Texto
R. Contreras

IVÁN SÁNCHEZ LÓPEZ, CISO DEL GRUPO SANITAS

"La ciberseguridad es muy importante para Sanitas y cuidamos el enfoque cultural"

¿Cuál es su rol y su posición en el organigrama de Sanitas?

Mi cargo es el de CISO del Grupo Sanitas y soy responsable de la gestión e implementación del programa de Seguridad y Protección de la Información para el grupo, que tiene presencia en Europa y Latinoamérica. Si bien la cabecera está en España, a través de Sanitas, tenemos compañías en Europa (Polonia y Turquía) y Latinoamérica (Chile, Brasil, México y en Miami). Puesto que la seguridad es un ámbito prioritario, también es transversal a todas las compañías del grupo y por lo tanto tenemos la responsabilidad de asegurar que el programa de Seguridad, valga la redundancia, se ejecuta en todos los negocios de manera adecuada. Organizativamente pertenecemos a la función del CIO.

¿Cómo está considerada la ciberseguridad en su organización? ¿Hay algún plan estratégico al respecto?

<< La pandemia ha sido un estímulo en la digitalización de Sanitas. Como dato, de 300 videoconsultas diarias en los meses complicados se ha pasado a 5.000 actuales. En esta entrevista, Iván Sánchez detalla la estrategia de ciberseguridad de su área alineada con la transformación digital del grupo.

Desde que me incorporé a la organización, en 2015, hemos puesto en marcha diversas iniciativas, siempre con la ambición de mejorar y alcanzar una mayor madurez. Lo primero fue trazar un plan inicial en el que, alineado con la estrategia de transformación digital del negocio, sentamos las bases y revisamos la definición de la seguridad y su encaje organizativo. Este plan de seguridad ha ido evolucionando, con mucho foco y apoyo de la dirección de Sanitas, lo que nos ha permitido crecer en recursos y 'elevar' la función de seguridad en cuanto a su importancia estratégica. En los comités de dirección hay un slot recurrente para tratar aspectos relacionados con el ámbito de la ciberseguridad. Como puede verse, la seguridad es muy importante a nivel de grupo y cuidamos sobre todo el enfoque cultural. En cuanto a los planes estratégicos, si bien es fundamental mantener unos alineamientos base y tener claros los objetivos, nos hemos dado cuenta de la dificultad de definir planes estratégicos de la manera 'tradicional' (con planes a 3-4 años vista) en un entorno tecnológico y de amenazas tan cambiante. Por lo tanto, nuestro foco está en la protección de los ámbitos clave (puesto de trabajo, red y perímetro, data center, etc.) y de su mejora continua a través de la medición de la madurez usando frameworks como el NIST.

Las instituciones sanitarias han sido las grandes heroínas en la pandemia. ¿Cómo ha contribuido su departamento en esta misión?

La presión asistencial fue muy grande. En los meses más complicados atendimos a 1.400 pacientes con Covid, y duplicamos nuestra capacidad de las UCI gracias a la construcción de hospitales de campaña en los Hospitales de La Moraleja y La Zarzuela. Este crecimiento fue acompañado de equipamiento TI y tecnología sanitaria. Por otro lado, teníamos que seguir dando cobertura a la actividad asistencial habitual para cualquier otro tipo de situación. Nuestro papel como seguridad consistió en estar más cerca de las áreas asistenciales, y de dotar de movilidad a las no asistenciales. Se incrementaron las llamadas al call center para cuestiones relacionadas con soporte IT o de seguridad y de este modo teníamos que integrar conectividad con seguridad, y la digitalización tomó impulso. Como dato, si antes teníamos unas 300 videoconsultas diariamente, en estos momentos la cifra se ha disparado hasta las 5.000 videoconsultas diarias. Como sector de salud hemos funcionado muy bien, mostrando gran capacidad de resiliencia. Nosotros estamos integrados en el departamento TI, y nuestra involucración ha sido diaria. Tenemos mucha carga operacional, como es facilitar una conectividad remota segura y gestionar los dispositivos.

Durante estos meses el ransomware se ha cebado con hospitales y otros centros. ¿Cuáles han sido los ataques más habituales que han detectado?

Somos conscientes de que el ransomware es la principal tipología de ataque por el beneficio económico que lleva detrás y hay muchas compañías que están siendo víctimas de esta otra 'pandemia digital'. Algo que quisiera destacar es que no debemos 'criminalizar' a las víctimas del ransomware, sino que hay que ayudarlas, y posteriormente se analizará el cómo y el por qué ha pasado. Las compañías luchamos contra adversarios que cada vez son más expertos y tienen más recursos. Creo que Wannacry fue el primer gran ataque de estas características que nos abrió los ojos y desde ese momento nos dotamos de sistemas y de herramientas para prevenir el secuestro de información. Pero hay que decirlo una vez más: el riesgo cero no existe para nadie. La conversación no debe empezar por un "¿Nos puede pasar a nosotros?" sino por un "¿En caso de que nos ocurra, sabemos qué impacto tendría y cómo nos recuperaríamos"? Y este es un enfoque organizacional de compañía, no es una cuestión que el área de seguridad pueda resolver por sí sola.

