1. Erronka proposatzen duten erakundeak

HABIC: ALCAD, BURDINOLA, DAISALUX, OJMAR

2. Erronka

Nola hobe dezakegu espazioen ekipamenduen industriako gailu adimendunen babes digitala eta konexioen zibersegurtasuna?

3. Balizko konponbide aplikagarriak

- Zibersegurtasuna: aktiboen segurtasuna eta ziber-adimena
- Software eta hardwarearen segurtasun-ingeniaritza
- Segurtasunaren kudeaketa eta *threat intelligence*

4. Testuingurua

Geroz eta gehiago dira eraikin eta instalazio "adimendunak", BMS (Building Management Systems) sistemen edo eraikinen kudeaketa-sistema adimendunen bidez kontrolatuak. **Eraikin horietan ezarritako teknologiek** (adimendunak ez diren beste batzuetan ipinitakoen antzera) balio handiko funtzionaltasunak ematen dituzte, eta horrek abantaila ugari eta efizientzia ematen dizkiete erabiltzaileei, baina **ziber-arrisku garrantzitsuak ere izan ditzakete**. Nagusiki, teknologia horiek hardware (sentsoreak, kontsolak...) eta software (nagusiki protokoloak dituzten programa informatikoak) artean banatzen dira. Alde horretatik, erronka proposatzen duten enpresak hardware-fabrikatzaileak dira nagusiki (softwarea ere diseinatzen duten arren), eta gailuak konektatzeko protokolo jabeak dituzte.

Aurreko guztiarekin, geroz eta **beharrezkoagoa da teknologia horiek modu seguru eta babestuan ezartzea** (eta, erronka proposatzen duten enpresen kasuan, larrialdietako argiak - Daisalux, laborategiko beira-arasak - Burdinola, telekomunikazio-plataformak - Alcad, sarraila adimendunak - Ojmar), eraso digitalek eragin ditzaketen erantzukizun fisiko eta zibernetikoko arriskuak ekiditeko. Teknologi horiek, batzuetan, konexioak izan ditzakete azpiegituretako barneko sareekin (zerbitzariak), adibidez ospitaleak, laborategiak eta beste instalazio kritiko batzuk, eta, beraz, hasierako helburu erakargarriak izan daitezke ziber-erasotzaileentzat.

Beraz, **espazioen ekipamenduen sektoreak eta bertako enpresek** arrisku jakinak dituzte euren sistema edo produktuak xede-eraikinetan integratzeko orduan. Alde horretatik, hau da arazo nagusia: **ekipamenduen (gailua eta kontrolagailua) eta azpiegituren (zerbitzariak) arteko komunikazio-protokoloen segurtasun eskasa**: segurtasun-neurri gehiago eta hobeak sartu beharko lituzkete, adibidez zifratzea edo autentifikatzea. Honako hauek dira sistema eta produktu horiek eraikinetan modu seguruan sartzeko beste arazo edo erronka batzuk: **sarearen eta muturretik muturrerako zibersegutasunaren**

gainbegiratze- eta bideragarritasun-falta, **eraikin osoan instalatutako Internet konexio desberdin eta anitzak, kontrol zentralizaturik gabe**, **partxeak kudeatzeko** praktika akastunak edo **seguruak ez diren urruneko sarbide-prozesuak.**

5. Azpierronkak eta helburuak

Errealitate horren aurrean, funtsezkoa da komunikazio-protokoloak diseinatzea eta horren eta konexiorako *gateways* direlakoen aurrean segurtasun-neurri egokiak hartzea. Halaber, urrats bat atzerago, garrantzitsua da dagokion ekipamendua maneiatzen duen sentsorikaren hardwarea kontrolatzen duen firmwarearen zibersegurtasuna ziurtatzea. Horretarako, eragiten dieten zenbait fase ikuskatu behar dira, adibidez erabiltzaileen kontrola, suebakien erabilera, VPN bidezko urruneko sarbideak, etab.

Protokolo-mailako segurtasun-neurriak ezartzeaz gain, oso garrantzitsua da aintzat hartzea sistemen babesari buruzko neurri orokorrak, adibidez hauek: pasahitzen politika, sare-segmentazio egokia, ekipoen gotortzea eta sistemak emandako informazioa kontrolatzea. Kasu honetan, aintzat hartuta erronka proposatzen duten enpresek "*in-house*" eraikitako protokolo jabeak dituztela eta aurretik azaldutako arazoetako batzuk dituztela, bi motako lankidetza-proiektuak ikusten dituzte startupekin:

1. **Analisi digital forentseak/Gailu/protokolo/konexioen zibersegurtasun-auditoretzak egitea:** arrisku-mapa bat sortzeko eta jarduketak lehenesteko, egungo egoeraren diagnostikotik sare-protokoloen sekurizazioaren diseinura arte (enkriptatzea), hautemandako *leaks*/*breachs* potentzialean aurrean. Honako proiektu hauetan ere bihur daitezke:
    - **Zibersegurtasun-eragiketen zentro bat finkatzea**, gorabeherak prebenitzeko, zuzenean monitorizatzeko eta mehatxuei erantzuteko.
    - **IDS/IPS sistemak*** (*Intrusor Detection Systems*), beste hardware-gailu batzuk edo software-aplikazio batzuk ezartzea, intrusio-sinadura ezagunak erabiltzeko sarrera eta irteerako sare-trafikoa hauteman eta aztertzeko, jarduera anormalen bila.
    - ***End to end* edo arintzeko zibersegurtasun-konponbideak** eskaintzea zerbitzua ukatzeko eraso banatuak (DDoS) ekiditeko, erabiltzaile legitimoek konektagarritasua galtzea ekiditeko eta zerbitzariak eta konexioak (Fire, Gate eta Cloud) zerbitzutik kanpo uztea ekiditeko.
    - **Sarbide eta komunikazioak autentifikatzea** sareko elementuen artean, modu zentralizatu edo banatuan, **kostu txikiko gailuen bidez.**
2. Bigarrenik, lotura izango luke instalazioen urruneko monitorizazio- eta mantentze-zerbitzuen hornikuntza seguruarekin eta sentsoreen manipulazioarekin, urruneko konexio babestuen bidez. Konexioaren gaineko segurtasuna ziurtatzeko (desberdina da bezeroaren arabera: txartel mugikorra, Wi-Fi sare paraleloa...) eta hardwareari zibersegurtasuna emateko (IoT), sistemaren filtraziora irekitako ateak murriztuz.

**Mota horretako zerbitzuen funtzionamendua ere baloratuko da kostu txikiko mikrokontrolagailu/prozesagailuetan, tokiko gailuaren, zentralaren eta kanpoaldearekiko komunikazio-pasabidearen mailan.*