Destinatario: Mesa de Contratación

Asunto: Informe acerca del cumplimiento de los requisitos mínimos definidos en los pliegos de prescripciones técnicas – oferta de SERMICRO

Una vez examinada la documentación de aclaración de oferta presentada por la licitadora SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS, S.A.U. (SERMICRO), rubricada el 11 de agosto de 2023 por Alfonso José Ruiz de Apodaca, en representación de la licitadora, nuevamente resulta insuficiente para acreditar el cumplimiento de los requisitos determinados en el Pliego de Prescripciones Técnicas y de los extremos ofertados objeto de valoración (informe y requerimiento de 16 de agosto de2023, CSV HUACDZ49JFLT9URLCD93), motivo por el cual se requirió a SERMICRO que llevara a cabo una demostración de los productos ofertados al objeto de proceder: 1) a la aclaración de los extremos de su oferta; 2) a la realización de una demostración de las funcionalidades de los productos ofertados; 3) a la entrega de los agentes ofertados con el fin de instalarlos en equipos de la Diputación de León para poder examinar, de manera autónoma, las diferentes características y funcionalidades que brindan y así comprobar que se ajustan a lo exigido en los pliegos de contratación y a lo ofertado.

Una vez llevada a cabo por parte de SERMICRO la demostración de la solución ofertada, a lo largo de diferentes sesiones desde el 22 de agosto de 2023 hasta el 13 de octubre de 2023, el técnico que suscribe procede a informar acerca del cumplimiento de la solución ofertada en relación con los requisitos mínimos determinados en los pliegos que rigen la contratación:

I. ACERCA DEL PAQUETE 2 DE SEGURIDA OFERTADO

El técnico que suscribe mantiene lo ya informado el 24 de mayo de 2023 (CSV HUACCMJXHT3C2YEREK77):

> *“SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS, S.A.U. (SERMICRO) - NIF: A78032315 - No cumple los siguientes requisitos PPT:*
>
> *1- ‘2.2 PAQUETE 2 DE SEGURIDAD Capacidades de protección de la navegación por DNS, mediante agente con su consola de seguridad asociada, equivalente en funcionalidad, de carácter general, a Umbrella Roaming Client de Cisco Umbrella, o a Windows Roaming Client de DNSFilter, o a DNSWatchGo de Watchguard.’*
>
> *2- ‘Dada la heterogeneidad de equipamiento y redes de los ayuntamientos, es de vital importancia que las soluciones a suministrar sean de fácil implantación, sin necesidad de adquisición de equipamiento físico en la Diputación o en los ayuntamientos, precisándose únicamente la instalación de uno o varios agentes software en cada PC y servidor (el mínimo imprescindible)’.*

Para las 2.700 unidades de 'Paquete de seguridad 2 – licencias de seguridad por 3 años.' se ofertan 2.700 unidades de 'Kaspersky Security for Internet Gateway' solución de seguridad que, según declara el fabricante en su web, está basada en proxy (no en protección DNS mediante agente), necesitándose para ello el despliegue de un servidor o appliance. No se basa, por tanto, en la instalación de un simple agente en los dispositivos a proteger ni se trata de una protección DNS, por lo que no es equivalente en funcionalidad a Umbrella Roaming Client de Cisco Umbrella, o a Windows Roaming Client de DNSFilter, o a DNSWatchGo de Watchguard."

Acerca de lo anterior, SERMICRO alega en la documentación aclaratoria rubricada el 11 de agosto de 2023 lo siguiente:

*"**Nivel de seguridad 1.** El primer nivel de seguridad se cubre mediante nuestro agente de red, el cual comunica toda la información contra la consola central (Kaspersky Security Center). Este agente de red se instala localmente en el equipo junto con KES (Kaspersky Endpoint security) Ambos aplicativos se pueden instalar de manera independiente o mediante una misma tarea. // Agente de red + KES + KSN https://support.kaspersky.com/ksc/13.2/es-ES/3305.htm*

***Nivel de seguridad 2.** El nivel de seguridad 2, es cubierto mediante nuestro segundo agente independiente KEA (Kaspersky Endpoint agent). Este agente se encarga de recoger toda la telemetría de la máquina, no solo a nivel DNS. Registra la telemetría de cualquier indicador de compromiso que se generara en el equipo (modificaciones de registro, elevación de permisos, consultas DNS, IP´s, descubrimiento, etc). // Agente/Sensor + EDR Expert: https://support.kaspersky.com/KEA/3.14/en-US/199051.htm*

Adicionalmente es importante destacar con lo arriba descrito se cumple al 100% el requerimiento del pliego.

