LITORALPRESS

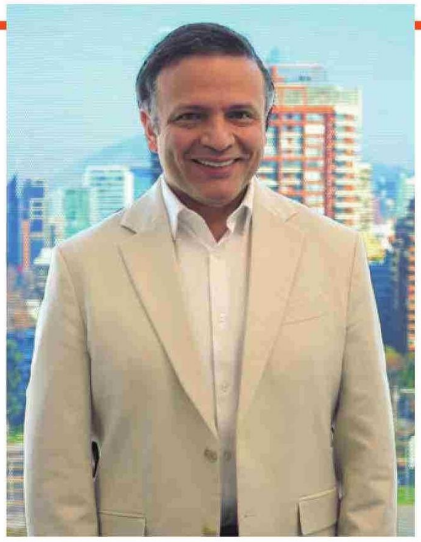
Fecha: 29-07-2024
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: "La ciberseguridad está convirtiéndose en el desafio numero uno de negocios para todas las organizaciones"

Pág. : 38
Cm2: 400,5

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

Jaime Chanagá, Field CISO de Fortinet

"La ciberseguridad está convirtiéndose en el desafío número uno de negocios para todas las organizaciones"



Como Field CISO de Fortinet, Jaime Chanagá tiene una gran responsabilidad en terreno, visitando empresas privadas y públicas, para conocer de cerca el impacto de la ciberseguridad en cada negocio de la Región. Su experiencia de 28 años en el mundo de la tecnología y más de 25 como CISO en compañías ligadas a salud, finanzas y telecomunicaciones lo convierten en un referente en este tema. Channel News conversó con el ejecutivo en su reciente visita a Chile.

La ciberseguridad en América Latina fue el gran tema del 2023 y lo es también en 2024. ¿Coincide con eso?

Definitivamente sí. La ciberseguridad está convirtiéndose en el desafío número uno de negocios para todas las organizaciones del sector privado y también para las iniciativas de gobierno digital en América Latina.

Hay que ser realistas respecto a que Internet no tiene fronteras ni límites, y tampoco lo tienen los riesgos que representa para cualquier empresa, sea cual sea el rubro. Mientras una organización esté conectada a Internet, el riesgo es global, y hablando de riesgos en América Latina, no cabe duda que son crecientes.

Según nuestro laboratorio FortiGuard Labs, que es una organización dentro de Fortinet, conformado por más de 500 expertos en inteligencia de amenazas, dark web, analistas de datos y ciber armamentos- América Latina y Caribe sufrió más de 200 mil millones de ciberataques en 2023. Se trata de ataques sofisticados, que ponen en riesgo infraestructuras, información confidencial de gobiernos y datos críticos a nivel de las personas.

¿Cómo ha evolucionado la conciencia de la ciberseguridad?

Las ciber amenazas no son nuevas, pero ciertamente hoy hay más concientización, especialmente en el sector privado, a nivel de la alta dirección. Durante el último año he tenido la posibilidad de participar en juntas directivas de grandes empresas en países de toda la región, y puedo afirmar con certeza que la mayor preocupación es el ciber riesgo, que no es sólo robo de información, sino además daño a la reputación de las empresas.

Esa preocupación de las organizaciones, ¿se condice con la inversión que están haciendo en ciberseguridad?

No siempre ni necesariamente. Hay algunos sectores que están invirtiendo, pero otros aún están luchando con los desafíos económicos del negocio. Por ejemplo, sabemos que a nivel mundial más del 90% de los hospitales sufren ciberataques, sin embargo, el sector salud invierte considerablemente menos que la banca, porque la banca -por la naturaleza de su negocio y porque han sido atacados por tantos años- está más concientizada y tiene más presupuesto para hacer esas inversiones. En el caso de los hospitales, es más complejo porque muchas veces tienen que decidir si proteger las bombas de infusión -que en su mayoría se controlan remotamente y podrían ser hackeadas y provocar sobredosis en pacientes- o invertir en nuevos equipos de resonancias magnéticas para salvar vidas.

Entonces, ¿cuáles son las industrias más atacadas en América Latina?

