LEGÁLITAS

COMUNICACIÓN DE CRISIS DESPUÉS DE SUFRIR UN CIBERATAQUE

Si desgraciadamente hemos sufrido un ciberataque debemos reaccionar cuanto antes. En primer lugar habrá que **identificar el grado de afectación**: si se han visto dañados nuestros equipos, si hemos dañado los de nuestros clientes, si hemos puesto en peligro sus datos personales o si la actividad comercial se ha visto afectada. Debemos saber todo lo que ha pasado y contárselo, si fuera necesario, a nuestros clientes o a la opinión pública. Nuestra imagen está en juego y debemos **reducir el impacto negativo** que se pueda generar

1 ¿POR DÓNDE EMPEZAR?

Lo primero que debemos hacer es **analizar y evaluar el alcance del ataque**: ¿nos ha afectado solo a nosotros o también se ha extendido entre nuestros clientes? ¿Les hemos infectado sin querer con algún software malicioso? ¿El ataque nos permite trabajar normalmente o tendremos que parar y dejar de prestar servicio a nuestros clientes?

2 MEDICIÓN DEL ALCANCE. ¿A QUIÉN HA AFECTADO EL ATAQUE?

Solo a nosotros

NIVEL 1

Solo nos ha afectado a nosotros. No hemos perjudicado a terceros y, en un breve espacio de tiempo, podremos reanudar nuestra actividad normalmente. Dentro de lo malo hemos tenido suerte.
Solución: centrémonos en poner remedio a nuestro problema y continuar con el trabajo.

NIVEL 2

Solo nos ha afectado a nosotros, pero nos impide seguir prestando servicio en condiciones óptimas o hay riesgo elevado de que así suceda.
Solución: comunicar a clientes y proveedores lo sucedido y apelar a su comprensión.

Hemos perjudicado a terceros o podemos hacerlo si no reaccionamos

NIVEL 3

Existe un alto riesgo de infectar y trasladar nuestro problema a clientes o proveedores. Por ejemplo, les hemos enviado por email un virus que podría contagiarles.
Solución: informar de la situación y alertar sobre esta posibilidad.

NIVEL 4

¡Nos ha afectado a todos! El ataque ha provocado la paralización de nuestra compañía y de la actividad de nuestros clientes.
Solución: Apagar y aislar los equipos infectados. Informar de la situación y alertar sobre esta posibilidad.

LEGÁLITAS

El Ciberataque se ha hecho público en Redes Sociales o medios de comunicación

NIVEL 5

La noticia ha trascendido y la opinión pública ha comenzado a hablar del hecho.

SOLUCIÓN

Informar de la situación y alertar sobre esta posibilidad, contactando simultáneamente con clientes/proveedores (mediante el modelo del NIVEL que corresponda) y, si procede, los medios de comunicación o redes donde se haya recogido la noticia.

Vías de comunicación:

PARA CLIENTES Y PROVEEDORES

- Email. Dirigido a todos los clientes.
- Teléfono. Es más directo y rápido. Si el envío de mail genera problemas, será mejor utilizar esta vía, o las dos.
- SMS o WhatsApp. Utilizar como anuncio de una llamada posterior, servirá para alertar rápidamente sobre lo sucedido.

PARA MEDIOS DE COMUNICACIÓN Y REDES SOCIALES

No es necesario contactar con todos, puesto que daremos mayor difusión sin necesitarlo. No olvidemos que sufrir un ciberataque es algo que no nos reportará buena imagen.

- Mail. En el caso de contactar con los medios que se hayan hecho eco del problema.
- Teléfono. Más directo, por ejemplo, para avisar del envío del comunicado o solicitar el destinatario del mismo.
- Redes Sociales. Valorar si responder directamente al autor del comentario o hacerlo público a todos los fans o seguidores si el problema fuese demasiado grave. También, notificar la resolución del mismo y agradecer la colaboración y comprensión de los afectados.

¿Problema solucionado?

SÍ

El ataque ha sido controlado y la actividad se reanuda con total normalidad.
Solución: comunicar a los clientes que todo ha acabado.

NO

El ataque continúa o se están reparando los daños. Si se alarga en el tiempo, valorar la emisión de nuevas comunicaciones que informen sobre la persistencia del problema y del esfuerzo que se está realizando para solucionarlo.