www.mexis.net

ES POCO PROBABLE RECUPERAR DATOS CIFRADOS CON RANSOMWARE. PERO EXISTE OTRA OPCIÓN

Como examinador forense hay muchas opciones que con el paso del tiempo se han usado o intentado:

ingeniería reversa del ransomware, usar claves del mismo grupo que cifra los equipos en incidentes anteriores y hasta el análisis forense de la memoria para ver si se encuentra la llave. Todo esto ha dejado de funcionar.

No es un secreto que el ransomware se ha convertido en una de las amenazas digitales más desafiantes para las empresas. Estos ataques no solo paralizan las operaciones, sino que también ponen en riesgo la información crítica de la organización en caso de exfiltraciones como mecanismo para presionar por el pago del rescate. **Recuperar datos cifrados durante un ataque de ransomware es extremadamente difícil y, en muchos casos, imposible.**

Como examinador forense hay muchas opciones que con el paso del tiempo se han usado o intentado: ingeniería reversa del ransomware, usar claves del mismo grupo que cifra los equipos en incidentes anteriores y hasta el análisis forense de la memoria para ver si se encuentra la llave. **Todo esto ha dejado de funcionar.**

En este contexto, una estrategia efectiva que puede marcar la diferencia es respaldar la información cifrada.

Según el “Informe de Tendencias de Ransomware 2024” de Veeam, **solo el 57% de las empresas logra recuperar sus datos después de un ataque de ransomware,** lo que deja a muchas organizaciones vulnerables a una pérdida sustancial de información y un impacto negativo en sus negocios.

Obviamente la recomendación siempre será tener respaldos, **¿pero si no se tienen?**

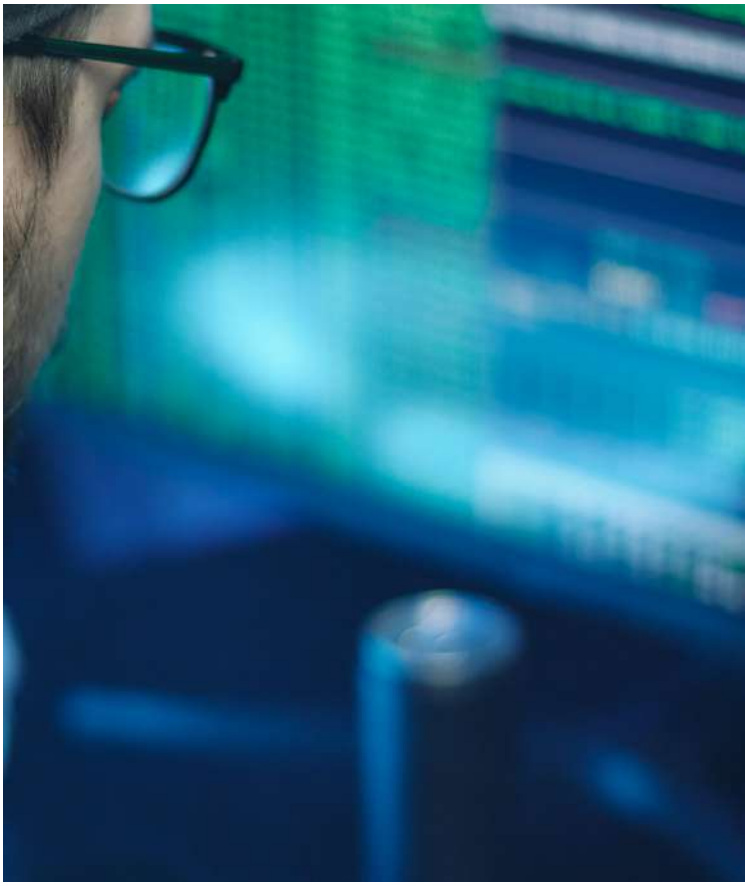
Uno de los ejemplos más recientes y relevantes es el caso LockBit, **un grupo de ransomware que ha sido responsable de miles de infecciones en los últimos años.**

