

IBM Security: Responder a los incidentes de ciberseguridad sigue siendo el mayor desafío para las empresas

77% de las empresas carecen de planes adecuados de respuesta ante incidentes; mientras que el 69% informa que los fondos para la ciberresiliencia son insuficientes.

CAMBRIDGE - 21 mar 2018: IBM Security anunció los resultados de un estudio global que explora los factores y desafíos de ser una organización ciberresiliente. El estudio encontró que el 77% de los encuestados admiten no tener un plan formal de respuesta a incidentes de seguridad cibernética (CSIRP) aplicado sistemáticamente en toda su organización. Casi la mitad de los encuestados informaron que su plan de respuesta a incidentes es informal o completamente inexistente.

A pesar de esta falta de planificación formal, el 72% de las organizaciones se sienten más ciberresilientes hoy que el año pasado. Las organizaciones altamente resilientes (61%) atribuyen su confianza a su capacidad para contratar personal calificado -aunque las organizaciones necesitan tanto tecnología como personas para ser ciberresponsables. De hecho, el 60% de los encuestados considera que la falta de inversión en inteligencia artificial (IA) y el aprendizaje automático es la mayor barrera para la ciberresiliencia.

Esta confianza puede estar fuera de lugar, con el análisis que revela que el 57% de los encuestados dijo que el tiempo para resolver un incidente ha aumentado, mientras que el 65% informó que la gravedad de los ataques ha aumentado. Estas áreas representan algunos de los factores clave que afectan la resiliencia cibernética. Estos problemas se complican aún más por el hecho de que solo el 31% cuenta con un presupuesto de ciberresiliencia adecuado y dificultad para retener y contratar profesionales de seguridad de TI (77%).

"Las organizaciones pueden sentirse más ciberresilientes hoy en día y la razón principal por la cual fue contratar personal calificado", dijo Ted Julian, vicepresidente de gestión de productos y cofundador de IBM Resilient.

"Tener el personal adecuado en su lugar es fundamental, pero armarlos con las herramientas más modernas para aumentar su trabajo es igualmente importante. Un plan de respuesta que orquesta la inteligencia humana con inteligencia artificial es la única forma en que los equipos de seguridad van a adelantarse a la amenaza y mejorar la resiliencia cibernética en general".

La falta de un CSIRP constante es una tendencia persistente cada año a pesar de ser un hallazgo clave en el *Cost of a Data Breach Study* de 2017. El costo de una violación de datos fue casi \$1 millón más bajo en promedio cuando las organizaciones pudieron contener el incumplimiento en menos de treinta días, lo que resalta el valor y la importancia de tener un CSIRP fuerte.

Dirigida por el Ponemon Institute y patrocinada por IBM Resilient, *The 2018 Cyber Resilient Organization* es el tercer estudio anual de referencia sobre ciberresiliencia: la capacidad de una organización para mantener su propósito principal e integridad ante los ataques cibernéticos. La encuesta global ofrece información de más de 2.800 profesionales de seguridad y TI de todo el mundo, incluido Estados Unidos, Reino Unido, Francia, Alemania, Brasil, Asia-Pacífico, Medio Oriente y Australia.

"Un enfoque claro en algunas áreas cruciales puede marcar una gran diferencia cuando se trata de ciberresiliencia", dijo el Dr. Larry Ponemon. "Asegurar que el equipo de seguridad esté equipado con un plan de respuesta ante incidentes, personal y presupuesto adecuados llevará a una postura de seguridad más sólida y una mejor resiliencia cibernética".

[El resumen ejecutivo de estos hallazgos se puede descargar aquí.](#)

Algunos puntos clave del estudio incluyen:

- La dotación de personal para las actividades relacionadas con la ciberresiliencia es inadecuada
 - La segunda barrera más grande para la resiliencia cibernética es tener personal calificado insuficiente dedicado a la ciberseguridad.
 - El 29% de los encuestados informaron tener personal ideal para lograr la resiliencia cibernética.
 - El 50% dice que el actual CISO o líder de seguridad de su organización ha estado funcionando durante tres años o menos. 23% informa que actualmente no tiene un CISO o líder de seguridad.
 - Las organizaciones no están listas para el nuevo Reglamento General de Protección de Datos (GDPR)
 - El GDPR entrará en vigencia en mayo de 2018 y exigirá que las organizaciones tengan un plan de respuesta a incidentes.
 - El 77% de los encuestados no tiene un plan de respuesta ante incidentes que se aplica de manera consistente en toda la empresa.
 - La mayoría de los países no reportan confianza en su capacidad para cumplir con el GDPR.
-