NOTA DE PRENSA
05 / 05 / 2020

Vicarius protege a los teletrabajadores con parcheo virtual

> Vicarius ofrecerá a los empleados que trabajan en remoto protección mediante el parcheo virtual y asistencia de protección en aplicaciones de terceros

Internet se ha convertido en el mayor aliado para los negocios, tanto para mantener sus servicios activos como para continuar las relaciones con los clientes. El mejor ejemplo de ello ha sido ver cómo, a medida que la pandemia avanzaba, las empresas han cambiado la oficina por el teletrabajo que lleva al empleado a disponer de conexión a Internet sin interrupciones para acceder a las aplicaciones que utilizaba en la oficina.

Paralelamente, la crisis por coronavirus está provocando un aumento de las ciberamenazas, sobre todo en el sector sanitario y las instituciones gubernamentales y financieras. Sólo en Italia, los ciberataques han aumentado un 30% desde que comenzó el brote por coronavirus. Con las instituciones más vulnerables que nunca, es necesario tomar medidas y precauciones adecuadas para proteger las aplicaciones y los activos de las organizaciones.

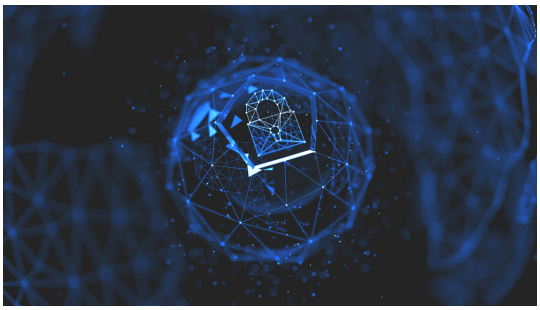
Con la intención de minimizar el riesgo de ciberataques, el fabricante de ciberseguridad Vicarius ha anunciado que ofrecerá a los trabajadores en remoto protección de las aplicaciones que utilizan mediante el análisis de vulnerabilidades así como el parcheo virtual de cualquier vulnerabilidad que se detecte en las mismas. “Nuestras soluciones permiten identificar y bloquear las vulnerabilidades de software. Estas herramientas son las que necesitan con más urgencia la mayoría de los trabajadores en remoto ya que al estar teletrabajando no se dispone de las mismas medidas de protección que en la oficina, siendo más fácil explotar vulnerabilidades de determinadas aplicaciones al no estar parcheadas aún o no poder desplegar esos parches de seguridad tan rápidamente como si estuvieran en los centros de trabajo. Desafortunadamente, estas soluciones son indispensables hoy en día”, afirma Michael Assraf, CEO de Vicarius.

El sector sanitario, objetivo de los cibercriminales

Muchas instituciones sanitarias están sufriendo esta oleada de ciberataques. Por ejemplo, la organización Mundial de la Salud emitió un informe a finales de marzo advirtiendo del aumento de ataques phishing. Por su parte, Worldometers, un rastreador de estadísticas internacionales, apuntó que el objetivo era ataques DDoS y 'actos maliciosos'. Y adicionalmente, el Departamento de Salud y Servicios Humanos de Estados Unidos sufrió un ciberataque a finales del marzo.

Para dar respuesta a estos ataques, Vicarius propone la solución TOPIA que permite identificar las vulnerabilidades, priorizar las amenazas y aplicar parches de seguridad en caso de que existan o bien optar por un parche virtual hasta que los fabricantes saquen el parche definitivo –que muchas veces tardan meses– creando una ventana de tiempo donde los atacantes pueden aprovechar dicha vulnerabilidad. Las herramientas de evaluación de TOPIA identifican activamente los riesgos y eliminan las amenazas, proporcionando a las organizaciones una visión completa y unos conocimientos procesables en tiempo real.

Vicarius se distribuye en la Península Ibérica e Italia a través de Ingecom, Value Added Distributor (VAD) especializado en soluciones de ciberseguridad y ciberinteligencia.



Contacto de prensa:

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