BOLETÍN DE ALERTAS DE CIBERSEGURIDAD Y SALUD.

#27 BOLETÍN
JUNIO 2021

Bienvenido al boletín de alertas de ciberseguridad y salud de S2 Grupo.
El objetivo es que os resulte de utilidad y que, entre todos, podamos aportar contenidos interesantes específicos para el sector de la salud. Este boletín nace como canal de comunicación con nuestros clientes y por eso preferimos, de momento, que sea a través del correo electrónico, pero siéntete libre de compartirlo con otros colegas a los que pienses que les puede ser de interés: **La seguridad sigue siendo cosa de todos.**

NOTICIAS

1. A mediados de mayo, un ataque causado por el ransomware Conti forzó el cierre de los sistemas informáticos del sistema de salud de Irlanda. El ataque ha sido catalogado de alto riesgo, y ha afectado a la mayoría de hospitales y otras instituciones sanitarias. Algunas instituciones no se han visto forzadas a cancelar citas, pero han advertido a los pacientes de que las pueden surgir cambios o retrasos; otras como el hospital de Dublín se han visto forzados a cancelar citas de pacientes de ambulatorio. Compartimos con vosotros la noticia. [Inglés 1 | Inglés 2]

2. Los ataques de tipo ransomware a hospitales siguen creciendo. Junto con el ataque al sistema nacional de salud de Irlanda, este mes hemos conocido el ataque a Scripps Health (red de hospitales y atención ambulatoria en EEUU) y ataques a numerosos hospitales en Nueva Zelanda. En el primer caso, el ataque ha afectado a los sistemas durante semanas: los pacientes tuvieron que ser recolocados en otros hospitales y la pérdida de los sistemas web y de gestión de pacientes obligaron a acceder a historiales y otra documentación en formato offline. En el caso de Nueva Zelanda, el ataque ha sido centrado en los sistemas IT: los sistemas clínicos e informáticos han sido interrumpidos. Esto ha generado mucho caos, varias operaciones han tenido que ser pospuestas y las interacciones con los clientes se han tenido que llevar a cabo también de forma offline. [Inglés 1 | Inglés 2 | Inglés 3]

3 Crecen los fraudes relacionados con la pandemia: los ciberdelincuentes están recurriendo sobre todo a campañas de Spam y phishig. Por ejemplo, se detectó una campaña en Reino Unido en la que se pedían datos de tarjetas bancarias para ir a vacunarse. Otra pauta frecuente son encuestas falsas relacionadas con la vacunación. Se anima a hacer una encuesta de satisfacción con la vacuna a cambio de una tarjeta regalo del valor de $50 y así consiguen robar datos personales y financieros, ya que en este caso también se solicitan datos bancarios. [Español 1 | Español 2]

BOLETINES Y ACTUALIZACIONES

VENDEDOR	PUBLICACIÓN	DETALLES
SAP		Parches
Oracle		Boletín
Microsoft		Actualizaciones

PENSAMOS QUE PODRÍA INTERESARTE

1. Moody' Investor Services ha advertido recientemente que los ciberataques a hospitales y sistemas de salud seguirán creciendo, y que tenemos que estar preparados para ello. Para conocer las causas y algunas cifras clave os invitamos a leer este artículo, en el que destacan que la asistencia médica en remoto y la interconectividad junto con los ataques ransomware a dispositivos médicos como posibles causas de este impulso. [Inglés 1]

2. Ya está disponible el nuevo informe Verizon Data Breach Investigations Report (DBIR). En esta última edición destacan como hallazgo relevante que la mayoría de incidentes de filtración de datos se relacionan con causas externas como hacking en vez de errores internos. Concretamente, subrayan la intrusión en los sistemas, ataques en páginas y aplicaciones web y errores de empleados como las principales causas. Os dejamos una noticia en la que podéis encontrar un resumen explicativo y el enlace al informe. [Inglés 1 | Inglés 2]

3. Ante el creciente impacto de los ataques ransomware a los sistemas nacionales de salud, son varias las administraciones que están diseñando planes estratégicos. Este mes conocimos la noticia de que el presidente Biden ha diseñado un plan de choque para hacer frente a los ciberataques de tipo ransomware en hospitales. En este artículo podéis encontrar todos los detalles. [Inglés 1]

¿Echas de menos alguna información que te gustaría que incluyéramos?
¿Quieres que entrevistemos a alguien de referencia en el mundo de ciberseguridad y salud?
¿Quieres compartir alguna iniciativa interesante de tu organización?

Escríbenos a **clientes@s2grupo.es** y haznos llegar tu propuesta.

S2 GRUPO
Anticipando un mundo **ciberseguro**