PayPal: ¿Tiene la suficiente seguridad como para que nuestra información esté a salvo?

PayPal es una empresa estadounidense perteneciente al sector del comercio electrónico, que permite realizar pagos en sitios web o transferir dinero entre usuarios de la plataforma mediante el correo electrónico. Paypal, a pesar de operar con dinero, no se considera una entidad financiera, aunque sí tiene que cumplir una serie de normas para regular las transferencias de dinero. Una de sus mayores ventajas es la protección que brinda al comprador, cuando éste no ha recibido el producto pagado, o no se corresponde con su descripción. El negocio de la compañía se centra en las comisiones que cobra por cada transacción, aproximadamente entre el 1,9% y 3,4% de la operación.

Sin embargo, al ser una plataforma de pagos y transferencias online, pronto aparecieron los hackers tratando de buscar las vulnerabilidades del sistema, y lo consiguieron, eludiendo el mecanismo de autenticación, lo que les permitía realizar pagos desde las cuentas de los usuarios, evidentemente sin su consentimiento.

En 2014, la consultora de seguridad Duo Security fue la encargada de detectar esta brecha en el sistema, como comenta en su blog oficial. La vulnerabilidad se encontraba en el proceso de autenticación que ofrece PayPal en su API para los servicios web. Esta API pueden utilizarla terceras partes para realizar la autenticación a través de PayPal.

PayPal, ante esta amenaza y potencial pérdida de usuarios, trató de buscar una solución eficaz para hacer más fuerte su sistema de seguridad y evitar que sus clientes puedan sufrir estafas o robos de identidad. Además, la compañía consideraba que la solución debía estar orientada no solo a la amenaza detectada en ese momento, sino que debía ser sostenible y activa para poder hacer frente a posibles amenazas en un futuro. Para este caso concreto, la solución se basó en incluir una capa de seguridad adicional (2FA) que los usuarios podían añadir a su cuenta, para poder contar con una protección adicional. Este método de seguridad consiste en verificar la identidad del usuario en dos pasos: por un lado, datos que el cliente conoce (dirección de correo electrónico), y por otro lado, una información adicional que no sea

tan fácilmente accesible, como podría ser un link de confirmación enviado a la dirección de correo que se ha proporcionado.

Analizando casos de fallos en la seguridad como este, PayPal ha decidido en 2015 potenciar la seguridad de la compañía, adquiriendo para ello la empresa israelí CyActive, dedicada a la ciberseguridad, cuya premisa es ser capaces de predecir lo que los hackers maliciosos van a hacer, anticipándose y mitigando esos ataques. Desde CyActive pretenden explotar los recursos existentes para llegar a nuevas soluciones con su tecnología, y lo hacen de la siguiente manera: el malware que viene con programas originales, cuando llega en versiones avanzadas, tiene los mismos componentes básicos que las versiones anteriores del mismo software, lo que permite ver claramente los métodos que los hackers están utilizando ahora, y poder anticiparse a las que van a utilizar.

Como conclusión, parece que tras el ataque comentado anteriormente y otras potenciales amenazas que hayan detectado, han visto la importancia de mantener elevados niveles de seguridad, sobre todo teniendo en cuenta que manejan información financiera muy delicada de todos sus clientes. Por ello, una de las medidas tomadas, como la compra de CyActive, puede evitar que sus clientes se sientan inseguros al aportar a PayPal datos como el número de tarjeta de crédito o las claves, y creo que esa seguridad puede ser una de las claves del éxito para una compañía como PayPal.