AJUNTAMENT DE TORTOSA
SECRETARIA GENERAL
Aprovat per la Junta de Govern Local en sessió de data 28 de març de 2022.

El secretari accidental,

PLEC DE PRESCRIPCIONS TÈCNIQUES PER AL SUBMINISTRAMENT EN MODALITAT D'ARRENDAMENT D'ÚS DE LLICÈNCIES I FUTURES ACTUALITZACIONS DE PROGRAMARI ANTIVIRUS

1.- Objecte del contracte

L'objecte del present plec és determinar les condicions tècniques que han de regir la contractació del subministrament en modalitat d'arrendament d'ús de les llicències i futures actualitzacions del programari antivirus "Panda Adaptive Defense 360" per a llocs de treball i servidors. La contractació d'un servei de protecció completa d'equips (els llocs de treball dels usuaris i servidors) controlant el comportament de cada un dels processos executats al parc informàtic de l'Ajuntament de Tortosa a més de proveir dels mitjans de detecció i desinfecció de *malware*. Així com les eines necessàries per a la seva gestió i administració per part del propi Ajuntament i el servei de suport per part del fabricant.

Actualment l'Ajuntament disposa de llicències de diferents versions del producte "PANDA ADAPTIVE DEFENSE 360" en modalitat d'arrendament d'ús que deriven de dos contractes amb diferents proveïdors. Un, amb 330 llicències, que atén les necessitats dels diferents departaments municipals i que es gestionat per la unitat d'informàtica, que finalitza el dia 6 de juny de 2022. I un altre que gestiona el Centre de Formació Ocupacional per protegir els equips del centre que es destinen a la realització de programes subvencionats, per al que disposen de 95 llicències i que finalitza a finals del mes de març.

L'objectiu és unificar aquestes necessitats mitjançant la realització d'un sol contracte, que ha de resultar més eficient, flexible i econòmic per a l'Ajuntament, si bé mantenint la possibilitat de facturació del contracte per centres de cost a l'efecte de fer més eficient la imputació de costos pels diferents programes subvencionats.

L'objecte del present contracte consisteix en la contractació del subministrament en modalitat d'arrendament d'ús, amb efecte des del dia 6 de juny de 2022, de la llicència per un període de tres (3) anys següent:

Nom del Producte	Codi de producte	Número de llicències
Panda Adaptive Defense 360 3 anys	A3AD360C	501

Les llicències subministrades han de permetre mantenir tota les configuracions de perfils i grups que ja es troben definides actualment així com l'històric i donar continuïtat al sistema de seguretat sense escletxes en el moment del canvi així com disposar del suport especialitzat durant el període de vigència del contracte.

2.- Requisits tècnics

2.1. – Actius a protegir

La solució ha de donar protecció inicialment a 501 equips. La solució ha de ser escalable i permetre que, si durant la durada del contracte fossin necessàries llicències addicionals,

aquestes s'integren funcionalment dintre de la solució oferta.

2.2.- Ubicació plataforma

Amb la finalitat de reduir els costos de manteniment i explotació de la solució, no haurà de ser necessari l'ús d'una plataforma interna, es precisa una solució basada en *cloud*. És requisit mínim que la plataforma on s'allotgi la infraestructura es trobi fora de les nostres instal·lacions i operada pel fabricant de la solució en un model *cloud*, el qual permeti el creixement i escalabilitat de la plataforma. Assegurant que independentment del nombre de nodes de la instal·lació la plataforma funcioni amb el mateix nivell d'eficiència i eficàcia.

La plataforma ha d'estar allotjada a la Unió Europea.

Existeixen nodes que estan distribuïts per diferents seus i fins i tot en mobilitat per la qual cosa aquests aprofitaran la disponibilitat de la infraestructura *cloud* perquè estiguin integrats de forma completa en la configuració i actualització de la solució.

La plataforma de gestió ha de cobrir els principals nivells de certificació com és la ISO 27001.

2.3.- Components del servei

2.3.1. Infraestructura Cloud

La solució proveirà, des del núvol, el conjunt de servidors, bases de dades i processos de tractament de la informació relacionada amb el servei. Els processos capturats dels clients seran tractats en el núvol de tal forma que l'impacte sobre els sistemes corporatius sigui mínim.

