

Confiança en els serveis públics electrònics

L'administració electrònica suposa una transformació de la mateixa Administració, per donar un millor servei a la societat i als interessos generals. Així, es plantegen reptes com, per exemple, quines han de ser les mesures a establir per controlar i garantir la qualitat de les dades personals, o com es regulen aquestes dades en les interconnexions entre les administracions públiques.

Cal aconseguir que la ciutadania confiï en les seves administracions. Qüestions com què hem de fer per garantir el compliment de les mesures de seguretat, com afectarà l'administració electrònica els fitxers no automatitzats, i com es regula el principi del consentiment, sorgeixen com a nous elements a analitzar.

En aquest sentit, és important l'aprovació i ulterior publicació, el propassat mes de gener, de l'Esquema Nacional de Seguretat i de l'Esquema Nacional d'Interoperabilitat, en l'àmbit de l'administració electrònica.

Esther Mitjans Perelló
Directora Agència Catalana de Protecció de Dades

Mesures de
seguretat
RLOPD



Esquema
Nacional de
Seguretat

Destaquem... Publicació de l'Esquema Nacional de Seguretat

Al BOE del 29 de gener passat es va publicar el Reial decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'administració electrònica. La creació de l'ENS es preveu a l'art. 42.2 d'aquesta disposició i té per objecte establir els principis i requisits de la política de seguretat en l'ús dels mitjans electrònics, en relació amb l'administració electrònica.

En el mateix BOE també es publica el Reial decret 4/2010, que regula l'Esquema Nacional d'Interoperabilitat, en el mateix àmbit de l'administració electrònica. Tots dos decrets formen part del desplegament de la Llei 11/2007, d'accés electrònic dels ciutadans als serveis públics.

Durant els propers mesos caldrà estudiar aquest nou marc de seguretat de la informació, relacionat amb l'accés electrònic dels ciutadans als serveis públics, que s'afegeix a les mesures de seguretat previstes per a la protecció de les dades de caràcter personal.

Des de la perspectiva del dret a la protecció de dades, això requerirà analitzar de quina manera s'integrarà i conviurà amb les mesures de seguretat previstes al reglament de desplegament de la Llei orgànica de protecció de dades. Sens dubte, al 2010 parlarem molt d'aquesta qüestió.

Aquí teniu l'enllaç directe al text publicat al BOE:
<http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>

Parlem... de l'autenticació en autoserveis de tràmits administratius

El desenvolupament de l'administració electrònica no passa exclusivament per facilitar l'accés dels ciutadans als serveis electrònics mitjançant Internet. L'existència de sistemes d'autoservei de tràmits administratius entraria, també, dins del concepte d'ús de mitjans electrònics en el desenvolupament de l'activitat administrativa o de servei públic.

En aquest article n'analitzem breument les qüestions més rellevants des del vessant tècnic, un aspecte que cal tenir en compte per assegurar que els processos d'autenticació realitzats en "terminals d'autoservei" s'adeqüen plenament a la normativa de protecció de dades.

+info

Continguts	
Confiança en els serveis públics	1
Destaquem...	1
Parlem de...	1
Incidents de seguretat relacionats amb la protecció de dades	2
On anar...	2
Tecnologia i protecció de dades	3
Butlletí revisió vulnerabilitats	4
Enllacem amb...	4
Autenticació en autoserveis	5

Incidents de seguretat relacionats amb la protecció de dades

Un desastre a AT&T fa que usuaris de Facebook accedeixin a comptes aliens (gener 2010)

Una fallada en el trànsit de comunicacions de la companyia de telecomunicacions AT&T ha provocat que tres dels seus clients accedissin, sense voler-ho, a comptes de Facebook que no eren seus.

Les tres persones utilitzen el servei d'Internet sense fils d'AT&T i s'havien connectat a la xarxa social des dels seus telèfons mòbils. Un d'aquests usuaris afirma que, en intentar accedir al seu perfil de Facebook, el servidor el va redirigir automàticament al perfil d'un altre usuari, sense demanar-li les dades d'accés (usuari i contrasenya).

