cesicat

GUIA D'ÚS DEL CORREU ELECTRÒNIC

Índex

Qui fem aquesta guia

El Centre de Seguretat de la Informació de Catalunya, CESICAT, és l'organisme executor del Pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de març de 2009. La missió d'aquest pla és la de garantir una Societat de la Informació Segura Catalana per a tots. Amb aquesta finalitat, es crea el CESICAT com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

El Pla nacional d'impuls de la seguretat TIC a Catalunya s'estructura al voltant de quatre objectius estratègics principals que seran desenvolupats pel CESICAT:

- Executar l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya
- Donar suport a la protecció de les infraestructures crítiques TIC nacionals
- Promocionar un teixit empresarial català sòlid en seguretat TIC
- Incrementar la confiança i protecció de la ciutadania catalana en la societat de la informació.

La forma jurídica del CESICAT és la de "fundació del sector públic de l'administració de la Generalitat".

Amb l'objectiu de proporcionar unes bones pràctiques i uns coneixements mínims en seguretat de la informació, el CESICAT ofereix com a servei preventiu un conjunt de guies de seguretat adreçades a ciutadans, empreses, administracions públiques i universitats.

www.cesicat.cat

Introducció

Audiència

Aquesta guia està adreçada als usuaris d'Universitats i Centres de Recerca, Administracions públiques catalanes i PIME que utilitzen el correu electrònic dins de l'entorn professional.

Indirectament, també pot resultar d'interès per als administradors de plataformes de correu electrònic i per als responsables de seguretat d'aquestes comunitats, doncs els pot ser útil a l'hora de conscienciar els usuaris de l'organització pel que fa a l'ús d'aquest servei corporatiu i pot ajudar a proposar mesures per fer més segures aquestes plataformes.

Aquesta guia també s'ha pensat per als responsables de seguretat que pertanyin a organitzacions que en un futur pròxim vulguin implantar un Sistema de Gestió per a la Seguretat de la Informació (SGSI). Si bé aquesta guia no es podria incorporar directament dins del cos normatiu del sistema de gestió, sí que inclou tots els aspectes i les recomanacions que l'organització hauria de tenir presents durant la implantació prèvia a la superació del procés de certificació.

Abast

Aquest document no s'ha desenvolupat per a cap plataforma o client de correu electrònic en concret, sinó que pretén assolir unes bones pràctiques en seguretat de la informació mitjançant l'ús responsable del correu electrònic.

Per tant, tota conclusió que es pugui extreure d'aquesta guia serà aplicable a qualsevol solució particular de correu electrònic, doncs bona part de les recomanacions aquí incloses tenen

incidència directa en l'ús que els usuaris fan del correu electrònic i, indirectament, en el producte que utilitzen.

Aspectes legals i normatius

La present guia s'ha elaborat tenint en compte les recomanacions provinents de l'estàndard internacional ISO 27002, que queden recollides als controls següents:

- 10.4.1 Controls contra codi maliciós.
- 10.8.1 Polítiques i procediments per a l'intercanvi d'informació.
- 10.8.4 Missatgeria electrònica.
- 10.10.1 Registres d'auditoria (logging).
- 11.3.1 Ús de les contrasenyes.
- 11.4.2 Autenticació d'usuari per a les connexions externes.
- 11.5.1 Processos de connexió segurs.
- 11.5.2 Identificació i autenticació d'usuaris.
- 12.2.3 Integritat dels missatges.
- 13.1.1 Notificar dels esdeveniments de seguretat.
- 15.1.2 Drets de la propietat intel·lectual.

El compliment d'aquesta guia també afavorirà el compliment del Reial decret 1720/2007 associat a la Llei Orgànica de Protecció de Dades de Caràcter Personal.

Descripció general

Què és i en què consisteix?

El correu electrònic és un dels serveis principals que ofereix la xarxa a l'hora de comunicar-nos ràpidament mitjançant missatges.

Tal com succeeix amb el correu postal, tothom posseeix una adreça, en aquest cas electrònica, a on es poden enviar els missatges, entenent per missatge tant comunicacions de text, com l'enviament d'imatges, so o filmacions. Aquesta adreça electrònica la proporciona la pròpia organització als treballadors.

