NOTA DE PRENSA
14 / 02 / 2019

¿Están las organizaciones preparadas para el próximo ciberataque?

> El daño que provoca sufrir un ciberataque está aumentando y podría llegar a alcanzar los 6 trillones de dólares en 2021

Los ciberdelincuentes son los maestros del crimen en constante evolución, probando y afinando sus técnicas para extraer información valiosa y sensible para su propio beneficio. Existe una amplia gama de formas para lanzar ciberataques. Por ejemplo, los ataques de Amenazas Persistentes Avanzadas (Advanced Persistent Threat o APT por sus siglas en inglés) que llevan a cabo sofisticados intentos de hackear a personas, negocios o países; ataques phishing para robar información sensible; robo de contraseñas; y ataques ransomware. El daño que provoca sufrir alguno de estos ciberataques está aumentando tanto que podría alcanzar los 6 trillones de dólares en 2021.

Las organizaciones de todos los tipos y tamaños se enfrentan a diario a estos ciberataques, sabiendo que nunca llegarán a estar 100% seguros. Cualquier hacker habilidoso puede atacar incluso los puntos más protegidos si es lo suficientemente persistente. Esto les deja en una situación muy desesperante, ya que las empresas sólo pueden aguardar a que se produzca un ciberataque para después mitigar el daño sustancial causado. El Fondo Monetario Internacional (IMF) estima que las instituciones financieras tienen unas pérdidas anuales de cientos de billones de dólares de media al año por culpa de los ciberataques.

Las organizaciones son conscientes de esto y están buscando la forma de protegerse: adquiriendo más productos de seguridad que puedan ayudarles a prevenir un nuevo ataque o redactando e imponiendo nuevos procedimientos para proteger su red y a sus empleados. Además, están implementando programas de capacitación para educar a su personal sobre ciberseguridad, contratando a expertos y a consultores para reducir los riesgos, y revisando las relaciones con sus proveedores de servicios para asegurarse de que se cumplen las reglas de seguridad en los datos más

críticos.

Por otro lado, las organizaciones también están siendo bombardeadas con llamadas a la acción que van desde proteger el acceso remoto, encriptar paquetes de datos o revisar las políticas de las credenciales hasta actualizar y parchear las vulnerabilidades, y ejecutar agentes. Todo esto es abrumador y requiere mucho tiempo y dinero, pero ¿cómo pueden saber las organizaciones si están realmente preparadas para el próximo ciberataque?

Mejor ser proactivos que reactivos

En este sentido, las empresas están buscando un enfoque estratégico que no sólo agilice sus esfuerzos en materia de ciberseguridad, sino que también obtenga los beneficios que desean, necesitan y esperan. Este enfoque debe ser proactivo y no reactivo. Las organizaciones necesitan estar preparadas antes de que se produzca un ciberataque. Para ello, hay que tener en cuenta que la mayoría de las brechas son diferentes –aunque los ciberdelincuentes pueden usar ataques vectoriales similares– y que nunca serán las mismas vulnerabilidades. Esto significa que deben estar preparados para ataques tanto conocidos como desconocidos.

Para poder hacer frente a estos tipos de ataques, las organizaciones necesitan pensar y actuar como los verdaderos actores de amenazas, utilizando una amplia gama de herramientas de malware y técnicas de ataque de manera segura y controlada. Para apoyar a las organizaciones, el fabricante **Cymulate**, experto en tecnología avanzada, permite ejecutar simulaciones de ciberataques sofisticados en cualquier momento. Con la plataforma de simulación de ataques BAS (Breach & Attack Simulation) de Cymulate es posible ejecutar ciberataques reales en el propio entorno de producción de una organización de manera segura, sin dañar la red empresarial. Además, permite comprobar cómo podrían enfrentarse a un ataque en tiempo real.

La plataforma BAS ofrece una perspectiva innovadora respecto a las prácticas ya existentes en políticas y control de seguridad, así como identificar todos los defectos que tenga una organización en temas de seguridad. La plataforma proporciona no sólo resultados de simulación, sino también recomendaciones sobre cómo mitigar las vulnerabilidades detectadas, lo que permite a las organizaciones de todos los tamaños realizar los cambios necesarios en sus productos y servicios de seguridad de datos y en sus políticas y sus programas de formación para impulsar la ciberseguridad. Recuerde: ¡estar prevenido vale por dos!

Artículo escrito por Eyal Aharoni, COO de Cymulate.

Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net