Segons sembla, el problema el va causar una vulnerabilitat de l'encaminador (*router*), que fa que la xarxa barregi les identitats dels usuaris.

Aquest forat de seguretat pot causar problemes seriosos, ja que no se sap si afecta només Facebook o també pot posar en perill la privacitat dels comptes de correu electrònic, o fins i tot altres llocs web amb contingut personal.

És possible que aquest problema no afecti tots aquells llocs web que mantenen codificada la sessió de l'usuari (SSL), com per exemple les entitats bancàries en línia.

Font: viruslist.com

Microsoft investiga un forat en la privacitat de Hotmail (febrer 2010)

Segons ha informat Microsoft, la companyia està revisant l'incident reportat per alguns usuaris del servei de correu Hotmail als quals se'ls va mostrar, accidentalment, la safata d'entrada d'altres usuaris. L'incident es va produir quan intentaven accedir al seu compte de correu, utilitzant el telèfon mòbil.

Els usuaris afectats van dir que en entrar al servei de correu apareixia una safata d'entrada que no era seva i que, cada vegada que hi tornaven a entrar, apareixia una safata d'entrada diferent de l'anterior.

Paral·lelament, el servei d'ingrés de Windows Live va estar inactiu durant una hora. Això va impedir que molts usuaris poguessin accedir als serveis que en depenen, com és el cas del correu Hotmail.

En la seva declaració, Microsoft va dir que "Microsoft es pren la privacitat dels seus clients seriosament. Immediatament després de tenir coneixement d'aquests incidents, vam començar una investigació. Un cop haguem completat la investigació, prendrem les mesures necessàries".

Segons els primers indicis, els dos incidents estan relacionats.

Font: Segu-info

Presenten una denúncia contra Google Buzz per violar la llei de privacitat dels Estats Units (febrer 2010)

El centre d'informació sobre privacitat electrònica (EPIC) dels EUA va presentar una denúncia davant la Comissió Federal de Comerç (FTC), en què informava que el nou servei de Google, anomenat Buzz, viola la llei federal de protecció de l'usuari.

Aquesta denúncia s'ha presentat després que, en el seu llançament, aquest nou servei permetés per defecte que els usuaris compartissin la seva activitat social amb els seus contactes de Gmail. Després de les queixes dels usuaris, Google va corregir aquest error.

La denúncia d'EPIC insta la FTC a reclamar a Google que Buzz sigui un servei completament independent, de manera que deixi d'utilitzar la llista de contactes privada de Gmail per crear una xarxa social encoberta.

Google va posar en marxa Buzz el 9 de febrer i el va activar per a tots els usuaris de Gmail. Segons EPIC, els usuaris van veure com la seva llista de contactes freqüents es convertia en una llista pública d'usuaris que, posteriorment, es publicava en un perfil de l'usuari també públic. Segons EPIC, encara que Google ha modificat el servei dues vegades des del seu llançament, "les violacions de la privacitat encara persisteixen".

Font: Segu-info

On anar...

Congressos i esdeveniments

VI Ciclo de conferencias UPM—TASSI Temas Avanzados en Seguridad y Sociedad de la Información

Del 23 de febrer al 25 de maig de 2010. UPM, Madrid
<http://www.lpsi.eui.upm.es/GANLESI/GANLESI.htm>

CeBIT

Del 2 al 6 de març de 2010. Sophia Antipolis (França)
http://www.cebit.de/homepage_d

Fòrum Assessors Wolters Kluwer 2010

3 de març de 2010. Barcelona
<http://foroasesores.wke.es/>

Jutges, fiscals i policies en la prevenció del delicte

11 i 12 de març de 2010. ISPC, Mollet del Vallès
http://www.gencat.cat/interior/epc/docs/jornades/ispc_jornades14.htm

Fourth Annual IT Security Entrepreneurs Forum (ITSEF IV)

16 i 17 de març de 2010. Universitat de Stanford (CA), EUA
<http://www.security-innovation.org/itsef/>

