

RANSOMWARE: PREVENCIÓN Y PROTECCIÓN

PROTECCIÓN EN TIEMPO REAL

El ransomware es una amenaza creciente, ya que los delincuentes han encontrado la manera de monetizar los programas malintencionados paralizando los sistemas informáticos y exigiendo que se pague un rescate por su liberación. A diferencia de otros programas malintencionados, que a menudo tienen que permanecer ocultos durante largos períodos de tiempo para funcionar con eficacia, el ransomware está diseñado para ejecutarse rápidamente a través de spear-phishing, sitios web comprometidos y descargas fraudulentas. Las instituciones financieras son particularmente vulnerables al impacto del ransomware, puesto que pueden amenazar la capacidad de mover fondos rápida y eficientemente, y porque se consideran objetivos lucrativos. No obstante, los delincuentes a veces incumplen sus promesas: incluso después de pagar un rescate, algunos atacantes no eliminan el software malintencionado o revelan datos confidenciales.

- Invierta en sistemas de protección antimalware que se adapten a la nueva inteligencia de amenazas en tiempo real.
- Evalúe la seguridad de todos los dispositivos conectados a las redes que contienen información confidencial o esencial. Conecte todos los sistemas no esenciales a una red independiente.
 - Tenga especial cuidado cuando introduzca «dispositivos inteligentes» o IoT en sus espacios de trabajo, ya que estos sistemas suelen tener sistemas de seguridad más débiles o inexistentes, y pueden ser utilizados como puntos de acceso a sistemas esenciales.
 - Tenga en cuenta la seguridad de las configuraciones de trabajo a distancia. Asegúrese de que las herramientas de seguridad funcionen fuera de la red para supervisar todo el tráfico de la web.
- Promueva la formación de los empleados en torno a los ataques de phishing y la necesidad de una protección de contraseñas sólida.
- Considere la posibilidad de aplicar la autenticación multifactorial en toda su organización, si es viable.
- Mantenga todos los programas y sistemas actualizados periódicamente. Cambie la configuración para permitir actualizaciones automáticas si es posible.
- Desarrolle un plan de respuesta a incidentes y de gestión de crisis sobre cómo hacer frente a un ataque de ransomware y a la pérdida de datos importantes.
- Prepare un plan de comunicación externa en caso de un ataque de ransomware.

COPIAS DE SEGURIDAD DE DATOS

- Invierta en sistemas de copia de seguridad que sean seguros y se actualicen periódicamente, y que mantengan sus datos protegidos.
 - Si utiliza USB o discos duros, desconecte físicamente estos dispositivos de los equipos conectados en red después de que las copias de seguridad hayan terminado.
 - Si utiliza el almacenamiento en la nube, equipe los servidores con encriptación de alto nivel y autenticación multifactorial.
- Cree una copia de solo lectura del libro mayor para la recuperación de desastres en el peor de los casos.
- Desarrolle sistemas que permitan la recuperación y reparación automatizadas de datos.
- Elabore escenarios para evaluar el tiempo que se tardará en recuperar los datos y servicios comerciales críticos.

ENTORNO NORMATIVO

- Evalúe las directrices normativas y legales pertinentes para el ransomware en su entorno operativo.
 - Considere las directrices específicas para cada país. Prepare un plan para la evaluación periódica de las directrices cambiantes.
 - Considere las directrices específicas del sector financiero.
 - Considere los requisitos legales y normativos internacionales.
- Valore los riesgos que conlleva el pago de un rescate. En algunos casos, pagar un rescate podría infringir los regímenes de sanciones vigentes contra los agentes hostiles.
- Coordínesse con las fuerzas del orden locales. Establezca conexiones para compartir rápidamente la información en caso de un ataque.
- Evalúe los beneficios y desventajas de las pólizas de seguro cibernético frente a ataques de ransomware.

Evaluación de la preparación de su organización frente a ataques de ransomware

Tenga en cuenta las siguientes preguntas al elaborar un plan de prevención y protección frente a ataques de ransomware.

1. ¿Su organización realiza **copias de seguridad programadas periódicamente**?
 - ¿Estas copias de seguridad están desconectadas de su red, ya sea a través de sistemas de almacenamiento en la nube o de USB o discos duros que nunca han sido conectados a la red?
2. ¿Hay algún **dispositivo no esencial** conectado a la red de su organización?
 - ¿Pueden ser trasladados a otras redes que no contengan datos confidenciales?
3. ¿Comprende su organización los **riesgos normativos y jurídicos** que conlleva el pago de un rescate?
 - Las directrices jurídicas al respecto varían de un país a otro y se actualizan con frecuencia.
4. ¿Su organización actualiza periódicamente sus sistemas de software? ¿Están **automatizadas** las actualizaciones?
5. ¿Tiene su organización un **plan para hacer frente a un ataque de ransomware** y pérdida de datos?
6. ¿Tiene su organización una **póliza de seguro cibernético**? Si es así, ¿cómo cubre el plan los ataques de ransomware?
 - Algunos planes prohíben explícitamente el pago de rescates, mientras que otros cubren dicho pago como parte de la póliza.