¿Qué tan maduros se consideran los CIO en temas de seguridad en la nube?

La mitad de los líderes globales de TI dicen que no tienen «plena confianza» en su capacidad para responder a datos, phishing de malware, cadena de suministro, ransomware, nube y ataques a aplicaciones e Internet de las Cosas, según una nueva encuesta global realizada por especialistas.

Adicionalmente, cuando se les preguntó acerca de sus capacidades de respuesta a ataques, menos de la mitad **(45%)** de los encuestados dijeron que pueden responder eficazmente a los incidentes, mitigar las amenazas **(43%)** o comprender la naturaleza de las amenazas a las que se enfrentan **(42%).**

La encuesta aplicada a **1,420** profesionales de TI también revela incertidumbre generalizada de que las organizaciones posean el talento y las habilidades para enfrentar los desafíos de ciberseguridad, mientras que el **86%** de los encuestados mencionó que sus organizaciones carecen de las habilidades y la experiencia necesarias para responder a una creciente variedad de amenazas.

Tendencias de TI que impulsan la complejidad cibernética.

La ubicuidad de la nube, las metodologías DevOps y la condensación de los ciclos de desarrollo, junto con otras tendencias de TI, han hecho que abordar las ciberamenazas sea una tarea cada vez más compleja. La mitad de los encuestados **(49%)** citan el crecimiento en la nube y el IoT como desafíos clave, seguidos de nuevas amenazas y métodos de ataque **(46%)** y el crecimiento en los volúmenes de datos, operaciones digitales y trabajo remoto **(45%),** que ha generado mayores oportunidades para los atacantes.

El **48%** de los encuestados dice que su capacidad para administrar la seguridad de las aplicaciones en un entorno más complejo está influenciada por nuevas formas de trabajo, incluidas DevOps y prácticas de desarrollo ágil. Otras dinámicas incluyen ciclos de lanzamiento / entrega más rápidos **(46%),** el crecimiento en arquitecturas de aplicaciones de microservicio **(46%),** entornos híbridos / multinube **(46%)** y entornos de tiempo de ejecución de contenedores **(44%).**

En sus respuestas sobre la naturaleza y los objetivos de los ciberataques que más les preocupan, los ataques a la red / plataforma **(58%)** lideran el camino, seguidos por los ataques a aplicaciones web **(52%)** y los ataques al sistema operativo de red **(51%).** La mitad **(50%)** están preocupados por las amenazas persistentes avanzadas (APT), mientras que el **47%** señalan la implicación de credenciales robadas y el **41%** están preocupados por la exposición no autorizada a datos.

Fuente de información:
https://cio.com.mx/

Puntos débiles de talento y dotación de personal.

Más de la mitad **(52%)** de los encuestados dicen que tienen dificultades para contratar y retener talentos en ciberseguridad, con las mayores brechas de habilidades en las áreas de seguridad en la nube **(33%)** y seguridad de la red **(30%),** que los encuestados también identificaron como los roles más críticos. En toda la empresa, los líderes de TI citan la falta de experiencia **(86%),** falta de recursos **(81%),** falta de tiempo **(70%)** y la falta de información de capacitación **(63%)** como los desafíos más urgentes de ciberseguridad y cumplimiento.

El acceso a la nube, los datos, las aplicaciones, la red y la identidad es manejado con mayor frecuencia por el personal interno, mientras que casi la mitad **(49%)** subcontrata la seguridad de riesgos integrados y **(43%)** asigna tareas a los socios externos para ayudar con la seguridad de la red.