El experto en ciberseguridad, Adolfo Hernández, explica el panorama actual del sector

El déficit de talento en ciberseguridad incrementa los riesgos digitales de las empresas

- **Contar con capital humano cualificado es imprescindible para potenciar el sector de la ciberseguridad. Se prevé que para el 2022 serán necesarios en Europa 350.000 perfiles de experto en ciberseguridad.**
- **El especialista en ciberseguridad puede venir de diferentes disciplinas académicas; no necesariamente son ingenieros o expertos en sistemas.**
- **Cuidar de la ciberseguridad se ha convertido en un factor clave que dota de confianza y buena reputación a las empresas.**

Madrid, 27 de febrero de 2019. Solo en el año 2017, el CNN-CERT (Centro de Respuesta a Incidentes del Centro Criptológico Nacional del CNI) gestionó un total de 26.500 ciber incidentes, lo que ha supuesto un 26,55% más que en 2016. Este dato de crecimiento refleja la delicada situación en la que se encuentran las empresas y, sobre todo, la presión que tienen los profesionales a la hora de proteger a las entidades tanto públicas como privadas de este tipo de amenazas online.

Los costes de la ciberseguridad para las empresas han aumentado de forma exponencial. El auge del "cibercrimen como servicio" (*cybercrime-as-a-service*) y la popularización de herramientas y servicios de *hacking* antes accesible a unos pocos, han desdibujado el perfil del cibercriminal clásico, haciendo que prácticamente cualquier persona pueda acceder a ellos atraído por el reclamo del beneficio económico y facilidad de los ciberataques. Además, a esta situación se le suma la deficiencia de candidatos cualificados en seguridad TI, que hace que las empresas estén expuestas a más riesgos pues su capacidad de control y respuesta es limitada.

The Valley Talent, *headhunter* experto en talento del ámbito digital y tecnológico de nivel senior y directivo, especializado, entre otros, en el sector de la ciberseguridad, ha celebrado un desayuno temático sobre la seguridad de la web. El encuentro ha sido liderado por **Adolfo Hernández,** subdirector y cofounder de ***THIBER***, *the cibersecurity think tank*, centro de investigación especializado en la protección del ciberespacio. Durante el mismo, se analizó el tema de "**Cómo gestionar riesgos digitales corporativos para aprovechar las ventajas de la economía digital**". Las conclusiones de esta conversación han arrojado algo de luz sobre las principales tendencias y los retos que rigen el sector de la ciberseguridad en la actualidad:

- **La identificación, atracción y retención de talento será clave**

Uno de los principales retos de las empresas para poder abarcar las amenazas de ciberseguridad es ser capaces de identificar, atraer y retener al talento profesional. Según Adolfo Hernández, España es una potencia de talento especializado en esta área y se ha convertido en un *offshoring* de ciberseguridad; como así lo demuestra la creación de diversos *hubs* y centros de referencia y

excelencia en ciberseguridad de diversas multinacionales, así como la existencia de un tejido empresarial creciente regional que ofrece servicios de calidad a precios competitivos.

Según un estudio de ISC2 (Consorcio internacional de Certificación de Seguridad de Sistemas de Información), para el 2022 serán necesarios en Europa 350.000 puestos de trabajo para profesionales ciber, a pesar del hecho de que la extensa experiencia técnica no es un prerrequisito indispensable para entrar en el sector. De hecho, no todos los perfiles de ciberseguridad tienen que ser ingenieros; también son necesarias otras figuras como politólogos y criminólogos que ayuden a entender la motivación, el modelo económico y los perfiles tras los ciberataques.

