasun politika egokia izatea eta sarbideen eta erabiltzaileen kudeaketa beharrezkoak dira, operazio sistemetara bidegabeko sarbide batek suposa lezakeen arriskua murrizteko.

Zure sare industriala edo bertako gailu edo sistemaren bat internetera konektatuta dago (zeinahi direla ezarritako babes mekanismoak)?



14. grafikoa – Internetera konektatutako automatizazio sareen gailuak.

Internetera gailurik konektatuta daukaten ez dakitela adierazten dutenen ehunekoa kezkagarria da (%13), batez ere konexio iraunkorrak baldin badira. Kasu horretan babes falta dagoela esan nahi du eta, hortaz, prozesu kritikoetan operatzen duten sistemen eskuragarritasuna edo integritatea arriskuan jar dezaketen gailuak agerian daudela.

Gaur egun hainbat ekimen daude agerian dauden IPak antzemateko –esate batera Shodan[4] ezaguna, Censys edo ZoomEye–. Tresna horiek hainbat eremuren araberako iragazkia egitea ahalbidetzen dute eta horrela erabiltzaileak bere erakundearen barnean agerian dauden eta ahulak diren ekipoak antzeman ditzake, gaian ezagutza handirik izan gabe ere. Horregatik, gure sareek eta gailuek daukaten agerpen mailaren ebaluazio bat egitea beharrezkoa da, horiek kontrolatzeko eta modu egokian kontrolatzeko.

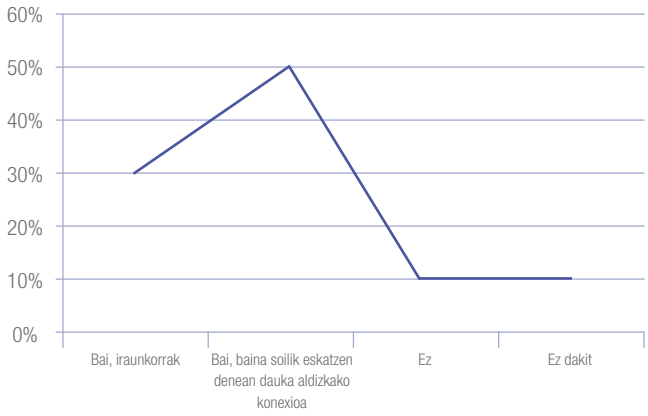
Internetetik sarbidea duten kontrol industrialeko sistemak egoteak, horiek daukaten segurtasun maila eskasak, eta kontrolatzen dituzten prozesuei lotutako kritikotasun maila altuak onartezin eta jasanezin bihurtzen dute arriskua erakunde industrialentzat.

Zure sare industrialak sarbideak ditu urrunetik?

Erakundeek beren prozesuak aurrera eramateko behar duten gaitasun teknologiko askirik ez dutenean, ingurune industrialen espezializazio maila altuak eskaera teknologiko horri erantzuteko gaitasuna daukaten hornitzaileak eskatzen ditu. Horregatik, instalazioak, sistemak edo ekipamendua abian jarri ondoren, laguntza behar da etorkizuneko beharrei aurre egiteko, bai gertakariek edo bai eskaerek eragindakoak. Ahal den heinean, urrunetik eman daiteke zerbitzu hori, eta horrek merkatu egiten ditu teknikari adituen bidaiengatik sortutako kostuak.

Jarduera askok eskatzen dute IT, OT eta bestelako hornitzaileen aldetik gainbegiratze iraunkorra –24 ordu, 365 egun– produkzio, laguntza eta mantentze maila altuko gailuetan. Hiperkonektatuta dagoen mundu batean, 4.0 industria sareetatik oso mendekoa den industria da dagoeneko.

Sare industrialak sarbideak ditu urrunetik sistemen gainbegiraketa edota kontrola ahalbidetzeko?



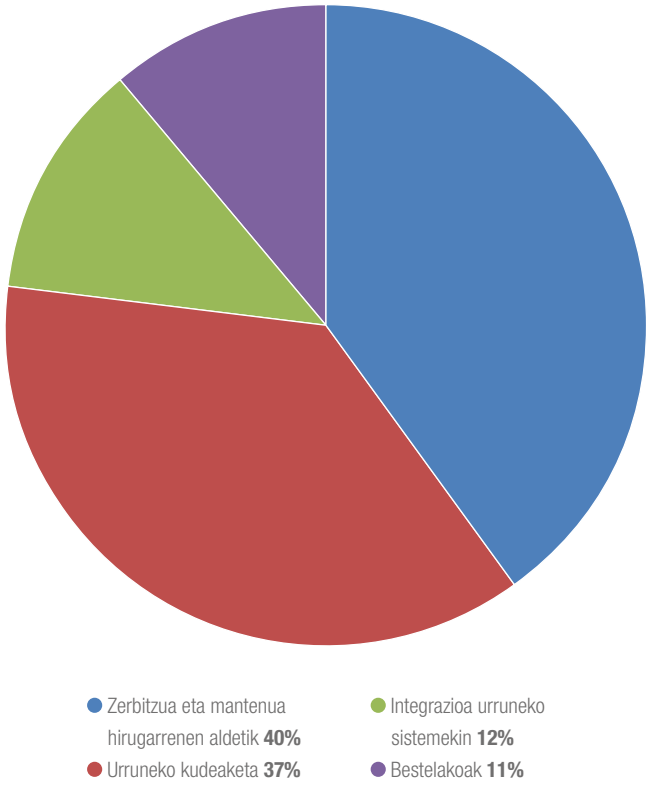
15. grafikoa – Urruneko sarbidea

Aurreko galderan baiezko erantzuna eman bada, zein da arrazoia?

