Texto
Andrea Gómez

CÓMO DAR RESPUESTA A LAS NUEVAS AMENAZAS CENTRA EL ENCUENTRO VIRTUAL

El reto de la seguridad en tiempos de pandemia

<< El coronavirus no es el único virus que nos ha traído la pandemia. Este último año nos ha traído muchos cambios, la digitalización de los negocios ha avanzado a pasos agigantados, motivada por las nuevas necesidades que iban surgiendo. La normalización del teletrabajo ha traído consigo uno de los desarrollos y despliegues tecnológicos más rápidos de la historia, pero también abre puertas de acceso al cibercrimen.

La urgencia en los primeros meses para tratar de adaptarse a lo que estaba pasando, sin tener que frenar el negocio, generó grandes brechas de seguridad y cumplimiento, y los ciberdelincuentes aprovecharon con picardía este caos generalizado para atacar todo tipo de negocios y estructuras. Ahora que las empresas han tenido tiempo para adaptarse y planificar, la ciberseguridad se ha vuelto una prioridad. Es un área que tiene que estar en el centro del negocio y se han de redoblar los esfuerzos para proteger a todos los usuarios y los datos de la organización.

Para conocer el impacto de los nuevos ciberataques y los cambios que han tenido que implantar las empresas para aumentar la prevención y protección frente a las amenazas, Computing, de la mano del proveedor de herramientas de ciberseguridad, Sophos, organizó una encuentro virtual con expertos y directores de seguridad de diferentes sectores, los cuales pudieron contar su experiencia y poner puntos en común.

Ricardo Maté, director general de Sophos Iberia, abrió el debate con una pequeña reflexión, "desde Sophos tenemos un departamento muy relevante, que es Sophos Labs, con más de 300 analistas que están monitorizando constantemente las amenazas, y hemos detectado que el cibercrimen está cada vez más organizado y es más letal. No solo vemos un incremento en los ataques, sino que estos cada vez son de mayor impacto".

Para el directivo, "la ciberseguridad se ha vuelto un deporte interactivo, ya no basta con tener los mejores sistemas de protección, sino que hay que monitorizarlos 24/7, sigue habiendo una falta muy grande de recursos y talento, y la mayoría de las compañías no pueden permitirse grandes equipos monitorizando a tiempo completo la situación, por lo que se ha convertido un poco en la tormenta perfecta".

"Escucho atentamente a Ricardo, y estoy de acuerdo con él, pero también me gustaría ponerle el punto positivo al asunto", se sumó al debate Guzmán Garmendia, CIO del Gobierno de Navarra. "Hemos vivido un momento muy duro, pero desde el punto de vista tecnológico nunca hemos vivido un momento tan dulce. Hemos crecido mucho digitalmente y los equipos de seguridad de las empresas han adquirido la relevancia y esencialidad que merecen. Pero está claro que cuanto más crecemos digitalmente, más lo hace la delincuencia en las redes". Garmendia indicó a su vez: "Tenemos que invertir, y cada vez nos cuesta menos trasladar la importancia de invertir en ciberseguridad a nuestros mayores. Coche más grande, seguro más caro".

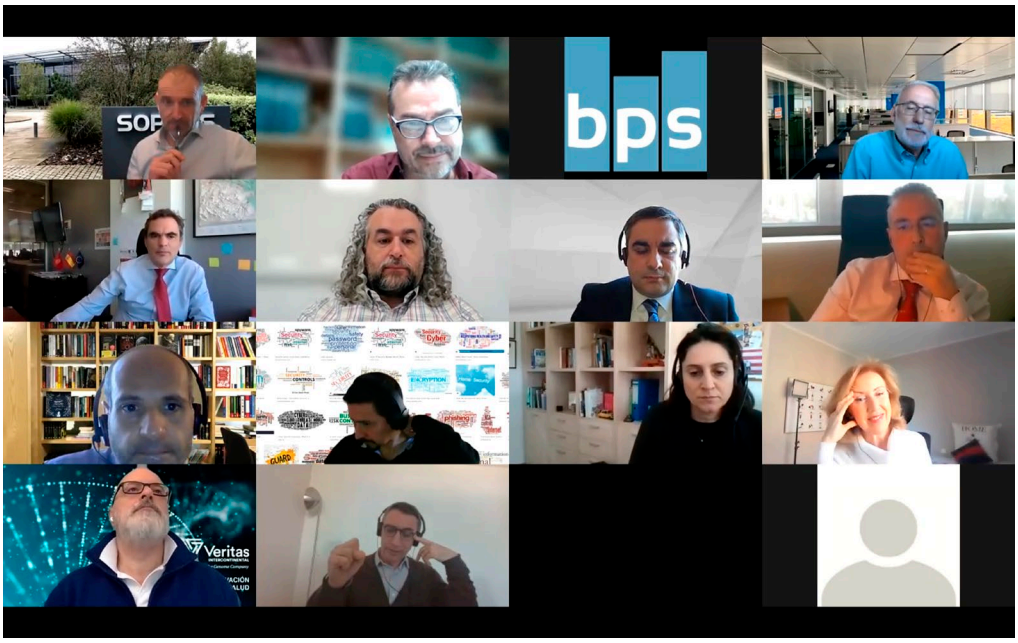
"La popularización del ransomware ha contribuido a la concienciación de las Direcciones

