PROYECTO DE APLICACIÓN:

Descripción de los hechos: Una institución educativa sufre un ataque de ransomware, donde los archivos de la institución son cifrados y se exige un rescate para desbloquearlos. Como resultado, los sistemas de la institución se ven comprometidos y se interrumpe el acceso a la información crítica, como registros estudiantiles y documentos administrativos. La institución se ve obligada a tomar medidas de emergencia, como desconectar los sistemas afectados, informar a las autoridades competentes y contratar servicios de expertos en ciberseguridad para mitigar el ataque. Responda a las siguientes preguntas:

1. ¿Qué tipo de delito informático se ha cometido en este caso?

a) Ataque de ransomware.

b) Acceso no autorizado.

c) No es un delito informático.

2. ¿Qué medidas de seguridad podrían haberse implementado para prevenir el ataque descrito? (Puede marcar más de una alternativa). Respuesta:

a) Actualización regular del software y sistemas.

b) Uso de contraseñas fuertes y autenticación de dos factores.

c) Realización de copias de seguridad periódicas de los datos.

3. ¿Cuáles podrían ser las consecuencias legales para el perpetrador del ataque de ransomware?

a) Penas de prisión.

b) Multas económicas.

c) Ambas opciones son correctas.

4. ¿Qué medidas legales podrían tomarse para investigar y perseguir al perpetrador del ataque? (Puede marcar más de una alternativa)

a) Cooperación internacional entre agencias de ciberseguridad.

b) Obtención de órdenes judiciales para acceder a datos y evidencias.

c) Establecimiento de recompensas para informantes que ayuden a identificar al perpetrador.

1. Respuesta: a.

El ataque descrito es un claro ejemplo de un ataque de ransomware, donde los archivos son cifrados y se exige un rescate para desbloquearlos.

2. Respuesta: a,b y c.

Mantener los sistemas y software actualizados puede evitar que los atacantes exploten vulnerabilidades conocidas además las contraseñas fuertes y el doble factor de autenticación

reducen el riesgo de accesos no autorizados. Finalmente, las copias de seguridad periódicas aseguran que la institución pueda recuperar sus datos sin necesidad de pagar un rescate.

3. Respuesta: c.

El perpetrador de un ataque de ransomware puede enfrentarse tanto a penas de prisión como a multas económicas, dependiendo de la legislación aplicable y la gravedad del delito.

4. Respuesta: a, b y c.

La cooperación internacional es esencial dado que muchos delitos informáticos tienen una dimensión transnacional por lo que las órdenes judiciales son necesarias para obtener acceso legal a datos y evidencias que puedan incriminar al perpetrador y las recompensas pueden motivar a personas con información relevante a colaborar con las autoridades.