Ransomware un enemigo visible

El ransomware es un tipo de malware que cifra archivos importantes en el almacenamiento local y de la red, que exige un rescate para liberarlos. Los hackers desarrollan este malware para ganar dinero a través de la extorsión digital.

El ransomware está cifrado, por lo que la clave no puede forzarse y la única forma de recuperar la información es por medio de un respaldo.

La forma en que trabaja el ransomware es **especialmente dañina,** otros tipos de malware destruyen o roban los datos pero dejan abiertas otras opciones de recuperación. **Con el ransomware, si no hay respaldos, debe pagar el rescate para recuperar los datos.** A veces las entidades afectadas pagan el rescate y el atacante no envía la clave para descifrar los archivos.

Tips para reducir el riesgo de ataques desde TI

Elabora una estrategia de prevención ante incidentes en la que incluyas protección de datos, copias de seguridad inmutables y la herramientas para crear una cultura cibersegura.

Establece procedimientos de respuesta tras un incidente capacitando a tu personal y programando ejercicios de formación de manera periódica.

Implementa medidas de detección de ataques de ransomware desplegando políticas de análisis basadas en el comportamiento.

Realiza una copia de seguridad de tus datos y archivos

Con la llegada de redes más seguras y el almacenamiento en la nube, **muchas empresas no realizan copias de seguridad** de archivos y datos.

Educa a tus colaboradores para reconocer las amenazas potenciales

La **educación del usuario interno de la organización** siempre ha sido un elemento clave para evitar infecciones de malware. Este mismo principio también se aplica al ransomware.

Limita el acceso a aquellos que lo necesitan

Con el fin de minimizar el impacto potencial de un ataque de ransomware exitoso, tu organización debe asegurarse de que **los usuarios solo tengan acceso a la información y los recursos necesarios** para ejecutar sus tareas.

Actualiza constantemente los sistemas de protección

Desde el punto de vista de la ciberseguridad, siempre es beneficioso **mantener los antivirus actualizados.**

Utiliza sistemas de seguridad multicapa con tecnologías avanzadas de prevención de amenazas

La implementación de un sistema de varias capas para la seguridad es la mejor forma de defenderse del ransomware y del daño que podría causar. Además de las protecciones tradicionales, como antivirus e IPS, **tu compañía necesita incorporar capas adicionales** para evitar el malware nuevo y desconocido.

9 Tips para reducir el riesgo de ransomware desde el usuario final

1

Evita hacer clic en enlaces no verificados

Si un enlace está en un **correo electrónico no deseado o en un sitio web extraño, evítalo.** A menudo, los piratas informáticos propagan el ransomware a través de un enlace malicioso que inicia la descarga de un malware.

Escanea los correos electrónicos en busca de malware

Las herramientas de escaneo de correo electrónico **detectan a menudo software malicioso.** Una vez que el escáner detecta un malware, el correo electrónico puede eliminarse, de modo que no consigue llegar a la bandeja de entrada.

2

3

Usa firewalls (cortafuegos) y protección de punto final

Los firewalls escanean el tráfico proveniente de ambos lados, **examinándolos en busca de malware y otras amenazas.**

Descarga únicamente desde sitios de confianza

La ingeniería social ejerce presión sobre el usuario, generalmente a través del miedo, para que realice una acción específica, en este caso, **hacer clic en un enlace malicioso.**

4

5

Conserva copias de seguridad de los datos importantes

A los atacantes de ransomware les gusta **aprovecharse de los usuarios que dependen de ciertos datos** para operar sus organizaciones.

Usa una VPN cuando recurras a una red pública de Wi-Fi

Una VPN **cifra los datos** que fluyen hacia y desde el dispositivo mientras estás conectado a internet.

6

7

Usa software de seguridad

El software de seguridad **verifica los archivos que entran en tu computadora desde internet.** Cuando se detecta un archivo malicioso, el software evita que entre en tu equipo.

Evita usar dispositivos USB desconocidos

Se puede utilizar un dispositivo de bus en serie universal (USB) para **almacenar un archivo malicioso que podría contener ransomware.** Un USB aparentemente benévolo puede capturar tu computadora en muy poco tiempo.

8

9

Cuida tus datos personales

Con los datos personales correctos, un ciberdelincuente **puede tender una variedad de trampas para introducir el ransomware** en tu computadora o engañarte para que lo instales en tu dispositivo por mano propia.

Ventajas de una arquitectura para ransomware

Protege
todos los componentes TI, desde la nube y el perímetro de la red hasta el endpoint y el usuario.

Implementa una estrategia
que protege las soluciones empresariales en todas las fases de la cadena de eliminación de una ataque de ransomware.

Integra perfectamente
los conocimientos y la inteligencia frente a la detección de amenazas.

Reduce los riesgos
de amenazas más allá del ransomware, proporcionando otras ventajas como la visibilidad.

En **Gtd Colombia** buscamos siempre establecer y aplicar las mejores prácticas en los servicios que ofrecemos por eso nos apoyamos en los **Marcos de Trabajo: NIST Gestión de Riesgo del Ransomware**

Perímetro y seguridad en la nube

- **Detectar malware** en el perímetro de la red local o en su infraestructura en la nube pública.
- **Ir más allá del perímetro** y proteger los servicios empresariales para que no se utilicen como vectores de ransomware.

Segmentación interna

- **Inspeccionar el tráfico** de la red interna en busca de malware procedente de amenazas internas en cada segmento de la red.