EUSKO JAURLARITZA
GOBIERNO VASCO

Aurrera!

33. zk.

2009ko martxoa

Informatika eta Telekomunikazioetako Teknologia Berriak jendarteratzeko aldizkaria

Bulego Teknologikoak argitaratua
Informatika eta Telekomunikazio Zuzendaritza

AURKIBIDEA

Segurtasuna. Hitz horrexek laburtzen ditu *Aurrera!* buletin berri honen lehenengo bi gaiak.

"Kanpoko gailu mugikorren segurtasuna" da lehenengoaren izenburua, eta gailu mugikor berrien segurtasuna kontuan hartzen ez duten erakundeen arazoak azaltzen ditu.

Bigarren gaiak, berriz, **"Identitateen kudeaketa"** du izenburu, eta gaur egun erakunde handiek aplikazioetara sartzeko erabiltzaileen sarbide-kode eta -pasahitz guztiak kudeatzeko dituzten arazoak lantzen ditu. Zenbait kontzeptu jorratzen ditu artikuluak; besteak beste, erabiltzailearen profilaren *bizi-zikloa*, *metadirektorioa* edo *«single sign-on»* deritzona.

"Alboan" atalaren barruan, **Euskal Herriko Agintaritzaren Aldizkariarekin** (EHAA) lotutako azken berrikuntza jakinaraziko dizuegu: urtarrilaren 1etik aurrera, EHAA ez da paperezko euskarrian argitaratuko, eta, beraz, formatu elektronikoan bakarrik eskura daiteke. Aldizkariak izandako aldaketa garrantzitsu horren haritik, erabakia zergatik hartu den, zer irtenbide teknologiko hartu diren (sinadura elektronikoa) eta gaiari buruzko beste zenbait datu interesgarri ere azalduko dizkizuegu.

Bestalde, "Laburrak" atalean, PuntuEus elkarteak interneten **.eus domeinua** martxan jartzeko bultzatutako ekimenaren berri ematen dugu. Bigarrenik, EJIEk egindako azken erosketa aipatzen dugu. Izan ere ***superordenagailu*** bat erosi du. Ekipo berri horrek zerbitzua emango die, besteak beste, meteorologia-zerbitzuari eta Euskal Herriko Unibertsitateari, goi-mailako ikerketa klimatologikoen garapenerako.

Eta, bukatzeko, konturatuko zinetenez, ale honetan *Aurrera!* buletinaren diseinua eguneratu dugu, hiru urtez aurpegi bera erakutsi ondoren. Aldaketa horren bidez, aldizkaria erakargarriago egitea eta erabiltzaileek artikuluak errazago irakurri ahal izatea lortu nahi dugu. Alde horretatik, aldizkariaren diseinuaz eta edukiaz arduratzen den talde teknologikoak pozik jasoko ditu zuen iritziak eta iradokizunak.

Kanpoko gailu mugikorren segurtasuna (lapurretak eta galerak)

Gaur egun, teknologia mugikorrek abantaila nabariak eskaintzen dizkiete pertsona, enpresa edo erakundeei, baina, aldi berean, horrelako gailuak erabiltzeak arrisku handiak ditu. Izan ere, erakunde askok ez dute martxan jartzen gailu horien erabilerari buruzko segurtasun-politikarik.

HIZTEGIA

[1] **PDA**: ***P**ersonal **D**igital **A**ssistant* (morroi digital pertsonala) ingelesezko kontzeptuaren laburdura. Eskuzko gailua da, jatorrian agenda elektronikoa izandakoa (egutegia, kontaktu-zerrenda, oharrak eta oroigarriak), eta idazketa ezagutzen duen sistema bat du. Gaur egun, etxeko eta enpresako ordenagailu gisa erabiltzen da posta elektronikoa ikusteko, interneten nabigatzeko, fitxategiak irakurtzeko, multimedia-edukiak erreproduzitzeko, ordenagailu pertsonal batekin sinkronizatzeko, GPS bidez nabigatzeko...

(Informazio gehiago nahi izanez gero, ikus 18 zk.ko *AURRERA* buletina, "*Mugikortasun -irtenbideak*" izenburua duena).

Mugikortasun-teknologiak asko hedatzen ari dira norbanakoen artean nahiz enpresetan. Telefonia mugikorraren arrakasta da horren lekuko, hazkunde esponentziala izan baitu denbora laburrean. Teknologia horiek aukera ematen dute bizitza profesionala eta pertsonala bateratzeko, eta, hain zuzen, hori da arrakastaren gakoa.

Teknologia mugikorrak erabili ahal izateko, hainbat gailuz baliatzen gara ("gailu eramangarriak"); adibidez, telefono mugikor adimendunak (*smartphones*), ordenagailu eramangarriak, USB memoriak (*USB flash drives, pen-drive´s* edo *memory sticks* ere esaten zaie), kanpoko disko eramangarriak, PDAk[1], etab.

Erakundeek prest egon behar dute, batetik, zerbitzu mugikor horiek eskaintzeko eta, bestetik, horien erabilerak sor ditzakeen arriskuak kontrolatzeko eta, hala, mundu osoko terminal mugikorrek dituzten aldaketen abiadurari eta horien heterogeneotasunari aurre egiteko.

INFORMAZIO-GALERAK

Batez ere, informazio-galerek sortzen dituzte erakundeetako segurtasun-arazo larrienak. Gainera, erakundearen izen ona kalte dezakete, erakundearen aurkako legezko akzioei eta sor daitezkeen arazo ekonomikoei aurre egin beharraz batera.

Hainbat faktorek eragin ditzakete datu-ihesak, baina, batez ere, bi hauek:

. Nahita eragindakoek

. Hutsegite, lapurreta edo galerek eragindakoek

> "Gartner Group-en arabera, 2009an, gailuen %25 baino gehiago PDAk eta telefono mugikor adimendunak izango dira."

Azken horiek (hutsegiteak, lapurretak eta galerak) uste baino maizago gertatzen dira, eta, gainera, ez dira eraso tekniko konplexuekin egiten.

Erakunde askok aitortzen dute ez dutela segurtasun-estrategiarik arazo horiei aurre egiteko, nahiz eta badakiten jabetza intelektuala eta isilpeko datuen segurtasuna oinarri-oinarrizkoak direla negozioak arrakasta izan dezan. Askotan, datuen galerarekin lotutako arazoak konpontzeko estrategiaren bat dagoenean ere gertatzen dira horrelakoak, eta, beraz, badirudi gailu mugikorren babesa ez dela behar den arduraz gauzatzen.

Oro har, **segurtasun-politika eta -prozedurak** erakundea kanpoko erasoetatik babesteko izaten dira, baina, normalean, ez dituzte kontuan izaten barnetik etor daitezkeen mehatxuak (adibidez, arduraz baliatu beharreko datuak dituen USB memoria bat galtzea barne-mailako mehatxutzat har daiteke). Hala, kanpoko erasoak dagoeneko

ez dira enpresen segurtasunaren aurkako mehatxurik larriena, baizik eta barneko informazio-ihesak.

