Ajuntament de Badalona

Expedient: 2023/31334N
Ref. Addic.:
UO Responsable: D. Informàtica i TIC
Assumpte: Servei relay, antivirus i antispam perimetral pel correu electrònic

Procediment: Incoació Expedient de Contractació (P1)
Interessat/da:
Representant:

PLEC DE PRESCRIPCIONS TÈCNIQUES PER AL CONTRACTE DEL SERVEI DE MANTENIMENT DE L'ACTUAL PLATAFORMA DELS SERVEIS DE RELAY, D'ANTIVIRUS I ANTISPAM EN EL CORREU ELECTRÒNIC DE L'AJUNTAMENT DE BADALONA

1. Justificació

L'Ajuntament considera convenient la renovació dels serveis de relay, d'antivirus i antispam en el correu corporatiu de l'Ajuntament de l'actual plataforma en cloud computing.

L'objectiu del contracte és disposar de les eines de control i supervisió per tal de garantir la seguretat dels correus electrònics de l'Ajuntament de Badalona.

Per la prestació òptima dels serveis amb els nivells de qualitat requerits, és necessari la renovació dels serveis de relay, d'antivirus i antispam en el correu corporatiu adients i que s'adaptin a les necessitats actuals i futures. Per així poder proporcionar uns serveis de qualitat als ciutadans i ciutadanes.

L'objectiu del contracte és disposar de les eines de control i supervisió per tal de garantir la seguretat dels correus electrònics de l'Ajuntament de Badalona.

2. Objecte del contracte

L'objecte del contracte és la renovació dels serveis de relay, d'antivirus i antispam en el correu corporatiu de l'Ajuntament de l'actual plataforma en cloud computing.

Aquest contracte no s'ha dividit en lots perquè la realització independent de les seves prestacions ens dificultaria la correcte execució des del punt de vista tècnic, ja que es tracta d'uns serveis molt interrelacionats i deprenents uns amb els altres.

3. Durada del contracte

S'estableix en un any sense prorroga.

4. Descripció dels serveis

4.1 Definició

L'objecte del contracte és la renovació dels serveis de relay, d'antivirus i antispam en el correu corporatiu de l'Ajuntament de l'actual plataforma en cloud computing.

L'actual plataforma en cloud computing que te l'Ajuntament és la proporcionada pel fabricant HornetSecurity.

Els serveis a contractar mitjançant l'adjudicació del contracte són els següents:

- Spam and Malware Protection
- Advanced Threat Protection (ATP)

També hi ha diversos dominis, tots gestionats pel mateix MTA:

- badalona.cat
- aj-badalona.es (alies de badalona.cat)

Els serveis a contractar no es podran modificar.

Tots els serveis hauran d'estar a nom de l'Ajuntament de Badalona i enregistrades a les plataformes de gestió corresponents.

4.2 Característiques generals del servei

Donat que el sistema ha d'estar en arquitectura cloud computing el CPD des d'on el licitador presta els serveis ha d'acomplir amb les següents característiques:

- Ha d'estar localitzat a Espanya o a un país de la Comunitat Econòmica Europea.

4.3 Gestió i control

L'adjudicatari nomenarà una persona de contacte que serà el coordinador de tots els assumptes relacionats amb la gestió del servei.

També es requereix un servei de suport per a incidències i peticions relacionades amb el servei proporcionat, d'acord amb els SLA establerts a l'apartat 5.2 i que s'haurà d'explicar en la memòria tècnica.

5. Gestió dels serveis

5.1 Detall dels serveis

Es requereixen els següents serveis i funcionalitats associats a aquesta solució:

5.1.1. Protecció antivirus, antispam, antimalware de correus

El sistema ha d'analitzar tot el tràfic de correu electrònic per verificar que estigui lliure de virus, i malware. També s'han d'aturar els correus spam detectats, s'han de passar filtres de phishing i s'han d'analitzar els fitxers adjunts. Tanmateix s'ha de protegir el servidor de correu de l'Ajuntament d'atacs de DoS i DdoS.

