13 Tips para prevenir el Ransomware

En Trend Micro nuestro equipo de especialistas en Ransomware se dedica a analizar casos de clientes y prevenir futuros ataques de secuestro de datos. Si quieres tener una plática con uno de ellos, por favor solicítalo y déjanos tus datos.

Protección de email y servidores web

1.¿Qué ocurre cuando un email con links llega al servidor de correo de tu empresa?

TIP

Muchos ataques de Ransomware son desarrollados a la medida de la víctima y en consecuencia, usan links desconocidos para la seguridad tradicional. Un análisis completo analiza la antigüedad de esos links y los testea en un entorno tipo "sandbox" antes de autorizarlos en tu empresa.

2.¿Qué ocurre cuando un email con attachments llega al servidor de correo de tu empresa?

TIP

Muchos ataques de Ransomware son desarrollados a la medida de la víctima y, en consecuencia, usan archivos (PDF, XLS y otros) desconocidos para la seguridad tradicional. Un entorno tipo "sandbox" simula las acciones de ese archivo antes de autorizarlo en tu empresa.

Protección de endpoints

3.¿Qué ocurre cuando una aplicación desconocida intenta ejecutarse en un dispositivo?

TIP

Muchos ataques de Ransomware usan aplicaciones maliciosas desarrolladas a la medida de la víctima y desconocidas para la seguridad tradicional. Una "whitelist" de aplicaciones autorizadas limita el riesgo al controlar qué puede ejecutarse y qué no en los dispositivos del usuario.

4.¿Qué ocurre cuando una aplicación intenta cifrar archivos?

TIP

El Ransomware intenta cifrar grandes volúmenes de datos en corto tiempo. Si una aplicación no autorizada o un proceso malicioso intenta cifrar varios archivos, este proceso debe ser inmediatamente identificado y bloqueado.

5.¿Qué ocurre cuando un dispositivo en su empresa presenta vulnerabilidades?

TIP

La distribución y testing de parches es un proceso complejo y riesgoso para la empresa. Detectar dispositivos con vulnerabilidades y remediarlas limita la superficie de ataque disponible para un Ransomware.

6.¿Qué ocurre cuando un dispositivo es vulnerable pero no existe un parche publicado?

TIP

Los fabricantes de aplicaciones (Adobe, Oracle, Microsoft y otros) pueden demorar semanas en publicar un parche. Y su distribución en tu empresa puede llevar mucho tiempo más. Una solución de "virtual patching" protege a esos equipos aun cuando el parche no haya sido instalado.

Protección de redes

7.¿Qué ocurre cuando un dispositivo intenta conectarse a sitios externos sospechosos?

TIP

Muchos ataques de Ransomware son desarrollados a la medida de la víctima y en consecuencia, usan links desconocidos para la seguridad tradicional. Un análisis completo analiza la antigüedad de esos links y los testea en un entorno tipo "sandbox" antes de autorizarlos en tu empresa.

8.¿Qué ocurre cuando un dispositivo intenta conectarse con otros dispositivos dentro de la empresa?

TIP

El Ransomware busca propagarse mediante la red interna para infectar a otros dispositivos. Analizar el tráfico de red y los comportamientos típicos de un Ransomware permite detectar dispositivos infectados, limitar su propagación y mitigar su capacidad de hacer daño en la empresa.

Protección de servidores

9.¿Qué ocurre cuando un dispositivo intenta acceder a carpetas compartidas en un Servidor?

TIP

El Ransomware puede cifrar carpetas compartidas en un dispositivo remoto desde el equipo infectado. Ese comportamiento típico de un Ransomware puede ser difícil de detectar y prevenir, a menos de que se analice de manera coordinada entre los dispositivos de ataque y de destino.

10.¿Cómo funcionan los procesos de backup y respaldo en tu empresa?

TIP

En caso de que un ataque de Ransomware ocurra, es importante estar prevenido con adecuadas políticas de backup automatizado de endpoints y servidores.

11.¿Dónde son almacenadas las copias de backup y respaldo?

TIP

Luego de secuestrar archivos locales y remotos, el Ransomware intentan cifrar los archivos de backup y respaldo. Si es posible considera hacer respaldo en servicios en la nube y que estén aislados de la red empresarial.

Políticas de seguridad

12.¿Han ocurrido incidentes de Ransomware en tu empresa?

Incidentes de Ransomware aislados y aún en pequeña escala pueden indicar la presencia de código malicioso en la organización. Ataques previos y aparentemente mitigados pueden haber sembrado la infraestructura ara un ataque posterior. Es clave detectar y mitigar esos focos para impedir nuevos incidentes.

13.¿Cómo crees que reaccionaría un usuario de tu empresa a un incidente de Ransomware?

Políticas de seguridad debidamente comunicadas y que involucren al equipo de TI son importantes para evitar la propagación de ataques. Un incidente de pequeña escala puede generar complicaciones serias si no es debidamente mitigado. En ningún caso es recomendable el pago de rescates, ya que esto no garantiza recuperar la información cifrada.

En Trend Micro nuestro equipo de especialistas en Ransomware se dedica a analizar casos de clientes y prevenir futuros ataques de secuestro de datos. Si quieres tener una plática con uno de ellos, por favor solicítalo y déjanos tus datos.