it Digital Security

Mejorando tu seguridad con Servicios Gestionados

WatchGuard

SOPHOS

Mejorando tu seguridad con Servicios Gestionados

Los servicio gestionados en general, y los de ciberseguridad en particular, se han convertido en parte fundamental de la gestión empresarial. Los servicios gestionados surgen como una solución que permite seguir desarrollando el negocio sin las limitaciones habituales propias de asumir la planificación, gestión de proyectos y la contratación de perfiles profesionales.

Fotos: Ania Lewandowska

Para debatir sobre sus ventajas qué se espera de ellos, qué se echa en falta y cómo ayudan a los responsables de ciberseguridad de las empresas a hacer frente a los retos que se les plantean cada día, IT Digital Security ha organizado un Encuentro ITDS en el que han participado Elena García Mascaraque, Global Director Managed Security Service Providers en WatchGuard Technologies; Álvaro Fernández, Sales Manager Iberia de Sophos; Alfonso Delgado, Responsable de Infraestructura y Seguridad IT de la Asociación Española contra el Cáncer; Teniente Coronel Carlos Córdoba Fernández, Jefe del Área de Centros de Operaciones de Ciberseguridad del Centro Criptológico Nacional CCN-CERT; Luis Villafruela, Head of Cibersecurity de Iberdrola; David Cerrato de la Macorra, IT Director & CISO de KRUK España y Luis Ballesteros, CISO de WiZink.

"A un servicio gestionado le pediría saber adaptarse a las empresas al que van dirigido"

Alfonso Delgado, Responsable de Infraestructura y Seguridad IT, Asociación Española contra el Cáncer

Iniciamos la reunión preguntando a los asistentes por los retos de ciberseguridad a los que se están enfrentando. En los bancos siempre ha habido robos, atracos, pero mientras que antes los delincuentes tenían que hacerlo de manera presencial, "ahora lo intentan desde cualquier parte del mundo, en remoto y sin que se les vea la cara", comenta Luis Ballesteros, CISO de Wi-Zink, como uno de los retos a los que se enfrenta. No olvida que, además, los ciberataques son más sofisticados, que las motivaciones ya no solo son económicas y que el perímetro de seguridad ha desaparecido.

En su doble función de director de TI y responsable de ciberseguridad de Kruk España, una empresa que se encarga de gestión de deuda, David Cerrato explica que entre sus retos está el cumplir con las normas de seguridad que exige cada banco. Además, el ser una empresa polaca ha hecho que el riesgo se haya multiplicado durante la guerra Ucrania-Rusia. Añade que evolucionar al ritmo que se requiere para asegurar el negocio es también un reto importante.

Representante del CCN (Centro Criptológico Nacional), el Teniente Coronel Carlos Córdoba Fernández destacaba que los atacantes están ahora perfectamente organizados y que, si bien los pequeños organismos compran medidas de seguridad, el robo de credenciales se ha convertido en un reto porque con ellas te saltas todas esas medidas, por lo que hay que comprobar

comportamientos extraños. Sobre APTs, espionaje con móviles, etc., son temas con los que no hay que asustar a las pequeñas empresas.

A priori se puede pensar que una ONG no va a ser víctima de un ciberataque, pero según Alfonso Delgado, Responsable de Infraestructura y Seguridad IT de la Asociación Española contra el Cáncer (AEC), son víctimas de ataques automatizados e incluso dirigidos, como medio de llegar a otras empresas. Menciona la concienciación como un reto importante y que la externalización de servicios de seguridad es fundamental, sobre todo entre las pymes.

En su turno, Luis Villafruela, Head of Cibersecurity de Iberdrola, explica que si bien no tan avanzado como la banca, en Iberdrola se lleva tiempo invirtiendo y evolucionando en temas de ciberseguridad. Destaca como retos la pérdida de perímetro, así como la concienciación y el poder coordinar un plan de seguridad que tenga los mismos niveles en todos los eslabones de la cadena.

Destaca Elena García Mascaraque el papel que la filosofía Zero Trust tiene en la realidad a la que se enfrentan las empresas. Plantea que controlar el acceso a los sistemas, el comportamiento de los usuarios con medidas de control del endpoint, tecnologías de autenticación multifactor, y un servicio de monitorización de las amenazas de seguridad 24/7 son tres pilares sencillos que, desde diferentes grados de complejidad, cualquier empresa debería poder acceder.