Aztertutako enpresetako kontrol industrialen sistemetara urruneko sarbidea ezartzeko arrazoi nagusia horiek kudeatu ahal izatea da; hala adierazten du inkestatuen ehuneko altu batek (%77). Horietatik %37 sare industrialera sartzen da hirugarren eragile batzuek urrunetik laguntza eta mantenu lanak egin ahal izan ditzaten. Egoera honek erakundeen arriskua areagotu egiten du. Hornitzaile horiek instalazioetarako konexioa behar dute kontratatu zaizkien lanak egin ahal izateko. Beraz, beste aukerarik ez dagoen heinean, ekipoetara sarbidea eman beharko diegu gure kontrolik gabe, haien erabilpen, egoera eta segurtasun mailaren inolako ezagutzarik gabe. Gainera, egoera hori larriagotu egiten da sarbidea lokala denean, ingurune berean konektibitatea lortzen baita, segurtasun perimetraleko inolako elementutik pasatu gabe. Hori aski arrazoi izan beharko litzateke ingurune industrialean zerbitzuak ematen dituzten hirugarren enpresei zibersegurtasun baldintzak exijitzeko.

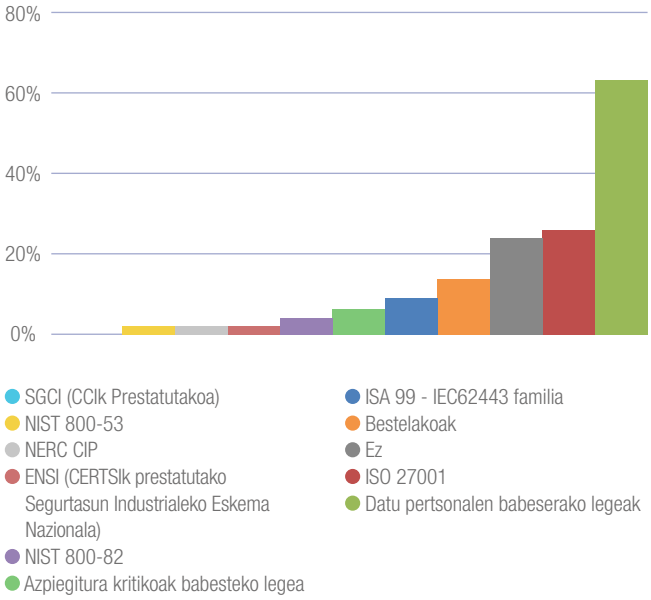
[4] https://www.shodan.io/ Shodan da Internetera konektatuta dauden gailuen munduko lehen bilaketa motorra.
https://censys.io/
https://www.zoomeye.org/

Sare industrialak zergatik dauzka urruneko sarbideak?



16. grafikoa – Urruneko sarbidea erabiltzeko arrazoiak.

Eremu industrialean arau eta estandarrak erabiltzen ari zarete?



17. grafikoa – Segurtasun Zibernetiko Industrialean erabilitako arauak.

ARAU ETA EREDUEN ERABILERA

Zer arau erabiltzen dira zure enpresaren Zibersegurtasun Industrialaren eremuan?

Enpresa gehienek enpresaren Zibersegurtasun Industriala ezartzeko arauak erabiltzen dituzte, baina kopuru garrantzitsu batek dio ez dituela erabiltzen (%23).

Grafikoan ikus daitekeenez, lekurik nagusia Datu Pertsonalen Babeserako Legeak (%64), ISO 27001 familiak (%25), eta ondoren IEC 62443 familiak (lehen ISA-99) eta Azpiegitura Kritikoen Babeserako Legearen ezarpenak hartzen dute. Datu horrek erakusten duenez, operazio inguruneetan arauak aplikatzen ari diren arren, ez da modu egokian egiten ari. Izan ere, oro har, operazio sistemek ez lituzkete izaera pertsonal edo konfidentzialeko datuak gorde behar.

Zibersegurtasun Industrialaren eremuari soilik dagozkionen artean CCIren SGCI gida eta sektoreko arautegiak daude, NERC CIP esate baterako, energia elektrikoko sistemen azpiegitura kritikoen babesari zuzendua. Nabarmen nagusiak dira datu pertsonalen babesari buruzkoak, %60 baino gehiagorekin, eta ISO 27001, %20arekin. Horrek erakusten du euskal erakunde industrialak ahaleginak zentratzen ari direla informazio sistemen babesean eta, aldiz, oso neurri txikian ari direla operazio sistemetan zentratzen. Azken kasu hori batez ere ematen da erakundeak azpiegitura kritikoen operadoreak ere baldin badira eta legez behartuta badaude.