2.3.2. Agent, a desplegar en els equips.

L'agent desplegat permetrà la comunicació i gestió de punt la protecció d'antivirus tradicional així com de la protecció de processos desconeguts.

Recollirà la informació corresponent als esdeveniments i els components que els produeixen, sense recopilar informació, ni documents d'usuari. L'impacte sobre els dispositius del parc haurà de ser menor al 5% de rendiment de la CPU, memòria i disc.

L'agent ha de ser capaç de protegir equips de sobretaula i portàtils amb els sistemes operatius següents:

- Des de Microsoft Windows XP SP3 fins a Microsoft Windows 11.

Haurà de protegir equips servidors amb les versions de sistema operatiu:

- Des de Microsoft Windows 2003 fins a Microsoft Windows Server 2022.

La desinstal·lació de la protecció haurà de protegir-se mitjançant contrasenya.

La solució deu poder desplegar-se de manera silenciosa mitjançant els següents mecanismes: per adreça IP, rang d'adreces IP, nom de màquina i grups de Directori Actiu basat en polítiques de domini.

2.3.3. Consola Web

La solució proporcionarà una interfície en el qual es puguin consultar les dades en temps real, descarregar informes/alertes, accedir a la configuració i disposar de les actualitzacions dels agents.

Els administradors municipals del servei podran gestionar des d'una única consola i de manera centralitzada, mitjançant qualsevol navegador web la seguretat i productivitat de totes les estacions de treball i servidors Windows fins i tot ordinadors portàtils i oficines remotes.

2.4.- Protecció

La protecció sol·licitada es dividirà en dues parts:

- Endpoint Protection Platform (EPP)
- Endpoint detection and response (EDR)

Aquestes dues parts tindran que estar combinades i fusionades a nivell de configuració, tan sols estaran dividides a nivell de funcionalitats. I estar compost per un sol agent i una sola solució. No es permetrà l'ús de diferents components.

2.4.1.- Endpoint Protection Platform

La solució de EPP (Endpoint Protection Platform) ha de comptar com a mínim amb les següents funcionalitats:

- Antivirus per a arxius, correu i web. Permetent la detecció i desinfecció de qualsevol tipus d'amenaça. Detectant malware per comportament. El correu detectarà tant en SMTP com en POP3. Quant a la protecció web quan es detecti intents d'accés a pàgines web que continguin elements maliciosos, els bloquejarà.
- Firewall personal gestionat en local o de forma centralitzada des de la consola web. Ha de permetre:
    - Bloquejar les connexions entrants i/o sortints de les aplicacions que desitgi
    - Prevenció d'intrusions
    - Crear regles de firewall per a permetre/denegar el trànsit en sentit entrant/sortint dels equips seleccionats per a determinats protocols/ports.
- Bloqueig de tots els dispositius o dispositius específics (unitats d'emmagatzematge extraïbles, dispositius de captura d'imatges, unitats de CD/DVD, mòdems USB, Bluetooth, etc.), impedint l'entrada de malware i fugides d'informació. Permetent la definició de diferents accions per a cada tipus de dispositiu (bloqueig, accés, lectura/escriptura).
- Bloqueig d'accés a pàgines web no desitjades. Ha de ser possible configurar aquesta protecció basada en categories encara que es podran també afegir llistes blanques i negres de llocs i dominis permesos.

2.4.2.- Endpoint detection and response

Es requereix una solució de tipus EDR (endpoint detection and response) per a protegir com a mínim de les següents amenaces:

- Malware avançat
- PUP (potential unwanted programs)
- Amenaces zeroday tipus ransomware
- Troians de nova generació indetectables pels antivirus.

Aquesta solució haurà d'evitar al màxim les infeccions de forma proactiva. La solució ha d'aportar contramesures diferents a les següents:

- Signatures locals, que requereixen de constants actualitzacions
- Motors heurístics, que necessiten d'un ús de CPU i poden produir falsos positius.
- Sistemes de llistes blanques, ja que no disposem de personal suficient per a l'administració d'aquest tipus de sistemes.
- Sistemes de sandboxing que consumeix recursos i el malware pot eludir-los.