5.1.2. Sandboxing, reescriptura d'URLs, ATP i altres funcionalitats.

La plataforma ha de donar anàlisi dinàmic de missatges utilitzant un Sandbox que analitzi els canvis mentre els arxius adjunts s'executen o mentre s'accedeix a una URL sospitosa de fishing o descàrrega inadequada.

Aquest sistema també ha de detectar connexions sospitoses, per exemple si l'arxiu intenta comunicar-se amb un servidor per carregar un codi maliciós.

La protecció avançada contra Threads (ATP, Advanced Thread Protection) protegirà de ataques cibernètics, com ransomware, el spyware i els virus que podrien arribar a manipular o danyar els processos operatius.

Amb aquesta utilitat es pretén reduir al mínim possible les infeccions o pèrdua d'informació a través de correu electrònic, que per altra banda, és la major porta d'entrada d'aquests codis maliciosos.

5.1.2.1 Servei Sandboxing.

Les proteccions antivirus tradicionals no són suficients per detectar i detenir completament l'entrada de correus amb arxius adjunts infectats, degut a que els motors antivirus tradicionals s'actualitzen normalment cada 24 hores. Això és molt de temps sense protecció contra els milers de nous virus o mutacions que apareixen diàriament i que poden arribar a infectar xarxes senceres, amb el risc de paralitzar, en el nostre cas, tota l'administració pública.

Contra aquesta amenaça, es fa imprescindible la contractació d'un servei de sandboxing que, explicat en poques paraules, el que fa és pujar qualsevol arxiu adjunt a un correu a un ordinador virtual generat al servidor del proveïdor del servei. Un cop pujat a l'entorn virtual segur, el fitxer adjunt s'executa i s'analitza el seu comportament, per detectar de si es tracta d'un arxiu maliciós. Si no es detecta cap comportament anormal passats uns minuts, el correu amb l'adjunt és entregat al seu destinatari.

5.1.2.2. Funció de reescriptura d'URLs.

Cada vegada és més freqüent que els missatges de correu portin adreces d'Internet i enllaços a serveis de descàrrega de fitxers com Dropbox, Wetransfer, Google Drive, etc. Això està sent aprofitat pels ciber-delinqüents per llençar atacs dirigits amb correu amb enllaços que porten a descàrregues malicioses capaces d'infectar no només el PC de l'usuari, sinó tota una xarxa corporativa.

Per això es fa també totalment necessari disposar d'un servei de reescriptura d'URLs. Essencialment, aquest servei el que fa és analitzar i reescriure mentre s'analitza el destí de qualsevol enllaç que es trobi dins del cos d'un missatge que entra a la xarxa municipal, per certificar que el contingut a descarregar no és maliciós.

La reescriptura d'URL de protecció avançada contra amenaces combina la verificació del temps de clic amb els mètodes d'inspecció del lloc. La verificació del temps de clic bloqueja l'accés a llocs maliciosos mitjançant l'ús de les creixents bases de dades d'intel·ligència d'URL i dominis d'Hornetsecurity que contenen milers de milions de conjunts de dades de pesca i programari maliciós. Quan la verificació inicial passa, el servei escaneja el lloc de destinació per detectar indicadors maliciosos de compromís, per exemple, enllaços incrustats a càrregues útils malicioses o formularis de pesca. Després de completar aquestes exploracions i si el lloc objectiu no s'ha declarat maliciós, l'usuari és redirigit al lloc.

5.1.2.3 Serveis que inclou el ATP

La plataforma ha de donar anàlisi dinàmic de missatges utilitzant un Sandbox que analitzi els canvis mentre els arxius adjunts s'executen o mentre s'accedeix a una URL sospitosa de fishing o descàrrega inadequada.

Aquest sistema també ha de detectar connexions sospitoses, per exemple si l'arxiu intenta comunicar-se amb un servidor per carregar un codi maliciós.

