Publicado en Madrid el 30/11/2023

4 factores han provocado el aumento de la concienciación sobre la importancia de la ciberseguridad

The Valley ha organizado la jornada "Explore Ciberseguridad" donde distintos expertos han analizado cuáles son los principales retos en ciberseguridad a los que se enfrentan las empresas hoy en día

El creciente número de ciberataques y ciberamenazas ha propiciado la necesidad de que las empresas adopten medidas para protegerse en un mundo cada vez más conectado digitalmente y han puesto en relieve la importancia de invertir en formación y concienciación de los empleados. En este sentido, la ciberseguridad está cobrando un papel protagonista. En España, este sector ya cuenta con 1.600 empresas y se espera que alcance los 83.000 empleos en 2024.

La necesidad de proteger los datos, infraestructuras críticas y sistemas vitales se ha vuelto imperativa en el mundo digital actual. La mitad de las empresas españolas sufrieron ataques de ciberseguridad el pasado ejercicio, una situación que empeora cada año y que supone un alto impacto económico para las compañías afectadas. En este sentido, la resiliencia empresarial es crucial en un entorno donde las ciberamenazas son cada vez más sofisticadas y frecuentes.

En un mundo cada vez más conectado digitalmente y a medida que evolucionan las amenazas cibernéticas y la interconexión global, la ciberseguridad se ha posicionado como un elemento esencial de cualquier empresa para mantener la estabilidad, la confianza y la integridad. Y es que, el auge de la inteligencia artificial (IA) ha generado un aumento de los desafíos en ciberseguridad, ya que esta tecnología proporciona nuevos vectores de ataques emergentes, haciéndolos más sofisticados y difíciles de detectar. Por lo tanto, se necesita un enfoque integral que combine esta tecnología con otras estrategias de seguridad para garantizar una protección efectiva contra las amenazas cibernéticas en constante evolución.

En España, el sector de la ciberseguridad aglutina ya a 1.600 empresas y se espera que alcance los 83.000 empleos el próximo año, situando al país en la cuarta posición del ranking mundial de ciberseguridad, según datos del Gobierno. Asimismo, el Instituto Nacional de Ciberseguridad (INCIBE) señala que este sector es el que menor tasa de desempleo tiene en España y, se estima que, para 2024, se necesitarán 80.000 profesionales de ciberseguridad.

Dada la creciente importancia que está cobrando la ciberseguridad a nivel mundial, los expertos de The Valley han identificado 4 factores clave que han generado esta situación:

Aumento de la conectividad. El internet de las cosas (IoT) ha aumentado exponencialmente el número de dispositivos conectados, ampliando la superficie de ataque. Además, la sociedad actual depende

enormemente de la tecnología digital para trabajar, comunicarse, hacer transacciones financieras y más, lo que incrementa la sensibilidad a posibles ciberataques.

Desarrollo acelerado de tecnologías emergentes. La rápida adopción de nuevas tecnologías como la inteligencia artificial, el blockchain y la computación en la nube también genera preocupaciones sobre su seguridad. Además, este avance tecnológico ha supuesto el incremento en la sofisticación de los ataques, como el ransomware y las amenazas basadas en inteligencia artificial, ha creado mayores riesgos y vulnerabilidades.

Mayor concienciación sobre su impacto económico y social. Los ciberataques pueden tener consecuencias económicas significativas para empresas y particulares. Además, las brechas de seguridad pueden afectar la confianza del cliente y la reputación de las empresas.

Incremento de la preocupación de la privacidad de los datos. Las brechas de seguridad y los ataques cibernéticos frecuentes han generado una mayor conciencia pública sobre la importancia de la seguridad digital. La recopilación masiva de datos y su almacenamiento digitalizado aumentan la preocupación por la privacidad y la seguridad de estos datos. Ante este panorama, los gobiernos y las entidades reguladoras están implementando normativas más estrictas para garantizar la seguridad de los datos y la protección de la privacidad.

Jornada "Explore Ciberseguridad"

Para analizar la ciber resiliencia de las empresas y el panorama de las ciberamenazas, en The Place, el espacio de innovación de The Valley, se ha celebrado la jornada "Explore Ciberseguridad". La jornada ha contado con la participación de Victor Deutsch, Former Telefónica. Profesor y consultor de ciberseguridad y autor de «Ciberseguridad para directivos», y Eduardo Brenes, Territory Manager SonicWall Iberia y Advisory Board Member en Cisoverso.

La capacidad de las empresas de hacer frente a las ciberamenazas no solo supone una protección para sí mismas, sino que también contribuye al panorama internacional de la ciberseguridad, promoviendo estándares más altos y generando confianza en el ecosistema digital a nivel global. Por eso, y teniendo en cuenta el panorama actual, es esencial que las empresas inviertan en programas de formación y concienciación en ciberseguridad para educar a sus empleados sobre las mejores prácticas de seguridad, promoviendo una cultura empresarial centrada en la protección de datos y la prevención de amenazas cibernéticas. Esta concienciación debe ser continua y adaptarse a medida que evolucionan las tácticas de los ciberdelincuentes. Además, aunque los responsables tienen un papel prioritario ante un ataque, todos los equipos tienen que involucrarse en dar seguridad a la compañía.

"Seguir concienciando a los usuarios en materia de ciberseguridad es una de las principales medidas de protección ante los ciberataques. Crear campañas de concienciación y fomentar las formaciones en seguridad y privacidad es un punto fundamental en cualquier compañía. Además, es importante ser capaces de identificar a los usuarios y verificar la integridad del equipo, con el objetivo de asegurar que la persona que está detrás de Internet no es un robot. En este sentido, cada vez cobra más importancia la autenticación multifactorial (MFA) que combina contraseñas y token de seguridad y verificación biométrica.", así como ha destacado Victor Deutsch.

Por su parte, Eduardo Brenes, ha afirmado que "aunque existen muchos tipos de amenazas o riesgos en Internet y se van modificando con los años, el 95% de los casos de ciberseguridad se da por un factor humano, algo que se vuelve todavía más importante con la IA. En este sentido, el 135% de los

ataques emplea un lenguaje novedoso y el 75% aplica IAG en el trabajo lo que dificulta detectar que es real y que no. De esta forma, teniendo en cuenta que la gran mayoría de los incidentes de seguridad son provocados por insiders (personas dentro de la organización que provocan un ataque por intencionalidad o negligencia), la mejor forma de reducir los incidentes de seguridad y crear una organización resiliente es minimizar la exposición de la organización los riesgos y, para ello, la concienciación y la gestión de crisis son los dos pilares más importantes".

Datos de contacto:
Redacción
Comunicación
609601048

Nota de prensa publicada en: Madrid

Categorías: Nacional Inteligencia Artificial y Robótica Eventos Ciberseguridad Recursos humanos

NotasdePrensa
https://www.notasdeprensa.es