El sistema de protecció ha de ser capaç de classificar el 100% dels processos executats en les maquines, generant un classificació de malware o goodware.

És un requisit que es produeixi el bloqueig dels processos desconeguts que s'intenti executar per a evitar la possibilitat de danyar les dades accessibles per la maquina (com pot ser el xifrat no desitjat) o el robatori o accés de dades.

Ha d'incloure un sistema Anti-Exploit que permet la detecció i bloqueig de l'ús de exploits coneguts o desconeguts.

S'ha de poder establir diferents nivells de bloqueig (més o menys restrictius) així com diferents nivells en la capacitat dels usuaris de poder desbloquejar individualment els processos bloquejats pel sistema.

2.4.3.- Plataforma de gestió d'informació auditada

El sistema ha de generar informació forense relacionada amb cada equip de tal forma que pugui ser explotada posteriorment. La informació generada pel sistema de protecció es dividirà en tres parts:

1. Informació inclosa en la consola núvol: El sistema ha d'incloure informe per amenaça detectada en la qual es correlacioni les accions que ha fet el procés o en el context que ha estat implicat, per exemple si ha estat descarregat d'Internet o ha estat extret d'un fitxer comprimit. L'entorn ha de ser amigable i fàcil de seguir, sense exigir grans coneixements d'amenaces avançades. A més ha d'incloure informes d'estat de les proteccions, de les deteccions de malware i informes executius amb el resum de la informació global.

   Els informes s'han de poder obtenir de forma immediata amb les dades en temps real i també de forma periòdica per correu electrònic i en diferents formats per al seu posterior tractament.

2. Informació d'esdeveniments: ha de disposar d'un sistema SIEM en núvol que permeti recopilar dades dels esdeveniments produïts en els processos. Aquest haurà d'emmagatzemar tant els esdeveniments produïts per amenaces com aquells que no ho són. El sistema ha de ser capaç de gestionar les dades emmagatzemades per a poder realitzar les funcions normals d'un sistema de base de dades, com són: filtrat, agrupacions o camps calculats. Ha d'incloure la possibilitat d'exportar la informació i la possibilitat de realitzar gràfics representatius de les dades emmagatzemades. La informació que ha d'emmagatzemar aquest sistema és la següent:

   a. Informació relacionada amb les alertes detectades en els equips, ha d'incloure informació de si es va produir l'execució del procés o no i de quin procés es tracta.
   b. Informació dels arxius executables i comprimits descarregats d'altres ubicacions.
   c. Informació dels processos que accedeixin a fitxers de dades com són per exemple arxius de WinWord, Excel, Acrobat PDF, etc. Així com la informació de

saber quins equips, amb quins usuaris han accedit a un arxiu concret, on es pugui detectar possibles fugides de dades.
d. Informació relacionada amb els processos executats a la màquina controlant els usuaris que els llancen.
e. Informació de les connexions que es produeixen des d'un equip tant externes a la xarxa com internes, ha d'incloure quin procés les realitza.
f. Informació relacionada amb els accessos al registre de Windows.
g. Accions d'intercepció d'esdeveniments dels drivers existents en el SO (ex. Hooks de teclat, pantalla, etc.) així com tota instal·lació, esborrat, modificació i execució de "drivers" (controladors de dispositius del SO) involucrats en l'incident de seguretat.
h. Informació relacionada amb el consum d'ample banda relacionat amb aplicacions i usuaris.
i. Relació d'aplicacions vulnerables en els equips i quines d'elles s'estan executant.

3. Ha d'incloure panells pre-configurats amb informació maquetada de les diferents informacions que s'inclouen. Es necessiten els següents panells:

   a. Processos executats en les maquines per fabricant de processos.
   b. Aplicacions instal·lades i executades
   c. Consum d'ample banda usat per les aplicacions i usuaris
   d. Destinació de les connexions.
   e. Màquines en les que hi ha hagut accés dels usuaris.