Komunikabideetan oso maiz entzuten dira arduraz baliatu beharreko datuen ihesak izan dituzten enpresa garrantzitsuei buruzko berriak, enpresako edo azpikontratatutako langile batek

"Gailu eramangarriak enpresa-segurtasunaren «zulotzat» hartzen dira."

gailu mugikorrak galdu dituelako. Adibidez, Erresuma Batuko gobernuak lau milioi herritar ingururen informazioa galdu zuen urte bakar batean, CDak galtzeagatik eta ekipo eramangarriak lapurtzeagatik.

Beraz, argi dago ihes horiek saihesteko —agian, ezinezkoa da galtzea edo lapurtzea saihestea, baina, ondoren, datuetara sarbidea izatea galaraz daiteke— segurtasun-politikak eta -prozedurak jarri behar direla martxan, batetik, komunikazioak seguruak izateko (adibidez, VPN[2] bidez) eta, bestetik, gailu mugikorrak baimendutako pertsonek bakarrik erabiltzeko eta, horrez gain, gailuan jasotako datuen babesa bermatzeko (baimendu gabeko erabilerak edo irakurtzeko saiakuntzak, galera edo lapurreta kasuan). Horretarako, tresna espezializatuak erabili behar dira.

Orain arte, perimetro jakin baten babesa zuen oinarri segurtasunak, baina, mugikortasuna dela -eta, perimetro hori izugarri "hedatu" da.

Beheko taulan azaltzen den bezala, Informazioaren Segurtasunerako Kudeaketa Sistemen (ISKS/SGSI) bidez —adibidez, ISO 27002:2005 eredua—, informazio-aktiboen arriskua murriztu nahi da, aurrez arriskuaren azterketa eta ebaluazioa eginez eta, ondoren,

ISO 27002:2005

ISO 27002:2005 eredua da *Informazioaren Segurtasunaren Kudeaketa Sistema (ISKS/SGSI)* ezartzeko estandarra (**nazioarteko estandar ziurtagarria**). Eredu horren bidez, informazio-aktiboen arriskua "murriztu egiten" da. Horretarako, **arriskuaren azterketa eta ebaluazioa** egiten da aurrez. Hala, erakundearen eragiketak egiten jarraitzea ziurtatzen da, eta erakundearen informazio-aktiboak kaltetzeko arriskua minimizatzen.

Aurrez definitutako arrisku-kudeaketaren eremuan aplikatzen da estandarra, eta argi izan behar da eremu horren barruko salbuespenek bateragarriak izan behar dutela arauak ezarritakoarekin.

Pauso hauek eman behar dira arriskuaren maila ebaluatzeko (arriskuen analisia):

- ✓Informazio-aktiboak identifikatzea
- ✓Identifikatutako aktiboak tasatzea
- ✓Aktibo bakoitzaren mehatxuak identifikatu, eta mehatxu hori gauzatzeko probabilitatea kalkulatzea
- ✓Ahultasunak eta mehatxuek ahultasun horiei eragiteko aukera identifikatzea
- ✓Aktiboek duten arrisku-maila kalkulatzea
- ✓Mehatxuen lehentasunak ezartzea, arrisku-mailaren arabera

Lan horiek egin ondoren, arriskua ebaluatu behar da, irizpide hauek erabiliz:

- ✦Arriskuaren inpaktu ekonomikoa
- ✦Erakundeak hasierako egoera berreskuratzeko behar duen denbora
- ✦Arriskua gauzatzeko aukera
- ✦Enpresaren jarduerak eteteko aukera

Arriskua ebaluatu eta arriskuarekin lotutako aktibo garrantzitsuak kontabilizatu ondoren, estrategia egokia aukeratu behar da arriskua minimizatzeko.

Lau bide har daitezke arriskuari aurre egiteko:

-Murriztea
-Onartzea
-Transferitzea (adibidez, aseguru-etxe baten bidez)
-Saihestea

HIZTEGIA

[2] **VPN**: *Virtual Private Network* edo "sare birtual pribatua" kanal publikoen bidez eraikitako sarea da. Adibidez, sistema batzuek internet bidez sareak eratzeko aukera ematen dute informazioa garraiatzeko. Sistema horiek enkriptazioak eta bestelako segurtasun-sistemak erabiltzen dituzte, sarea baimendutako erabiltzaileek bakarrik erabiltzeko eta informazioa ez atzemateko.

(ikus 1 zk.ko eta 2 zk.ko *AURRERA* buletinetako "*E-business*" eta "*Windows 2000-ren migrazioa*" artikuluak, hurrenez hurren).

arriskuari aurre eginez ("domeinuak", "kontrol-helburuak" eta "kontrolak" erabiliz).

INFORMAZIOA BABESTEKO TEKNOLOGIAK

Beraz, ezinbestekoa da sistema eramangarriei segurtasun-neurriak ezartzea.

Lehen azpimarratu dugunez, helburua da galdu edo lapurtutako gailu mugikor baten edukietara sartzeko eragozpenak jartzea hura eskuratu duenari.

Gaur egun, fabrikatzaile adina teknologia ditugu merkatuan, eta horietako bakoitzak eremu jakin bat hartzen du.

> "Gailu mugikorrei dagokienez, pasahitz-, zifratze- eta enkriptatze-sistemek mahaigaineko ordenagailuen ereduak betetzen dituzte, besterik gabe."

Erabiltzaileen kautotzea

Erabiltzaileak kautotzeko aplikazioak dira lehenengo segurtasun-maila edo oinarrizkoa. Abiapuntu horretatik IT (informazio-teknologiak) sailek gailuen segurtasuna handitu dezakete politika eta ziurtagiri berrien bidez, memoria-txartelak eta diskoak enkriptatuz eta gailu jakin bateko informazioa urrutitik edo bertatik bertara ezabatzeko aukerak aztertuz.

Pasahitzen erabilera

Pasahitzek beste segurtasun-maila bat ematen dute. Izan ere, ziurtatzen dute ekipo horretara sartzeko baimena duen erabiltzailea dela ekipoa erabiltzen ari dena, "izena" eta "pasahitza" sartzeko interfaze klasikoaren bidez (mahaigaineko ekipo korporatibo edo pertsonaletan egiten den bezala).

Informazioa zifratzea

Gailu mugikorrekin lotutako sistema eragile gehienek zifratzeko tresnak eskaintzen dituzte (adibidez, Windows Mobile sistemak CryptoAPI[3] tresnetan oinarritutako zifratze-zerbitzuak eskaintzen ditu).

Disko gogor eramangarri eta USB memoria askok programa jabeak izaten dituzte, horietan jasotako datuak enkriptatu ahal izateko.

