EL PAÍS
ECONOMÍA

Peligro: ciberataques a empresas

Una oleada de fraudes en Twitter y Facebook revela la fragilidad y los elevados riesgos que corren las marcas, incluso las más grandes, en las redes sociales

MIGUEL ÁNGEL GARCÍA VEGA 3 MAR 2013 - 01:00 CET

Archivado en:

De repente, McDonald's había comprado Burger King. De repente, Chrysler había vendido Jeep. Y de repente, todo era una gran mentira. Un fraude. Los últimos ataques que han sufrido las cuentas de Twitter de esos gigantes empresariales, publicando información falsa o directamente ultrajante, revelan la fragilidad de las marcas en las redes sociales.

Vodafone Egipto, Pfizer, USA Today, Reuters, Gizmodo, Fox News, NBC News, Cadillac, Bank of Melbourne... todas han sido atacadas por*hackers* entre 2011 y 2013. Hay más, muchas más, pero la discreción manda. Nadie quiere transmitir una imagen de flaqueza.

Piensen en la credibilidad que comunica un banco cuya cuenta en Facebook o Twitter ha sido pirateada. Pero todas las compañías, “desde corporaciones bancarias hasta organizaciones de caridad locales, pueden ser un objetivo”, advierte Andrew Rose, analista de la consultora Forrester Research. Mientras tanto, crece la sensación de peligro en el mundo digital.

La firma de seguridad Ponemon Institute acaba de presentar un estudio elaborado entre 650 responsables de tecnología de diversos bancos que relata que el 43% de ellos cree que las agresiones empeorarán este año. “Algunas empresas sufren hasta 400 ataques diarios”, asegura Claudia Gómez, responsable de ciberriesgos del bróker asegurador Aon España. Nadie está a salvo. “Casi todos nuestros clientes ya han tenido algún susto”, revela la experta.

Nadie está a salvo. Algunas compañías reciben cientos de ataques diarios

La presencia de las marcas en las redes sociales implica asumir riesgos, porque estas plataformas “se han convertido en la última frontera para los *hackers* que quieren provocar el caos y también —esto sucede últimamente— robar información y dinero a usuarios desprevenidos”, relata Ray Bruck, cofundador de Social iQ Networks, una empresa de San Francisco especializada en seguridad digital. “Hemos pasado del cibercafé al ciberterrorismo”, asevera una fuente de la industria.

Aunque ese peligro, como hemos visto, alcanza a todas las empresas, en España las entidades financieras, la industria turística y el sector hotelero son los más expuestos. Los tres manejan el bien más codiciado por un *hacker:* la información. O sea, listados de clientes, números de tarjetas de crédito, planes de inversión, propiedad intelectual. Son productos que se transforman en dinero con facilidad.

Hablamos de un botín a la altura del pirata Barbarroja. La consultora Gartner estima que las redes sociales generaron el año pasado unos ingresos de 16.900 millones de dólares (12.900 millones de euros). Es más, Twitter acaba de dejar con la boca abierta a muchos analistas al trascender que generará ventas de 1.000 millones de dólares (766,4 millones de euros) en 2014. Crece dos veces más rápido de lo que muchos expertos pensaban. Y LinkedIn, que no se queda atrás, ha ingresado 304 millones de dólares (232,2 millones de euros) en el último trimestre de 2012, un 81% más que en el mismo periodo de 2011.

El impacto del cibercrimen supera los 300.000 millones anuales

Pese a todo, estos buenos resultados económicos no deberían ocultar el problema que se esconde en las redes y que evidencian tanto los adjetivos que usan los expertos como los números que manejan. “El coste [para las empresas] es asombroso. El cibercrimen tiene un impacto de 400.000 millones de dólares (305.000 millones de euros) en la economía mundial. Más que el tráfico de drogas”, calcula Dean Nicolls, vicepresidente de *marketing* de TeleSign, una compañía californiana dedicada a la protección de redes sociales.

