La escasez de talento en ciberseguridad

Un estudio de la falta de competencias en ciberseguridad a nivel internacional

La escasez mundial de talento cualificado en ciberseguridad agrava la tarea ya difícil de proteger contra el volumen creciente de amenazas avanzadas y sofisticadas. El CSIS (del inglés, Center for Strategic and International Studies, Centro de estudios estratégicos e internacionales) ha realizado un estudio para cuantificar la escasez de profesionales especializados en ciberseguridad en ocho países (Alemania, Australia, Estados Unidos, Francia, Israel, Japón, México y Reino Unido). Se ha encuestado a los responsables de la toma de decisiones (TI), tanto del sector público como del sector privado, en relación a cuatro áreas clave del desarrollo de la plantilla en el ámbito de la ciberseguridad: gasto en seguridad, programas de formación, estrategias del empleador y políticas públicas. El estudio ofrece información de gran utilidad que puede ayudar a las empresas y a los organismos públicos a desarrollar un equipo de trabajo especializado en ciberseguridad más sólido y sostenible, y que disponga de las competencias necesarias. También incluye varias recomendaciones concretas sobre cómo solucionar el déficit actual de talento en el campo de la ciberseguridad y cómo mejorar la ciberseguridad en su conjunto.

Conclusiones principales

- Existe una escasez generalizada de profesionales especializados en ciberseguridad. Según el estudio del CSIS, el 82 % de los encuestados manifestaron sufrir falta de especialistas en ciberseguridad en sus organizaciones. La reducida oferta frente a la alta demanda de profesionales en este campo ha provocado un aumento de sus salarios. En Estados Unidos, en los puestos de trabajo de profesionales de la ciberseguridad el salario es hasta un 10 % superior al de otros empleados de TI.
- La escasez de talento aumenta la vulnerabilidad de las organizaciones frente a los ciberdelincuentes. El 71 % de los encuestados corroboran esta idea. Uno de cada cuatro declaran que efectivamente la falta de personal de ciberseguridad ha contribuido a la pérdida de datos o al robo y los daños causados a la reputación de la organización.

- Hay una gran demanda de algunas competencias. Las competencias más demandadas en los ocho países son la detección de intrusiones, el desarrollo de software seguro y la mitigación de ataques.
- La formación práctica es la mejor forma de adquirir competencias en ciberseguridad. Aunque aproximadamente el 50 % de los responsables de la toma de decisiones encuestados dan prioridad a una licenciatura en la disciplina técnica relevante en los requisitos para obtener un puesto de trabajo, la mayoría creen que la experiencia, los conocimientos sobre hacking y los certificados profesionales son mejores medios para adquirir las habilidades que se precisan en este campo.
- La tecnología puede compensar la falta de talento. Aproximadamente 9 de cada 10 encuestados afirmaron que la tecnología de seguridad podría ayudar a suplir carencias y el 55 % consideran que en un plazo de cinco años, las soluciones de seguridad serán lo bastante avanzadas para satisfacer las necesidades de sus organizaciones. Además, declararon que externalizan las funciones y procesos de seguridad que se prestan a la automatización.
- Los gobiernos no invierten lo necesario en ciberseguridad. El 76 % de los encuestados afirman que en su país la Administración no invierte lo suficiente en programas destinados a desarrollar el talento en el campo de la ciberseguridad, y creen que las leyes y normativas sobre ciberseguridad son inapropiadas.

Cuatro dimensiones de la escasez de personal especializado en ciberseguridad

Gasto en ciberseguridad

Se estima que el gasto total en ciberseguridad en el mundo será de más de 100 000 millones de dólares en los próximos cuatro a cinco años[1]. Este gasto se atribuye en su mayoría al gobierno de Estados Unidos y a la industria de servicios financieros, que son los mayores consumidores de tecnología y servicios de seguridad, y además, el principal objetivo de los delincuentes. Gracias a la fuerte inversión en ciberseguridad, estos dos sectores están mejor equipados para abordar el problema de la escasez de personal y pueden fomentar mejores prácticas en cuanto a formación y contratación.

Formación

Como señala el informe del CSIS, si bien contar con un título universitario puede ser uno de los requisitos mínimos para conseguir un puesto como experto en ciberseguridad, la mayoría de los responsables de la toma de decisiones consideran que la experiencia práctica es la mejor formación para este trabajo; solo un 23 % de los encuestados declararon que los programas de formación preparan a los estudiantes para acceder al sector. Según el estudio, Estados Unidos y el Reino Unido ocupan los primeros puestos en cuanto a inversión actual en formación sobre ciberseguridad, mientras que México, Francia y Japón están al final de la lista. Más del 25 % de los encuestados citaron los certificados profesionales como un medio eficaz para demostrar sus competencias. Y según dos de cada cinco, los conocimientos de hacking son la mejor forma de obtener competencias.

