EXAMEN 07/08/2024

DESCRIPCIÓN GENERAL DE LA PRÁCTICA:

Esta actividad evaluable consiste en cuatro apartados. En el primero se trabaja con las amenazas y riesgos. En la segunda se trabaja con contramedidas. En la tercera se trata con sistemas de autenticación segura y en la cuarta se utilizarán reglas de filtrado de un firewall.

INSTRUCCIONES ESPECÍFICAS:

La actividad consta de 4 apartados:

1. Una empresa proporciona alojamiento de páginas web, con un sistema de información valorado en 250.000 €. Un análisis de riesgos revela que hay dos amenazas:
    a. Un fallo del suministro eléctrico, caracterizado por:
        i. Impacto o daño = 10.000 €
        ii. Probabilidad de ocurrencia de la amenaza= 0.1
    b. Un ataque dirigido desde internet, caracterizado por:
        i. Impacto o daño =500.000 €
        ii. Probabilidad de ocurrencia de la amenaza= 0.005

El modelo de seguridad de la empresa tiene el criterio de optimizar la inversión concentrando los recursos en eliminar la mayor amenaza, y asumir el riesgo de las amenazas menores.

Se pide que:

a. Se cuantifique el riesgo de cada amenaza.
b. Se calcule el presupuesto en seguridad que resultaría justificado invertir.
c. Se calcule el riesgo que asume la empresa tras la inversión.

2. En una empresa ocurren muchos incidentes de seguridad; algunos son de pequeña importancia, como las frecuentes interrupciones en la conexión a internet, y otros son más críticos, como las paradas del sistema durante jornadas completas, debido a errores en los servidores.

También se producen fugas de información, pequeños hurtos de periféricos, y otros accesorios. La empresa también es consciente del incumplimiento de alguna ley referente a la información.

La Dirección expone la situación, y pide que se proponga un plan de acción para corregir todos esos problemas.

Se pide:

a. Resumir brevemente las acciones a realizar, dando al menos una justificación de las mismas.

3. La empresa dispone de una cantidad elevada de personal que trabaja fuera de la empresa, en las instalaciones del cliente, por amplios periodos de tiempo. Los trabajadores usan un portátil con lector de huella para conectarse a la red de la empresa. Cuando los trabajadores cambian de cliente, se tienen que intercambiar los portátiles, para poder usar las aplicaciones apropiadas, y es práctica común decir a otros la contraseña propia, de manera que unos usuarios acceden con las credenciales de otros.

Se pide:

a. Describe un sistema de autenticación fuerte que mejore la seguridad del sistema.

4. Una empresa dispone de un servidor web y de un servidor de correo electrónico, y ambos comparten la IP pública 15.15.15.15.

El servidor web debe ser accesible desde el exterior, empleando el protocolo HTTPS. El servidor de correo debe poder recibir el correo que le envían otros servidores externos, así como enviar correo (tiene la dirección IP privada 192.168.100.20). Además, se permite que los usuarios de la red privada (con rango de red 192.168.100.0/24) puedan navegar libremente por internet.

Se pide:

a. Configure las reglas de acceso en el firewall perimetral.

Protocolo (TCP/UDP)	**Puerto**	**IP Origen**	**IP Destino**	**Acción**

Nota. Los servicios, puertos y protocolos a utilizar son los siguientes:

Servicio	**Protocolo**	**Puerto**
Navegación Web	HTTP	80 (TCP)
Navegación Web Segura	HTTPS	443 (TCP)
Envío de Correo	SMTP	25 (TCP)

1. Para abordar la situación, vamos a seguir los siguientes pasos:

a. ***<u>CUANTIFICACIÓN DEL RIESGO DE CADA AMENAZA</u>***

Se calcula con el producto de la probabilidad de ocurrencia y del impacto y/o daño.

1. FALLO DEL SUMINISTRO ELÉCTRICO:
   - Impacto y/o daño = 10000€
   - Probabilidad de ocurrencia = 0.1
   - Riesgo total = 10000 x 0.1 = 1000€

2. ATAQUE DIRIGIDO DESDE INTERNET:
   - Impacto y/o daño = 500000€
   - Probabilidad de ocurrencia = 0.005
   - Riesgo total = 500000 x 0.005 = 2500€

b. ***<u>CÁLCULO DEL PRESUPUESTO EN SEGURIDAD QUE RESULTARÍA JUSTIFICADO INVERTIR</u>***

Se busca optimizar la inversión concentrando los recursos y eliminando la mayor amenaza, asumiendo el riesgo de amenazas menores. Por consiguiente, se invierte en reducir el riesgo de amenaza con mayor riesgo, ya que:

- Es el ataque dirigido desde Internet con un riesgo de 2500€.