Sobre la base d'aquesta informació també s'inclouran alertes que permetin la detecció d'activitats no desitjades, com l'execució de diferents aplicacions, amplada de banda usada, accés a determinats equips, obertura de fitxers, etc.

2.4.4. Servei d'alerta d'amenaces (Threat Hunting)

Es requereix un servei que alerti i prengui les mesures correctives adequades quan es detecti una activitat anòmala en els equips basada en el comportament normal auditat anteriorment al parc d'equips.

Aquest servei haurà d'estar ofert pel fabricant de la solució EDR per tècnics especialitzats usant les dades que hagi recollit en l'auditoria forense.

Han de poder realitzar l'alerta i la inclusió en la intel·ligència del sistema EDR de les mesures correctives.

2.5.- Neteja de sistemes

Es requereix un sistema de neteja dels equips de tal forma que es pugui realitzar a demanda una neteja de rastres d'amenaces o programes no desitjats que l'antivirus no hagi pogut eliminar pel desconeixement de l'amenaça o per no estar inclòs en la desinfecció del producte d'antivirus.

El sistema de neteja ha de ser configurable i transparent per a l'usuari final de tal forma que sigui possible llançar-lo a qualsevol equip independentment d'on estigui localitzat.

2.6.- Informació

El sistema ha de generar informació forense relacionada amb cada equip de tal forma que pugui ser explotada posteriorment. El sistema haurà d'incloure informe per amenaça detectada en la qual es correlacioni les accions que ha fet el procés o en el context que ha estat implicat, per exemple si ha estat descarregat d'Internet o ha estat extret d'un fitxer comprimit. A més ha d'incloure informes d'estat de les proteccions, de les deteccions de malware i algun informe executiu amb el resum de la informació global.
Els informes s'han de poder obtenir de forma immediata amb les dades en temps real i també de forma periòdica per correu electrònic i en diferents formats per al seu posterior tractament.

2.7.- Certificacions i esquema nacional de seguretat

La solució obligatòriament ha d'estar inclosa en el "Catàleg de Productes de Seguretat de les Tecnologies de la Informació i la Comunicació." (CPSTIC) Publicat pel CCN (Centre Criptogràfic Nacional), dins de la família de protecció del Lloc de treball com a QUALIFICAT.

La solució ha de tenir la certificació de garantia EAL2+ en avaluació de l'estàndard Common Criteria (https://www.commoncriteriaportal.org/)

Tecnologia Cloud Pública, és obligatòria que tingui la certificació de conformitat enfront del ENS, de categoria alta.

3.- Suport tècnic 24x7x365

S'establirà el manteniment i assistència tècnica que permeti assegurar el correcte funcionament en tots els llocs i servidors de l'organització mitjançant:

- Servei de suport ofert pel fabricant per telèfon en català o castellà amb telèfon d'accés prioritari.
- Service Packs i hotfixes: accés a les millores tècniques del producte durant el temps d'activació del servei
- Web de suport: accés a fòrums, blogs, informació sobre últimes amenaces, enciclopèdia de virus, ...
- Suport tècnic via email 24x7x365, per tècnics certificats en la solució implementada
- Accés a anàlisi online de virus ocults
- Accés il·limitat al Helpdesk: sense límit d'incidències

El contracte haurà d'incloure una visita a l'Ajuntament de Tortosa cada sis mesos d'una durada de 4 hores per part d'un tècnic especialista en la solució del fabricant.

4.- Condicions de Lliurament

El lliurament de l'objecte del contracte es realitzarà per l'empresa adjudicatària segons les indicacions que li facilitarà el responsable del contracte.

L'empresa adjudicatària haurà de lliurar el corresponent document en el qual consti el número de llicències a lliurar, així com el número de contracte d'aquestes i el número de client atorgat pel fabricant a l'Ajuntament de Tortosa.

5.- Termini del lliurament

L'empresa adjudicatària queda obligada a efectuar el subministrament com a màxim el dia 7 de juny de 2022, data en que finalitza la vigència de les llicències de que actualment disposa

Ajuntament de Tortosa

l'Ajuntament.

Tortosa,

El Cap de la Unitat de Sistemes d'Informació