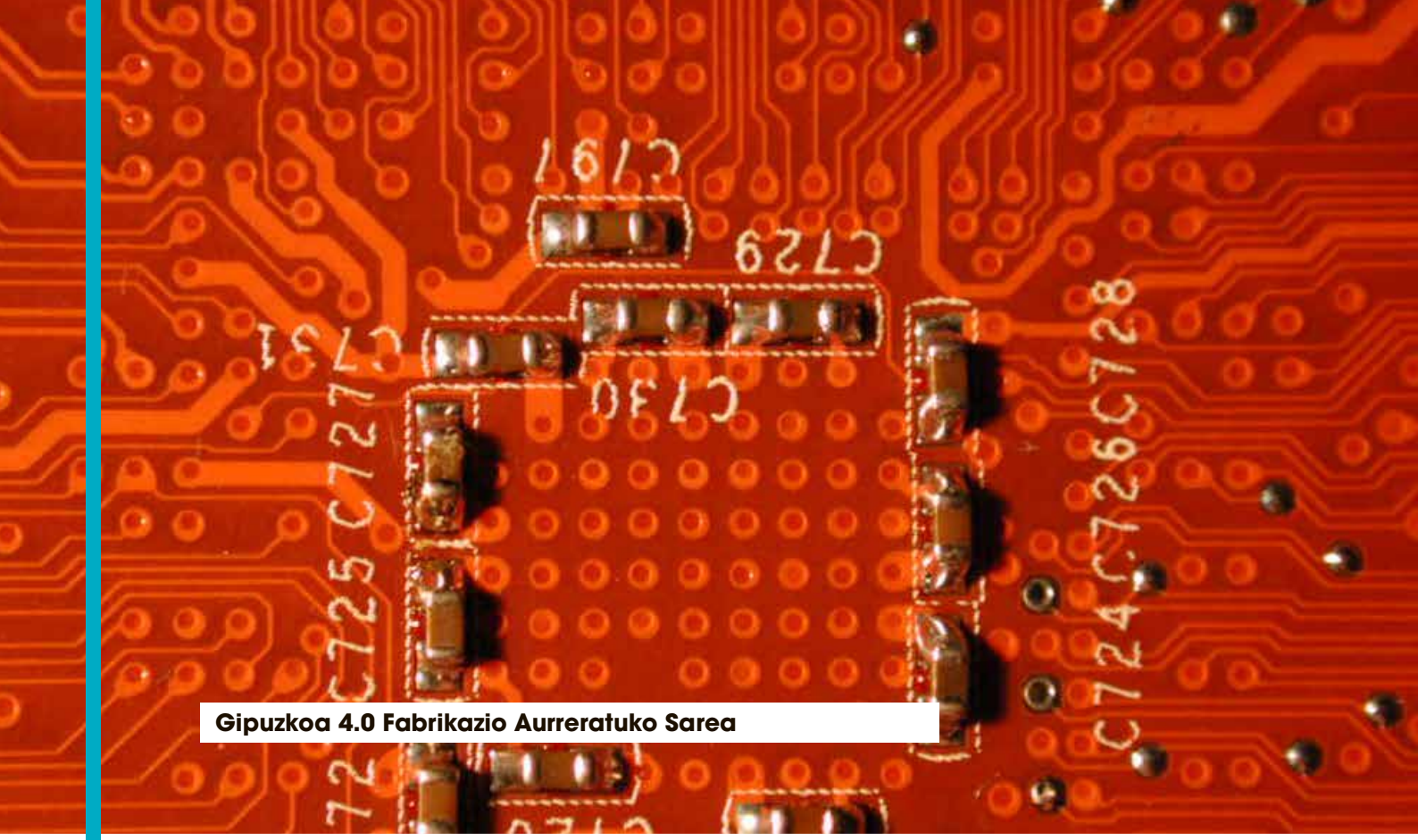


Gipuzkoa 4.0 Fabrikazio Aurreratuko Sarea

its
LINKED TO Egile

DMP Fabrika Zibersegurua

Enpresan txertatzeko aukerak eta gakoak

ORAININDUSTRI4.
Laugarren industria-iraultzarako prest

ORAIN
EKONOMIA

Gipuzkoako
Foru Aldundia
Diputación Foral
de Gipuzkoa

ORAIN
GIPUZKOA

Industria 4.0 kontzeptuen hedadura zuzenean erlazionatuta dago komunikatzeko eta interkonexiorako behar handiagorekin. Garapen horrek, aldi berean, kanpoko erasoen hazkunde kezkagarria ekarri du, baita pabiloi industrialetako produkzio guneetan zibersegurtasun egokiaren politika bat ezartzeko beharra ere. Hori dela-eta, zibersegurtasuna digitalizazio eta optimizazio prozesuetan jarduten duten enpresen agendetako nahitaezko elementu bat da.

Hain zuzen ere, horixe izan da DMPren (Egile Taldearen sektore aeronautikorako zehaztasun osagaien fabrikatzailea) kezketako bat. Enpresa honek behar industrial hori ITSren (zibersegurtasunean espezializatutako bere enpresa) gaitasunekin aprobetxatzea erabaki zuen Unit71 ekimena abian jartzeko: prozesu industrialak, beren problematika eta industriaren alderdi operazionalean azpiegitura eta sistema erabakigarriak babestu ahal izateko beharrezko babesgarriak ezagutzen dituen taldea da.

1

Apustuaren jatorria: Dibertsifikazioa Industria 4.0tik eta Industria 4.0rako

Egile Corporation XXI 2005ean sortu zen (gaur egun 300 pertsona inguruko plantilla du) eta Euskadiko dibertsifikazio korporatiboaren adibide arrakastatsu nagusienetako bat da. Konpetentzia nagusi gisa Muturreko Zehaztasunaren Mekanikatik eta izaera berritzaile eta ekintzaile