- Su presupuesto en seguridad es justificado, por lo tanto, el riesgo total de la amenaza más grande.

PRESUPUESTO EN SEGURIDAD JUSTIFICADO = 2500€.

c. <u>RIESGO QUE ASUME LA EMPRESA TRAS LA INVERSIÓN</u>

Se asume que la empresa tras la inversión, dicha inversión elimina el riesgo de amenaza más grande (ataque dirigido desde Internet).

1. RIESGO DE FALLO DEL SUMINISTRO ELÉCTRICO:
   - Sin cambios en la probabilidad ni en el impacto.
   - Riesgo = 10000 x 0.1 = 1000€

2. RIESGO DE ATAQUE DIRIGIDO DESDE INTERNET:
   - La inversión elimina el riesgo
   - Riesgo = 0€

3. RIESGO TOTAL ASUMIDO POR LA EMPRESA TRAS LA INVERSIÓN:
   - Riesgo total = 1000 + 0 = 1000€ (Riesgo de fallo del suministro eléctrico + Riesgo de ataque dirigido desde Internet)

En definitiva:

a. El riesgo de cada amenaza es de 1000€ por el fallo del suministro eléctrico y 2500€ por el ataque dirigido desde Internet.
b. Su presupuesto en seguridad justificado es de 2500€.
c. El riesgo asumido tras la inversión es de 1000€.

2. Para abordar los diversos incidentes de seguridad en la empresa, se debe gestionar el siguiente plan de acción:

1. ***MEJORAR LA INFRAESTRUCTURA DE RED Y CONECTIVIDAD***
    - Su acción es actualizar o reemplazar los equipos de red y garantizar una conexión más estable de Internet.
    - Su justificación son las frecuentes interrupciones en la conexión a Internet que pueden afectar a la productividad y disponibilidad de los servicios. Todo ello es para mejorar la infraestructura que reducirá dichos problemas y aumentará la estabilidad operativa.
2. ***IMPLEMENTAR SOLUCIONES DE RESPALDO Y RECUPERACIÓN DE DESASTRES***
    - Su acción es establecer un sistema de respaldo regular con un plan de recuperación de desastres para los servidores.
    - Su justificación son las paradas prolongadas del sistema que pueden causar pérdidas significativas de tiempo y datos. Esto con un plan sólido asegura la continuidad del negocio y minimizará el impacto en caso de fallos del sistema.
3. ***FORTALECER LAS MEDIDAS DE SEGURIDAD FÍSICA***
    - Su acción es instalar las medidas de seguridad adicionales (cámaras de vigilancia) y controles de acceso para periféricos y otros accesorios.
    - Su justificación es la protección contra los pequeños hurtos y el acceso no autorizado a los equipos, que es esencial para evitar las pérdidas y proteger así los recursos físicos de la empresa.
4. ***IMPLEMENTAR POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CUMPLIMIENTO LEGAL***
    - Su acción es revisar y actualizar las políticas de seguridad de la información asegurar el cumplimiento de las leyes y regulaciones pertinentes.
    - Su justificación es el incumplimiento legal que puede resultar en sanciones y daños a la reputación de la empresa. Alinear las políticas con las leyes ayudará a mitigar los riesgos y garantizando la conformidad.
5. ***CAPACITACIÓN CONTINUA DEL PERSONAL EN LA SEGURIDAD***

- Su acción es ofrecer formación regular en seguridad de la información y prácticas de protección de datos para todo el personal.
- Su justificación es la conciencia y el comportamiento del personal, que son clave para la prevención de incidentes de seguridad. La formación continua fortalece la capacidad del equipo para reconocer y manejar las amenazas.

6. ***REALIZAR AUDITORÍAS Y EVALUACIONES DE RIESGOS PERIÓDICAS***
   - Su acción es llevar a cabo auditorías y evaluaciones de riesgos de forma regular para identificar y abordar nuevas vulnerabilidades.
   - Su justificación son las amenazas y vulnerabilidades que cambian con el tiempo. Las evaluaciones periódicas permiten ajustar las medidas de seguridad y adaptarse así a nuevos desafíos.

