EUSKO JAURLARITZA
GOBIERNO VASCO

51. zk.
2015eko martxoa

Aurrera!

Berrikuntzaren eta Teknologia Berrien dibulgaziozko aldizkaria

Bulego Teknologikoak argitaratua
Informatika eta Telekomunikazioetako Zuzendaritza

AURKIBIDEA

Teknologia Berriak gure bizitzan txertatzen ditugun heinean, lan egiteko modua ere aldatu egiten da. Izan ere, gaur egun, ezinezkoa iruditzen zaigu lan egitea posta elektronikorik gabe, gailu mugikorrik gabe... Aurrera buletin honetako lehen gaian, Informazioaren eta Komunikazioen Teknologiei eta lan-merkatuan sartzen ari diren gazteen belaunaldi berriei buruzko hausnarketa egingo dugu, eta horrek zer nola eragiten duen eta eragingo duen oraingo eta etorkizuneko lan egiteko moduan.

Badakigu Teknologia Berrien mundua etengabe berritzen ari dela, eta segurtasun informatikoaren mundua ez da salbuespen. Hori horrela izanik, informazio-sistemei eraso egiteko modu berriak sortzen dira egunetik egunera. Zibersegurtasunaren munduan, azken joera APT izeneko mehatxu edo eraso bideratuak dira (ingelesezko siglak dira eta «Mehatxu Iraunkor Aurreratuak» esan nahi du). Gai hori lantzeko idatzi dugun artikuluan mehatxu horien ezaugarri garrantzitsuenak zeintzuk diren azalduko dugu.

«Alboan» atalean Eustat izan dugu laguntzaile. Oraingoan, Erakunde Autonomoa inkesta elektronikoen estandarizazioa hobetzen aritu da azken urteotan, eta lan horren ondorioak aurkeztu dizkigute arduradunek; horri esker, galde-sorten softwarearen garapenarekin eta mantentze-lanarekin lotutako kostuak murriztu dituzte, baita galde-sorten kalitatea hobetu ere. Artikuluan ikusiko dugu nola egin duten.

Hegazkinean sartu eta aireratzera zoazelarik, ziur behin baino gehiagotan entzun izan duzula esaldi hau: «arren, itzali telefono mugikorrak». Bada, antza, EASA Aireko Segurtasunaren Europako Agintaritzak gure gailu elektronikoak itzali gabe bidaiatzeko aukera emango digu. «Berri laburrak» atalean aurkituko duzu informazio gehiago.

Atal horretako bigarren berria Software Libreari buruzkoa da. Izan ere, Ubuntu sistema eragilearekin funtzionatuko duen lehen telefono mugikorra atera dute merkatura. Horri buruzko xehetasun guztiak ezagutzeko, irakur ezazue prestatu dizuegun berria.

Lan egiteko modu berriak

Baliteke amaitzear egotea «bulego tradizionalen» garaia. Izan ere, gaur egun, enpresa berrietako langile askok ez dute bulegora egunero joan beharrik, ezta ordutegi zorrotzik bete beharrik ere, batik bat, Teknologia Berriei esker; izan ere, gailu mugikorrei esker nahi dugun tokian lan egiteko aukera baitugu.

HIZTEGIA

[1] **Telelana:** Eusko Jaurlaritzaren Telelaneko Proiektuari buruzko informazioa:

«*92/2012 DEKRETUA, maiatzaren 29koa, Euskal Autonomia Erkidegoko Administrazio Orokorreko eta bere erakunde autonomiadunetako enplegatu publikoek zerbitzua telelanaren bidez modalitate ez-presentzialean nola eman arautuko duen Akordioa onartzeko dena*»
(111. EHAA, 2012ko ekainaren 7koa)

Telelanari buruzko alderdi eta ezaugarri gehiago ezagutzeko, liburu hau kontsulta dezakezue: *El Libro Blanco del teletrabajo en España* (2012ko ekaina, Fundación Masfamilia)

www.teledislab.es/descargas/libroblancoteletrabajoespana.pdf

Teknologiaren zabalkundearekin jaio eta hazi dira, eta gaur egun eskutan hartuta bizi dira; 18 eta 33 urte bitarte dituzte. Internet eta sare sozialak baliatuta, informazioa lortzen dute, jakintza, zaletasunak eta iritziak partekatzen dituzte, eta kontsumitu ere kontsumitu egiten dute, edozein ordutan eta edozein tokitatik, **mugikortasunean**. «Izaki sozialak» dira, eta uneoro konektatuta bizi dira: ***millennial*** esaten zaie; edo bestela *Y belaunaldia* edo *Net Generation*. Hala, 2025. urtean, munduko lan-indarraren % 75 izango dira, Deloitte kontsultoretzak iragarri duenez.

Millennial hauek ezagutu duten munduan nonahi dago Internet; informazioa ez dute beste belaunaldiek bezala prozesatzen; noranzko biko komunikatzeko modu berria dute sare sozialei esker, asko parte hartzen dute eta digitalki adituak dira. Azken batean, teknologia eta konektibitatea ulertzeko/erabiltzeko modu berezia dute, eta lanean ere horixe bera aurkitzea edo erabili ahal izatea espero dute.

Deloitte kontsultoretzak txosten bat egin du *millennial* horien **Eskari eta espektatiba handiei** buruz: «*Lider bihurtzen ari dira jada teknologian eta beste industria batzuetan, eta pentsamendu berritzaileak eta trebetasunen garapena sustatzen dituzten erakundeetan, gizarteari ekarpen positiboa egiten dioten erakundeetan lan egin nahi dute*».

Belaunaldi horri entzutea aukera handia da eta industrian ez ezik, zerbitzu publikoetan ere eragina izan beharko luke erronka berriei aurre egiteko; izan ere, pertsona horiek idatziko baitute etorkizuna, baikorrak, energiaz beterik eta berritzaileak diren aldetik.

«*Millennial*ak munduko lan-indarraren % 75 izango dira 2025. urtean»

TEKNOLOGIA

Jakin badakigu lan-inguruneak aldatzen ari direla. IKTek, hodeiak, *smartphone*ek eta *tablet*ek bulegoaren hormak «eraitsi» dituzte: langune birtualak, langileak mugikortasunean, kideak toki berean ez dauden taldeak... Eta, bestalde, legezko betebeharrei jarraiki lan-segurtasuneko neurriak ezarri beharra eta enpresa-munduan kontzientziazio handiagoa eta prestasun handiagoa izatea lan-ingurune seguruei eta pertsona zoriontsuei dagokienez; horixe da talentuari eusteko politiken arauetako bat. Nola ez, **Administrazio Publikoak** ez dira joera horretan salbuespen, eta mota horietako gero eta proiektu gehiago daude: Telelaguntza, Telelana[1], herritarrekin elkarreragiteko *app*ak...

