

Los Servicios Gestionados de Seguridad a examen



Statistics

Analytics

Los servicios gestionados de seguridad a examen

Si una cosa ha quedado clara durante la pandemia es que el perímetro de seguridad ha dejado de existir como consecuencia de la adopción masiva del teletrabajo y una aceleración en la adopción de la nube. Se le une una creciente complejidad de los procesos de las organizaciones, de la confluencia entre la IT y la OT, un incremento de las ciberamenazas, una mayor profesionalización de los ciberdelincuentes, que no dudan en utilizar, ellos también, tecnologías de inteligencia artificial para garantizar el éxito de sus ataques.

Los entornos IT también se hacen más complejos. Se habla ahora de microarquitecturas, de contenedores, de desarrollo ágil, de computación en el Edge, de moverse en entornos cada vez más complejos que hay que asegurar con la misma diligencia que se ponía en proteger un servidor de correo on-premise... en aquellos años.

Se suma una enorme falta de profesionales que hacen necesario el compartirlos. Se hace necesario un soporte de seguridad integral que permita a las organizaciones mantenerse seguras y



itds

Encuentros ITDS

además alejarse de la primera línea de defensa para prestar atención al cliente y al crecimiento de su empresa.

Los proveedores de servicios de seguridad gestionados, o MSSP, se han convertido en un recurso de incalculable valor para las empresas que desean incrementar sus niveles de seguridad.

A nivel global, el mercado de servicios de seguridad gestionada crecerá de 31.600 millones de dólares en 2020 a 46.400 millones de dólares en 2025, lo que representa un tasa de crecimiento anual del 8,0% durante el periodo.

Con el objetivo de saber a ciencia cierta cuál es la situación a la que se enfrentan los respon-

sables de ciberseguridad de las empresas, qué debe esperarse de los servicios de seguridad gestionados, qué elementos se echan en falta, o cómo saber escoger la mejor entre una enorme oferta, se ha celebrado una mesa redonda bajo el título “Los Servicios de Seguridad Gestionada a examen”, que ha reunido a Javier Sánchez, CISO de Haya Real Estate; Daniel Zapico, CISO de Globalia; Manuel Barrio Pare-

des, CISO de Solvia; Carlos Asún, CISO de Food Delivery Brands y Rafael Luque, CISO de INECO, de una parte y a Francisco Valencia, Director General de Secure&IT; Álvaro Fernández, Enterprise Account Executive de Sophos Iberia y Carlos Tortosa, Director de grandes cuentas de ESET, de otra.

A continuación, podrán leer un resumen de las intervenciones de cada uno de los participantes.

Los Servicios de Seguridad Gestionada a examen

LOS SERVICIOS DE SEGURIDAD GESTIONADA A EXAMEN

CLICAR PARA VER EL VÍDEO



SOPHOS



Managed Threat Response

Tome medidas contra las ciberamenazas

Un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

Más información



LA VISIÓN DE LAS EMPRESAS

**GLOBALIA. Daniel Zapico, CISO**

Retos tenemos muchísimos dice Daniel Zapico, CISO de Globalia. En relación a los servicios gestionados plantea este directivo que quizá la pregunta sería ¿qué nos lleva a los servicios gestionados? Una de las razones es la dificultad de encontrar perfiles, “no hay gente, y menos aún gente lo suficientemente cualificada”, dice, añadiendo que si además hablamos de tareas de seguridad ofensiva suelen ser gente muy inteligente, a los que es difícil mantener motivados y son difíciles de retener.

¿Qué papel juegan los servicios gestionados de seguridad? Explica el CISO de Globalia que la compañía cuenta con personal interno muy cualificado y con experiencia, pero que “en una parte importante” los procesos de seguridad están sustentados sobre proveedores de servicios, que “tienen una visibili-

“De los servicios gestionados espero que sean servicios gestionados, y no recursos cedidos”

Daniel Zapico, CISO, Globalia

dad muy extensa de lo que pasa en otras empresas y sectores”.