Sistema biometrikoak

Sistema biometrikoak (giza gorputzaren ezaugarri berezien ebaluazioa) modan daude gailu mugikorren segurtasunaren arloan. Hasieran, segurtasun-sistemetan eta presentzia-kontroletan integratu ziren, eta, gaur egun, gailu horietara guztiz egokituta daude. Sistema biometrikoek "datu-base" bat behar dute pertsona bakoitzarekin lotutako ereduak biltzeko, eta abantaila hauek dituzte sistema klasikoekin alderatuta:

- Beharrezkoa da erabiltzailearen presentzia fisikoa
- Ez da beharrezkoa pasahitz bat gogoratzea edo txartel bat izatea

SISTEMA BIOMETRIKOEN TAXONOMIA

Nagusiki, hiru sistema biometriko mota daude:

✓ Hatz-marka identifikatzea

✓ Irisaren irakurketa

✓ Aurpegia eskaneatzea

Lehenengoa da ezagunena (**hatz-marka bidez identifikatzea**), eta bi modutara egin daiteke: hatzarekin presioa eginez edo hatza arrastatuz. Lehenengo, erabiltzailearen hatz-marka erregistratu behar da, hatza sentsorean ondo kokatuz edo arrastatuz. Hala, sentsoreak hatza digitalizatzen du eta hatz-markaren irudia egiten du. Ondoren, irudiaren puntu jakin batzuk jasotzen ditu, eta algoritmo baten bidez, datu numeriko bihurtzen ditu puntu horiek. Hain zuzen, datu horiek enkriptatzen eta gordetzen dira, eta ez irudia. Sistemara sartzean, operazio bera egiten da, eta jasotako datu matematikoa aurrez datu-basean gordetakoarekin konparatzen da.

Ahurreko zainen sarearen mapa egiten duen sistema ere erabil daiteke, oraindik ezezaguna den arren (adibidez, Fujitsu-ren Palm Secure ekipoak kontaktu gabeko ezagutze-teknologia hori erabiltzen du).

Irisa irakurtzeko eta **aurpegia eskaneatzeko** teknikak, berriz, konplexuagoak dira, eta ezezagunagoak. Hala eta guztiz ere, hainbat ekipok (adibidez, Asus U6), webcam integratu

HIZTEGIA

[3] **CryptoAPI**: Ingelesezko *Cryptographic Application Programming Interface* kontzeptuaren laburdura da. Aplikazioak programatzeko interfazea (API) da, Microsoft Windows-en parte gisa hornitzen dena, eta eskaintzen dituen funtzioen bidez, aplikazioetako datuak malgu zifratu edo sinatu daitezke, erabiltzailearen datu pribatu garrantzitsuak eta isilpekoak babestearekin batera.

baten bidez eta SmartLogon programa erabiliz, jabearen aurpegia ezagutzen dute, eta sarbide segurua ziurtatzen dute aurpegia eskaneatuz.

DLP TEKNOLOGIA: ARDURAZ BALIATU BEHARREKO INFORMAZIOAREN IHESAK NOLA SAIHESTU

Informazio-segurtasunaren arloko teknologiek badute beste teknologia berritzaile bat, duela gutxi ezagutarazi dena: DLP (*Data Loss Prevention* edo *Data Leak Protection*). Berez, ez da segurtasun-mekanismo eta -prozedura desberdinen batura besterik. **Arduraz baliatu beharreko edo isilpeko informazioaren ihesak saihestea du helburu** teknologia horrek, hau da, barne-erabiltzaileen bidez, informazio hori erakundetik ez ateratzea lortu nahi du, funtsean.

Funtzionamendua

Informaziora sartzeko, informazioa transmititzeko edo kopiatzeko modua kontrolatzen du. Aurrez, informazioa eta datuak edukiaren arabera sailkatzen dira, eta, irteerako artxiboen edukiak eta testuingurua aztertu ondoren, sistemak dagokion ekintza aplikatzen du (monitorizatzea, zifratzea, blokeatzea, berrogeialdia...). Politika hori erakundearen barruan bakarrik erabil daiteke. DLP teknologiekin, babesaren perimetroaren barruan ez daude babestu beharreko baliabideak bakarrik, baita babestu beharreko edukiak ere.

GAILU MUGIKORRAK BABESTEKO GOMENDIOAK

Teknologiak babes-metodo desberdinak konbinatzeko joera du, eta, beraz, ezin konta ahala aukera daude segurtasunerako (adibidez, pasahitzak eta kode zifratuak kudeatzeko segurtasun-irtenbideak teknika biometrikoekin konbinatuta eta hardwarean eta softwarean oinarrituta).

Bestalde, malware[4]-arekin lotutako arazoei dagokienez, azpimarratu behar da, neurri handi batean, erabilitako gailu-motak, babeserako instalatutako softwareak, definitutako segurtasun-politikak eta azken erabiltzaileen kudeaketa arduratsuak baldintzatzen dituela arazo horiek.

Oinarrizko neurri hauek hartzea gomendatzen da:

- ✓Segurtasun-politika eta -prozeduretan ingurune mugikorra hartu behar da kontuan (ISKS/SGSI sistema bat ezartzen badugu, aurreratuta daukagu lanaren zati handi bat).
- ✓Erabiltzaileentzako jardunbide egokien gida egitea komeni da, eta trebakuntzari eta kontzientziazioari garrantzia ematea.
- ✓Segurtasun-kopiak egiteko plana gailu mugikorren ikuspegitik (fisikoki gailu mugikorretik bereiz biltegiratuta).
- ✓Urrutitik berrasieratzeko eta ezabatzeko prozedurak eta mekanismoak erabil daitezke. Horrez gain, politika hori aplikatzeko prozedura argi edukitzea komeni da.
- ✓Gailurako sarbide-kontrola aplikatu behar da, hau da, erabiltzaileak desaktibatzeko aukerarik ez du izan behar. Segurtasun-politika argi baten bidez egin behar da hori (hatz-marken irakurgailua, txartel-irakurgailua... abiarazteko pasahitzarekin eta BIOSekin batera).
- ✓Horrelako gailuen kudeaketa zentralizatua egitea komeni da (inbentarioa, karga-aplikazioak, komunikazioak, VPN...).
- ✓Arduraz erabili beharrekoak diren erakundearen datuak zifratzea (gailutik disko gogorra ateratzen bada irakurtezina izatea).
- ✓Software kaltegarriaren (*malware*) aurkako babesa.
- ✓Sarbide-puntuetako politikak kontrolatzea.
- ✓Informazio-ihesak prebenitzea (adibidez, DLP teknologiak erabiliz). ❑

HIZTEGIA

[4] **Malwarea:** Edozein software, makro, Activex, Javascript... elementu hauetako bat edo batzuk kaltetzea helburu duena: ekipoak, sistema informatikoak, komunikazio-sareak eta erabiltzaileak —horiek jakinaren gainean egon gabe— (sistema geldotzea, iruzurrezko erabilerak, informazioa lapurtzea...). Adibidez, birusak, harrak, troiarrak, *jokes* (txantxetako programak), *hoaxes* (zurrumurruak), bonba logikoak, *spyware*, *adware*, *keyloggers* (teklatuaren gaineko pultsazioak erregistratzen dituzten programak edo gailuak), etab.