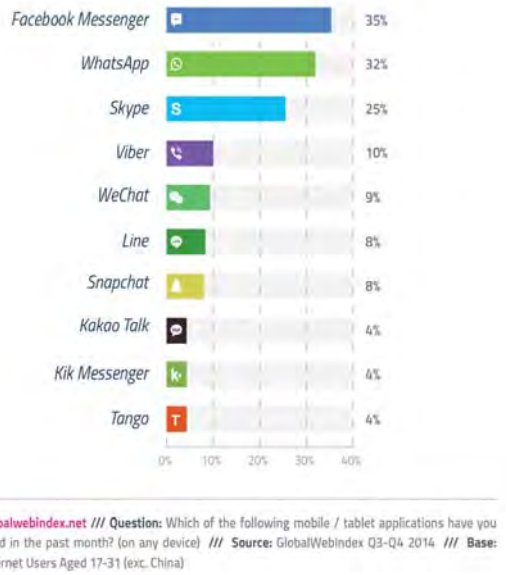
Randstad konpainiak talentuaren kudeaketari eta fidelizazioari buruzko txostena egin du, eta, azken txosten horren arabera, 40 urtetik beherako langileen kasuan, lan egiteko enpresa bat hautatzeko garaian gehien balioesten duten faktoreetako bat soldata da, baina baita **punta-**

puntako teknologien erabilera ere. Era berean, lan-giroa eta lana eta bizitza pribatua bateragarri egitea ere faktore erabakigarriak dira enpresa bat edo erakunde publiko bat hautatzeko garaian.

Azterlan horren arabera, *employer branding* esaten zaion horretan, lehentasunetako bat lana eta familia bateragarri egiteko erraztasunak ematea da. «*Langileak pozik egon behar du bere lanpostuan, eta ez du kezkarik izan behar, bizitza pribatuan eragin negatiborik izan ez dezan; izan ere, horrek guztiak zuzen-zuzenean eragiten baitu bere produktibitatean*», dio txostenak. Azken datu bat: aurten ere, Teknologiaren eta Elektronikaren sektoreetan lan egin nahi du jende gehienak.

Izan ere, langileak pozik egoteak, lantokiaz harro egoteak eragin positiboa baitu erakundearen produktibitatean. **Great Place To Work**en arabera, «*lan egiteko toki bikainek erakundearen helburuak betetzea lortzen dute inspirazioaren, komunikazioaren eta entzutearen bitartez. Langileek beren onen-onena ematen dute, baldin eta eskerrak ematen bazaizkie, garatzeko aukera eman eta zaindu egiten badira*».

***Millennial*ek erabiltzen dituzten mezularitza-sistemak**



globalwebindex.net /// **Question:** Which of the following mobile / tablet applications have you used in the past month? (on any device) /// **Source:** GlobalWebIndex Q3-Q4 2014 /// **Base:** Internet Users Aged 17-31 (exc. China)

Mundu globalizatu honetan, enpresek –publiko nahiz pribatu– ezin dute baliabide baliotsu eta urrienetako bat alferrik xahutu: **denbora**. Langileen eta lan-emaileen arteko harremanetan jarrera berriak bilatu behar dira, bi aldeentzat balioa sortzea ahalbidetzearren. Malgutasun horrek hamaika onura eragiten ditu, bai langilearentzat, bai elkarreragiten duten lantaldeentzat. Enpresak eta, nola ez, gizartea, oro har, ere onuradun izaten dira.

Eta ingurune teknologikoa eta demografikoa aldatzen bada, lan-harremanak ere egoera berrira egokitu beharko dira. Ekologia, dibertsitatea, nazioartekotzea, inklusioa, generoa, **mugikortasuna**, hiri adimendunak[2], informazioa,

«Lan egiteko moduari dagokionez, benetako kultura-aldaketa gertatzen ari da; aldaketa hori ez da teknologikoa, teknologiak ahalbidetutakoa baizik»

gardentasuna edo **teknologia;** kontzeptu horiek enpresari ere atxikitzen zaizkio iraunkortasunaren bitartez. Lan egiteko modu berri horietan sakontzea ezinbestekoa da hazkunde ekonomiko iraunkorra lortzeko —hau da, enplegu iraunkorra eta kalitatezkoa sorraraziko duen hazkundea lortzeko—.

Gaur egun, Interneti esker, pertsona guztiak daude konektatuta; *on-line*, alegia. Are gehiago, Teknologia Berriei esker enpresak kudea daitezke fisikoki bulegoan egon gabe.

*Millennial*ak, teknologia, konektibitatea, talentua, malgutasuna, bateragarritasuna, produktibitatea, efizientzia... Testuinguru horretan, beharrezkoa al da lan egiteko beste modu bat? Gauza bat argi dago: ez gaude jada duela zenbait urteko egoera berean. Aldatu egin da testuingurua, eta, gu aldatzen ez bagara eta, batik bat, gure pentsamoldea aldatzen ez badugu, «zaharkituta» geratuko gara. **New Way to Work** edo «lan egiteko modu berri» hori barneratu beharrean gaude, **mugikortasunean**, **malgutasunean** eta **efizientzian** oinarritzen den modu hori, *millennial*entzat ez ezik, «etorkin» digitalentzat ere onuragarri baita. Horrek guztiak onura ekarriko dio erakundeko langileei, enpresari berari eta, azken batean, oro har, gizarteari, baita bizitza erraztu ere.

Lan egiteko modu berri hori merkatua aztertzeko ekimen bihurtzen ari da jada; erakundeei «lantalde birtualen» inpaktua eta politika egokienak ulertzen laguntzeko diseinatuta dago, egungo munduarekin konprometitutako enpresa izatera iristeko.

HIZTEGIA

[2] **Hiri adimenduna**: ingelesezko *smart city* terminoaren itzulpena da.

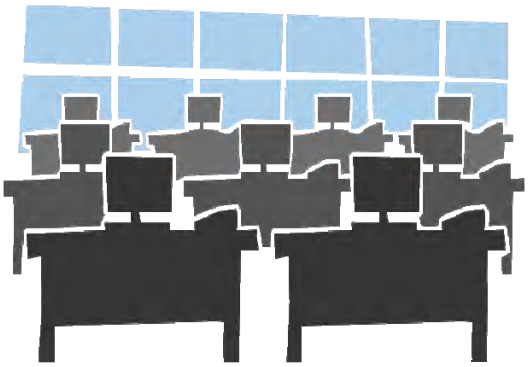
«Hiri adimenduna» edo «hiri eraginkorra» ere esaten zaio; hiri-garapen mota bat da, **iraunkortasunean** oinarritzen den garapena, eta gai da erakunde, enpresa eta biztanleen oinarrizko premiei behar bezala erantzuteko, bai alderdi ekonomikoan, bai alderdi operatibo, sozial eta ingurumenekoetan; bestela esateko, garapen ekonomikoa eta ingurumen-garapena jasangarria eta **iraunkorra** da, gobernantza **partizipatiboa** du, baliabide naturalen kudeaketa zuhurra eta burutsua egiten du, eta herritarren denbora egoki baliatzen du.