La protecció avançada contra Threads (ATP, Advanced Thread Protection) protegirà de ataques cibernètics, com ransomware, el spyware i els virus que podrien arribar a manipular o danyar els processos operatius.

Amb aquesta utilitat es pretén reduir al mínim possible les infeccions o pèrdua d'informació a través de correu electrònic, que per altra banda, és la major porta d'entrada d'aquests codis maliciosos.

El servei ha de incloure un tercer motor d'antivirus premium: basat en signatures de definicions de malware locals i motors heurístics.

En resum , el sistema ha de poder realitzar:

- Anàlisis Sandboxing d'arxius.
- Anàlisis de URL i links maliciosos.

5.1.2.4 Altres funcionalitats

Freezing: Els correus electrònics que no es poden classificar de manera definitiva, però que són sospitosos, es retenen durant un curt període de temps congelant-los. El correu electrònic es torna a escanejar: tan aviat com els motors de detecció de virus reben el «hit», el correu electrònic es trasllada directament a la quarantena.

Alertes en temps real: Que notifiquen als equips de seguretat informàtica corporatius sobre atacs detectats en temps real.

Alertes Ex-Post: Que notifiquen als equips de seguretat informàtica corporatius si un correu electrònic que ja s'ha lliurat es classifica posteriorment com a maliciós, amb una avaluació detallada de l'atac que permeti iniciar immediatament les contramesures pertinents.

5.1.2.5 Perfils d'usuari

El sistema ha de proporcionar dos perfils d'usuari diferenciats. El perfil administrador, per a que personal del departament de TIC pugui consultar i gestionar regles, llistes blanques i negres, etc. i un

perfil d'usuari per a que el propi usuari pugui ser autònom en la recuperació dels e-mails identificats com a falsos positius o fins i tot pugui gestionar les seves llistes blanques i negres.

5.1.2.6 Panel de control

La gestió de regles i llistes per evitar l'spam seran gestionades per l'Ajuntament i l'adjudicatari, donant la possibilitat a l'administrador de l'Ajuntament a comunicar incidències per a perfeccionar la detecció o bé poder-ho gestionar d'una manera més autònoma.

Informes i estadístiques

El sistema ha de proporcionar un sistema automàtic de reports i estadístiques per analitzar l'ús i funcionament de la plataforma.

Així mateix, cada usuari ha de rebre un report individualitzat diari amb el resum de correus electrònics adreçats a la seva adreça i que el sistema ha posat en quarantena com a possible spam, donant la possibilitat de rebre'l.

5.1.2.7 Seguiment del servei

Es requereix la formalització de reunions periòdiques del servei, amb un mínim d'una reunió semestral, per:

- avaluar la situació del servei,
- detectar desviaments en el servei susceptibles de ser tractats, o
- per a propostes de futur en quant a nous serveis, o
- canvis de model de funcionament que puguin sorgir en el futur.

També cal que l'adjudicatari informi de les noves funcionalitats de la plataforma i configuri, segons indicacions del servei tècnic de l'Ajuntament de Badalona, aquestes funcionalitats, prèvia comunicació i explicació del servei.

5.2 Acord de Nivell de Servei (SLA)

S'estableixen els següents paràmetres mínims de nivell de servei (SLA), valorant-se la seva millora.

Paràmetre	SLA mínim exigit
Horari d'atenció telefònic o per correu electrònic	De dilluns a divendres de 8 a 18 hores
Temps de resposta a incidències	2 hores
Temps de resolució d'incidències	4 hores
Temps de resposta a peticions	4 hores
Temps de resolució a peticions	8 hores
Taxa de reconeixement d'spam	99,9%

Taxa de reconeixement de virus	99,8%
Taxa màxima de falsos positius	0,005 %

5.3 Termini de desenvolupament i entrega

El termini màxim de la aplicació dels serveis no podrà superar el termini d'un mes des de la formalització del contracte.

