6124201

Tiraje: 22000

Cm²: 1,142.57

Alto Nivel
19/09/2024
Sección: Primera Página: 030-031

ALTO NIVEL

Por · Claudia Cerezo

CÓMO POTENCIAR LA CIBERRESILIENCIA

Paula Álvarez
Socia de Technology & Transformation y especialista en ciberseguridad en Deloitte Spanish Latin America

Los ciberdelincuentes están adoptando nuevas tecnologías, como la IA generativa, para aumentar el número de mercados en los que pueden operar. Responder a esto requiere una inversión en soluciones y talento que muchas organizaciones no pueden afrontar. ¿Qué hacer entonces para protegerse?

RETRATO | ARTURO AGUIRRE TAPIA

Poco a poco, la inteligencia artificial generativa (IAGen) cambiará por completo el panorama de la ciberseguridad. Los primeros impactos ya comenzaron a verse. Hace algunos meses, en redes sociales circuló un video en el cual el empresario Carlos Slim promovía un supuesto proyecto para invertir dinero y obtener rendimientos altos. En la imagen, Slim solicita a la gente redirigirse a un enlace para llenar un formulario y así poder ganar hasta 21,000 pesos al día. El video es totalmente falso, pues fue manipulado con IA.

Este tipo de fraudes no son cosa menor. De hecho, el Foro Económico Mundial ha catalogado la ciberdelincuencia, la ciberseguridad y los efectos adversos de la IA entre los 10 principales riesgos mundiales a corto plazo, y también ha hecho un llamado a las empresas para potenciar su ciberresiliencia.

En entrevista con **Alto Nivel**, Paula Álvarez, socia de Technology & Transformation y especialista en ciberseguridad en Deloitte Spanish Latin America, explora los retos a los que se enfrentan los líderes empresariales en materia de ciberseguridad.

AN • Paula, ahora que los ciberdelincuentes están usando herramientas cada vez más sofisticadas para perpetrar ataques, como la IA, ¿cómo las empresas pueden crear un ciberespacio más seguro?

Hoy en día, apenas estamos viendo efectos muy pequeños de la IAGen, que es la que realmente va a cambiar el panorama de la ciberseguridad, por su capacidad para generar noticias falsas, hacer phishing o programar ciberataques totalmente nuevos y más difíciles de detectar. Lo que viene a futuro es realmente grave, así que las empresas deben combinar soluciones tecnológicas, algunas con IA, con servicios de consultoría especializada y mucha concientización y capacitación de personas, ya que los colaboradores de una organización son el eslabón más vulnerable.

Todos estos elementos deben articularse muy bien para definir una estrategia de ciberseguridad integral y multidisciplinaria. El problema es que muchas veces no se realiza de esta manera. Las organizaciones van poniendo herramientas, ejecutando proyectos, pero no existe un plan rector con un enfoque holístico.

Es muy común que las organizaciones implementen soluciones y herramientas tecnológicas potentes, pero que les saquen poco provecho. Adicionalmente, muchas organizaciones quieren manejar numerosos temas de seguridad de manera interna, cuando ese no es su giro principal de negocio. El talento y la especialización se han vuelto muy escasos en este ámbito, y realmente es mucho más efectivo tercerizar estos procesos, herramientas y controles.

AN • Muchas empresas están incrementando sus presupuestos en ciberseguridad, pero con el crecimiento y la sofisticación de los delitos, no hay dinero que alcance. ¿Cómo sacar el mejor provecho a las inversiones en ciberseguridad? ¿Cuál es el primer paso para garantizar que la estrategia de una empresa funcione?

El paso cero es hacer una evaluación de madurez de sus capacidades de ciberseguridad para saber dónde están hoy, incluyendo un benchmark con respecto al nivel de madurez de la industria. De ahí se debe definir el objetivo a alcanzar en determinado tiempo y se genera un plan de transformación. Para esta evaluación se utilizan marcos internacionales reconocidos. Nosotros tenemos un

modelo que se basa en los tres principales marcos: ISO 27001 [para establecer un sistema de gestión de la seguridad de la información], el marco de ciberseguridad NIST [del Instituto Nacional de Estándares y Tecnología de Estados Unidos] y CIS [las prácticas recomendadas por el Centro de Seguridad en Internet].

Para la evaluación de la madurez en ciberseguridad usamos los cinco niveles del modelo CMMI. En el nivel 1 se encuentran las empresas menos maduras y en el nivel 5, las organizaciones con un nivel de madurez óptimo. La evaluación de capacidades de ciberseguridad se realiza a través de una consultoría especializada.

