Me han atacado, y ahora ¿qué?

Pautas para sobreponerse al robo de datos

Diego Rodríguez Gutiérrez

A primeros de agosto se destaparon los delitos cometidos por una red criminal rusa en Internet. Se trata, según los expertos, del mayor robo de contraseñas producido jamás

Mucho se ha hablado en los días sucesivos sobre cómo velar por la seguridad de la información en las organizaciones pero, ¿qué hacer cuando el ataque ya se ha producido?

El blog Infoworld.com, dedicado a la tecnología de las empresas, detalla una serie de pautas a seguir cuando el daño ya está hecho. La manera de reaccionar de cualquier organismo tras la catástrofe puede hacer que se hunda aún más o por el contrario le puede permitir salir reforzado ante sus clientes, socios o incluso ante sus competidores.

Difundirlo más pronto que tarde

Algunas organizaciones tratan de resistirse a que la pérdida de datos se haga pública y lo esconden el mayor tiempo posible. Sin embargo, en la mayoría de los casos todo acaba saliendo a la luz y cuando la prensa o el medio que sea se hace eco de que la entidad ha ocultado información no suele dejarla bien parada ante la opinión pública. El gigante de las subastas *eBay* guardó silencio durante meses aunque eran conscientes de la existencia de una importante violación de datos en la gestión de las cuentas de sus empleados y ahora tiene incómodos pleitos pendientes. Por el contrario, *Spotify* se ganó los elogios de los expertos y reforzó la confianza de sus clientes cuando emitió un anuncio público para dar a conocer una pequeña incidencia de seguridad con una aplicación móvil.

Decir toda la verdad y nada más que la verdad

En la línea del anterior consejo, se trata de difundir el hecho, pero también darle la importancia que tiene, ni más ni menos. El ladrón siempre es muy astuto y si se da constancia de un fallo sin darle la suficiente relevancia, la amenaza de robo aumentará aún más.

No olvidar ningún canal de comunicación

Parece claro que lo correcto es difundir el ataque. Pero hay que asegurarse también de que todos los interesados se enteren. Para ello las organizaciones deben utilizar todos sus medios habituales para comunicarse con sus clientes, proveedores y socios (webs, redes sociales, etc.). Otro palo para *eBay*: cuando por fin reconoce

su error, se limita a hacer un comunicado de prensa, no actualiza la información en su web y tarda semanas en notificarlo, mediante email, a sus propios usuarios.

Los clientes son más importantes que la bolsa

Una práctica común de algunas empresas tras un desastre de pérdida de información es centrarse en calmar a los inversores. Parece que solo es importante el valor de las acciones cuando la tranquilidad de los clientes será el aspecto que mantenga el crédito del organismo. Una buena medida contraria a esta postura podría ser por ejemplo garantizar una recompensa económica por los posibles daños ocasionados a los afectados.

Interpretar objetivamente el robo

Hay empresas que tratan de argumentar su pasividad, ante errores de seguridad en el acceso a su información, mediante la falta de constancia del uso de sus datos fuera de su organización. Es un error evidente: un coche robado no es menos robado por el hecho de que no se vea circular.

No escatimar a la hora de dar detalles "sangrientos"

Hacer una descripción pormenorizada de lo sucedido no es hacer más leña del árbol caído porque puede, además de acreditar que no se esconde nada, analizar todos los hechos paso a paso para poder evaluar las estrategias seguidas y corregirlas si fuera necesario para posibles futuras ocasiones.

Mirar hacia adelante y no hacia atrás

Los hechos pasados no pueden rectificarse pero los futuros sí. Conviene presentarse ante los clientes como una entidad que aprende de sus errores. Se trata de dar a conocer nuevas estrategias de seguridad capaces de hacer pensar que no se volverán a producir ataques.

Mueva algunos muebles

Puede ser positivo que esa renovación de cara al futuro sea profunda en cuanto a cambiar las cosas de sitio. Los usuarios suelen ver con buenos ojos que la distribución de las plataformas de los servicios que reciben cambie si es por motivos de seguridad.■