El phishing con la Covid-19 como cebo también ha proliferado. ¿Puede constatar este hecho?

El correo sigue siendo el principal vector de entrada de ciberataques, con el phishing como una tendencia cada vez más creciente. Hay que establecer una cultura de seguridad que involucre a todas las personas y que provenga de la dirección. Durante los meses álgidos de la pandemia, intensificamos la comunicación con los empleados, para que estuvieran formados e informados de que la seguridad es crucial para la organización. Contamos con roles específicos en nuestros equipos que trabajan la comunicación, mano a mano con el departamento de comunicación interna, que nos ayuda muchísimo a llegar a toda la organi-

"No debemos criminalizar a las víctimas del ransomware, sino ayudarles y analizar cómo y por qué pasó"

¿QUÉ PROYECTOS EN CIBERSEGURIDAD ABORDAN EN ESTOS MOMENTOS?

Nuestro proyecto de transformación digital tiene un gran impacto en el área de ciberseguridad. La digitalización no aumenta necesariamente el riesgo, pero sí la superficie de ataque. Todos los servicios que demandan los pacientes hay que securizarlos. La tasa de crecimiento de eSalud va a tener un ritmo del 20 por ciento, como son las videoconsultas o la salud conectada. De esta manera, es el hospital el que va al paciente, y no al contrario. Otro proyecto relevante es el cloud. Tenemos una estrategia de consolidación en la nube a medio plazo. Cambia el paradigma, y tenemos que dotarnos de soluciones como Cloud Security Posture Management, que permitan verificar los controles en on premise y trasladarlos a la nube, securizando la transición.

¿SE INAUGURA UNA NUEVA ERA DE CIBERSEGURIDAD, MÁS DIGITAL QUE HASTA LA FECHA?

Estamos en un mundo nuevo. La ciberseguridad se ha convertido en algo transversal y crítico para las compañías, pero también para la sociedad. Con la digitalización se abre un nuevo escenario, pero también aparecen nuevos riesgos que afectan a los estados y los gobiernos, y a los ciudadanos en particular. Hay un gran campo de batalla, y hay que librar la guerra al cibercrimen sumando la resiliencia de todos.

zación. Todo ello lo reforzamos con campañas de phishing ético para mejorar la preparación de los empleados.

¿Cuáles son sus principales socios tecnológicos?

En este sentido, somos agnósticos. Buscamos los que mejor se adaptan a nuestras necesidades con criterios operacionales y de costes. No recurrimos a un modelo de 'full outsourcing', tenemos proveedores que nos apoyan en áreas como la monitorización y SOC, hacking ético o gestión de identidades. Pero no nos gusta tener un abanico muy amplio de proveedores por la dificultad de gestión y limitación de economías de escala, de manera que relevantes son unos cuatro o cinco proveedores. Trabajamos con proveedores que aprenden de nosotros y son capaces de evolucionar sus servicios, a la vez que aprendemos de ellos. Mantenemos un modelo mixto bien balanceado entre recursos internos y externos, que hemos podido implementar gracias a que la inversión en seguridad nos ha permitido hacerlo a la vez que la plantilla del área de seguridad se ha duplicado desde 2017.

Ahora que la mayoría de las empresas trabajan en modo híbrido, con un mayor peso del teletrabajo y una reducción gradual del presentismo, ¿resulta más complicado establecer una ciberseguridad más eficaz?

Depende del nivel de preparación previo de cada compañía. En el caso de Sanitas, cuando se decretó el estado de alarma en marzo contábamos con sistemas de trabajo remoto seguro con los mecanismos de seguridad adecuados. Esto nos permitió pasar de unos 200 a más de 2.000 empleados trabajando en remoto de manera concurrente y sin exponernos a riesgos innecesarios. También contábamos con soluciones basadas en cloud que nos proporcionaban seguridad y visibilidad fuera de nuestro entorno, como proxy o EDR: en un escenario tradicional si el usuario se conecta en su casa y con su fibra, pierdes el control de su navegación o de la gestión del EDR. Pero con estas soluciones basadas en cloud hemos podido seguir aplicando los controles de seguridad en el escenario de trabajo remoto. Pero también nos hemos dado cuenta de la necesidad de mejora en otras áreas, y ya hemos definido un plan de aceleración para este nuevo escenario de trabajo con un modelo de zero trust: no hay que confiar en la red ni en los dispositivos, eres tan fuerte como el más débil eslabón de tu organización. ■

"La transformación digital no aumenta necesariamente el riesgo, pero sí la superficie de ataque"