Durante su intervención, Álvaro Fernández, Sales Manager Iberia de Sophos, destaca que, aunque positiva, la normativa es un reto, así como la

"El mensaje hacia la administración pública es que la seguridad gestionada es obligatoria porque todo se ha vuelto mucho más complicado y ya no vale un antivirus"

Carlos Córdoba Fernández, Jefe del Área de Centros de Operaciones de Ciberseguridad del Centro Criptológico Nacional CCN-CERT

evolución de los ataques, que obliga a las empresas a vigilar y monitorizar lo que está ocurriendo, algo nada fácil porque se necesita contar con un equipo de gente especialista en ciberseguridad, "lo que demuestra la necesidad de contar con servicios de seguridad gestionados".

Proveedores de confianza

La atomización que existe en el mercado de seguridad a nivelo de fabricantes se refleja también en la cantidad de proveedores de servicios que existen en el mercado. Habla David Cerrato de los Golden Providers, o proveedores de confianza con los que poder establecer una relación y saber en todo momento quién y cómo se está dando el servicio "para protegerte no sólo de los ataques externos, sino de los internos". Con más de 300 están en el departamento de IT, "nos consideramos una empresa tecnológica", dice Cerrato explicando que se trabaja con proveedores porque "no puedes saberlo todo", y que la clave está en saber quién de todos esos proveedores es que el que sabes lo que necesitas que sepa. "El gran secreto es cómo escoger", asegura.

"Para nosotros externalizar los servicios es fundamental", asegura el responsable de Infraestructura y Seguridad IT de Asociación Española contra el Cáncer. Añade Alfonso Delgado que hay muchos básicos que en muchas empresas no están cubiertos porque no cuentan con especialistas y se mantiene de acuerdo con David Cerrado en lo que se refiere a saber escoger el proveedor de confianza que sepa lo que necesita el cliente; "la externalización es

"El reto es tener el partner de alto nivel con gente buena dentro de la empresa y que el conjunto de servicios y soluciones estén bien enlazadas"

Luis Villafruela, Head of Cibersecurity, Iberdrola

fundamental. Necesitamos contar no sólo con proveedores que tengan el conocimiento, sino que miren por el cliente, no solo por el por el negocio", comenta.

Los proveedores son totalmente necesarios. Lo hacen mejor y de manera más eficiente. Lo asegura durante este Encuentro ITDS Luis Ballesteros. Añade que no se puede ser experto en todo, que "no hay que olvidar que la responsabilidad no se delega" y que cada empresa debe saber dónde está, dónde quiere llegar, y establecer un marco de ciberseguridad que, en opinión del CISO de WiZink, debe tener cuatro dominios fundamentales: gobierno, protección, vigilancia y resiliencia. Respecto al contrato con proveedores, empieza con la parte de la selección de proveedores para lo que hay que hacer un procedimiento interno de validación que establezca "que se van a cumplir las expectativas que esperas a nivel de servicio, y además van a gestionar tu información confidencial tal como tú lo harías".

Para Carlos Córdoba Fernández hay una fase clave: La responsabilidad no se delega. En el caso de las entidades locales o diputaciones, que es lo que compete al Jefe del Área de Centros de Operaciones de Ciberseguridad del CCN, "el problema es que hay una persona o ninguna" y hay que concienciarles de que ellos tienen una responsabilidad. El mensaje hacia la administración pública es que la seguridad gestionada es obligatoria porque todo se ha vuelto mucho más complicado y ya no vale un antivirus, pero "no podéis olvidaros de que la responsabilidad es vuestra". Desde el CCN se impulsa

"El gran secreto es cómo escoger a tu proveedor de servicios de confianza"

David Cerrato de la Macorra,
IT Director & CISO, KRUK España

la compra de tecnología a través del Catálogo STIC, al tiempo que la Red Nacional de SOC está impulsando la compartición de información entre proveedores, porque “el que piense que haciendo la guerra por su lado va a triunfar, está totalmente equivocado”.

Explica Luis Villafruela que en Iberdrola existen distintos niveles de servicios gestionados. Si bien la parte de gobierno no se delega, sí que se cuenta con proveedores en otras cuestiones, como el mantenimiento de la postura de seguridad. Reconoce que existe un “proceso de selección de proveedores ya muy evolucionado y que “el reto es tener el partner de alto nivel con gente buena dentro de la empresa y que el conjunto de servicios y soluciones estén bien enlazadas”.

Dice Álvaro Fernández que los servicios de seguridad gestionados aparecen por necesidad y que la seguridad se ha convertido en habilitadora del negocio. Asegura también que el talento es clave, no sólo conseguirlo, sino retenerlo, así como la escalabilidad del servicio que se está dando. Explica que desde Sophos se ha invertido mucho en tecnología, así como en Inteligencia Artificial para poder escalar que ha permitido, en tres años, pasar de cero a doce mil clientes en el servicio de detección y respuesta. Desde Sophos estamos siendo pioneros en ofrecer los servicios de detección y respuesta (MDR) no sólo sobre tecnología de Sophos, sino sobre tecnología de terceros para proteger al máximo nivel a las organizaciones.