Si bé quan utilitzem el correu postal fem servir sobres de paper, bústies tancades amb clau o mecanismes de confirmació de recepció, entre d'altres solucions, per tal de garantir que la informació arribi en les condicions que desitgem, dins del món digital també cal adoptar un conjunt de mesures de seguretat.

Finalitat

La finalitat del correu electrònic és proporcionar una comunicació ràpida entre persones d'arreu del món. El fet d'utilitzar Internet facilita una comunicació quasi instantània, contràriament a les limitacions del món físic.

Aquest servei, per tant, agilitza en gran mesura les gestions i comunicacions d'una organització, sempre que els usuaris l'emprin correctament. En cas contrari, el servei no només pot consumir considerablement els canals de comunicació digitals de l'organització a la qual pertany i impedir que d'altres serveis informàtics que utilitzin aquests canals de comunicació funcionin amb un

rendiment òptim, sinó que també pot comprometre'n la infraestructura informàtica si algun tipus de descàrrega inclou la introducció de codi maliciós dins de la xarxa particular de l'organització en qüestió.

Casos d'estudi

Per què es rep un gran volum de correu brossa

Descripció

Encara que un correu electrònic hagi estat identificat automàticament per la plataforma de l'organització on s'envia com a correu brossa, tant pot ser que aquest correu sigui realment perillós com que es tracti d'un correu ordinari que ha estat etiquetat incorrectament. Aquest segon cas és el que es denomina un "fals positiu".

Si bé quan s'envien correus electrònics únicament de text, arriben sense problemes al destinatari, quan aquests correus incorporen fitxers de tipus executable, com aplicacions o presentacions, de vegades la plataforma de correu de l'organització els etiqueta erròniament com a correu no desitjat com a mesura de prevenció, encara que aquests correus realment no siguin perillosos. Aquesta situació també pot produir-se quan s'adjunta un fitxer molt voluminós a un correu electrònic, per tal d'impedir que aquests tipus de correus puguin arribar a saturar el servei corporatiu i causar un mal funcionament. En aquestes situacions cal parlar amb l'administrador de la plataforma perquè el correu pugui ser entregat correctament al destinatari o bé sol·licitar a l'emissor que torni a enviar el correu electrònic modificant l'extensió del fitxer adjunt o enviant la informació fragmentada en diversos correus electrònics de menor mida.

Encara que existeixin falsos positius, són molts els correus brossa reals que s'envien diàriament a través d'Internet. Utilitzar o registrar l'adreça de correu electrònic en entorns o serveis digitals no corporatius, com ara xar-

xes socials, pàgines personals o llistes de distribució de notícies, ajuda a difondre l'existència i vigència de l'adreça de correu electrònic i, per tant, l'adreça es converteixen en candidata a ser inclosa en llistes de distribució de campanyes de màrqueting de tercers o de missatges fraudulents, entre d'altres.

Utilitzar el correu electrònic professional per a qüestions personals, com ara el reenviament de missatges de correu electrònic en cadena, també ajuda difondre l'adreça de correu electrònic.

D'altra banda, si un dels nostres contactes en algun moment ha resultat infectat per algun tipus de codi maliciós que propicia l'enviament indiscriminat de missatges de correu electrònic als contactes de la seva agenda electrònica, és probable que finalment l'adreça de correu electrònic de l'emissor hagi estat inclosa a la llista negra de la plataforma corporativa del receptor.

Amenaces

Infecció per codi maliciós

Els fitxers adjunts als correus electrònics poden estar infectats per codi maliciós. Aquest tipus de codi podria arribar a paralitzar la infraestructura informàtica de tota l'organització i impedir l'operativa habitual dels membres.

Pesca (*phising*) combinada amb enginyeria social

Si bé hi ha correus electrònics que no són perillosos per si mateixos perquè no incorporen codi maliciós que es pugui activar una cop l'usuari executi l'arxiu on s'amaga, sí que a vegades incorporen un missatge dirigit a espantar l'usuari de tal manera que aquest estigui disposat a actuar immediatament.

Aquests tipus de missatges acostumen a incorporar un enllaç cap a una pàgina web que, tot i que sembla legítima, és una imitació de la pàgina real mitjançant la qual es roben l'identificador d'usuari i la contrasenya d'accés de la víctima.