Expodidàctica

Del 18 al 20 de març de 2010. Barcelona
<http://www.expodidactica.com/>

IADIS International Conference Information Systems 2010

Del 18 al 20 de març de 2010. Oporto (Portugal)
<http://www.is-conf.org/>

Rooted CON—Congreso de Seguridad Informática

Del 18 al 20 de març de 2010. Madrid
<http://www.rootedcon.es/>

La privacitat a l'Administració electrònica a l'Estat autonòmic

19 de març de 2010. Barcelona
http://www.apd.cat/ca/curs_jornada_activitat.php?cat_id=170&curs_id=109

Social Networks: Impacts of Clicking and Connecting on the Web

22 de març de 2010. Calgary (Canadà)
<http://conted.ucalgary.ca/search/publicCourseSearchDetails.do?met=load&courseId=1719663&selectedCategoryId=10237&selectedProgramAreaId=&selectedProgramStreamId=>

Les dades personals dels menors a Internet

24 de març. UdL, Lleida
<http://www.paeria.es/acces/presentacions/menors2010/index.asp>

Tecnologia i protecció de dades

La UE actualitzarà la directiva sobre protecció de dades per adaptar-la a les xarxes socials

La nova responsable de Justícia, Drets Fonamentals i Ciutadania de la UE, Viviane Reding, assumint encara en funcions la cartera de Societat de la Informació, va explicar que la Comissió Europea modernitzarà la directiva de 1995 sobre protecció de dades, per tenir en compte els efectes de les xarxes socials (Facebook, Twitter...).

En un col·loqui amb motiu del Dia Europeu de la Protecció de Dades, la comissària va afirmar que el món ha canviat molt des de 1995, quan la normativa comunitària tan sols preveia que la informació d'una persona podia utilitzar-se per raons legítimes i amb el seu consentiment previ. A l'actualitat, les xarxes socials que utilitzen més de 40 milions d'europers permeten que la informació personal sigui fàcilment accessible, incloses les fotografies. Reding, a més, va recordar altres noves realitats en la protecció de dades, com que "la publicitat d'Internet basada en el comportament converteix en moneda de canvi el nostre historial de cerques".

El proper 9 de febrer, l'executiu comunitari farà públiques les conclusions dels treballs preparatoris per a la reforma de la nova directiva de protecció de dades. En aquesta mateixa data, es donaran a conèixer els resultats de la implementació a les principals xarxes socials de l'obligació que es van imposar de no fer visibles, per defecte, els resultats de perfils personals de menors d'edat.

La comissària va fer una crida a les empreses de tecnologia per tal que inverteixin en innovació i perquè, a l'hora de dissenyar nous productes, tinguin presents les opcions de privacitat des del principi.

<http://es.noticias.yahoo.com/3/20100129/tc-la-ce-modernizar-la-directiva-sobre-56149c7.html>

L'Agència Catalana de Protecció de Dades i el Departament d'Educació aborden la protecció de dades entre els joves

El 27 de gener passat, l'Agència Catalana de Protecció de Dades i el Departament d'Educació van celebrar la jornada "Joves 2.0 i privacitat", amb la col·laboració de CosmoCaixa i del Cescicat. En aquesta Jornada, adreçada a professionals de l'educació, es va debatre sobre la importància de l'educació en matèria de protecció de dades en els àmbits educatius.

La Jornada va analitzar la seguretat de la informació i els possibles riscos per a la privacitat dels menors, tant en l'entorn de webs de centres educatius com a les xarxes socials.

La conferència inaugural, "Privacy for children and young people", va ser a càrrec de Tanya Byron, psicòloga infantil i autora de l'informe *Safer children in a digital world*. La Dra. Byron va tractar dels riscos de les noves tecnologies per als menors i la importància de l'educació per salvaguardar-ne la privacitat, i va parlar de la necessitat de coneixement perquè infants i joves es mantinguin segurs. Va remarcar que per la seva condició d'infants ja estan exposats a riscos i que, per això, malgrat l'esclatxa tecnològica generacional, els cal l'ajuda dels adults a l'hora de prendre decisions encertades. Byron conclou que la família, la indústria i l'Administració s'han de responsabilitzar de la seguretat dels menors a Internet.

