¡Marchando una de *ransom(every)ware*!

Luis Fernández Delgado
Editor
lfernandez@codasic.com

Quiso el destino que un servidor se enterase recientemente de que un hospital levantino fue incapaz de suministrar a un paciente una prueba médica que precisaba con insistencia, tras habérsela hecho en la citada instalación. Tras repetidas evasivas, los representantes de la entidad sanitaria acabaron por confesar al demandante –casualmente, una experta en privacidad– que nunca podrían proporcionársela porque durante la fecha y periodo en que se la hicieron, fueron objeto de un ciberataque cuya resultante fue la destrucción irrecuperable de su información médica, incluida la de respaldo. Tras admitir el desaguisado, y a preguntas del damnificado, acabaron admitiendo también que nunca comunicaron el ciberataque a entidad u organismo alguno y que, como mucho, pusieron un anuncio en un diario local pidiendo disculpas. Este bochornoso –e inquietante– incidente es uno de los tantos que últimamente asolan, a escala planetaria, a todo el ecosistema social basado en TIC.

> ¿Para cuándo un pacto nacional contra el *ransomware* como perfecto ejemplo de lo que sí sería auténtica colaboración pública-privada?

Qué bien viene a colación el clásico dicho: "Lo que funciona, no lo toques" y cuán de acuerdo deben estar con ello la ciberdelincuencia, 'jartita' ella de deyectar a espuertas y 'tirando' a todo oleadas industrializadas de *ransom(every)ware* para todo el patio digital, sea corporativo, pyme o individual, tanto da. Tan bien les va con la ciberextorsión a granel que su gula digital aún tiene para rato, como bien vaticinan la centena larga de expertos que en el especial de esta edición de SIC evidencian, cual tecnoarúspices, quién narices va a estar habitando y royendo las entrañas de nuestras queridas TI/OT.

De hecho, datos recientes del estudio periódico de Coveware arrojan clarificadora luz sobre el fenómeno: el importe medio de los rescates se duplicó en el último trimestre de 2019 alcanzando los 76.305 euros; el 98% de las empresas que pagaron rescate recibieron la herramienta de descifrado, llegando a recuperar hasta un 97% de la información comprometida en plazos medios de 16,2 días en empresas damnificadas con media de 610 trabajadores. Se advierten ya nítidas especializaciones de técnicas y familias por sectores concretos como el sanitario o de industria... ¡Mmm aquí hay tomate!

Entre tanto, sus estropicios no están haciendo suficientemente mella en los actores a quienes se les encomienda el constructo de una sociedad digital que hace aguas por su precipitación en edificarlo a velocidad de vértigo, sin red e incapacitados para custodiar y proteger su normal devenir. Como cruel aviso a navegantes asoman ya inquietantes noticias de centenares de despidos en empresas desvalidas idas a pique por carecer de prácticas de respaldo frente al *ransomware*. A no mucho tardar rodarán cabezas de C-level. Resulta paradójico que un gran número de organizaciones estén propiciando el auge de los ciberseguros para precisamente poder paliar el terrible impacto de estos severos incidentes.

Ante la abundante casuística actual cabe preguntarse algunas clarividentes cuestiones derivadas de la situación. Así, un suponer: ¿Pueden los servicios públicos españoles con la ley en la mano optar por pagar rescates saltándose directrices gubernamentales, si las hubiera (como sucediera recientemente en dos localidades estadounidenses en Florida)? ¿Existe vacío legal a la hora de adoptar, o no, estas decisiones frente a las extorsiones con el miedo adicional y creciente a que además se publique información confidencial?

Ante la insuficiente contención tecnológica a día de hoy para neutralizar el fenómeno –más allá de las consabidas actualizaciones pero aún incapaz de crear aislamiento de entrada con chequeo previo eficaz– no queda otra que echar mano de la concienciación y exacerbarla.

¿Por qué en lugar de que los escasos ciberbomberos hoy disponibles sigan tratando de sofocar a salto de mata las brutales oleadas de teas digitales con escuálidas mangueras, no se convoca un cónclave para aunar y optimizar esfuerzos para una mayor y mejor contundencia? ¿Para cuándo un pacto nacional contra el *ransomware* como perfecto ejemplo de lo que sí sería auténtica colaboración pública-privada? ¿Tan difícil resultaría poner de acuerdo a los actores gubernamentales concernidos y al sector oferente para, de la mano, hacer énfasis en la divulgación-concienciación, en lugar de la consabida dispersión de esfuerzos. ¡Compartan juego señores, apaguen fuegos! ●