EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

66. zk.

2018ko abendua

Berrikuntza eta Teknologia Berrien dibulgaziozko aldizkaria
Bulego Teknologikoak argitaratua
Informatika eta Telekomunikazio Zuzendaritza

AURKIBIDEA

Ale berri honetan kontzeptu berri bat aurkezten dizuegu, «***DevOps***» izenekoa. Kontzeptu hori jorratzen dugun lehenengo gaian ikusiko dugunez, benetan ez da lan-metodologia berria, baina antza denez, gaur egun azaleratzen ari da erakunde berrien artean, enpresei malgutasuna eskaintzen baitie, garatzen dituzten softwareko produktuak (aplikazioak) euren bezeroei ematerakoan.

Bestalde, kondairak dioenez, rockero zaharrak sekula ez dira hiltzen… eta horrez gain hauxe esan genezake: hackerrek informazioa lortzeko eta pertsonei iruzur egiteko erabiltzen dituzten metodo zaharrak ere ez; izan ere, aspaldidanik **nortasunak ordezteko** erabiltzen diren metodo asko aise dabiltza han eta hemen, erasoa jasan baina euren burua nola defendatu ez dakiten pertsonei (edo enpresei) kalte handiak sortzen. Horregatik, kasurik tipikoenetako batzuk errepasatuko ditugu, labur, eta, batez ere, horiek detektatzen eta saihesten ikasiko dugu. Halaber, Eusko Jaurlaritza bere langileak kontzientziatzeko eta prestatzeko zer ekimen egiten ari den azalduko dizuegu.

«Alboan» atalean duela gutxi Eusko Jaurlaritzaren **Ibilgailu atala**ren aplikazioan gehitu den hobekuntza bat aurkezten dizuegu. Hobekuntza horren helburu nagusia da sailek eta Baliabide Orokorren Zuzendaritzak euren artean paper gutxiago truka dezatela. Artikuluan ikusiko dugu zertan datzan hori.

Ideiak eta esperientziak trukatzea gauza ona da beti, eta duela gutxi, Eusko Jaurlaritzak software askeari eta kode irekiari buruzko enpresa arloko topaketarik handienean, aurten Bilbon egin den **LibreCon2018** izenekoan, parte hartu du. Askoz xehetasun gehiago kontatuko dizkizuegu *«Ixteko»* atalean.

«Protagonistak» atalean, **Hedy Lamarr**-en bizitza errepasatuko dugu, labur, hain zuzen ere telekomunikazioen arloan asmatzailerik handienetako bat izateaz gain aktore ere izan zen emakumea.

Ahaztu baino lehen,

Zorionak
eta 2019. urte oparoa izan dezazuela!

Honela funtzionatzen du DevOps metodologiak

DevOps[1] mugimenduak lotura estua dauka softwarea garatzeko metodologia arinekin. Artikulu honetan azalduko dugu zein den bere jatorria, zein bere ezaugarriak, bai eta erakunde handiei eskaintzen dizkien abantailak ere.

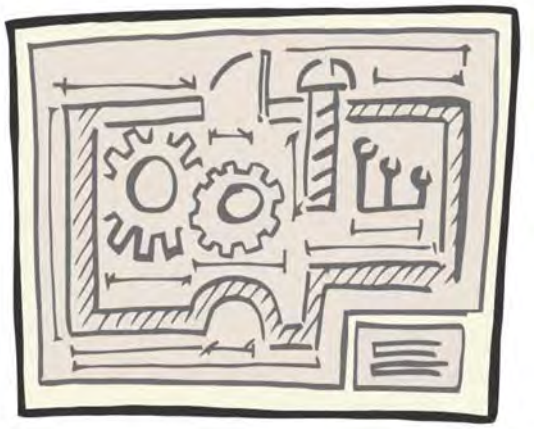
[1] **DevOps**: *development* (euskaraz, garapena) eta *operations* (eragiketak) hitzen ingelesezko akronimoa da. Funtsean softwarearen ingeniaritzako jardunbidea da; bere helburua da softwarearen garapena (Dev) eta softwarearen eragiketa (Ops) bateratzea.

DevOps mugimenduaren ezaugarri nagusia da softwarea eraikitzeko edo garatzeko urrats guztietan automatizazioa eta monitorizazioa aldeztea, integraziotik, probetatik eta askapenetik hasita azpiegituraren inplementazio eta administraziora arte.

DevOps-en helburua honako hauek lortzea da: garapen-ziklo laburragoak, inplementaziorako maiztasun handiagoa, merkaturatze fidagarriagoak, helburu komertzialekin modu estu-estuan bat eginez.

[Iturria: Wikipedia]

90eko hamarkadara arte, aplikazio informatikoak garatzean «kateko» ereduaren metodologiari jarraitzen zitzaion. Metodologia horren ezaugarria zen baliozkotzerakoan eta hurrengo fasearekin jarraitu eta bezeroari azken produktua (programa informatikoa edo softwarea) ematerakoan, urrats oso egituratu eta zorrotzak izatea.



Askotan burokratikotzat eta moteltzat jotzen zen metodologia horri erantzunez, 90eko hamarkadaren erdialdean metodologia askoz arinago eta ez hain murriztaileago bat sustatzeko helburua zuen mugimendua sortu zen.

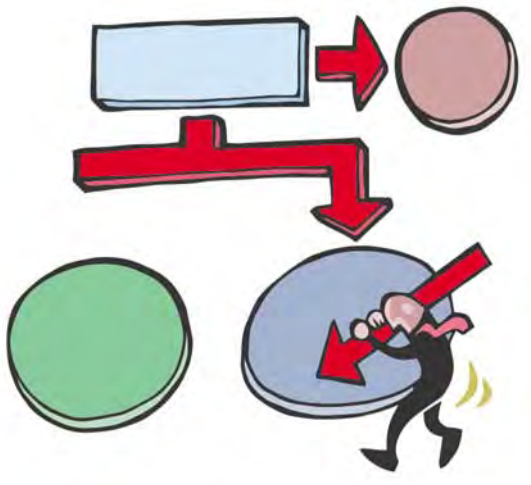
Geroago, zehazki 2001ean, Snowbird-en (Utah) informatikako konbentzio bat egin zen; bertan, hainbat pertsonak «metodo arinak» izena aukeratu zuten mugimendu berri hori izendatzeko. Dena dela, garrantzitsua da gogora ekartzea 2000. urtea baino lehen arinaren antzeko metodo asko sortu zirela. Hauek dira metodo horien artean nabarmenenetako batzuk: Scrum (1986), Crystal Clear, muturreko programazioa (ingelesez eXtreme Programming edo XP, 1996), software moldagarriaren garapena, *feature driven development*, Sistema dinamikoak garatzeko metodoa (ingelesez *Dynamic Systems Development Method* edo DSDM, 1995).