indartsu batetik abiatuta (I+Gn egiten duen urteko inbertsio zifra konstanteetan islatua, bere diru-sarreren % 10etik gorakoa baita) erakundeen egitura bat eraikitzeko gai izan da balio handiko eta etorkizuneko proiekzioa duten nitxoetan sektore estrategikoetan. Hala, sektore horiek hauek dira besteak beste: aeronautika eta segurtasuna, osasuna, energia eta ura, zientziaren industria, ontzi metalikoa eta trokelgintza, baita izaera estrategikoa duten sostengu jarduera batzuk ere.

Sektore estrategikoak eta Egile Taldeko enpresak

Dibertsifikazioaren estrategia korporatiboaren esparru honetan eta ordura arte batik bat barne izaera izan duten zerbitzuen eskaintza batetik abiatuta, 2007an ITS Security enpresa sortu zen. Zibersegurtasuneko zerbitzuen kudeaketan espezializatutako integratzailea da eta bere zorroan hala auditoretzea, aholkularitza, egiaztapena eta integrazioa nola bestelako euskarri zerbitzu aurreratuak eskaintzen ditu, esaterako, zibersegurtasuneko plan integralak prestatzea edo zehaztea.

Mekanizazioko jarduera industrialetan zentratutako sare korporatibo batekin, batzuk bereziki kritikoak diren sektoreetan esaterako aeronatikaren kasuan, ITS bere ahaleginak Industria 4.0ren munduan zentratzen hasi zen, taldeko enpresei laguntza ematen zibersegurtasun industrialaren alderdi batzuetan.

Apustu horren eta etorkizuna izan dezakeen nitxo bat identifikatzearen ondorioz, **ITSk 2015 UNIT 71 jarri zuen martxan, zibersegurtasun industrialean aditua** den unitate bat; industriaren negozioak jarraitzea bermatzeko zerbitzuak eta irtenbideak eskaintzen ditu unitate horrek.