[Iturria: Wikipedia]

Informazio gehiago nahi izanez gero, irakurri *Datu masiboak (Big Data)* izeneko artikulua 44. Aurrera aldizkarian (2013ko ekaina).

www.euskadi.eus/informatika

Alabaina, **kultura- edo filosofia-aldaketa** horrek arrisku eta mehatxuak ere baditu, eta ebaluatu egin behar dira. Kanpotik begiratuta, adibidez, erakundeak gainditu beharreko mehatxu garrantzitsuena ingurunearen dinamika da, **aurrekontuetan murrizketak** egitea eskatzen baitu eta epe luzera baino gehiago, **epe motzera**



begiratzen baitu. Teknologian inbertitzeko beldurra dela-eta, egiturazko elementuetan inbertitu beharrean egoeraren araberako elementuetan inbertitzera iritsi daiteke. **Industriaren garaitik** jaso dugun herentzia ere mehatxu garbia da lan egiteko eta komunikatzeko modu berrientzat.

Hala ere, erakundeak hamaika aukera balia ditzake: hasteko, **IKTen efektu biderkatzailea** erakundearen jardueraren norainokoan. Enpresa lehiakideekiko bereiztea lehiakortasun-abantaila da enpresarentzat, eta errentagarritasunean edo negozio-bolumenaren gorakadan zuzenean eragiten du. Lege-araudien aldaketei aurrea hartzea eta aldaketetara egokitzea ere aukera handitzat hartzen da, erakundean zeharkako malgutasuna sortzen baitu. Esan gabe doa alderdi horiek guztiak Administrazio Publikoan bertan ere aplika daitezkeela, aurrekontua kontrolatzeko neurriak, iraunkortasunaren eta batera-garritasunaren alde egitea eta antzeko neurriak «arautzat» dituzten aldetik.

KOMUNIKAZIO BATERATUAK

Zalantzarik gabe, **teknologiak** katalizatzaile izan behar du, lan egiteko modu berri horretara iristen laguntzeko, arazorik gabe lan egin dezagun nahi dugun edo behar dugun tokitik. Horrekin batera, kultura aldatzen bada —erakunde horietan behar-beharrezkoa, arrakastaren gakoa baita—, koktel perfektua izango dugu aurre egiteko jendearen harreman pertsonaletan eta lan-harremanetan gertatzen ari denari.

Puntu horretara iritsita, galdera hau egin beharko genioke geure buruari: teknologiaren katalizatzaile-eginkizun hori nola bihur daiteke konponbide sortzen diren arazo berrien aurrean? Ikuspegi sinplifikatzaile batetik begiratuta, orokorrean «**Komunikazio Bateratuak**»[3] esaten zaion horren barruan egongo da bidea; izendapen hori gehiegi erabiltzen da, eta nahierara interpretatzen du fabrikatzaile bakoitzak. Dena den, laburbiltzeko, **funtzionalitate** gutxi batzuk erabiltzean datza:

- **Zenbaki bakarra eta gailu gogokoena**. Norbait lokalizatu nahi izan dugunean, zenbat aldiz deitu behar izan diogu lehenik telefono finkora, gero mugikorrera...? Egunean zenbat minutu galtzen ditugu norbait lokalizatzeko hainbat bide erabili behar ditugunean? Funtzionaltasun horri esker, erabiltzaile bakoitzak erabaki dezake nola nahi duen bera lokalizatzea, non dagoen gorabehera, baita komunikazioko zein gailutan ere. Gainerako erabiltzaileek zenbaki bakarra izan behar dute, eta gure bideratze-arauek egingo dute gainerako lana.

- **Presentzia**. Une bakoitzean lokalizatzeko zer erabilgarritasun-maila izan nahi dugun erabakitzeko gai izan behar dugu, ordutegiaren, gure jardueraren edo beste faktore batzuen arabera.
- **Postontzi bakarra**. Funtzionaltasun horri esker, postontzi bakarra izango dugu, eta gure

HIZTEGIA

[3] **Komunikazio Bateratuak:** informazio gehiago nahi izanez gero, irakurri *Komunikazio bateratuak* izeneko artikulua 46. Aurrera aldizkarian (2013ko abendua).

www.euskadi.eus/informatika

mezu guztiak bertan zentralizatuko dira; izan ere, ba al du zentzurik, adibidez, telefono finkoan ahots-postontzi bat eta mugikorrean beste bat izateak?

«Lana jada ez da toki edo ordutegi jakin bat, jarduera bat baizik»

- **Berehalako mezularitza**[4]. Ez dugu zertan beti ahots-dei bat egin norbaiti zerbait esateko. Agian, funtzionalitate horrek hobekien azaltzen duena zera da, nola hedatu diren bat-batean horrelako aplikazioak, dela eremu pertsonalean, dela enpresaren eremuan.
- **Aplikazio mugikorrak**. Erabateko mugikortasuna du mundu honek, eta «hiperkonektatuta» dago; hala, bulegoan egon edo beste nonbait egon, ezinbestekoa da tresna berdinak izatea, eta aplikazio mugikorrei esker kudea daiteke hori.
- **Web bidezko konferentziak eta lankidetza-tresnak**. Lantaldeak gero eta «birtualagoak» badira, pertsona bakoitza toki batean badago... funtsezkoa da talde horiek biltzeko tresnak izatea. Seguruenik, hori da elementu garrantzitsuenetako bat, eta xehetasunez aztertuko dugu; tresnari berari ez ezik, tresna erabiltzeko moduari ere erreparatuko diogu bereziki. Izan ere, hainbat **gomendio** eman ditzakegu tresna horiek eraginkortasunez erabiltzeko, jende askok teknologia horiek erabiltzeko garaian izaten duen frustraziorik izan ez dezagun:
  - Lankidetza-saioa (audio edo web bidez) baterako deialdia egitea, baina soilik behar-beharrezkoa denean; ez da ona gauza guztietarako horrelako saioak antolatzea. Batzuetan, mezu elektroniko bat bidaltzea edo dei bat egitea aski izaten da arazoa konpontzeko. Ondorioak: ez da ona bilera gehiegi egitea.
  - «Agenda Korporatiboa» edo antzeko tresna bat erabiltzea bileran parte hartu behar duten pertsona guztiek egutegian idatzita izateko (memoria ez da fidagarria). Zenbait funtzionalitate —hala nola **zenbaki bakarra** eta **presentzia-egoera**— funtsezkoak dira mugikortasunean lan egiten duten guztientzat.
  - Behar-beharrezkoak direnei eta ekarpenen bat egin dezaketenei soilik bidaltzea deialdia. Izan ere, bilera bat ez da produktiboagoa izango partaide gehiago daudelako.
  - Saio baten iraupena deialdian jartzen duena izango da, ez gehiago, eta deialdian agertzen diren gai guztiak aztertu beharko lirateke (ildo beretik, gai-zerrenda izatea funtsezkoa da). Ordubete iraun beharrean ordu-erdi irauten badu, askoz hobeto (parte-hartzaileek eskertuko dute).
  - Sistema konfiguratzea parte-hartzaileei sistemak berak deitzeko, edo bestela, parte-hartzaileek dei dezatela asistentzia derrigorrezkoa baldin bada.
  - Irudi batek mila hitzek baino gehiago balio omen duenez... bilera batean zaudela, ez izan zalantzarik eta erabili *WebCollaboration* tresnak, oso eraginkorrak baitira.