Les diferents intervencions al llarg de la Jornada van oferir als assistents una aproximació als entorns digitals utilitzats als centres educa-

tius i van incidir en la importància de les xarxes socials i els potencials riscos que poden representar per als joves. Es va tractar, així mateix, de la forma en què s'ha d'informar els joves per tal que siguin receptius, i es va mostrar com es pot utilitzar Internet en l'àmbit universitari per facilitar el traspàs del coneixement tant a professors com a alumnes.

http://blocs.xtec.cat/joves_privacitat/

L'AEPD posa en marxa Evalúa, un programa que permet analitzar el grau d'acompliment de la LOPD

L'Agència Espanyola de Protecció de Dades ha presentat Evalúa, un programa senzill, anònim i gratuït que permet a empreses i administracions autoavaluar el grau de compliment de la Llei orgànica de protecció de dades.

Aquesta eina ofereix resposta als dubtes més habituals entre les persones que tracten dades personals, mitjançant un autotest basat en preguntes amb múltiples respostes. El temps estimat per emplenar el formulari és de 45 a 60 minuts. Un cop finalitzat, genera un informe amb indicacions i recursos que orienten al compliment del que disposa la LOPD.

El programa consta de dos nivells d'autoavaluació:

- El primer és un test bàsic, per conèixer el nivell d'acompliment de la normativa de protecció de dades.
- El segon permet verificar fàcilment si es compleix amb les mesures de seguretat exigibles en cada cas.

Aquesta eina està disponible a la pàgina web de l'Agència Espanyola de Protecció de Dades (www.agpd.es).

http://www.agpd.es/portalweb/revista_prensa/revista_prensa/2010/notas_prensa/common/enero/280110_presentacion_evalua.pdf

El compliment de la LOPD en entorns cloud

LOPDGEST, amb la seva proposta per al compliment de la LOPD, ha arribat a la conclusió que la popularització de l'ús del *cloud computing*¹ en l'àmbit empresarial no està exempt de riscos. Aquests riscos es deriven, sobretot, d'un mal ús de l'eina o de l'incompliment de les mesures de seguretat necessàries per a una total protecció de la informació, i es refereixen tant a la vulnerabilitat de la integritat d'aquesta informació com a l'accés de personal no autoritzat.

LOPDGEST proposa diverses mesures, algunes de les quals són tècniques, com ara l'establiment de mesures d'identificació i autenticació d'usuaris, per tal que no es pugui tenir un accés lògic a la informació. Per una altra banda, també posa de manifest la necessitat de fer còpies de seguretat i de xifrar les dades especialment sensibles, quan hagin de viatjar per xarxes públiques.

¹ *cloud computing*: filosofia de desenvolupament de programari que permet oferir serveis informàtics a través d'Internet.

Font: Revista TCN, núm. 455

Butlletí revisió vulnerabilitats

Virus social

Cucs, troians, virus, programari maliciós en general... Tots coneixem la perillositat d'alguns arxius adjunts al correu electrònic (encara recordem el virus "I love you"), que aprofiten totes les vulnerabilitats possibles per infectar els usuaris, ja siguin les del sistema o el desconeixement del mateix usuari. També sabem del perill que pot suposar navegar per certes URL sospitoses o compromeses, sense coneixement del propietari dels continguts.

Cada dia n'apareixen una infinitat i es coneixen bé les mesures de sentit comú per evitar, fins on és possible, que infectin els equips. La novetat és el canvi en la forma d'expansió d'aquest codi maliciós: ara tenim el Koob-face, el famós virus que s'estén a través de les xarxes socials Facebook i MySpace. És el que anomenem *virus social*.

Tot i que ja se n'ha parlat molt, a continuació donem un exemple de missatge enviat amb aquest virus (recordeu que no heu de seguir l'enllaç!):

Assumpte: tua foto?!!

"és aquest la teva foto?!"

<http://www.facebook.com//6ffa7;readinfo163178191351372640.sendzsafez.info/gp735tq/>
"Vés amb compte!"

El funcionament d'aquest programari maliciós és força senzill:

1. L'usuari clica l'enllaç del vídeo.
2. Apareix un element emergent, que requereix que l'usuari actualitzi l'Adobe Flash Player.
3. L'usuari accepta la instal·lació del *malware* i queda infectat.



