Por qué pagar el rescate debería ser su última opción

Imagine despertarse para encontrar todo el mundo digital de su empresa oculto detrás de un mensaje ominoso que exige el pago. Esta es la realidad del ransomware, una amenaza cibernética creciente que afecta tanto a empresas como a personas, y a menudo las deja con una opción difícil: pagar el rescate o arriesgarse a perder datos críticos.

A pesar de los esfuerzos internacionales para contenerlos, los ataques de ransomware han aumentado en los últimos años, lo que les costó a las víctimas miles de millones y alteró las operaciones en todas las industrias. La decisión de pagar es tentadora, especialmente cuando los medios de subsistencia, la reputación y los datos sensibles se encuentran en el equilibrio. Sin embargo, pagar el rescate no es una solución garantizada y puede crear más problemas de

los que resuelve.

En esta publicación, analizaremos por qué pagar el rescate no debería ser su única opción y, de hecho, debería ser probablemente su última opción. Exploraremos los riesgos de ceder a los atacantes, destacaremos la importancia de las defensas proactivas y describiremos estrategias alternativas para recuperarnos del ransomware sin financiar a los ciberdelincuentes.

Los riesgos de pagar el rescate

Pagar un rescate después de un ataque de ransomware puede parecer la salida más fácil y el camino más rápido hacia la recuperación, pero viene con riesgos significativos que a menudo superan los posibles beneficios.

Sin garantía de recuperación de datos

Una de las realidades más alarmantes de pagar un rescate es que no hay certeza de que recuperará sus datos. Los estudios demuestran que hasta el 35 % de las víctimas que pagan nunca reciben las claves de descifrado prometidas, lo que las deja con datos perdidos y una pérdida financiera. En algunos casos, las herramientas de descifrado proporcionadas son ineficaces, lo que hace que las víctimas no puedan restaurar completamente sus sistemas. Por ejemplo, el ataque de 2021 a Colonial Pipeline llevó a un pago de rescate de 4,4 millones de USD, pero incluso después de recibir la herramienta de descifrado, la empresa tuvo dificultades con su rendimiento lento e incompleto. Esta demora destacó que pagar no siempre es la solución rápida que las víctimas esperan.

Mayor probabilidad de futuros ataques

Pagar el rescate puede marcarlo como un objetivo fácil para ataques futuros. Los ciberdelincuentes a menudo comparten listas de víctimas que han pagado rescates, rotulándolas como “pagadores dispuestos”. De hecho, el 80 % de las organizaciones que pagan rescates son golpeadas nuevamente, a veces por el mismo grupo o por otros atacantes oportunistas.

Implicaciones éticas y legales

Cuando paga un rescate, está financiando directamente a organizaciones criminales, lo que les permite mejorar sus capacidades y apuntar a más víctimas. Muchos grupos de ransomware tienen vínculos con actividades ilícitas más amplias, incluido el terrorismo, el tráfico de personas y el contrabando de armas. Pagar el rescate perpetúa estas redes y sus impactos perjudiciales. Además, pagar un rescate podría ponerlo en peligro legal. Los gobiernos de países como los EE. UU. han advertido que el pago de rescates a entidades vinculadas a organizaciones sancionadas puede violar las leyes.

Costos ocultos más allá del rescate

Incluso si recupera el acceso a sus datos, el pago de rescate suele ser solo el comienzo de la consecuencia financiera. Con frecuencia, las empresas enfrentan costos relacionados con el tiempo de inactividad, la restauración del sistema, la pérdida de ingresos y el daño a la reputación.

Estrategias alternativas a considerar

Estas alternativas pueden ayudarlo a mitigar el daño, recuperar el control y prevenir ataques futuros, todo sin financiar a ciberdelincuentes.

las copias de seguridad

Una de las formas más confiables de recuperarse del ransomware y evitar tener que pagar es restaurar sus sistemas y datos de copias de seguridad seguras. Las organizaciones que mantienen estrategias de copia de seguridad sólidas a menudo se recuperan más rápidamente y con menos impactos a largo plazo.