AN • ¿Qué tan bien preparadas están las organizaciones para hacer frente a un ciberataque, tomando en cuenta su nivel de madurez?

La mayoría de las organizaciones llevan años de atraso con respecto a tener un programa de ciberseguridad maduro que les permita estar razonablemente protegidas. Las empresas necesitan invertir no solamente en herramientas tecnológicas, sino en consultoría y en recursos especializados en materia de ciberseguridad. Los ciberdelincuentes con dinero a disposición, mientras que las organizaciones se enfrentan con presupuestos limitados, falta de talento, entre otras cosas, por lo que la velocidad de implementación de programas de ciberseguridad es más lenta que la evolución del cibercrimen.

Es imperativo que las organizaciones, sus consejos y comités directivos despierten y actúen frente a esta situación, si es que no lo han hecho. Esto no es un tema tecnológico; es un asunto que le corresponde atender al negocio. Las organizaciones deben trabajar diligentemente en cerrar esa brecha en materia de ciberseguridad.

AN • Además de presupuestos limitados, ¿qué otros retos tienen que enfrentar las organizaciones para mejorar la seguridad de su información y de sus sistemas?

La escasez de talento expecializado en ciberseguridad y la falta de concientización a nivel C-suite. Aunque esto ha ido mejorando significativamente, algunas organizaciones siguen enfocadas en el cumplimiento, en obtener una certificación o en cumplir con requisitos regulatorios, pero no se centran en un enfoque de riesgos.

La complejidad tecnológica crece día con día. Antes hablábamos de operaciones centralizadas en un data center, pero hoy tenemos múltiples plataformas, herramientas, niveles de interacción entre las mismas; es decir, la superficie de ataque es mucho mayor y eso debe tomarse en cuenta.

AN • ¿Cuál es la principal preocupación que enfrentan los líderes empresariales en materia de ciberseguridad?

El ransomware, que generalmente conlleva que se paren operaciones. El tiempo de recuperación de un ciberataque dependerá de qué tan preparada está la organización para hacerle frente. Ese tiempo puede llegar a ser muchas semanas y, por supuesto, implica pérdidas muy grandes, como daño a la imagen y a la reputación.

Las principales entradas para este tipo de ataque son: los accesos remotos de redes virtuales privadas no protegidos adecuadamente (en especial, no contar con doble factor de autenticación para ingresar a la red); la explotación de vulnerabilidades en los firewalls, que ocurren por la falta de actualización de parches de seguridad de los sistemas; y el ataque sobre las personas que se hace mediante phishing e ingeniería social, para robar credenciales de acceso o lograr que se descarguen y ejecuten archivos con software malicioso.

Uno de los miedos más grandes de los líderes de empresas es, precisamente, que no pare la operación en empresas industriales, como manufactura, minería o energía. Antes ocurrían más ciberataques en oficinas administrativas, pero ahora están aumentando los ataques en industrias que tienen sistemas OT (*Operational Technology*), como empresas de ferrocarriles, plantas nucleares, de tratamiento de agua, etcétera. En estas instalaciones hay que mejorar mucho la protección, porque la operación es 7x24 y no cuentan con expertos en seguridad informática.

AN • Por último, Paula, ¿cómo pueden las empresas detectar un ciberataque y qué deben hacer?

Para comenzar, las empresas deben tener programas que incluyan la capacidad de detección temprana e inteligencia para poder adelantarse a un ciberdelito, pero eso no es así en muchísimos casos. Generalmente, las organizaciones se enteran de que fueron víctimas mucho más tarde. Algunas pueden tardar meses, y mientras tanto el enemigo está dentro de la red, moviéndose y estudiando qué información extraer o qué golpe dar (dependiendo del tipo de ataque).

Adicionalmente, las organizaciones deben tener planes de respuesta a incidentes, que implican playbooks de cómo responder diferentes escenarios, así como un plan de crisis que debe incluir aspectos de comunicación interna y externa. La idea es contener los ataques y minimizar el daño. Y, como última capa, existe lo que llamamos el plan de continuidad, que sirve para restablecer los sistemas y datos.

El desafío es que muchas organizaciones no cuentan con esos planes o solo los tienen por cumplir, pero no necesariamente son efectivos al momento de ejecutarse, o se encuentran muy desactualizados. **AN**