Estrategias del empleador

¿Cuáles son las estrategias de contratación principales para atraer y retener a profesionales de la ciberseguridad? El salario es la primera, seguida por la formación, la reputación del departamento de TI y las oportunidades de progresar. Casi el 50 % de los participantes en la encuesta consideran que la falta de formación o financiación para programas de certificación son motivos habituales por los que los empleados abandonan una empresa. La creación de un equipo de ciberseguridad competente lleva su tiempo, por lo que las organizaciones recurren a la tecnología para suplir las carencias. Aproximadamente 9 de cada 10 encuestados manifestaron que los avances tecnológicos en ciberseguridad podrían compensar la escasez de expertos. Además, existe la opción ampliamente

aceptada de externalizar determinadas funciones de seguridad, como la evaluación y mitigación de riesgos, la supervisión y administración del acceso a la red, y la reparación de los sistemas que han sufrido un ataque. Más del 60 % de los participantes externalizan al menos algún aspecto del trabajo de ciberseguridad.

Políticas públicas

Muchos países, como Estados Unidos, Reino Unido, Israel y Australia, están aumentando sus esfuerzos para paliar la falta de personal en el campo de la ciberseguridad. La mayoría de los países disponen también de legislación específica para mejorar la formación en ciberseguridad, sin embargo más del 75 % de los encuestados afirman que sus gobiernos no invierten lo suficiente en el desarrollo del talento en ciberseguridad, y el mismo porcentaje consideran que las leyes y normativas relativas a la ciberseguridad en sus países son insuficientes.

Recomendaciones

Redefinir los requisitos mínimos para obtener un puesto de trabajo básico en ciberseguridad y aceptar canales de formación no tradicionales

Pocas universidades y centros educativos en el mundo ofrecen la especialidad de ciberseguridad, por lo que, según indican los datos del estudio del CSIS, los responsables de contratación deben otorgar más valor a los certificados profesionales y a la experiencia práctica que a los títulos universitarios. Las universidades y otros centros educativos deben comenzar a ofrecer este tipo de formación práctica en ciberseguridad para que las personas cualificadas puedan desarrollar sus habilidades. Este tipo de programas presentan una oportunidad para los gobiernos, el sector privado y los centros educativos de colaborar con el fin de mejorar el plan de estudios y proporcionar becas y oportunidades de formación.

Diversificar el campo de la ciberseguridad

Según algunos estudios, las mujeres y las minorías tienen una presencia inferior en este campo. Además, las estrictas leyes de inmigración limitan aún más la fuente de trabajadores cualificados para empleos en el campo de la ciberseguridad. Para ampliar el personal de ciberseguridad rápidamente en Estados Unidos y en otros países con leyes de inmigración similares, bastaría con incrementar el número de permisos de trabajo e incluir a las minorías y a las mujeres. Otra barrera para incrementar la plantilla de ciberseguridad es el estigma asociado a las personas que tienen experiencia en hacking. Los empleadores deben desarrollar una actitud más flexible hacia la contratación de personas involucradas en el mundo del hacking, ya que sus conocimientos y aptitudes pueden ser extremadamente valiosos.

Ofrecer más oportunidades de formación externa

Los programas de formación continua son fundamentales para retener el talento en ciberseguridad, ya que la falta de este tipo de programas influye negativamente en las decisiones de las personas que buscan empleo. Los gobiernos y el sector privado deben colaborar para hallar la forma de mejorar las oportunidades de formación tanto para estudiantes como para empleados actuales que desean mejorar sus competencias.

Desarrollar las capacidades de automatización

La encuesta del CSIS revela que las organizaciones se plantean automatizar las funciones de ciberseguridad para remediar la deficiencia de expertos, lo que significa que los empleados de ciberseguridad se verán obligados a adaptar sus conocimientos a estos nuevos procesos. Gracias a la eficacia operativa que aporta la automatización, los profesionales podrán dedicar su tiempo y su esfuerzo a detectar, analizar y solucionar las amenazas más sofisticadas.

Recopilar datos y desarrollar mejores parámetros de evaluación
Si recopilan datos sobre el mercado de trabajo de la ciberseguridad y se estandarizan las funciones laborales, el sector privado, la Administración y los centros educativos pueden diseñar una clasificación de competencias en ciberseguridad claramente definidas y de gran valor que se aplique a todos los sectores de la industria.

Conclusión

Para garantizar una seguridad eficaz es fundamental contar con una plantilla sólida, y ahora más que nunca. La escasez mundial de profesionales de ciberseguridad se puede suplir mediante la incorporación de individuos más cualificados, para lo que se requieren mejoras en la educación, una mayor diversidad de empleados, la adopción de tecnologías de seguridad y la recopilación de datos.

Visite **mcafee.com/skillsshortage** para leer el informe completo.

1. http://www.forbes.com/sites/stevemorgan/2016/02/12/cybersecurity-market-outlook-for-2016-to-2020/#185c567a74a4

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com