Afortunadamente, el 19 de febrero de 2024, las autoridades tomaron medidas para desmantelar la infraestructura de ransomware como servicio (RaaS) de LockBit. Esta operación, conocida como Operación Cronos, **resultó en la incautación de más de 11,000 dominios y 34 servidores, así como en la recuperación de más de 7,000 claves de descifrado. E**ste tipo de intervención muestra cómo una acción coordinada puede tener un impacto significativo en la lucha contra el ransomware, permitiendo a muchas víctimas recuperar sus datos sin pagar el rescate.

Mantener una copia de la información cifrada puede parecer una medida contradictoria, pero es crucial para la recuperación futura. Cuando las autoridades logran obtener las claves de descifrado, las empresas que han guardado copias de sus datos cifrados pueden recuperar su información de manera efectiva.

Además, estas copias son esenciales para las investigaciones forenses, ayudando a los expertos en ciberseguridad a entender mejor el ataque, identificar a los atacantes y prevenir futuros incidentes.

Guardar estas copias también puede ser un requisito legal en muchos casos, asegurando que las empresas cumplan con las regulaciones y puedan proporcionar evidencias si es necesario.



Un playbook dentro del proceso de respuesta a incidentes en ciberseguridad es un conjunto de procedimientos y estrategias predefinidas que guían dicha respuesta. Estos documentos detallan los pasos a seguir en caso de un ciberataque, asegurando que todas las acciones sean coherentes y efectivas. **Incluir la estrategia de respaldar la información cifrada en el playbook de respuesta a incidentes puede mejorar significativamente las posibilidades de recuperación después de un ataque de ransomware.** Un buen playbook no solo proporciona un plan, sino que también garantiza que todos en la organización estén alineados y preparados para actuar rápidamente en momentos de crisis.

La alta administración debe estar preparada para tomar decisiones críticas, como si pagar o no el rescate, pero también para evaluar si su equipo de ciberseguridad está listo para enfrentar un ataque de ransomware. **Por ello, aquí hay algunas preguntas clave que pueden ayudar a determinar el nivel de preparación del equipo o para poder incentivar que se realicen cambios importantes:**

- **¿Tenemos un playbook de respuesta a incidentes que incluya estrategias para manejar ataques de ransomware?** Es fundamental tener procedimientos claros y bien documentados que guíen la respuesta del equipo durante un incidente.

- **¿Tenemos apoyo externo para atender un incidente que sea más grande de lo que podemos atender?** El contar con especialistas externos que no sean únicamente administradores de tecnología de ciberseguridad es un gran diferenciador.

- **¿Guardamos copias de seguridad regulares y también copias de los datos cifrados en caso de un ataque?** Asegurarse de que las copias de seguridad incluyan datos cifrados puede ser crucial para la recuperación posterior.

- **¿Estamos en contacto con servicios especializados de respuesta a incidentes que puedan asistir en caso de un ataque?** Contar con el apoyo de expertos externos puede proporcionar conocimientos y herramientas adicionales para manejar situaciones complejas.