- **El cibercrimen y la confianza**

El cibercrimen supone no solo la mayor vertiente criminal en crecimiento interanual, sino que, además, se ha convertido en un problema de confianza en el mercado digital, explica Adolfo Hernández. La ciberseguridad se ha transformado en un factor imprescindible para medir la confianza de una entidad. Por este motivo, Moody's está ya estudiando cómo incluir en el futuro el nivel de peligro que ostenta una entidad en ciberseguridad en las calificaciones de crédito empresarial. En este sentido, es importante tener en cuenta que un ciberataque va más allá de ser un problema económico, y se puede convertir en un problema reputacional grave para el afectado.

- **La hiperconectividad como obstáculo de la ciberseguridad**

Entre las características del ciberespacio que representan un mayor obstáculo para la ciberseguridad, destaca la hiperconectividad. Actualmente, el Internet de las cosas hace que un ciberataque no afecte solo a un dispositivo, sino que pueda tener repercusión en móviles, Smart TV, vehículos conectados, cámaras de seguridad y muchos otros.

En 2019, la población digital ha ascendido a más de 7.000 millones de usuarios, de los cuales más de 3.200 millones son usuarios activos de Internet, y además, existen millones de objetos conectados a través del Internet de las coas (IoT). Estos datos son una prueba de que lo que hace la hiperconectividad es ampliar cada vez más nuestra superficie conectada, y a mayor conexión, mayor exposición ante riesgos.

- **Existe una clara simetría entre los que protegen y los que atacan**

La relación entre el profesional de ciberseguridad y el ciber atacante es claramente asimétrica, según explica Adolfo Hernández. El encargado de proteger a una empresa de amenazas se encuentra en su día a día con diversas tareas que van más allá del objetivo de defenderse ante todos los ataques posibles, entre las que se mencionan lidiar con departamentos de auditoría, trabajar con presupuestos limitados, falta de sensibilización corporativa, escasez de talento especializado, tareas de cumplimiento normativo y otras. Mientras que, por otro lado, el perfil atacante solo debe encontrar una vulnerabilidad para atacar y ser efectivo. Esto es la asimetría; y por eso, **The Valley Talent** considera fundamental que las empresas tengan la capacidad de identificar al talento cualificado e integrarle en sus estructuras corporativas, para así poder tener un mayor margen de respuesta ante ciberataques.

Aquellos que cuenten con los mejores recursos tecnológicos y humanos desarrollarán cibercapacidades para afrontar con garantías el reto digital. Y es que, aunque el ciberespacio ha

desdibujado los esquemas establecidos, el reto sigue siendo conseguir que el cibercrimen no sea rentable y que la ciberseguridad sea un trabajo menos asimétrico.

Acerca de The Valley Talent

THE VALLEY TALENT es un *headhunter* especialista en la búsqueda de talento del ámbito tecnológico y digital, en perfiles directivos e intermedios para liderar la constante evolución digital a la que se enfrentan las organizaciones. Son un grupo de profesionales con más de 10 años de experiencia en la búsqueda de talento y con la capacidad de dar una respuesta eficaz y rápida a las necesidades de incorporación de nuevas capacidades, derivadas de la economía digital, independientemente del sector o tamaño de tu organización. Entre ellas, destaca la ciberseguridad, uno de los campos que más está creciendo en términos de atracción de talento y cuya demanda de perfiles se encuentra al alza.

www.thevalleytalent.es

Acerca de The Valley

THE VALLEY es un ecosistema digital donde se une formación, talento y emprendimiento a través de la actividad de la escuela, THE VALLEY DIGITAL BUSINESS SCHOOL, el coworking para startups digitales y THE VALLEY TALENT, un headhunter especializado en perfiles digitales. Con sede en Madrid, Barcelona y Canarias, el objetivo es fomentar las sinergias y el networking entre profesores, alumnos y emprendedores con el fin de generar proyectos innovadores de éxito para el sector digital. **www.thevalley.es**

Para más información:

Trescom Comunicación:
Sara Gonzalo / Alba Tortosa / Jennifer Rocha
91 411 58 68 / 615 18 41 66
sara.gonzalo@trescom.es, alba.tortosa@trescom.es, jennifer.rocha@trescom.es