MEDIO: PORTAL DINERO EN IMAGEN

FECHA: 07/MARZO/2022

Ciberataques son cada vez más sofisticados y con mayor alcance

HACKER

7 MAR, 2022

El conflicto bélico entre Rusia y Ucrania aumenta el riesgo de ataques cibernéticos indirectos, es decir, que afecten a gobiernos o entidades que tengan negocios en ambos países, que impongan sanciones o que interfieran.

Para los expertos de Fitch Ratings, el ataque conocido como NotPetya, ocurrido en 2017, es un ejemplo de los riesgos que existen actualmente. Dicho ataque inicialmente tuvo como objetivo el gobierno y las entidades financieras de Ucrania, sin embargo, terminó afectando a los sistemas informáticos de todo el mundo y costó miles o de millones de dólares en daños.

"El conflicto actual amplifica la tendencia de ataques con mayor volumen y sofisticación, con los correspondientes riesgos financieros, de reputación y legales significativos para los emisores", advirtieron en un comunicado. Esto porque, de acuerdo con cifras de SonicWall, se ha observado un aumento de mil 885% en los ataques a objetivos gubernamentales, 755% en atención médica, 152% en educación y 21% en comercio minorista en el último año.

Las agencias gubernamentales en todo el mundo destacaron el aumento del riesgo cibernético en medio de la profundización de la actual crisis europea. Por ejemplo, la Agencia de Seguridad de Infraestructura y Ciberseguridad, el Buró Federal de Investigaciones y la Agencia de Seguridad Nacional de Estados Unidos avisaron a las entidades de infraestructura crítica sobre un mayor riesgo de ataques patrocinados por el estado ruso.

Ante esta situación, varias empresas se han enfocado en contar con resiliencia cibernética, una evaluación continua de amenazas y medidas para la continuidad comercial o recuperación ante ético desastres. Algunas compañías o entidades también han optado por contratar ciberseguros.

Por Aura Hernández