Consulta expediente 2019 00000075 Contratación del suministro e implantación de la nueva infraestructura de seguridad de la CCA

PREGUNTA, página 7 del pliego de prescripciones técnicas:

"Capacidad de descifrar tráfico SSH y detección de aplicaciones no legítimas."

Sobre estas dos capacidades:

El protocolo SSH es un protocolo de administración remota que requiere de autenticación y del uso de certificados publico/privados, los Firewalls además tienen la capacidad de identificarlos mediante firmas de aplicación del protocolo, por tanto si se permite el acceso SSH desde ciertas IPs, rangos, o usuarios entendemos que se permite el uso de los comandos intrínsecos del protocolo y que no es necesario descifrar este tráfico. Igualmente este protocolo nunca se suele publicar y por tanto no son accesibles desde el exterior, ya que solo están permitidos mediante el uso de las licencias de VPN como las requeridas en el Pliego de Prescripciones Técnicas. Todas estas medidas hacen imposible el acceso a equipos con SSH de usuarios no legítimos.

El equipo es capaz de detectar aplicaciones no legitimas mediante el uso de una base de datos miles de firmas de aplicaciones que permiten detectar cualquier anomalía.

¿Son suficientes este conjunto de medidas para la protección del protocolo SSH y para la detección y protección de aplicaciones de la cámara de Cuentas?

RESPUESTA: Si.

PREGUNTA, página 8 del pliego de prescripciones técnicas:

"Utilización de la identificación de aplicaciones como criterio para seleccionar los perfiles de protección de vulnerabilidades, de forma que se apliquen solo aquellas firmas específicas según la aplicación que se está utilizando."

Las aplicaciones están basadas en un servicio sobre el cual estas funcionan, si solo se protege la aplicación quedaría vulnerable a posibles ataques que afecten al servicio/protocolo, ¿sería posible la selección de estos perfiles mediante los servicios en los que se apoyan para establecer igualmente la protección?

RESPUESTA: Si, si se implementan medidas complementarias a nivel de aplicación que suplan estas funcionalidades; no bastará con la simple selección de servicio/protocolo. Estas medidas no deben prestarse desde la nube.

PREGUNTA, página 8 del pliego de prescripciones técnicas:

"Posibilidad de que las medidas de protección ante ataques de DoS, puedan ser activadas atendiendo a criterios como la zona o conjunto de interfaces desde donde se origina el tráfico, zona o conjunto de interfaces hacia dónde va dirigido el tráfico y pudiendo restringir dentro de

estos interfaces las direcciones IP origen y destino a inspeccionar o el usuario interno de la red que puede estar originando el ataque."

¿Sería suficiente para la Cámara de Cuentas el poder restringir IP Origen, IP destino o usuario interno independientemente de las zonas, interfaces o conjuntos de interfaces?

RESPUESTA: Si.

PREGUNTA, página 9 del pliego de prescripciones técnicas:

"Los interfaces del firewall deben soportar los siguientes modos de funcionamiento: modo TAP para monitorizar tráfico de forma pasiva a través de puertos mirror, modo transparente para inspección de tráfico en el flujo de datos y despliegues "in line", modo layer 2 o switching y modo layer 3 o routing y la capacidad de usarlos todos de forma simultánea."

El firewall es capaz de monitorizar el tráfico de forma pasiva independientemente del modo en que se despliegue tanto en modo in-line, switching o haciendo routing, ¿entendemos que es suficiente para lo que requiere la Cámara de Cuentas?

RESPUESTA: Si.

PREGUNTA, página 9 del pliego de prescripciones técnicas:

"Capacidad de realizar policy based routing en base a IP o en base a red de origen, o también basado en usuarios/grupos o por tipo de aplicación"

El firewall es capaz de realizar routing basado en políticas de IP, redes o agrupación de las mismas siendo capaz de encaminar el trafico según se desee. Igualmente el equipo permite tanto rutas estáticas, como los principales protocolos de encaminamiento dinámicos como RIP, OSPF o incluso BGP. ¿Se alinea con los requerimientos del escenario de enrutamiento sobre líneas de comunicaciones de datos de la Cámara de Cuentas?

RESPUESTA: Si.

PREGUNTA, gestión de la seguridad: respecto del SIEM, volumetrías asociadas para la valoración (EPSs y número de fuentes a integrar, o número de fuentes y volumen de logs a almacenar) y horario del servicio.

RESPUESTA:

Número de fuentes: servidores Windows, servidores Linux, VMWARE y electrónica de red (CISCO).

Volumen de logs a almacenar: 1 Gbyte/día sin comprimir, pero tiene un amplio margen de racionalización.

Horario del servicio: dependerá de la oferta realizada.

PREGUNTA, gestión de la seguridad: respecto de la gestión de vulnerabilidades, ¿cuántas IPs internas y externas hay que analizar y con qué periodicidad?

RESPUESTA:

IPs internas y externas: 95 IPs internas y 18 IPs externas, lo cual no implica que estos números no puedan variar.

Periodicidad: dependerá de la oferta realizada.

PREGUNTA, plazo de garantía.

RESPUESTA: 3 años, ampliables según criterios de adjudicación.