A través de WatchGuard for SOC, WatchGuard provee de tecnología para proveedores de servicios a terceros, o MSSPs, o servicios internos de seguridad. “Nuestra filosofía es que la seguridad sea consumida como servicio y crear plataformas de seguridad”, explica Elena García Mascaraque, añadiendo que la Unified Security Platform de WatchGuard permite integrar no sólo soluciones de la compañía sino de terceros “permitiendo hacer sencillo lo complejo”, que no es otra cosa que la gestión de una ciberseguridad basada en decenas de herramientas.

La responsable de servicios MSSP de WatchGuard comentaba también que esa tendencia de seguridad a través de plataforma se convierte en fundamental el tema de las certificaciones y cumplimiento normativo porque se trabaja con datos muy sensibles “y vuestra tranquilidad también es la nuestra”; además de tener acceso a telemetría de 365 días que permiten a los SOCS hacer las investigaciones.

¿Qué le pedirías a un Servicio de Seguridad Gestionado?

Retención de talento es uno de los elementos que pediría el responsable de ciberseguridad de Iberdrola a un servicio gestionado. Explica Luis Villafruela que en ocasiones se encuentra con una

"Los proveedores son totalmente necesarios. Lo hacen mejor y de manera más eficiente. Pero no hay que olvidar que la responsabilidad no se delega"

Luis Ballesteros, CISO, WiZink

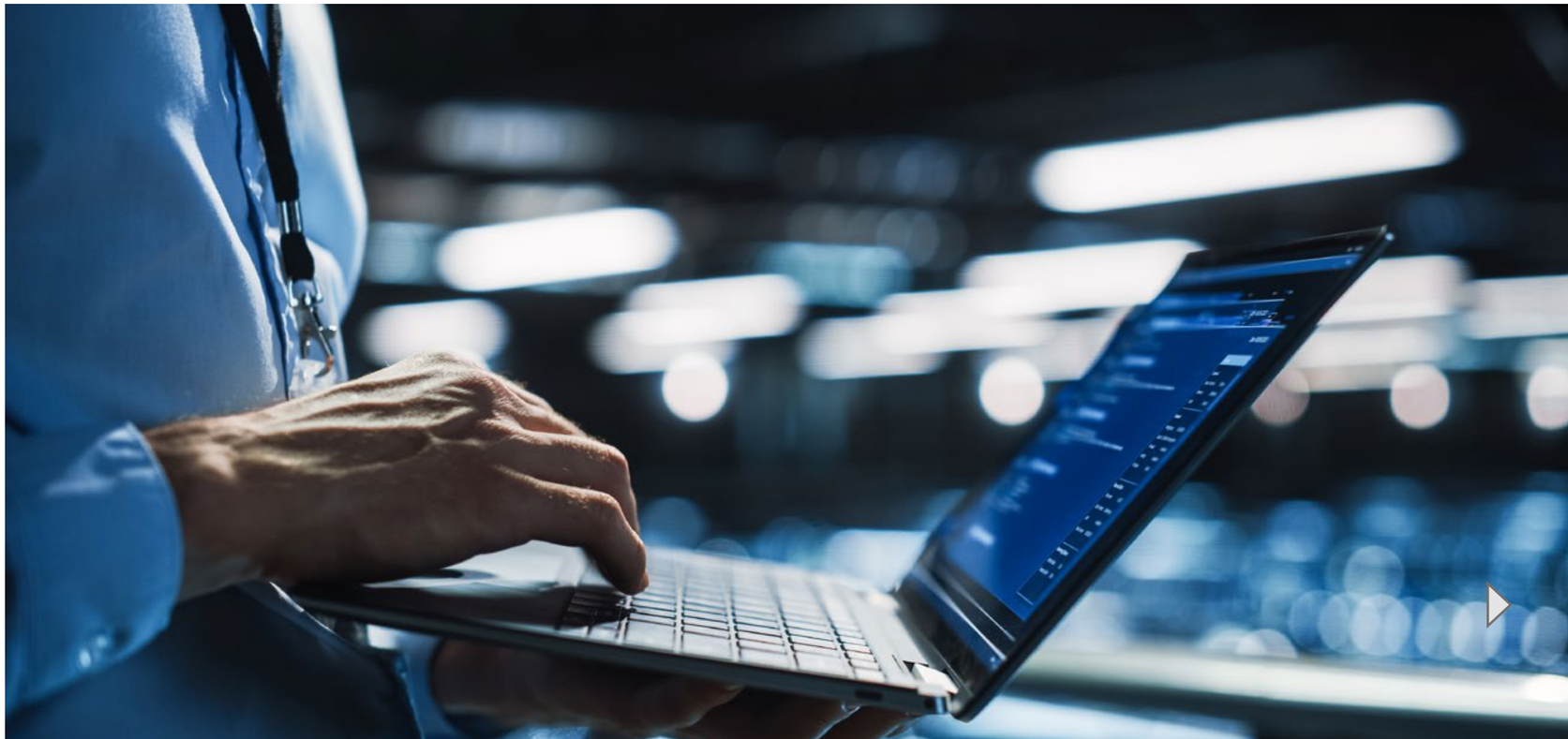
merma en la calidad del servicio prestado, “y eso es porque la rotación de personal es impresionante y los que llegan nuevos no tienen tanta experiencia”. Apunta también en su lista de deseos la convergencia de soluciones, sobre lo que asegura que se está haciendo un buen trabajo; y la compartición de inteligencia, “contar con plataformas comunes que permitan compartir IoCs, compartir ciberinteligencia”.