Junto al dinero, el otro factor que justifica esta oleada de ataques llega de la tecnología. “Las marcas están siendo pirateadas porque son un objetivo relativamente sencillo, con contraseñas fáciles de recordar y que se comparten con mucha gente y grupos”, reflexiona Ian Schafer, consejero delegado de la agencia de publicidad digital Deep Focus. Ese hábito (mezcla de pereza y mala memoria) de usar una misma clave para el banco, las redes sociales o el teléfono inteligente acarrea problemas. “Tenemos que darnos cuenta de que nuestra contraseña es un activo cada vez más valioso”, apostilla Francisco Pérez, secretario de Aerco-PSM (asociación española de responsables de comunidades *online).* Y lo es en términos prácticos y económicos.

Ante esta situación, algunas plataformas, como Google, Facebook o Dropbox, están incrementando su seguridad (con dos niveles de autentificación), y se espera que pronto Twitter haga lo mismo. Porque hay fallas evidentes. Las redes sociales —aconseja Dean Nicolls, de TeleSign— necesitan asegurarse de que solo acceden a ellas los usuarios legitimados, y además deben emplear herramientas automáticas que eliminen en tiempo real contenido ofensivo y malicioso.

Porque si no lo hacen, y los piratas se cuelan, las consecuencias económicas pueden ser profundas. Los especialistas las nombran de corrido, como un niño recita la tabla de multiplicar. Pérdida de usuarios, daños en la reputación corporativa, mediciones de visitas irreales, dificultad para saber cuántos usuarios son auténticos, abandono de anunciantes. ¿Cómo no vas a tener problemas si, por ejemplo, proporcionas datos incorrectos a tus patrocinadores? Entonces, ¿quién querrá anunciarse contigo?

Un coste difícil de calcular

¿Cómo se puede calcular el coste de los ciberataques para una empresa? ¿Qué precio tiene la reputación de Burger King? ¿Cuánto vale la de Chyrsler? Imposible cifrarlo.
Pese a ser incuantificable, el peligro late ahí fuera. “Existen dos tipos de empresas”, señala Javier Zamora, profesor del IESE. “Las que saben que han sido *hackeadas* y las que no”.
El entorno se vuelve cada vez más hostil. El *spam* —detalla la firma estadounidense de seguridad digital Impermium— afecta ya al 40% de las cuentas de las redes sociales y al 8% de los mensajes transmitidos. Evidencias de este tipo han empujado a las compañías españolas a comprender la hondura del desafío. Por eso, el problema “ha salido de los sótanos del departamento de informática y cada vez la alta dirección se encuentra más implicada”, observa Diego Bueno, director de servicios de seguridad y privacidad de KPMG. Hace algunos años, los *hackers* operaban en garajes con escasos medios, hoy recurren a edificios repletos de tecnología. Tiempos nuevos, espacios distintos, pero idénticos objetivos: la flaqueza de las marcas.

Aunque esta es una fragilidad exterior, hay otra que procede de dentro. El *community manager* (la persona encargada de gestionar la presencia de una empresa en las redes sociales) puede equivocarse en sus mensajes, el responsable de relaciones públicas podría errar la estrategia de comunicación y la información confidencial puede verterse fuera. La primera consecuencia sería que los pleitos se empezarían a acumular sobre la mesa. La segunda afectaría a la cuenta de resultados de la firma.

¿Culpables? De esta indefensión son “tan responsables los *hackers*como las propias redes”, asevera Víctor Mirabet, consejero delegado de la consultora de marcas Colemann CBX. Igual de claro lo tienen en Coca-Cola a la hora de repartir responsabilidades. “Estos soportes no pertenecen a las enseñas. Si una red social se cae o se *hackea*, no podemos hacer nada excepto informar a nuestros consumidores”, justifican en el fabricante de refrescos.

Pero ¿y el coste económico directo? Imposible cuantificarlo. Aun así, Ray Kruck, de Social iQ Networks, lo cifra, para una marca normal, entre 25.000 y 50.000 dólares (19.000 y 38.214 euros). Sin embargo, estas cantidades solo sirven por recomponer el desaguisado de imagen a corto plazo. De hecho, la analista Tina Ong calcula que una red social con 50 millones de miembros que genere 9,5 dólares (ingreso estándar en 2012) al año por usuario y anuncio y que perdiera el 5% (tasa media de abandono) de sus integrantes debería afrontar unas potenciales minusvalías anuales de 23,7 millones de dólares (18,07 millones de euros). Pero son estimaciones.