3. Para mejorar la seguridad del sistema del entorno con trabajadores que usar ordenadores portátiles en las instalaciones del cliente y se intercambian los equipos, es necesario implementar un Sistema de Autenticación Fuerte basado en Autenticación Multifactor (MFA). A continuación, describiremos los sistemas:

1. ***SISTEMA DE AUTENTICACIÓN FUERTE:***
   a. ***Autenticación Multifactor (MFA):***
      i. Factor 1, Contraseña: Cada usuario deber tener una contraseña fuerte y única. No debe ser compartida con nadie bajo ningún concepto.
      ii. Factor 2, Token de Seguridad: Utilizar un token físico de seguridad (llave USB o dispositivo de generación de códigos temporales) o un token de software (autenticación en el móvil), ya que proporciona con código temporal que cambia cada cierto tiempo.

iii. Factor 3, Biometría: El lector de huellas dactilares integrado en el portátil para la autenticación biométrica. Esto asegura que sólo el usuario autorizado pueda acceder al dispositivo.

b. Autenticación en el Cambio de Cliente:

i. Cuando el usuario cambia de cliente y usa un nuevo portátil, el sistema solicita una autenticación completa con los tres factores antes de permitir el acceso a la red de la empresa y de las aplicaciones específicas.

c. Políticas de Contraseñas:

i. Implementar políticas estrictas de las contraseñas para que puedan ser cambiadas regularmente, con una complejidad suficiente (números, letras y caracteres especiales), y además muy importante, no deber ser compartidas.

d. Control de Acceso Basado en Rol (RBAC):

i. Asignar los permisos y accesos según los roles a cada usuario para que así puedan tener acceso a los recursos necesarios para sus tareas y roles específicos, minimizando así el riesgo de acceso no autorizado.

ii. Registrar todas las autenticaciones y acceso para no monitorear y detectar cualquier actividad sospechosa y/o intentos de acceso no autorizados.

e. Registro y Monitoreo de Accesos:

i. Registrar todas las autenticaciones y acceso para no monitorear y detectar cualquier actividad sospechosa y/o intentos de acceso no autorizados.

En conclusión:

- Hay que tener una contraseña que solamente los usuarios conocedores puedan acceder a su cuenta.
- El token de seguridad añade una capa adicional al requerir algo que el usuario posee.
- Una biometría garantiza que el sólo el usuario autorizado pueda acceder al dispositivo, evitando el uso compartido de credenciales.
- Las políticas y RBAC aseguran que el acceso sea apropiado y controlado, reduciendo así el riesgo de exposición innecesaria de datos.

4.

Protocolo	**Puerto**	**IP de Origen**	**IP de Destino**	**Acción**
TCP	443	0.0.0.0/0	15.15.15.15	Permitir
TCP	25	0.0.0.0/0	15.15.15.15	Permitir
TCP	25	192.168.100.20	0.0.0.0/0	Permitir
TCP	80	192.168.100.0/24	0.0.0.0/0	Permitir
TCP/UDP	Todos	192.168.100.0/24	0.0.0.0/0	Permitir
Todos	Todos	Todos	Todos	Denegar

Su explicación es la siguiente:

- La regla 1 permite el tráfico HTTPS (Puerto 443) desde cualquier IP externa hacia el servidor web (IP Pública 15.15.15.15). Permite que el servidor web sea accesible desde el exterior usando HTTPS.
- La regla 2 permite el tráfico SMTF (Puerto 25) desde cualquier dirección IP externa hacia el servidor de correo (IP Pública 15.15.15.15). Permite que el servidor de correo reciba correos desde el exterior.
- La regla 3 permite el tráfico SMTP (Puerto 25) desde el servidor de correo interno (IP Privada 192.168.100.20) hacia cualquier dirección IP externa. Permite que el servidor de correo envíe correos a otros servidores externos.

- La regla 4 permite la navegación web (HTTP, Puerto 80) desde la red interna (192.168.100.0/24) hacia cualquier dirección IP externa. Permite que los usuarios naveguen por Internet.
- La regla 5 permite que todo el tráfico de respuesta desde cualquier dirección IP externa hacia la red interna (192.168.100.0/24). Asegura que las respuestas a las solicitudes realizadas por los usuarios y servicios internos sean permitidas.
- La regla 6 bloquea todo el tráfico no especificado en las reglas anteriores. Esto asegura que sólo el trafico deseado y permitido sea aceptado por el firewall.