Correu brossa

Recepció de grans volums de correu electrònic no desitjat a les bústies professionals dels usuaris que ocupen espai del servidor de correu electrònic inútilment i consumeixen temps de l'usuari a l'hora d'eliminar-los de la bústia de correu.

Denegació de servei

Col·lapse de la plataforma de correu corporativa a causa de la recepció de nombrosos correus electrònics no desitjats o de correus electrònics molt voluminosos.

Per què cal una contrasenya d'accés al correu electrònic

Descripció

El correu electrònic serveix per enviar missatges digitals en nom d'un professional. Per evitar que una tercera persona pugui enviar un missatge des d'una bústia de correu electrònic que no sigui seva, l'accés a aquesta bústia es protegeix mitjançant algun tipus de control d'accés. El control d'accés més habitual utilitzat per les organitzacions és la combinació d'un identificador d'usuari i una contrasenya.

Si el propietari d'aquesta bústia no gestiona correctament la seva contrasenya, podria donar-se el cas que una tercera persona enviés missatges en nom del titular de la bústia. És per aquest motiu que moltes organitzacions difonen internament entre els seus usuaris una norma de contrasenyes per tal de conscienciar el seu personal de la necessitat de vetllar per la correcta definició d'una contrasenya que sigui prou segura com per no ser descoberta fàcilment per una tercera persona i per tal d'assegurar que aquesta contrasenya es protegeix adequadament.

També cal tenir present que els avenços tecnològics que s'han anat produint han propiciat que es pugui accedir al correu electrònic utilitzant dispositius mòbils com els telèfons mòbils, dispositius PDA, etc., que permeten emmagatzemar localment els correus electrònics. Per tant, la pèrdua d'aquests dispositius pot comprometre la confidencialitat de la informació que emmagatzemen i fer possible que un tercer utilitzi el dispositiu mòbil per enviar correus electrònics suplantant la identitat de l'usuari.

Amenaces

Suplantació d'identitat

Si una tercera persona aconsegueix tenir accés a la nostra bústia de correu, podrà fer-se passar per nosaltres sense aixecar sospites. S'ha de tenir especialment present que molts dispositius mòbils permeten descarregar el correu directament al dispositiu sense que per fer-ho se sol·liciti a l'usuari cap contrasenya per accedir al correu electrònic. Aquesta informació ja es troba configurada per defecte al dispositiu de l'usuari per evitar que aquest l'hagi d'introduir en cada descàrrega automàtica de correu, que pot estar programada per a què es produeixi molt freqüentment.

Pèrdua d'informació confidencial

Si algú diferent al propietari del compte de correu electrònic hi pot tenir accés, pot apropiar-se de tota la informació emmagatzemada a les bústies d'aquest compte de correu.

En el cas dels dispositius mòbils, perdre el dispositiu mitjançant el qual es té accés al correu electrònic corporatiu permet a qui el trobi, no només tenir accés a la informació guardada al propi dispositiu, sinó també a tota la informació de la bústia de correu.

Com gestionar correus electrònics amb seguretat

Descripció

Molts professionals realitzen la seva activitat diària a les instal·lacions de la seva organització, però també existeix una gran nombre de professionals que utilitza infraestructures telemàtiques que permeten moure's pel territori. És en aquest últim cas, quan s'utilitzen infraestructures de l'organització combinades amb infraestructures de tercers, que la confidencialitat en l'intercanvi d'informació per correu electrònic pot veure's compromesa.

D'entrada, pot ser que aquest usuari no utilitzi un client local per descarregar-se el correu (Outlook, Eudora, etc.) perquè, per exemple, utilitza un ordinador d'un tercer i accedeix al correu mitjançant una pàgina web. Si accedim a

aquesta pàgina web mitjançant el protocol HTTP, el canal de comunicació no estarà xifrat enlloc d'HTTPS (correu web), per la qual cosa una tercera persona podria interceptar el missatge enviat.

D'altres usuaris, en canvi, potser es poden descarregar el correu localment des d'una ubicació remota, però per fer-ho utilitzen xarxes públiques de connexió a Internet. Aquestes xarxes públiques poden ser centres telemàtics, punts lliures d'accés sense fil, etc. Si aquest canal de comunicació no està xifrat, el missatge podria ser interceptat.