Tornen els dialers

Si mirem cap enrere, recordarem l'època en què les línies ADSL eren només quelcom que algú havia llegit en fòrums americans. Llavors, qui volgués tenir Internet havia de buscar-se un ISP i, després, utilitzar un mòdem i pagar una xifra gens menyspreable a Telefónica per la durada de la trucada.

En aquell temps, una de les amenaces que més disgustos va causar van ser els famosos *dialers*, programes maliciosos que alteraven l'accés telefònic a xarxes perquè, en comptes de trucar a un innocent número de telèfon, la trucada es fes a un número amb sobretarifació (a Espanya, típicament un 906). Amb l'arribada de l'ADSL i la seva popularització, aquest mercat negre va desaparèixer perquè ja ningú no usava mòdems.

Ara, segons es llegeix a The Register (<http://www.theregister.co.uk/>), el concepte ressorgeix. Aquesta vegada l'infectat no és el telèfon convencional, sinó el telèfon mòbil, i el que fan aquests *dialers* és enviar successivament missatges a números amb taxes exorbitants.

A Espanya, les operadores ja investiguen per poder fer front als troians per a mòbils. En el cas de Symbian, per exemple, en les seves últimes versions no es pot instal·lar cap aplicació *unsigned* (sense signatura digital), cosa que en teoria hauria de neutralitzar aquest tipus de programes maliciosos.

Virus més detectats

Virus más detectados (ult. 24h)	
Nombre	Incidencias
Krap.AH	(41,9%)
Hetsky.Q	(20,2%)
Bredlab.SMP	(19,0%)
MIME Overflow	(11,6%)
Hetsky.P	(4,0%)
Bredlab.SME	(0,9%)
Zafi.D	(0,4%)
Muestra: 42.340.961 Detecciones: 59.656	

Font: INTECO

Enllacem amb...

<http://www.hispasec.com>

La pàgina d'Hispacec Sistemas conté un dels serveis que podem considerar com a degà dels serveis dedicats a la seguretat de la informació, almenys en el context de l'Estat espanyol. Ens referim al butlletí electrònic de seguretat *Una al dia*, que ja fa 11 anys que es publica diàriament.

Aquest butlletí permet al responsables de seguretat i, en general, als professionals dedicats al món de la seguretat, rebre informació detallada i contrastada sobre els últims incidents de seguretat. També informa de qüestions més de fons, relacionades amb la seguretat de la informació. Cal destacar la rigorositat de totes les seves informacions.

La subscripció al butlletí resulta quasi obligada per a qualsevol professional amb responsabilitat en matèria de seguretat. És gratuïta i es pot fer des de la pàgina principal del lloc d'Hispacec.

L'autenticació en autoserveis de tràmits administratius

Ramon Miralles. Coordinador d'Auditoria i Seguretat de la Informació
Agència Catalana de Protecció de Dades

El reglament de desplegament de la LOPD, aprovat pel RD 1720/2007 (RLOPD), defineix el procés d'autenticació com el «*procediment de comprovació de la identitat d'un usuari*» (art. 5.2.b). Per tant, té com a finalitat verificar que un usuari (art. 5.2.p RLOPD) que intenta accedir a un recurs d'un sistema d'informació, o a les dades que gestiona, és realment qui diu ser, a fi de d'autoritzar-ne o no l'accés al sistema o informació.

El principi de seguretat de les dades, regulat per l'art. 9 de la LOPD, obliga els responsables de fitxers i, si escau, els encarregats del tractament, a garantir la seguretat de les dades que tracten. Una de les finalitats d'aquesta protecció és evitar l'accés no autoritzat a les dades.

Una possible conseqüència de l'autenticació incorrecta de les persones que accedeixen a la informació de caràcter personal és que es produeixi una revelació de les dades a una persona que no és la interessada (art. 5.1.c RLOPD).

