Ajuntament de Sabadell

CODI DE VERIFICACIÓ	603X 3P6G 2N5S 3S0S 0XKT				
EXPEDIENT NÚM.	TIC/2024/5	DOCUMENT NÚM.	TIC18I005C	DATA	16-02-2024
ÀREA	Àrea d'Economia i Serveis Centrals				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Renovació de llicències Centre d'Operacions de Ciberseguretat				

Plec de Prescripcions Tècniques pel Subministrament de subscripcions de les llicències per les eines que formen part del SOC de l'Ajuntament de Sabadell

Ajuntament de Sabadell

Sabadell, febrer 2024

1. INTRODUCCIÓ 3

2. OBJECTE 3

3. ABAST 4

3.1. Security Information and Event Management (SIEM) 4

3.1.1. Acords De Nivell De Servei (SLA) 4

3.2. Web Application Firewall (WAF) 4

3.2.1. Requeriments 5

3.3. Network Acces Control (NAC) 5

3.3.1. Requeriments 6

3.4. Kaspersky Automated Security Awareness Platform – Conscienciació dels usuaris en ciberseguretat 6

4. TERMINIS 6

CODI DE VERIFICACIÓ	603X 3P6G 2N5S 3S0S 0XKT				
EXPEDIENT NÚM.	TIC/2024/5	DOCUMENT NÚM.	TIC18I005C	DATA	16-02-2024
ÀREA	Àrea d'Economia i Serveis Centrals				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Renovació de llicències Centre d'Operacions de Ciberseguretat				

INTRODUCCIÓ

L'Ajuntament de Sabadell disposa d'una infraestructura informàtica i de telecomunicacions sobre la que es dona servei tant a la organització interna com a la ciutadania, donant compliment als requeriments normatius establerts per les Lleis 39/2015 i 40/2015 i el Reial Decret 203/2021.

Sobre aquesta infraestructura, hi ha implantades diferents solucions tecnològiques per garantir la gestió electrònica integral dels diferents processos i procediments administratius. Avui en dia, s'han implantat eines per, entre altres, possibilitar la relació telemàtica amb els ciutadans, per garantir la interconnexió de dades i documents amb altres administracions, per garantir una gestió basada en el document i l'arxiu electrònic, etc.

El canvi normatiu expressat en aquestes lleis, ha comportat que aquests sistemes d'informació estiguin exposats a internet i els fa vulnerables a possibles atacs que poden comprometre'n la disponibilitat, la integritat i la confidencialitat de les dades tractades.

El disseny i l'operació d'aquestes eines recau en el Programa de Tecnologia i Sistema del Servei de Tecnologia i Transformació Organitzativa de l'Ajuntament de Sabadell.

En aquest marc, l'any 2022, l'Ajuntament va adquirir tot un seguit d'eines amb aquesta finalitat:

- Eina MONICA NGSIEM, dos appliances físics que l'allotgen i llicències pel seu funcionament, que permet:
  - una recopilació centralitzada i en temps real de logs i evidències de cadascuna de les aplicacions que composen el Centre d'Operacions,
  - la classificació de logs i evidències per temàtica,
  - l'anàlisi ràpid i àgil dels diferents logs i evidències recollits.
- Eina de Control d'Accés a Xarxa (NAC) del fabricant HPE Aruba Networkinng anomenada ClearPass, que ha estat vinculada a MONICA NGSIEM i que permet controlar i restringir l'accés a la xarxa corporativa interna.
- Eina Web Application Firewall (WAF), que permet protegir a l'Ajuntament de possibles atacs múltiples als servidors d'aplicacions web de la xarxa interna, també vinculada a MONICA NGSIEM.
- Eina Kaspersky Automated Security Awareness Platform, per promoure la sensibilització entre els treballadors de l'Ajuntament i la formació en seguretat.

OBJECTE

L'objecte de la present contractació és el subministrament de les subscripcions a les llicències SIEM, NAC, WAF i Eina de Formació en ciberseguretat, incloent el manteniment del Hardware i el Software de la eina MONICA NGSIEM adquirida al 2022, durant un període de 3 anys.

ABAST

El contracte inclourà el subministrament de la subscripcions de les llicències esmentades en SIEM, NAC, WAF i Eina de Formació. També inclourà el manteniment del Hardware i el Software de la Eina MONICA NGSIEM, així com el suport en la definició de noves alertes dins la plataforma.

Security Information and Event Management (SIEM)

El SIEM de l'Ajuntament de Sabadell rep la quantitat de 1250 esdeveniments per segon i això genera un volum aproximat de 50GB d'alertes diàries, en un sistema de 250 actius i 27 monitors.

La renovació de la subscripció de les llicències de l'eina MONICA NG-SIEM inclou la llicencia d'ús del programari, la gestió dels appliances MONICA NG-SIEM amb S/N: E263790X2A02230 i E263790X2A02238, les actualitzacions de la plataforma, el suport en la gestió i el funcionament de la plataforma, la validació de les alertes actives i el suport en la definició de noves fonts, alertes i monitors. Aquestes subscripció ha d'incloure la revisió anual de tota la plataforma per garantir el correcte funcionament de la mateixa.

L'empresa adjudicatària haurà d'estar habilitada pel fabricant de l'Eina MONICA NGSIEM per realitzar les subscripcions i caldrà presentar document acreditatiu d'aquest habilitació.

