¿ESTAMOS PREPARADOS ANTE UN ATAQUE INFORMATICO DE RANSOMWARE?

Como se pudo haber observado durante el último fin de semana, una nueva cepa de virus (del tipo Ransomware) ha sido liberado, ocasionando caos en los sistemas informáticos de todo el mundo. El Cyberataque de Wannacrypt (nombre del ransomware) ha tenido en vilo a la población mundial, y sus efectos aún todavía no han podido ser cuantificados debido a que no todo ha sido corregido o actualizado, y puede que algunos no sepan aún que lo tienen. Los expertos comentan incluso que se debe estar preparado ante un nuevo ataque porque como se sabe, este virus puede tener nuevas versiones y hacerse más fuerte.

Este virus, normalmente descargado a través de un archivo adjunto de correo electrónico, buscará archivos, tanto en su computadora como en los servidores, y los cifrará. El objetivo del criminal es que, para descifrarlos les envíes dinero (en la forma de una moneda digital llamada Bitcoin) para que puedan darles la contraseña y desbloquear los archivos. Hacer un pago a estos delincuentes no es lo más recomendable, ya que nunca se tendría la garantía de que le devuelvan las llaves o que les puedan volver a pedir un monto adicional para continuar con la extorsión.

Sin embargo, recomendamos tener en cuenta estos consejos y compartirlos dentro de sus equipos de trabajo, colegas y amigos;

1. **Asegurar de que sus sistemas estén completamente actualizados con los últimos parches de seguridad.** Microsoft y otros proveedores de tecnología son conscientes de las vulnerabilidades de su software y envían periódicamente actualizaciones que ayudan a corregir estas vulnerabilidades.

2. **Nunca hacer clic en un enlace, Pop-Up o abrir un archivo adjunto en un correo electrónico que no esté esperando.** Los correos electrónicos que contienen “requerimientos urgentes”, enlaces a “facturas, boletas, recibos” y archivos adjuntos con “información adicional” son las principales formas de propagación de estos virus. Al hacer clic en estos enlaces o abrir un archivo adjunto, se instalará un software en su computadora o dispositivo móvil que cifrará o destruirá datos en su equipo y en cualquier otros que se encuentre conectado (como por ejemplo la red interna o casera).

3. **Asegurar de que su software antivirus esté actualizado.** El software antivirus actualizado puede protegerlo de los virus, y por ello debe validar de que se actualiza de forma periódica y automática a fin de asegurarse de que el parche o la actualización está funcionando ya que algunos virus intentan desactivar el software antivirus.

4. **Realizar una copia de seguridad de su información.** Realizar una copia de seguridad regular de su información significará que, si sus archivos se cifran o destruyen, puede recuperar los archivos de la copia de seguridad obtenida. También deberá asegurarse de que estas copias de seguridad se comprueban regularmente. No lo olvide, sus datos son tan seguros como su última copia de seguridad.

5. **Aislar los equipos afectados por virus dentro de la empresa.** En caso de verse afectado con un virus, separe el equipo de la red de la empresa y asegúrese de hacer revisiones y escaneos de seguridad hasta eliminar completamente el riesgo.

6. **Crear conciencia de seguridad dentro de la empresa**. Involucrar a las Gerencias y áreas de la empresa en el conocimiento de temas relacionados con la Cyber Seguridad, comunicando con claridad que un ataque de virus informático podría detener las operaciones por un tiempo prolongado.

Hay herramientas automatizadas disponibles para el monitoreo y escaneo de todo el tráfico que llega a la red de nuestras organizaciones, y aunque estas por lo general están asociadas a un costo, se debe ver más bien como una inversión necesaria para asegurar la continuidad de las operaciones en las empresas.

Raúl Villanueva

GRC Manager en Mazars Perú