Así mismo Kaspersky incluye en su propuesta un nivel adicional para garantizar el 100% de la navegación web.

En este caso la protección, se aplica a nivel perimetral para que independientemente de que cualquier servicio, no esté disponible, los equipos siempre estén protegidos y monitorizados a nivel de navegación, analizando todo el tráfico entrante y saliente de cualquiera de ellas a través de web traffic security."

Sobre lo alegado, una vez examinada la documentación aclaratoria y la consola de los agentes de seguridad objeto de demostración, el técnico que suscribe comprueba que el *"nivel de seguridad 2"* no puede considerarse una capacidad de protección de la navegación por DNS equivalente en funcionalidad, de carácter general, a la requerida en el pliego de prescripciones técnicas (*equivalente en funcionalidad, de carácter general, a Umbrella Roaming Client de Cisco Umbrella, o a Windows Roaming Client de DNSFilter, o a DNSWatchGo de Watchguard*). Se comprueba que se trata de una capacidad protección EDR automática (tecnología y estrategias de protección distinta a la exigida como paquete de seguridad 2) que no admite configuración específica en

relación con DNS, tal y como se requiere en el pliego de prescripciones técnicas - "Capacidad de gestión multientidad o por grupos de dispositivos, para aplicar diferentes medidas de seguridad por ayuntamiento o entidad (aproximadamente 200)"- no pudiéndose aplicar configuraciones sobre dominios o clases de dominios concretos en esta capacidad EDR (ej. una lista blanca de dominios). Además, el mencionado agente no se corresponde con lo ofertado por SERMICRO como PAQUETE 2 DE SEGURIDAD: "Kaspersky Security for Internet Gateway European Edition. 2500-4999 node 3 year add-on license - 2.700 unidades".

Además, tras configurar en la consola de demostración los referidos agentes Kaspersky Endpoint Security y Kaspersky Endpoint Agent para su despliegue, la propia consola de demostración comenzó a señalar lo siguiente:

> "A partir de la versión 11.7, Kaspersky Endpoint Security incluye la funcionalidad de Kaspersky Endpoint Agent. Cuenta con directivas configuradas en Kaspersky Endpoint Agent. Transfiera los ajustes de la configuración de la directiva de Kaspersky Endpoint Agent a las directivas de Kaspersky Endpoint Security".

Lo anterior muestra que la funcionalidad del agente **Kaspersky Endpoint Agent** estaría incluida dentro del agente **Kaspersky Endpoint Security** (la consola anima a la transferencia de la configuración y a la migración a un único agente), por lo que si siguiéramos las indicaciones del fabricante el "nivel de seguridad 2" alegado por SERMICRO finalmente no estaría soportado por un agente diferente al que argumenta como "nivel de seguridad 1" (compartiendo la misma inteligencia/infraestructura KES).

No obstante, como ya se informó el 24 de mayo, el *"nivel adicional para garantizar el 100% de la navegación web (…) a través de web traffic security.",* lo realmente ofertado por SERMICRO como PAQUETE 2 DE SEGURIDAD (*"Kaspersky Security for Internet Gateway European Edition. 2500-4999 node 3 year add-on license - 2.700 unidades"),* está basada en proxy, y por tanto no se trata de una protección DNS mediante agente a instalar en los equipos a proteger, ya que requiere el despliegue de un servidor o appliance, contraviniendo lo exigido en el pliego de prescripciones técnicas:

- 2.2 PAQUETE 2 DE SEGURIDAD Capacidades de protección de la navegación por DNS, mediante agente con su consola de seguridad asociada
- Precisándose únicamente la instalación de uno o varios agentes software en cada PC y servidor (el mínimo imprescindible).

II. ACERCA DE LAS CAPACIDADES DE ACCESO A LA CONSOLA POWERSHELL

Aun siendo los anteriores incumplimientos motivo suficiente por sí mismos para la exclusión de la oferta presentada por SERMICRO, debe destacarse la relevancia del siguiente incumplimiento de su oferta en relación con los siguientes requisitos:

- **Requisito 1:** Capacidades de despliegue de software y scripts y capacidades de soporte remoto - Capacidad de acceso a consola powershell de los usuarios de manera autónoma, sin necesidad de interrupción a los mismos.
- **Requisito 2:** Las capacidades de seguridad de los agentes dependerán única y exclusivamente de las infraestructuras del fabricante, en su nube.