Acords De Nivell De Servei (SLA)

Temps de resposta de les incidències

Es considera temps de resposta al que transcorre des de la comunicació fins a l'inici de la fase de resolució (comunicació entre el tècnic assignat i l'Ajuntament). Aquest no serà superior a 24 hores.

Temps de resolució

Es considera temps de resolució al que transcorre des de la comunicació de la incidència fins a la seva completa resolució. El temps mig de resolució no superarà les 72 hores.

Web Application Firewall (WAF)

És objecte del contracte el subministrament de subscripcions de les llicències WAF (*Web Application Firewall*) CloudFlare Business que analitzi i filtri el tràfic adreçat a aplicacions web específiques.

La solució aportada haurà de gestionar el tràfic d'un únic domini (Sabadell.cat) amb diferents webs allotjades i amb els seus corresponents certificats SSL, durant un període de 3 anys.

CODI DE VERIFICACIÓ	603X 3P6G 2N5S 3S0S 0XKT				
EXPEDIENT NÚM.	TIC/2024/5	DOCUMENT NÚM.	TIC18I005C	DATA	16-02-2024
ÀREA	Àrea d'Economia i Serveis Centrals				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Renovació de llicències Centre d'Operacions de Ciberseguretat				

El principal motiu de la contractació del WAF és protegir els webs municipals enfront d'atacs DDoS, fora de la infraestructura municipal.

Requeriments

- Mitigació d'atacs DDoS il·limitada,
- Protecció enfront d'atacs com DoS, DDoS, diferents tipus d'injecció, *spoofing*, explotació de vulnerabilitats conegudes, etc..
- 25 conjunts de regles personalitzades, en el WAF,
- Càrrega personalitzada individual o compartida, sobre SSL/TLS 1.2 y 1.3,
- Conformitat amb PCI DSS 3.2,
- TTL d'expiració mínim de caché perimetral establert en 30 minuts,
- Certificat SSL universal,
- Anàlisis de *bots* sofisticats i *bots* bàsics,
- Fins a 50 regles per pàgina,
- Acord de nivell de servei: 100% actiu,
- Cal integrar mitjançant API's, web services o logs amb el MONICA NGSIEM de que disposa l'Ajuntament.
- Suport remot ininterromput per correu electrònic, eines de *ticketing* i *chat,*
- Registres d'auditoria i anàlisi per intervals de temps de 15 minuts,
- Subscripció per un període de 3 anys,
- Sistema de pagament per quota anual i no per ús.

En la posada en marxa del servei, l'adjudicatari haurà de donar suport als tècnics municipals en les següents tasques:

- Anàlisi del domini a protegir,
- Suport en la definició de les regles,
- Suport en la integració amb el MONICA NGSIEM.

Network Access Control (NAC)

A l'any 2022 l'Ajuntament de Sabadell va adquirir una eina de Control d'Accés a Xarxa (NAC) del fabricant HPE Aruba Networkinng anomenada ClearPass. Amb aquesta eina els tècnics municipals poden controlar que només els usuaris i els equips / dispositius

autoritzats tinguin accés als recursos i serveis de xarxa en funció del seu nivell i perfil d'accés i concentrar les alertes a MONICA NGSIEM.

En concret, es disposa d'un clúster format per dos virtual appliances actiu / passiu on poden connectar-se de forma concurrent fins a 1000 dispositius finals.

Part Number	Descripció	Quantitat
JZ399AAE	Aruba ClearPass Cx000V VM Appl E-LTU	2
JZ402AAE	Aruba ClearPass NL AC 1K CE E-LTU	1

És objecte del contracte el subministrament de les subscripcions a les actualitzacions i al manteniment i suport del programari de seguretat adquirit per un període de 3 anys:

- Suport tècnic il·limitat HPE Software
- HPE Software Updates SVC

Requeriments

Aquesta Eina haurà d'estar integrada amb el MONICA NGSIEM de que ja disposa l'Ajuntament de Sabadell.

Kaspersky Automated Security Awareness Platform – Conscienciació dels usuaris en ciberseguretat

Amb el propòsit de garantir que tota la plantilla de l'Ajuntament de Sabadell adquireix un nivell de seguretat òptim es demana una eina d'anàlisi, sensibilització i formació en seguretat pels treballadors municipals. Aquesta eina haurà d'abordar els diferents aspectes relacionats amb la Seguretat en les Tecnologies de la Informació, incidint en el coneixement dels riscos i les amenaces a que poden ser sotmesos els usuaris, el coneixement sobre l'ús segur de les eines informàtiques i les bones pràctiques que permetin reduir l'exposició i els danys ocasionats en cas d'atac.

L'Ajuntament de Sabadell ja va incorporar al gener del 2023 l'eina Kaspersky Automated Security Awareness Platform i aleshores es va dur a terme un projecte que contemplava la introducció d'un conjunt de píndoles formatives que van ser presentades als usuaris, l'oferta de diferents unitats didàctiques en Seguretat en les TIC i les eines que permetien la gestió d'aquestes unitats i l'avaluació del seu seguiment.

La voluntat de l'Ajuntament de Sabadell és continuar amb aquesta eina i estendre aquesta conscienciació a la totalitat dels treballadors municipals. És per això que es demana a l'empresa adjudicatària que es comprometi a subministrar:

- **300 llicències** de Kaspersky Automated Security Awareness Platform, que hauran de ser activades per un període de 3 anys.

TERMINIS

La durada de les subscripcions serà de 36 mesos.

Salvador Maza, Raimon
CAP PROGRAMA TECNOLOGIA I SISTEMA
26/04/2024 12:21