Publicado en Madrid el 01/02/2023

Privacidad de la información y ciberseguridad: los dos grandes desafíos de las empresas para el 2023, según IMMUNE Institute Technology

Proteger la integridad y la seguridad de los datos se ha convertido en un reto que hay que asumir con la misma velocidad con la que la tecnología avanza. El volumen de incidentes de ciberseguridad está aumentando cada vez más en todo el mundo, pero todavía existen conceptos erróneos en torno a ella. Para afrontar los riesgos, la regulación de protección de datos personales y sobre ciberseguridad deben ser elementos esenciales e inseparables dentro del ámbito empresarial

En 2021 se neutralizaron más de 10.000 ciberataques sobre servicios esenciales en España, según datos del Ministerio del Interior. Asimismo, uno de cada seis delitos se comete ya en el ciberespacio, lo que convierte la ciberseguridad y la protección legal de la privacidad de los datos en uno de los principales retos del 2023. Pensar en la seguridad de los servicios digitales y de los datos, y establecer un sistema de ciberseguridad defensa fuerte e integrado con las actividades del negocio es la clave para afrontar el desafío que supone proteger la organización ante las ciberamenazas.

La tecnología no ha parado de crecer hasta asumir un papel esencial en el contexto social actual. Internet se ha convertido en el sitio donde todo un mundo vuelca su información, tanto a nivel laboral como personal: desde las transacciones bancarias hasta los viajes. Esto provoca que la privacidad de los datos se diluya, por lo que garantizar la integridad y la seguridad de los mismos se ha convertido en un reto que asumir con la misma velocidad con la que la tecnología avanza. Son muchas las organizaciones y empresas de todo el mundo que ya están invirtiendo en tecnología relacionada con la ciberseguridad para proteger su capital intelectual.

"Las medidas de ciberseguridad están diseñadas para combatir las amenazas que se originan tanto desde dentro como desde fuera de una organización en cuestión. La información se multiplica rápidamente, y los sistemas que los procesan, por lo que existen infinidad de amenazas: robos de activos financieros, bloqueo de los sistemas, suplantación de identidad, etc. Estas no sólo son causadas por los mismos usuarios de la red, sino que también pueden estar provocadas por errores de programación, fallos electrónicos o incluso catástrofes naturales", explica Miguel Rego, director del área de ciberseguridad de IMMUNE Institute Technology.

En este sentido, los expertos en ciberseguridad se han convertido en uno de los roles fundamentales dentro de las empresas de todos los sectores. En IMMUNE Technology Institute, la escuela de referencia en tecnología en España, explican la importancia de formar a los expertos en ciberseguridad siendo conscientes de que la protección de la información es algo esencial para todas las personas. Asimismo, aseguran, es importante tener en cuenta la falsedad de los mitos en torno a la ciberseguridad y su papel. El volumen de incidentes de ciberseguridad está aumentando cada vez más en todo el mundo, pero todavía existen conceptos erróneos en torno a ella, incluida la idea de que:

Los ciberataques vienen de personas externas. Los atacantes pueden ser tanto externos como internos, y pueden formar parte de grupos organizados, incluso de formaciones apoyadas por gobiernos e instituciones relevantes.

Los riesgos están controlados. Pensar que los posibles ciberataques son conocidos sólo aumenta el peligro de sufrir uno. La realidad es que el riesgo es cada vez mayor y puede venir de negligencias o errores humanos que no tengan como objetivo poner en peligro la privacidad de los datos.

Un software antivirus básico es suficiente para proteger la empresa. Contar con un buen antivirus es importante, pero en la actualidad se necesitan herramientas específicas dedicadas a luchar contra amenazas concretas en la red.

Es suficiente con asegurar el sistema y los dispositivos de la empresa. Uno de los grandes mitos de la ciberseguridad es creer que se debe asegurar sólo la infraestructura de la empresa (ordenadores, servidores internos, dispositivos de red etc.), descuidando la protección de dispositivos móviles que se conectan a redes externas vulnerables, como las propias redes domésticas de los empleados o algunas redes públicas inseguras. Esto es un error, ya que los ciberdelincuentes son plenamente conscientes de que es mucho más fácil extraer información de un empleado de baja jerarquía que de un gran directivo.

'Mi sector es seguro'. Todos los sectores cuentan con una gran información de datos subidos a internet, lo que hace que todos sean vulnerables a sufrir un posible ciberataque. Además, los ciberdelincuentes están explotando cada vez más las necesidades de las redes de comunicación que existen en casi todas las organizaciones, sean públicas o privadas.

En palabras de Miguel Rego, director del área de ciberseguridad de IMMUNE Institute Technology, "un ciberataque individual puede provocar la pérdida de datos importantes para esa persona, pero lo realmente preocupante es lo que puede provocar a nivel colectivo, ya que las infraestructuras sociales, las instituciones, e incluso los centros de salud o las empresas de servicios financieros son objetivos claros de estos ataques, y su defensa es fundamental para el correcto funcionamiento de la sociedad".

Datos de contacto:
Cristina Moreira
914115868

Nota de prensa publicada en: Madrid

Categorías: Nacional Software Ciberseguridad Servicios Técnicos

NotasdePrensa
https://www.notasdeprensa.es