El lloc de lliurament serà a les instal·lacions de l'Ajuntament de Badalona.

6. Equip de treball

L'adjudicatari haurà de informar del personal tècnic o unitats tècniques de les que es disposi per a l'execució del contracte.

L'empresa adjudicatària ha de disposar d'una persona encarregada de supervisar i coordinar la prestació del servei. Qualsevol incidència haurà de ser resolta sense que afecti a la prestació normal del servei.

El licitador haurà d'acreditar mitjançant la presentació d'una declaració responsable amb el compromís d'adscriure a l'execució del contracte els mitjans tècnics, materials i humans suficients per executar aquest contracte.

Disposar de les següents certificacions:

- Per part del fabricant:
  - Certificació en ENS, nivell mig com a mínim o declaració responsable que està realitzant la corresponent certificació.
- Per part de l'adjudicatari
  - Certificació de l'empresa com a Partner de Hornetsecurity.

7. Confidencialitat

L'empresa adjudicatària queda obligada a no divulgar cap dada o informació obtinguda durant l'execució del contracte, referent a dades personals com a organització, mitjans tècnics, mesures de seguretat, etc.

Excepte autorització expressa, no podrà extreure ni utilitzar informació (especialment dades personals), tant dels sistemes informàtics com de qualsevol altre origen. Aquesta serà posada a disposició de l'empresa adjudicatària per part de l'Ajuntament quan sigui necessària.

Igualment l'empresa adjudicatària ha de complir les obligacions legals que imposa el nou Reglament Europeu sobre Protecció de Dades Personals, així com la legislació associada que se'n derivi, durant l'execució del contracte.

8. Accions per a una contractació pública responsable

El servei objecte del contracte es desenvoluparà respectant les normes sociolaborals vigents a Espanya i en la Unió Europea, i de l'Organització Internacional del Treball.

En la determinació del pressupost del contracte s'haurà de tenir en compte el salari base i totes aquelles retribucions establertes en el conveni, pactes o contractes laborals que resultin de l'aplicació al contracte.

En el desenvolupament del servei objecte del contracte s'hauran d'adoptar, en tot cas, les mesures previstes en matèria de seguretat i salut en el treball, i les mesures necessàries per evitar que de l'execució del contracte es puguin derivar danys al personal municipal o a la ciutadania en general.

L'empresa adjudicatària en el moment de formalitzar el contracte, acreditarà mitjançant declaració responsable l'afiliació i l'alta en la Seguretat Social de les persones treballadores destinades a l'execució del contracte. Aquesta obligació s'estendrà a tot el personal subcontractat per l'empresa adjudicatària principal.

En tot cas s'haurà de respectar el principi de no discriminació per raó de gènere i s'haurà d'evitar l'ús del llenguatge i imatges sexistes, que es fa extensiu a la documentació que presenti el/s licitador/s.

9. Facturació de la despesa

Abonament del preu i requisits de facturació

1. El pagament del preu del contracte que se'n derivi de la tramitació d' aquest procediment es realitzarà, contra les factures que de forma **mensual**, a mes vençut i de forma electrònica d'acord amb les previsions de la llei estatal 25/2013, de 27 de desembre, d'impuls de la factura electrònica i creació del registre comptable de factures en el sector públic, presenti el contractista, sempre i quan aquestes reuneixin els requisits reglamentaris i siguin conformades o validades pel responsable del contracte.

2. La facturació inclourà la identificació de l'òrgan administratiu amb competències en matèria de comptabilitat pública, la Intervenció General, així mateix, haurà d'identificar l'òrgan de contractació. Tot això, de conformitat amb la Disposició addicional 32.2 de la LCSP.

3. Tanmateix, els requisits de facturació s'adaptaran als canvis que al llarg de la vigència del contracte estableixin les disposicions de caràcter general aplicables o les bases d'execució del pressupost o altra normativa municipal.

Signatures requerides:

Perfil Signatari-Data de signatura