Las copias de seguridad sirven como una red de seguridad digital, lo que le permite restaurar datos y sistemas críticos sin sucumbir a las demandas de rescate. Cuando un ataque de ransomware encripta sus archivos, las copias de seguridad proporcionan una copia no infectada de sus datos, lo que le permite:

- Restaure rápidamente las operaciones.
- Minimice el tiempo de inactividad y las pérdidas financieras.
- Evite pagar el rescate y alimentar el delito cibernético.

Por ejemplo, las empresas con sistemas de copia de seguridad robustos a menudo se recuperan en días o incluso horas, mientras que las que no tienen copias de seguridad pueden enfrentar semanas de interrupciones y costos cada vez más elevados.

Consejos para configurar y mantener copias de seguridad eficaces

1. Siga la regla 3-2-1

La estrategia de copia de seguridad 3-2-1 ampliamente recomendada garantiza que sus datos estén bien protegidos:

- Conserve tres copias de sus datos.
- Almacénelos en dos tipos diferentes de medios (p. ej., unidades externas, almacenamiento en la nube).
- Mantenga una copia fuera del sitio o fuera de línea para protegerla de los ataques de ransomware.

2. Programe copias de seguridad automáticas

La automatización de las copias de seguridad garantiza que no se pierdan datos críticos. Configure copias de seguridad diarias o semanales según el volumen y la importancia de sus datos.

3. Pruebe sus copias de seguridad regularmente

Las copias de seguridad solo son útiles si funcionan cuando las necesita. Realice restauraciones de prueba regulares para verificar que sus datos estén completos y que su proceso de recuperación sea efectivo.

4. Cifre los datos de la copia de seguridad

Proteja las copias de seguridad del acceso no autorizado encriptándolas, especialmente si se almacenan en la nube o en dispositivos portátiles.

5. Implemente el control de versiones

Use copias de seguridad con versiones para conservar varias copias de sus datos. Esto garantiza que pueda restaurar una versión no infectada incluso si se vieron comprometidas las copias de seguridad recientes.

Protección del almacenamiento fuera de línea: Su última línea de defensa

Un paso crítico es almacenar las copias de seguridad en una ubicación segura y fuera de línea, completamente desconectada de su red principal. Este enfoque de "espacio libre de aire" garantiza que el ransomware no pueda encriptar sus copias de seguridad junto con sus archivos activos.

Por ejemplo, algunas organizaciones utilizan almacenamiento de escritura una vez leída y muchas (WORM), lo que evita que los datos se alteren después de guardarlos. Otros confían en dispositivos dedicados fuera de línea que solo están conectados durante las ventanas de copia de seguridad programadas.

Herramientas de descifrado

Las herramientas de descifrado están diseñadas para revertir el cifrado utilizado por variantes específicas de ransomware, lo que les da a las víctimas la oportunidad de recuperar el acceso a sus archivos sin financiar a

ciberdelincuentes.

En algunos casos, hay herramientas de descifrado gratuitas disponibles para variantes específicas de ransomware. Las organizaciones de ciberseguridad y coaliciones como No More Ransom proporcionan estas herramientas, que son desarrolladas por expertos que han descifrado el cifrado de ransomware. Antes de pagar, verifique si existe una solución para el ransomware con el que está lidiando.

Cómo usar las herramientas de descifrado

1. Identifique la variante de ransomware

Antes de usar una herramienta de descifrado, es fundamental identificar la cepa de ransomware que afecta su sistema. Las herramientas como Ransomware de ID le permiten cargar la nota de rescate o el archivo cifrado para determinar el tipo de ransomware.

2. Descargue la herramienta correcta

Visite una fuente de confianza para descargar la herramienta correspondiente a su variante de ransomware. Evite los sitios web aleatorios, ya que algunos pueden distribuir herramientas falsas que comprometan aún más su sistema.

3. Siga las instrucciones

Cada herramienta viene con instrucciones específicas. Por lo general, esto incluye instalar el software, escanear su sistema y seleccionar los archivos cifrados para el descifrado. Asegúrese de que su sistema esté aislado de la red para evitar la reinfección durante este proceso.

