LITORALPRESS

Fecha: 29-06-2022
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Actualidad
Título: CUÁLES SON LOS PRINCIPALES CONSEJOS DE CIBERSEGURIDAD para líderes empresariales en servicios financieros

Pág. : 13
Cm2: 745,7

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

DIEGO AGUIRRE

A JUICIO DE LOS EXPERTOS:

CUÁLES SON LOS PRINCIPALES CONSEJOS DE CIBERSEGURIDAD para líderes empresariales en servicios financieros

◆ Mentalidad centrada en el riesgo, entenderla como una responsabilidad a nivel organizacional e invertir en sistemas con herramientas que permitan la prevención y no solo la reacción, son algunos de los tips que los especialistas entregan a los altos ejecutivos de esta industria.

De acuerdo con el último X-Force Threat Intelligence Index, de IBM, la industria financiera fue la segunda más atacada globalmente en 2021, con Latinoamérica recibiendo el 9% de los ciberataques. El acceso a servidores surgió como el principal tipo de embestida a las organizaciones de servicios financieros y de seguros, representando el 14% de todos los ataques. Seguido por ransomware, configuraciones incorrectas y fraude, empatados en el segundo lugar con un 10% cada uno. En nuestra región, el principal tipo de agresión fue el ransomware, que representó el 29% de los ataques en general.

Ante este escenario, tres especialistas en ciberseguridad entregan consejos a líderes empresariales en servicios financieros para combatir las vulnerabilidades. Estos van desde mantener un mentalidad centrada en el riesgo hasta realizar inversiones en sistemas con herramientas que permitan la prevención y no solo la reacción frente a los ataques.

CENTRADO EN EL RIESGO

Paola Peñarrieta, socia adjunta de Consultoría en Riesgo Tecnológico en Servicios Financieros de EY, dice que lo primordial es enfrentar la seguridad cibernética con una mentalidad centrada en el riesgo. "Primero es importante entender a qué amenazas se enfrentan, el nivel de riesgo que están dispuestos a aceptar y, con esa información, establecer una estrategia que permita priorizar la inversión para las áreas más relevantes, ya que hoy no se trata de si los atacantes vulnerarán las defensas, sino de cuándo lo harán y cuánto daño causarán", explica.

Asimismo, entender la ciberseguridad como una responsabilidad compartida y primordial desde el directorio de la compañía y que trasciende al resto de la organización es otro de los consejos que entregan los expertos, ya que el compromiso ante esta debe ser transversal mediante todas las acciones.

Diego Macor, gerente de Ciberseguridad de IBM Sudamérica, suma a estos consejos el dar continuas mejoras a la privacidad y protección de datos. "Las empresas deben asegurarse de que se realicen fuertes controles de seguridad de datos para evitar el acceso no autorizado, desde los datos de monitoreo para detectar la actividad sospechosa, hasta el cifrado de datos sensibles donde sea que vayan. Estas políticas de privacidad adecuadas deben ser implementadas para mantener la confianza de los clientes", detalla.

Por su parte, Ricardo Seguel, director del Magíster en Ciberseguridad de la Universidad Adolfo Ibáñez, explica que las compañías de la industria financiera han invertido por más de 20 años en seguridad cibernética, siendo los bancos los que lideran en este rubro. Sin embargo, dice, en el último tiempo han ocurrido incidentes graves en dichas entidades, demostrando que ninguna organización está exenta de ser atacada y que la inversión en ciberseguridad debe ser consistente con la cultura organizacional.

CASO DE ÉXITO

"Es por esto que invertir en sistemas de ciberinteligencia para contar con herramientas de prevención y no solo de reacción es importante, junto con reforzar los protocolos de contratación de proveedores y recursos humanos internos o subcontratados para disminuir el riesgo de que haya infiltrados de bandas de ciberdelincuentes o del cibercrimen al interior de la organización", añade el académico.

Según los especialistas, el riesgo de ciberseguridad tiene que ser preocupación a nivel de directorio y una de las inquietudes debe ser saber cómo supervisar y anticiparse a las amenazas.

"En este sentido, uno de los casos de éxito que hemos visto es la implementación de un panel de control del riesgo cibernético", comenta Peñarrieta. Y explica: "Con el fin de resolver la visibilidad limitada que existía en relación con la posición de seguridad cibernética de un banco, se diseñó, desarrolló e implementó un tablero centralizado de riesgos cibernéticos, para lo que fue necesario identificar las fuentes de datos y desarrollar métricas relevantes sobre los niveles actuales y futuros de amenazas entregando información en tiempo real para una toma de decisiones más rápida".

El resultado de lo anterior permitió contar con una vista detallada de todos los programas de ciberseguridad de la organización en un tablero dinámico y centralizado, contando con métricas ajustadas para cada rol en la organización según la relevancia e informes detallados.

Las empresas deben asegurarse de que se realicen fuertes controles de seguridad.

HYPO PHOTOS

RECOMENDACIONES

Mejorar la privacidad y protección de datos internos y de clientes: tener más usuarios digitales significa que las empresas también tendrán datos más sensibles del consumidor por proteger.

Ciberseguridad desde el directorio: esta tiene que trascender en la organización, siendo parte de la cultura organizacional donde todos los colaboradores deben estar comprometidos con la seguridad en todas sus acciones.

Invertir en prevención y no solo reacción: entender que no es un gasto, sino que una inversión, e invertir en un sistema de ciberinteligencia para contar con herramientas de prevención y no solo de reacción.

Enfrentar la ciberseguridad con una mentalidad centrada en el riesgo: entender a qué amenazas se enfrentan, el nivel de riesgo que están dispuestos a aceptar y, con esa información, establecer una estrategia que permita priorizar la inversión para las áreas más relevantes. La resiliencia cibernética va más allá de la seguridad cibernética tradicional y enfatiza la continuidad y la recuperación.