Denboraren poderioz, metodologia horiek guztiak apurka egonkortu egin ziren, eta gaur egun erakunde askok metodologia horietako bat edo beste erabiltzen dute.

BESTE ESPARRU BATZUK

Ikusi dugunez, «metodologia arinak» izenekoak ez dira gauza berria, eta aspalditik erabiltzen dira, baina batez ere softwarearen **plangintza** eta **garapen**aren arloan.

Informatikak software baten plangintza, garapena eta ezarpena barnean hartzen dituenez, esan daiteke «jauzi» bat zegoela —edo dagoela— softwarea garatzerakoan



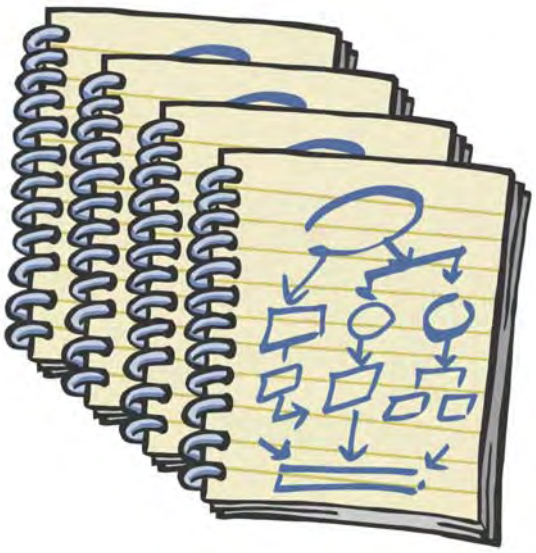
erabiltzen den metodologiaren eta erakunde bateko azpiegitura baten edo Datuak Prozesatzeko Zentro (DPZ) baten barruan aplikazioak ezartzerakoan betetzen den prozeduraren artean. Eta hori arazoa da.

«Jauzi» hori gainditzeko, ekimen batzuek **metodologia arinen helmena** azpiegituren eta sistemen administrazioaren esparrura hedatzearen alde egiten dute. Eta hor sortzen da DevOps kontzeptua.

[ikus *«Azpiegitura arinak»* koadroa]

DEVOPS-EN JATORRIA

Garai batean, metodologia arinek enpresei aukera ematen zieten euren bezeroentzat garatzen zuten softwarea maiztasun handiagoaz ateratzeko (emateko). Enpresa horiek arazo bat zeukaten: euren barneko prozesu askoren erritmoa egokitu behar



izaten zuten, parte hartzen zuten arlo guztiak (bertsioen kudeaketa, aplikazioak merkaturatzea, integrazio etengabeko tresnak eta etengabeko entrega) lerrokatuta egon zitezen.

Enpresa batzuek, adibidez, egunean hamar hedapen baino gehiago egiten dituzte. Mota horretako sistemak «etengabeko hedapenak» (*continuous deployment*) edo «etengabeko emateak» (*continuous delivery*) izenez ezagutzen dira.

«"Metodologia arinak" aspalditik erabiltzen dira, baina batik bat softwarearen plangintza eta garapenean»

Etengabeko hedapenen ideia honako honetan datza: proiektu baten integrazioak ahalik eta sarrien egitean, horrela hutsegiteak ahalik eta azkarren detektatzeko.

Integrazioan, proiektu oso baten proben konpilazioa eta burutzapena sartzen da, eta normalean prozesua honelakoa izaten da: aldizka (adibidez, ordu gutxi batzuez behin), iturriak deskargatzen dira bertsioen kontrolerako erabiltzen den aplikaziotik, adibidez Git[2]-etik; konpilatzen da, beharrezkoak diren probak egiten dira eta txostenak sortzen dira.

AZPIEGITURA ARINAK

Yhens Wasna eta Patrick Debois ingeniariak DevOps terminoaren «gurasoak» direla esaten da; izan ere, 2008ko abuztuan Toronton (Kanada) egindako *«Agile 2008»* biltzarrean eman zuten *«Azpiegitura Arina eta Eragiketak»* izenburuko hitzaldian sortu zen.

Topaketa hartan hainbat erronka planteatu zen, besteak beste metodologia «arina»ren filosofia nola txerta zitekeen azpiegituraren eta sistemen administrazioan eremuan.

Eta une hartatik aurrera DevOps terminoa apurka hedatzen hasi zen.

[2] **Git:** Linus Torvaldsek diseinatutako softwarea da; garatzen ditugun bertsioak kontrolatzeko modua ematen du, batez ere iturri-kodeko fitxategi ugarirekin lan egiten denean. Software horren bidez fitxategietan egiten diren aldaketen erregistroa egin daiteke, eta hainbat pertsonaren lana koordinatu ere bai.

Gaur egun hainbat aplikazio dago, adibidez honako hauek:

- Bezeroa-Zerbitzaria ereduan oinarrituak:
  - Concurrent Versions System (CVS)
  - Subversion (svn)
  - AccuRev
  - Visual SourceSafe
- Eredu banatuan oinarrituak:
  - Aegis
  - Bazaar
  - Git
  - BitKeeper

Informazio gehiago nahi izanez gero, Aurrera aldizkariko 54. zenbakian argitaratutako «*GitHub: kodea liberatzeko plataforma soziala*» artikulua kontsulta dezakezue (2015eko abendua)

Laburbilduta, lan egiteko modu berri hori oso gomendagarria da sarritan edo denbora gutxian behin emateak egin behar dituzten enpresentzat.

DevOps, beraz, metodologia arinek softwarea garatzerakoan izan zuten arrakastari esker sortu zen.