(ikus 3 zk.ko AURRERA buletina, "*Segurtasuna: birusa*" artikulua)

Identitateen kudeaketa

Gaur egun, erabiltzaileek gero eta pasahitz gehiago dituzte aplikazio guztietara sartzeko. Hori dela-eta, erakundeek arazoak dituzte pasahitz horiek kudeatzeko (alta edo baja eman eta pasahitza aldatu). Aldi berean, erabiltzaileei gero eta gehiago ahazten zaizkie, eta horrek ere segurtasun-arazo larriak sor diezazkioke erakundeari eta erabiltzaileari berari.

HIZTEGIA

[5] **Bizi-zikloa**: Erabiltzailearen profilak hiru fase hauek ditu:

- **Sorrera**: Erabiltzailea erakundera iristen denean, profil bat sortu behar da behar diren datuekin.
- **Mantentzea**: Profila sortu ondoren, erabiltzailearen kontua kudeatu egin behar da (adibidez, pasahitza edo izena aldatu, baimenak eman...).
- **Baliogabetzea**: Erabiltzaileak erakundea uzten duenean, baimen guztiak ezabatu egin behar dira erabiltzen dituen sistemen sarbidea galarazteko.

[6] **Identitateen kudeaketa**: (*Identity Management* edo *IdM*) baliabide jakin batzuk (aplikazioak) erabiltzen dituen pertsonaren identitatea zentralizatuta kudeatu eta kontrolatzeko sistemen eta prozesuen multzoari esaten zaio. Hala, identitateen kudeaketaren bidez, erabiltzaileak baliabide horiekin zer egin dezakeen eta nondik, nola eta noiz konekta daitekeen zehazten da. Gaur egun, informazio guztia hainbat sistematan sakabanatuta egoten da, eta, ondorioz, zaila da informazio hori kudeatzea.

Erakunde publiko eta pribatu askok erabiltzaileen kudeaketa-arazoei egin behar diete aurre egunero: erabiltzaile-kodea sortzea, pribilegioak esleitu edo aldatzea eta profila kendu edo ezabatzea. Erabiltzailearen profilaren *bizi-zikloa*[5] esaten zaio prozesu horri.

Adibide honekin argiago ulertuko dugu: pertsona bat gure erakundean sartzen den bakoitzean honelako galderei erantzun behar diegu: zer aplikaziotarako sarbidea izan behar du? Zer baimenekin konfiguratu behar da sarbide hori? Pertsona horri buruzko zer informazio behar dugu aplikazio horretarako? Edo, pertsona horren postua aldatuz gero, zer baldintza berri bete behar ditu? Zer aplikaziori eragiten die aldaketak?... Pentsatzekoa denez, eta alor bakoitzeko informatika-arduradunen ikuspegitik, gero eta zailagoa da egoera hori kontrolatzea, erabiltzaile horri alta eman behar baitiogu hainbat sistema desberdinetan.

Gehienetan, bizi-zikloak sortu ahala kudeatzen dira, hau da, alta-eskaera dagokion sailari egitean eta pertsona bakoitzaren beharren arabera. Baina ahalik eta epe laburrenean erabiltzaileari alta ematea bezain garrantzitsua da sarbide-baimen guztiak garaiz baliogabetzea.

Adituen arabera, *Identitateen kudeaketa*[6] (IdM) izeneko teknologiak dira arazo horiei guztiei irtenbidea emateko egokienak.

IDENTITATEEN KUDEAKETA

Egoera ideal batean, erakunde orok **prozesu automatizatu** bat izan behar luke, erabiltzaileek aplikazio guztietara sarbidea izateko eta, langile batek erakundea uzten duenean, sarbide-baimen guztiak baliogabetzeko. Baina erakunde gehienak urrun daude egoera ideal horretatik.

Gaur egun, erabiltzaileen datu guztiak, baimenak... mantentzea hain konplexua izanik, ahal den neurrian, erabiltzaileen identitate eta baimenen kudeaketa errazteko tresnak erabiltzeko interesa agertzen hasi dira erakunde handiak.

Tresna horiek ez dira berriak, baina orain hasi dira arazo horiei guztiei batera aurre egiten. Horretarako, tresna horien bidez, erabiltzailearen *bizi-zikloaren* prozesu asko kontrolatu eta automatizatzen dira. Orain arte, erakunde bakoitzak berariazko teknika bat erabiltzen zuen prozesu bakoitzerako (*ad hoc*).

Azken batean, prozesua erraztu eta produktibitatea hobetzeko eta, horrez gain, akatsak ezabatu eta sistema batetik besterako datuen inkoherentziak detektatzeko sistema bat lortu nahi da.

ZERGATIK ORAIN?

Identitateen kudeaketa betidanik egin izan da —baita *mainframe* eta *midframe* sistemen garaietan ere—, baina 90eko hamarkadara arte ez ziren hasi erabiltzaileen kudeaketa ere kontuan hartzen zuten informazio-sistemak xehetasun gehiagorekin lantzen.

Lehen, erraza zen erabiltzailea “sortu” (alta

eman) eta baimenak ematea, egunero baimen gutxi kudeatu behar izaten baitziren. Gainera, barne-erabiltzaileak bakarrik izaten ziren, eta informazio-teknologien (IT) sistemetara sartzeko barne-sareak bakarrik erabil zitezkeen.

Gaur egun, ordea, erabiltzaile gehiago daude (barnekoak, kanpokoak, kolaboratzaileak, bezeroak edo hornitzaileak), erabiltzaile horiek kanal berrien bidez jotzen dute baliabideetara, aplikazio eta sistema asko daude bakoitza bere kautotze- eta baimen-moduluarekin,

> "*Single Sign-On* (SSO) sistemaren bidez, erabiltzailea behin bakarrik erregistra daiteke, eta, ondoren, hainbat aplikaziotara sar daiteke, berriz identifikatu gabe."

erabiltzaileek hainbat baimen dituzte baimen-mekanismo desberdinetan oinarrituta, Datuak Babesteko Lege Organikoarekin (DBLO) lotutako alderdiak bete behar dira (kontu-ikuskaritzako aztarnak edo log-ak...), etab.

IRTENBIDEAK

Arazoari aurre egiteko, hau da erakundeek duten oztopo handiena: erakundean instalatuta dauden azpiegituren heterogeneotasuna, eta, gainera, ugari dira sistema zaharkituak.

