IDEAL GRANADA INNOVA+

PAÍS: España
PÁGINAS: 1-3
TARIFA: 18006 €
ÁREA: 2556 CM² - 284%

FRECUENCIA: Mensual
O.J.D.: 12610
E.G.M.: 126000
SECCIÓN: INNOVACION

29 Mayo, 2019

¿Y si su hospital fuera 'hackeado'?

El riesgo de ataque cibernético a los centros sanitarios es real y un simple virus puede falsear diagnósticos, cambiar citas o modificar pruebas [P2Y3]

IDEAL GRANADA INNOVA+

PAÍS: España
PÁGINAS: 1-3
TARIFA: 18006 €
ÁREA: 2556 CM² - 284%

FRECUENCIA: Mensual
O.J.D.: 12610
E.G.M.: 126000
SECCIÓN: INNOVACION

29 Mayo, 2019

Código rojo en la seguridad de los hospitales

HACKEO EN LA **RED SANITARIA**

JOSÉ A. GONZÁLEZ

Un ataque cibernético al mundo sanitario puede provocar desde una cancelación de una cita a un diagnóstico erróneo, y eso solo con acceder a la red de un centro sin necesidad de una invasión a gran escala

MADRID. El 12 de mayo de 2017, los ciberdelincuentes aprovecharon la vulnerabilidad EternalBlue, desarrollada por la Agencia de Seguridad Nacional estadounidense y filtrada por el grupo The Shadow Brokers, que permite atacar computadores con el sistema operativo Microsoft Windows no actualizados debidamente. En la memoria este ataque ha quedado grabado como Wannacry.

Este 'ransomware', un tipo de virus maligno que encripta información a cambio de dinero, paralizó a todo el mundo. Lo sufrieron usuarios, empresas y también servicios públicos. El más afectado fue el Sistema Nacional Saludo británico (NHS por sus siglas en inglés. El 1% de toda la atención del sistema se interrumpió una semana.

La visión generalizada del 'hacker' es de un joven con sudadera y capucha que busca información o comprometer un sistema para su propio beneficio o su satisfacción. Sin embargo, dista mucho de la realidad. «La ciberdelincuencia mueve ingentes cantidades de dinero», advierte Javier Osuna, director de la división de Consultoría y Servicios de Ciberseguridad.

El ataque obligó a cancelar más de 19.000 citas, lo que costó al NHS 20 millones de libras esterlinas en una semana, una factura a la que hay que sumar otros 72 millones en la posterior limpieza y actualización de todos sus servicios. «Un año después aún no estaban todos parcheados», señala Bosco Espinosa de los Monteros, 'presales manager' para Europa de Kaspersky Lab.

Dos años después toca hacer balance. «La gente está concienciada, pero todavía hay trabajo por hacer», añade Espinosa de los Monteros. La activación de Wannacry llegó por un clic en un 'link' malicioso y desató la infección. «Es necesario también esa concienciación a todos los trabajadores», apunta Marco Lozano, experto en el área de empresas y profesionales de INCIBE, el Instituto Nacional de Ciberseguridad.

La respuesta de los expertos ante la pregunta de un posible ataque a un hospital es unánime: «sí». Pero la concienciación de sus responsables administrativos deja dudas: «Por desgracia, no suele ser una de sus preocupaciones principales, aunque cada vez más existe una mayor concienciación sobre los problemas que pueden ser provocados por un ciberataque», puntualiza Josep Albors, responsable de concienciación de ESET España. «La seguridad no ha cambiado con respecto a años anteriores, no están suficientemente protegidos», añade Eusebio Nieva, director técnico de Check Point en España y Portugal.

Objetivo preferente

El sector sanitario es uno de los más intensivos en inversiones en innovación e I+D, representando más de un 20% de los fondos empleados en innovación en España. Además, casi el 9% del PIB corresponde a las inversiones que el Estado destina a Sanidad. «Estos son los ingredientes esenciales para determinar que es un sector clave para la economía y por lo tanto puede ser un objetivo claro para los 'hackers', especialmente si tenemos en cuenta que la información que se maneja es extremadamente sensible por diferentes motivos», apunta Adolfo Fernández Valmayor, secretario general de la Fundación IDIS.

Hasta la fecha, la gran mayoría de ataques que han recibido los centros hospitalarios han sido generales y no específicos contra sus instalaciones. «El vector de ataque más utilizado es el 'mail'», apunta Arturo Gordo, jefe del Departamento de Seguridad y Sistemas de HM Hospitales. «En estos casos por muchas medidas que adoptemos, dependemos en gran medida del usuario y por eso es importante realizar labores de concienciación y prestar una atención especial en los cursos de personal de nueva incorporación», añade.

Un ataque específico pondría en jaque el buen funcionamiento de las instalaciones y la seguridad de los pacientes. «No es lo mismo comprometer la red wifi para disponer de internet gratis que inutilizar/alterar sistemas, robar o modificar información, o bien los sistemas y aplicaciones encargadas de mantener la habitabilidad de las instalaciones, los dispositivos de los propios empleados, los sistemas de control de almacenamiento de medicamentos», alerta Osuna.

