Copermática Software
SIEMPRE INNOVANDO

Tomelloso
P° San Isidro,13
Tfnos. 902 44 33 33
926 53 98 90
Fax: 926 51 46 87
13700 Tomelloso (CR)

Madrid
Orense, 85
Edificio Lexengton
Tfno. 902 44 33 33
28020 Madrid

Valencia
Avda. Cortes Valencianas 39, 1°Piso
Centro de Negocios Geminis Center
Tfno. 902 44 33 33
46015 Valencia

Sevilla
Gramil, 1
Tfno. 902 44 33 33
41008 Sevilla

copermatica@copermatica.com
www.copermatica.es

LAS 7 MEJORES PRÁCTICAS PARA PREVENIR Y MITIGAR ATAQUES RANSOMWARE.

¿Qué es Ransomware?

Ransomware es tan terrorífico como su nombre. Los hackers utilizan esta técnica para bloquear sus dispositivos y exigir un rescate a cambio de recuperar el acceso. El Ransomware le pone en una situación muy angustiosa, por lo que es mejor saber cómo prevenirlo.

Los ataques Ransomware se han incrementado hasta tal punto que ahora se han convertido en una de las principales amenazas a la estabilidad financiera, reputación y seguridad de los datos de la empresa. El problema es que los atacantes son más expertos en tecnología con el tiempo, y ya no requiere que una persona haga "clic" en un enlace para infectar su sistema.

Las webs legales ahora pueden contener código malicioso, software desactualizado u obsoleto que permite a los hackers corromper los sistemas de los usuarios finales.

Aunque hay opción de pagar a los hackers responsables de los ataques Ransomware, sólo sirve para alentarlos y no garantiza que tu red se salve de ataques futuros. Así que la mejor opción es prevenir y mitigar Ransomware.

I. **Formar a los empleados sobre acciones adecuadas durante los ataques Ransomware.** Similar a otro tipo de malware, Ransomware infecta a la mayoría de sistemas por vía descarga, archivos anexos en el correo electrónico, y las visitas a páginas de Internet. Es crítico para una empresa educar a los empleados a través de informarles sobre las trampas a evitar. Una vez que adviertes que tu seguridad ha sido comprometida y que Ransomware ha infectado tus sistemas, toma una acción inmediata:

   - Si es posible, antes de apagar el sistema, recupera información de la memoria
   - para investigar posteriormente el descifrado de los datos.
   - Apaga el sistema para detener la marea del ataque.
   - Intenta recordar el portador del ataque (correo electrónico, ...)
   - Notifica a las autoridades competentes para que inicien una investigación. Evita el acceso a cualquier servidor que utilice Ransomware.

Copermática Software
SIEMPRE INNOVANDO

Tomelloso
P° San Isidro,13
Tfnos. 902 44 33 33
926 53 98 90
Fax: 926 51 46 87
13700 Tomelloso (CR)

Madrid
Orense, 85
Edificio Lexengton
Tfno. 902 44 33 33
28020 Madrid

Valencia
Avda. Cortes Valencianas 39, 1°Piso
Centro de Negocios Geminis Center
Tfno. 902 44 33 33
46015 Valencia

Sevilla
Gramil, 1
Tfno. 902 44 33 33
41008 Sevilla

copermatica@copermatica.com
www.copermatica.es

II. **Realizar copias de seguridad del sistema de forma regular.** No hay ninguna solución más eficaz e infalible que la copia de seguridad de sus datos con regularidad, y la verificación de todo el sistema. Ransomware encripta ficheros, copias "sombra" y puntos de restauración de Windows. En efecto, bloquea todos los métodos de restaurar parcialmente los datos después de un ataque. Es primordial que almacene las copias de seguridad en un sistema diferente.

III. **Revisar los permisos del sistema**. Es una práctica importante ya que puede marcar la diferencia entre el inicio de ataques Ransomware y mitigar el impacto.

IV. **Mantener el software actualizado**. Una de las reglas más esenciales para proteger el sistema como la detección temprana del Ransomware, es asegurar que el software instalado en tu máquina se encuentra actualizado y mantenido de manera frecuente y consistente. Debes poner el foco principal en el software de seguridad y anti-malware (anti-virus).

V. **Protegerse ante correos corruptos.** Filtrar los correos correctamente reduce la posibilidad de un ataque con éxito de Ransomware. La mayoría de las veces, Ransomware se encuentra en un archivo adjunto ejecutable (archivos MS Office: Word, Excel, ..., ficheros zip, macros, ...)

VI. **Usar la administración inteligente de parches.** A través de procesos centralizados de la administración de parches se protege toda la empresa de forma más proactiva, evitando vulnerabilidades.

VII. **Asegurar la red**. Ejemplo es el uso de cortafuegos (firewalls), muy útil para redirigir o bloquear protocolos como el RDP (escritorio remoto) junto con otros servicios de administración de red, incluso iniciar el proceso de filtrado de correo no deseado para que no llegue a la bandeja de entrada de los usuarios.

El número de ataques Ransomware se incrementa con el paso del tiempo. Aunque las organizaciones gubernamentales y las agencias de aplicación de la ley trabajan juntas para manejar este problema de manera exhaustiva, lo mejor para una empresa es poner sus escudos para prevenir y mitigar el ataque Ransomware.

(Fuente: TechGenix - Benjamin Roussey – Septiembre 2017