SUPUESTO TEÓRICO-PRÁCTICO

D4: SEGURIDAD

CASO 1: DISEÑO DE UNA RED SEGURA PARA UN GRUPO DE INVESTIGACIÓN

Contexto:

Eres el responsable de diseñar una red segura para un grupo de investigación dentro del CSIC. Este grupo trabaja en proyectos científicos importantes y maneja datos sensibles que deben ser protegidos de manera rigurosa. Además, el acceso a estos datos debe ser seguro y eficiente para los miembros del grupo de investigación dispersos en diferentes ubicaciones geográficas.

Requisitos y Características de Partida:

Confidencialidad de Datos:

- Los datos de investigación son sensibles y deben ser protegidos contra accesos no autorizados tanto desde dentro como desde fuera de la red.
- Es necesario establecer políticas de acceso basadas en roles para garantizar que solo las personas autorizadas puedan acceder a datos específicos.

Integridad de Datos:

- Los datos de investigación no deben ser modificados o alterados por personas no autorizadas.
- Se deben implementar mecanismos para verificar la integridad de los datos durante su transmisión y almacenamiento.

Disponibilidad del Sistema:

- Hay que asegurar que la red esté disponible en todo momento para los miembros del grupo de investigación, incluso en caso de fallos o ataques.

Acceso Remoto Seguro:

- Proporcionar un método seguro para que los miembros del grupo accedan a la red y los datos de investigación desde ubicaciones remotas.
- Utilizar tecnologías como VPN (Red Privada Virtual) para establecer conexiones seguras a través de Internet.

Monitorización y Detección de Amenazas:

- Implementar herramientas de monitoreo de red para identificar y responder rápidamente a posibles amenazas de seguridad.
- Establecer alertas para detectar actividades inusuales o intentos de acceso no autorizado.

Preguntas para Evaluación:

Bloque 1: Política de Acceso y Colaboración

- ¿Cómo diseñaría una política de acceso que equilibre la necesidad de confidencialidad de los datos de investigación con la colaboración efectiva entre los miembros del grupo?
- ¿Qué medidas específicas implementaría para garantizar que solo las personas autorizadas tengan acceso a datos sensibles?
- En un entorno donde los miembros del grupo de investigación necesitan acceder a la red de forma remota, ¿qué acciones o tecnologías de acceso seguro implementaría para asegurar que las conexiones remotas sean seguras y protegidas contra amenazas externas?

Bloque 2: Seguridad Técnica y Acceso Remoto

- ¿Qué tecnologías y métodos de autenticación consideraría para garantizar un acceso remoto seguro para los miembros del grupo de investigación que necesitan trabajar desde ubicaciones fuera de las instalaciones del CSIC?
- ¿Cómo implementaría el cifrado de extremo a extremo para proteger la confidencialidad de los datos durante su transmisión, especialmente cuando se accede a través de redes públicas?

Bloque 3: Monitorización y Respuesta a Amenazas

- ¿Qué herramientas y técnicas utilizaría para monitorizar la red del grupo de investigación en busca de actividades inusuales o posibles intrusiones?
- En el caso de detectar alguna amenaza, ¿cómo respondería a las mismas?
- ¿Qué estrategias implementaría para realizar auditorías regulares de seguridad y evaluar la eficacia de las políticas y medidas de seguridad existentes en la red del grupo de investigación?

SUPUESTO TEÓRICO-PRÁCTICO

D4: SEGURIDAD

CASO 2: GESTIÓN DE UN ATAQUE DE RANSOMWARE EN UN GRUPO DE INVESTIGACIÓN

Introducción:

Eres el responsable de seguridad de la información de un grupo de investigación relevante dentro del CSIC. En el entorno de este grupo de investigación, se ha producido un ataque de ransomware que ha afectado a los sistemas de almacenamiento de datos cruciales para las investigaciones: el ransomware ha cifrado archivos y bases de datos esenciales de vital importancia y cuya pérdida, modificación o divulgación no autorizada podría tener un impacto negativo significativo sobre los proyectos en curso y futuros del grupo y del propio CSIC. Las líneas de trabajo de grupo de investigación han quedado completamente paralizadas. Los atacantes exigen un rescate para proporcionar la clave de descifrado y liberar los datos. La prioridad es minimizar los efectos del ataque, reducir la propagación del ransomware y aplicar lecciones aprendidas para evitar futuros incidentes similares.

Requisitos y Características de Partida:

Integridad y Confidencialidad de los Datos de Investigación:

- La información cifrada por los atacantes es de fundamental importancia, tanto para los proyectos actuales y futuros del grupo de investigación, como para el mismo CSIC y otras Agencias y Organismos oficiales.
- La confidencialidad debe mantenerse intacta en todo momento, ya que cualquier fuga de información podría tener consecuencias operativas, económicas, legales, reputacionales e, incluso, sociopolíticas críticas.

Restauración y Recuperación de Datos:

- La restauración de los datos cifrados a su estado original es crucial para reanudar las líneas de trabajo del grupo de investigación.
- La integridad y no repudio de los datos recuperados es fundamental.

Prevención y Seguridad Futura:

- Se habrá de identificar el vector de ataque para fortalecer las medidas de seguridad y prevenir futuros ataques similares.
- Se habrá de contar con soluciones de seguridad con las que detectar y bloquear posibles amenazas semejantes en el futuro.

Comunicación y Colaboración:

- Se habrá de contar con unos planes de comunicación claros, completos y transparentes, tanto internos hacia el grupo de investigación como externos hacia las áreas expertas del CSIC.

- Se deberá considerar la colaboración de expertos en seguridad de la información y equipos de respuesta ante incidentes, tanto internos del CSIC como externos (e.g., INCIBE, CCN_CERT, etc.) para analizar el incidente.

Preguntas para Evaluación:

Bloque 1: Evaluación de la Situación y Acciones Iniciales

- ¿Cómo identificaría el vector de ataque del ransomware en el grupo de investigación y qué pasos tomaría para contener la propagación del malware?
- Considerando la importancia de la confidencialidad de los datos de investigación, ¿qué medidas tomaría para asegurar que la comunicación interna sobre el ataque del ransomware sea segura y efectiva?
- Ante la demanda de rescate del atacante, autor del ataque del ransomware, ¿cuál sería su enfoque en relación con el pago del rescate? ¿Qué factores consideraría al tomar esta decisión?

Bloque 2: Restauración de Datos y Seguridad Futura

- Después de aislar el ransomware, ¿cuál sería su estrategia para restaurar los datos cifrados y asegurar la integridad de los archivos y bases de datos de investigación?
- ¿Qué medidas implementaría para prevenir futuros ataques de ransomware en el grupo de investigación? ¿Qué tecnologías o prácticas de seguridad consideraría esenciales para evitar incidentes similares?
- ¿Cómo garantizaría que los sistemas de respaldo sean seguros y estén protegidos contra el cifrado por parte de un atacante de ransomware?

Bloque 3: Comunicación y Colaboración

- ¿Cómo manejaría la comunicación con los miembros del grupo de investigación durante y después del incidente? ¿Qué información compartiría y qué canales de comunicación establecería para mantener a todos informados?
- ¿Qué tipo de colaboración buscaría con expertos en ciberseguridad y equipos de respuesta a incidentes? ¿Qué rol tendrían estos expertos en la gestión del ataque de ransomware?