Limitaciones y riesgos de las herramientas de descifrado

No todas las variantes de ransomware tienen herramientas de descifrado

disponibles públicamente. Los ciberdelincuentes evolucionan constantemente sus métodos de encriptación, lo que dificulta que los investigadores desarrollen herramientas para cepas más nuevas.

Incluso con una herramienta de descifrado, no hay garantía de recuperación total de datos. Algunos archivos pueden permanecer corruptos o parcialmente descifrados, especialmente si el proceso de encriptación fue interrumpido o mal ejecutado por el propio ransomware.

Los ciberdelincuentes a veces crean herramientas de descifrado falsas para explotar aún más a las víctimas. Solo utilice herramientas de fuentes confiables para evitar daños adicionales.

Por último, las herramientas de descifrado solo abordan el problema inmediato de acceder a sus datos. No protegen su sistema ni eliminan las vulnerabilidades que provocaron el ataque.

Servicios profesionales

Involucrar a los profesionales de ciberseguridad puede ser crucial para administrar un ataque de ransomware. Estos expertos pueden evaluar el alcance del ataque, poner en cuarentena los sistemas afectados para evitar una mayor propagación, ayudar a restaurar las operaciones de manera segura e identificar vulnerabilidades. La ayuda profesional a menudo reduce el tiempo de inactividad y garantiza una respuesta integral al ataque.

Los profesionales externos pueden ofrecer:

- **Conocimiento y experiencia expertos:** Los profesionales de ciberseguridad se ocupan del ransomware y otras amenazas cibernéticas de forma regular, lo que les brinda una comprensión profunda de cómo responder de manera eficiente. Están familiarizados con las últimas variantes de ransomware, vectores de ataque y métodos de recuperación.
- **Resolución más rápida:** Los profesionales pueden evaluar rápidamente

la situación e implementar una respuesta estructurada, reduciendo el tiempo de inactividad y limitando la interrupción operativa.

- **Asistencia integral:** Más allá de la recuperación inmediata, los expertos proporcionan información sobre cómo ocurrió el ataque, lo que ayuda a abordar las vulnerabilidades y mejorar las defensas.

Servicios ofrecidos por profesionales de ciberseguridad

Los profesionales de ciberseguridad ofrecen una variedad de servicios, entre ellos:

1. Análisis forense

Los profesionales investigan cómo el ransomware infiltró su sistema. Identifican vulnerabilidades, ya sea a través de phishing, contraseñas débiles o software obsoleto, para evitar que vuelvan a ocurrir.

2. Recuperación de datos

Los expertos utilizan herramientas avanzadas para intentar la restauración de datos, incluida la recuperación de archivos no cifrados o parcialmente cifrados. En algunos casos, pueden ayudar a usar de manera segura herramientas de descifrado legítimas.

3. Cuarentena y restauración del sistema

Los profesionales aíslan los sistemas afectados para evitar que el ransomware se propague. Trabajan para restaurar los sistemas al estado operativo y, al mismo tiempo, garantizan que no quede malware residual.

4. Comunicación e informe de incidentes

Muchas empresas ayudan a informar el ataque a organismos reguladores o de aplicación de la ley. También pueden ayudar a redactar la comunicación para las partes interesadas, minimizando el daño a la reputación.

5. Fortalecimiento de la seguridad

Después de abordar el problema inmediato, los expertos ayudan a fortalecer sus defensas. Esto puede incluir la implementación de la protección del endpoint, la configuración de sistemas de detección de intrusos y la capacitación de los empleados sobre las mejores prácticas de ciberseguridad.

Elegir una empresa de ciberseguridad de buena reputación

Al seleccionar una empresa de ciberseguridad, asegúrese de buscar empresas con certificaciones como CISSP, CEH o CISM. Verifique su experiencia con los incidentes de ransomware y la recuperación. También debe pedir referencias o ejemplos de casos similares que hayan manejado y buscar reseñas o recomendaciones de fuentes confiables.

Pregunte cómo manejan los incidentes de ransomware, incluida su postura sobre el pago de rescates.

Ransomware requieren atención inmediata, así que elija una empresa con disponibilidad las 24 horas del día, los 7 días de la semana. Asegúrese de que tengan un proceso estructurado para responder rápidamente a las emergencias.