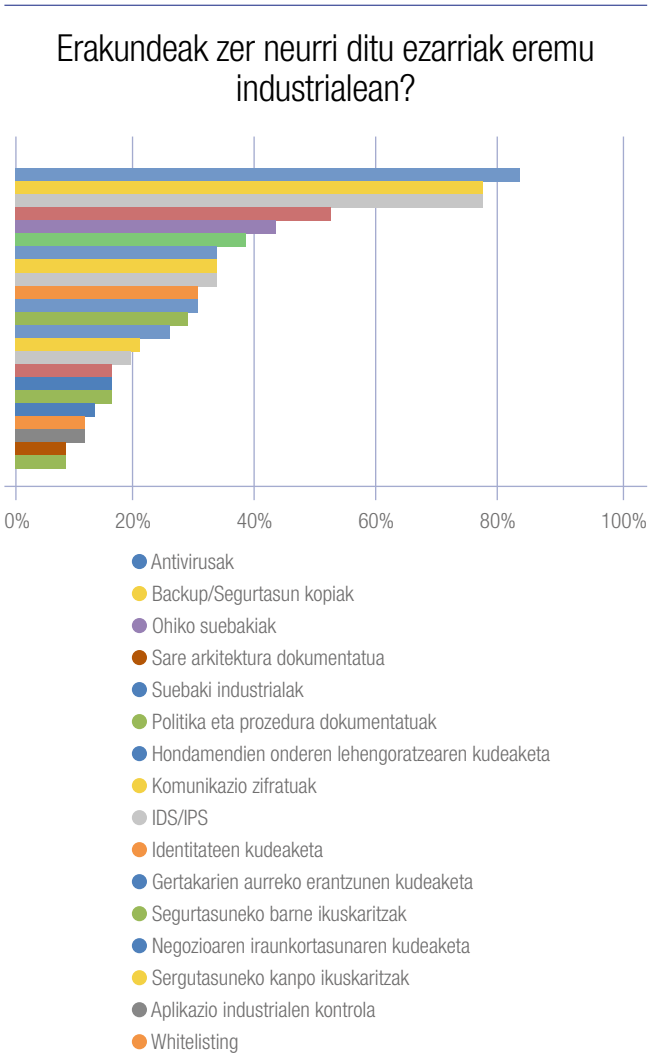
ZIBERSEGURTASUN INDUSTRIALARI BURUZKO NEURRIAK

Segurtasun Industrialari buruzko zer neurri jarri ditu dagoeneko abian zure enpresak?

Aztertutako ia enpresa guztiek diotenez, Zibersegurtasun Industrialeko neurriren bat ezarrita daukate. Neurri teknikoen artetik ohikoenak ondokoak dira (eragin maila handienetik txikienerako

ordenan): babes kopia automatizatuen soluzioak, antibirusak, backup edo segurtasun kopiak eta ohiko suebakiak; kudeaketa neurrien artean, berriz, dokumentatutako sareko arkitekturaren mantenua nabarmendu daiteke.

Era berean, leku garrantzitsua daukate suebaki industrialek eta politiken eta prozeduren definizioak.



18. grafikoa – Segurtasun Zibernetiko Industrialean erabilitako neurriak.

Gaur egun sare eta sistema industrialetan ezarritako hainbat zibersegurtasun neurri daude, baina guztiek ez daukate eraginkortasun maila berdina. Batzuk ingurune horietan aplikatzen dira irizpide egokirik gabe, hau da, IT inguruneetatik datoz baina OTetarako gaitasunik ez daukate. Esate baterako, ingurune industrialek duten trafikoak ezaugarri bereziak ditu, batez ere protokoloei dagokienez, horietako asko aplikazioaren eremuari soilik dagozkionak; edo portaera eredu jakin batzuen sorkuntza, trafikoa iragazten duen gailu bakoitzari mugatuak (komunikatzeko gaitasuna duten beste gailu batzuekin alderatuta, informazio mugatua trukatuz, eta lehenetsitako baimenekin, beste aldagai batzuen artean). Era horretara tresnak egokitu egiten dira eta indartsuago eta eraginkorrago egiten dira, beren lana OT inguruneetan garatzeko.

Pixkanaka, zibersegurtasun industrialaren arduradunen kontzientziazio eta informazio maila handiagoek lagundu egiten dute IT alorretik datozen gailuen inplementazio kopuruak jaits daitezen, OT inguruneetarako bereziki diseinatuak izan direnen mesedetan. Horrek eskatzen du IT soluzioak egokitzea industriaren behar eta berezitasunei. Horixe da, hain zuzen, suebakien kasua; grafikoan pixkanaka presentzia handiagoa hartzen joango dira, IT inguruneetarako diseinatutakoek protagonismoa galtzen duten arte.

04.

Zibersegurtasun Industrialaren merkatua

04.

