S2 GRUPO
Anticipando un mundo ciberseguro

BOLETÍN DE ALERTAS DE CIBERSEGURIDAD Y SALUD.

#34 BOLETÍN
FEBRERO 2022

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.**

"Como ya adelantamos en el anterior boletín, el sector sanitario estará en el punto de mira de los ciberdelincuentes en 2022. En España el inicio de año ha venido marcado por diferentes ataques a sistemas sanitarios, lo que nos recuerda la importancia de apostar por la ciberseguridad en este ámbito"

NOTICIAS

1 Durante este comienzo de año 2022 ya se han reportado durante el mes de enero 3 ciberataques a entidades sanitarias españolas, concretamente la sanidad balear, el hospital centro de Andalucía y la HUCA de Asturias.

Los ciberataques han afectado de distinta manera a estas organizaciones. Para las dos primeras, los problemas más graves son la posible filtración de datos de pacientes, así como información del estado del COVID-19, documentos, contratos comerciales, DNIs, etc…

Sin embargo, el ciberataque detectado en el hospital de la HUCA sí que ha provocado el cierre temporal de algunos servicios, llegando incluso a dejar a 200 pacientes pendientes de su tratamiento.

Por suerte se especifica que todos los ataques mencionados fueron detectados a tiempo por lo que las consecuencias se alejan del escenario más grave. No obstante nos hace reflexionar sobre la vulnerabilidad del sector sanitario ante la ciberdelincuencia y la importancia de prestarle especial atención,

Español-1 / Inglés / Español-2

NOTICIAS

2

En el mes de enero de 2022 la fiscalía de Nueva York ha anunciado un acuerdo de 600.000$ con el proveedor EyeMed para resolver numerosas denuncias relacionadas con una filtración de datos que tuvo lugar en 2020 y en la que se vieron afectadas más de 2.1 millones de personas. Hace dos años los ciberdelincuentes obtuvieron acceso a una cuenta de correo de la organización EyeMed que contenía información sensible.

Posteriormente los atacantes usaron dicha cuenta para enviar 2000 correos phishing con el objetivo de obtener credenciales de la plataforma y en ese momento se notificó y bloqueó la intrusión. No obstante, la fiscalía ha determinado recientemente que en el momento de la intrusión no se había implementado un 2FA ni los requisitos suficientes de administración de contraseñas, lo que acabó afectando a millones de personas.

Finalmente la organización afrontará la multa y la necesidad de implementar protocolos de seguridad actualizados para prevenir futuros ataques.

Inglés

ALERTAS

VENDEDOR	SISTEMA	CRITICIDAD	DESCRPCIÓN	FUENTE
Philips	Vue PACS	Crítica	Podría permitir a una persona o proceso no autorizado espiar, ver o modificar datos, obtener acceso al sistema, realizar la ejecución de código, instalar software no autorizado, o afectar la integridad de los datos del sistema de tal manera que impacte negativamente en la confidencialidad, integridad o disponibilidad.	Inglés

BOLETINES Y ACTUALIZACIONES

VENDEDOR	PUBLICACIÓN	DETALLES
SAP		[Parches]
Oracle		[Boletín]
Microsoft		[Actualizaciones]

PENSAMOS QUE PODRÍA INTERESARTE

1 ¿Conoces el término Bockchain? Hoy en día es una tecnología que está en boca de todos y que tiene implicaciones en todos los sectores. Plantea una gran revolución en todo tipo de ámbitos ofreciendo una base de datos distribuida y segura eliminando a los intermediarios, que se puede aplicar a todo tipo de transacciones que no tienen por qué ser necesariamente económicas. En el siguiente artículo de nuestro blog Security Art Work explicamos uno de los aspectos en los que podría utilizarse estrictamente relacionado con el ámbito sanitario: garantizar la protección de datos personales.

Español-1

2 Como ya se hemos mencionado en otros boletines, los dispositivos médicos están más avanzados e interconectados que nunca y actualmente son un foco de ciberataques. En Beccker's Hospital Review se han diseñado una serie de buenas prácticas para ayudar a mejorar su seguridad:

1. Realizar una verificación de inventario para el análisis de riesgos
2. Trabajar con los proveedores para garantizar que los dispositivos y los sistemas se mantengan seguros
3. Proteger los activos y los dispositivos a lo largo de su ciclo de vida
4. Monitorizar el tráfico de red
5. Establecer prácticas seguras para dispositivos personales

Inglés-1

3 Kaspersky presenta una política de ciberseguridad para dispositivos biónicos cuyo objetivo es reducir los riesgos para el uso de este tipo de dispositivos que pretenden el perfeccionamiento humano. Dicho por su director del Equipo Global de Investigación y Análisis en Europa: "Estamos convencidos de que, para construir un mundo digital más seguro para el mañana, necesitamos asegurar digitalmente el futuro del perfeccionamiento humano hoy". Para más información visitar el siguiente artículo:

Español-2

¿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**