Publicado en Madrid el 10/04/2018

Hacker ético, CISO, CSO o DPO, expertos en ciberseguridad más demandados en 2018, según The Valley Talent

The Valley Talent, headhunter especialista en la búsqueda de talento digital, explica el procedimiento a seguir desde el departamento de RRHH para integrar un plan en la empresa que minimice los riesgos y el impacto de cualquier incidente de seguridad

El último Informe de Riesgos del Foro Económico Mundial situó los ciberataques y el robo y fraude de datos como dos de los cinco principales riesgos en términos de probabilidad. Según dicho documento, el coste del cibercrimen en los próximos cinco años para las empresas podría alcanzar los 8 billones de dólares.

Ahora mismo, cualquier entidad que tenga presencia online, genere información en su actividad de negocio o cuyos sistemas estén alojados en la nube está expuesta. Por suerte, las organizaciones empiezan a ser conscientes de la necesidad de elaborar un plan que minimice los riesgos y el impacto de cualquier incidente de seguridad. La enorme transcendencia de sucesos como el ocurrido el año pasado con el macro ataque del ransomware 'Wannacry' ha hecho saltar las alarmas.

Tal y como indica Miriam López, CEO de The Valley Talent, los perfiles de ciberseguridad están tomando un papel fundamental en las organizaciones y desde la dirección de las compañías están apoyando la creación de estos equipos. Respecto a los perfiles más idóneos a contratar, hay diferentes tipos de profesionales encargados de gestionar este tema. Algunos de los más demandados son:

CISO (Chief Information Security Officer). Es el encargado de alinear estrategia de ciberseguridad con los objetivos de la empresa. Se encargará de establecer las políticas de seguridad de la entidad en función de la actividad de la misma y de establecer las medidas y controles necesarios.

CSO (Chief Security Officer). Es el responsable ejecutivo de la seguridad interna de la organización. En sus manos está establecer los planes de continuidad, tener una visión completa del negocio, estar al tanto de la normativa, conocer los posibles riesgos en ciberseguridad, etc.

DPO (data protection officer). Tiene un perfil jurídico y de cumplimiento normativo (compliance) y, según la nueva normativa europea de Protección de Datos, será exigible en la Administración y en determinadas empresas privadas.

Analistas de seguridad. Es el encargado de detectar cualquier posible vulnerabilidad técnica en los sistemas informáticos y redes de la compañía.

Arquitectos de seguridad. Es el responsable de diseñar la arquitectura de ciberseguridad previa con el fin de asegurar todos los desarrollos que se realicen en el entorno.

Hackers éticos. Muy al día en las técnicas que utilizan los ciberdelincuentes, su labor se basa en poner a prueba los sistemas de seguridad de las empresas para analizar sus peligros y así ponerles remedio.

Especialistas forenses. Es el especialista en realizar análisis detallados postmortem de sistemas y redes tras un incidente de seguridad o ciberataque.

Especialista en incidencias. Es el responsable de coordinar las actividades en caso de incidencias de seguridad y, como “orquestador”, activará el plan de control para que los equipos trabajen alineados y las incidencias tengan el menor impacto posible.

Responsables de inteligencia. Serán los expertos en conocer cualquier amenaza en el exterior, velarán por la reputación de la compañía de cara a identificar cualquier posible “intruso” y analizarán el nivel de amenazas del exterior.

Respecto a las capacidades que deben tener, aunque las aptitudes variarán, en general se requiere que tengan gran capacidad analítica, sean transversales y que sepan trabajar bajo presión. A nivel técnico, deberán formular planes para salvaguardar archivos informáticos, tener soltura en el manejo de diferentes sistemas operativos, redes y lenguajes de programación, implementar protocolos criptográficos y herramientas de seguridad, analizar y detectar amenazas y desarrollar técnicas para prevenirlos, conocer la normativa vigente, controlar el análisis de malware etc.

A la hora de ubicar estos perfiles en la organización, dependiendo del tamaño de la empresa, estos profesionales se integrarán de forma diferente. Si se contratan de manera interna, estos suelen ubicarse en los departamentos de IT, de Seguridad, de Sistemas y Ciberseguridad, de I+D, etc. No obstante, siempre deberán estar adjuntos al área de dirección y contar con un enfoque generalizado que tenga en cuenta al resto de departamentos de la organización.

No obstante, no hay que olvidar que la formación interna también es importante. La mayoría de las brechas de seguridad se producen por el incumplimiento de los protocolos por parte de la plantilla. Para ello, será preciso poner su disposición ciertas nociones que protejan la seguridad de la empresa: confirmar la identidad de todo aquel que solicite información, contraseñas a buen recaudo, evitar guardar información sensible de la empresa en el disco duro, no instalar programas de fuentes desconocidas, actualizar el antivirus en los ordenadores etc.

También está muy asentada la opción de contratar una póliza de ciberseguros. Muchas aseguradoras incluyen en su oferta seguros ciberriesgo como solución frente a posibles amenazas. Suelen cubrir tanto los daños de la empresa como los perjuicios económicos que puedan causar a terceros o a los propios empleados. Eso sí, para su contratación, se exige que ya exista cierto nivel de seguridad.

Datos de contacto:
Redacción

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional E-Commerce Ciberseguridad Recursos humanos