L'art. 93.1 del RLOPD obliga el responsable del fitxer o tractament a «*adoptar les mesures que garanteixin la correcta identificació i autenticació dels usuaris*». Per tant, un procés d'autenticació que no impedeixi, d'una forma raonable i proporcionada a l'estat de les tecnologies i a les característiques del sistema d'accés, que un tercer (no autoritzat o legítimat) pugui accedir a les dades personals d'una altra persona, pot suposar que les dades s'estiguin tractant sense les condicions de seguretat exigides.

Els processos d'autenticació d'usuaris relacionats amb l'accés a sistemes d'informació, és a dir a tractaments automatitzats, es consideren més o menys robustos (nivell de garantia de la identitat verificada) segons els factors d'autenticació que aportin el mecanisme de verificació utilitzat.

A nivell teòric es consideren 3 possibles factors d'autenticació:

- El que l'usuari coneix (típicament una paraula de pas o PIN)
- El que l'usuari té (un certificat digital, un testimoni USB (*token*), una targeta de coordenades, etc.)
- El que l'usuari és (dades biomètriques)

Per determinar la robustesa d'un procés d'autenticació, es fa referència a quins d'aquests factors preveu el procediment d'autenticació. D'aquesta manera, s'anomenen "de doble factor" si, per exemple, utilitzen una informació que l'usuari coneix i alguna "cosa" que l'usuari té; el cas típic seria una targeta utilitzada per accedir a un caixer automàtic d'una entitat financera (es té una targeta i se'n coneix el PIN).

Evidentment, com més factors es combinin, i més complexos siguin, en major mesura s'impedirà que algú no autoritzat pugui accedir a un sistema d'informació o a les dades que conté.

Certament, també la proporcionalitat s'ha de tenir en compte a l'hora de determinar com ha de ser el procés d'autenticació. Per tant, s'ha de valorar quines són les dades a les quals es donarà accés i quina és la interfície d'accés que s'utilitzarà, a fi que un excés de robustesa no n'arribi a dificultar extraordinàriament l'accés, o bé sigui excessiu en relació a les dades o sistemes que es volen protegir.

En relació a la qüestió de sistemes d'autoservei relacionats amb la tramitació administrativa o, en general, amb serveis de les administracions, cal tenir en compte el següent:

- Un procés d'autenticació basat exclusivament en la possessió (fotocòpia o original) o coneixement de dades d'un document d'identitat (DNI o targeta sanitària, per exemple) pot permetre que persones diferents de la persona interessada o afectada accedeixin, amb excessiva facilitat, a les dades que proporciona el sistema d'autoservei.
- Tot i que habitualment aquests sistemes comencen amb tràmits poc crítics, si la previsió és anar-ne afegint els riscos d'aquest servei es van incrementant. Per tant, el més aconsellable és que, des de l'inici, el mecanisme d'autenticació ofereixi les màximes garanties.
- Una mesura proporcionada és preveure un mecanisme d'autenticació de doble factor. És a dir, combinar la presentació o coneixement del DNI amb un codi, paraula, informació, PIN, etc. que, a priori, es consideri que només coneix la persona identificada en el DNI o document identificatiu mitjançant el qual es vol fer la gestió. En aquest sentit, el DNI seria l'usuari i allò que coneix l'usuari, la paraula de pas que l'autentica.
- Òbviament, la paraula de pas no ha de figurar o no s'ha de deduir del document d'identitat. Però sí que, per exemple, podria ser una de les informacions que formés part del sistema d'informació al qual es vol accedir, o alguna altra informació que es proporcionés *ad hoc* a l'usuari (per exemple, un PIN lliurat per l'administració pública per als tràmits en línia).
- L'ús de DNI electrònic o altres targetes o dispositius que incorporin funcions criptogràfiques basades en sistemes de clau pública (certificats digitals de CATCert, per exemple), juntament amb la necessitat de PIN per utilitzar el dispositiu, resulten proporcionats i suficientment robustos als efectes de garantir un accés autoritzat a les dades.

I, per últim, l'ús de dispositius biomètrics requereix una anàlisi detallada, en especial quant a quin impacte produeixen sobre la privacitat de les persones. L'ús ha de ser proporcionat, ja que a priori poden ser més intrusius que d'altres sistemes i poden causar rebuig entre els usuaris.