“A un servicio gestionado le pediría saber adaptarse a las empresas al que van dirigido”, asegura con rotundidad Alfonso Delgado, poniendo como ejemplo que no se puede querer vender un servicio de SOC a una empresa que no tenga el directorio activo en orden. Sobre que se delegue la responsabilidad en el servicio gestionado, apunta también el responsable de ciberseguridad de la AEC que en ocasiones “no hay conocimiento interno y te tienes que fiar de lo que te digan. Es muy importante la formación porque uno no puede ser CISO o responsable de ciberseguridad sin tener los conocimientos para, aunque sea, contratar una empresa y hacerle seguimiento de lo que tiene que hacer”.

“Profesionalidad” es lo que el Teniente Coronel Carlos Córdoba Fernández pediría a un servicio de seguridad gestionada. Menciona que rara es la empresa de seguridad que no venda SOAR, IA o machine learning, pero que, cuando hablamos de pymes, “lo que se necesita es algo muy sencillo, muy básico, que te proteja en el 95% de los casos y que cueste 100€ al mes”. Comenta también el Jefe del Área de Centros de Operaciones de Ciberseguridad, Centro Criptológico Nacional

"Nuestra filosofía es que la seguridad sea consumida como servicio y crear plataformas de seguridad"

Elena García Mascaraque, Global Director Managed Security Service Providers, WatchGuard Technologies



"Desde Sophos estamos siendo pioneros en ofrecer los servicios de MDR no sólo sobre tecnología de Sophos, sino sobre tecnología de terceros"

Álvaro Fernández,
Sales Manager Iberia, Sophos

CCN-CERT, que hay quienes se aprovechan de una falta de conocimiento para vender de más.

En el caso de David Cerrato de la Macorra, lo que pediría es conocimiento real, "una verdadera formación en ciberseguridad, que entienda lo que se está haciendo".

Retención de talento, flexibilidad y adaptación al entorno son los tres elementos que Luis Ballesteros pediría a un proveedor de servicios gestionados, porque "estamos contratando servicios gestionados porque lo hacen mejor y más eficiente. Y si de verdad queremos y que lo hagan mejor y más eficiente lo que no puede ser es 'café para todos' porque no es lo mismo proteger un comercio, una entidad financiera o una red eléctrica". Respecto a la opción de compartir conocimiento entre todo el ecosistema de seguridad, comenta Ballesteros que es algo que se lleva haciendo en el sector bancario, donde "tenemos muy claro que somos competencia en mercado, pero no en ciberseguridad, y esto se ha ido extendiendo".

Se plantea también durante el debate la necesidad de establecer, cuando se pueda, dos capas, una de consultoría de seguridad y otra del servicio en sí mismo. Si bien para las empresas grandes estas dos capas están diferenciadas, en entornos más pequeñas la línea es más difusa; en todo caso, para Alfonso Delgado "es fundamental recibir más consultoría de ciberseguridad que identifique los mínimos". Al respecto menciona David Cerrato que en Angeco, la Asociación Nacional de Entidades de Gestión de Cobro, se busca establecer unas guías de mejores prácticas, "unos básicos de lo que deberías implantar para poder trabajar con otras empresas. Tener una lista de 'to do' que me permita ir a un proveedor y decirle qué necesito tener".

Enlaces de interés...

- EncuentrosITDS. Seguridad proactiva, ¿hasta dónde estás dispuesto a llegar?
- Encuentros ITDS. De la continuidad de negocio a la resiliencia segura
- Encuentros ITDS. Los servicios gestionados de seguridad a examen

Compartir en RRSS