LA OTRA 'OLA' DE 2020: CIBERATAQUES A HOSPITALES

LA INTERPOL Y EL CNI ALERTAN DEL INCREMENTO DE ESTAS AGRESIONES. ACTUAR SOBRE UNA SIMPLE FOTOCOPIADORA PUEDE BLOQUEAR TODOS LOS SERVICIOS DE UN CENTRO SANITARIO. POR **ALBERTO CORNEJO**

En el análisis que a continuación proponemos se debe partir de una primera premisa: cualquier máquina, dispositivo o sistema conectado a la Red es susceptible de ser vulnerado. Piensa ahora en la alta digitalización –tanto en logística como en labores de gestión– que incorporan los centros sanitarios, así como la especial sensibilidad y confidencialidad que requiere el manejo de datos clínicos. Combina todo lo anterior y encontrarás la respuesta a por qué las instituciones médicas –y, en especial, los hospitales– son, de un tiempo a esta parte, objetivo predilecto de ciberdelincuentes.

EN UN 2020 EN EL QUE, DEBIDO A LA PANDEMIA, SE HA HABLADO CONTINUAMENTE DE 'OLAS', también puede asegurarse que asistimos actualmente a una *ola* de ciberataques a estas infraestructuras. Ya en abril –coincidiendo con el inicio de la expansión de la covid-19–, la Interpol emitió un comunicado en el que alertaba del "incremento significativo" de ataques de *ransomware* –secuestro de datos a cambio de un rescate– a hospitales de todo el mundo. En España, el Centro Criptográfico Nacional –dependiente del CNI– ha avisado también del aumento de la ciberdelincuencia contra centros médicos. A tenor de un estudio realizado por el instituto Sans, ya en 2019 se produjeron 50 000 ciberataques a organizaciones relacionadas con la salud.

"El 99 % de los ciberataques a centros sanitarios son de tipo *ransomware*, es decir, esconden una motivación o chantaje económico", explica Sancho Lerena, presidente y fundador de Ártica, compañía especializada en la monitorización de infraestructuras tecnológicas; entre ellas, las de hospitales nacionales e internacionales. Este experto en ciberseguridad e inteligencia artificial recuerda que "una máquina de rayos X, una simple fotocopiadora del centro o, incluso, el ordenador del facultativo pueden sufrir un DoS (Denial of Service) y llegar a bloquear el funcionamiento de todo el hospital".

