CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Manual de estrategias para actuar ante ataques de ransomware

Cómo prepararse, responder y recuperarse ante un ataque de ransomware

En 2021

“cada 11 segundos”

una nueva organización
será víctima de ransomware,
según el investigador de mercado Cybersecurity Ventures. [1]

Manual de estrategias para actuar ante ataques de ransomware

¿Pagar o no pagar? Esta pregunta es a menudo la primera que muchas organizaciones se plantean después de sufrir un ataque de ransomware.

Por desgracia, la elección no es sencilla. Muchas organizaciones simplemente no saben cómo protegerse contra el ransomware. Esta guía tiene como objetivo proporcionar una hoja de ruta para que las organizaciones (por ejemplo, pequeñas y medianas empresas, Gobiernos estatales y locales) se protejan contra esta creciente amenaza.

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

Todas las organizaciones corren el riesgo de que un actor maligno cifre sus datos de gran valor (sobre clientes, empleados, operaciones) para que la organización pierda el acceso a ellos. **Un ataque de ransomware lo lleva a cabo un agente maligno para retener los datos de una organización a cambio de un rescate.** Estos actores malignos pueden acceder a los datos de una organización a través de distintos medios, incluido el phishing y el software sin parches. Las empresas de software emiten parches para las vulnerabilidades que encuentran en sus programas; muchos usuarios no se descargan los parches, lo que significa que otras partes malintencionadas pueden aprovechar las vulnerabilidades.

Una organización que crea una cultura de preparación cibernética puede resistir a un ataque de ransomware adoptando medidas preventivas (por ejemplo, creando una copia de seguridad de los datos críticos) y desarrollando y probando un plan de respuesta ante incidentes de ransomware. Una organización debe centrarse en tres pasos: **prepararse, responder y recuperarse.**

PASO 1:

Prepararse

PASO 2:

Responder

PASO 3:

Recuperarse

guide@cyberreadinessinstitute.org

Prepararse

Asegúrese de que su empresa realice copias de seguridad de sus datos de forma habitual; el almacenamiento de datos en la nube es una herramienta que se suele utilizar para realizar copias de seguridad. Si sus empleados guardan información comercial importante en sus propios ordenadores, su organización también debe proporcionar instrucciones claras a sus empleados sobre cómo realizar copias de seguridad de sus datos de manera habitual. Entre los elementos clave para protegerse contra el ransomware se incluyen los siguientes:

- Dé prioridad a los datos más importantes para su organización y realice una copia de seguridad. Asegúrese de poder volver a instalarlos a partir de las copias de seguridad, que a menudo se encuentran en la nube, y de que las copias de seguridad se someten a pruebas con frecuencia.
- La detección temprana es importante, por lo que debe asegurarse de que su personal sepa cómo informar de un posible incidente de ransomware o de un comportamiento inusual en la red.
- Si es posible, contrate a un proveedor que pueda ofrecer asistencia de respuesta si se produce un incidente. Establezca un contrato previo al evento para que tenga acceso al proveedor de inmediato.

Dado que los actores malignos suelen utilizar el phishing para infectar un sistema con ransomware, es fundamental contar con una política antiphishing. Realice pruebas de phishing rutinarias para que los empleados puedan detectar un correo electrónico de phishing antes de hacer clic en enlaces o archivos adjuntos peligrosos y, cuando sea posible, utilice programas de software antiphishing.

Actualice su software con los últimos parches de seguridad. Con este paso preventivo fundamental, los agentes malignos tendrán más dificultades para comprometer la seguridad de su sistema.

Desarrolle una política para toda la organización relativa a los ataques de ransomware. Es mucho más sencillo mantener esas conversaciones cuando no se tiene la presión de responder a un ataque. Debe plantearse estas preguntas: ¿qué datos son los más importantes para su organización? ¿Su seguro cubre el ransomware? ¿Estaría dispuesto a pagar un rescate? Si es así, ¿comprende cómo usar bitcoin y otras criptomonedas?

Hable sobre este asunto y aplique una política en toda la organización con respecto a los ataques de ransomware. **Es mucho más sencillo mantener esas conversaciones cuando no se tiene la presión de responder a un ataque.**

¿Los datos **son críticos para sus operaciones?**

¿Su organización ha determinado previamente que **no hay problema en pagar un rescate?**

¿Su seguro **cubre el ransomware?**

Responder

Si un empleado o la organización se enfrenta a una solicitud de rescate, su organización debe evaluar en primer lugar la legitimidad de la solicitud de rescate poniéndose en contacto con el responsable de TI. Si es legítimo, se presentan dos posibilidades:

1 **Su organización cuenta con copias de seguridad que funcionan.**
No necesita preocuparse por el ransomware.
Restaura sus datos por completo y vuelve a trabajar.

2 **Los datos que se mantienen como rehenes son necesarios y no dispone de copias de seguridad que funcionen.**

a. Compruebe si los datos existen en algún otro lugar de la organización (p. ej., archivos de caché, correo electrónico) para que pueda “unir” los datos juntos y sustituir los que se han utilizado como rehenes.

b. Si no puede acceder a los datos en ningún otro lugar, hágase estas preguntas:

- ¿Los datos son críticos para sus operaciones?
- ¿Su organización ha determinado previamente que no hay problema en pagar un rescate?
- ¿Su seguro lo cubre?

