ZIBERSEGURTASUNA

Zibersegurtasunaren liburu zuria

SARRERA

Digitalizazioak onura handiak ekartzen ditu garraioaren eraginkortasun operatiboan (erabilgarritasuna, edukiera, puntualtasuna eta mantentze-gaitasuna), baita bidaiarien esperientzia eta erosotasun hobea ere. Gainera, ezinbestean areagotzen du zibermehatxuekiko ahultasuna. Joera hauek mugikortasun-operadoreak eta publikoa aurrekaririk gabeko zibersegurtasun-arriskuen aurrean jartzen dituzte.

Arrisku horiekin, garraio-sistemaren Zerbitzuaren Kalitatea (QoS) kaltetu egin daiteke (garraio-sistemaren fidagarritasuna), bidaiarien segurtasuna eta, oro har, operadoreen ospearen kalteak. Zibermehatxuek bidaiarien ordenagailuetan eta mugikorretan ere eragina izan dezakete.

Zibersegurtasunaren ikuspegiak segurtasun-mehatxuen aurka babesteko behar den babes sakona eskaini behar du, garraio-operadoreak beren betebeharrak betetzeko prest daudela ziurtatuz.

Erronka gehigarri bat da gero eta informatika teknologia eta telekomunikazio estandar gehiago (TCP/IP, 4 & 5G, WiFi) integratzeko joera garraio-sistema ezinbesteko batean. Horrek garraio-sistemaren arkitektura-diseinuan eragina izateaz gain, mantentze-fasean ere izango du eragina sistemaren bizitza osoan zehar mehatxu berriak kontuan hartzeko.

CAF: EPE LUZERAKO BAZKIDE FIDAGARRIA SEGURTASUNERAKO ETA BEZEROEN ERAGINKORTASUN OPERATIBORAKO

Teknologia digitala (adimen artifiziala, IIoT, big data, telekomunikazioak, blockchain, etab.) eta COTS bezalako produktu estandarrak funtsezkoak izango dira mugikortasun-operadoreei euren erronka berriei aurre egiten laguntzeko, hau da:

- Zerbitzuaren kalitatea handitzeko (erabilgarritasuna, fidagarritasuna),
- Garraio sistemen ahalmena handitzea, inbertsio-maila gutxituz,
- Operazio-kostuak murriztea gero eta lehia irekiagoaren presiopean.

Bilakaera teknologiko handi hau garraio-sistemaren funtsezko ezaugarriak mantenduz eta segurtasunari arreta berezia jarriz gauzatu behar da.

CAF mugikortasunaren negozioan presente dago garraio-zorro zabal bati esker, besteak beste: 1) trenbidea, mugikortasun-sistemen ardatza direnak, 2) errepidea, autobusen negozioan Europako lider gisa. Balio-kateari dagokionez, CAFek finantzaketa, giltza eskuan proiektu globalak, material mugikorra, seinaleztapena, osagai eta zerbitzuetan ere presente dago, hala nola mantentze tradizionala edo prediktiboa bezalako jardueretan.

CAFen lehentasunezko helburua beti izan da sistema seguruak eskaintzea operadoreen eraginkortasun operatiboari dagokionez. Mehatxu berri hauei aurre eginez, CAFek hasiera batean erabaki zuen ekimen bat abian jartzea, CAFen barne-taldeen gaitasunen heldutasun-maila egokia izateko eta ziberseguratuta, bai trenbideentzako bai errepideetako operadoreentzako diseinuko produktuen eta sistemen zorroaren bidez.

CAF ZIBERSEGURTASUN GAITASUNA ETA ZORROA

Zibersegurtasunak eragina du telekomunikazioetan, produktuetan, zibersegurtasun arriskuen kudeaketan, segurtasunean, funtzionamenduaren segurtasunean, mantentze-lanetan garraio sistemen bizitza osoan zehar eta, azkenik, bezeroen eta hornitzaileen langileen sentsibilizazioan eta prestakuntzan. CAF zibersegurtasun programa hainbat ardatzetan egituratu da beharrezkoak diren alderdi guztiak estaltzeko, CAFeko bazkideak eta azpikontratatuak barne.

- Zibersegurtasun programaren ardatz nagusi bat CAFeko langile nagusien sentsibilizazioari eta prestakuntzari dago lotuta. Helburua ez da CAFen kultura-heldutasun maila bermatzea soilik, baizik eta bezeroei laguntza ematea proiektu baten fase guztietan, merkataritzatik hasi eta proiektuen entrega eta mantentze-lanetaraino.

- Bigarren ardatzeko helburu bat “diseinuaren bidez ziberseguratutako” soluzioen entrega ziurtatzea da. Estandar nazionalez gain, industriako estandarrak ondo finkatuta jarraitzeko erabakia hartu zen, hala nola IEC 62443 eta CENELEC TS-50701 trenbideetarako eta UNECE R155/156 autobusetarako.

