

FORTINET

ANDRÉS PÉREZ, VICEPRESIDENTE DE VENTAS FORTINET CHILE:

“Tenemos una responsabilidad con la sociedad que va más allá de la tecnología”

La ciberseguridad en Chile y la región exige que organizaciones y gobiernos reconozcan la transformación de las amenazas cibernéticas de ataques individuales a ecosistemas criminales integrados y automatizados. Aquí, el especialista aborda los mayores desafíos que tenemos en este ámbito como país.

De acuerdo a datos obtenidos por Forti-Guard Labs, el laboratorio de inteligencia y análisis de amenazas de Fortinet, el año pasado Chile fue víctima de 26.6 mil millones de intentos de ciberataques, siendo julio y agosto los meses con mayor actividad.

Esto indica que el panorama de amenazas no para de crecer, todo lo contrario. "La importancia de la ciberseguridad se ha vuelto cada vez más relevante, sobre todo después de la pandemia. Porque cambió el paradigma completamente. Tuvimos que adaptarnos, conectarnos desde las casas y la forma de trabajar también cambió. Personas, empresas, gobiernos, todos tuvimos que adaptarnos, pero este huracán de cambios hizo que creciera en paralelo un nuevo negocio para los ciberdelincuentes que aprovechan la masividad. Así, su target objetivo se amplió al 100%. Por lo tanto, hoy el desafío de la ciberseguridad es brutalmente mayor", explica Andrés Pérez, vicepresidente de Ventas Fortinet Chile.

Sin duda, hoy la ciberseguridad es transversal a la sociedad completa ¿Cuál es el escenario que se vive en Chile?

Chile tiene una de las mejores conectividades a nivel mundial, en penetración de Internet, cobertura, rapidez. Lo cual dista bastante de los demás países de la Región. Por lo mismo, los desafíos son mayores. La masificación de la Inteligencia Artificial (IA) hoy también es aprovechada por los ciberdelincuentes, por lo cual no solo estamos más expuestos, también debemos defendernos de otra manera, tomando conciencia de la identidad digital, apoyando las leyes de ciberseguridad y protección de datos. En definitiva, entendiendo que la ciberseguridad nos compete a todos. El ecosistema de empresas, gobierno y personas tiene que lograr entender los riesgos y su impacto para tomar medidas. Y para eso, compañías como Fortinet tenemos la obligación de concientizar y educar.

¿De qué manera Fortinet aborda esa responsabilidad?

Implementamos una iniciativa, promovida por el equipo de Ingeniería, que realiza charlas y talleres en colegios, universidades y otras organizaciones, de manera gratuita. Tenemos que llegar a todos, a niños, jóvenes, adultos mayores. Tenemos una responsabilidad con la sociedad que va más allá de la tecnología. Además, entregamos a las empresas servicios de concientización, ciertamente. No obstante, como compañía también somos sometidos a auditorías internas, de forma permanente.

Además, la compañía cuenta con un equipo de asesores legales para aportar en las implicancias y alcances de la normativa vigente



El ecosistema de empresas, gobierno y personas tiene que lograr entender los riesgos y su impacto para tomar medidas.

de ciberseguridad y protección de datos personales.

Otro desafío es la falta de especialistas. Se estima que se necesitan 1,3 millones de profesionales en la región para cubrir la creciente brecha de talento especializado...

Hay que romper paradigmas. La ciberseguridad tiene un muy amplio espectro de trabajo y es un área bien remunerada. Desde Fortinet incentivamos la relación con universidades, hemos entregado equipamiento para laboratorios, realizamos trabajo de concientización y tenemos cursos gratuitos de ciberseguridad, entre otras iniciativas.

El reciente apagón nos llevó a muchos

Claves de ciberseguridad 2025

- Transformar la seguridad en una ventaja competitiva
- Incorporar la gestión de riesgos en el corazón de la gobernanza
- Invertir en arquitecturas Zero Trust y modelos descentralizados
- Impulsar la inteligencia artificial y el análisis predictivo
- Promover una cultura de seguridad en todos los niveles
- Construir resiliencia con énfasis en continuidad y recuperación

a pensar que fue un ataque a la infraestructura crítica ¿Estamos preparados para una situación así?

Sin duda, tenemos mucho aún que mejorar y entender el impacto que puede tener un ataque a los servicios básicos. Esto, porque puede afectar a la población en su totalidad. El impacto aquí es tremendamente alto. El apagón sirvió para dimensionar lo que puede pasar y el gran desafío que tenemos ahí como país. Tenemos que aprender a convivir en el ciberespacio, sin miedo, comprendiendo los riesgos y cómo tomar medidas de resguardo.

www.fortinet.com