CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Libreto para Ransomeware

Cómo prepararse para responder a y recuperarse de un ataque de Ransomeware (*secuestro de datos)

Para el 2021

“cada 11 segundos”

una nueva organización será víctima de un ataque de secuestro de datos, según el investigador de mercado Cybersecurity Ventures.[1]

El libreto de Ransomware

¿Pagar o no pagar? Esta es a menudo la primera pregunta que muchas organizaciones consideran después de ser golpeadas con un ataque de secuestro de datos.

Desafortunadamente, la elección no es sencilla. Muchas organizaciones simplemente no saben cómo protegerse contra el ataque. Esta guía tiene por objeto proporcionar una hoja de ruta para las organizaciones (por ejemplo, las pequeñas y medianas empresas y los gobiernos estatales y locales) para protegerse de esta creciente amenaza.

[1] umbrella.cisco.com/blog/2019/12/17/ransomware-defense-for-dummies-2nd-edition

Todas las organizaciones corren el riesgo de tener sus valiosos datos - sobre los clientes, empleados, operaciones - encriptados por un actor malicioso para que la organización pierde el acceso a ellos. **Un ataque de secuestro de datos es llevado a cabo por un actor malicioso para mantener los datos de una organización como rehenes contra el pago de un rescate.** Los actores malintencionados pueden ganar el acceso a los datos de una organización a través de diversos medios, incluido el phishing y/o los softwares no actualizados (sin parches). Los parches son emitidos por las compañías de software para vulnerabilidades que encuentran en sus programas; muchos usuarios no descargan los parches, lo que significa que las vulnerabilidades pueden ser explotadas.

Una organización que construye una cultura de preparación cibernética puede ser resistente contra un ataque de secuestro de tatos tomando acciones preventivas (por ejemplo, creando una copia de seguridad de datos críticos) y desarrollando y probando un plan de respuesta a incidentes de este tipo. Una organización debe centrarse en tres pasos: **Preparar, responder y recuperar.**

PASO 1

Prepara

PASO 2

Responde

PASO 3

Recupera

Prepara

Asegúrate de que tu empresa haga regularmente una copia de seguridad de sus datos; el almacenamiento de datos en la nube es una herramienta común utilizada para las copias de seguridad. Si tus empleados guardan información importante en sus propias computadoras, tu organización también debería dar instrucciones claras a los empleados sobre cómo hacer copias de seguridad de sus datos de manera regular. Elementos clave para protegerse del secuestro de datos incluyen:

- Priorizar los datos que son más críticos para su organización y hacer una copia de seguridad. Asegúrate de que puedes reinstalar desde las copias de seguridad, que a menudo están en la nube, y que las copias de seguridad se prueban con frecuencia.
- La detección temprana es importante, así que asegúrate de que tu fuerza laboral sepa cómo reportar un posible incidente de rescate o un comportamiento inusual en la red.
- En lo posible, contratar un proveedor que pueda proporcionar apoyo de respuesta si ocurre un incidente. Establecer un contrato antes del evento para que tenga acceso al vendedor inmediatamente.

Dado que los agentes malintencionados suelen utilizar el phishing para infectar un sistema con un ataque de secuestro de datos, es crucial tener una política contra el phishing. Llevar a cabo una rutina de prueba de phishing para que los empleados sean capaces de detectar un correo electrónico de phishing antes de hacer clic en cualquier enlace o archivos adjuntos peligrosos y, en lo posible, usar un programa de software anti-phishing.

Actualiza tu software con la últimos parches de seguridad. Este paso preventivo crítico hace más difícil que los actores maliciosos comprometan su sistema.

Desarrollar una política a nivel de toda la organización con respecto a ataques de secuestro de datos. Es mucho más fácil tener estas discusiones cuando la presión de la respuesta no está ya encima. Preguntas a considerar: ¿Qué datos son más críticos para su organización? ¿Cubre su seguro el rescate? ¿Está de acuerdo con el pago de un rescate? Si es así, ¿entiende cómo usar bitcoin y/o otras monedas encriptadas?