  CAF zibersegurtasunak bezeroei laguntzen die garraio-sistemen inplementazio osoan eta hainbat hamarkadatako operazio faseetan, mantentze-lanak eta segurtasun-zaintza barne: sistemak hedatzeko fasean, bezeroen zibersegurtasun arrisku nagusiekin lankidetzan identifikatuz eta diseinuaren arintze egokia ezarriz CAFen “diseinu bidezko ziberseguratuta” produktuak erabiliz,

- Proiektuak emateaz gain, bezeroei laguntza eman beharra dago mehatxuei eta ahultasunen zaintzari eta kudeaketari esker, adabakien kudeaketari, Segurtasun Eragiketa Zentroari (SOC) etengabe kontrolatzeko eta segurtasun jarrera hobetzeko, prebenitu, detektatu, aztertu eta zibersegurtasuneko gertakariei erantzutea. CAFek jarduera horiek gauzatzeko tresnak garatzeko ibilbide-orri bat definitu du. Hurrengo pausoek lehen bidalketen esperientziaren itzulera hartuko dute kontuan eta bezeroen behar berriak aurreikusiko dituzte garraioaren industriaren heldutasun-hazkundearen ondorioz.

- Ardatz bat zibersegurtasunaren berrikuntzara dedikatzen da. Zibersegurtasuna CAFeko berrikuntza prozesu globalean sartu da. CAF zibersegurtasun-eskaintza teknologiaren abangoardian mantentzeak aukera emango die CAFeko bezeroei bidaiarien segurtasuna, garraio-sistemen operazio eraginkortasuna eta bidaiarien erosotasuna bermatzea.

Trenbideek ezinbesteko sistema gisa segurtasunez funtzionatzeko gai izango dira erasoak jasaten dituztenean, saihestu ezin den zerbait, zibersegurtasun diseinuaren kontzeptupean garatutako sistema kritikoak babestuz. Ez da zerbitzuen kalitatea edo bidaiarien ekipo elektronikoen erasoak edo galera ekonomikoak soilik, bidaiarien segurtasun kontua ere bada.

Praktika egokien eta zibersegurtasun estandarren ildotik, CAFek garraio-sistemen ezarpen, mantentze- eta segurtasun-zaintzako jardueretarako trebetasun egokiak dituzten eta ziberseguratuta dauden operadoreei laguntzeko konpromisoa hartu du.

GALDERAK ETA ERANTZUNAK

Garraio-industriak zibera-eraso asko jasaten al ditu?
Zibersegurtasun IT arloarekin alderatuta, garraio industriak eraso kopuru txiki samarra jasaten ari da. Hala ere, garraio sistemak berebiziko garrantzia duten sistemak dira. Ondorioak negargarriak izan daitezke eta operadorearen ospearentzat kaltegarriak izan daitezke. Erasotzaileei dagokienez, mehatxu iraunkor aurreratuak (APT) dira gure industriarako arriskutsuenak. Finantza baliabide garrantzitsuak dituzte eta estatuen kontrolpean. Ukrainako gerra bezalako azken gertakariek ziber-babesa indartzeko premiazkoa dela adierazi dute. Digitalizazioaren eta telekomunikazio estandarizatuen joerak eraso kopurua areagotuko du.

Zeintzuk dira operadoreen beharrak eta eskakizunak?
Zibersegurtasun-heldutasun maila oso desberdina da oraindik operadore batetik bestera. CAFek proiektu batzuk ditu eskakizun maila altua den herrialdeetan. Herrialde hauentzako gutxieneko produktuak eta sistemak “diseinuaren arabera ziberseguratuta” ematea da. Horrez gain, garraio-sistemaren bizitzan zehar, maiz eguneratzeak ezarri behar dira eboluzioko mehatxuei aurre egiteko.

Zein da zibersegurtasunaren eragina gidaririk gabeko sistemetan?
Gidaririk gabeko trenaren teknologia metroan erabiltzen da, baina bihar linea nagusietan, autobusetan, tranbietan integratuko da. Industriaren joera nagusia da garraio sistemen ahalmena eta zerbitzuaren kalitatea handitu beharra dagoelako. Arriskuen azterketarako eremu gehigarri baten beharra sortuko du. Hau da, gizakiak ez duela erabaki-prozesua kontrolatuko eta automatizazio-maila trenen/autobusen ontziko produktuen eta bide-bazterreko telekomunikazio estandarago batean oinarrituta egongo da.

Zein da zibersegurtasunaren eragina CAFeko proiektuen eguneroko jardueran?
Garrantzitsuena da zibersegurtasuna proiektuaren bizi-ziklo osoan integratzea eskakizunen azterketatik proiektuaren amaieran sistemaren ziurtagirira arte. Segurtasun jardueraren oso antzekoa da. Zibersegurtasunaren berezitasun nagusietako bat diseinu-fasean sistemaren mantentze-gaitasuna kontuan hartuko dela ziurtatzearen garrantzia da, zibersegurtasunak maiz adabakiak ekarriko baititu mehatxu berriak arintzeko.