«No es lo mismo comprometer la red wifi que alterar sistemas o incluso controlar dispositivos»

Los expertos alertan de la carencia de planes directores en la sanidad pública para sus equipos y redes

Una vulnerabilidad que es común y «es fundamental haber hecho los deberes con antelación», puntualiza Osuna. Los hospitales tienen que trabajar en cuatro líneas fundamentales: prevenir y proteger, disponer de la capacidad de detección necesaria, establecer los mecanismos de reacción, contención y análisis apropiados, y planificar la recuperación posterior. Adicionalmente, es crítico fortalecer la totalidad de los eslabones de la cadena, señala.

«Se hacen auditorías anuales de nuestros sistemas con empresas externas de seguridad mediante metodologías de caja negra, caja blanca, 'hacking' ético, 'pentesting', etc... y si se detectan vulnerabilidades en los informes que realizan se toman las medidas oportunas para bloquearlas», apostilla Gordo en la misma línea.

En los hospitales públicos «no existe un plan director, al menos que yo conozca», destaca Lozano. Una protección básica «pasa por tener los sistemas informáticos lo más actualizados posible, contar con soluciones de seguridad modernas y actualizadas y segmentar las redes para evitar que una amenaza se propague por sistemas críticos del hospital», sentencia Josep Albors, responsable de concienciación de ESET España.

Wannacry, la gripe virtual que infectó la sanidad británica

La infección duró una semana y costó decenas de millones de libras en Londres a las autoridades

:: **J. A. GONZÁLEZ**

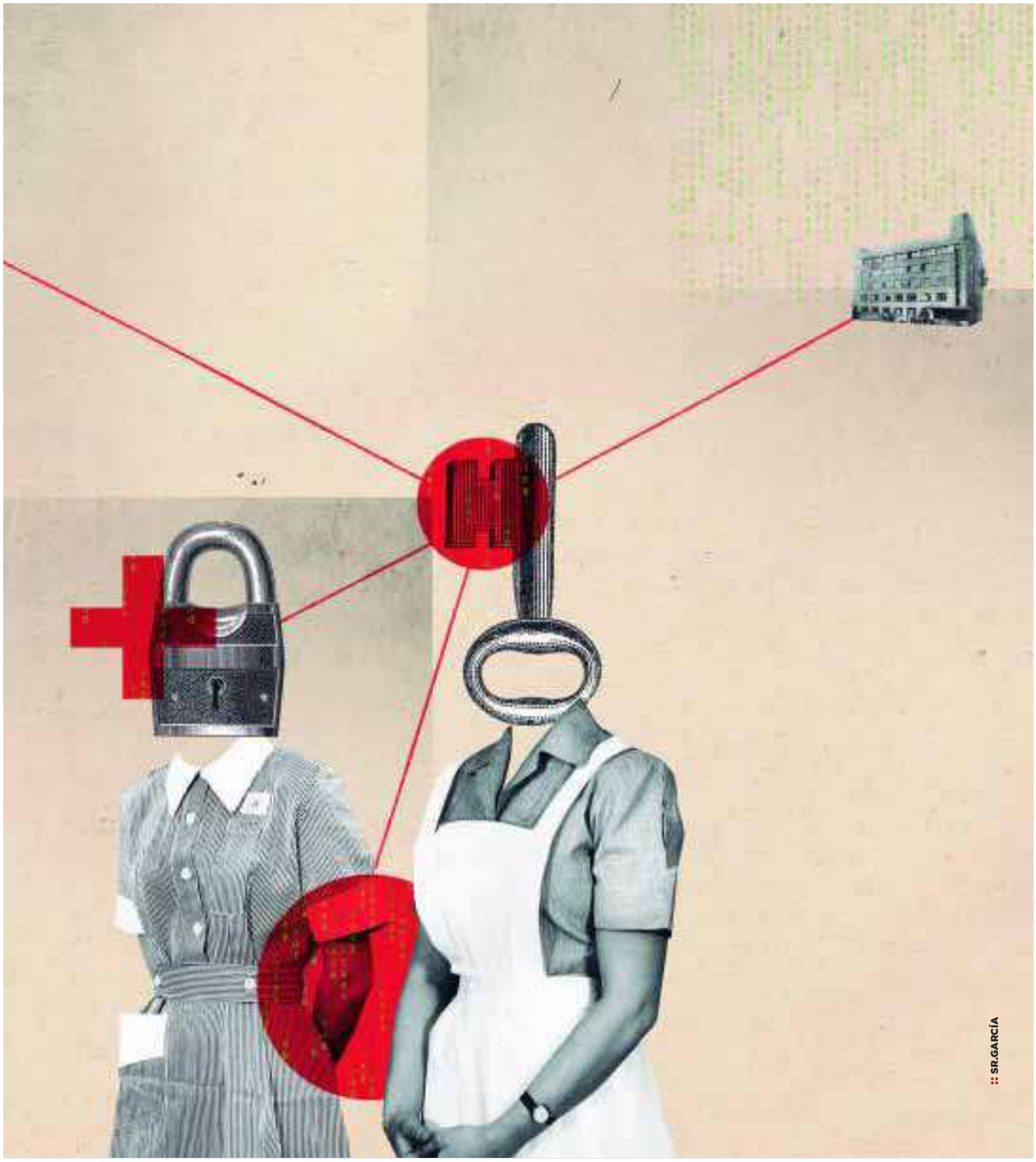
MADRID. A la 1 de la tarde del 12 de mayo de 2017, el NHS británico, el equivalente a la seguridad social española, alertó al Departamento de Salud y Asistencia Social de la existencia de varios