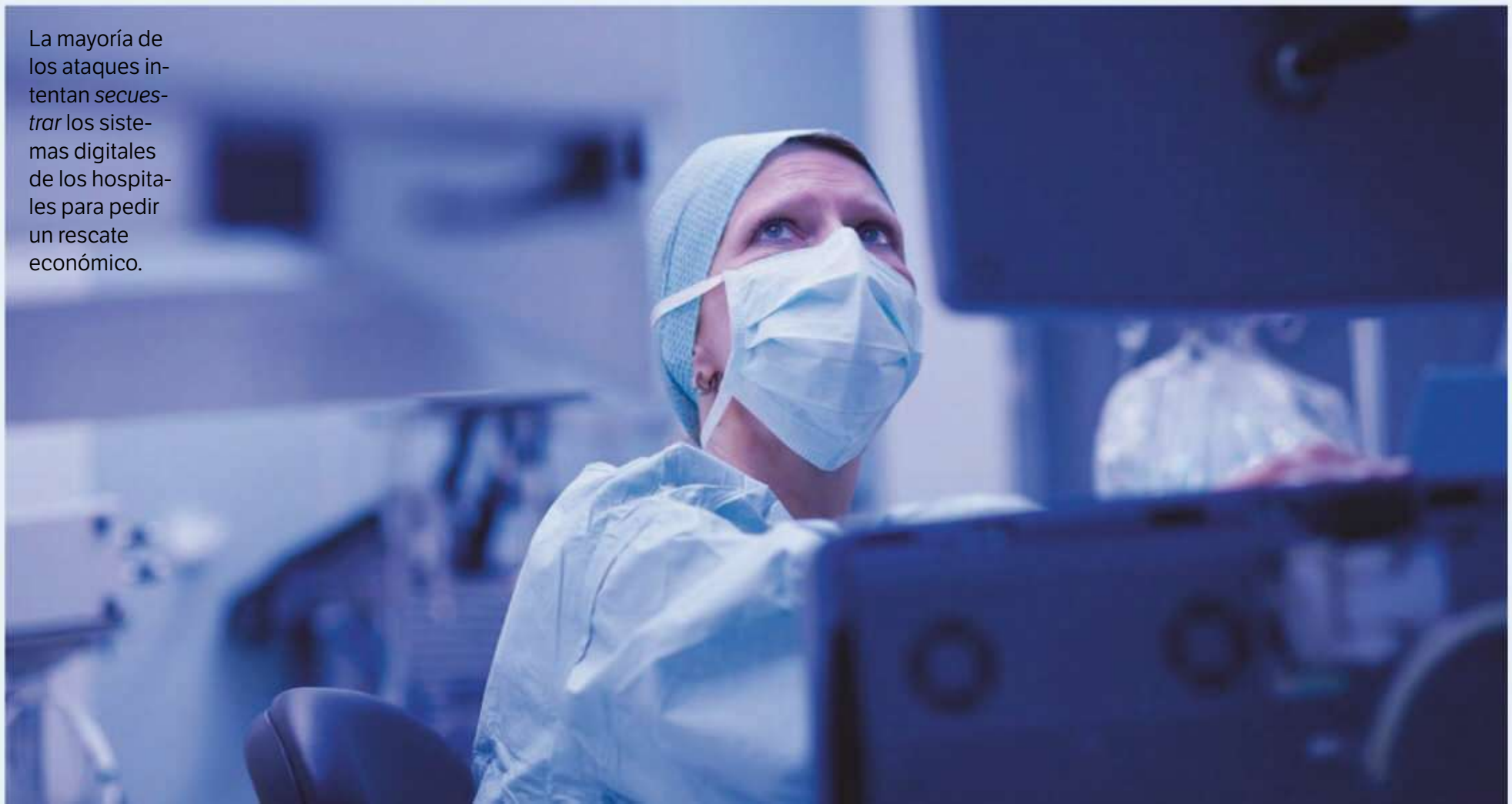
Pero ¿por qué están en el punto de mira de estas organizaciones criminales? "La dependencia de lo digital vuelven muy jugosos los ataques a estos centros. Los ciberdelincuentes saben que la información sanitaria es crítica y confidencial, y, por ende, las consecuencias que acarrea su acción tanto en la paralización de la actividad asistencial como en la reputación de la institución. Así pueden exigir una compensación para evitar o parar el ataque", indica Lerena. Pero, por desgracia, no todo son implicaciones económicas. En Alemania, el hospital universitario Uniklink (Düsseldorf) sufrió una agresión que paralizó el servicio de urgencias durante trece días y provocó la muerte indirecta de una paciente. ◻

CÓMO CONSTRUIR UN ESCUDO INTEGRAL

La creciente ola de ataques ha propiciado, como no podría ser de otra manera, la necesidad de invertir más en ciberseguridad. Un escudo que debe ser integral. "No tiene sentido proteger el 99 % del equipamiento y sistemas del centro y *descuidar* la seguridad de cualquier máquina; en un hospital, todo está conectado", explica el experto Sancho Lerena.

Debido a ello, se debe apostar por softwares de control y monitorización para todos los servidores y sistemas. ¿El objetivo? "Vigilar en tiempo real el funcionamiento de cada aparato y detectar cualquier incidencia que pueda prever posibles ciberataques", destaca. De manera especial, hay que proteger la información "más sensible", como los expedientes de los pacientes, y evitar filtraciones de los registros médicos a internet.

SHUTTERSTOCK



GETTY

La mayoría de los ataques intentan *secuestrar* los sistemas digitales de los hospitales para pedir un rescate económico.