Unitatea martxan jartzearekin batera, DMPn (aeronautikaren alorrean zentratuen dagoen enpresa) erabaki zen ITS UNIT 71rekin batera bere fabrikaren zibersegurtasuna areagotu dezakeen proiektu estrategiko bati heltzea; izan ere, bere bezeroek kezka gero eta handiagoa dute gai horrekiko eta gaur egun elementu bereizlea da eta, epe laburrean, merkatuaren eskakizun bihurtzea espero dute. Proiektuaren azken helburua hirukoitza da:

- **Erabilgarritasuna areagotzea**, makinak orduak gal ditzala saihestuz, bai kanpoko erasoengatik edo barneko eragiketa txar batengatik.
- **Segurtasuna bermatzea**, era egokian biltegiratuz tailerrean sortutako informazioa eta ziurtatuz aldaketak soilik gauza ditzaketela baimen egokiak dituzten pertsonek.
- **Konfidentzialtasuna babestea**, hirugarrenek balio estrategiko handiko eta bereziki kritikoa den informaziorako, aireontzien osagaiez ari baikara, sarbidea izatea saihesten da.

Aurrerago zehatzago deskribatzen da proiektuaren irismena eta edukia.

2 Zibersegurtasun industrialaren gakoak: Gero eta beharrezkoagoa

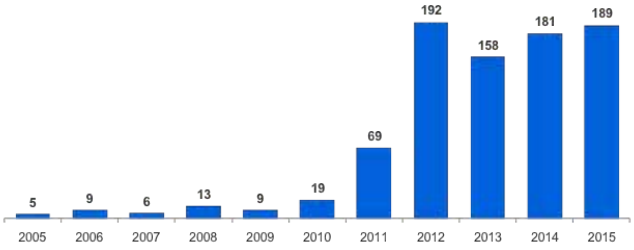
Industria 4.0 munduan kokatzen diren kontzeptu desberdinen baitan, zibersegurtasuna da ziurrenik enpresen aldetik arreta gutxien jasotzen ari den kontzeptuetako bat, nahiz eta horrek arriskua ekarri.

Industria 4.0 era intrintsekoan lotua dago interkonexioarekin eta informazio trukearekin, bai prozesu industrialaren baitan bai beste sistema korporatibo batzuekin edo Internetekin, enpresa baten jardueran gero eta integratuagoak dauden gailu ugariren bidez (ordenagailua, telefono mugikorrak, tabletak, inprimagailuak, etab.). Baina gero eta handiagoa den irekiera maila hori ez da arriskua areagotzen duen faktore bakarra; izan ere, besteak beste, alderdi hauek: osagaien edo softwareen estandarizazioak, WIFI sare ez-seguruek, informaziorako sarbidearen protokolo eskasek, USB gailuak era desegokian erabiltzeak edo gaizki konfiguratutako firewall-ek fabrikako informazioaren segurtasuna inoiz baino gehiago auzitan jartzen dute.

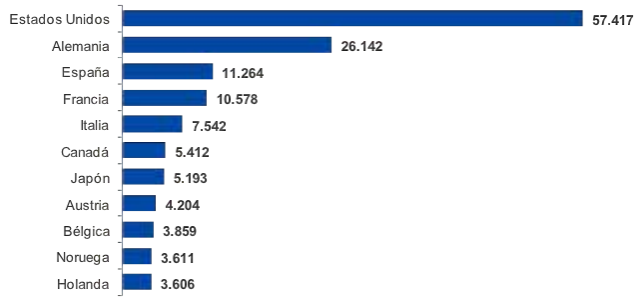
Faktore horien konbinazioaren ondorioz, **kontrol industrialaren sistemak (SCI) gero eta ahulagoak dira.** 2015ean, Kaspersky Lab enpresak egindako azterlan batek guztira 189 ahultasun identifikatu zituen horrelako sistemetan; beraz, hazkunde esponentziala izan du, 2010ean detektatutako 19 kasurekin erkatuz gero.