PARADIGMA ALDAKETA

Zalantzarik gabe, aldatzen ari da enpresa tradizionalen paradigma. Horren ondorioz, lan-sare tradizionala desagertzen ari da, eta, horren ordez, berria ezartzen; hain zuzen ere, **ordutegien malgutasuna eta mugikortasuna** nagusi diren sarea.

Lan egiteko moduari dagokionez, benetako kultura-aldaketa gertatzen ari da; aldaketa hori ez da teknologikoa, teknologiak ahalbidetutakoa baizik, eta agian esaldi honekin laburbildu dezakegu: «*Lana jada ez da toki edo ordutegi jakin bat, jarduera bat baizik*». ❑

HIZTEGIA

[4] **Berehalako mezularitza**: iraganean, berehalako mezularitzako bezero hauek izan ziren erabilienak: ICQ, Yahoo! Messenger, Pidgin, AIM (AOL Instant Messenger), Google Talk (gaur egun Hangouts) eta Windows Live Messenger (egun Skype-n txertatuta dago).

Gaur egun, berehalako mezularitza mugikorretarako aplikazioetara, plataforma anitzeko aplikazioetara bideratu da gehienbat, edo bestela, funtzionatzeko inolako aplikaziorik behar ez duten web-zerbitzu bihurtu dira. Bereziki garrantzitsuak dira honako hauek: Facebook_Messenger, Skype, Line, Hangouts, Telegram eta Whatsapp.

Era berean, lankidetza sozialeko tresna berriak sortzen hasi dira WebRTCan oinarrituta (esaterako, besteak beste, Unify enpresaren Circuit) eta tresna horiek ahotsa, bideoa, pantaila partekatzeko aukera, berehalako mezularitza eta fitxate-giak elkartrukatzeko aukera biltzen dituzte interfaze berean, komu-nikazioa arinagoa, erra-zagoa eta naturalagoa izan dadin.

Zibersegurtasuna: APT (Mehatxu Iraunkor Aurreratuak) izeneko mehatxu bideratuak

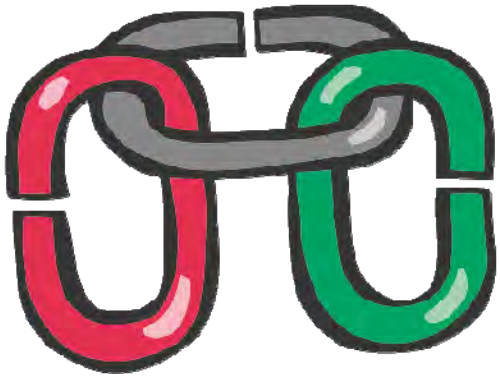
2015. urte honetarako zibersegurtasunaren arloko aurreikuspenen arabera, areagotu egingo dira *Mehatxu Iraunkor Aurreratuak* (APT, ingelesez) esaten zaien mehatxu edo eraso bideratuak; gai horri buruzko azalpenak ematen saiatuko gara, bada.

HIZTEGIA

[5] **Ziberespazioa:** William Gibson idazleak 1984. urtean idatzitako *Neuromante* nobelari esker egin zen ezagun hitz hori; Internet hitza eta Ziberespazioa hitza ez dira nahastu behar, azken horrek zera adierazten du, konputagailu baten bitartez edonoren esku dagoen ukiezin bat, toki fisiko jakin batekin translaziorik gabe.

Iturria: http://es.wikipedia.org/wiki/Ciberespacio

Zibersegurtasunaren eremuan —ziber-espazioan[5] arriskua kudeatzea da zibersegurtasuna—, 2015. urte honetarako joera APT izeneko eraso edo mehatxuen gorakada nabarmena da; APT izenak jatorri militarra du, eta 2006. urtean Estatu Batuetan erabili zen lehen aldiz, *Mehatxu Iraunkor Aurreratuak* izendatzeko.



EGUNGO EGOERA

Informazioaren eta Komunikazioen Teknologien (IKT) garapenetan, ahulezia eta segurtasun-akatsak eguneroko kontu izaten dira, hainbat arrazoirengatik: behar adina egiaztatu gabeko produktu eta bertsioak kaleratzeagatik, garatutako produktuen kalitate txikiagatik, produktuen konplexutasunagatik beragatik eta abarrengatik; ahulezia horiek naturaltzat hartzen dira eta akats horietako asko konpontzen dituzte a posteriori kaleratzen diren eguneratzeen bidez —«adabaki» esaten zaie zenbait kasutan— (2014ko abenduko 50. AURRERA aldizkarian, *Web -aplikazioak arriskuan: XSS*, izeneko artikuluaren barruko atal batean *Nola lortu web-aplikazioa segurua izatea?* aztertu genuen); produktu edo zerbitzuaren fabrikatzaileak zenbait ahuleziaren berri ematen du, zuzentzeko, baina egia da, halaber, hirugarrenek ere ahulezia asko detektatzen dituztela produktua edo zerbitzua kaleratu duena ahulezia horietaz jabetu ere egin gabe, eta, hirugarren horrek asmo txarrez jokatuz gero, arazo larriak eragin dakizkieke segurtasun-akatsa duen produktu/zerbitzu hori erabiltzen duten erakundeei.

ADVANCED PERSISTENT THREATS

APT siglak dira, ingelesezko *Advanced Persistent Threats* (Mehatxu Iraunkor Aurreratuak) hitzen siglak, eta ezaugarri berezi-bereziak dituen eraso mota bat izendatzeko erabiltzen dira; hona hemen ezaugarriak: iraupena denboran, ofizialki ezezagunak diren ahuleziak erabiltzea, eta xede zehatzen aurka bideratzen direla. Ikus dezagun zer esan nahi duten izen hori osatzen duten hiru hitzok:

