Práctica Nro 2

Univ: Cristian Kevin Gallardo Coro

ANÁLISIS DE RIESGOS

DETERMINAR EL ALCANCE

Las oficinas y la sucursal de la financiera La Caridad

IDENTIFICAR LOS ACTIVOS

Software y Aplicaciones (Registros, Aplicación Movil, Sofware DLP)

Dispositivos (Switches)

VALORAR LOS ACTIVOS

ACTIVO	IMPORTANCIA
SOFTWARE Y APLICACIONES	
(Registros D=3 + I=5 + C=3) => 11/3 = 3.67 => 4	ALTO
(Aplicacion Movil D=2 + I=2 + C=2) => 6/3 = 2	BAJO
(Software DLP D=3 + I=3 + C=1) => 7/3 = 2.33 => 2	BAJO
DISPOSITIVOS	
(Switches D=5 + I=4 + C=2) => 13/3 => 4.33 => 4	ALTO

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_01	Registros	Logs y resgtros del sistema	Analista de Datos	Sistema (lógico)	Computadoras de la empresa	ALTO
ID_02	Aplicación Movil	Aplicación de la entidad financiera	Desarrolador Web	Sistema (Lógico)	Entidad Financiera	BAJO
ID_03	Software	Software para evitar perder información	Jefe del departamento de TI	Sistema (lógico)	Computadoras de la empresa	BAJO

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_01	Switches	Switches controlados de manera remota	Ingeneniero en Redes	Dispositivo de Red (Fisico)	Departamento de Redes	ALTO

IDENTIFICAR LAS AMENAZAS

Software y Aplicaciones

- En los últimos seis meses, se identificaron en los registros o logs del servidor web, peticiones de conexión provenientes de direcciones Ips que de acuerdo a una revisión la gran mayoría de ellas corresponden a ip registradas para países europeos (AMENAZA: ATAQUES INTENCIONADOS) => Acceso no autorizado, las peticiones provenientes de las direcciones Ips ajenas a la empresa e incluso al país, es una muestra casi clara de un ataque realizado por ciber atacantes a la empresa.
- Debido a presión de la alta dirección, la aplicación móvil fue lanzada a producción, únicamente siendo testeada con pruebas de caja blanca y caja negra (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) => Deficiencias en la organización, vulnerabilidades de los programas, una mala organización produjo un lanzamiento prematuro sin haberse hecho todas las pruebas de seguridad, esto puede abrir a varias vulnerabilidades en la aplicación comprometiendo información muy sensible.
- Recientemente finalizo el tiempo de licencia que se cancelaba por un software (DLP) que monitoreaba el tráfico, controlando que ningún documento digital etiquetado como confidencial pueda ser enviado por email, mensajería, etc (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) => Escapes de información, la falta de un software muy importante como es un DLP supondría un peligro enorme al no haber control del envío de material confidencial el cual podría fácilmente poder caer en manos de terceros.

Dispositivos

- Para la administración remota de todos los switches de la red interna, se tiene habilitado el protocolo telnet para hacer modificaciones de manera rápida. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) => Errores de configuración, al hacer el uso del protocolo telnet, un protocolo muy inseguro el cual fácilmente podría ser usado por personas ajenas a la empresa con fines maliciosos.

IDENTIFICAR VULNERABILIDADES

Software y Aplicaciones

- En los últimos seis meses, se identificaron en los registros o logs del servidor web, peticiones de conexión provenientes de direcciones Ips que de acuerdo a una revisión la gran mayoría de ellas corresponden a ip registradas para países europeos => **Ausencia de control de cambios eficaz**, las peticiones provenientes de las direcciones Ips ajenas a la empresa e incluso al país, es una muestra casi clara de un ataque realizado por ciber atacantes a la empresa.
- Debido a presión de la alta dirección, la aplicación móvil fue lanzada a producción, únicamente siendo testeada con pruebas de caja blanca y caja negra => **Ausencia de control de cambios eficaz**, una mala organización produjo un lanzamiento prematuro sin haberse hecho todas las pruebas de seguridad, esto puede abrir a varias vulnerabilidades en la aplicación comprometiendo información muy sensible.
- Recientemente finalizo el tiempo de licencia que se cancelaba por un software (DLP) que monitoreaba el tráfico, controlando que ningún documento digital etiquetado como

confidencial pueda ser enviado por email, mensajería, etc =>**Defectos bien conocidos de software**, la falta de un software muy importante como es un DLP supondría un peligro enorme al no haber control del envío de material confidencial el cual podría fácilmente poder caer en manos de terceros.

Dispositivos

- Para la administración remota de todos los switches de la red interna, se tiene habilitado el protocolo telnet para hacer modificaciones de manera rápida =>**Ausencia de un eficiente control de cambios en la configuración**, al hacer el uso del protocolo telnet, un protocolo muy inseguro el cual fácilmente podría ser usado por personas ajenas a la empresa con fines maliciosos.