

El cifrado o encriptación, un paso más en seguridad informática

Medidas sofisticadas de seguridad informática como el cifrado empiezan a utilizarse en muchas empresas para enfrentarse a los ataques cibernéticos. Hasta ahora la seguridad informática de una empresa podía cubrirse con medidas básicas como antivirus y firewalls, y la adopción de prácticas seguras.

Sin embargo, los métodos seguidos por los piratas informáticos han avanzado, y las medidas para repeler sus ataques deben hacerlo al mismo ritmo. Más aún si se tiene en cuenta que las puertas de entrada se han multiplicado al mismo ritmo que el desarrollo tecnológico. Deben protegerse redes, servidores y lo que es más complicado, todos los dispositivos conectados a la red y a su vez a internet. Este último detalle amplía exponencialmente los peligros con el Internet de las cosas, que dota de conexión a casi cualquier objeto de uso en la empresa.

Algunas cifras

Desde 2011 hasta 2014 **se han incrementado los delitos informáticos en un 210%**, y en el pasado ejercicio se tramitaron más de 20.000 procedimientos judiciales por este motivo en España, según la Fiscalía de Criminalidad informática. Esto da una ligera idea del volumen de ataques informáticos a los que se enfrentan a diario particulares y empresas.

Pero eso no es todo. En 2015, el Instituto Nacional de Ciberseguridad interceptó hasta 63 ataques cibernéticos dirigidos a controlar o paralizar infraestructuras esenciales como el sistema energético, el financiero o los transportes. Este dato da pistas sobre el alcance que pueden llegar a tener dichos ataques y su capacidad para saltar barreras hasta en las organizaciones más fuertemente blindadas.

Cifrarlo todo

Una de las soluciones que aporta la tecnología a esta problemática es el cifrado, un sistema mediante el que se aplican algoritmos de codificación a la información sensible para hacerla incomprensible sin la clave para descifrarla. Estos algoritmos pueden aplicarse a:

- **Datos:** puede aplicarse a la comunicación entre personas, como los emails, pero también al almacenamiento de datos, como servidores o dispositivos, y al acceso al software. Además de cifrar los accesos, comunicaciones y datos, conviene realizar copias de seguridad, asimismo cifradas.
- **Accesos wifi:** además de los accesos directos por conexión por red, es fundamental cifrar las redes wifi y los accesos a la misma.
- **Medios de pago:** en sectores como el retail, es importante reforzar la seguridad en todos los dispositivos, también los medios de pago, particularmente si se acepta pago por móvil. El ecommerce es un sector especialmente sensible a los ataques, y además basa su

servicio en la fiabilidad. Por lo tanto, es crucial que las webs y apps de ecommerce cuenten con sistemas de cifrado que refuerce la seguridad en las operaciones que se realicen a través de ellas.

Finalmente, la tecnología en sí misma no es suficiente. Además de reforzar su seguridad, es fundamental formar y concienciar a quienes la utilizan para que sigan una serie de hábitos que complementen estas medidas. El cifrado es un paso clave para reforzar la seguridad, pero no será suficiente sin la actitud y la intervención humana.