Ahultasun horiek gainera Internet bidez erraz eskura daitezkeen osagaietan daude. 2015ean egindako kontsulta batean, Shodan bilaketa motorrak (SCIren espezifikoa) eskainitako emaitzek 226.228 osagai identifikatu zituzten 170 herrialdetako 188.019 ostalaritan. Urrunetik sarbidea izateko zerbitzari gehienak Estatu Batuetan daude, ondoren Alemanian eta hirugarren lekuan dago Espainia.

Laburbilduz, **gero eta enpresa konektatu gehiago daude** eta, askotan, sare isolatu baterako egokiak diren segurtasun mailekin sortu diren osagai eta protokoloak dituzten instalazioak dituzte, baina ez dira egokiak sare konektatu baterako eta, horregatik, kanpoko erasoak (edo pertsona baimenduek praxi txarrak) izateko harrapakin errazak dira eta horrek ondorioak izaten ditu, hala nola, makinak gelditzea, informazioa lapurtzea edo inpaktu erlazionala, arazoak bezeroei ere eragiten badie.



Ahultasun kopuruen bilakaera SCIn urteka (iturria: Kaspersky Lab)

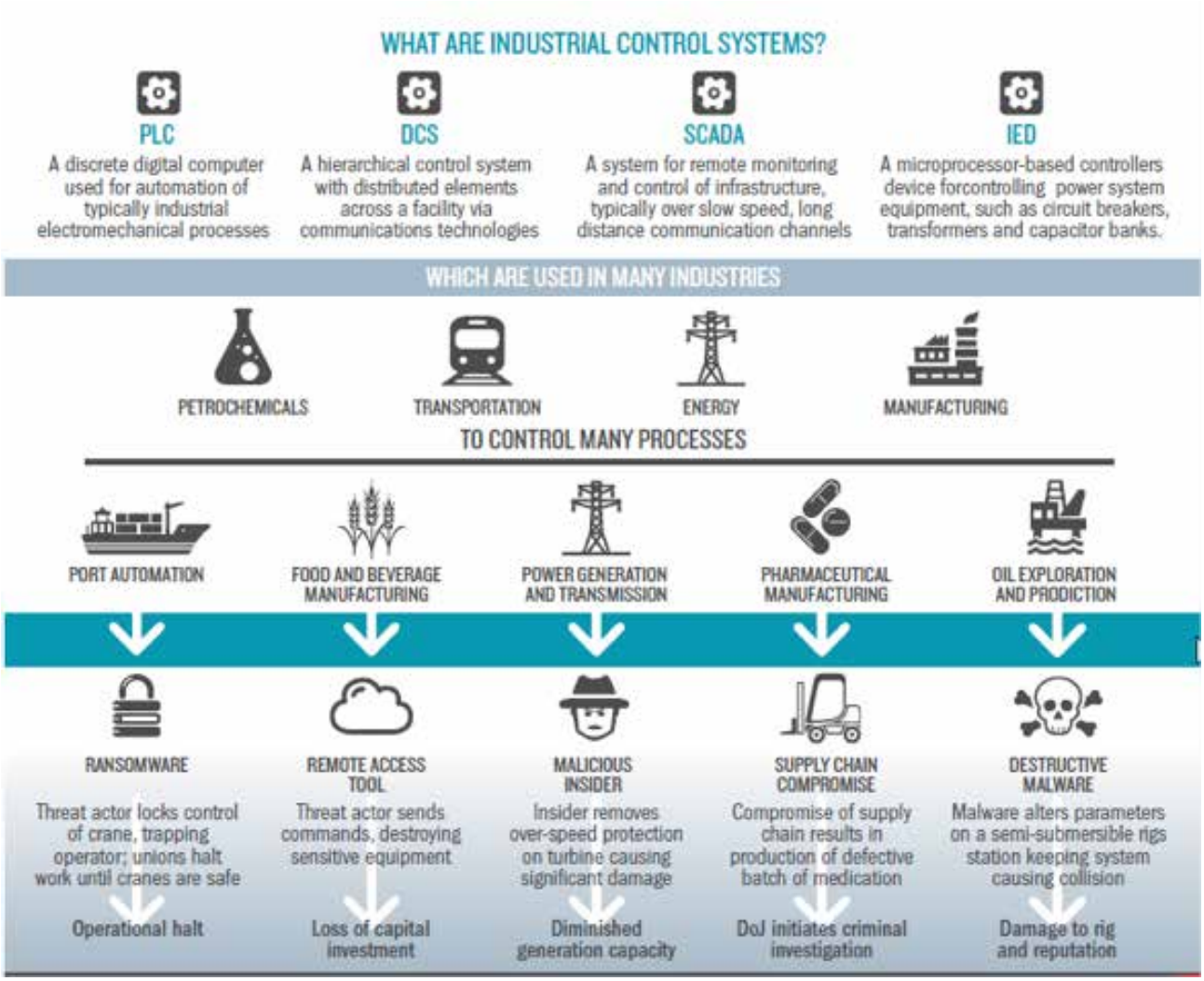


Urrunetik sarbidea izateko SCI 2015ean (iturria: Kaspersky Lab)

2015ean soilik SClekin inpaktu oso esanguratsuak izan dituzten gertakari zehatzen kasu ugari daude. Ukrainan, Prykarpattyaoblenergo enpresa energetikoari egindako eraso batek 80.000 pertsonatik gora elektrizitaterik gabe utzi zituen, 30 azpiestazio ingururen etengailuak deskonektatuz. Ura kudeatzen duen enpresa bateko (Kemuri Water Company izenordearekin ezagutzen da) beste gertakari batekin, arrotzek edateko ura tratatzeko erabiltzen diren konposatu kimikoak aldatu zituzten. Polonian, eraso batek lurrean utzi zituen Frederic Chopin Airport aireportuko 1.400 bidaiari baino gehiago. Alemanian, hacker talde batek altzairu fabrika bateko produkzio softwarearen kontrola hartu zuen eta kalte material esanguratsuak sortu zituzten instalazioetan.

