RANSOMWARE

Importante...

Lamentablemente hemos recibido de dos importantes miembros de nuestra cartera de clientes que han sido atacado por un malware, específicamente del tipo ramsonware. Afectando notablemente su continuidad de negocios y cifrando el activo más importante de la casa de bolsa como lo es la información e incluso perdiendo la gran materia de estos. Muchos asumimos que con solo tener una solución de antivirus licenciada estamos blindados de cara a este tipo de secuestros cibernéticos, y nada se aleja más de la realidad que esta premisa. Las soluciones de antivirus son una parte de las herramientas que utilizamos para defendernos, básicamente la salud de nuestra información está en nuestras manos, asumir mayor responsabilidad al navegar, contar con apoyo de nuestros equipos tecnológicos para poder obtener sistemas operativos actualizados, estrategias de respaldos adecuadas son otros punto que conjugados pueden ofrecernos más seguridad.

¿Pero sabemos que el ransomware? El ransomware es un tipo de software malicioso se usa para extorsionar. Cuando un dispositivo logra ser atacado con éxito, el malware bloquea la pantalla o cifra la información almacenada en el disco y se solicita un rescate a la víctima con los detalles para efectuar el pago.

¿Cómo reconocer el ransomware?

Si te han atacado, el ransomware te mostrará en la mayoría de casos un mensaje de rescate en la pantalla, o añadiendo un archivo de texto (mensaje) de las carpetas afectadas. Muchas familias de ransomware también cambian la extensión de los archivos cifrados.

Todos los tipos de ransomware antes mencionados solicitan un pago y la mayoría de ellos piden que se realice en bitcoins o alguna otra criptomoneda difícil de rastrear. A cambio, los operadores prometen descifrar la información o restaurar el acceso al dispositivo afectado. Debemos resaltar que no existe ninguna garantía de que los cibercriminales cumplirán con su parte del trato (y algunas veces no pueden hacerlo, a propósito, o debido a problemas de codificación). Por lo tanto, LAsistemas recomienda NO pagar la suma solicitada, al menos no antes de contactar con su personal soporte técnico.

¿Pero cómo puedo mantenerme protegido?

Reglas básicas que deberías seguir para evitar perder tu información:

- Realiza copias de seguridad de tu información de forma periódica.
- Realiza múltiples copias de seguridad de tu información, no se recomienda solo realizas respaldos locales. Apóyate en herramientas de respaldos en líneas, MS Azure, Idrive, One Drive, Google Drive.
- Mantén tus programas actualizados – incluyendo el sistema operativo-, parcheados y en la última versión.
- Usa una red privada virtual (VPN).
- Utiliza contraseñas robustas y agenda cambios periódicamente de estas.

LAsistemas siempre procurando el bienestar de sus clientes les tiende la mano y les ofrece nuestros servicios de hospedaje en MS Azure que cuentan con todos los niveles de seguridad necesarios para mantener la continuidad de tu negocio. No dejes tu activo más preciado en manos inexpertas. Llámanos que podemos guiarte hacia el camino correcto, también puedes darles un vistazo a nuestros productos y ponerte en contacto con nosotros a través de nuestro portal web: https://lasistemas.com/nube-azure/ o a través de la dirección de correo soporte@lasistemas.com