MEDIO: PORTAL PARÉNTESIS
FECHA: 24/FEBRERO/2022

Comunicación Financiera

(paréntesis.com)

¡Guerra cibernética! EU espera que conflicto en Ucrania desencadene ciberataques

Conforme avanza el enfrentamiento entre Estados Unidos y Rusia por el conflicto en Ucrania, los ciberataques y el ransomware, son una amenaza también.

Conforme avanza el **enfrentamiento entre Estados Unidos y Rusia por el conflicto en Ucrania, los ciberataques son una amenaza** también.

El gobierno de Estados Unidos está en alerta máxima ante la posibilidad de que el conflicto se extienda al ciberespacio, donde Rusia ha demostrado su capacidad para causar interrupciones y daños significativos en el pasado.

El martes, **un alto funcionario cibernético del FBI advirtió a las empresas estadounidenses** y a los gobiernos locales que deben estar atentos a posibles ataques de ransomware. Previamente, varias agencias estadounidenses emitieron una advertencia similar a los ejecutivos de los principales bancos estadounidenses.

Hay varias formas en que los piratas informáticos rusos podrían interrumpir las empresas estadounidenses y el público en general. Desde que comenzó el conflicto entre Ucrania y Rusia, **Ucrania ha enfrentado múltiples ataques cibernéticos**, este miércoles el sitio web del parlamento del país fue blanco de un ataque, así como varios bancos y agencias gubernamentales.

Las empresas de todo el mundo que trabajan con organizaciones en Ucrania deben tener especial cuidado, ya que las conexiones a los sistemas ucranianos podrían usarse como un punto de acceso para otros objetivos.

En un informe del martes, l**os analistas de S&P Global Ratings señalaron "un mayor riesgo de ataques cibernéticos en Ucrania**... lo que podría generar efectos colaterales para las corporaciones, los gobiernos y otras partes en la región y más allá".

Cómo se prepara Estados Unidos ante la amenaza de ciberataques rusos

La dependencia que tiene Ucrania de la tecnología extranjera representa un riesgo cibernético para Estados Unidos. Por ejemplo, **Ucrania no tiene satélites propios** por lo cual usa satélites comerciales para obtener imágenes y algunas de las compañías detrás de esos satélites comerciales están ubicadas en Estados Unidos y representa una vulnerabilidad para ese país.

Asimismo, **todas las cosas en los Estados Unidos que ayudan directamente a la maquinaria militar ucraniana se consideran un blanco fácil** para los rusos. Por su parte, los atacantes cibernéticos rusos apuntan cada vez más a la infraestructura estadounidense a gran escala, y los consumidores no pueden hacer mucho.

Por ello, **la defensa más importante es garantizar que se corrijan las posibles vulnerabilidades de los dispositivos de los ciudadanos estadounidenses**, a través de actualizaciones de software, autenticación de dos factores y más soluciones de seguridad.

La responsabilidad de preparación recae en el sector público y privado. **La administración de Biden se ha centrado en reforzar las defensas cibernéticas de Estados Unidos** en los últimos meses para protegerse contra ataques en el extranjero, incluidas entidades gubernamentales y empresas importantes. Pero las vulnerabilidades siempre existen, y **todo lo que necesitan los ciberdelincuentes es una oportunidad.**