Si bé la confidencialitat de la informació és important quan s'utilitzen recursos de tercers, també ho és per a aquells missatges que, encara que no surtin de la xarxa interna de l'organització, contenen informació confidencial. Així, un missatge intercanviat entre dos membres d'una mateixa organització que es troben en un mateix espai sense utilitzar mecanismes de xifrat podria ser interceptat internament per una altra persona de l'organització o enviat a un destinatari incorrecte, amb la qual cosa es comprometria el secret d'aquesta informació.

Amenaces

Pèrdua d'informació confidencial

Si una persona diferent del destinatari legítim pot llegir la informació que li envia un emissor, pot apropiar-se de la informació a la qual ha tingut accés sense que el destinatari real se'n adoni.

Recomanacions

Cadascun dels escenaris plantejats en aquesta guia exposa un seguit d'amenaces que, si es materialitzen al llarg del temps, en major o menor mesura, tindran efectes perjudicials per a l'usuari i, fins i tot, per a l'organització a la qual pertany. Per tal d'evitar que això succeeixi o minimitzar-ne l'efecte si és que l'amenaça no pot es pot eludir totalment, a continuació es proporcionen tot un conjunt de recomanacions dirigides als usuaris que utilitzen correus electrònics en l'àmbit professional.

Recomanacions per tal de minimitzar la presència de correu brossa a les bústies professionals dels usuaris

L'usuari haurà de tenir en compte les recomanacions següents per tal de disminuir el risc que suposa el rebre correus brossa a la bústia de correu professional:

- Sempre que sigui possible, és millor enviar correus electrònics que no continguin documents adjunts, incorporant la informació al cos del missatge i no en un fitxer independent.
- A l'assumpte del missatge cal escriure una frase que ajudi el receptor a saber de què tracta i que permeti filtrar-lo, prioritzar-lo, arxivar-lo i més endavant recuperar-lo.
- No obrir missatges de correu electrònic i, encara menys, fitxers adjunts en els supòsits que es descriuen a continuació. Esborrar aquests missatges sense obrir-los i, a continuació, eliminar-los de la paperera.
- Si es desconeix qui és el remitent del missatge.

- Si el títol del missatge no indica quin és el motiu del missatge.
- Si el missatge és inesperat o per algun motiu resulta estrany, independentment de qui en sigui l'emissor. Possiblement es tracta de correu brossa o d'un missatge generat per virus o un altre codi maliciós.
- No adjuntar imatges o fitxers voluminosos al missatge (fitxers amb imatges, fotografies, presentacions, etc.), si existeix una altra manera de compartir la informació amb el destinatari (directoris compartits, espais de col·laboració, etc). Si és imprescindible adjuntar un fitxer, cal incloure al contingut del missatge una breu descripció del mateix i indicar el format en què s'envia.
- Comprimir sempre que sigui possible els fitxers adjunts i no enviar directament fitxers executables, ni fitxers tipus script.
- No contestar mai els missatges de correu brossa, ni respondre a l'opció de "donar de baixa la subscripció" d'aquests missatges, per evitar donar a conèixer als emissors d'aquest tipus de correus que es tracta d'una adreça de correu vàlida i evitar així que pugin intensificar l'enviament de correu brossa.
- No respondre mai a sol·licituds de claus que arribin mitjançant el correu electrònic. Cal desconfiar de qualsevol petició de dades personals i no proporcionar mai informació personal o financera en resposta a un correu electrònic, ni utilitzar enllaços incorporats a aquests correus electrònics o a pàgines web de tercers.
- Desactivar la funció de "vista prèvia" als clients de correu electrònic (Outlook, Thunderbird, Eudora, Lotus Notes, etc.), per evitar infeccions víriques.
- És recomanable que qualsevol incidència (problema o mal funcionament) o anomalia (comportament estrany o inesperat) del correu electrònic que detecti l'usuari siguin notificats al més aviat possible a l'administrador o operador del servei mitjançant el procediment existent dins l'organització per evitar possibles mals majors.
- La majoria dels servidors de correu electrònic estan dotats de solucions de seguretat que escanegen els missatges d'entrada i sortida per prevenir possibles infeccions. No obstant això, si es té sospita d'infecció per virus o altre codi maliciós, no s'ha de fer servir el correu electrònic per evitar-ne la propagació interna.