ZIBERSEGURTASUN INDUSTRIALEKO JARDUERA BERRIEN AURREIKUSPENA

PROIEKTU BERRIETARAKO BALDINTZAK

ZIBERSEGURTASUN INDUSTRIALEKO PROIEKTUEN KONTRATAZIOA

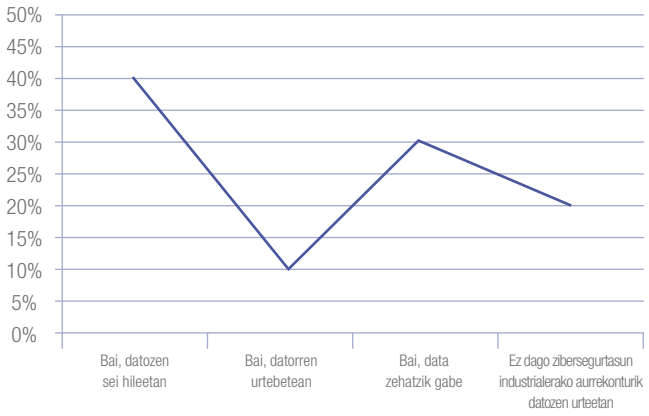
ZIURTAGIRI PROFESIONALAK

ZIBERSEGURTASUN INDUSTRIALEKO JARDUERA BERRIEN AURREIKUSPENA

Aurreikusita daukazue jarduera berriak abiatzea Zibersegurtasun Industrialaren alorrean?

Aztertutako enpresen %80 erabakigarri batek Zibersegurtasun Industrialaren alorreko jarduerak abiatzea aurreikusten du, eta horien artetik %10ak datorren urtean egingo du. %40a datozen sei hilabeteetan inplementatzeko fasean dago dagoeneko, eta hortaz, aurrekontu berezia esleitua du. Aztertutako enpresen %20ak soilik ez du oraindik aurreikusten Zibersegurtasun Industrialeko ekintzarik beren aurrekontuetan.

Aurreikusita daukazu jarduera berriak abaitzea Zibersegurtasun Industrialaren eremuan?



19. grafikoa – Zibersegurtasun Industrialeko jarduera berrien aurreikuspena.

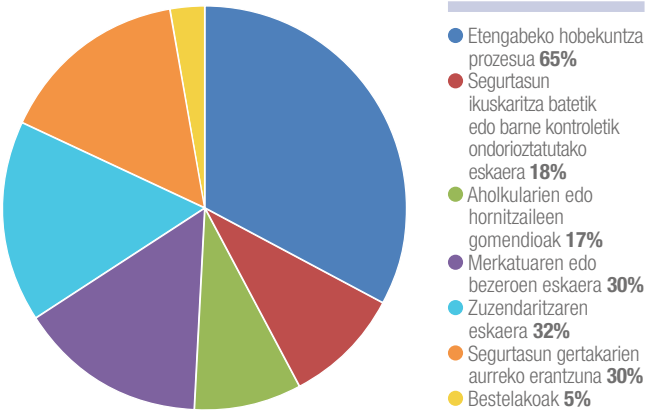
Berehalako eskaeratik ondorioztatzen den lehen ondorioa eskaintza zabalago baten premia da, bai hornitzaile kopuruari dagokionez, bai sektore eta bezero bakoitzaren beharretara egokitutako produktu eta zerbitzuen aniztasunari dagokionez. Zentzu horretan, 2016tik Zibersegurtasun Industrialaren Zentroak zibersegurtasun industrialeko zerbitzu eta soluzioen hornitzaileen katalogo bat argitaratzen du[5], eremu horretan hornitzaileen industria ezaugarritzen duena. Hortaz, ezinbestekoa da erakundeen barnean zibersegurtasun industrialaren alorrean aurrera eramaten diren ekintza guztiak 'Zibersegurtasun Industrialaren Arduraduna' izeneko barne arduradunak lideratzea, kontrolatzea, kudeatzea eta gainbegiratzea.

Oraindik altua da arduradun hori izendatu ez duten erakundeen kopurua. Hortaz, ekintza horiek, azken finean, ez daukate erakundearen barnean pertsona gaitu baten –prestakuntza, aurrekontu eta erabaki agintaritzari dagokionez– inplikazioa eta babesa.

Prestakuntzari dagokionez, profesional askorentzat aukera handi bat da hau, beraientzat eskaera iturri bat sortzea suposatzen duelako. Profesionalek beren lanbideak dibertsifikatu edo birmolda ditzakete, eta horretarako trebakuntza eta prestakuntza beharko dituzte; horrek ere hezkuntza merkatu berezia garatzen lagunduko du. Helburu bikoitza beharko da horretan: batetik, kalitatezko prestakuntza profesionala eskaini beharko da ikuspuntu praktikotik, eta bestetik, profesionalek eta beren erakundeek behar duten malgutasunarekin antolatu beharko da. CCIk 2018ko urte honetan abian jarri du Zibersegurtasun Industrialeko Lanbide Eskola[6], eta hori gehitu egiten zaio lehenagotik abian jarritako beste ekimen batzuei, esate baterako, Mondragon Unibertsitateko Zibersegurtasun Masterra, Arabako Ingeniari Industrialen Elkargo Ofizialaren dibulgazio jardunaldiak, eta Indussec 2018, IndustriSec 2018, Basque Cybersecurity Day edo BIMH bezalako topaketak.

Zibersegurtasun Industrialaren arloan proiektuak exekutatzeko eta konponbideak ezartzeko motibazioak zein dira?

Industriaren eremuan proiektuak exekutatzeko eta zibersegurtasun konponbideak ezartzeko motibazioak zein dira?



20. grafikoa – Zibersegurtasun Industrialeko Proiektuak exekutatzeko motibazioa.