Recuperarse

Ha logrado apagar el fuego y es hora de volver a la normalidad. El alcance del ataque de ransomware y la gravedad de su impacto en sus operaciones diarias determinarán cuánto tiempo y esfuerzo necesitará para recuperarse. Utilice el incidente como una experiencia de aprendizaje para reforzar la importancia de los principios de la preparación cibernética, como los parches y la concienciación sobre el phishing.

Al asegurarse de que su software esté siempre actualizado con los últimos parches de seguridad, será más difícil acceder a su sistema. Del mismo modo, impartir de forma habitual formación sobre phishing minimiza el error humano y los posibles puntos de acceso a su sistema. Al igual que con cualquier vulneración de seguridad, notifique a todas las partes afectadas, restablezca los ID de usuario y las contraseñas de todos los dispositivos que hayan sido objetivo del ataque, actualice el software en todos los dispositivos y vuelva a instalar sus datos a partir de las copias de seguridad una vez que se haya neutralizado la amenaza del ransomware.

Es especialmente importante asegurarse de que los parches se actualicen después del ataque. Si se han restaurado los datos, a veces pueden volver a aparecer vulnerabilidades a las que se aplicaron parches antes del ransomware.

El Programa de preparación cibernética incluye instrucciones detalladas y plantillas para ayudarle a crear sus propias políticas y un plan de respuesta ante incidentes, con el fin de prepararse, responder y recuperarse ante un ataque de ransomware. Regístrese gratis en **BeCyberReady.com**.

Para conocer ejemplos reales de cómo empresas y municipios han respondido a un ataque de ransomware, visite **Noticias sobre preparación cibernética.**

El Programa de preparación cibernética incluye instrucciones detalladas y plantillas para ayudarle a crear sus propias políticas y un plan de respuesta ante incidentes, con el fin de **prepararse, responder y recuperarse ante un ataque de ransomware.**

Guía de toma de decisiones ante ataques de ransomware

PREPARARSE

¿Ha establecido prioridades en sus datos y sistemas para saber qué es lo más crítico para sus operaciones empresariales?

- 👍 → ¿Cuenta con un plan de respuesta ante incidentes que cubra el ransomware?
  - 👍 → ¿Dispone de una copia de seguridad actual?
    - 👍 → ¿Lo ha probado en el último mes?
      - 👍 → ¡Enhorabuena! **Está preparado.**
      - 👎 → Pruebe su copia de seguridad para asegurarse de que puede recuperar los datos, sobre todo los más críticos para sus operaciones empresariales.
    - 👎 → Realice una copia de seguridad de su sistema y de todos los datos.
  - 👎 → Desarrolle un plan de respuesta ante incidentes que cubra el ransomware. Visite **BeCyberReady.com** para acceder a una plantilla para crear un plan de respuesta ante incidentes.
- 👎 → Identifique aquello que es más valioso. Visite **BeCyberReady.com** para acceder a una lista de verificación para establecer prioridades.

Esperemos que no sea víctima de un ataque de ransomware. **No está EN ABSOLUTO preparado.**

⚠ Se produce un incidente de ransomware ⚠

RESPONDER

Aísle el incidente y desconecte de la red los equipos infectados. A continuación, proceda.

- 👍 → Bien hecho. **¡Pase directamente a Recuperarse!**
- 👎 → ¿Dispone de un servicio de asistencia de TI con el que contactar?
  - 👍 → ¿Puede usted o el servicio de asistencia de TI realizar copias de seguridad en tiempo real?
    - 👍 → Vaya a la copia de seguridad en tiempo real y elimine el malware.
    - 👎 → ¿Dispone de seguro cibernético?
      - 👍 → ¿Su póliza cubre eventos de rescate?
        - 👍 → Vaya a la copia de seguridad en tiempo real y elimine el malware.
        - 👎 → No puede recuperar los datos… **debe decidir si pagar o no.**
      - 👎 → No puede recuperar los datos… **debe decidir si pagar o no.**
  - 👎 → ¿Los datos que se mantienen como rehenes son valiosos para su negocio?
    - 👍 → ¿Su póliza cubre eventos de rescate?
      - 👍 → Vaya a la copia de seguridad en tiempo real y elimine el malware.
      - 👎 → No puede recuperar los datos… **debe decidir si pagar o no.**
    - 👎 → Vaya a la copia de seguridad en tiempo real y elimine el malware.

RECUPERARSE

Vaya a la copia de seguridad en tiempo real y elimine el malware.

Restablezca los ID de usuario y cambie las contraseñas

Realice una instalación limpia desde su copia de seguridad

Actualice su software

Vuelva a instalar los datos de forma selectiva

¡Ha vuelto a su actividad normal! Regístrese en el Programa de preparación cibernética gratuito en **BeCyberReady.com** para evitar más ataques de ransomware en el futuro.

CYBERREADINESSINSTITUTE.ORG

guide@cyberreadinessinstitute.org