- **Mehatxua (*threat*)**: AURRERA! aldizkariaren aurreko alean azaldu genuenez, **ahulezia edo segurtasun-akats bat** zera da, informazio-sistema baten (edo haren segurtasun-prozeduren, edo haren barne-kontrolen eta abarren) ahulgunea da; hura erabil daiteke segurtasun-istripu bat eragiteko; hots, ahulezia horri etekina ateratzeko aukera izatea **mehatxu bat** da, eta **eraso bat egiteko aukera dago** (betiere mehatxu hori informazio-sistemaren edo harekin zerikusia duen aktibo/baliabide baten gainean gauzatzen bada, segurtasun-istripu hori ekintza bihurtzen da, **kaltea** eragin baitezake). Lehen ere esan dugunez, APT mehatxuek ezezagunak diren ahuleziak baliatzen dituzte eta, beraz, «ohiko» segurtasun-neurriek ez dute eragin handirik izaten kasu horretan.
- **Iraunkorra (*persistent*)**: ezaugarri hori lotuta dago intentsitatearekin, tinkotasunarekin eta ahaleginarekin, baina ez du zertan erasoaren iraupenarekin loturik egon; adibidez, zerbitzua ukatze bidezko eraso batek (DoS[6] erasoa) denboran asko iraun dezake, eta ez du zertan APT motakoa izan. Kasu honetan, iraunkor

hitzak zera esan nahi du, xedea aldez aurretik aztertu eta ikertzeko fase bat dagoela (hasierako prestakuntza-fasea) —fase hori biziki garrantzitsua da erasoa gauzatzeko garaian (lehen fase horren emaitzaren arabera, erasoa ongi edo gaizki atera daiteke)— eta eraso hori aktibo edo ezkutuan egon daitekeela, detektatu gabe. Oro har, horrelako erasoek ez dute garrantzi txikia izaten eta, beraz, denbora eta baliabide asko baliatzen dira finkatutako helburuak betetze aldera. Denboran iraunkor izateak zera esan nahi du, erasotzen den sistemaren administratzaileek ez dutela erasoaren berri izan behar; horretarako, administratzaile horiek detektatzeko moduko beste eraso batzuk egiten dituzte, APT erasoa estaltzeko.

- **Aurreratua (*advanced*)**: erasotzaileek gaitasun tekniko handia dutela adierazten du ezaugarri horrek, eta, aldi berean, ahuleziak teknifikazio-maila handiko ikuspegi berritzaile batetik ustiatzen direla; horrek zera esan nahi du, «sinaduretan» («sinadura» batek zeroen eta baten kate jakin bat errekonozitzen du testuinguru jakin batean, eta alarma pizten du; sinadura horiek aldizka eguneratu behar izaten dira) oinarritutako erasoak detektatzeko metodo tradizionalek —birusen aurkako egungo programek horrela lan egiten dute— ez dutela funtzionatzen kasu horietan. Horregatik, goi-mailako kualifikazioa izaten dute zibergaizkile horiek. Oro har, zibergaizkile horiek delitu-erakundeetako (talde antolatu espezializatuak) kide izaten dira, baita gobernuetako kide ere, horrelako ekintzak egiteko baliabide ekonomikoak bideratzen baitituzte.

«Segurtasun-eredu tradizionalak ez du balio *mehatxu iraunkor aurreratuei* aurre egiteko»

APT ERASO BATEN HELBURUAK

Hasieran, erasoek ez zuten helburu zehatzik izaten, eraso orokorrak izaten ziren, kaltea eragitea beste xederik gabe; orain, aldiz, erasoak oso aurreratu eta selektiboak dira (xedeak argi eta garbi zehaztuta izaten dituzte). Xede nagusiak honako hauek izaten dira, besteak beste: enpresa-arloko espioitza, gobernuen helburuak, aktibo

Trend Micro Security-ren 2015erako iragarpenak

Sarreran esan dugunez, zibersegurtasunaren eremuko 2015erako iragarpenen arabera, APT erasoak nabarmen handituko dira.

Trend Micro enpresak *The invisible becomes visible (Ikusezina ikusgai)* izena duen txostena egin du (Txostena: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-invisible-becomes-visible.pdf); txosten horretan, zibersegurtasunaren eremurako honako iragarpen hauek egin ditu:

- ✓ Zibergaizkile gehiagok joko du sare iluna (**darknet**[7]) esaten zaion horretara eta sarbide esklusiboko foroetara ziberkrimenarekin lotutako produktuak partekatu eta saltzeko.
- ✓ Mugikorrarekin ordaintzeko metodo berriek eraso mota berriak sortzea eragingo dute.
- ✓ Kode irekian (*open source*) oinarritutako aplikazio mugikorretan ahuleziak ustiatzeko saiakera gehiago egongo dira.
- ✓ Ziberjarduera handiagoaren ondorioz, *hackeatzeko* tresna eta saiakera handiagoak eta eraginkorragoak egongo dira.
- ✓ Ustiapen-*kit*ak (zibergaizkileek egin eta hirugarrenei saltzen dizkieten tresnak dira, erasoak egiteko) Android sistemara bideratuko dira, ahulezia mugikorrak erabakigarriak izango baitira gailuak infektatzeko.
- ✓ **Mehatxu bideratuak (APT) ziberkrimena bezain garrantzitsu bihurtuko dira.**
- ✓ Aniztasun teknologikoari esker, gauzen interneteko gailuak mehatxu masiboen aurrean babestuta egongo dira, baina ez, ordea, prozesatzen diren datuak.
- ✓ Mehatxu larriagoak sortuko dira lineako bankari eta finantza-motibazioa duten erakundeei dagokienez.

HIZTEGIA

[6] **DoS erasoa:** *Denial of Service*, Zerbitzua Ukatzea, beste eraso mota bat; kasu horretan, gure informazio-sistemako (baliabidea edo zerbitzua) aktibo bat zerbitzutik at uzten da, hau da, sisteman sartzeko eskubidea duten pertsona edo zerbitzuei sarbidea ukatzen zaie. Horrelako eraso bat egiteko modurik oinarrizkoena honako hau da: zerbitzari bat (posta elektronikoaren edo web-orrien zerbitzaria) sartzeko eskaera masiboekin gainezka jartzea.

[7] ***Darknet***: *sare iluna* esan nahi du; banatutako sare pribatu bat da, eta bertan informazioa elkartrukatzen duten pertsonen anonimotasuna zaintzea du xede. Sare publikoen gainean muntatuta egoten dira baina sare horietaz aparte jarduten dute; bertako edukiak ez dira jendearentzat, oro har, eskuragarri egoten eta, horretaz gain, bilaketa-motorrek ez dute sare horietan bilatzen. Beraz, edukia ezkutuan geratzen da.

militarrak, jabetza intelektuala, komunikabide masiboak eta telebista, telekomunikazioetako eta sateliteen operadoreak, azpiegitura kritikoak —ikus *Azpiegitura Kritikoak* taula—, eta finantza-informazioa; hau da, sektore guztietan eta industria-eredu guztietan gertatzen dira.

APT erasoak egiteko *malware*[8] konbinazio zehatz bat erabiltzen da, erasotzen den xedearen arabera; praktikan horrek badu ondorio bat: horrelako erasoak detektatzea ohikoak detektatzea baino askoz ere konplexuagoa izatea.