“No elijo el mismo tipo de proveedor para desarrollar la capa de gobierno, de control interno, o desarrollar el plan director de seguridad que un proveedor para gestionar una tecnología. Creo que son proveedores distintos y no creo que todo el mundo valga para todo, ni muchísimo menos”, asegura Daniel.

Plantea el directivo que trabajar con proveedores de servicios hace que te pongas en sus manos, que tengas que transferir mucho de tu conocimiento tácito y que se llegue a tener riesgo de concentración y de perder conocimiento por transferir excesivas partes a un proveedor; “al final tienes que poner en la balanza y elegir”.

“Yo de los servicios gestionados esperaré que sean servicios gestionados”, dice Daniel Zapico de manera contundente, explicando que “en España estamos acostumbrados al outsourcing: te pongo una persona y me desentiendo”. Dice el CISO de Globalia que un servicio gestionado es un servicio donde

se han definido procesos, actividades, SLA, interfaces... “y no es te pongo gente y me la gestinas tú”.

Por otra parte, menciona Zapico el riesgo de que se creen silos cuando se trabaja con diferentes proveedores y se tienen que integrar diferentes tecnologías, algo que “ni es trivial ni es sencillo”. Añade que en ocasiones es difícil asegurarse que “tus proveedores conocen tus procesos y servicios de verdad; no sobre el papel; no sólo ponerlo en marcha sino mantenerlo y conseguir una mejor continua según va avanzando el servicio.

Además de las pertinentes consultas a otros colegas, a la hora de escoger un proveedor Daniel Zapico apuesta por contar con unas RFPs muy bien hechas, con todo claramente definido, incluidas fases de entrega, devolución del servicio o penalizaciones en caso de que se quieran imponer. Apuesta el CISO de Globalia por contratos relativamente cortos en el tiempo (1 o 2 años), “lo cual en determinadas cosas será un poco problemática, y es verdad que incrementa el coste, pero al mismo tiempo te da flexibilidad”.



FOOD DELIVERY BRANDS GROUP (Telepizza, Pizza Hut, Jeno's, Apache). Carlos Asún, CISO

Dice Carlos Asún, CISO en Food Delivery Brands, que identificar los niveles de riesgo y de gestión es muy importante para "establecer un entorno seguro con los servicios gestionados". Añade que "nos apoyamos mucho en el outsourcing y en los servicios gestionados", y que es importante que estos servicios estén alineados con el negocio, conozcan los diferentes entornos críticos y den una respuesta ágil, porque en el caso de Food Delivery Brands, "cualquier inconveniente impacta mucho en un plazo muy corto de tiempo".

"Aunque hacemos todos los procesos de investigación del proveedor, de la documentación que contestan en las RFPs que emitimos, y se analiza a nivel técnico los niveles que pueden llegar a tener... Hay veces que se nos escapa algún detalle", apunta Carlos Asún. Dice también el CISO de Food Delivery Brands que, de un servicio gestionado, lo

"De un servicio gestionado espero que la experiencia y el conocimiento sea lo más alto posible"

Carlos Asún, CISO, Food Delivery Brands

que espera es que la experiencia y el conocimiento sea lo más alto posible.

También espera que los proveedores "sean muy ágiles en ciertos procesos y en ciertas circunstancias, y totalmente proactivos en temas de amenazas, vulnerabilidades, etcétera". Entender el negocio y sus riesgos es algo que también demanda Carlos Asún a los proveedores. Así como "el saber gestionar las necesidades bidireccionalmente entre todos los proveedores que están dando servicios a un mismo cliente; trabajar en equipo".

"A la hora de escoger el mejor servicio gestionado hay que tener bien claro qué es lo prioritario para tu compañía"

Rafael Luque, CISO, Ineco

Sobre lo que echa en falta de un proveedor de servicios, lo resumen Carlos Asún con dos palabras: cercanía y exclusividad.