KULTURA ALDAKETA

Normalean gauza berri guztiekin gertatzen denez, erakunde batean DevOps metodologia arrakastaz ezartzeko, **aldaketaren kudeaketa**[3] egokia egin behar da, bai kulturaren ikuspuntutik, bai antolaketaren ikuspuntutik.

Arrazoia honako hau da: metodologia berri honen oinarria da orain arte bakoitza bere

[Irudia: Wikipedia]

aldetik edo konpartimentu estankoetan jardun duten arloen artean (halakoak dira **Garapen** arloa eta **Sistemen** arloa) **lankidetza**, **komunikazioa** eta **integrazioa** bultzatzea (aholkularitza-enpresa batzuek **Segurtasun** taldeak eta **Kalitate** Ingeniaritzako taldeak ere sartzen dituzte DevOps eredu berriaren barruan).

DevOps, beraz, softwarearen garatzaileen eta sistemen administratzaileen arteko integrazioan oinarritzen da.

Benetan aldaketa handia da, eta edozein erakunde edo entitatetako prozesuei nahiz teknologiei eta langileei eragiten die. Laburbilduta, erakunde osoan ekin behar zaie aldaketa horiei, eta ez bakarrik IKTez arduratzen den arloan; hala, **diziplinarteko lana** egiteko modua sortzen da, edo pertsona batzuen iritziz... lan egiteko filosofia berria.

Hainbesteraino non, parte hartzen dutenen lana errazteko, tresna batzuk dauden eskura, software produktu baten bizi-zikloa banatzen

den faseetako batean edo batzuetan erabil daitezkeen tresnak:

1. **Iturri-kodea**: iturri-kodea garatzeko, berrikusteko eta administratzeko tresnak; kodeen bategitea
2. **Eraikuntza**: integraziorako tresnak eta konpilazioaren egoera
3. **Proba**: etengabeko probarako tresnak
4. **Paketea**: paketeen errepositorioa, aplikazioa inplementatu baino lehenagoko banaketa
5. **Merkaturatzea**: aldaketen kudeaketa, onespenak eta bertsioen automatizazioa
6. **Konfiguratzea**: azpiegitura konfiguratu eta kudeatzea
7. **Kontrola**: aplikazioen errendimendua, azken erabiltzailearen esperientzia eta abar monitorizatzea.

Fase horietako batzuetan erabil daitezkeen aplikazioetako batzuk honako hauek dira: Solano CI, Bamboo, Pipeline, Apache Continuum, Hudson, Jenkins, GoCD, CruiseControl edo Anthill (Java proiektuetarako) edo CruiseControl.Net, Team Foun-dation Build .Net-erako; horien eginkizuna exekuzioak kontrolatzea da, beste tresna batzuetan oinarrituta; hona hemen tresna horiek: Ant edo Maven (Java proiek-

[3] **Aldaketaren kudeaketa:** Erakunde batek aldaketa bat egin nahi badu, horren ondorioz eragin handiago edo txikiagoa jasango du (Zuzendaritzan, erdimailako arduradunen artean, azken erabiltzaileen artean, egituran, teknologian...).

Horregatik, aldaketa hori arrakastaz osatu nahi bada, oinarrizkoa eta funtsezkoa da prozesu hori behar bezala kudeatzea, eta modu horretan aukerak aprobetxatzea eta prozesuan sortuko diren mehatxuak gainditzea.

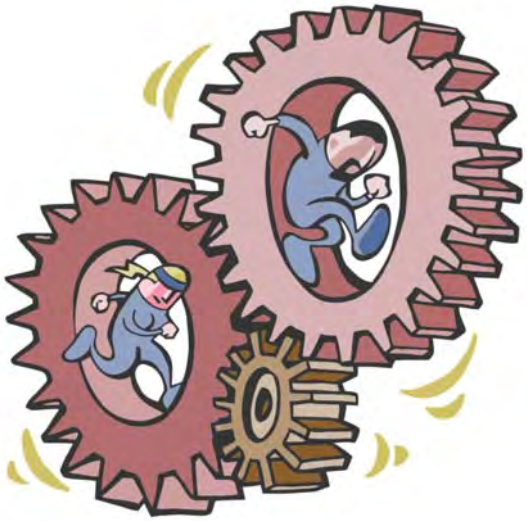
Informazio gehiago nahi izanez gero, Aurrera aldizkariko 30. zenbakian argitaratutako «*Aldaketa (ongi) kudeatzen jakitea*» artikulua kontsulta dezakezue (2008ko ekaina)

tuetarako), edo Nant edo MSBUILD (.Net-erako); horien eginkizunak, berriz, konpilazioak egitea, probak burutzea eta txostenak sortzea dira.

[ikus tresnen eskema grafikoa]

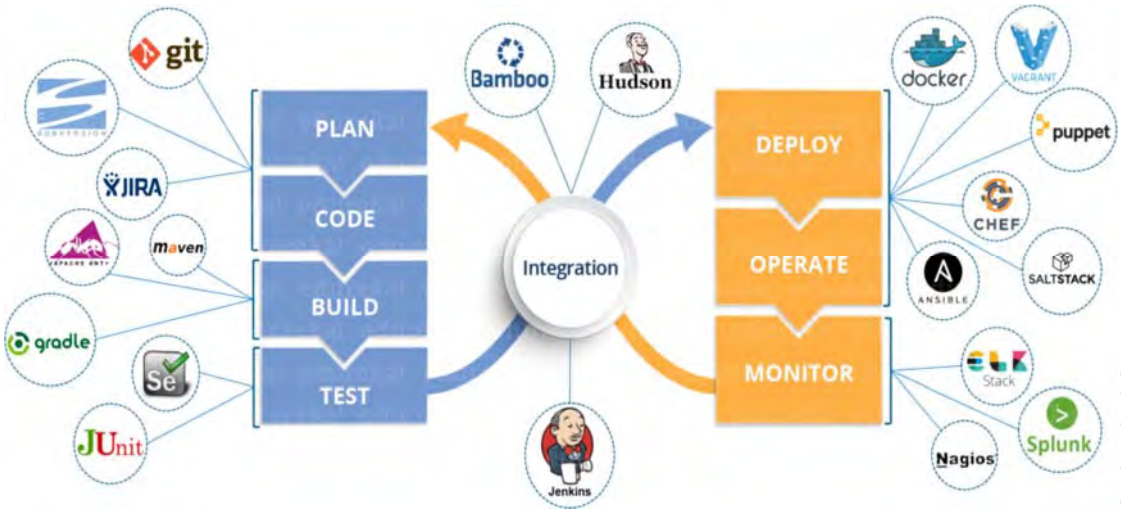
«DevOps-en ideia da metodologia arinen helmena azpiegituren eta sistemen administrazioaren esparrura hedatzea»