Discutir y acordar una política en relación con los ataques de secuestro de datos para toda la organización. **Es mucho más fácil tener estas discusiones cuando la presión de la respuesta no está ya encima.**

¿Son los datos críticos **para sus operaciones?**

¿Se ha predeterminado que está **bien pagar un rescate?**

¿El rescate está cubierto por su **seguro?**

Responde

Si un empleado o la organización se enfrenta a una solicitud de rescate, su organización debe evaluar primero la legitimidad de la solicitud de rescate contactando con su director de informática. Si es legítima, se presentan dos posibles escenarios:

1 **Su organización tiene copias de seguridad que funcionan. No tienes que preocuparte por el rescate. Restaura tus datos completamente y vuelve al trabajo.**

2 **Los datos que tienen como rehenes son necesarios y no hay copias de seguridad que funcionen.**

a. Comprobar si los datos existen en algún otro lugar de la organización (por ejemplo, archivos de caché, correo electrónico) para que pueda “grabar” los datos para reemplazar lo que está siendo retenido como rehén e

b. Si no puede acceder a los datos en otro lugar, haga las siguientes preguntas:

- ¿Es la información crítica para sus operaciones?
- ¿Su organización ha predeterminado que está bien pagar un rescate?
- ¿Su seguro lo cubre?

Recuperar

El fuego se ha apagado y es hora de volver a la normalidad. El alcance del ataque del secuestro de datos y la gravedad de su impacto en sus operaciones diarias determinará cuánto tiempo y esfuerzo se necesita para recuperarse. Usar el incidente como una experiencia de aprendizaje para reforzar la importancia de los principios de la preparación cibernética como son la actualización del software (parches) y la conciencia del phishing.

Asegurarse de que su software esté siempre actualizado con los últimos parches de seguridad hará que sea más difícil de penetrar tu sistema. De la misma manera, hacer cumplir el entrenamiento rutinario sobre phishing minimiza el error humano y los posibles puntos de entrada en tu sistema. Como con cualquier violación de la seguridad, notifique a todas las partes afectadas, restablezca los ID de usuario y las contraseñas de todos los dispositivos comprometidos, actualice el software en todos los dispositivos, y reinstale los datos de las copias de seguridad una vez que la amenaza de secuestro de datos haya sido neutralizada.

Es especialmente importante asegurarse de que los parches sean actualizado después del ataque. Si los datos han sido restaurados, a veces las vulnerabilidades que fueron parcheadas antes del rescate pueden reaparecer.

El Programa de Preparación Cibernética incluye instrucciones y plantillas para ayudarte a crear tu propia políticas y plan de respuesta a incidentes para prepararse, responder y recuperarse de un ataque de secuestro de datos. Regístrese gratis en **BeCyberReady.com**.

Para leer sobre ejemplos reales de cómo las empresas y entidades gubernamentales respondieron a un ataque de secuestro de datos, por favor visite: **Noticias de Preparación Cibernética.**

El Programa de Preparación Cibernética incluye instrucciones detalladas y plantillas para ayudarle a crear sus propias políticas y plan de respuesta a incidentes para prepararse, **responder y recuperarse de un ataque de secuestro de datos.**

Guía de decisión de Ransomware

PREPÁR

¿Has priorizado tus datos y sistemas para saber qué es lo mas importante para tus operaciones comerciales?

¿Tienes un plan de respuesta a incidentes que cubra el ransomware?

Identifica lo que es más valioso. Ve a **BeCyberReady.com** para acceder a una lista de verificación de prioridades.

¿Tienes una copia de seguridad actual?

Desarrolla un plan de respuesta a incidentes que cubra el rescate. Ve a **BeCyberReady.com** para acceder a una plantilla de plan de respuesta a incidentes.

¿Lo has probado en el último mes?

Haz una copia de seguridad de tu sistema y todos los datos.

Felicitaciones. **Estás preparado.**

Prueba tu copia de seguridad para asegurarte de que puedes recuperar tus datos, especialmente los más críticos para tus operaciones comerciales.

Ojalá no sufras un ataque de secuestro de datos. **No estás realmente preparado.**

⚠ Ocurre un incidente de secuestro de datos ⚠

RESPON

Aísla el incidente y elimina el ordenador o ordenadores infectados de la red. Luego proceda.

Buen trabajo. **¡Ve directamente a Recuperación!**

¿Tienes un soporte informático para contactar?

¿Puedes o tu soporte informático hacer una copia de seguridad en tiempo real?

¿Son los datos retenidos como rehenes valiosos para su negocio?

¿Tienes un contra seguro ransomware?

¿Tu póliza cubre los eventos de rescate?

Tus datos son irrecuperables… **decidir si pagar o no.**

RECUP

Entra en la copia de seguridad en tiempo real y limpia el malware.

Reiniciar los ID's de usuarios y cambia las contraseñas

Haz una instalación limpia de tu copia de seguridad

Actualiza tu software

Reinstala los datos selectivamente

¡Estás operacional de nuevo! Regístrate en el programa gratuito Cyber Readiness Programa en **BeCyberReady.com** para evitar más ataques de secuestro de datos en el futuro.

CYBERREADINESSINSTITUTE.ORG

guide@cyberreadinessinstitute.org