Para el CISO de Food Delivery Brands Carlos Asún, a la hora de escoger el mejor proveedor de servicios, se deben tener en cuenta muchos factores. No sólo hay que hacer mucho análisis, sino preguntar también entre los compañeros y conocer sus experiencias, así como ver cómo responden los proveedores a las RFPs y reuniones de defensa de las mismas. Añade que para evitar posibles errores hay que contar con una serie de contramedidas, como es no ligarse mucho a un único proveedor y cerrar muy bien los contratos.



INECO. Rafael Luque, CISO

Uno de los problemas a los que se enfrentan los responsables de seguridad es el propio perfil de los CISO, dice Rafael Luque, CISO de INECO. Explica este directivo que no sólo hay que "mantener un

conocimiento de la tecnología, que va evolucionando bastante rápido”, sino que hay que gestionar un equipo, así como servicios vinculados a la seguridad para completar las necesidades de protección sin tener que incrementar el coste de personal propio de la compañía, lo “obliga a delegar parte del control de la seguridad en proveedores”

¿Qué papel juegan los servicios gestionados de seguridad? Un servicio gestionado de seguridad te ofrece más calidad y ayuda en todo lo relacionado con la seguridad de tu empresa; “tú puedes enfocar toda tu inversión en seguridad en una compañía que te ofrezca garantía y calidad, con personal formado y capacitado”, lo que resulta mucho eficiente para una empresa.

Lo que se espera es ofrecer más calidad a la hora de cubrir el ámbito de la seguridad respecto a lo que se podría hacer de forma interna porque los proveedores tienen una visión un poco más global, tienen la experiencia de haber trabajado con distintos clientes y con distintas tecnologías.

En cuanto a lo que se echa en falta, uno de los problemas importantes que tienen los proveedores de servicios gestionados de seguridad es que el papel lo aguanta todo, pero en la práctica se pierde un poco el control del desempeño de ese servicio.

A la hora de escoger el mejor servicio gestionado hay que “tener bien claro qué es lo prioritario para tí”. Depende, por tanto, “de lo que tú tengas ya en tu casa, del conocimiento que tengas en tu casa” y de los recursos que tenga cada uno.



SOLVIA. Manuel Barrio Paredes, CISO

Uno de los principales retos a los que nos enfrentamos cuando hablamos de servicios gestionados es “encontrar un socio tecnológico que entienda ese servicio como parte de su empresa”, dice Manuel Barrio Paredes, CISO de Solvia. Añade que es difícil encontrar proveedores que sientan como suyos los procesos y tecnologías, “sobre todo cuando son proveedores que dan servicio muchas empresas”.

“Tenemos casi el 100% de los servicios externalizados, tanto a nivel de IT como de seguridad”, dice, mencionando la falta de talento o la dificultad de encontrar personal muy especializado en ciertas tecnologías, lo que lleva recurrir a los proveedores de servicios de seguridad gestionados.

“Lo que más echamos falta a veces cuando contratamos servicios gestionados son perfiles realmente especialistas para determinados sistemas o aplicaciones. Las empresas de servicios no siempre pueden poner las empresas a gente senior”, dice

“De algunos proveedores de servicios, se echa en falta que sienta la empresa del cliente como suya”

Manuel Barrio Paredes, CISO, Solvia

Manuel Barrio. Añade que, por desgracia, en casi todos servicios gestionados al final entre lo que se redacta en la oferta por parte del proveedor cuando se presenta a un RFP y el servicio finalmente prestado suele haber bastantes “Claro oscuros” ya que después suele pasar que no es la gente realmente especializada quien atiende ese servicio.

Dice también el CISO de Solvia que se ha encontrado con casos en los que el proveedor de servicios no conoce bien el negocio, que se centra mucho en la parte técnica, pero no en el negocio que sustenta esa parte técnica; “se echa en falta que sienta esa empresa como suya y conozca hasta el último detalle y cómo afecta a negocio cualquier incidente o que pueda ocurrir en los sistemas que está gestionando”.