Halaber, kasu askotan, erakundeak konturatzen dira aplikazio asko ez direla egokiak "**roletan**" oinarritutako sarbidearen euskarri gisa; beraz, gaitasun hori gaineratu behar diote aplikazioari, eta hori oso konplexua eta garestia da[7].

Hala, rolak definitu, sortu eta egokitzeko prozesua luzea izaten da eta ahalegin eta denbora handia eskatzen du. Lan hori egiteko, informatikako arduradunek harreman estua izan behar dute erakundearen alor guztiekin, erabiltzaileen profilak eta bakoitzari eman beharreko sarbide-eskubideak adosteko.

Hala eta guztiz ere, gure aplikazioak, ondo definitutako rolik badagoen ala ez... aztertzen hasi aurretik, irtenbide informatiko horien aholkulariek erabiltzen dituzten **kontzeptu** batzuk ezagutzea komeni da:

- **Pasahitzen kudeaketa**: Erabiltzaileek identifikadorea eta pasahitza erabili ohi dute sistemetara konektatzeko. Pasahitzek (gakoak) beste erabiltzaile batzuek ezagutzeko arriskua dute (erabiltzaileek paperetan idazten dituzte, hacker-ek asmatu egin ditzakete...). Gainera, DBLO garatzen duen araudiak pasahitza aldatzeko betebeharra ezartzen du. Hori dela-eta, aldizka sarbide-gakoak aldatzea komeni da. Sistema moderno askok —bereziki, barne-mailakoak— pasahitzak aldatzeko betebeharra ezartzen diete erabiltzaileei (adibidez, 30 egunean behin). Erabiltzaileek pasahitz asko dituztenean sistema desberdinetan eta bakoitza data desberdinean amaitzen denean, erabiltzaileek paperean idazten dituzte edo, bestela, ahaztu egiten zaizkie. Arazo horiek saihesteko, identitateak kudeatzeko sistemek irtenbidea ematen dute, batetik, gakoa ahazten denerako —posta elektroniko bidez bidaltzen da erabiltzailearen gakoa— eta, bestetik, aplikazio guztietan gakoa aldatzeko —kasu horretan, erabiltzaileari galdera egiten zaio berak bakarrik jakin dezakeen zerbaiti buruz eta, ondoren, gako berria onartzen du, zeina aplikazio guztietara hedatzen den modu automatiko eta gardenean—.

- **Erabiltzaileen hornikuntza** (*user provisioning*): Kontzeptu hori dago identitate digitala kudeatzeko bizi-zikloaren oinarrian, eta erakundeen direktorioen azpiegituran erabiltzaileen informazioari buruzko abantailak ematean datza. Hala, erabiltzaile-kontuak emateko eta baliogabetzeko prozesua azkartzen du, baita informazio-baliabideetara sartzeko eskubideak ere (besteak beste, posta elektronikoa, telefono-zerbitzua, aplikazioak, intranet eta estranet sarbidea eta Erabiltzailearen Laguntza Zentroa (ELZ/CAU) edo *help-desk* zerbitzuak). Sistema horiek barneko erabiltzaileen profilak kudeatzen dituzte, eta ez dute kanpoko direktorioak erabiltzerik erabiltzailearen identifikazioa, kautotasuna eta baimenak egiaztatzeko. Hainbat sistemaren bidez, erabiltzaileen identitatearen administrazioa modu zentralizatuan koordinatzen saiatzen dira. Aplikazio batean kudeatzen da identitatea, eta, ondoren, gainerako aplikazioetara transmititzen da. Erabiltzaileen hornikuntza-sistemen eragozpen handiena da garestiak izaten direla eta denbora asko behar dela martxan jartzeko (kasu batzuetan, zenbait urte).

- **Metadirektorioa**[8]**:** Identitateen administrazioa eta informazio-sarbidea osatzen duen

HIZTEGIA

[7] **Kostuak**: Identitateak kudeatzeko sistemak abantaila handiak eskaintzen dituen arren, hainbat azterketaren arabera, irtenbide horiek guztiak martxan jartzea oso garestia izan daiteke, eta, erakundea zenbat eta handiagoa izan, orduan eta konplexuagoa da. Aholkularien arabera, erakundeek 20-30 dolar ordaindu behar dute erabiltzaile bakoitzeko softwarean eta bi-sei aldiz gehiago integrazioan.

egituraren bihotza da. Direktorio korporatiboak erabiltzaile guztien datuak (helbidea, telefonoa, izena, etab.) eta erakundearen beste tresna batzuk (adibidez, erabiltzaile-taldeak, zerbitzariak, inprimagailuak, etab.) zentralizatuta kudeatzeko diseinatuta daude. Bezeroen aplikazioek datu horietara sarbidea dute —irakurri eta idazteko— protokolo estandar baten bidez (adibidez, **LDAP** edo *light-weight directory access protocol* eta X.500). Direktorioen bidez, aplikazioak konfiguratu egin daitezke erabiltzaileen datuak iturri zentralizatu batetik hartzeko, sistema bakoitzak bere erabiltzaile-zerrenda, kautotze-datuak... kudeatu beharrean. Direktorioen eragozpen handiena da lehendik dauden sistemetan integratu behar dutela (*mainframes*, aplikazio zaharrak eta beste sistema batzuk). Izan ere, sistema horiek ez dira gai direktorio horiekin funtzionatzeko edo, bestela, egokitzapen garestiak behar dituzte.

- **Single Sign-On (SSO)**: Erabiltzaileei behin bakarrik erregistratu, eta, aplikazio bakoitzean identifikatzeko beharrik gabe, baimendutako beste aplikazio batzuetara sartzeko aukera ematen dien kautotze-mekanismoa da. Sistema zahar askok ez dute funtzionatzen erabiltzaileak identifikatzeko eta kautotzeko kanpoko bitartekoekin. Hala ere, erabiltzaileen kredentzialak aplikazioetatik kanpo bil daitezke, eta, ondoren, behar denean, aplikazio horietan automatikoki sartu. *Single sign-on* sistemek horixe egiten dute aplikazio zaharretan. Lanpostuetan softwarea instalatu behar denez, sistema horiek erakunde barruan erabiltzeko bakarrik balio dute. Dena den, sistema horrek hainbat eragozpen ditu erakunde handietan: integratzeko kostuak, segurtasunari buruzko zalantzak —SSO sistemek erabiltzaile guztiek aplikazio bakoitzean dituzten pasahitzak biltzen dituzte—, erabilgarritasunari buruzko kezka —izan ere, SSO sistemak huts egiten badu, erabiltzaile askok ezin dute aplikazioetara konektatu eta, aldi batez, ezin dute lanik egin— Horrelakorik ez gertatzeko, sarbide alternatiboak sortu ohi dira.

Oro har, SSO produktuek kautotze-fasea biltzen dute, eta aplikazioaren esku uzten dute baimena ematea. Bereziki, web-aplikazioetan dira erabilgarriak.