RICARDO MATÉ, DIRECTOR GENERAL DE SOPHOS IBERIA

"DESDE SOPHOS DAMOS RESPUESTA A ESTE INCREMENTO TAN IMPORTANTE DE LOS CIBERATAQUES"

Estamos asistiendo a un incremento muy importante de los ciberataques, ejecutados por grupos dirigidos desde algunos estados. Se están llevando a cabo acciones de gran impacto, como la vulnerabilidad explotada de Microsoft Exchange o el ataque de ransomware a Acer, por el que le exigían un rescate de 50 millones de dólares. Todo esto nos debe hacer reflexionar sobre si estamos suficientemente protegidos y tenemos los recursos necesarios para podernos defender en el caso de ser víctima de uno de estos ataques. Desde Sophos tenemos la respuesta, nuestras soluciones de ciberseguridad evolucionada y el concepto de seguridad sincronizada nos ayudan por un lado a tener la mejor protección, y poder llevar a cabo la detección de manera instantánea y automática para poder responder a cualquier incidente. Pero esto no es suficiente, necesitamos que nuestros entornos estén monitorizados 24/7 por expertos en amenazas, y esto lo garantizamos gracias a nuestros servicios de Manage Threat Response. Y si aun a pesar de todo esto, hubiéramos sido víctimas de un ataque, ponemos a disposición de las empresas el servicio de Rapid Response, una asistencia increíblemente rápida a la hora de identificar y neutralizar amenazas activas contra una empresa. Todo esto es lo que Sophos es capaz de proporcionar a todos los clientes independientemente de su tamaño.

"Tenemos que invertir, cada vez nos cuesta menos trasladar la importancia de invertir en ciberseguridad a nuestros mayores. Coche más grande, seguro más caro"



Generales de las empresas, y eso nos facilita el aumento de presupuesto, y poder tener más herramientas", añadía Alfredo Delgado, director de Tecnologías de la Información y Comunicaciones de Aplicalia. "Aun así parece que siempre vamos por detrás de los ciberdelincuentes, por mucho que queramos, su ingenio se ha disparado y parecen tener siempre un plan B, nosotros vamos resolviendo a remolque de su ingenio".

Ángel Luis Sánchez, CTO del Servicio Madrileño de Salud, constataba que "ha sido un año complicado, nuestro grado de exposición es cada vez mayor. Hay cada vez más gente teletrabajando y más servicios telemáticos, lo que aumenta mucho las vías de entrada para el ciberdelincuente". Desde su punto de vista, "la detección y protección es importante, pero no podemos olvidarnos de la respuesta. Cuando las organizaciones son tan grandes, a veces los ataques son inevitables, pero tienes que estar preparado para ser capaz de responder ante ellos. En Sanidad no podemos permitirnos ningún paro de actividad".

Los pilares de la ciberseguridad

"En un ataque de ransomware es vital reaccionar desde un primer momento, y eso hemos podido hacerlo contratando un SOC externo", explicaba Joan Centellas, CISO de Penguin Random House. "Creo que en ciberseguridad debemos tener tres pilares claros, el primero es disponer de las herramientas técnicas necesarias; el segundo es el talento, tener personal especializado que maneje esas herramientas y situaciones; y el tercero es la concienciación de los usuarios. Por mucho que tengas las mejores herramientas o un equipo que está monitorizando 24/7, siempre va a haber vías de entrada que no queden cubiertas".

Adrián Perelló, CIO del grupo AM Cargo, aclaraba en primer término que "soy responsable de un grupo de empresas pequeño comparado a otros gigantes con los que comparto debate, por lo que no siempre podemos tener las herramientas que nos gustaría por falta de recursos", y añadía: "Estamos reforzando mucho la concienciación del usuario con soluciones creativas; podemos poner todas las barreras que queramos, pero el 'click' del usuario final es muy peligroso y no siempre podemos controlarlo. Los ataques han evolucionado igual de rápido que la tecnología y se han profesionalizado". En el caso de las pymes, Perelló considera crucial que la consola que te den sea amigable y fácil de usar, "hemos hecho un gran esfuerzo por buscar herramientas que no requieran de una gran especialización, pero que aun así nos muestren lo que pasa".

Roche es una firma que ha evolucionado de varias formas, de acuerdo con Jairo Serrano, director de Seguridad Informática. "Hemos apostado por la concienciación del usuario final y la digitalización, ya que las tecnologías legacy nos han impactado gravemente, al no tener el mismo desarrollo que otros aplicativos más modernos". De forma más específica apuntaba: "Podemos hacer miles de ejercicios para parar el phishing, pero siempre habrá alguien más creativo, por lo que nuestra apuesta ha estado muy centrada en formar y especializar al usuario para evitar los riesgos".