A la hora de escoger un servicio gestionado generalmente se consulta primero a otros responsables de ciberseguridad, y también a los propios

"Del proveedor de servicio demando una actitud más proactiva"

Javier Sánchez, CISO, HAYA Real Estate

fabricantes, a quien se les pregunta que empresa es la que tiene más experiencia en un producto, o el que tiene menos problemas. Añade Manuel Barrios que "intentamos hacer los menos experimentos posibles con productos o soluciones nuevas, e intentamos en la mayor medida posible, optar por tecnologías y soluciones ya con experiencia en el sector".



HAYA REAL STATE. Javier Sánchez, CISO

"Retos tenemos todos", dice Javier Sánchez, CISO, Haya Real Estate, cuando se plantean cuáles son los desafíos a los que se enfrentan los responsables de ciberseguridad. Buscar perfiles es complicado, y aparte de que no los hay "tampoco nos interesa", ya

que si está muy especializado en una tecnología o producto y este cambia, tienes un problema, "y esta es la principal ventaja de un servicio gestionado", junto con la experiencia que aporta a la hora de saber escoger una tecnología determinada.

Sin tener externalizada toda la seguridad, dice Javier Sánchez que los servicios gestionados de seguridad se consideran, dentro de los planes de la compañía, "como proveedores críticos" porque "tenemos gran parte de nuestra protección de seguridad delegada en ellos y en el caso que ellos estuvieran una caída, podríamos tener un gran problema".

"Yo siempre espero de un servicio gestionado, y lo que demando además, es que nos acompañen en esta evolución hacia un mundo en el que podamos considerar que tenemos los suficientes controles para dormir tranquilos", dice Javier Sánchez. Menciona el directivo que esta demanda implica una actitud más proactiva, que sea el proveedor de servicio el que proponga, como expertos en seguridad, qué podría hacerse, nuevas ideas. "Lo que a mí me aportaría valor es que me diga hacia dónde vamos, qué tendencias hay, novedades, cuál es el siguiente paso. Eso es lo que yo demando ahora de un servicio gestionado".



A la hora de escoger entre los diferentes servicios de seguridad gestionados se parte "de la experiencia que hayamos tenido con ese proveedor; en ocasiones porque nos preguntamos entre nosotros, y otras veces es e intuición y suerte", dice Javier Sánchez Salas, que, para empezar, opta por pedir opinión a colegas.

Necesitas un

PLAN

**DE CONTINUIDAD
DE NEGOCIO**

B



LA VISIÓN DE LA INDUSTRIA IT

SECURE&IT. Francisco Valencia, CEO &IT

“El principal reto de un proveedor de servicios es dar respuesta a los retos a los que se enfrentan los responsables de seguridad”, asegura Francisco Valencia. El problema con la rotación y la retención del talento que tienen las empresas, y para lo cual contratan a proveedores no hace sino “trasladarnos el problema a nosotros, porque efectivamente hay un problema increíble de falta de recursos”.

Otro reto es ayudar a los CISOs a socializar el riesgo, porque cuando existe un incidente y tenemos que responder al mismo tenemos que hablar no solo con IT, sino con recursos humanos, con asesoría jurídica, con la dirección financiera o con la dirección general... El CISO tiene un rol muy transversal y nosotros tenemos que dar soporte a esa transversalidad.

Secure&IT cuenta actualmente con unos 200 clientes aproximadamente, todos del rango de 400, 500 o 600 empleados, más o menos, explica Francisco Valencia. Añade el directivo que justo en este nivel de empresa se produce una frontera muy interesante: “por debajo lo que buscan es rellenar el check que tienen que poner los consejos de administración cuando dicen si han hecho ya seguridad en su casa o no. Para poner el check contrata un servicio de seguridad gestionada, y como no tienen muy claro, a ese nivel, qué es lo que te están



