Por qué tu empresa debe contar con un servicio de ciberseguridad

El robo de datos a empresas es una **peligrosa tendencia al alza**. Así se desprende del informe 2018 DNS Threat que, entre otras cifras preocupantes, destaca que nada menos que **el 39% de las empresas europeas han sufrido la sustracción de información importante** y que cada ataque ha costado de media unos 734.000 euros. En España, el caso es más preocupante si cabe **porque el 48% de empresas nacionales han confirmado caídas en sus páginas webs**, en gran parte debidas a ataques que exponen la vulnerabilidad de sus sistemas.

No es nada extraño que la ciberseguridad sea, por ello, un campo de trabajo en auge. Cada vez son más las empresas que para proteger sus datos **acuden a asesorías expertas** en las que confiar la salvaguarda de su presencia online. Una de las más punteras del sector, **Dolbuck**, realiza todo tipo de acciones para comprobar primero el estado de la seguridad de la empresa y, posteriormente, llevar a cabo las acciones necesarias para **protegerla de los hackers**.

Son numerosos los ejemplos de robos de datos. El más reciente ha sido este 7 de

septiembre. La compañía aérea British Airways **ha sufrido el robo masivo en línea** de los datos que podría concernir a unas 380.000 tarjetas de crédito, a causa de un fallo informático.

Estos fallos **pueden prevenirse**. En primer lugar, las auditorías previas establecen el estado actual de la seguridad de la empresa. Una vez detectados las posibles vulnerabilidades se confecciona un **plan director de ciberseguridad** personalizado. También se ofrece **apoyo** en todos los ámbitos de la seguridad online: arquitectura de sistemas y virtualización, auditorías de redes, auditorías perimetrales, auditorías de páginas webs, hacking ético y pentesting.

Pero para cerciorarse, **nada mejor que simular ataques** para poner al sistema a prueba. Una vez montada una estructura robusta el servicio no se queda ahí. También **se forma** al departamento IT de la empresa y se les **brinda ayuda** para implantar herramientas de gestión.

Con los cambios recientes en el **Reglamento General de Proteccion de Datos**, ponerse al día es necesario. El asesoramiento en este asunto, aparte de la implantación del **Esquema Nacional de Seguridad ISO 27001** es clave y también es un servicio disponible.

¿Pero qué ocurre si he sufrido un ataque? La asesoría también cuenta con investigaciones digitales, **informática forense** e incluso acompaña a la empresa a los juicios como peritos informáticos si fuera necesario.