Tresna eta teknologia horien guztien bidez, aplikazioen bizi-zikloa automatizatzen da[4]. Orain arte eskuzkoak eta geldoak ziren prozesuetako batzuk —adibidez kodea eguneratzea, ingurune berria prestatzea eta abar—, teknologia berri honi esker azkarragoa eta jarraituagoa den beste modu batean egin daitezke. Gainera, segurtasun-arauak betetzea ere errazagoa da, alderdi horiek prozesuan bertan integratuta daudelako.



ONDORIOA

Lehenago esan denez, DevOps izeneko lan egiteko modu berri honen helburu nagusia da enpresaren beharrizanei arin erantzutea; hori lortzeko, probak egiten dira etengabe, emateak egiten dira etengabe, eta gainbegiratu egiten da etengabe. ❑



[Irudia: Edureka]

[4] **Aplikazioen bizi-zikloa:** aplikazio informatiko bat garatzeko betetzen den prozesua da. Jarraitu beharreko hainbat eredu dago; eredu horietako bakoitzak ikuspuntu diferentea hartzen du prozesu horretan gertatzen diren jarduera batzuk eta besteak antolatzerakoan.

Softwarea garatzeko hainbat eredu espezifiko dago; ezagunenak honako hauek dira:

- ✓ Katekoa
- ✓ Kiribilezkoa
- ✓ Iteratibo eta inkrementala
- ✓ Arina

Interneteko arrisku zaharrak: phishing-a edo identitatearen ordezpena

Interneten gero eta arrisku gehiago dauzkagu zelatan. Hala ere, hainbat azterlanek frogatzen duenez, haietariko gehienak ezagun zaharrak dira, eta, hala ere, arrakasta izaten jarraitzen dute. Ikus ditzagun zenbait adibide, baita halakoak saihesteko modua ere.

Eguberri jaietan gaude, eta sasoi hau aproposa da urte berria dela-eta zoriona opa diguten lagunen (edo enpresen) mezuak jasotzeko. Hain zuzen ere, arrazoi horregatik, kontu handiz ibili behar dugu egun hauetan jasotzen ditugun mezu guzti-guztiekin, izan ere, haien atzean arrisku larria egon daiteke gure «segurtasun informatiko»rako.

Arrazoia da mezu horietako batzuk hackerrek gure sistemetan sartzeko eta informazio pertsonala edo konfidentziala lapurtzeko erabiltzen duten atea izan daitezkeela. Horretarako sarrien erabiltzen diren tekniketako batzuk dira gizarte ingeniaritza[5], troiarrak, *phishing*-a, *ransomware-a*[6]...

Pertsona baten datuak lortzeko metodorik ohikoena troiarrak, harrak edo birusak barnean dituzten posta elektronikoko mezuak bidaltzea da; haiek gure ordenagailua infektatzen dute eta hackerren edo gaizkileen mendean uzten dute.

Halaber, teknologiak aurrera egin ahala, beste pertsona batzuei iruzur egiten dabiltzan pertsonen argitasuna ere handiagoa da eta gailu mugikor berrien «zirrikituetatik sartzen» dira, datuak gure sare sozialetatik ateratzeko edo, besterik gabe, guri telefonoz deituz: inkestatzaileen edo enpresa bateko saltzaileen plantak egiten dituzte, eta haiekin kontratatuta daukagun zerbitzuan aldaketak edo hobekuntzak eskaintzen dizkigute.

2019rako aurreikuspenek diotenez, erasoak bortitzagoak eta bizkorragoak izango dira, hainbesteraino non izen bat sortu den jada, «*vaporworm*[7]», *malware* berri bat definitzeko.

Dena dela, izen bat eduki edo beste bat eduki, teknika horien guztien helburua bat eta bera da, pertsona baten (edo enpresa baten) aurka kanpoko eraso bat egitea datu pertsonalak, konfidentzialak edo pribatuak lortzeko eta, gero, pertsona horren itxurak eginez, kontu korronteak husteko, haren kontura produktuak erosteko eta abar.

Kasu honetan hizpide hartuko dugu *phishing*-a edo nortasunak faltsutzea.

PHISHING-A

Hasteko, zera esango dugu: *phishing*-a **iruzur** mota bat da, eta, horretan, pertsona batek (email bidez) pertsona baten edo enpresa baten itxura eginez zenbait datu eskatzen dizkio erabiltzaileari: kreditu-txartelaren zenbakia, pasahitza...

Jende fidakor askok bere informazio pertsonala *phisher*rei edo iruzurgileei erraz ematen dielako du halako arrakasta «nortasuna lapurtzeak».

[5] **Gizarte ingeniaritza:** Gizarte ingeniaritzak (ingelesezko *Social Engineering*-etik) barnean hartzen ditu hacker batek pertsona bati, azken hori «informazio sentikorra» ematen ari izateaz konturatzen ez dela, informazioa (pasahitz bat, adibidez) ateratzeko edo erabiltzaile horrek ekintza jakin bat egin dezala (adibidez, birus bat barnean duen fitxategi bat irekitzea) lortzeko erabiltzen dituen amarru, engainu eta teknika guztiak.

[6] **Ransomware:** termino hori ingelesezko bi hitz elkartzetik dator: *ransom* (erreskatea) eta *ware*, softwaretik. Programa maltzur bat da (*malware*), gure ordenagailurako sarbidea murrizten eta gure informazioa enkriptatzen duena. Informazio hori berreskuratzeko, hackerrari erreskate bat ordaindu beharko diogu.

[7] **Vaporworm:** *malware* mota berri bat da, fitxategirik erabiltzen ez duena eta har baten antzeko ezaugarriak dituena; bere burua hedatzeko gai da sistema kalteberetan zehar hedatzeko, bere burua Internetetik ezabatzeko eta enpresen aurkako *ransomware* erasoak egiteko.