HIZTEGIA

[8] **Metadirektorioa**: Burton Group aholkularitzako analista batek erabili zuen lehen aldiz "metadirektorio" terminoa, eta "*enpresako direktorio guztien batura*" gisa definitu zuen. Hala eta guztiz ere, Kim Cameron, Zoomit enpresako sortzaileetako batena da, berez, esaldi hori. Cameronek dolar baten truke saldu zion zita hori Burton Group-i, 1997an.

[9] **ELZ/CAUren intzidentziak**: 2008an, Eusko Jaurlaritzako EAZk segurtasun-intzidentzia hauek kudeatu zituen (XLNet, domeinua...):

- Guztira, 7.482 kasu (erantzundako intzidentzia guztien (hau da, 81.227 kasu) %9,21)
- Iraupena, guztira: 2.257 ordu
- Batez besteko iraupena intzidentzia bakoitzeko: 18 minutu

Azkenik, EAEko administrazioaren barruan, Osakidetzak landutako identitateen kudeaketa-proiektua eta Single Sign-On (SSO) proiektua aipatu behar dira. Proiektu horrek **Norbide** izena du.

ABANTAILAK

Identitateak kudeatzeko sistema izateak hainbat abantaila ditu:

✓ **Kudeaketa-kostuak aurreztea**: Datuen sendotasuna ziurtatzen da, zeren datu guztiak direktorio bakar batean eguneratzen dira, eta hortik beste sistemetara automatikoki zabaltzen. Hartara, erabiltzaile bati sarbidea emateko egin beharreko lana murriztu egiten da, akatsak minimizatu egiten dira, eta arazo gutxiago izaten dira.

✓ **Segurtasuna handitzea**: Langilearen estatusean izandako edozein aldaketa azkar eta eraginkor "hedatu" eta eguneratu daiteke sistema informatikoen bidez (langileak erakundearen barruan egoteari uzten dionean, sistemak automatikoki baliogabetzen ditu haren kontuak, eta, hala, baimendu gabeko sarbideak, jabe ezezaguneko kontuak... izateko arriskua murriztu egiten da). Oro har, segurtasunak hobera egiten du, zeren, pasahitz bat baino gehiago gogoratu behar ez denez, erabiltzaileak ez du zertan pasahitzak post-it-etan idatzi eta teklatuaren gainean utzi.

✓ **Lehiatzeko abantaila**: Erakundearen produktibitatea handitu egiten da. Sistema berriak murriztu egiten ditu ELZ/CAUren kostuak[9] (*help-desk*), pasahitzak doitzeko eskuz egin beharreko eragiketa gutxiago behar direlako.

✓ **Erabiltzailearen esperientzia hobetzea**: Erabiltzaileak pasahitz bakar bat gogoratu behar du sistema guztietarako.

✓ **Legezko eskakizunak betetzea**: Erakundea hobeto prestatuta dago indarrean dagoen araudia betetzeko (DBLO, etab.) eta kontu-ikuskariei arau horiek betetzen dituztela egiaztatzeko (txostenen eta ikuskaritza -frogen bidez).

- **Identitate federatua:** Sistema horren bidez, erabiltzaileek identifikazio pertsonal bera erabil dezakete (erabiltzailea, pasahitza) beste enpresa batzuen sareetan erregistratzeko. Hala, erakundeek informazioa parteka dezakete direktorio-, segurtasun- eta kautotze-teknologiak ere partekatu behar izan gabe. "Konfiantza-zirkuluan" oinarritzen den sistema da, zeinaren arabera, erabiltzailea sare jakin batean (domeinua) ezagutzen duten eta berariazko zerbitzu batzuetara sar daitekeen. Sare desberdinen arteko konfiantza izatea da sistemaren zailtasun handiena. Industriak itun bat ezarri du —*Liberty Alliance Project*— estandar irekiak eta neutralak garatu, eta identitate federatua eta *WebServices*-ak bultzatzeko.

"Erakunde bakoitzak prozesu automatizatu bat izan behar luke erabiltzaileei aplikazio guztietarako sarbidea emateko."

Merkatuko identitateen kudeaketarako irtenbideak[10] aztertuz gero, konturatuko gara produktu horietako batzuk biltegietan oinarritzen direla (direktorioen estrategia), beste batzuk kudeaketa-prozesuetan —baliozkotze-zirkuituak, eskuordetzeak...— (hornikuntzaren estrategia) eta hirugarren batzuk erabiltzailearen postuan eta aplikazioen eta zerbitzuen sarbide kontrolatuan (*logon* edo erabiltzaile bakarraren kodearen estrategia).

Edonola ere, produktu horiek guztiek **osagai komun** batzuk dituzte:

✓**Integrazio-sistema:** osagai horren bidez, lehendik dauden sistemek modu independentean erabilitako sarbide-informazioa jasotzen da lehendik dauden hainbat iturri heterogeneotatik (direktorioak, sistema eragileak, datu-baseak...), eta identitateen kudeaketa-sistema berrian txertatzen da.

✓**Hornikuntza-sistema:** erabiltzaile berriei alta emateaz eta rol bat esleitzeaz arduratzen da, eta, erabiltzaileentzat garden, kautotze-lekuetara zabaltzen du informazio hori.

✓**Autokudeaketa-sistema:** erakunde baten erabiltzaileen laguntza-zentroaren (ELZ/CAU) lan handiena gakoak kudeatzea izaten da. Hori dela-eta, prozesua arintzeko, erabiltzaileari aukera ematen zaio alta emateko edo aldaketa bat egiteko behar diren datuak emateko, eta, ondoren, dagokion arduradunak baliozkotzen ditu datu horiek.

✓**Sinkronizazio-motorra:** erabiltzailearen identitate desberdinak, erabiltzaileak sarbidea duen sistemak eta rol-aldaketak zentralizatuta kudeatzeko aukera ematen du, aldaketa guztiak zerbitzu korporatibo guztietara hedatuz.

✓**Kontu-ikuskaritzako sistema:** aldaketa guztiak gordetzeko aukera ematen du, azterketa edo ikuskaritza bat (barnekoa edo kanpokoa) egiten denerako.

ONDORIOAK ETA ETORKIZUNA

Identitateen kudeaketaren teknologia ez da berria, baina erakundeek inoiz baino gehiago behar dituzte baliabide horiek. Merkatuan dauden teknologia batzuk beste batzuk baino gehiago garatu dira. Direktorioak, pasahitzen kudeatzaileak edo web-eko *single sign-on* sistemak oso hedatuta daude eta hobekuntza errealak eta kuantifikagarriak eskaintzen dituzte. Erabiltzaileak hornitzeko teknologiak, berriz, abantaila handiak izango dituela uste da, baina oraindik gutxi hedatu da.