Por último, debe solicitar un desglose claro de los costos y lo que se incluye en su paquete de servicios. Tenga cuidado con las empresas que requieren grandes pagos iniciales sin explicar sus métodos.

Qué esperar de sus servicios

- **Evaluación inicial:** Una revisión exhaustiva del ataque de ransomware, incluido su alcance e impacto.
- **Plan de acción:** Un plan de recuperación y mitigación paso a paso adaptado a su situación
- **Actualizaciones periódicas:** Comunicación transparente sobre el progreso y los hallazgos
- **Medidas de seguimiento:** Recomendaciones posteriores al incidente para fortalecer la ciberseguridad y reducir los riesgos futuros

Fortalecimiento de su seguridad cibernética

La mejor ofensa contra el ransomware es una buena defensa. La implementación de medidas proactivas de ciberseguridad no solo reduce el riesgo de sufrir ataques, sino que también minimiza los posibles daños si ocurre un incidente.

Asegúrese de:

Mantenga actualizados el software y los sistemas: Aplique regularmente parches y actualizaciones para solucionar vulnerabilidades en sistemas operativos, aplicaciones y firmware. Habilite las actualizaciones automáticas siempre que sea posible para garantizar que sus sistemas estén siempre protegidos.

Use contraseñas seguras y únicas: Cree contraseñas complejas con una combinación de letras, números y símbolos. Evite reutilizar contraseñas en varias cuentas. Use un administrador de contraseñas para generar y almacenar contraseñas seguras.

Implemente la autenticación multifactor (MFA): Agregue un nivel adicional de seguridad al requerir una segunda forma de verificación, como un código enviado a su teléfono o autenticación biométrica.

Educar a los empleados sobre la ciberseguridad: Capacite al personal para que reconozca los correos electrónicos de phishing y los enlaces sospechosos. Realice simulacros regulares y sesiones de concientización para reforzar los

buenos hábitos de ciberseguridad. Enfatice la importancia de informar las posibles amenazas de inmediato.

Restrinja el acceso a datos confidenciales: Implemente controles de acceso basados en roles (RBAC) para limitar quién puede ver o modificar archivos críticos. Use el principio de privilegio mínimo, que les otorga a los usuarios acceso solo a los datos y sistemas necesarios para su función.

Realice copias de seguridad de los datos regularmente: Mantenga copias de seguridad seguras y sin conexión como una protección contra fallas contra ataques de ransomware. Pruebe los procesos de copia de seguridad y recuperación periódicamente para garantizar la funcionalidad.

Desarrolle una cultura de ciberseguridad: Asegúrese de que la gerencia priorice e invierta en medidas de ciberseguridad. Realice evaluaciones periódicas de vulnerabilidades y pruebas de penetración para identificar puntos débiles. Desarrolle y pruebe un plan de respuesta detallado para minimizar la confusión durante un ataque.

Conclusiones

Ransomware son una amenaza cada vez más generalizada, con el potencial de interrumpir vidas y negocios. Sin embargo, como hemos analizado, pagar el rescate no es su única opción y debería considerarse el último recurso después de que haya agotado todas las demás opciones. El pago conlleva riesgos significativos, desde la recuperación de datos poco confiables hasta las consecuencias éticas y legales.

En cambio, adoptar estrategias alternativas puede conducir a resultados más seguros y sustentables. Restaurar las copias de seguridad regulares y seguras, utilizar herramientas de descifrado y buscar ayuda de profesionales de ciberseguridad son solo algunas de las formas de recuperarse sin recompensar a los ciberdelincuentes. Las medidas proactivas, como actualizar software, usar contraseñas seguras e invertir en herramientas de seguridad avanzadas como firewalls y sistemas de detección de intrusos, son igualmente vitales para la prevención.

La conclusión clave es clara: La mejor defensa contra el ransomware es una combinación de preparación, resistencia y un plan de respuesta bien estructurado. Al seguir estos pasos ahora, puede proteger sus datos y sistemas, reducir su vulnerabilidad y asegurarse de estar equipado para manejar un ataque en caso de que ocurra uno.

Recuerde que el ransomware prospera con la falta de preparación. No espere a que un ataque actúe, fortalezca sus defensas hoy.