Erasoaren funtzionamendua oso erraza da:

Iruzurgileak enpresa baten itxurak egiten ditu eta hartzaileari sinestarazten dio datu horiek web ofizial batek eskatzen dizkiola, benetan hala ez den arren. Bitxia da, baina delitu honetan, erasoa egiteko ez da behar tresna eta/edo jakintza bereziegirik. Are gehiago, erabiltzen diren teknikak ez dira berriak, eta aspalditik ezagutzen dira.

«Informazio-sistemen SEGURTASUNA ez dago pertsona bakar baten mendean, eta guztiok jarri behar dugu gure harri-koskorra»

Erasotzaileak hainbat bide erabil dezake azken erabiltzailearengana, hau da, bere biktimarengana, heltzeko:

- ✓ **Posta elektronikoa**: metodorik ohikoena da. Kasu horretan, posta elektronikoko mezu bat bidaltzen zaie pertsona askori, erakunde ofizial baten itxura eginez, erabiltzaile batzuen datuak eskuratzeko. Datuak eskatzeko arrazoiak honako hauek izaten dira: segurtasuna, ordenagailuaren mantentze-lanak, zerbitzua hobetzea, inkesta bati erantzutea edo beste edozein aitzakia, pertsonak bere datu sekretuak eman ditzan. Mezuan inprimakiak ager daitezke, lotura faltsuak, logotipo ofizialak eta abar, mezuak ofiziala dela eman dezan eta susmorik egon ez dadin. Azken erabiltzaileak bere informazioa ematea da helburua, eta (berak jakin gabe) iruzurgileari bidaltzea, horrek geroago iruzurrerako erabil dezan.
- ✓ **Web orria**: kasu honetan benetako erakunde baten (normalean banku baten) web-orriaren itxura du. Erabiltzaileak bere datu pribatuak beteko ditu web faltsu horretan dagoen inprimaki batean.
- ✓ **Telefono-deia**: erabiltzaileak ustezko erakunde baten telefono-deia jasotzen du, iruzurgileak erakunde horren plantak egiten ditu, eta datu pribatuak eskatzen dizkio. Halaxe gertatzen da Errentaren Aitorpena iristen den sasoian: zibergaizkileek —Ogasuneko langileak direlakoan— zergadunei deitu eta kontu korrontearen datuak eskatzen dizkiete, eta hala egin ezean zehapena jasoko dutela esanez mehatxu egiten diete.

Normalean, diruarekin zerikusia duten sasizerbitzuak izaten dira: online bankua, online enkanteak eta kreditu-txartelak. Horrela, erabiltzailearen gakoa jakinda, iruzurgileak nahierara mugi dezake dirua, baita beste banku bateko kontura transferitu ere.

Antzeko eraso bat, nortasunak faltsutuz ere egiten dena, honako hau izan daiteke, adibidez: erakunde bateko erabiltzaile batek «bere» sistema-administratzailearen edo Erabiltzailearen Laguntza Zentroaren [ELZ/CAU] deia jasotzea eta (engainu horren bidez) zuzenean euren pasahitzak eskatzea.

Duela gutxi hedabideetan agertu da ustezko Microsoften zerbitzu tekniko bati buruzko iruzurra; aspaldi erabili zen, baina berriro agertu da. Kasu honetan, zibergaizkileak herritar partikularrekin harremanetan jartzen dira (baita sektore publikoan lan egiten duten pertsonekin ere).

Funtzionamendua honako hau da: normalean, ingelesez gaizki hitz egiten duen pertsona batek telefono-dei bat egiten du eta gurekin harremanetan jartzen da. Hackerrak esaten digunez, gure ordenagailua ustez birus batek infektatu du, ordenagailu horrek Estatu Batuetako Gobernuko erakundeei erasotzen die eta haiek lagundu egingo digute ordenagailua «garbitzen». Horretarako, urruneko kontrolerako software bat deskargatzea eta exekutatzea gomendatzen digu (normalean Teamviewer programa),

ARTIKULUAK

Hona hemen Aurrera aldizkarian ziberdelituei eta segurtasun informatikoari buruz argitaratu diren artikulu batzuk:

- ➢ *«Segurtasuna: birusak»* (Aurrera 3. zk., 2001eko martxoa)
- ➢ *«Gizarte Ingeniaritza»* (Aurrera 13. zk., 2004ko martxoa)
- ➢ *«EJIE: Birusak eta eraso informatikoak»* (Aurrera 14. zk., 2004ko ekaina)
- ➢ *«Ransomware: gorantz ari den mehatxua»* (Aurrera 55. zk., 2016ko martxoa)
- ➢ *«Datu-lapurreta, interneten»* (Aurrera 61. zk., 2017ko iraila)
- ➢ *«Zibersegurtasunerako Euskal Zentroa (BCSC)»* (Aurrera 63. zk., 2018ko martxoa)

gure saiorako identifikazioa eskatzen digu eta baimena eskatzen digute geure ordenagailuaren kontrola hartzeko. Hortik aurrera gure ordenagailuaren informazioa zifratzen duen software bat jaisten dute eta kasu honetan «erreskate» bat eskatzen digute informazio hori berreskuratu ahal izateko. «Erreskatea» «bitcoin»etan ordainduko da, jarrai ez diezaieten. Eta gertatu ohi denez, ordaindu arren, ordenagailuaren informazioak zifratuta jarraituko du, eta, beraz, haien mendean jarraituko dugu.

[8] **GureSeK:** GureSeK (euskarazko *«Gure Segurtasun Kudeaketa»*tik dator) deritzo Euskal Autonomia Erkidegoko Administrazio Orokorrak eta beraren erakunde autonomoek (sailek eta erakunde autonomoek) herritarrei ematen dizkieten zerbitzu elektronikoen segurtasuna kudeatzeko erabiltzen den informazioaren segurtasunaren kudeaketarako prozesu edo sistemari (ISKS).

KONTRANEURRIAK

Arrisku horiek saihesteko (edo haien eragina ahalik eta gehien murrizteko) modurik onena ongi informatuta egotea da. Horretarako, Eusko Jaurlaritzak, Segurtasun eta Pribatutasun Batzordeak koordinatzen duen **GureSeK**[8] izeneko **prestakuntza-plan**aren barruan, azken hilabeteetan simulakro batzuk egin ditu, mezu faltsuak erabiliz.