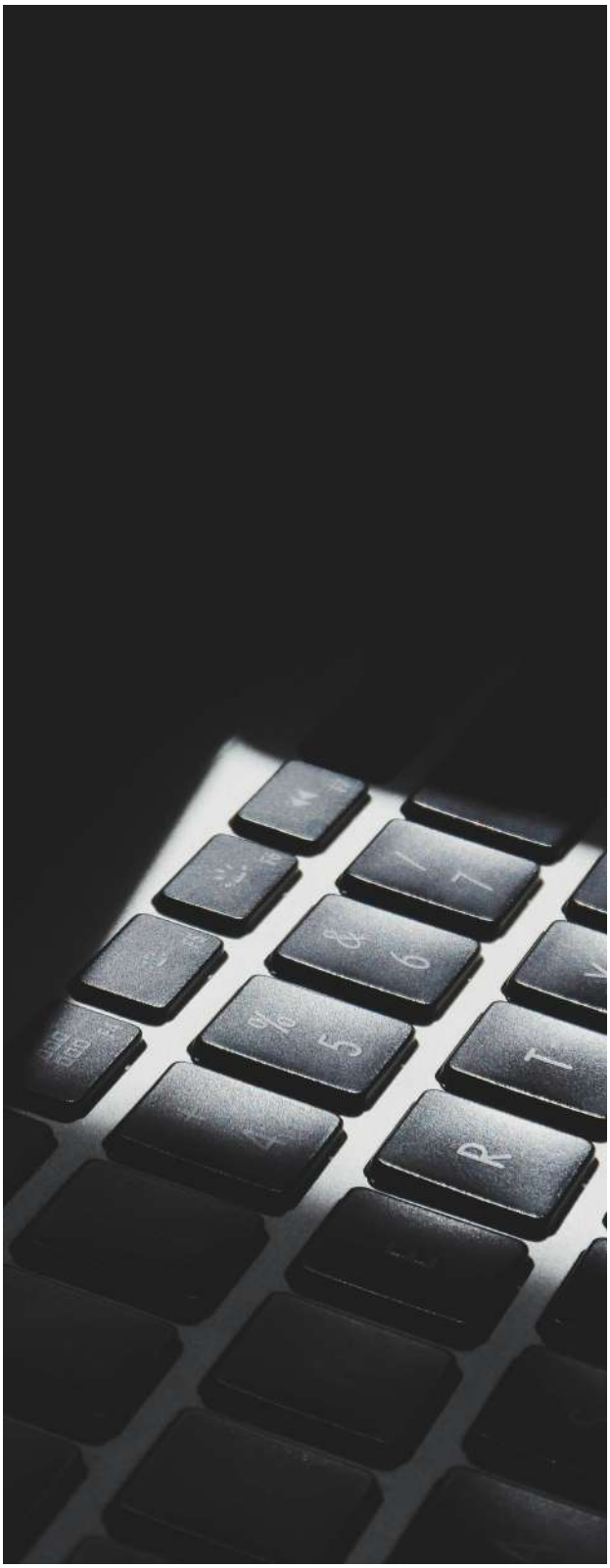
- **¿Hemos considerado las implicaciones legales y de cumplimiento relacionadas con un ataque de ransomware?** Es importante estar al tanto de las regulaciones y asegurarse de que todas las acciones cumplan con los requisitos legales.

La recomendación general es no pagar el rescate, ya que no garantiza la recuperación de los datos y puede alentar a los atacantes a seguir con sus actividades delictivas. También hay que considerar que el Departamento de Justicia de los Estados Unidos así como otras agencias en dicho país han señalado que el pagar rescates podría violar las leyes de sanciones y **han advertido que aquellos que paguen podrían ser acreedores a sanciones.** Esto no ha sucedido hasta el momento.

Sin embargo, la decisión final debe basarse en una evaluación cuidadosa de la situación y las capacidades de recuperación disponibles. **Es crucial que la alta administración tenga un entendimiento claro de las implicaciones y esté preparada para tomar decisiones informadas bajo presión.**

Recuperar datos cifrados durante un ataque de ransomware es un desafío significativo. Respaldar la información cifrada y estar preparado con un playbook bien definido puede marcar la diferencia en la capacidad de una empresa para recuperarse de un ataque.

La capacidad de una empresa para responder eficazmente a un ataque de ransomware puede determinar su supervivencia. La preparación no solo implica tener las herramientas y tecnologías adecuadas, sino también contar con el apoyo de expertos que puedan guiar y asesorar durante y después de un incidente.



Fuente de información: forbes.com
Autor: Andrés Velázquez