FRANCISCO VALENCIA,
CEO &IT

 **CLICAR PARA VER EL VÍDEO**

"El CISO tiene un rol muy transversal y nosotros tenemos que dar soporte a esa transversalidad"

Francisco Valencia, CEO &IT

"Un servicio tiene que ser transparente, medible, y el dueño tiene que ser el cliente"

Álvaro Fernández,
Enterprise Executive, Sophos Iberia

contratando, al final te piden un llave en mano y ahí desarrollamos un servicio que se llama Gold Security", donde la compañía se encarga de la seguridad desde distintos ámbitos: legales, con protección de datos o propiedad intelectual o industrial o código penal, hasta el forense de hacking ético pasando por el SIEM o toda la monitorización y en general todos los servicios que una empresa necesitan.

"Hasta ese nivel es todo muy sencillo porque nos constituimos como responsables de seguridad de las organizaciones", dice el CEO de Secure&IT.

Lo que ocurre por encima de ese tamaño de empresa es que todo se segmenta muchísimo, unos quieren la monitorización, o solo la respuesta ante ataques... y en ese punto se producen un reto que es muy importante que es la interrelación con otros proveedores y otros departamentos que gestionan los sistemas.

Dice Francisco Valencia que el mismo problema que tiene un CISO a la hora de seleccionar un proveedor de servicios "lo tengo yo como provee-



ÁLVARO FERNÁNDEZ,
ENTREPRISE EXECUTIVE, SOPHOS IBERIA



CLICAR PARA
VER EL VÍDEO

dor a la hora de seleccionar un fabricante. Con qué producto marcas toda tu estrategia para defender al cliente". Añade el directivo que "una empresa como la nuestra vive de vuestra seguridad" y que Secure&IT no vende tecnología sino seguridad.

Añade este proveedor de servicios que en el caso de su compañía no se tiene a ningún empleado en outsourcing y que cada cliente cuenta con tres perfiles, el abogado, el ingenio y el experto en procesos,

"que forman parte, o invitamos a que formen parte, del Comité de Seguridad y Cumplimiento".

SOPHOS. Álvaro Fernández, Enterprise Executive Fabricante de seguridad, explica Álvaro Fernández, Enterprise Executive de Sophos Iberia que Sophos ha sido muy meticuloso a la hora de desarrollar productos que puedan ser gestionados por terceros, y que el reto es escuchar al mercado, entender cuál-

les son las necesidades de los partner y plasmarlo en la tecnología.

En ciberseguridad hay que alinear tres cosas: personas, procesos y tecnología. Para las empresas es muy complicado poder alinearlas por sí solas, y los proveedores de servicios pueden ayudarles. Destaca también Álvaro Fernández que un servicio tiene que ser transparente por lo que, por un lado, los proveedores tenemos que ser muy claros, y por otro los clientes tienen que preguntar y ser muy meticulosos a la hora de entender qué es lo que pueden esperar de este servicio.

Uno de los gap que ha detectado su compañía, y donde Sophos ha hecho una propuesta de servicio importante, es en la detección y respuesta. Explica el ejecutivo de Sophos que las soluciones EDR (endpoint detection and response) ofrecen mucha capacidad de ver cosas para poder responder a las amenazas, pero se necesita poner recursos que estén formados, recursos que es complicado conseguir y que nosotros ofrecemos como servicio.

“El servicio por excelencia en seguridad es la gestión”, asegura Álvaro Fernández cuando se le pregunta por los servicios de seguridad que más de demandan. Añade que hay dos tipos de servicios, por un lado, la gestión de la detección y el dar una respuesta ante las amenazas que se encuentran, “y que no deja de ser el tener a expertos por detrás haciendo un threat hunting a través de nuestro EDR”, y un segundo tipo de servicios de respuesta rápida ante incidente “que desgraciadamente se

“Nosotros entendemos un servicio sí gestionado y con un proveedor que sea cercano”

Carlos Tortosa, responsable de grandes cuentas, ESET

demanda mucho” y que ayudan a las empresas a afrontar un incidente a restablecer el servicio.