[5] https://www.cci-es.org/catalogo

[6] https://www.cci-es.org/escuela Escuela Profesional de Ciberseguridad Industrial del Centro de Ciberseguridad Industrial

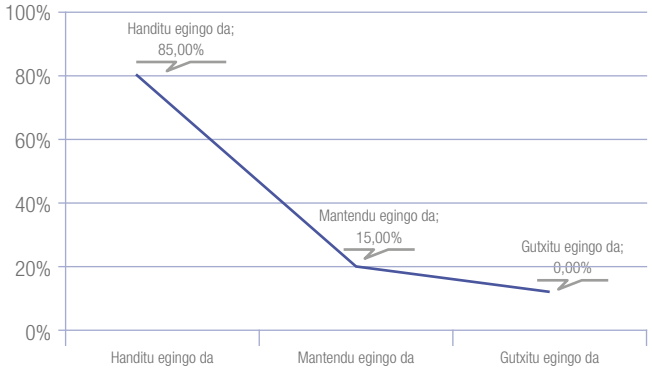
Inkestatutako enpresek ezberdintasunak erakusten dituzte zibersegurtasun industrialeko neurriak ezartzerakoan dituzten motibazioei dagokienez. Motibaziorik nagusiena hobekuntza iraunkorra da, %65arekin. Koherentea da gaur eguneko agertokiarekin, non prozesu industrialek dituzten mehatxuak aldatzen ari diren osagai teknologiak sartzen ari direlako; esate baterako, informazioaren teknologia, onura bat badakarrena, baina arriskua ere bai. Eta azken horren aurrean industriak ez daude prestaturik.

Arrazoi horri berari loturik, %30ak aitortzen du zibersegurtasuneko gertakarien aurrean jartzen dituela neurriak abian, berriz ere ezinbesteko metodo bezala ingurune berrira egokitzeko. Adierazgarria da testuinguru horretan beste faktore garrantzitsu batzuek daukaten presentzia handia, esate baterako Zuzendaritzaren eskaerak edo merkatuaren beharrak. Honek erakusten du arrisku honen kudeaketan heldutasuna hazi egin dela, eta horrek merkatuari eta enpresei eskatzen die aitortzea Zibersegurtasun Industrialaren arloan eskaera badagoela eta konponbide bereziak ezarri behar direla.

Zure ustez datozen urteetan Zibersegurtasun Industrialaren gaian zein izango da finantza inbertsioen joera zure enpresan?

Aztertutako enpresen multzo handi batek (%85) uste du Zibersegurtasun Industrialean egiten den inbertsioa hazi egingo dela, %15ak uste du mantendu egingo dela eta inork ez du esan jaitsiko dela.

Zure ustez datozen urteetan Zibersegurtasun Industrialaren gaian giza baliabideen inbertsionari eta aurrekontuari dagokionez zein izango da joera, 4.0 Industrian aplikatuko dena barne?



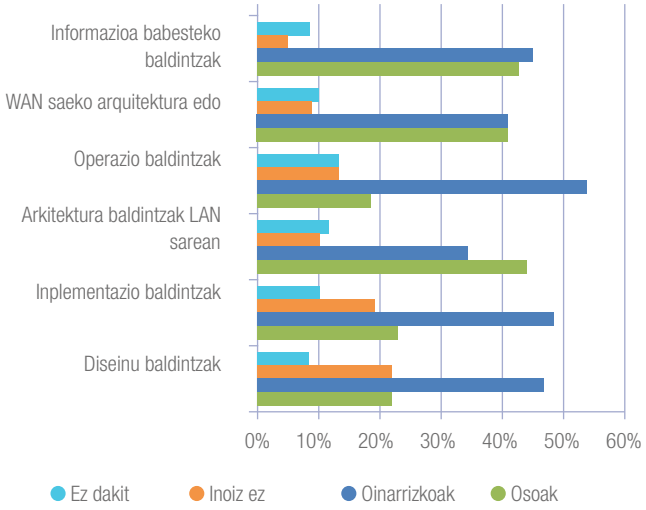
21. grafikoa – Inbertsioen joera Zibersegurtasun Industrialaren arloan.

PROIEKTU BERRIETARAKO BALDINTZAK

Enpresaren proiektu berrietan Zibersegurtasun Industrialeko baldintzak jasotzen dira?

Aztertutako enpresa industrial gehienek Zibersegurtasun Industrialeko oinarrizko baldintzak edo baldintza guztiak jasotzen dituzte beren proiektu berrien alderdi guztietan. Nolanahi ere, oso kezkagarria da enpresen %22ak horrelakorik oraindik ez kontuan hartzea. Zalantzarik gabe, agertoki hori eboluzionatuz joango da automatizazio teknologien garapen eta integrazio ekipoek Zibersegurtasun Industrialari buruz duten kontzientzia maila handituz doan heinean. Eta nola ez, zibersegurtasuneko gertakari batek alarmak piztu eta Zuzendaritzaren erabakiak eragiten dituen kasuetan. Orduan aurrekontuak zibersegurtasunaren ezarpenerako sail berezi bat izaten hasiko dira erakundearen proiektuen bizitza zikloko fase guztietan.

Proiektu berrietan edo duela gutxi garatutakoetan zibersegurtasun Industrialeko baldintzak jasotzen dira (esate baterako, 4.0 Industriara egokitzeari buruzkoetan)?