Edonola ere, datozen zenbakietan ere irtenbide horiei buruz hitz egiten jarraituko dugu, seguru. ❑

HIZTEGIA

[10] **Identitateak kudeatzeko irtenbideak:** Merkatuko fabrikatzaile batzuen eta haien produktuen zerrenda:

- **Sun Microsystems**: *Sun Java Identity Manager* (SJIM)
- **Computer Associates**: *eTrust Identity and Access Management Suite*
- **Novell**: *Nsure*
- **IBM**: *Tivoli Identity Manager* (TIM)
- **BMC**: *BMC*
- **Oracle**: *Oracle Identity Management* (OIM)
- **Microsoft**: *Identity Integration Server* (MIIS)

ALBOAN:
EHAA elektroniko berria

EUSKAL HERRIKO AGINTARITZAREN ALDIZKARIA
BOLETÍN OFICIAL DEL PAÍS VASCO

"Edizio digitala da orain legearen aurrean balioa duen formatu bakarra."

Euskal Herriko Agintaritzaren Aldizkaria (EHAA) Euskal Autonomia Erkidegoko aldizkari ofiziala da. Hor argitaratzen dira argitalpen ofiziala behar duten dokumentuak, indarrean dagoen ordenamendu juridikoaren arabera.

Denborarekin, eta teknologia berrien bilakaerari esker, aldizkaria baliabideak optimizatuz joan da azken urteotan: batetik, barne-funtzionamenduari dagokionez, eta, bestetik, kanpora begira —alegia, herritarrei— eskaintzen duen zerbitzuari dagokionez.

"Informazioaren zabalkunde selektiborako harpidedunen kopurua %15,61 handiagoa izan zen 2008an 2007an baino."

Tresna informatikoen etengabeko aurrerapenei, tresna horiek orokortzeari eta bitarteko elektroniko, informatiko eta telematiko berriak martxan jartzeari esker, aldizkari ofizialak garai berrietara egokituz joan behar izan du, behin eta berriro.

EHAA sarbide unibertsala eta doakoa duen zerbitzu publikoa da, eta orain arte argitaratutako aldizkari guztiak hartzen ditu bere baitan, baita II. Errepublikan (1936-1937) eta Euskadiko Kontseilu Nagusiak autonomia aurreko garaian (1978-1980) argitaratutakoak ere.

Gaur egun, EHAAren web orriaren bidez, aldizkariko edozein laburpen edota xedapen ikus daiteke, web orrian urtea, hilabetea, eguna eta aldizkariaren zenbakia zehaztuta. Bilaketen bidez, BRS datu-base dokumentalarekin aurkitutako xedapen guztien testuak agertzen dira, PDF (*Portable Document Format*) formatuko bertsiorako lotura zuzenarekin batera.

Horrez gain, argitaratutako xedapenen edukia gaika antolatuta dago, edozein informazio-mota bilatu ahal izateko.

Bestalde, EHAAk harpidetzeko aukera ematen du, egunero, posta elektroniko bidezko ohar-zerbitzua jaso ahal izateko (EHAAren *Informazioaren Zabalkunde Selektiboa* edo IZS/DSI zerbitzua). Zerbitzu horren bidez, helbide elektronikoa duen edozein pertsona edo erakunde harpidetu daiteke, eta, izena ematean, gaikako profil jakin bat zehaztu ondoren, zehaztutako baldintzekin bat datozen xedapenak jasotzen ditu, egunero eta doan.

DIGITALIZAZIOA, ZERTARAKO?

2009ko urtarrilaren 2an jarri zen martxan EHAA elektroniko berria. Hala, euskadi.net webgunearen bidez, herritarrak benetako, manipulatu gabeko eta elektronikoki sinatutako dokumentu ofizial bat kontsulta dezake, lehengo paperezko dokumentuaren ordez.

Besteak beste, EHAAren argitalpen-arduradunek (Jaurlaritzaren Idazkaritzako eta Legebiltzarrarekiko Harremanetarako Zuzendaritza) arrazoi hauengatik jarri dute martxan aldizkari elektronikoa: batetik, paperezko edizioaren harpidedun-kopurua pixkanaka txikitzen ari zelako (zehazki, 2007 eta 2008 artean, 300 harpidedun gutxiago zituen, eta 2009rako are murrizketa handiagoa aurreikusten zen) eta, bestetik, webgunean egindako kontsulten kopurua handitu egin zelako (2008an, 366.870 bisitari), baita informazioaren zabalkunde selektiborako harpidetzak ere (2008ko abenduaren 31n 15.050 harpidedun, eta %15,61eko hazkundea 2007arekiko).

ABANTAILAK

Paperezko edizioa desagertzeak ondorio hauek ditu, nagusiki:

- Papera aurreztea. Horri esker, batetik, onura ekonomikoa lortzen da eta, bestetik, mesede egiten zaio ingurumenari eta ekologiari, garapen iraunkorra hobetzen delako.

- Edizioa digitala izanik, eta paperezko faszikulurik argitaratzen ez denez, inprenta-zerbitzuak berrikusi egin behar izan dira.
- Ez da jatorrizkoaren bigarren kopiarik behar itzulpenak, zuzenketak, orrazketak... egiteko.
- Kanpoko zerbitzuekiko mendekotasuna murriztu egin da. Testuak maketatu eta diseinatzera mugatzen da orain zerbitzu hori.
- Prozesua arinagoa da, inprimatzeko betebehar teknikoak desagertu egin baitira. Bertsio elektronikoak ez du mugarik; orrialde-kopuruak ez du eraginik edizio-denboran.
- Diseinu-zerbitzuak egun bat lehenago bidaltzen ditu testuak. Inprimatzeko eta banatzeko denbora desagertu denez, ez dago hurrengo egunera arte itxaron beharrik.
- Artxibatzeko espazioa eta altzari-kopurua murriztu egin dira.
- Artxibatzeko prozesua desagertzearekin batera, jatorrizko testuak, kopiak, argitaratutako aldizkariak, koadernatutako liburuak... artxibatzeko lanak ere murriztu egin dira.

ALDERDI TEKNIKOAK

Formatu digital berria erabiltzeko, besteak beste, sinadura elektroniko aitortua behar da (**Izenpe**-k ematen du). Sinadura horren bidez, testuen kautotasuna, osotasuna eta aldagaiztasuna ziurtatzen dira.


29 ZK. BOPV - viernes 28 de noviembre de 2008 28887

Disposiciones Generales

DEPARTAMENTO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA
DEPARTAMENTO DE VIVIENDA Y ASUNTOS SOCIALES

6622

Pauso hauek ematen dira: EHAAren zerbitzuak diseinu-zerbitzuak bidalitako testuak onetsi ondoren (laburpen, xedapen eta eranskinetan banatutako artxiboak), argitalpena berretsi egiten du hurrengo egunerako. Prozesu hori gauzatzeko, sinadura elektroniko bidezko kudeaketa-aplikazioa erabiltzen da (sinadura-zerbitzu horizontala). Jaurlaritzaren Idazkaritzako eta Legebiltzarrarekiko Harremanetarako Administrazio Organoak ezartzen du ziurtagiri-politika.