Para la demostración de la "Capacidad de acceso a consola powershell de los usuarios de manera autónoma, sin necesidad de interrupción a los mismos" - que no es lo mismo que una ejecución remota de scripts powershell- SERMICRO propone ejecutar una serie de tareas en el PC al que se pretende acceder (es importante señalar que lo propuesto exige que todas y cada una de estas tareas se ejecuten por el técnico de soporte y mantenimiento cada vez que precisa acceder a la consola del PC de un usuario en esta modalidad, lo que es totalmente inoperativo y nada ágil):

- **Tarea 1:** Habilitar manualmente la característica de acceso a sesión remota powershell (Enable-PSRemoting) en el PC del usuario cuya consola se pretende acceder ("está totalmente NO recomendado ya que pone en peligro la seguridad de los equipos a los que se aplique", según se explica en la demostración). Se propone la ejecución de un script remoto para habilitar esta característica del PC (Enable-PSRemoting -force). **Observación del técnico que suscribe:** se comprueba 1) que esta modalidad de acceso a la consola propuesta se está realizando a través de capacidades de conexión remota al margen de los agentes ofertados; 2) que al habilitar la ejecución remota con la opción "-force" permite que cualquier dispositivo que se encuentre en la misma red que el PC del usuario pueda conectarse a este y ejecutar comandos, lo que pone en grave riesgo la seguridad del PC y de la red.
- **Tarea 2:** A continuación, acceder manualmente mediante comando "Enter-PSSession" a la consola del PC del usuario. **Observación del técnico que suscribe:** se comprueba que la modalidad de acceso propuesta únicamente se puede materializar si el PC del usuario se encuentra directamente accesible desde el PC del trabajador de soporte y mantenimiento, y se comprueba además que se realiza al margen de las capacidades de conexión remota de los agentes ofertados; en consecuencia con esta solución los técnicos de la Diputación de León no podrían dar soporte remoto en esta modalidad a PCs de empleados en las redes heterogéneas de los ayuntamientos ni a los PCs de la Diputación que se encuentren en redes distintas a la corporativa, como son las de los trabajadores sociales que se encuentran repartidos por la provincia, al resultar todas ellas redes ajenas a la Diputación y sin conectividad directa por parte de sus técnicos.
- **Tarea 3:** Finalmente, deshabilitar en el PC del usuario la característica de acceso a sesión remota powershell, mediante una acción manual que debe realizar el técnico de soporte tras finalizar la actuación ("Para NO disminuir el nivel de seguridad en nuestro entorno se recomienda encarecidamente volver a deshabilitar Sesión remota de PowerShell. Se puede hacer de varias formas, aquí explicamos dos de ellas // 1. Mediante una tarea EDR ([EDR] PS Remote OFF) // 2. Al cerrar la sesión PowerShell. Antes de cerrar PS, Deshabilitamos la configuración.", se explica en la demostración). **Observación del técnico que suscribe:** esto podría provocar que se dejara habilitada la característica de acceso a sesión remota powershell por olvido o por pérdida de conectividad con el PC del usuario, lo que pondría al

PC del usuario en una grave situación de riesgo ya que cualquier dispositivo en su misma red podría ejecutar comandos en su consola.

En definitiva, se observa que la solución demostrada por SERMICRO, totalmente insegura e inadecuada, no está basada en las capacidades de soporte remoto de los agentes ofertados, obligando además a activar y desactivar características en los PCs de los usuarios que los ponen en una situación grave de riesgo.

Se concluye, por tanto, que los agentes ofertados no proporcionan acceso de forma nativa y por si mismos a las consolas powershell de los PCs en los que se encuentran instalados ni desde/hacia cualquier localización que cuente con conectividad con las consolas del/os agente/s (único requisito de comunicación). Por ende, los agentes ofertados no cumplen lo requerido en el pliego de prescripciones técnicas.

PROPUESTA

Por cuanto antecede, dado que lo ofertado incumple varios de los requisitos mínimos exigidos en los pliegos que rigen la contratación, **SE PROPONE** la exclusión de la proposición de SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRÓNICOS, S.A.U. (SERMICRO) - NIF: A78032315.