22. grafikoa – Zibersegurtasun Industrialaren baldintzak Proiektu berrietan.

ZIBERSEGURTASUN INDUSTRIALEKO PROIEKTUEN KONTRATAZIOA

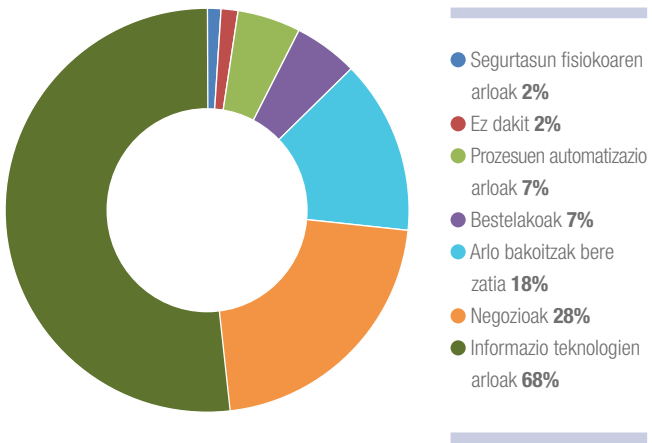
Zure enpresan automatizazio sareetarako Segurtasun Digitaleko proiektuen kontratazioari buruzko erabakia nork hartzen du?

Azterketaren arabera, zibersegurtasun Industrialeko kontratazioei buruzko erabaki gehienak ITen arloak hartzen ditu (%68), hain zuzen ere, eta lehen ikusi dugunagatik, zibersegurtasun industrialeko lanetan inplikazio eta parte hartze handiena duen arloa. Negozio arloak ere, %28arekin, parte hartzen du arlo honi buruzko erabakietan.

Soilik enpresen %7ak uzten du kontratazioari buruzko erabaki ahalmena prozesuen automatizazio arloaren esku, nahiz eta seguruenik bere langileen artean oraindik ezjakintasun handiagoa dagoen.

Beste %18 batek adierazten du kontratazio erabakiak hartzen dituela dagokion antolakuntza unitate bakoitzak (arlo bakoitzak bere zatia).

Zure erakundean zibersegurtasun proiektuen kontratazioari buruzko erabakia nork hartzen du?



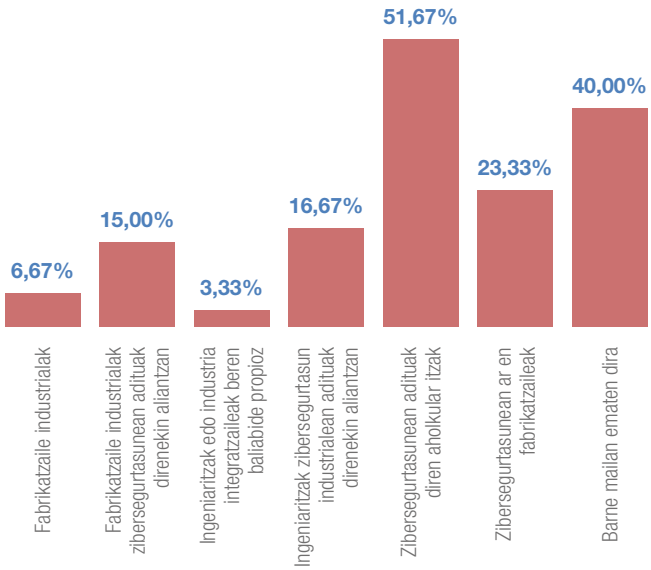
23. grafikoa – Kontratazio erabakiak.

Zein dira zure enpresaren automatizazio sareetarako Zibersegurtasun hornitzaileak?

Enpresa industrialetarako Zibersegurtasunaren hornitzaile diren enpresa motei dagokienez, azterketak erakusten du joera nabarmena dagoela zibersegurtasunean adituak diren enpresa aholkularien alde (%52). Nolanahi ere, garrantzitsua da zerbitzu horiek barne mailan ematen dituztela adierazten dutenen multzoa ere (%40), nahiz eta erabaki honen ondorioa profesional kualifikatuen falta izan daitekeen.

Ehuneko txikiagoarekin ageri dira zibersegurtasunaren fabrikatzaileak (%23), ingeniaritzak edo industria integratzaileak zibersegurtasun industrialean adituak direnekin aliantzan (%17), eta azkenik fabrikatzaile industrialak zibersegurtasunean adituak direnekin aliantzan (%15).

Zure erakundean zein dira zibersegurtasunaren hornitzaileak?



24. grafikoa – Segurtasun Zibernetiko Industrialaren hornitzaileak.