IDEAL GRANADA INNOVA+

PAÍS: España
PÁGINAS: 1-3
TARIFA: 18006 €
ÁREA: 2556 CM² - 284%

FRECUENCIA: Mensual
O.J.D.: 12610
E.G.M.: 126000
SECCIÓN: INNOVACION

29 Mayo, 2019



ataques 'ransomware' que afectaban a varios hospitales. Tres horas después se declaraba un importante incidente de seguridad.

El brote había provocado la interrupción de al menos 80 de los 236 fideicomisos hospitalarios en Inglaterra, así como 603 organizaciones de atención primaria y afiliadas del NHS, lo que resultó en sistemas infectados, miles de citas canceladas y el desvío de pacientes.

La Oficina Nacional de Auditoría concluyó sobre el impacto de WannaCry que el servicio de salud de Gran Bretaña no estaba preparado para un ataque cibernético de esa escala, a pesar de haber sido advertido de una amenaza ya en 2014. «Las amenazas derivadas del fenómeno del 'phishing' y el 'ransomware' entre otros, sirven para poner de manifiesto el valor de la información que manejamos», relata Adolfo Fernández Valmayor, secretario general de la Fundación IDIS.

El Departamento de Salud ha intentado calcular el coste financiero de WannaCry y la cifra alcanzó, según sus estimaciones, los 92 millones de libras. La estimación incluye, además, la pérdida de atención al paciente causada por el acceso reducido a la información y la cancelación de citas durante el ataque que costó 19 millones de libras.

Sin embargo, no es el único coste. A la factura hay que añadir un millón de libras para abonar los honorarios de los consultores en tecnologías de la información y seguridad en la semana del 12 al 18 de mayo para restaurar los sistemas afectados por el ataque.

El ataque cibernético provocó que 200.000 computadoras bloquearan a los usuarios con mensajes de error con letras rojas que exigían la criptomoneda bitcoin. El ataque fue atribuido a piratas informáticos de Corea del Norte después de una investigación de un año de duración.

El ataque provocó que 200.000 ordenadores dieran error y se apuntó a piratas norcoreanos

Los hospitales británicos tenían un sistema operativo de 17 años, lo que agravó sus vulnerabilidades

En el momento de los ataques se criticó al NHS por usar sistemas obsoletos, incluido Windows XP, un sistema operativo de 17 años que podría ser vulnerable a los ataques. «Los hospitales suelen tener equipos así. Se manejan con Windows 98, que hoy por hoy ya no está soportado y por eso tienen vulnerabilidades», señala Bosco Espinosa de los Monteros, de Kaspersky Lab.

Un simple virus puede falsear los tumores al hacer un TAC

:: J. A. G.

MADRID. Ya es sabido que un virus informático puede poner en serio peligro el funcionamiento de un equipo informático. Pero si se dirige contra cualquier equipamiento médico hablamos ya de un riesgo potencial para la salud.

Un grupo de investigadores del Ben-Gurion University Cyber Security Research Center de Israel han desarrollado un 'malware' que puede modificar las imágenes del TAC (escáner o tomografía axial computarizada) y mostrar nódulos cancerígenos falsos. Hasta la fecha los ataques contra hospitales iban encaminados a secuestrar información y ganar dinero con su rescate. Sin embargo, las brechas de seguridad serían importantes.

Estos investigadores israelíes apuntaron que su 'malware' nace para demostrar la baja seguridad de las herramientas de diagnóstico y las redes de los hospitales que manejan información sensible. En un estudio con expertos en radiología se les pidió a los facultativos diagnosticar condiciones basados en TAC de pulmones modificados por ese virus.

Los especialistas informaron de nódulos cancerígenos falsos el 99% de las veces. Pero cuándo el programa los escondió dieron un parte médico rechazando la presencia de cáncer el 94% de las veces.

El estudio abarca ejemplos de cáncer de pulmón, aunque un ataque como el que simula este 'malware' funcionaría para tumores cerebrales, enfermedades cardiacas, coágulos, lesiones de la columna vertebral, lesiones de ligamentos, artritis y fracturas.

Los expertos del Ben-Gurion denuncian que tanto hospitales como sus trabajadores dejan desprotegido el equipo y las redes que usan para transmitir y almacenar imágenes de TAC a los servicios de radiología o cualquier otro. Éstas se envían por el sistema de almacenamiento y transmisión de imágenes (PACS), muy común en centros sanitarios, sin cifrar o no están bien protegidas, por lo que un intruso puede entrar en la red, ver las pruebas y llegar a modificarlas.