La recesión económica podría incrementar la incidencia de ciberataques

CIUDAD DE MÉXICO. 03 de mayo de 2023.- Históricamente, las crisis han sido un momento ideal que los cibercriminales aprovechan derivado del pánico que se genera entre los usuarios, para tratar de engañar y propagar sus amenazas.

Sucedió en la crisis económica de 2009, en la que la intensa presión financiera elevó la incidencia de fraude en un 55.4%; en el plano online, el Centro de Denuncias de Delitos en Internet (IC3) del FBI registró un total de 336,655 casos, un aumento de 22.3% con respecto a 2008, lo que representaron pérdidas por USD $559.7 millones.

También ocurrió con la pandemia por la Covid-19, una emergencia sanitaria que, según la Interpol elevó en un 569% los casos de *malware* y *phishing* mediante sitios apócrifos con palabras clave como "coronavirus" o "COVID". La intención, propagar información falsa relacionada con la Covid-19 como señuelo para infiltrarse en los sistemas e infectar redes.

En la actualidad, el mundo se encuentra frente a una posible recesión económica. El Banco Mundial indica que mientras las tasas de interés a nivel global se elevaron el año pasado en respuesta a los históricos niveles inflacionarios, también se prevé que la economía mundial entre en un periodo de recesión con una serie de crisis económicas en los mercados emergentes.

Esto, desde la perspectiva de Strike y como ha sucedido en el pasado, podría incrementar de manera sustancial los índices de amenazas cibernéticas como el *ransomware*, el *malware*, la propagación de fraudes mediante *phishing* y otro tipo de ataques. Si bien los retos en materia de seguridad cibernética siempre son altos, cuando la coyuntura económica es desfavorable los riesgos son aún más altos.

"Cuando las empresas y economías atraviesan por momentos de pánico, los ciberdelincuentes buscarán la forma de aprovecharse de ello. Cada día los actores maliciosos se vuelven más sofisticados y crean nuevas técnicas de hacking para encontrar formas de intervenir los sistemas y robar información para su beneficio. Pensar como ellos para anticiparse y proteger las redes antes de que realicen cualquier movimiento, se vuelve fundamental", señala Santiago Ronseblatt, CEO y fundador de Strike.

Para ello, es importante acudir a soluciones de protección robustas y basadas en el *hacking* ético. Esto significa que, en lugar de adquirir herramientas tradicionales que se basan en procesos reactivos a la incidencia de cibercriminalidad, se deben realizar un escaneo como el *pentesting* que consisten en que un *hacker* ético, con técnicas y conocimientos similares a los de los cibercriminales, intervenga al sistema y detecte vulnerabilidades que podrían ser aprovechadas para atacar.

De esta forma, el *hacker* ético realiza un diagnóstico para la compañía que adquiere el servicio, indicando en un reporte en tiempo real las principales vulnerabilidades encontradas, el nivel de urgencia de cada una de ellas, y la solución para cerrar esas 'puertas de entrada' a la red, antes de que un *hacker* malicioso las encuentre.

En conclusión, es importante que las compañías, de todos los tamaños, sepan que el *hacking* ético es una herramienta clave en momentos de tensión y posible incremento de la incidencia delictiva *online*. El Foro Económico Mundial indica que el 93% de los jefes de seguridad cibernética y el 86% de los líderes de negocio en el mundo piensan que es "muy probable" que la inestabilidad geopolítica global orille a un evento catastrófico en materia de cibercrimen durante los próximos dos años, motivo por el cuál todos deben estar alerta y tener a la mano procesos confiables y proactivos en materia de protección digital.

-o0o-

Sobre Strike

Strike es una plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas. Esto se realiza a través de tests de penetración - o *pentests* - llevados a cabo por su red global de hackers éticos, conocidos como "Strikers", una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo ocasional o independiente. Más información en: https://strike.sh/

Síguenos en nuestras redes sociales:
Instagram - @strikesecurity
Twitter - @strike_secure
LinkedIn - Strike

Contacto para prensa México
another
Ahtziri Rangel | PR Expert
+ 52 1 55 1395 6970
ahtziri.rangel@another.co