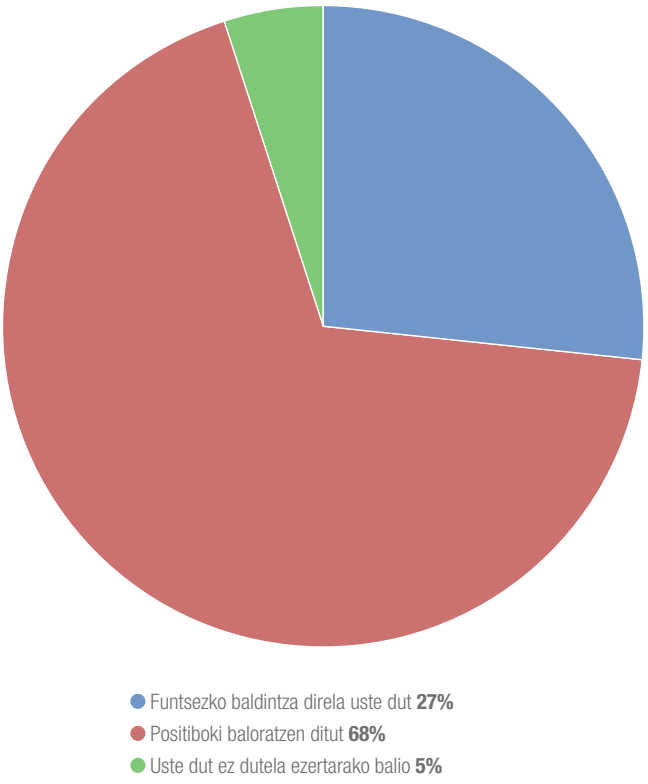
ZIURTAGIRI PROFESIONALAK

Nola baloratzen dituzu hornitzaile ekipoen ziurtagiri profesionalak Zibersegurtasun Industrialeko zerbitzuak kontratatzerakoan?

Zibersegurtasuneko proiektuak aurrera eramateko edo arlo horretako soluzioak ezartzeko ardura duten langileen prestakuntza da aldagairik erabakigarriena erakunde bakoitzaren beharretarako eta ezaugarrietarako egokienak diren neurriak hautatzeko eta abian jartzeko unean. Inkestatutako erakundeak horren jakitun dira, eta horregatik modu positiboan baloratu dute ziurtagiri profesionalak egotea Zibersegurtasun Industrialeko zerbitzuen hornitzaile diren enpresetako langileen artean. Emaitzen arabera balorazioa oso positiboa (%27) edo positiboa (%68) da, eta soilik enpresa horien artetik %5ak dio aipatutako ziurtagirien erabilgarritasuna edo balioa baxua dela.

CCIk uste du ziurtagiri profesionalak edo kredentzialak direla horien jabeak duen ezagutzaren, esperientziaren eta uneoro egunean egoteko kezkaren berme bat edo, behintzat, gutxieneko baldintza bat. Horrek ziurtagiri haiek baliozko irizpide bihurtzen ditu, langileen hautaketa prozesu guztietan aintzat hartu beharko liratekeenak, eta beraz, Zibersegurtasun Industrialeko zerbitzuak eskaintzen dituzten hornitzaileen hautaketa prozesuetan ere bai. Horregatik CCIk kredentzialen bere sistema propioa dauka[7], bai profesionalentzat eta bai ikasleentzat. Horren bitartez hainbat faktorerekiko konpromisoa sustatu nahi du: kalitate profesionala, prestakuntza, ezagutzak eta batzuen esperientzia eta beste batzuen bokazio goiztiarra. Proiektu honen helburua da, hain zuzen ere, ekosistema horretako profesionalen aitortza egitea, zibersegurtasun industrialean diharduten profesionalen aitortza hain zuzen, gai horrekin kezkatuta daudenak edo beren erakundeen barnean "ziberraren" ondorioekin kezkatutakoak, edo bere prestakuntzaren ardatz nagusi bezala gai hori dutenak, eta diziplina honen garapenarekin konpromiso bat erakusten dutenak.

Nola baloratzen dituzu hornitzaile ekipoaren ziurtagiri profesionalak alor honetako zerbitzuak kontratatzerakoan?



25. grafikoa – Ziurtagiriaren garrantziaren balorazioa.

[7] https://www.cci-es.org/credenciales

05.

Ondorioak

- Automatizazio eta kontrol sistemen arriskuaren kudeaketaren ardura nabarmen ari da hartzen informazio teknologien arloa, bere ekintzak ikuspuntu zibernetikotik planteatuz, fisikotik edo prozesuei lotutako ikuspuntu batetik baino gehiago. Horren arrazoia da arlo horiek daukaten heldutasun maila zibersegurtasunaren arloan, operazio industrialeko arlo teknikoek daukatenaren ondoan. Hau da, kasu gehienetan arazoari ikuspegi murriztu batetik heltzen zaio, oso ikuspegi informatikoa alegia, eta hortaz komenigarria litzakete ikuspegi orokorrago batetik ekitea, negozioaren arriskuaren kudeaketaren ikuspegitik hain zuzen.

- Beharrezkoa da erakundearen maila guztietan kontzientzia maila igotzea Zibersegurtasun Industrialaren beharrei eta berak dituen inplikazioei dagokienez. Jasotako datuetatik ondoriozta daitekeenez, instalazio industrialetan gertatutako zibergertakarietatik ondorioztatutako eraginak aitortu eta jakinarazterako mesfidantza dago. Eta hori egitea ezinbestekoa da erakundearen zuzendaritza eta negozioaren arloak arazoaren tamainaz jabe daitezen eta, horrela, hobetzeko beharrezkoak diren tresnak abian jar ditzaten (aurrekontua adibidez).