Hona hemen lortutako emaitzen laburpena:

2017an, Eusko Jaurlaritzak bere langile guztiei (guztira 5.960 pertsona dira) posta elektronikoko hiru mezu faltsu bidali zizkien, *phishing* eraso baten itxurak eginez.

Lehenengo mezuan, adibidez, azken erabiltzeari eskatzen zitzaion lotura batean klik egin zezala (lotura mezuan bertan agertzen zen), bere pasahitza kanpoko webgune batean alda zezan.

«Arrisku horiek saihesteko modurik onena ongi informatuta egotea da»

Bigarren kasuan, posta elektronikoko mezuak Correos enpresaren itxurak egiten zituen, eta orri batean sartu eta gure datuak emateko esaten zigun, pakete bat jaso ahal izateko.

Eta urte hartako hirugarren eta azken mezuan, posta elektronikoko mezu bat bidali zen Amazon enpresa multinazionalaren izenean; mezu hartan erabiltzaileari oparitxartel bat eskaintzen zitzaion, hark datu pertsonalak ematearen truke.

Aurten ere, 2018an, posta elektronikoko mezu faltsuen beste kanpaina bat egin da, eta kanpaina horren emaitzak honako hauek izan dira:

Azken kanpaina 2018ko azaroaren 5etik 9ra egin zen. Kasu honetan, apeu gisa **«Microsoft corps. Keys» faltsu batek igorritako ustez alerta bat** zekarren posta elektronikoko mezua erabili zen.

Mezu hori Eusko Jaurlaritzako 5.435 ordenagailutan jaso zen guztira, eta mezuan agertzen zen lotura faltsuan 1.620 pertsonak egin zuten klik (% 29,81ek).

Erabiltzailearen Laguntza Zentroak mezu susmagarri horri buruzko abisua emateko guztira 133 gorabehera edo dei jaso zituen (% 2,45). Horietako gehienak hilaren 6an, asteartean jaso ziren (hori dela-eta, Erabiltzailearen Laguntza Zentroak, deitzen ari ziren erabiltzaileei arreta egiteko eta zerbitzuaren gainerako atalak ez saturatzeko, grabaketa bat prestatu zuen).

ONDORIOA

Gero eta kontzientzia handiagoa dago, eta jasotako emaitzak batezbestekotik behera daude antzeko beste erakunde batzuekin alderatuta, baina atera diren ondorioetako bat da oraindik pertsona asko amarruan «jausten» direla eta posta elektronikoko mezuan bidaltzen dizkieten lotura faltsu horietan klik egiten dutela.

Horregatik, ekimen edo simulakro horien guztien azken helburua (eta etorkizunean egin ahal direnena) da **segurtasunari buruzko kontzientzia sortzea** gure erakundeko langile guztien artean (baita ordenagailu bat edo beste gailu elektroniko bat zuzenean erabiltzen ez dutenen artean ere); izan ere, informazio-sistemen SEGURTASUNA ez dago pertsona bakar baten mendean, eta guztiok ekarri behar dugu gure harri-koskorra. ❑

[9] **Segurtasunari buruzko prestakuntza**: IVAPek eskaintzen dituen ikastaroen katalogoaren barruan daukagu *«Informazioaren segurtasuna Administrazio elektronikoaren arloan»* izenburukoa (online formatuan, 10 orduko iraupenarekin). Honako hau da ikastaro horren gai-zerrenda:

- I. atala: Segurtasunaren kudeaketa
  1. Informazioaren segurtasunaren arloko kontzeptuak
  2. Segurtasun Eskema Nazionala
  3. Pertsonen eskubideak administrazio publikoekiko harremanetan
  4. Sinadura elektronikoa
  5. Segurtasun kopiak
- II. atala: Kasu praktikoak
- III. atala: Lanpostu korporatiboa
- IV. atala: Arau-esparrua

Informazio gehiago nahi izanez gero, webgune honetara joan:

www.ivap.eus

Gomendioak

Hona hemen kontuan hartu beharreko oinarrizko aholku batzuk, arrisku horiei buruzko informazioa edukitzeko, edo egoera susmagarri bat detektatzen dugunean egin beharreko urratsak:

- ✓ Segurtasunari buruzko hitzaldietara edo prestakuntza-ikastaroetara joatea.[9]
- ✓ Fitxategi erantsiak sekula ez irekitzea (bidaltzailea ezaguna bada ere), aurretiaz eskatu ez baditugu, batez ere .exe, .doc, .wls, .vbs edo .xls fitxategia bada.
- ✓ Posta elektronikoko mezuei erantsitako URLak (web helbideak) kontuz maneiatzea. *«Phishing»*-ak URL faltsuak erabiltzen ditu erabiltzaileak erakartzeko eta Interneteko orri jakin batzuk bisitatzera bultzatzeko. Orri horiek webgune legitimoen itxurak egiten dituzte informazio sentikorra eskatzeko, adibidez pasahitzak edo kontu-zenbakiak eskatzeko.
- ✓ Ez eman sekula telefono bidez sarearen ezaugarri teknikoei buruzko informaziorik, ezta sarearen kokaleku fisikorik edo sarearen ardura duten pertsonen izenik ere, eta are gutxiago ordenagailuen erabiltzaile-izenei eta pasahitzei buruzko informaziorik. (gomendagarria da aurretiaz

informazio hori eskatzen duen iturria benetakoa dela egiaztatzea).

- ✓ Dokumentazio teknikoa (edo informazio pertsonala jasotzen duena) suntsitu, ez bota sekula zaborrera. Ohikoa da paperontzira datu konfidentzial pila bat botatzea konturatu gabe (edo gure *password*-a eta abar dakarren paper bat teklatuaren azpian edo tiraderan uztea).
- ✓ Jokamolde susmagarrien berri ematea (adibidez, baimenik ez duten pertsonek erabili behar ez duten ordenagailu bat erabiltzen dutela ikusten badugu, eta abar)
- ✓ Informazio jakin bat baimenik gabe jakin nahi duen pertsona bat gurekin harremanetan jartzen bada, berehala jakinarazi beharko diogu Erabiltzailearen Laguntza Zentroari [ELZ/CAU] edo gure saileko segurtasuneko arduradunari, eta haren jarraibideak bete, jaso dugun deiaren edo posta elektronikoko mezuaren jatorria zein den jakin ahal izateko.