Sektore aeronautikoaren kasu zehatzean, hor kokatuko genituzke ITS eta DMPren kasua, 2013an AIAAk (American Institute of Aeronautics and Astronautics) nabarmendu zuen zibersegurtasuneko esparru komun bat jarri behar zela martxan gobernu, airelinea, aireportu eta ekipamendu hornitzaileentzat. Hegazkin bakoitzak milaka osagai izanik, erabakigarria da fabrikatzaileek zibersegurtasuneko kontzeptuei heltzea.

"AEBk zibererasoen erronka gorakorrari aurre egin behar dio, gure arerioek gure sare elektrikoak, erakunde finantzarioak, aireko trafikoa kontrolatzeko sistemak sabotatzeko gaitasuna baitute helburu (...)"
Barack Obama, nazioaren egoerari (2013)



Eraso moten eta balizko inpaktuen adibideak (iturria: Booz Allen)

3 Irtenbidearen xehetasunak: Segurtasuna eta makinen gehieneko erabilgarritasuna

DMPk aeronautika, espazio eta defentsarako sektoreentzako dituen fabrikazio prozesuek kalibrazio eta zehaztasun handia behar dute; beraz, **segurtasuneko edozein hutsegite edo gertakarik atzerapena ekar dezake entregetan, kostu bat eragiketan, lehengaiak galtzea eta baita bezeroak galtzea ere.** Bereziki erabakigarria da, halaber, informazioaren, bai DMPrena bai bezeroek ematen dietena, konfidentzialtasuna. Hain zuzen, interesa sortu da bere lehiakideetako bati antzeko kasu bat gertatu zaiola ezagutu baita. Lehiakide horri ustez Txinan lokalizatutako hacker batek informazioa lapurtu zion.