- Euskadiko industriaren digitalizazioa bizkortzen ari diren bi faktore nagusi identifikatzen dira ikerketan, eta horren ondorioz arrisku teknologikoa kudeatzeko beharra ere halaxe ari da bizkortzen, batez ere zibersegurtasunari lotutakoa. Lehenik, Europatik bultzatzen den arautze agertokia, esate baterako, azpiegitura kritikoen babesa edo, berriki, NIS zuzentaraua. Euskal enpresak beren jarduera dela-eta eraginda aurki daitezke, arautze agertoki horrek baldintzatu egiten baitu beren automatizazio eta kontrol industrialeko sistemei eragiten dieten arriskuek planteatzen dituzten erronkei aurre egiteko modua. Bigarrenik, globalizazioa bera. Horrek merkatu lehia handiagoa eragiten du, eta hori bereziki adierazgarria da azterketa honetan, inkesta euren borondatez betetzea erabaki duten erakundeen profila kontuan hartuta.

- Gainera, teknologia berriak barneratzen heldutasunik handiena duten sektoreen ekarpenak nabarmenak izan dira azterketan. Esperientzia horrek errazago egingo die 4.0 Industriara gerturatzeko prozesu naturala, eta horrekin batera, zibersegurtasun industrialera lotsa gutxiagoz hurbiltzea. Sektoreen arteko foroak edo enpresa anitzeko topaketak sustatzeak lagundu lezake heldutasun txikieneko erakundeak (edo nazioartekotze maila apalena dutenak) beren profilean aurrera egiten joan daitezen. Izan ere, nazioartekotu diren hemengo enpresa batzuen hornikuntza katearen zati dira bertako enpresa txikiak kasu askotan. Esperientzien trukea ekosistemarako oso onuragarria izan ohi da.

- Industriaren alorrean, merkatuak, enpresek eta zerbitzu hornitzaileek ekoizpen industrialaren inguruneetako zibersegurtasunean adituak diren profesionalak behar dituzte. Aztertutako euskal enpresen orokortasunari dagokionez, zibersegurtasunean prestatzeko ahaleginak nagusiki IT departamentuei esleitzen zaizkie oraindik ere. Egokia litzateke enpresako gainerako alorrak gaitzeko eta sentiberatzeko ahaleginak handituz joatea, batez ere kontrol sistemekin eta horien mantenuarekin dihardutenak.

- Prozesuen kontrol sareetan gehien erabiltzen diren zibersegurtasun teknologiak sare korporatiboetan ohikoenak direnak izaten jarraitzen dute, nahiz eta konponbide horiek ez diren beti egokienak ingurune industrialerako.

  Horregatik, ingurune horretarako bereziki prestatutako neurriak hartzea gomendatzen da, esate baterako: aplikazioen zerrenda zuriak (ingelesez *whitelisting*), suebaki industrialak, bide bakarreko pasabideak edo bidegabeko sarrerak prebenitzeko eta antzemateko sistemak (IDS) protokolo industrialak ezagutzeko ezaugarri bereziekin, besteak beste.

- Azterketak iradokitzen duenez, zibersegurtasuna barneratzeko arrazoi garrantzitsuenetako bat etengabeko hobekuntza izan da. Datu hori oso adierazgarria da. Izan ere, hortik ondorioztatzen da, gutxienez modu inplizituan, zibersegurtasuna ezartzea dela prozesuen kalitatean, eraginkortasunean eta segurtasunean hobekuntzak egiteko bide bat.

Azkenik, eta aurreko ondorio guztien testuinguru modura, azpimarratu beharra dago inkestatutako euskal erakundeen gehiengo adierazgarri batek (industria sektore guztietakoak) aurreikusia duela 2018an zehar Zibersegurtasun Industrialeko ekimenak abian jartzea. Horrek, ia guztiz seguru, gai honetara zuzendutako aurrekontuak haztea suposatuko du eta espero liteke, kuantifikatzea zaila bada ere, heldutasun maila orokorra handitzea.

glosarioa

› Zibersegurtasun Industriala	Erakunde eta azpiegitura industrialetan erabilitako informazioa kudeatu, prozesatu, gorde eta transmititzearen ondorioz sortzen den ziberespazioaren arriskua kudeatzeko diseinatu diren praktika, prozesu eta teknologien multzoa, pertsonen, prozesuen eta teknologien ikuspegiak baliatuz.
› IDS	Intrusión Detection Systems
› IDPS	Intrusion Detection and Prevention Systems
› IPS	Intrusion Prevention Systems
› IEC	International Electrotechnical Commission
› ISA	The International Society of Automation
› ISO	International Organization for Standardization
› IT	Information Technology
› NERC CIP	CIP Standards (Azpiegitura Kritikoen Babeserako Estandarrak)
› NIST	National Institute of Standards and Technology
› OT	Operation Technology
› SIEM	Security information and event management
› TO	Operazio Teknologia (Automatizazio Industriala)
› TI	Informazio Teknologia

Maiquez, 18 · 28009 MADRID
+34 910 910 751
info@CCI-es.org
www.CCI-es.org
blog.CCI-es.org
@info_CCI
www.linkedin.com/in/centrociberseguridadindustrial/

Arabako Parke Teknologikoa
+34 945 010 059
info@bcsc.eus
www.basquecybersecurity.eus
@basquecscentre
www.linkedin.com/company/basque-cybersecurity-centre/