ALBOAN:

Eusko Jaurlaritzaren Ibilgailu atala. Beste urrats bat zerbitzua digitalizatzeko

«Modulu berriak Eusko Jaurlaritzaren PLATEA Plataforma Teknologikoko soluzio batzuk erabiltzen ditu»

Apirilaren 11ko 71/2017 Dekretuak, Gobernantza Publiko eta Autogobernu Sailaren egitura organikoa eta funtzionala ezartzekoak, jasotzen duenez, **Zerbitzu Orokorretako Zuzendaritzar**en eskumenetako bat da *«Administrazioko Ibilgailuen Ataleko zerbitzuak eta ibilgailuak antolatzea, kudeatzea eta administratzea»*.

DIGITALIZAZIOA

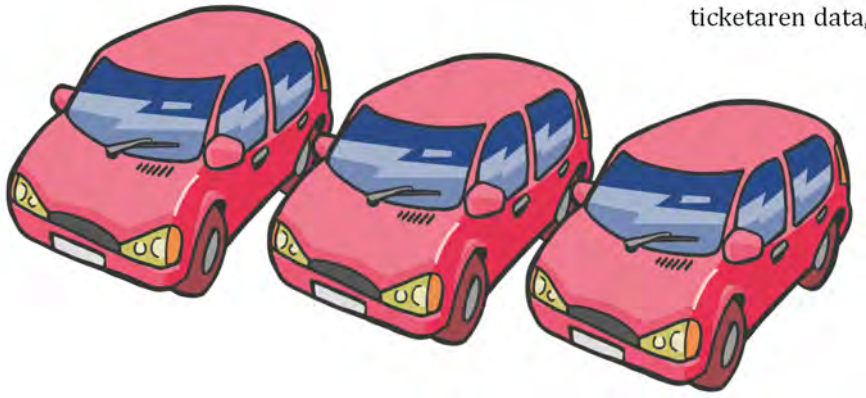
Ibilgailu Atalaren zerbitzuak gaur egun gutxi gorabehera **600 ibilgailu** kudeatzen ditu. Bere eginkizun nagusia da ibilgailu horiek Eusko Jaurlaritzako pertsonen eskura jartzea, lan arrazoiengatik behar badituzte. Kasu horietan **M05J aplikazioa**ren bidez eskatu beharko da. Aplikazio hori Jakinan dago erabilgarri.

Hilero, auto bat modu jarraituan esleituta daukaten pertsonek Ibilgailu Ataleko Zerbitzuari paper formatuan igortzen dizkiote egin dituzten eta justifikatu behar diren gastuen **jatorrizko ticketak eta/edo ordainagiriak**. Gero, Ibilgailu Atalaren Zerbitzuko arduradunak ticket horietan agertzen diren kontzeptu guzti-guztiak (data, zenbatekoa eta abar) aplikazioan sartzen ditu, baliozkotzeko.

Prozedura horrek behin edo behin arazoren bat sortu du, adibidez ticketik ekartzen ez denean, edo ticketak behar bezala heltzen ez direnean.

Zerbitzua nahiz zerbitzu horren kudeaketa hobetzeko, Baliabide Orokorren Zuzendaritzak duela gutxi hobekuntza nabarmena garatu du **M05J aplikazioa**n: utilitate edo modulu berri bat sartu du, *«Gastuen justifikazioa»* izenekoa; horren helburu nagusia da sailek eta Baliabide Orokorren Zuzendaritzak papera (ticketak eta ordainagiriak) trukatzeari uztea.

Hobekuntza horri esker, orain modu jarraituan auto bat esleituta daukaten pertsonek (gutxi gorabehera 300 dira) euren gastuen datuak aplikazioan zuzenean sar ditzakete jada; hona hemen datu horiek: ticketaren data, egotzi beharreko kontzeptua, gastuaren zenbatekoa etab. Eta hori, **paper-euskarriko agiri bat ere trukatu behar izan gabe**; izan ere, ticketak edo frogagiriak espedienteari erantsiko zaizkio, eta aplikazioan bertan gordeta geratuko dira. Gainera, erabiltzaile bakoitzak sartutako ticketen



historia kontsultatu ahal izango du.

Modulu berri honi esker, hainbat gauza hobetzen da: hutsegiteak saihesten dira datuak sartzerakoan; sailek eta Baliabide Orokorren Zuzendaritzak euren artean papera trukatzeari uzten diote erabat; ticketak galtzea eragozten da, eta abar.

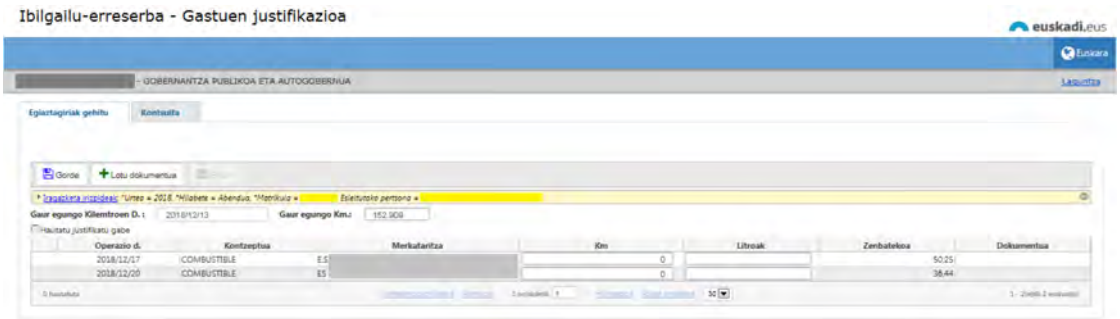
Funtzio berri hori apurka hedatuko da, Eusko Jaurlaritzako langile guztiek erabili ahal izan dezaten.