ASISTENTES

1 Ángel Luis Sánchez, Servicio Madrileño de Salud | **2** Adrián Perelló, Grupo AM Cargo | **3** Alfredo Delgado, Aplicalia | **4** Roger Cuadras, ARAG | **5** Guiu Ocón, Sophos | **6** Guzmán Garmendia, Gobierno de Navarra | **7** Jairo Serrano, Roche | **8** Francisca Huélamo, Travel Club | **9** Clara Belaña, Universitat Oberta de Catalunya | **10** Marco Merino, Veritas | **11** Joan Centellas, Penguin Random House

"En el sector público no somos muy diferentes a lo que habéis estado contando, lo único es que nuestra contratación es más lenta y eso a veces pasa factura", se sumaba al debate Clara Belaña, CIO de l'Universitat Oberta de Catalunya. "Me ha gustado lo que ha contado Joan sobre los tres pilares, ya que son muy relevantes, y en eso también estamos poniendo un poco el foco. La pandemia nos ha forzado a acelerar mucho las cosas y a buscar inversión para aplicar nuevas soluciones". Clara Belaña ilustraba la nueva situación, "al tener que externalizar parte de la gestión de nuestra ciberseguridad, ya que nuestro equipo era muy pequeño para hacer frente a todo lo que ha ido viniendo. Como ha dicho Guzmán, es positivo que el desarrollo tecnológico se haya acelerado, pero esto también ha llevado al colapso de muchos equipos técnicos".

"En mi caso, todas mis políticas están orientadas a proteger el dato, no al usuario", explicaba Marco Merino, CIO de Veritas Internacional. "El usuario no está formado ni se les puede exigir mucho control. Nosotros además contamos con muchos robots en nuestro personal, y la gestión y formación en ese caso no es tan simple. Somos un laboratorio y tratamos con datos altamente confidenciales, uno de los mayores problemas es la legislación, políticas como el GDPR fueron un dolor de cabeza terrible, y forzar a las empresas a cumplir ese plazo generó grandes brechas de seguridad".

Francisca Huélamo, directora de Tecnología e Innovación de Travel Club, indicaba que "desde que estamos confinados, el tema de la seguridad ha sido un reto muy importante, pero esto ya venía de antes. La legislación se ha puesto muy exigente en cuanto a los requisitos para custodiar los datos, en consecuencia, hemos tenido que desarrollar medidas técnicas y políticas para protegerlos. El riesgo no está únicamente en la tecnología, está también en el uso que hacen las personas de esta".

Roger Cuadras, CISO de Arag, hacía alusión al impacto en la carga de trabajo en el equipo informático "y esto puede tener consecuencias serias en el time-to-market o time-to-production. Pero también es cierto que las herramientas ayudan enormemente a mejorar la calidad del software. Creo que la ciberseguridad nos va a ayudar a mejorar la tecnología en general, pero para eso necesitamos acción e inversión, no podemos andar con medias tintas". En cuanto al GDPR, "yo creo que ha traído una mejora enorme, ha puesto muchos relojes en hora".

Retener talento y atraer inversión

"¿Cómo convencer a nuestros mayores? En nuestro caso lo hemos hecho por tres vías, en primer lugar, vamos a tener más ingresos, ya que mayor ciberseguridad implica mayor control fiscal; segundo, van a bajar los costes; y, por último, se están empezando a entender los riesgos que conlleva no tener una buena estrategia", contaba Garmendia. "Las Administraciones cada vez son más conscientes de que es importante tener personal cualificado, pero aun así nos cuesta mucho encontrarlo. Nosotros no podemos pagar lo mismo a los expertos en seguridad que la privada", añadía Ángel Luis Sánchez.

"En las pymes hay carencias muy grandes en recursos, herramientas y personal. Así y todo, la democratización de las herramientas está permitiendo a las pymes tener una seguridad y tranquilidad mayor", contaba Adrián Perelló. Finalmente, Ricardo Maté recomendó que "es importante que la ciberseguridad sea muy efectiva, pero también que sea sencilla de gestionar. El pilar sobre el que Sophos se asentó es una consola unificada en la nube -Sophos Central- desde la que se pueden gestionar todos nuestros productos. Hemos empezado a lanzar también servicios gestionados de amenazas, accesibles para cualquier empresa, ya que se paga en función del número de usuarios; pero estamos apostando mucho por la concienciación y formación en las organizaciones, así como por la visión 'zero trust network'. Sabemos que tenemos que ir mucho más allá y tratar de adelantarnos a los delincuentes. Esa es nuestra motivación desde Sophos".

Guiu Ocón, Territory Manager de Sophos Iberia, aludió a "los malos, son como el mal tiempo y aparecen en nuestros ratos de ocio, nos enfrentamos a gente con una motivación muy alta que ganan mucho dinero. ■