Kezka hori izanik, DMPk, ITS UNIT 71rekin batera, 2015ean proiektu estrategiko bat jarri zuen abian bere prozesu industrialen zibersegurtasuna bermatzeko. Gutxi gorabehera 12 hilabetean, lan talde bat du eta, bertan, UNIT 71ko pertsonez gain, produkzioko zuzendariak eta produkzio lineako bi pertsonek hartzen dute parte, alderdirik funtzionalenean zibersegurtasuneko teknikariei laguntza emateko ardura dutenek, hain justu.

Proiektuaren etapak nahiko estandarrak dira:

- Hasierako egoeraren diagnostikoa, DMPren gaur egungo egoeraren "argazki" bat atereaz.
- Ekintza plana, detektatutako gaitasun eta beharretara bideratua.
- Eragiketaren erabilgarritasuna bermatzeko prozesu berriak eta teknologia ezartzea.
- Kontrolak, prozedura eta teknologia era egokian gauzatzen ari dela benetan balioestea.

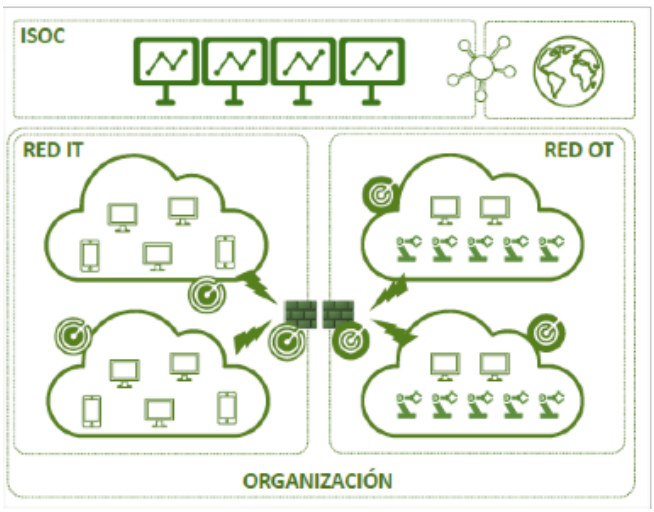
Proiektuaren jarduera fabrikaren sentsorizazioan zentratzen da Alerta Goiztiar eta Adimenaren Zerbitzuari (SATI) informazioa eskainiko dioten zunden bidez, **denbora errealean detektatzeko DMPren komunikazio sareetan dauden mehatxuak eta gertakariak,** aldi berean, ITS UNIT 71ren SOC (Security Operations Center) Industrialaren inguruan artikulatua.

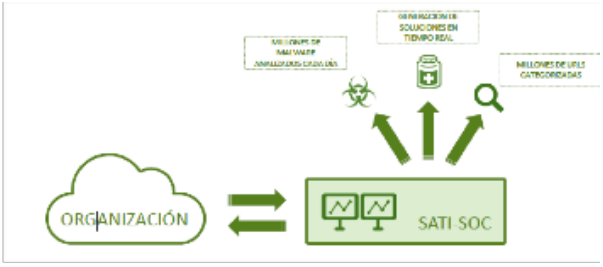
SATIk DMPren azpiegitura oraindik detektatzea erraza ez den har eta malware berrietatik babesten du. Gainera, munduko beste zentro batzuekin konektatua dago eta horri esker Interneteko sarearen ikuspegi global bat izan daiteke. Horrek malware familia, eraso kanpainak, eragileak, jarrera maltzurrak eta exploit-ak detektatzea errazten du.