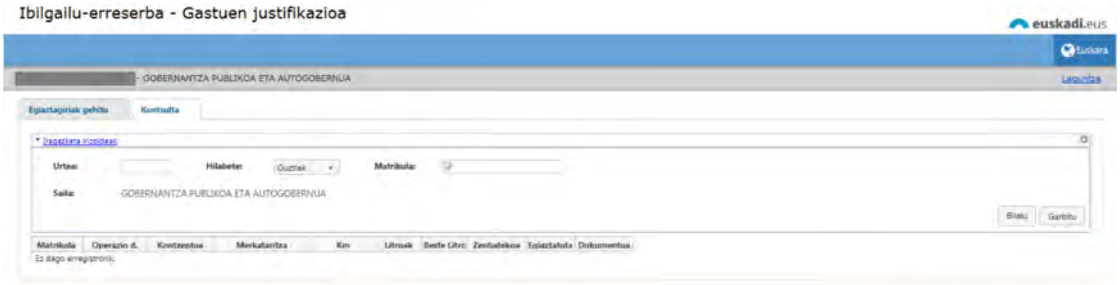
ALDERDI TEKNIKOAK

Ikuspuntu teknikoago batetik, zera esan behar da: modulu berria EJIE sozietate publikoko langileek garatu dute, J2EE garapen-plataforma erabiliz, UDA Framework-aren azken bertsioan oinarrituta. Weblogic 11g-en euskarria dauka (aplikazio-zerbitzari gisa), eta Oracle 12c erabiltzen du datu-baseen zerbitzari gisa. Segurtasunaren kudeaketa, hau da, erabiltzaileen identifikazioa, XLNets-ekin integratuta dago, Eusko Jaurlaritzaren JASO intranetean erabiltzeko. Gainera, sailek eta erakunde autonomoek eransten dituzten agiriak Eusko Jaurlaritzako Dokumentuak Kudeatzeko Sisteman, dokusi-n, integratzen dira.

Dena dela, Ibilgailu Atalaren M05J aplikazioaren hobekuntzak harago doaz; izan ere, datorren urtean funtzio berriak garatzea aurreikusten da; funtzio horiek planifikatzen ari dira, eta apurka aurkeztuko dizkizuegu. ❑

«Proiektuaren helburua da sailek eta Baliabide Orokorren Zuzendaritzak euren artean paperik ez trukatzea»





Araudia:

300/1999 Dekretua, uztailaren 27koa, Administrazioko Parke Higikorra arautzen duena

Kontrazala!!

66. zk.

2018ko abendua

IXTEKO

LibreCon2018

Iragan azaroaren 21ean eta 22an **Bilbo**ko Euskalduna Jauregian LibreCon-en aurtengo edizioa egin zen, software askeari eta kode irekiari buruzko enpresa-topaketarik handiena.

Bi egun horietan *open source* soluzioak eskaintzeari dagokionez berritzaileenak diren enpresetako batzuen aurkezpenak ikusteko aukera izan genuen.

Eusko Jaurlaritzak eta EJIE Informatika Elkarteak ekitaldi horretan **mahai-inguru** batean parte hartu zuten. *«Liberatzea edo berrerabiltzea, non jarri behar du arreta administrazio publikoak?»* izenburu zeukan mahai-inguru hori Eusko Jaurlaritzako sailburuordeak, Nerea Karmele López-Uribarri Goicoleak, moderatu zuen. Euskadiko Kontratazio Publikoko Plataformaren arrakasta azaldu zen, eta Eusko Jaurlaritzak softwarearen berrerabileraren arloan indarreko araudia betetzeko egin behar dituen hurrengo urratsei buruz gogoeta egin zen.

Halaber, EJIEk (Oscar Guadillaren eskutik) *«Blockchain: Administrazio Publikoaren elkarlan-eredu berria»* izenburuko **ponentzia** eman zuen. Ponentzia horretan, garatzen ari diren ekimenetako batzuk eta beste administrazio batzuekiko balizko elkarlan-proiektuak azaldu ziren.

Info+: http://www.librecon.io

PROTAGONISTAK

Hedy Lamarr, asmatzailea

Hedy Lamarr aktore, asmatzaile eta telekomunikazioetako ingeniaria (1914-2000) azaroaren 9an jaio zen. George Antheil musikariarekin batera espektro hedatuaren —telekomunikazioetan erabiltzen den modulazio-teknika baten— lehenengo bertsio bat asmatu zuen. Hain zuzen ere, urtero, azaroaren 9an, **Asmatzailearen Nazioarteko Eguna** ospatzen da haren omenez.

Bere lehenengo senarra Europako itzalik handieneko gizonetako bat izan zen, eta Bigarren Mundu Gerraren aurretik, Hitlerren eta Mussoliniren armategien horniduraz arduratu zen. Horregatik, ohorezko ariar izendatu zuten, jatorriz judutarra izan arren.

Hedyk ezin zuen deus ere egin bere senarraren baimenik gabe; horregatik, bere bizimoduaren hutsaltasun jasanezinaz nazkaturik, berriro ingeniaritza karrerari ekin zion. Lan-bileretara joaten zen, eta bilera horietan, bide batez nazien armagintza arloko azken teknologiaren ezaugarriei buruzko informazioa ikasi eta bildu zuen.

AEBetara ihes egin ostean, Hedyk bere ingeniari prestakuntza berriki sortutako *National Inventors Council*-en esku jarri zuen. Bere lagun Antheilekin batera, 1941eko ekainean, *Secret Communication System* izenekoaren patentea erregistratu zuten.

Militarren artean patente horri buruzko interesa piztu zen, baina askotariko iritziak sortu ziren. AEBko itsas armadak zioenez, sistema hura kaltebera zen neurriz gain, erabiltzen neketsua ere bai, eta, beraz, proiektua baztertu egin zuen. Lamarr eta Antheil hartaz ahaztu ziren, eta zinematografiara itzuli ziren. 1957an, ordea, Estatu Batuetako Silvania Electronics Systems Division enpresako ingeniari batzuek garatu egin zuten Hedyk eta Georgek patentatutako sistema, eta Gobernuak sistema hori transmisio militarretarako egokitu zuen, patentea iraungi eta hiru urtera.

[Artikuluaren laburpena. Hemen jatorrizkoa https://mujeresconciencia.com/2015/11/30/hedy-lamarr-la-inventora/