MEHATXU AITZINDARIA: STUXNET

Stuxnet APT motako *malware*a da, eta, agian, APT deitutako lehen erasoa izan zen; 2010. urtean ezagutarazi zen jendaurrean, oro har, eta Irango zentral nuklearra infektatu zuen —zentral horrek zentrifugagailuak erabiltzen zituen uranioa aberasteko—. **Iranen programa nuklearra atzeratzea zuen xede** zentrifugagailu horiek kaltetuta; izan ere, hondatzen baldin baziren sistemaren presioa —balbula eta sentsoreen bitartez kontrolatzen zen— areagotu egiten zen (APT hori Windows ekipoak eta SCADA sistemak[9] infektatzeko diseinatuta zegoen); beraz, balbula eta sentsore horiek kontrolatzen zituzten kontrolagailuak gobernatzeko asmoz egin zen erasoa, baina puntu gorenera iritsi gabe, hau da, zentral nuklearra suntsitu gabe. Helburua «*zentralean kalteak maiz eragitea*» zen, gehiegizko estresagatik. Erasoak bigarren fase bat ere izan zuen: zentralean lan egiten zuten kanpoko kontratisten ordenagailuak infektatuta lortu zuten sartzea, eta haien ekipoak zentral nuklearraren ordenagailuekin konektatu zituztelarik, ordenagailu horiek infektatu eta zentrifugagailuen errotoreak kontrolatu zituzten errotazio-abiaduraren irakurketak faltsututa. Bigarren bertsio horrek *zero eguna* (*0-day*[10]) izeneko ahuleziak baliatu zituen. Erasoa hilabete luzez ezkutuan egotea lortu zuten.

APT ERASO BATEN FASEAK

APT eraso guztiak desberdinak izaten dira xedearen arabera, baina zenbait fase eraso guztietan errepikatzen dira; hona hemen:

1. Hasierako prestakuntza: xedea eta bere sistemak aztertu eta ikertzea, izan ditzakeen ahulguneak detektatzeko, erasoa hortik jotzearren.
2. Hasierako intrusioa (sisteman detektatutako ahuleziak baliatuta): oro har, Webaren bitartez (urruneko *exploit*a) edo mezu elektroniko bati atxikitako fitxategi edo hiperesteken bitartez.
3. *Malware*a instalatzea: biktimaren barruan sartutakoan, *malware*a duen kodea exekutatzen da.
4. Irteerako konexioa: ohiko moduan urruneko administrazio-tresna baten bitartez (erasotzaileek maneiatzen duten **komando eta kontroleko zerbitzari** baten eta infektatutako makinaren arteko SSL kanal zifratu bat).
5. Hedapena: azken erabiltzailearen infektatutako gailuaren bitartez, APTa saiheska zabaltzen da xedearen bila (sistemaren administratzaileek ordenagailuak, datu-baseak, zerbitzariak...)
6. Datuen bilaketa eta ihesa: datuak bilatu eta ezohiko trafikoaren susmorik eragin gabe transferitzen dira (adibidez, konprimitutako blokeetan eta pasahitzarekin); halaber, datuak jasotzen dituen ordenagailuaz inor ez jabetzea ere lortu behar da.
7. Pistak ezabatzea: *malware* bidezko beste eraso batzuen bitartez (despistatzeko), instalatutako *malware*a ezabatu eta desinstalatzen da.

APT ERASO BAT DETEKTATZEA

Lehen ere esan dugunez, ohiko defentsa-moduek ez dute balio APT erasoei aurre egiteko.

Adibidez, lehen esandakoari jarraiki, babes-sistema estatikoak izaki (soilik lehendik ezagunak

HIZTEGIA

[8] ***Malware***: software gaiztoa, informazio-sistema batean kalteak eragitea edo infiltratzea xedea duela.

[9] **SCADA:** *Supervisory Control And Data Acquisition*, industria-prozesuetako datuak eskuratzeko, kontrolatzeko eta gainbegiratzeko sistemak.

[10] ***0-day***: eraso mota horretan, jendearentzat, oro har, eta produktu edo zerbitzuaren fabrikatzaileentzat ezezagunak diren ahuleziak ustiatzen dituen kode gaiztoa exekutatzen da.

diren erasoak identifikatzeko aukera ematen dute), sinaduretan oinarritutako teknikek ez dute funtzionatzen APT erasoen kasuan, eraso dinamiko eta polimorfikoak izaten baitira (denboran aldatzeko gaitasuna dute, zenbait aldagairen arabera).

Sandbox[11] izeneko konponbideak fitxategietan oinarritzen dira eta horiek ere ez dute arazoa konpontzen; izan ere, konponbide horietan, prozesuak ingurune birtual batean isolatzen dira, eta ingurune horrek fitxategiak (.EXE, .PDF, Microsoften Office fitxategiak eta abar) aztertzen ditu, baina aztertu beharreko objektu gehienak aztertu gabe geratzen dira, APT erasoen etapak ez dituzte aintzat hartzen eta ez dituzte korrelazioak ezartzen.

Hodeian dauden *antimalware* neurrien kasuan, datuak hodeira birbidali behar izaten dira aztertu ahal izateko, eta hori ez da gertatzen.

Horregatik guztiagatik, APT eraso edo mehatxuei aurre egiteko egungo defentsa-konponbideetan —konponbide tradizionalekin osatuta— honako ekintza hauek gauzatzen dira:

- ✓ Azterketa dinamikoa eta denbora errealean, hainbat ikuspuntutatik begiratuta: web-trafikoa, posta-trafikoa, enpresaren fitxategiak, trafiko mugikorra, enpresako postuak edo beste edozein objektu aztertzen dira.
- ✓ Azterketa horiek egin ostean, defentsa-ekipoak elkarrekin erlazionatzen dira, lortutako informazioa elkartrukatzen dute, eta informazio horri buruzko korrelazioak ezartzen dituzte.
- ✓ Fluxu susmagarriak ingurune birtualizatu batean exekutatzea denbora errealean, datuak erauzteko saiakerak detektatu eta blokatzeko asmoz. ❑

Azpiegitura kritikoak

Azpiegitura kritikoak oinarrizko zerbitzuak eskaintzen dituzten informazio teknologia, baliabideak, zerbitzuak eta sareak dira, eta nahi gabeko eteterik jasanez gero (arrazoi naturalengatik, teknikoengatik edo nahita egindako erasoengatik), ondorio larriak izango lituzke funtsezko hornidura-fluxuetan, oinarrizko zerbitzuen funtzionamenduan eta segurtasunean. **Apirilaren 28ko 8/2011 Legea**ren bitartez azpiegitura kritikoak babesteko neurriak ezartzen dira.

Azpiegitura baten kritikotasuna zehazteko irizpideak hiru dira: biktimen kopuru potentziala, inpaktu ekonomikoa eta inpaktu publikoa.

Lege horren lehentasunezko helburuak honako hauek dira: Azpiegitura Kritikoak babesteari dagokionez, Administrazio Publikoetako organoen jardunak zuzentzea eta koordinatzea ahalbidetuko duten estrategia eta egitura egokiak ezartzea, betiere aldez aurretik identifikatu eta hautatuta; horretaz gain, azpiegitura horien jabe eta kudeatzaile diren erakundeen lankidetza eta inplikazioa sustatzea, nahita egindako mota guztietako erasoen aurrean azpiegitura horien babes-maila optimizatze aldera. Era berean, kritikotzat jotzen diren azpiegituren operadore pribatuek nahiz Administrazio Publikoek beren gain hartu behar dituzten betebeharrak ere arautzen dira Lege horren bidez.