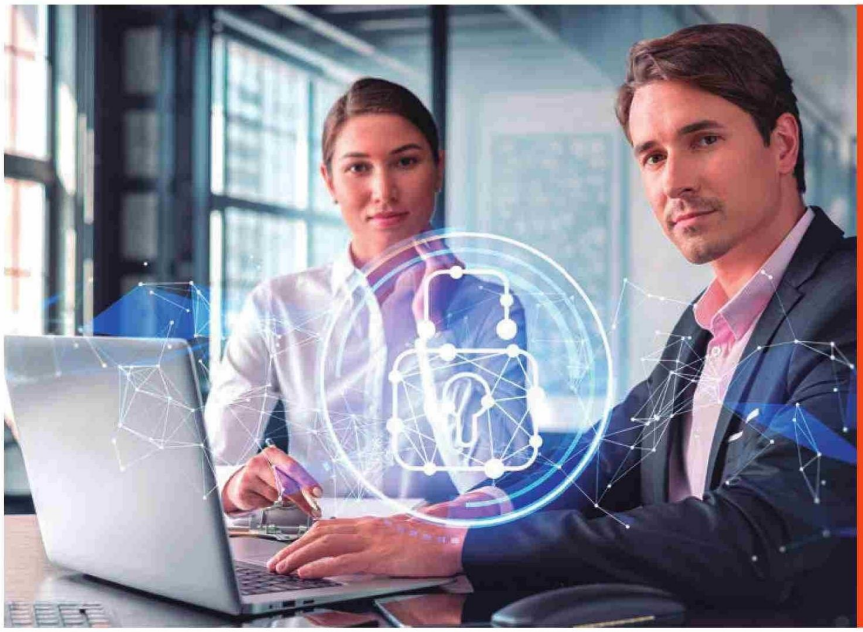
Hoy en día, en toda las Américas, nos encontramos frente al desafío de pro-

LITORALPRESS

Fecha: 29-07-2024
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: “La ciberseguridad está convirtiéndose en el desafio numero uno de negocios para todas las organizaciones”

Pág. : 39
Cm2: 409,1

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida



“La ciberseguridad está convirtiéndose en el desafío número uno de negocios para todas las organizaciones del sector privado y también para las iniciativas de gobierno digital en América Latina”

teger la infraestructura crítica. Dentro de la infraestructura crítica están todas las plataformas esenciales para que la sociedad funcione, responsables de servicios como salud, telecomunicaciones, seguridad, banca y energía. Durante los últimos años, algunas empresas de distribución eléctrica han sido hackeadas y se han visto imposibilitadas de entregar sus servicios, provocando gravísimos problemas en las comunidades que atienden.

Hay sectores que definitivamente deben invertir más. Por ejemplo, cuando vemos las agendas digitales de distintos gobiernos, observamos que en algunos casos se están haciendo fuertes inversiones en servicios digitales, pero no en plataformas de ciberseguridad que sean capaces de protegerlos.

Todo esto, ¿está “despertando” a los CISOs de América Latina?

Vemos que hay una mayor concientización más amplia y profunda a nivel de la alta dirección, sin embargo, en América Latina hay muy pocos CISOs nombrados como tales. De ellos, muchos están bajo el CIO, lo que representa un problema, porque se trata de dos funciones que en algún momento pueden tener un conflicto de interés.

Ahora bien, sí, cada vez más los CISOs están haciendo un trabajo extraordinario, mitigando el panorama de amenazas y de riesgos, que cambia segundo tras segundo. Pero hay una gran brecha que acortar, porque existen estadísticas sorprendentes que señalan que las empresas en América Latina demoran 204 días en detectar un incidente de ciberseguridad, es decir, que tardan cerca de 9 meses en darse cuenta que fueron hackeadas.

¿Qué temas forman parte de la lista de preocupaciones de las organizaciones, especialmente en esta segunda mitad del año?

Vemos una preocupación respecto a ciertas tendencias tecnológicas, entre ellas, la aceleración y el avance de la Inteligencia Artificial en materia de ciberseguridad y la seguridad que debe acompañar la explosión del IoT a todo nivel.

En base al contacto con CISOs y directivos de organizaciones en toda América Latina, Caribe y Canadá, puedo afirmar que los próximos dos años el panorama de la Inteligencia Artificial va a ser muy diferente, porque además la computación cuántica está entrando con fuerza en muchos sectores y eso acelerará el desarrollo de nuevos modelos de desarrollo y de aplicación de la Inteligencia Artificial.

En Fortinet proyectamos ese futuro y como estrategia hemos adoptado la Inteligencia Artificial para estudiar las amenazas. Actualmente tenemos 41 soluciones que adoptan la Inteligencia Artificial en el procesamiento de diferentes funciones de seguridad, o en algunos casos implementan Inteligencia Artificial Generativa para ayudar a las organizaciones a cerrar la brecha de talento que se requiere cubrir, que sólo en América Latina llegará a los 2 millones de profesionales de ciberseguridad este 2024.

Con la irrupción de la Inteligencia Artificial, seremos testigos de una revolución en muchos sectores industriales, lo que va a cambiar el panorama de las ciber amenazas en los próximos dos años y a volverlo todavía más demandante. /ChN