Si bé les recomanacions anteriors estan destinades a minimitzar la presència de correu brossa procedent de l'exterior de l'organització a la bústia de correu professional, hi ha un conjunt de bones pràctiques que, si s'observen, reduiran la presència de correus innecessaris d'àmbit corporatiu que, si bé no són nocius tècnicament, sí poden consumir temps i recursos personals i materials:

Escriure els missatges amb llenguatge professional; no ser massa informal o col·loquial. No escriure res que no es posaria en una carta. Cal ser neutral i evitar llenguatge sexista, insultant, abusiu o discriminador, que pogués ofendre o irritar els altres.

Cal ser respectuós amb el temps dels altres. Enviar missatges de correu únicament a les persones amb una necessitat legítima de la informació. No respondre a missatges si no aporten valor afegit.

Dirigir el missatge (camp “Per a:”) a les persones de les quals s’espera un acció o resposta. Enviar còpies (camp “a/c”) a les persones que es vol mantenir informades, però de les quals no s’espera cap acció o resposta.

Configurar els missatges amb l’opció “Importància alta” només en els casos realment urgents.

Utilitzar les opcions de seguiment dels missatges enviats (confirmació de recepció, etc.) quan realment sigui necessari i tenint en compte que només funcionarà si el servidor de correu del receptor està configurat per fer-ho.

En cas d’absència durant més d’un dia i quan el programari de correu ho permeti, és recomanable utilitzar l’opció “fora de l’oficina”, indicant el primer i últim dia d’absència, per notificar a les persones que ens envien missatges fins quan estarem absents i amb qui poden contactar en cas d’urgència.

Recomanacions per tal de minimitzar l’amenaça de perdre el control de la bústia de correu electrònic dels usuaris

L’usuari haurà de tenir en compte les recomanacions següents per tal de disminuir el risc que suposa el fet que un tercer pugui tenir accés a la seva bústia de correu electrònic sense el seu coneixement:

- Les credencials d’accés a les bústies de correu personals d’àmbit professional seran personals i intransferibles.
- L’usuari farà un ús adequat de les seves credencials d’accés i no les revelarà a tercers ni les apuntarà en cap suport (notes adhesives, blocs de notes, agenda, etc.) que s’escapi del seu control directe.
- En cas que de manera temporal o permanent sigui necessari que altres persones accedeixin a la bústia de l’usuari, ja sigui només per lectura, o per llegir i enviar missatges en el seu nom, no se’ls donarà a conèixer les credencials d’accés, sinó que l’usuari haurà de fer-ho a través de les opcions de “Delegació d’accés”, quan el programari de correu ho permeti. Si no és possible, una altra opció per permetre la lectura és reenviar el correu a la bústia de l’altra persona.
- És responsabilitat de l’usuari complir la norma de contrasenyes de la seva organització, especialment en els aspectes de confidencialitat i seguretat de la paraula de pas [1].
- Per raons de seguretat, s’evitarà activar l’opció de “Recordatori de contrasenya” per accedir a la bústia de correu professional, encara que això comporti la necessitat de realitzar el procés de validació cada vegada que s’activi l’enviament i recepció de missatges.
- En el cas dels dispositius mòbils que permetin accedir al correu electrònic, és aconsellable activar una contrasenya d’accés al dispositiu, per protegir la informació que conté o a la qual permet accedir.

Recomanacions per protegir la confidencialitat de la informació intercanviada per correu electrònic

L'usuari haurà de tenir en compte les recomanacions següents per tal d'evitar el risc de divulgació d'informació confidencial intercanviada mitjançant l'ús de bústies de correu electrònic:

- Les llistes de distribució s'utilitzen per difondre de manera massiva avisos, alarmes i comunicats. En el moment de crear-la cal definir qui tindrà accés a aquesta llista de distribució i qui serà el responsable de mantenir-la i gestionar-la.
- Abans d'enviar un missatge a una llista de distribució, és recomanable analitzar si no existeixen altres eines de comunicació massiva (butlletins, intranets, etc.) més adients per realitzar el comunicat. Sobretot, cal revisar si tots els membres de la llista realment han de rebre el missatge.
- Si es contesta un missatge, incorporar el cos del missatge al qual es respon, per mantenir intacta la cadena d'informació, però abans de respondre un missatge, cal assegurar-se que tota la informació que s'està reenviant pot ser revelada al destinatari.
- Si s'ha de reenviar un missatge amb informació confidencial, cal assegurar-se que tota la informació que s'està reenviant pot ser revelada al destinatari.
- Per enviar informació confidencial a través del correu electrònic, caldrà utilitzar mitjans de seguretat addicionals, doncs el correu en si mateix no és un mitjà de comunicació segur. Quan es disposi de certificat digital i es tingui la certesa que el receptor podrà desxifrar el missatge, es recomana fer-lo servir. En cas de no disposar de certificat digital es poden encriptar els fitxers que contenen la informació utilitzant, per exemple, les opcions d'encriptació amb contrasenya que inclouen les opcions de gravació de fitxers amb seguretat d'alguns programes d'ofimàtica (en aquest cas, cal triar les opcions de clau més llarga, com a mínim de 1.024 bits, i posar una paraula de pas de com a mínim 8 posicions, combinant lletres, nombres, símbols, majúscules i minúscules).
- El correu electrònic no sempre substitueix el telèfon i no garanteix la lectura per part del receptor. Abans d'enviar un missatge cal considerar si és el mitjà més adient per fer-ho. En cas d'urgència, és convenient advertir el receptor per telèfon de l'enviament del missatge i confirmar-ne la recepció. Caldrà utilitzar un certificat digital reconegut quan sigui necessari garantir jurídicament la identitat de l'emissor, la integritat de la informació continguda, la confidencialitat d'aquesta informació i la no refutació per part del receptor. Cada organització haurà d'indicar quines són les CA autoritzades, qui pot demanar un certificat i quin és el procediment de sol·licitud/aprovació de certificat digital o fer referència a un procediment específic de certificats digitals.
- L'accés al correu corporatiu des de l'exterior s'ha de fer de manera segura. Un cas habitual consisteix a habilitar als treballadors l'accés per Internet mitjançant correu web. Existeixen opcions més segures i recomanables com utilitzar l'accés via VPN (Virtual Private Network).
- Encara que s'enviïn xifrades, no escriure en un ma-

teix correu electrònic totes les dades d'accés a un sistema o document (identificador d'usuari, contrasenya, clau d'encriptació, etc.), independentment de qui les estigui demanant.

- És recomanable incorporar al peu dels correus electrònics que s'envien una clàusula estàndard per informar de la possible confidencialitat de la informació continguda al missatge i la responsabilitat associada a qui el rep. Si el sistema no afegeix aquesta clàusula automàticament, cal configurar la bústia de correu per tal que ho faci en l'enviament i reenviament de missatges. Una clàusula vàlida podria ser la següent:

****

La informació continguda en aquest missatge és confidencial. Si no en sou un dels destinataris definits o algú responsable de fer-los-el arribar, aleshores heu rebut aquest missatge per error i no esteu autoritzats a llegir-lo, retenir-lo o distribuir-lo. Us preguem que esborreu el missatge i els documents annexats, ho comuniqueu immediatament al remitent i us abstingueu d'utilitzar les dades personals que hi consten.

****

- Utilitzar únicament programari autoritzat per l'organització, la qual haurà valorat els avantatges i inconvenients del programari utilitzat dins de la corporació.

D'altra banda, l'usuari haurà de tenir en compte les recomanacions següents per tal d'evitar el risc de divulgació d'informació confidencial emmagatzemada a la seva bústia de correu electrònic o en un dispositiu mòbil:

