¿Cómo puede la industria aseguradora enfrentar los ciberataques?

La innovación digital en la industria de seguros se viene dando en un contexto de ciberriesgos de impacto y frecuencia crecientes. Así que la gestión de ciberamenazas es fundamental para la habilitación de nuevos negocios en las compañías del sector.

Samuel Iván Ardila
Socio de Asesoría en Riesgos, Cyber
Deloitte Spanish Latin America

Contexto y desafíos del entorno cibernético

Durante 2022 se detectaron más de 19,000 vulnerabilidades de ciberseguridad, siendo el *ransomware* la amenaza más crítica para todos los sectores de la industria, incluido el sector asegurador, facilitando la extorsión y la divulgación no autorizada de información sensible de las organizaciones. En este sentido, el Foro Económico Mundial clasificó a los riegos cibernéticos en el puesto 8 del ranking de riesgos globales de mayor criticidad en 2023.

El *ransomware* comienza a través de un acceso otorgado al atacante vía phishing o con la explotación de vulnerabilidades en las estaciones de trabajo de la organización. Posteriormente, el atacante se conecta a la red interna y comienza a identificar vulnerabilidades de seguridad en la plataforma tecnológica de la organización. Posteriormente, se mueve lateralmente en la red para comprometer los recursos tecnológicos críticos y/o extraer información sensible de la compañía. Con ello, la organización criminal da inicio a la extorsión y/o difamación de la organización. Este es tan solo un ejemplo de una realidad que ha colocado en riesgo la continuidad, la rentabilidad, la imagen e incluso la viabilidad de algunas compañías de la industria aseguradora.

La transformación digital de las compañías y el incremento de servicios en línea que son demandados por el mercado nos genera mayor exposición a riesgos cibernéticos. La integración de terceros en la cadena de valor también nos expone a ciberincidentes que podrían originarse fuera de la organización. El desafío al que nos enfrentamos es continuar adelante con estas iniciativas mientras mantenemos el nivel de los riesgos de ciberseguridad en un nivel aceptable.

¿Cómo prepararse para los ciberataques?

Las medidas de protección son necesarias para este tipo de ataques. La evaluación y mejora continua de las capacidades de gestión de la ciberseguridad de la organización es el motor de la protección, detección, respuesta y recuperación frente a los ataques o eventos cibernéticos. Dichas capacidades deben estar enfocadas principalmente a 1) asegurar las plataformas tecnológicas y mitigar la ocurrencia de eventos eludibles en estas; 2) acompañar el proceso de transformación digital; 3) desarrollar capacidades para detectar y responder ante incidentes de seguridad (tales como, inteligencia de amenazas, monitoreo de eventos y simulaciones ejecutivas, tácticas y técnicas); 4) proteger a la organización de riesgos de ciberseguridad derivados del acceso de terceras partes a información de la compañía.

Un ataque cibernético puede dar origen a una crisis importante, por ejemplo, como resultado de la fuga de información sensible. Las crisis dentro de las organizaciones se materializan de forma repentina e inesperada y en muchos casos a partir de un evento considerado inicialmente como de menor impacto. Un aspecto fundamental en la gestión de las crisis es la toma de decisiones inteligentes de forma urgente a partir de información incompleta. Dentro de los retos a manejar en la gestión de una crisis están: la sensación de pérdida de control sobre la situación, la alta presión interna y externa para dar respuestas y la sensibilidad de la comunicación interna y externa.

El tiempo es un factor crítico en la gestión del incidente y de la crisis que posteriormente se genere.

> La mejor forma en la que una organización puede mejorar sus capacidades para la gestión de una crisis cyber es el desarrollo de un programa de ciberresiliencia.

Al inicio una intrusión pasa desapercibida por lo que pasa tiempo para que esta sea detectada. Y una vez se identifica el incidente, comprender su impacto y alcance puede llevar días y hasta semanas. De forma posterior a la respuesta inicial del incidente se deberá desarrollar la activación del plan de continuidad del negocio, la recuperación de la plataforma tecnológica y la gestión de la crisis.

La mejor forma en la que una organización puede mejorar sus capacidades para la gestión de una crisis cyber es el desarrollo de un programa de ciberresiliencia que incluya la definición formal de las actividades de investigación, incluyendo el triage y el análisis de causa raíz, y la planeación de la recuperación de los procesos, la tecnología y el acceso a los datos que sean interrumpidos por un incidente de ciberseguridad.

Adicionalmente, es fundamental la preparación de los líderes de las compañías para enfrentar este tipo de situaciones. Y muy relacionado con esto, la efectividad de la toma de decisiones es uno de los mayores desafíos durante la gestión de crisis. Por lo tanto, es crucial que las organizaciones capaciten de forma anticipada a sus líderes a convertirse en transformadores durante las crisis cibernéticas, además de entrenarlos en herramientas y técnicas que puedan ayudarlos a gestionar la crisis. Lo anterior, apuntando a contrarrestar las tendencias y estilos de liderazgo de la organización que puedan jugar en su contra al momento de enfrentar una situación crítica.

YouTube

El video de la intervención de Samuel Ardila está **disponible** en el canal de Youtube de Fasecolda.

Clic aquí

Es importante identificar los participantes (socios de negocios, canales, clientes, proveedores y otros) del ecosistema digital del que hacen parte y gestionar los riesgos de ciberseguridad y continuidad originados por dicha interacción con terceros.

Samuel Ardila, en su intervención en la Convención Internacional de Seguros 2023 de Fasecolda.

Conclusión

Para enfrentar las ciberamenazas las organizaciones del sector asegurador, sus líderes y colaboradores deben adquirir conciencia del entorno cada vez más complejo que estamos enfrentando y el aumento de incidencias e impactos de los incidentes de ciberseguridad. Adicionalmente tal como hemos visto en incidentes recientes, es importante identificar los participantes (socios de negocios, canales, clientes, proveedores y otros) del ecosistema digital del que hacen parte y gestionar los riesgos de ciberseguridad y continuidad originados por dicha interacción con terceros. Y, por último, las compañías del sector no deben enfocarse solo en mejorar las medidas de protección, sino también las capacidades de detección, respuesta, recuperación y manejo de crisis ante ciberataques, como parte de un programa de ciber resiliencia integral.

Bibliografía

Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S.

Global Risk Report 2021, World Economic Forum,
http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

National Vulnerability Database, National Institute of Standards and Technology (NIST)
https://nvd.nist.gov/vuln/full-listing