“Un servicio tiene que ser transparente, medible, y el dueño tiene que ser el cliente”, dice Álvaro Fernández. Añade que, para escoger bien un servicio, un cliente debe “preguntar, comparar, ver exactamente lo que propone cada uno de los servicios y pensar cuál es el servicio que tú necesitas”. Además, “los servicios deben tener un objetivo y hay que cumplirlo, y si no, pues tendrá que haber penalizaciones”.

Es importante trabajar desde el primer momento de manera muy cercana con el fabricante e integrador para entender bien cuál es el servicio y poder tener diferentes alternativas para decidir la más idónea.

ESET. Carlos Tortosa, responsable de grandes cuentas, ESET

Refiriéndose a cómo las siglas acuñadas por algunas consultoras en ocasiones añaden complejidad a las tecnologías existentes en el mercado, dice Carlos Tortosa, responsable de grandes cuentas de ESET, que “tenemos que ser capaces de poner en valor el producto no por el nombre, sino por cómo te

va a proteger”. Para nosotros, continúa este directivo, es un reto “facilitar al proveedor servicios una herramienta concreta que te proteja ante una amenaza concreta. Y el nombre que nosotros le vamos a dar no tiene importancia”.

Entre los retos a los que se enfrenta ESET, destaca el directivo el hacer llegar al proveedor de servicios “cuál es la herramienta completa que se tiene que utilizar en cada situación, en cada cliente y cómo hacerla funcionar”. No tanto un reto como una obligación es que los proveedores de servicios que trabajan con nuestros productos tengan conocimiento suficiente para que la capa de protección os



cubra al cien por cien lo que realmente está diciendo. “Pero creo que es el reto principal en nuestro caso es dar formación al proveedor de servicio y darles las herramientas necesarias para ese nivel de protección”, añade el responsable de grandes cuentas de ESET.

Dice Carlos Tortosa que se está rebajando muchísimo el nivel de cliente que está solicitando un servicio gestionado. La empresa pequeña no es capaz de contratar un especialista en ciberseguridad, y lo más lógico es contratar un especialista en ciberseguridad, y si además tiene la capacidad de realizar un servicio de monitorización y de respuesta, muchísimo mejor.

Con las propuestas de servicios gestionados lo que estamos haciendo es llegar prácticamente a cualquier tipo de cliente, y lo que más se demanda es seguridad endpoint, que es lo mínimo, además de monitorización. Y después, en empresas un poco más grandes, lo que se solicita es una respuesta inmediata de un incidente, una resolución de manera remota.

ESET facilita a sus partners un servicio de monitorización de sus productos, con sus herramientas y acceso a la capacidad del departamento de soporte de la compañía. Se trata de una herramienta que “facilitamos a aquel distribuidor o partner que no tiene capacidad a nivel profesional y que sí tiene capacidad de llegar a una cantidad concreta de clientes, sean del tamaño que sea, porque hemos puesto un precio ajustado de servicios”.



CARLOS TORTOSA,
RESPONSABLE DE GRANDES CUENTAS, ESET



**CLICAR PARA
VER EL VÍDEO**

“Nosotros entendemos un servicio sí gestionado y con un proveedor que sea cercano. Para nosotros eso es lo lógico”, asegura Carlos Tortosa, añadiendo que su compañía trata en todo momento que la formación que tenga el proveedor del servicio sea la máxima posible.

¿Cómo se tiene que elegir un servicio gestionado? Primero, el proveedor tiene que ser de garantías; otra cosa serán los productos que inclu-

yan dentro de este servicio, dice Carlos Tortosa. Asegura en directo que “la necesidad de que el proveedor conozca las herramientas que os está facilitando y que no nos tengamos que fijar ya tanto en el nombre de las herramientas que utiliza, sino en la robustez y el conocimiento que tiene de las mismas, creo que debería de ser algo primordial para cualquiera de los responsables de seguridad”. **it**