Publicado en Castelló de la Plana, Castellón el 21/02/2023

Estudio de HelpRansomware: Hasta 2025, la industria médica invertirá $125 mil millones en ciberseguridad

El sector médico se ha convertido el objetivo principal del ransomware por sus datos confidenciales y margen de mejora digital

Hay muchas formas en que la información del sector médico puede verse comprometida, incluidos los errores humanos, la suplantación de identidad o los ataques de ransomware.

El ransomware es extremadamente malicioso y tiene la capacidad de detener las redes y provocar daños catastróficos a una infraestructura. La industria médica es consciente de esta amenaza y desde hace tres años hasta 2025 prevé gastar $125 mil millones en ciberseguridad. En las áreas de prevención, eliminación y desencriptación de ransomware se basan las funciones de HelpRansomware, en los últimos 25 años.

La compañía, liderada por Andrea Baggio y Juan Ricardo Palacio, es líder mundial en ciberseguridad y desencriptación.

La industria de la salud, principal objetivo de ransomware
Los hospitales son el blanco de ataques de ransomware por dos razones principales.

Primero, la industria tiene una gran cantidad de datos confidenciales sobre los pacientes, que los piratas informáticos pueden utilizar para extorsionar.

La segunda es que la mayoría de los equipos y servicios médicos aún no están digitalizados, por lo que son vulnerables a los delitos informáticos.

Los delincuentes se aprovechan de su vulnerabilidad, lo que obliga a los hospitales y centros médicos a pagar un rescate para recuperar los archivos encriptados.

Es más probable que la atención médica pague el rescate ocupando el primer lugar dentro de todos los sectores, con un 61%.

"No se debe pagar el rescate a los hackers", recalca Andrea Baggio, CEO EMEA HelpRansomware. De hecho, las organizaciones de atención médica que pagaron el rescate recuperaron solo el 65% de sus datos. Además, la comunicación con los ciberdelincuentes expone vulnerabilidad e interés por la

negociación.

El poder de la información en el ataque ransomware
"Hace unos cinco años, observamos un cambio de tendencia: algunas compañías no querían pagar porque eran conscientes de que, aunque lo hiciesen, no obtenían la data;

En ese instante, los piratas decidieron dar un paso más: extraer información importante y colgarla en la Deep Web", indica Juan Ricardo Palacio, CEO América HelpRansomware.

En páginas ubicadas en la Deep Web o Dark Web, venden los datos al mejor licitador o simplemente la ofrecen al público en general.

"El secuestro no es sacar la data, el secuestro es cifrar la data. Así impiden el acceso a la información", recalca Palacio.

Según los datos del Departamento de Salud y Servicios Humanos de EEUU, el coste por incidente de una filtración de datos en atención médica ha alcanzado los $10,10 millones.

En la era digital, el ransomware se ha convertido en un riesgo real para las empresas.

"Este virus produce una importante inactividad en las compañías, encriptando datos financieros, personales o patentes", concluye Baggio.

HelpRansomware ofrece una asistencia global de 24/7, garantizando el descifrado de datos, en un tiempo determinado y rápido. La empresa forma parte del grupo ReputationUP, multinacional especializada en la gestión de la reputación online.

Datos de contacto:
HelpRansomware
600790569

Nota de prensa publicada en: Castelló de la Plana, Castellón

Categorías: E-Commerce Software Ciberseguridad