2023

Universidad Andrés Bello®

Control 1 - Ciberseguridad

CASO 2, MAN IN THE MIDDLE

CORNEJO BENJAMÍN, FARFAN YERKO, FUENTES BASTIÁN, LARENAS RENZO, RETAMALES JUAN PABLO, SALVATICI NICOLAS

A. Identifique 10 activos tecnológicos y ordénelos según su criticidad.

1. Firewall.
2. Certificados de seguridad
3. Software de encriptación de datos
4. Red de comunicación de la empresa
5. Sistema de autentificación de dos factores
6. Equipos de conmutación y enrutamiento
7. Servidores de almacenamiento y procesamiento
8. Servidores de aplicaciones
9. Base de datos
10. Aplicación de banca en línea

B. Identifique 2 controles preventivos, 2 detectivos y 2 correctivos.

- Preventivo:
  - Uso de certificados SSL/TLS
  - Implementación de VPN
- Detectivo:
  - Sistema de detección de intrusiones (IDS)
  - Monitoreo del tráfico de Red
- Correctivo
  - Política de respuesta a incidente
  - revisión y actualización de políticas de Seguridad

C. Identifique el tipo de atacante (Black hat, White hat, Grey Hat)

Tipo de ataque: Black Hat

Es Black Hat porque efectúa un ataque MitM con el fin de comprometer la confidencialidad e integridad de la empresa interceptando y manipulando la comunicación e información entre clientes y los activos de la empresa, el resultado del ataque fue robo de información importante y realización de transacciones fraudulentas.

D. Recomiende un Ethical Hacking (Black box, White Box, Grey Box)

La recomendación vendría siendo de grey box, debido a que dicho ethical hacking trata de hacer ataque de prueba con la poca información que tiene sobre los clientes y la empresa, esto sería parecido a un Man-in-the-Middle (MitM), ya que este tipo de ataque utiliza la información que recibe solo mediante la interceptación de las comunicaciones.

Esto nos permite evaluar los sistemas y controles de seguridad de la empresa como por ejemplo la autenticación en dos factores.

E. Clasifique el incidente según ENISA.

En este caso el incidente se podría clasificar con más de una clase, siendo las siguientes:

1. Recopilación de información.
2. Información de seguridad de contenidos.
3. Fraude.

Esta clasificación se debe a que el atacante recopila información por medio de interceptar comunicaciones (1) y accede de manera no autorizada a la información de los clientes y la empresa (2). Además, realiza transacciones en nombre de los clientes sin previa autorización (3).

F. Reconozca el tipo de ataque

El tipo de ataque es Man-in-the-Middle, puesto que se interpone e intercepta la comunicación entre el cliente, las aplicaciones y servidores de la empresa.

G. Diseñe un plan de mitigación para el ataque según el Framework NIST.

Amenaza: Ataque MitM

IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
Vulnerabilidades:	**Controles:**	Auditorias (supervisión continua)	Aislar redes afectadas	Actualizar contraseñas
Redes Wi-Fi no seguras	Utilizar VPN	Pentesting / Ethical Hacking	Utilizar una red secundaria	Documentar lecciones aprendidas
Falta de cifrado de información	Encriptar información	Prueba de funcionalidad	Aislar dispositivos afectados	Evaluar efectividad de controles (ethical hacking)
Analizador de red	Autentificación multifactor		Informar a las autoridades	
Contraseña universal	Utilizar contraseñas distintas		Actualización de credenciales	

No contar con antivirus	Utilizar software antivirus		Bloqueo de IP	
Permitir acceso a páginas webs no seguras	Bloquear acceso a páginas web no seguras			
Falta de Firewall	Implementar Firewall			
Falta de uso de redes privadas (VPN)	Capacitar al personal para prevenir ciberdelitos			
No capacitar al personal en prevención de ciberdelitos				

Riesgos:
Robo de información
Filtración de datos
Daño de la imagen reputacional