La evolución del SOC, clave para enfrentar ciberamenazas

Por: Marcos Polanco, Director Ejecutivo de Ciberseguridad e Innovación de TELMEX-Scitum

La estrategia de seguridad de muchas organizaciones se ha enfocado en tratar de proteger, detectar y responder de la mejor forma posible ante las ciberamenazas que ponen en riesgo la viabilidad de los negocios, así como la confianza en las instituciones, lo cual las obliga a estar preparados para enfrentar los peores escenarios.

En la actualidad vivimos un entorno cada vez más complejo y con mayor incertidumbre y el paradigma ha cambiado. Ahora no se trata de preguntarnos si nos atacarán o no, sino de cuándo sucederá y si estaremos preparados.

Esta transformación se ha visto reflejada en al menos cuatro características:

1. Los ambientes de las Tecnologías de la Información (TI) han evolucionado a los servicios en la Nube, la virtualización, los microservicios, las aplicaciones móviles, entre otras.
2. El crecimiento promedio de 30% anual en el número de ciberataques en los últimos cinco años.
3. Las alertas de seguridad que requieren análisis generalmente sobrepasan la capacidad del personal, ya que su operación depende de muchas labores manuales.
4. La escasez de talento y el alto costo de personal calificado.

Una parte fundamental de esta estrategia ha sido contar con un SOC (*Centro de Operaciones de Seguridad, por sus siglas en inglés*), ya sea interno o tercerizado, cuya misión es detectar y responder a las ciberamenazas de una organización.

Hoy es necesario que estos centros consideren una serie de elementos nuevos para estar a la altura y enfrentar los retos que este entorno de amenazas cibernéticas representa. Algunos le llaman “Next Generation SOC”, “Cyber Security Operations Center” o “Intelligent SOC”. Como sea, lo importante es reducir la probabilidad de sufrir un incidente de seguridad y, en caso de materializarse un ataque, disminuir el tiempo de detección, análisis y contención.

Entre los elementos a contemplar está el uso de nuevas tecnologías basadas en la **inteligencia artificial** para automatizar las tareas básicas y repetitivas del SOC, con el fin de reducir las labores manuales, así como tener mayor precisión y velocidad en el análisis, filtrado, enriquecimiento de los eventos. De este modo, se logra una mayor capacidad para escalar y apalancar la experiencia del personal.

Asimismo, se debe incluir el uso de la **ciberinteligencia** para contextualizar las amenazas y priorizar de mejor forma las alertas en las que se debe focalizar el personal, también para proporcionar posibles cursos de acción y recomendaciones que faciliten la toma de decisiones.

Es fundamental también **investigar las amenazas** de forma continua, lo cual significa que además de atender las alertas recibidas -las cuales tienen puntos ciegos-, debemos ir a la caza del atacante al buscar indicios de actividades inusuales, rastros de conexiones, accesos no legítimos o cualquier indicador que ayude a detectar que algo está pasando.

Finalmente, en la **respuesta a incidentes** se pueden ejecutar tareas automáticamente a través de plataformas especializadas (llamadas "de orquestación") y se debe contar con planes de contención predefinidos (*playbooks y workflows*), los cuales deben aplicarse a través del flujo de atención a un incidente.

Estos elementos permitirán implementar un ciclo denominado OODA (*Observar-Orientar-Decidir-Actuar*), mediante el cual se busca tener la mayor visibilidad posible de lo que sucede en el entorno digital; procesar, analizar, enriquecer y contextualizar esa información para detectar lo antes posible las amenazas, entendiendo su impacto potencial al negocio y finalmente detonando las acciones necesarias para minimizar dicho impacto.

La buena noticia es que México posee uno de los SOC másavanzados de Latinoamérica, operado por TELMEX-Scitum, y a través del cual se contienen miles intentos de ataques diariamente.

Madurar nuesra preparación para responder a las ciberamnazas es imprescindible para la economía deMéxico, donde más de 22 millones de personas son afectadas por diversos delitos cibernéticos cada año, con un costo de hasta 5 mil millones de dólares, como calcula la Estrategia Nacional de Ciberseguridad del Gobierno Federal.