

JUGANDO A PERDER

Sin duda alguna, la compañía más zarandeada por todos los frentes últimamente es Sony, la multinacional por antonomasia del entretenimiento digital. Tras el pertinente cierre de su último ejercicio fiscal (a 31 de marzo), el gigante nipón –según detalla la agencia Reuters– ha tenido que “provisionar” 2.278 millones de euros para absorber el impacto que en sus negocios ha tenido la debacle provocada por el maremoto del pasado 11 de marzo. Parar temporalmente la producción de sus 10 plantas en Japón ha sido un auténtico desastre para los florecientes beneficios que venía registrando trimestralmente.

En consonancia con lo sucedido y con esos temas, tan inevitablemente vinculados a la supervivencia de la actividad mercantil, como son los de disponer de planes de continuidad de negocio, y de que las infraestructuras suministradoras de servicios críticos sigan funcionando, cabe reflexionar profundamente sobre lo acontecido. Y mire usted lector, qué casualidad: ya está vivo y coleando el estándar ISO 27031 (*Tecnología de la información. Técnicas de seguridad. Directrices para la información y la disponibilidad de la tecnología de comunicaciones para la continuidad del negocio*); y en estas tierras, con el triste incidente de Lorca en la retina, ya disponemos de la Ley de establecimiento de medidas para la protección de infraestructuras críticas y su primer desarrollo reglamentario. Toda una coincidencia.

Pero retomando lo afirmado al inicio de la columna, procede ahora destacar el batacazo adicional que Sony se está dando no ya en los escenarios físicos, sino en los virtuales; me refiero a la oleada de incursiones –en el momento de cierre de la edición aún seguían– de la que está siendo objeto por parte de ese lado oscuro digital, cada vez más conjurado a extraer chicha de las violaciones de sistemas TIC ajenos.

Según fuentes directas de la compañía agredida, el coste de los dos primeros ataques sufridos en abril a la red PlayStation Network y en mayo a Sony Online Entertainment –i con la sustracción de datos de 77 millones y de 25 millones de usuarios, respectivamente!– es de 122 millones de euros (¡más de 20.000 millones de las antiguas pesetas!), eso, imagínense, sin incluir los costes de pérdida de clientes y reputación. Y aún siguen azotándoles calamidades en Tailandia, Indonesia, Grecia y Canadá.

Lo más bochornoso del caso es que el consejero delegado de la afectada, Howard Stringer, con absoluta tranquilidad, ha declarado que “no cree que los daños sean enormes” y que, tras haber esperado una semana desde el incidente, no había constancia de que los datos robados hayan sido usados “indebidamente”.

Con todo, Sony se ha visto forzada a llevar a cabo un apresurado fortalecimiento de sus sistemas y redes (al parecer, evidenciaban estrechos agujeros por defectos en sus aplicaciones no reparados pese a las advertencias) y ha transferido el riesgo a Affinion International, quien bastionará en modo externalizado los datos de los clientes de la cedente.

Lo cierto del ‘affaire’ Sony es que supone, hasta el momento, la mayor sustracción de datos de ciberusuarios conocida y, dado el pedigrí de la afectada, la incursión cibernética con mayor eco mediático. Esto huele a aviso de navegantes: vendrán más. ●



LUIS G. FERNÁNDEZ
Editor
lfernandez@codasic.com