

Estudio de IBM: Más de la mitad de las organizaciones no están preparadas ante incidentes de ciberseguridad

El uso de la automatización mejoró la detección y contención de ataques cibernéticos en casi un 25%

Sólo el 30% cree que la cantidad de personal en ciberseguridad es suficiente para desempeñar un alto nivel de resiliencia cibernética

El 62% de los encuestados dijo que tanto las áreas de privacidad como de ciberseguridad deben trabajar conjuntamente para lograr la resiliencia cibernética dentro de sus organizaciones

Ciudad de México. Abril 15, 2019 - IBM Security anunció hoy los resultados de su estudio global que explora la preparación de las organizaciones cuando se trata de resistir y recuperarse de un ataque cibernético. El estudio, realizado por el *IBM Ponemon Institute*, encontró que la gran mayoría de las organizaciones encuestadas aún no están preparadas para responder adecuadamente a los incidentes de ciberseguridad, y el 77% de los encuestados en dicho estudio mencionan no tener un plan de respuesta a incidentes de ciberseguridad aplicado de manera consistente en toda su empresa.

A pesar de que los estudios demuestran que las empresas preparadas para responder de forma rápida y eficiente ante un ciberataque ahorran más de \$1 millón de dólares en el costo total del incidente, aún existe un déficit en la planificación de respuesta a incidentes de ciberseguridad. Éstos siguen siendo constantes en los últimos cuatro años que se ha realizado el estudio. De las organizaciones encuestadas más de la mitad (54%) no ponen a prueba sus planes de seguridad de forma regular, lo que reduce su capacidad de reacción para gestionar eficazmente los complejos procesos y la coordinación que se deben tener a raíz de un ataque.

Los problemas que enfrentan los equipos de ciberseguridad al implementar un plan de respuesta frente a los ataques cibernéticos también han afectado el cumplimiento del Reglamento General de Protección de Datos (GDPR). Casi la mitad de los encuestados (46%) mencionó que su organización aún no ha acatado en su totalidad las normas de este reglamento, a casi un año de su implementación.

"No planear es un error cuando se trata de responder a un ataque de ciberseguridad. Los planes y estrategias de ciberseguridad deben someterse a pruebas exigentes con regularidad y necesitan el apoyo total de la empresa para invertir tanto en las personas, los procesos y las tecnologías necesarios para mantenerlos", dijo Ted Julian, Vicepresidente de Gestión de Productos y cofundador de *IBM Resilient*. *"Cuando la planificación adecuada se combina con las inversiones en automatización, vemos compañías capaces de ahorrar millones de dólares durante un ataque".*

Otras conclusiones del estudio arrojaron que:

La automatización sigue emergiendo

Por primera vez, el estudio de este año analizó el impacto de la automatización en la resiliencia cibernética. Automatización se refiere a habilitar tecnologías de seguridad que aumentan o reemplazan la intervención humana en la identificación y la contención de las vulnerabilidades cibernéticas. Estas tecnologías dependen de la inteligencia artificial, aprendizaje automático, análisis y orquestación.

Cuando se les preguntó si su organización aprovechaba la automatización, sólo el 23% de los encuestados dijo que era un miembro importante, mientras que el 77% mencionó que sus organizaciones sólo usan la automatización de forma moderada, insignificante o que incluso no la usan. Sin embargo, las instituciones que

usan la automatización califican su capacidad de prevenir (69% frente al 53%), detectar (76% frente al 53%), responder (68% frente al 53%) y contener (74% frente al 49%) un ataque cibernético con un alto porcentaje.

De acuerdo con el [Estudio de Costos de Violación de Datos de 2018](#), el uso de la automatización es una oportunidad perdida para fortalecer la resiliencia cibernética, ya que las organizaciones que implementaron la automatización de seguridad de forma total, ahorraron \$ 1.5 millones en el costo total en una violación de datos, en contraste con las que no aprovecharon la automatización y pagaron un costo total mucho mayor.

La brecha de especialistas en ciberseguridad sigue impactando la resiliencia

La falta de habilidades y expertos de ciberseguridad parece estar impidiendo aún más su implementación, ya que las organizaciones comentan que el poco personal especializado obstaculizó su capacidad de gestionar adecuadamente los recursos, así como sus requerimientos. Los participantes de la encuesta afirmaron que carecen de personal para mantener y probar adecuadamente sus planes de acción ante ataques a pesar de que existen de 10 a 20 vacantes en los equipos de seguridad cibernética. De hecho, sólo el 30% de los entrevistados dijo que la cantidad de personal dedicada a la ciberseguridad es suficiente como para lograr un alto nivel de protección. Además, el 75% considera que la dificultad para contratar y retener al personal calificado es moderadamente alta.

Casi la mitad de los encuestados (48%) mencionó que su organización implementa demasiadas herramientas de seguridad de forma separada, lo que al largo plazo aumenta la complejidad operativa y reduce la visibilidad en general acerca de la seguridad.

La privacidad ya es una prioridad

Las organizaciones finalmente reconocen que la colaboración entre los equipos de privacidad y ciberseguridad puede mejorar la resiliencia cibernética. El 62% de las personas del estudio cree que alinearlos es vital para lograr un mejor desempeño. La mayoría cree que el rol de la privacidad es cada vez más importante, especialmente con la aparición de nuevas regulaciones como GDPR y la Ley de Privacidad del Consumidor de California, y están priorizando la protección de datos al tomar decisiones de compra de TI.

Cuando fueron cuestionados acerca de cuál era el factor principal para justificar un gasto en seguridad cibernética, el 56% concordó en la pérdida o el robo de información. Esto es especialmente cierto ya que los consumidores exigen mejores medidas de seguridad a las empresas para proteger activamente sus datos. Según una reciente encuesta de IBM, el 78% dice que la capacidad de una empresa para mantener sus datos privados es extremadamente importante, mientras que solo el 20% confía completamente en las organizaciones con las que interactúan.

Además, el 73% afirma tener un especialista del área, lo que demuestra que la privacidad de los datos se ha convertido en una prioridad para las organizaciones.

Acerca del estudio

Realizado por el Ponemon Institute y patrocinado por IBM Resilient, "The 2019 Cyber Resilient Organization" es el cuarto estudio anual de referencia sobre Resiliencia Cibernética (la capacidad de una organización para mantener su propósito e integridad principales frente a los ataques cibernéticos). El estudio presenta información de más de 3,600 profesionales de seguridad y TI de todo el mundo, incluidos Estados Unidos, Canadá, Reino Unido, Francia, Alemania, Brasil, Australia, Oriente Medio y Asia Pacífico.

Para obtener más información sobre los resultados completos del estudio, descargue "[The 2019 Cyber Resilient Organization](#)".