- Cal ser selectiu a l'hora d'emmagatzemar correus i conservar només els que puguin ser útils en el desenvolupament de la feina.
- És recomanable no guardar els missatges de manera sistemàtica i permanent i fer revisions de depuració periòdica.
- Guardar els missatges que s'hagin de conservar, en format no xifrat, en una ubicació que tingui garanties de confidencialitat, integritat i continuïtat. Comproveu la política aplicada en aquest servei, l'espai de memòria individual, els procediments de depuració automàtica periòdica, etc. És recomanable que, quan s'emmagatzemi el contingut dels correus electrònics, s'indiqui amb quina finalitat es fa.
- Com a norma general, tret que s'hagi fet servir una signatura electrònica, el correu electrònic no es pot considerar com un registre de negoci formal, perquè no garanteix l'autenticitat, integritat, exactitud, completesa, no refutació i preservació de l'evidència. A més, és informació subjecta a canvis de versió o programari, de manera que no s'hauria de guardar com a registre permanent. Existeixen altres maneres per formalitzar decisions o compromisos com ara actes de reunions, documents signats o registres autoritzats de veu.
- Utilitzar únicament programari autoritzat per l'organització, la qual haurà valorat els avantatges i inconvenients del programari utilitzat dins la corporació.

Conclusions

El correu electrònic es va fer servir per primer cop l'any 1965, quan encara ningú no s'imaginava la forta repercussió que tindria a les xarxes de comunicació actuals. Aquesta facilitat de comunicació, com s'ha pogut comprovar en el transcurs d'aquesta guia, té uns avantatges, però també uns inconvenients. Pel que fa als inconvenients, se n'han identificat de dues naturaleses diferents:
Un ús inapropiat del correu electrònic pot tenir un impacte social i econòmic negatiu per a l'organització (enviament de correus molestos o innecessaris, etc.).

Un ús del correu electrònic sense observar les degudes mesures de seguretat pot tenir un impacte negatiu econòmic, legal i d'imatge per a l'organització (divulgació de pressupostos, nòmines o dades personals, infecció dels sistemes informàtics per un virus, etc.).

És per aquest motiu que, cada vegada amb més freqüència, les organitzacions incorporen a les seves normes internes codis de conducta per a la utilització del correu electrònic, a fi i efecte de minimitzar l'impacte que podrien tenir per a l'organització determinades conductes dels usuaris quan utilitzen el correu corporatiu.t.

Glossari de termes

Certificat digital: el certificat digital és un sistema d'acreditació que permet a les parts tenir confiança en les transaccions a Internet, doncs garanteix la identitat del seu posseïdor a Internet mitjançant un sistema segur de claus administrat per un tercer de confiança (l'autoritat de certificació). El certificat permet realitzar, de manera segura i amb validesa legal, tot un conjunt d'accions que varia segons el tipus de certificat: signar documents, xifrar missatges, entrar a llocs restringits, identificar-se davant l'Administració, etc.

Codi maliciós: qualsevol codi informàtic destinat a realitzar accions fraudulentes. Es consideren codi maliciós els virus i cucs informàtics, els troians (permeten fer-se amb el control d'una màquina), etc.

Llista de distribució: és un conjunt d'adreces de correu electrònic que s'agrupen sota una única adreça de correu electrònic. Quan es fa un enviament a una llista de distribució, s'està fent l'enviament a totes les adreces incloses a la llista. La creació de llistes facilita l'enviament de missatges a grups de persones a qui ens adrecem habitualment de manera conjunta, doncs evita haver d'escriure totes les adreces de correu electrònic cada vegada i en pot garantir la privacitat.

Generalment els clients de correu permeten la creació de llistes de distribució personals, accessibles únicament per a l'usuari que les ha creades.

Les llistes de distribució globals, visibles per a qualsevol usuari del sistema de correu, han de ser creades per l'administrador del sistema.

Logging: procés de validació a un sistema o servei telemàtic.

Pesca o phishing: pràctica delictiva que consisteix a suplantar a la xarxa una empresa de confiança (normalment un banc, una caixa d'estalvis, una empresa asseguradora, etc.) per tal d'apropiar-se dels identificadors d'usuari i les contrasenyes associades dels seus clients en línia i, així, poder entrar als seus comptes i obtenir informació confidencial o bé un benefici econòmic directe.

Spam: pràctica d'enviar missatges de correu electrònic no sol·licitats. Generalment es tracta de publicitat de productes, serveis o pàgines web, però també pot incorporar codi maliciós o enllaços web per perpetrar atacs de phising. Les adreces de correu electrònic acostumen a ser robades, comprades, recol·lectades per la web o preses de cartes en cadena.

