RANSOMWARE

La Agencia de Seguridad, Ciberseguridad e Infraestructura (CISA) ha observado un aumento en los ataques de Ransomware en todo el mundo.

El *Ransomware* o **Secuestro de Datos** es un tipo de **software malicioso**, o **malware**, diseñado para **negar el acceso a un sistema informático o datos hasta que se pague un rescate**. El Ransomware generalmente se propaga a través de **correos electrónicos de phishing** o visitando sin saberlo un **sitio web infectado**.

El *Ransomware* puede ser devastador para un individuo o una organización. Cualquier persona con datos importantes almacenados en su computadora o red está en riesgo, incluidas las agencias gubernamentales o policiales y los sistemas de atención médica u otras entidades de infraestructura crítica. La **recuperación** puede ser un proceso difícil que puede requerir los servicios de un especialista de recuperación de datos acreditado, y algunas víctimas **pagan para recuperar sus archivos**. Sin embargo, **no hay garantía** de que las personas recuperen sus archivos si pagan el rescate.

CISA recomienda las siguientes precauciones para protegerse contra el *Ransomware*:

- **Actualice** el **software** y los **sistemas operativos** con los últimos parches. Las aplicaciones y los sistemas operativos **obsoletos** son el objetivo de la mayoría de los ataques.
- **Nunca** haga clic en **enlaces** ni abra **archivos adjuntos** en correos electrónicos no solicitados.
- Tenga especial cuidado con los archivos **adjuntos comprimidos** (ZIP, RAR, etc.)
- **Realice copias de seguridad** de datos de forma regular. Guárdelo en un dispositivo separado y guárdelo sin conexión.
- **Siga** prácticas seguras al navegar por Internet:

Además, las Organizaciones deben emplear las siguientes mejores prácticas:

- **Restringir** permisos de los usuarios para instalar y ejecutar aplicaciones de software, en otras palabras, aplicando el principio del **mínimo privilegio** a todos los sistemas y servicios. Restringir estos privilegios puede **evitar** que se ejecute malware o **limitar** su capacidad de propagarse a través de una red.

Si tienes preguntas, o necesitas información adicional, puedes escribir al área de seguridad de la información, con lzambrano@visanet.com.gt , jdepaz@visanet.com.gt o jcastellanos@visanet.com.gt

- Usar una **lista blanca** de aplicaciones para permitir que solo los **programas aprobados** se ejecuten en una red.
- **Habilitar filtros de spam** fuertes para evitar que los correos electrónicos de phishing lleguen a los usuarios finales y autentique el correo electrónico entrante para evitar la suplantación de identidad.
- **Escanee** todos los correos electrónicos entrantes y salientes para **detectar amenazas** y filtrar archivos ejecutables para que no lleguen a los usuarios finales.
- **Configure** firewalls para **bloquear el acceso** a direcciones IP maliciosas conocidas.
- Los ataques de Ransomware a menudo requieren que el elemento humano tenga éxito. Se debe **actualizar la capacitación** de los empleados en **reconocer amenazas cibernéticas, phishing y enlaces sospechosos**: los vectores más comunes para ataques de Ransomware.