Azpiegitura Kritikoak Babesteko Plan Nazionalaren arabera, Azpiegitura Kritikoak 12 sektore estrategikotan banatzen dira: zentralak eta energia-sareak, informazioaren eta komunikazioen teknologiak, finantza- eta zerga-sistema, osasun-sektorea, espazioa, ikerketa-instalazioak, elikadura, ura, garraioak, industria nuklearra, industria kimikoa eta administrazioa.

Kriptologia Zentro Nazionalak (CCN) Azpiegitura Kritikoak Babesteko Zentro Nazionalari lagundu egiten dio azpiegitura kritikoen gaineko zibererasoen tratamenduan, eta azpiegitura kritikoekin lotura duten segurtasun-gorabehera informatikoei eta SCADA[12] ahuleziei buruzko informazioa eguneratzen.

CCN Centro Criptológico Nacional

www.ccn.cni.es

HIZTEGIA

[11] ***Sandbox***: ingelesezko hitz horrek *hondar-kutxa* esan nahi du; prozesuak isolatzeko sistema bat da eta segurtasun informatikoko inguruneetan erabiltzen da: prozesu informatikoak modu seguruan eta bereizian exekutatzeko prozedura da.

[12] **SCADA ahuleziak:** industria-kontroleko sistemen segurtasunerako intereseko gidaliburuen multzoa. http://www.cnpic.es/Ciberseguridad/4_Guias_Scada/index.html

ALBOAN:

Inkesta elektronikoak estandarizatzea

«Eustatek web galde-sortak garatzeko *framework* bat sortu du»

2008. urtera arte, EUSTATek datuak biltzeko garatutako web-aplikazioak elkarrekiko loturarik gabe, modu independentean diseinatzen ziren; horren ondorioz, kasu askotan, arazo larriak sortzen ziren irizpideen uniformetasunarekin lotuta, diseinuari, kode-bikoizteari eta abarri zegokienez. Hori horrela izanik, ikuspuntu **funtzionaletik** begiratuta, garatutako aplikazio bakoitzak inkesta-prozesuan bete beharreko alderdi guztiak betetzen zituen, baina **diseinuaren eta eraikuntzaren** ikuspuntutik begiratuta, aplikazio bakoitzaren ezaugarriak desberdinak ziren aplikazioa garatu zuen enpresaren arabera.

Arazo horiek saihesteko, proiektu bat abiarazi zen honako **helburu** hauekin:

- Egungo web-aplikazio guztiak birmoldatzea garapen-plataforma bera erabilita
- Web-aplikazio guztien itxura bisuala bateratzea, diseinu-ereduak (irudiak, tipografia, nabigazioa...), alderdi teknikoak (pisua, kargatzeko abiadura, irisgarritasuna...) eta egiturazkoak (edukia...) barnean hartuta
- Web-inkesta guztientzat **sarrerako puntu bakarra** definitzea
- Arkitektura tekniko bakarra finkatzea ezarpena eta mantentze-lanak erraztearren

PROIEKTUAREN PLANGINTZA

Proiektuaren lan-plana honako hau zen:

- ✓ Web-inkesta guztientzat sarrerako atari bakarra sortzea, eta autentifikatzeko eta profilak kudeatzeko hainbat maila ere zehaztu ziren.
- ✓ Web-inkesta bat osatzen duten orri guztien oinarrizko esparrua sortzea. Horretarako, honako elementu hauek finkatu ziren: orrien antolamendua eta hierarkia, inkesta guztientzako komunak diren estilo-orriak, nabigatzeko oinarrizko mapa eta menuak, *feedback* mezuen interakziorako sistema bakarra, baliozkotzea eta oharrak, eta abar.
- ✓ Web-aplikazio guztientzako komunak diren software osagaien biltegia sortzea, horiek garatzeko behar den denbora murriztearren.
- ✓ Estilo-liburua garatzea.
- ✓ Web-aplikazio guztietan erabili beharreko erroreak kudeatzeko eta kontrolatzeko esparru bakarra sortzea.
- ✓ Web-inkestak baliozkotzeko sistema bakarra sortzea.
- ✓ Laguntza mota guztiak eta horiek bistaratzeko modua homogeneizatzea.

Lan hori guztia egiteko, hainbat urtetako plangintza egin zen:

- ➢ **2009-2010**: etorkizuneko inkesten estiloaren, diseinuaren eta proiektuaren alderdi teknikoa zehaztu zen
- ➢ **2011-2012**: software osagaiak garatu ziren eta inkesta pilotu bat estandar berriaren arabera egokitu zen
- ➢ **2012-2014**: orduko web-inkesta guztiak *framework* (programak/softwarea antolatzeko eta garatzeko balio duten software moduluen multzoa) berrira migratu ziren. Galde-sorta berriak zuzenean plataforma berriarekin garatzen dira

DESKRIBAPEN FUNTZIONALA

Sortu diren premiei erantzutearren, Eustatek *framework* bat sortu du erakunde autonomoak egiten dituen estatistika-eragiketa guztiak egiteko beharrezkoak diren web galde-sortak garatzeko. *Framework* horri esker, garapenak errazagoak dira, eta azken emaitzaren kalitatea bermatzen da; Eustatek bi helburu bete nahi izan ditu *framework* hori sortzeko garaian:

1. Galde-sorten **erabilgarritasuna** hobetzea,

erabiltzaileen lana errazagoa izan dadin (galde-sorta erakargarriagoak, nabigazio arina, laguntza egokiak eta abar).
2. Web galde-sorta berriak **kalitate** egokiarekin eta esfortzu gutxiagorekin garatzea.

Galde-sorten diseinu orokorra

Galde-sortak diseinatzeko arau guztiak zehazten dituen **estilo-liburua** egiteko, gaian adituak direnen gomendioak aztertu ziren eta, besteak beste, honako ildo hauek zehaztu ziren:

- Galde-sortaren orri guztietan sekzio bidezko eskema berdin-berdina erabiltzea, sekzio bakoitzak funtzionaltasuna zehatz bat izanik
- «Orrialdekatze» bidezko diseinua erabiltzea, irristatze horizontal nahiz bertikalak saihestuta
- Oinarrizko elementuak (*radio button*ak, goitibeherako zerrendak...) erabiltzea galdera motaren arabera eta mota horretarako egokiena den elementua hautatuta
- Datu-taulen diseinu espezifikoa, horrelako informazioa hobeto ulertzeko
- Hainbat mailatan zehaztutako laguntza-sistemak

Informazioa egiaztatzeko sistemak

Erantzunetan okerreko datu ahalik eta gehien saihestearren, erroreak kontrolatzeko eta baliozkotzeko sistema bat diseinatu da. Hiru baliozkotze mota zehaztu dira:

1. Orriari dagokiona: orri bereko kontrolen baliozkotzeak, edo kontrolen artekoak
2. Kohesioa: orri desberdinetako kontrolen arteko baliozkotzea
3. Luzetarakoak: kontrol espezifikoei buruzko baliozkotzeak, ohar moduan.