Internet bidezko kontsultarekin, herritarrek sinaduraren datuak ikusi eta xedapen bakoitzarekin lotutako sinadura elektronikoa egiazta dezakete, horren bidez, administrazioaren esku dagoen jatorrizko dokumentu elektronikoa benetakoa dela-eta ez dela manipulatu edo aldatu ziurtatzeko. Halaber, herritarrek aukera dute, jatorrizko dokumentu elektronikoa erraz begiratzeko.

ETORKIZUNERAKO PROPOSAMENAK

Gaur egungo lan-fluxu guztietatik papera kendu egin nahi denez —Eusko Jaurlaritzako barne-nahiz kanpo-eskatzaileena, eta, bereziki, organismo publiko handiena (EHU, UTAP, foru-aldundiak...) eta tokiko organismoena (udalak...)—, argitaratu beharreko gaien eskaerak kudeatzean, ezinbestekoa da denek ulertzea behin-betiko testuak direla. Beraz, “aurrerapenaren” kontzeptua eta “sortu ahala” egindako aldaketak desagertu egingo dira.

Izan ere, epeak murriztu egiten direnez, ez dago bidalketaren eta argitalpenaren arteko denborarik zuzenketak sartzeko. Bestetik, “aurrerapenak" erabiltzeak zehaztasun-gabezia handia sortzen du testuen segurtasunean eta, horrez gain, errepikatu egiten dira, formatuaren, zuzenketaren, orrazketaren eta itzulpenaren arloko lanak.

Halaber, EHAA digitalizatzearen bidez, legezko balioa zuen formatu bakarra —paperezko euskarria— desagertu egin da. Sistema informatikoaren funtzionamenduan eragina duten eta aldizkariaren edizio elektronikorako sarbidea galarazten duten gorabehera tekniko larririk izanez gero, lehendakariordeak kopiak paperezko euskarrian eta izaera ofizialarekin argitaratzeko baimena eman dezake.

Aurtengo urtarrilaz geroztik, herritarrek web orria bakarrik erabil dezakete aldizkariaren edizio digitala eskuratzeko, legearen aurrean balioa duen formatu bakarra baita orain.

Etorkizunera begira, argitalpenaren arduradunek uste dute beharrezkoa izango dela EHAAren webgunea berrikustea, hau da, sarbideko interfazea hobetu eta, diseinua eta funtzionalitateak berritzea (estilo-liburua, usagarritasuna, erabilerraztasuna, bilaketak, edukiak...). ❑

“Formatu elektroniko berriak sinadura elektroniko aitortua jasotzen du, zeinak testuen kautotasuna, osotasuna eta aldagaiztasuna ziurtatzen baititu.”

EHAA

Webgunea:

www.lehendakariordetza.ejgv.euskadi.net

Informazio gehiago nahi izanez gero, ikus:
Euskal Herriko Agintaritzaren Aldizkariaren abenduaren 23ko 217/2008 dekretua

LABURRAK!!

33. zk.

2009ko martxoa

.eus domeinua

Joan den urtarrilean aurkeztu zen **PuntuEus**, euskara, hezkuntza eta komunikazioaren arloko —besteak beste— hamaika erakundek osatutako elkartea, interneten .eus domeinua sortu eta kudeatzeko oniritzia lortzea helburu duena. Hala, euskararen eta euskal kulturaren komunitatea osatzen duten web orri guztiak identifikatuko dituen ikurra izatea lortu nahi da.

Hauek dira PuntuEus elkartea osatzen duten hamaika erakundeak: Euskaltzaindia, Euskararen Gizarte Erakundeen Kontseilua, Euskal Konfederazioa, Euskal Idazleen Elkartea, Euskal Herriko Unibertsitatea, Euskal Herriko Ikastolen Konfederazioa, Ikastolen Elkartea, EiTB, Interneten Euskara Sustatzeko Elkartea, Euskal Herriko Telekomunikazio Ingeniarien Elkartea eta Euskadiko Informatikako Ingeniarien Elkargo Ofiziala.

Estatuetako kodeak (.fr, .uk, .es), domeinu historikoak (.com, .net, .org) eta babestu gabeak (.biz, negozioetarako; .name, pertsonentzako) alde batera utzita, babestutako domeinuak komunitateei dagozkie, eta, beraz, komunitateek eurek sustatu behar dituzte.

ICANN (*Internet Corporation for Assigned Names and Numbers*) nazioarteko erakundea da interneteko domeinu-sistemaren kudeaketa-arduraduna, eta haren oniritzia lortzeko izapideek nahiko luze iraun dezakete (bi urte). Edonola ere, ekimenaren arduradunek .cat domeinuaren —Kataluniako hizkuntza- eta kultura-komunitatearena— bide bera egin nahi dute. Hark 2005ean lortu zuen oniritzia.

.cat domeinuak arrakasta izan ondoren, Europako zenbait herri ari dira saiatzen beren hizkuntza eta kultura interneten ikus dadin. Ahalegin horietan ari dira, adibidez, Galiziako, Bretainiako eta Galesko komunitateak, eta puntogal, pointbzh eta dotcym izenarekin ari dira lanean, hurrenez hurren, aitorpen hori lortzeko.

Hau da elkartearen webgunea: www.puntueus.org

Eusko Jaurlaritzak superordenagailu bat erosi du

Eusko Jaurlaritzak superordenagailu berri bat hornitu, instalatu, martxan jarri eta mantentzeko lehiaketa esleitu berri dio IBMri, milioi bat euro inguruko zenbatekoaren truke, Eusko Jaurlaritzaren Informatika Elkartea, S.A.ren bidez (EJIE). Superordenagailu horrek zerbitzua emango die **Euskal Herriko Meteorologia Zentroari**, unibertsitateei eta hainbat zentro teknologikori klimari buruzko goi-mailako ikerketak egiteko.

Estatu espainiarrean instalatuko den lehenengo iDataPlex superordenagailua izango da, prozesu-gaitasun eta energia-eraginkortasun handikoa. Superordenagiluaren potentziaz ohartzeko, Eusko Jaurlaritzaren superkonputazio-guneak 11 TeraFLOPSetik gorako kalkulu-potentzia lortuko du (11 bilioi eragiketa segundoko), hau da, 48 orduan egingo du ohiko ordenagailu batek 114 urtean egingo lukeena.

iDataPlex zerbitzariak Linux sistema eragilea egikaritzen du, eta lau nukleoko Xenon prozesagailuetan oinarritzen da.

Energia-eraginkortasunari dagokionez, hozteko teknologia berritzailea du. Horri esker, % 40ra arteko energia-aurrezkia lortzen du eta bost aldiz handiagoa du prozesatzeko gaitasuna.