La pràctica de l'enviament de correu brossa constitueix un problema que afecta de manera negativa tots els usuaris de la xarxa. La legislació vigent prohibeix de manera expressa l'emissió d'aquest tipus de correu.

Script: conjunt d'instruccions tècniques que s'executen de manera automàtica en un sistema.

VPN: en anglès, Virtual Private Network (VPN). És una tecnologia de xarxa que permet l'extensió de la xarxa local a una xarxa pública o no controlada, com per exemple Internet. La VPN aconsegueix aquest objectiu mitjançant la connexió d'usuaris des de diferents xarxes a través d'un túnel que es construeix sobre Internet o qualsevol xarxa pública. Aquest túnel utilitza mecanismes d'encriptació.

Referències i enllaços web

S'ha utilitzat com a referència en l'elaboració de l'actual guia:

•GE-GUI26-01 Guia d'us correu electrònic, del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI).

•[1] DOC-GUI-001 Guia gestió de contrasenyes: Aquest document és una guia de seguretat que consisteix en proporcionar unes bases d'ús i gestió correctes de les contrasenyes.
[PDF] http://www.cesicat.cat

A la web s'hi pot trobar informació rellevant, relacionada amb la matèria desenvolupada en aquesta guia:

•Estudi sobre la situació, naturalesa i impacte econòmic i social del correu electrònic no desitjat spam, INTECO, Juny 2008.
[PDF] http://www.inteco.es/file/1000136237

•Correu segur, Consejo Superior de investigaciones científicas CSIC.
http://www.iec.csic.es/CRIPTonOMiCon/correo/cifrado.html

•Xifrar missatges de correu electrònic, Microsoft.
http://office.microsoft.com/es-es/outlook/HP012305363082.aspx

•Com xifrar un missatge de correu electrònic individual a Outlook Web Access, Microsoft Technet, 19 de Maig del 2005.
http://technet.microsoft.com/es-es/library/aa997829%28EXCHG.65%29.aspx

•Firmat i xifrat de correus electrònics, Mozilla-hispano.
http://www.mozilla-hispano.org/documentacion/Firma_y_cifrado_de_correos_electr%C3%B3nicos

•Xifrat de correus per a novells, XTEC, any 2000.
[PDF]http://www.xtec.es/~acastan/textos/Cifrado%20de%20correo%20para%20novat@s.pdf

Eines

Eines de xifratge

GNUpg.
Implementació lliure del estàndard OpenPGP definit al RFC4880.
http://www.gnupg.org/

PGP.
Implementació i foment de d'utilització PGP i OpenPGP definit al RFC4880.
http://www.pgpi.org/

Enigmail.
Extensió pel client de correu Mozilla Thunderbird que integra OpenPGP.
http://enigmail.mozdev.org/home/index.php

FireGPG, GnuPGP aplicat al servei de correu Gmail.
Extensió per al navegador Mozilla Firefox sota llicència MPL (llicència pública de Mozilla) que proporciona una in-

terfície integrada de les operacions de GNUPG al text de qualsevol pàgina web, com xifrat, desxifrat, firma i verificació de firmes.

Clients suportats: Gmail, Yahoo, Rouncube, SquirreMail, Horde.

http://es.getfiregpg.org/

Eines anti-spam

SpamAssessin.

Plataformes: Windows, Mac, Linux/Unix.

http://spamassassin.apache.org/

SpamBayes.

Plataformes: Windows, Linux i Mac OS amb multitud de clients de correu, consultar a la pàgina de descarrega.

http://spambayes.sourceforge.net/

Spamihilator.

Plataformes: Windows amb Outlook, Opera, Eudora, Pegasus, Phoenix, Netscape, Thunderbird i IncrediMail.

http://www.spamihilator.com/

SpamTerrier.

Plataformes: Windows 2000/XP/Vista i 2003, suporta els clients The Bat!, Windows Mail, Outlook Express, Outlook totes les versions.

http://www.agnitum.com/products/spam-terrier/

Recursos de suport on-line

Hushmail

Servei a la xarxa que ofereix correu segur, bústia xifrada, correu electrònic xifrat amb servei d'antivirus i antispam. Utilitza els estàndards OpenPGP.

http://www.hushmail.com/

cesicat

Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat