

Codere pierde 744.000 euros en un ciberataque y reconoce falta de controles internos

La compañía informa al regulador estadounidense (SEC) que los atacantes se apropiaron de esa suma tras hackear el correo de un alto directivo de la filial online de la multinacional española del juego, que ya sufrió una brecha de seguridad en 2020

Codere ve riesgo de perder su licencia en España por un cambio legal que castiga la acumulación de sanciones muy graves.

La multinacional española del juego Codere ha reconocido al regulador estadounidense (la SEC), donde cotiza su filial Codere Online, la existencia de diversas deficiencias y “debilidades” en sus controles internos tras un ciberataque perpetrado el pasado ejercicio que ha provocado al grupo una salida de recursos que cifra en 744.000 euros.

Los atacantes se apropiaron de esa suma mediante facturas manipuladas tras hackear el correo de un alto directivo de su filial online. La empresa ya sufrió una brecha de seguridad en España a finales de 2020.

En este caso, los hechos se remontan al primer semestre de 2022. A través de la cuenta de correo de ese alto directivo de Codere, los atacantes “se hicieron pasar por agentes del equipo comercial de Codere Online” para enviar a diversos proveedores del grupo “solicitudes de pago ilegítimas adjuntando facturas manipuladas”.

El resultado es que Codere Online ha tenido que reconocer en sus cuentas que ha realizado “determinados pagos de facturas pendientes por un importe aproximado de 744 miles de euros a cuentas en el extranjero controladas por el suplantador”, y no por sus verdaderos proveedores, según ha explicado Codere a las autoridades estadounidenses.

La compañía señala que se puso en contacto con los bancos involucrados en las transferencias en cuanto tuvo conocimiento de los hechos. Pero, “hasta la fecha, Codere Online ha recuperado una mínima parte” de esa cifra. Según Codere, se trata de “un evento aislado” y con este ciberataque “no se pusieron en riesgo los depósitos de cuenta de los usuarios ni sus contraseñas”, ni se accedió a los datos confidenciales de sus usuarios.

“Codere Online continúa persiguiendo la recuperación de las cantidades transferidas” y “puede estar limitada en la información que puede divulgar” sobre este caso “ya que actualmente está considerando acciones legales”, dice la compañía en un documento que acaba de remitir a la SEC. El grupo se ha comprometido a detallar las medidas adoptadas para remediar esta situación en su informe anual.

Tras una investigación interna, la compañía ha señalado que, pese a que los atacantes tuvieron acceso a la información de la cuenta de correo de ese alto directivo, salvo por los datos disponibles en ella, “no hay evidencia” de que se haya tenido acceso a ninguna información corporativa de la compañía, incluyendo la financiera o contable. Esa investigación, añade, “no ha encontrado pruebas de la involucración de ningún empleado de la compañía” en el fraude.

Pero la dirección de la compañía ha tenido que reconocer a la SEC la existencia de diversas “debilidades” en sus controles internos. En primer lugar, “en el control interno sobre la información financiera” de la filial, por un “diseño inefectivo” y controles insuficientes sobre su sistema de pagos; y en segundo lugar, por la incapacidad de sus sistemas de ciberseguridad para evitar el ataque.

Así, la empresa ha reconocido que “Codere Online no mantuvo controles efectivos” sobre sus sistemas de tratamiento de la información “como consecuencia de la existencia de ciertas debilidades materiales en el control interno” sobre el reporte de su información financiera. Codere asegura que tras el incidente esos controles internos se han “mejorado” y se ha comprometido con la SEC a ampliarlos. Es, asegura, una de las “principales prioridades” de su equipo gestor.

El grupo dice a la SEC que este tipo de ataques informáticos “son, por naturaleza, tecnológicamente sofisticados y podrían ser imposibles de detectar y combatir”.

Brecha de seguridad

La compañía ha dado cuenta de este ciberataque después de que, en noviembre de 2020, notificase a la Agencia Española de Protección de Datos (AEPD) la existencia de una brecha de seguridad en sus sistemas informáticos. En este caso, Codere detectó tres consultas sospechosas desde el servidor de uno de sus data centers a la base de datos que recopila las cuentas de sus jugadores online.

En ella se recogen datos sensibles como códigos de usuario, contraseña encriptada, DNI, nacionalidad, país de residencia, profesión, nombre y apellidos, datos de localización y contacto (dirección postal, dirección de correo electrónico, teléfono), profesión, saldos en cuenta o número de cuenta bancaria.

La AEPD constató en junio de 2021 que se había producido una quiebra de seguridad de datos personales en los sistemas de Codere, pero archivó las actuaciones tras comprobar que no se habían detectado incidentes, ni anomalías, ni actividades sospechosas en las cuentas de los usuarios. Según la AEPD, Codere “disponía de medidas de seguridad razonables” y reaccionó de forma “diligente” para minimizar su impacto y evitar que se repita en el futuro.

El grupo reconoció que esta fue “la primera ocasión en la que se produce una brecha de seguridad de datos personales”. Inicialmente Codere notificó que habían podido verse afectados los datos de los 599.556 clientes que tenía registrados a esa fecha. Tras una auditoría externa cifró el número de posibles afectados en 64.281, a los que se informó por correo de esa brecha de seguridad.

Codere fue sancionada el pasado diciembre por la Comisión Nacional del Mercado de Valores (CNMV) con una multa de 100.000 euros por una infracción “muy grave” de la normativa del mercado de valores español, por incluir información “no veraz y engañosa” sobre los resultados de sus filiales en México, Colombia y Panamá, tras la incoación de un expediente sancionador en septiembre de 2021. La matriz del grupo dejó de cotizar en España a finales de ese año.

Fuente: eldiario.es

Link: https://www.eldiario.es/economia/codere-pierde-744-000-euros-ciberataque-reconoce-falta-controles-internos_1_9870318.html