Cómo protegerse de los ataques "ramsomware"

RESUMEN: El ramsomware es un software malicioso que se crea exclusivamente para dañar los equipos informáticos. Prohibiendo el acceso a todas o a determinadas partes de los archivos del sistema operativo infectado; pidiendo un rescate a cambio de la restricción.

CATEGORÍAS: CIBERSEGURIDAD

Nº HIPERVINCULOS: 2

El **ramsomware** es un software malicioso que se crea exclusivamente para dañar los equipos informáticos. Su traducción al castellano es "secuestro de datos", este software prohíbe el acceso a todas o a determinadas partes de los archivos del sistema operativo infectado; pidiendo un rescate a cambio de la restricción.

Su "modus operandi" es secuestrando los datos mediante la técnica de cifrado y realizando el robo de la información. Y lo que ofrece el **ciberdelicuente** a cambio de que pagues el rescate son las claves para poder descifrar de nuevo los datos.

Estos ataques son muy peligrosos, ya que su nivel de propagación es enorme y muy rápido. Pueden llegar a dejar inoperativos los sistemas informáticos de grandes empresas; como ocurrió el pasado año 2021 cuando hicieron un ataque al Servicio Público de Empleo Estatal (SEPE). Este suceso fue muy famoso y se prolongó durante varias semanas hasta poder arreglarlo.

Y otro gran problema es su coste. El coste de recuperación de un **ransomware** no es nada sencillo, ni rápido; es más bien, costoso y muy lento. La gran mayoría de empresas que han sufrido un ataque de este tipo han necesitado un mínimo de 2 o 3 días para poder recuperarse. Y estos han sido negocios con una buena base en ciberseguridad, que de no ser así pueden ser semanas o incluso meses con los dispositivos bloqueados.

¿Qué ocurre en el caso de que no accedas a pagar a los ciberdelicuentes?

Pues el primer punto al que debemos enfrentarnos es el de encontrarnos inoperativos, sin acceso a los sistemas de información. Lo que supone una gran pérdida de dinero para la empresa, ya que tiene que costear esas horas de los empleados que están parados y sin poder realizar ningún tipo de venta.

Luego por otro lado, se encuentra la recuperación total de los sistemas de información. Nos encontramos con la posibilidad de **no recuperar todos los datos al 100%.** En el mejor de los casos se dispondrá de un **backup** que deberá estar actualizado, y será de donde se podrá recuperar la información secuestrada; dependiendo de varios factores como tamaño, tecnología, lugar de almacenamiento, etc. Un proceso muy largo y costoso en el tiempo.

Por último, pero no por eso menos importante, el daño que le hace a la imagen de marca. Estos sucesos generan desconfianza a los clientes, da poca credibilidad de la seguridad de sus servicios y es posible que haya pérdidas en el negocio.

En el caso de que te hayan robado información, ponte en contacto con la Agencia Estatal de Protección de Datos que analizará el caso y dependiendo del alcance procederá a emitir una multa.

No queremos ser alarmantes, es solamente la realidad de las consecuencias y el impacto de este tipo de ataques.