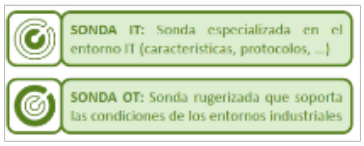
"Zibersegurtasuneko sistema bat airbag bat bezalakoa da, ez dakizu noiz salbatuko zaituen baina ez zenuke erosiko airbagik gabeko autorik"
Director I+D Grupo Egile

Monitorizazio eginkizunek diharduten bitartean, mehatxu adimentsuen plataforma, malware komunenen firmak sailkatzeaz gain, prozesu industrialen jarreretara bideratutako konpromiso adierazleez (intrusio bat adierazten dute) ere elikatzen da. Horrek kanpoko eta barneko mehatxuei buruzko ikuspegi bat eskaintzen du industriaren baitan eta DMPren kasu zehatzean.

Bestetik, mehatxu horiek produkzioaren erabilgarritasun adierazleetan eragin dezakete. Erlazio hori ere kontuan hartzen da proiektuaren barnean, gertakari baten benetako kostua ezagutzea erraztuz edo arintze erremintak inbertsioa itzultzea erraztuz; horrela, zibersegurtasunak negozioarekin bat egiten du.







Eragiketaren eskema

4 Beharrezko baliabideak: Ez-segurtasunaren kostua

Zibersegurtasuneko proiektu bati heltzea bestelako 4.0 teknologiak txertatzea baino errazagoa bada ere, zeren hein handi batean eremu honetako kanpoko aholkulari espezialista baten laguntza izan behar baita, badira kontuan izan beharreko zenbait barrera:

- **Inbertsio handia eskatzen du**, beti irismenaren araberakoa izango da baina, tamaina handiko enpresa baten kasuan, ehunka mila euro izan daitezke.

- **Zaila da inbertsioaren itzulkina kuantifikatzea**; hala, bestelako 4.0 teknologiek kostuak murriztu edo malgutasun handiagoa ekartzen badute ere, instalazio ez-seguru baten kostua ez da era zuzenean kuantifikatu eta balio ekarpenean egindako balorazioa enpresaren ikuspegi estrategikoaren mendekoa izango da.

- **Produkzio jardueran nolabaiteko eragozpena sortzen du**, zeren bere arrakasta bermatzeko, proiektuaren taldeak produkzio lineako pertsonak izan behar ditu eta, gainera, beharrezkoa izan daiteke makinetan aldaketak egitea.

Arrazoi horiek direla-eta, zibersegurtasunaren kasuan, bereziki erabakigarria da enpresako zuzendaritza zuzenean inplikatzea, proiektua erakundean etengabe babestu beharko baitu.

5 Ikasitako irakaspenak

DMP eta ITS UNIT 71en arteko elkarlan kasutik zenbait irakasgai interesgarri atera daitezke zibersegurtasuneko antzeko prozesu bati ekiteko interesa duten ETEentzat.

1. Zibersegurtasuna elementu bereizlea ere izan daiteke

Bezeroek gero eta gehiago baloratzen dute beren informazioaren eta prozesuen segurtasuna bermatuko duten hornitzaileak izatea. Berezi sektore aurreratuetan, esaterako aeronautikan, zibersegurtasuna gero eta gehiago hartzen da kontuan.

Horrelako proiektu bati aurre egiteak posizionamendu bat izan daiteke elementu bereizle gisa, eskakizun bat bihurtu baino lehen.

2. Prozesua enpresaren zuzendaritzak babestu behar du

Zibersegurtasunaren balioa objektibizatzeko zailtasunak (ez-segurtasunaren kostua) eta dauden barrerak direla-eta, bereziki erabakigarria da enpresako zuzendaritza zuzenean inplikatzea, proiektua erakundean etengabe babestu beharko baitu.

Hori da Egile Taldearen kasua, zeren apustu hau hala eskariaren aldetik egin baitu DMPn zibersegurtasuna txertatuz nola eskaintzaren aldetik, horrelako zerbitzuetan espezializatutako enpresa baten alde eginez, esaterako, ITS UNIT 71en alde.