Era berean, bistaratzen diren mezuak aurkezteko modua ere zaindu da (ahalik eta *atseginenak* izateko ahalegina egin da), galde-sorta ulergarriagoa izan dadin.

Nabigazioa

Nabigazio-logika jakin bat zehaztu da; horren arabera, orri batetik bestera nabiga daiteke aurreratze sekuentzialeko botoien bidez edo *nabigazio-mapa* baten bidez. Sistema horrek galde-sorta kontrolatzeko informazioa biltegiratzen du, hala nola, iraupena, noiz bete den eta abar.
Azkenik, nabigazio-sistemak grafoa kontrolatzeko mekanismo bat du; mekanismo horren bitartez galderak (edo galdera blokeak) aktibatu eta desaktibatzen dira, emandako erantzunen arabera.

Datuen segurtasuna

Datuei dagokienez, *aldez aurreko galde-sorta* bat prestatu da galde-sorta elektroniko guztien sarrerako puntu bakartzat; aldez aurreko galde-sorta horretan hainbat segurtasun-neurri biltzen dira, alde batetik, **datuak babesteko** eta, bestetik, **sarbideak kontrolatzeko**; era berean, intereseko beste informazio batzuen erregistroa ere biltzen du, azken erabiltzaileek inkestak betetzen dituztenean zer lan-karga dagoen aztertzeko aukera ematen duela.

ERRONKA BERRIAK

Proiektu hori ezarrita, Eustatek web galde-sorta guztiak **estandarizatzea** lortu du, dela diseinuaren ikuspegitik begiratuta, dela arkitekturaren ikuspegitik begiratuta; halaber, galde-sorten softwarea garatzeko eta mantentze-lanetako **kostuak murriztea** ere lortu du, galde-sorten **kalitatea** hobetzearekin batera.

Nolanahi ere, eta aurrera begira, beste gai batzuk aztertzen ari dira jada:

- Inkestatuaren «Ataria» zehaztu eta eratzea, Eustaten eta informatzaileen arteko interakzioa areagotzeko.
- Inkestatuen «identifikazioa» eta autentikazioa bermatzen duten sarbide-sistema berriak txertatzea.
- Gailu mugikorretarako *app* bertsioak sortzea.
- *Frameworka* zabaltzea osagai berriekin, funtzionaltasun berriak txertatzeko.
- Eta, azkenik, inkestak betetzen amaitzen dutenean erabiltzaileen gogobetetze-maila ebaluatzeko aukera emango duten sistemak txertatzea. ❑

«Proiektu horri esker, web-inkesta guztien garapeneko eta mantentze-lanetako kostuak murriztea lortu du Eustatek, baita horien kalitatea hobetzea ere»

[**informazio gehiago**]:

Eustat-en webgunea:

http://www.eustat.eus

ALBOAN

51. zk.

2015eko martxoa

BERRI LABURRAK!!

Telefonia mugikorra: «hegazkin modua»

Hegazkinetan ezin zen bidaiatu gailu elektroniko eramangarriak (PED, *Portable Electronic Devices)* konektatuta izanik (adibidez, *t*elefono adimendunak, *tablet*ak, ordenagailu eramangarriak, *e-reader* gailuak edo MP3 erreproduktoreak), baina EASA (*European Aviation Safety Agency*) Aireko Segurtasunaren Europako Agintaritzak 2013. urtean PED gailu horiek erabiltzeko baimena eman zuen, **betiere «hegazkin moduan»** (*aeroplane mode*) konfiguratuta baldin badaude, hau da, transmititzen ari ez badira: gailuaren hari gabeko konexioak desaktibatu egiten dira eta, hartara, ezin da irrati-seinalerik (Wi-Fi, Bluetooth, 3G…) jaso edo hartu; era berean, datu- eta ahots-konexioak ere desaktibatzen dira.

Gailu horiek beste garraiobide batzuetan —trenean, kasu— bezalaxe hegaldietan ere askatasunez erabiltzeko baimena ematearren lanean jardun zuen EASAk airelineekin. Horregatik, 2014ko irailaren 26tik aurrera erabili ahal izatea lortu zuen, gailua transmititzen ari den edo ez den alde batera utzita. Esan gabe doa, azken buruan, airelinea bakoitzak erabaki beharko duela PED horiek transmititzen ari direla erabiltzeko aukera emango duen (airelinea bakoitzak bermatu beharko du horrelako seinaleek ez dutela eraginik izango hegaldietan).

Segurtasun-arrazoiak direla medio, Europako aire-konpainiek kudeatzen dituzten aireontzietan PED gailuak erabiltzeko baldintza jakin batzuk arautu ditu EASAk, baina konpainia horiek EASA bera baino murriztaileagoak izan daitezkeela nabarmendu du.

EASAren webgunea: http://www.easa.europa.eu

Ubuntu duten lehen mugikorrak

Canonical software-enpresak eta BQ konpainiak Aquaris E4.5 Ubuntu Edition telefonoa aurkeztu berri dute Londresen, hau da, Ubuntu sistemarekin merkaturatuko den lehen *smartphone*a (gaur egun, **Linux**en banaketen artetik, mundu osoko ezagunenetako bat da Ubuntu).

Adituek diotenez, gama ertaineko terminal hori *early adopter* esaten zaienei zuzenduta dago, hau da, produktu berriak probatzea atsegin dutenei.

BQ enpresak jakinarazi duenez, gailu berria «librea» izango da, eta, beraz, telefoniako edozein operadorerekin erabili ahal izango da.

Hona hemen Aquaris E4.5 Ubuntu gailuaren ezaugarri tekniko nagusiak:

4,5 hazbeteko pantaila (bereizmena: 960×540 pixel), aurreko kamera (5 megapixel) eta atzeko kamera (8 megapixel), SoC Mediatek Quad Core ARM Cortex A7 prozesadorea (1.3 GHz), 1GBko RAM memoria eta 8 GBko barne-memoria, 2.150 mAh-ko bateria, MicroSD txartela, bi SIM txartel erabiltzeko aukera (Dual SIM). Neurriak: lodiera 9 mm, eta pisua 123 gr.

Beste ezaugarri garrantzitsu bat ere badu gailuak: nabigazioa *Scopes* izeneko ikuspegien bidez egiten duela [telefonoan gehien erabiltzen diren zerbitzuetara pantaila nagusitik sartzeko modua; gehien erabiltzen diren zerbitzu horiek gaiaren arabera multzokatzen dira: «musika», «gertaerak», eta abar; telefono mugikorrek egun erabiltzen dituzten *app* aplikazioen baliokideak izango lirateke).

Softwarearen etorkizuneko eguneratzeei (sistema eragilea eta aplikazioak) dagokienez, Canonical enpresa arduratuko da horretaz.