CASO 1 – SEGURIDAD DE SISTEMAS

Univ. Cristian Kevin Gallardo Coro

Institución: Financiera Oportunidad

DETERMINAR EL ALCANCE

Las oficinas de la institución Financiera Oportunidad y todos los procesos que se desarrollan en el sistema.

IDENTIFICAR LOS ACTIVOS

Podemos identificar los activos por grupos:

Dispositivos (Computadoras de los funcionarios)

Software y Aplicaciones (Antivirus y Antimalware gratuitos)

VALORAR LOS ACTIVOS

ACTIVO	IMPORTANCIA
Dispositivo (Computadora de funcionario D = 2 + I = 4 + C = 2) -> 8/3 -> 2.67 -> 3	MEDIO
Software y Aplicaciones (Antivirus y Antimalware gratuitos D = 4 + I = 3 + C = 1) -> 8/3 -> 2.67 -> 3	MEDIO

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_01	Computadora de funcionario	Dispositivo donde el funcionario realiza todas sus operaciones	Jefe del departamento de TI	Computadora (Físico)	Departamento de informática de la Financiera Oportunidad	MEDIO

ID	Nombre	descripción	Responsable	Tipo	Ubicación	Importancia
ID_01	Antivirus y Antimalware Gratuitos	Softwares que evitan la infiltración de malware hacia un dispositivo	Jefe del departamento de TI	Software (Lógico)	Computadoras del departamento de IT	MEDIO

IDENTIFICAR LAS AMENAZAS

Dispositivos

- Las computadoras utilizadas por los funcionarios les permiten instalar cualquier tipo de software (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> Errores de configuración, al permitir cualquier instalación el funcionario podría instalar cualquier tipo de software ajeno a los fines de la empresa, y también por error podrían descargar cualquier tipo de software infectado con un malware, el cual no debe ser permitido instalar.

Software y Aplicaciones

- Como respuesta a los ataques de ransomware, los cuales se están masificando en varias organizaciones similares, se procede a instalar antivirus y antimalware gratuitos en cada computadora (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> Vulnerabilidades de los programas, un antivirus o antimalware gratuito, no funciona en su totalidad, restringiendo algunas funciones las cuales pueden ser aprovechadas por los atacantes.

IDENTIFICAR VULNERABILIDADES

Dispositivos

- Las computadoras utilizadas por los funcionarios les permiten instalar cualquier tipo de software -> CONFIGURACION INCORRECTA DE PARAMETROS, al permitir cualquier instalación el funcionario podría instalar cualquier tipo de software ajeno a los fines de la empresa, y también por error podrían descargar cualquier tipo de software infectado con un malware, el cual no debe ser permitido instalar.

Software y Aplicaciones

- Como respuesta a los ataques de ransomware, los cuales se están masificando en varias organizaciones similares, se procede a instalar antivirus y antimalware gratuitos en cada computadora -> DEFECTOS BIEN CONOCIDOS DE SOFTWARE, un antivirus o antimalware gratuito, no funciona en su totalidad, restringiendo algunas funciones las cuales pueden ser aprovechadas por los atacantes.

EVALUAR EL RIESGO

Activo: Dispositivos

Nro.	**Descripción de Riesgo**	Probabilidad	Impacto				Riesgo
			Financiero	Imagen	Operativo	Total	
1	Instalación de Software sin supervisión	3	4	2	5	4	11
Riesgo Promedio							11

Activo: Software y Aplicaciones

Nro.	**Descripción de Riesgo**	Probabilidad	Impacto				Riesgo
			Financiero	Imagen	Operativo	Total	
1	Posibles ataques por uso de Antivirus y Antimalwares gratuitos	3	4	5	5	5	14
Riesgo Promedio							14

		Probabilidad	Impacto	ACTIVO
1	Instalación de Software sin supervición	3	4	Dispositivos
2	Posibles ataques por uso de Antivirus y Antimalwares gratuitos	3	5	Software y Aplicaciones

Matriz de Riesgos

IMPACTO	MUY ALTO (5)	MEDIO	MEDIO	2	MUY ALTO	MUY ALTO
	ALTO (4)	BAJO	MEDIO	1	ALTO	MUY ALTO
	MEDIO (3)	MUY BAJO	BAJO	MEDIO	ALTO	ALTO
	BAJO (2)	MUY BAJO	BAJO	BAJO	MEDIO	MEDIO
	MUY BAJO (1)	MUY BAJO	MUY BAJO	MUY BAJO	BAJO	MEDIO
		MUY BAJO (1)	BAJO (2)	MEDIO (3)	ALTO (4)	MUY ALTO (5)
	PROBABILIDAD					

TRATAR EL RIESGO

ACTIVO	RIESGO IDENTIFICADO
Dispositivos	Instalación de Software sin supervisión
Software y Aplicaciones	Posibles ataques por uso de Antivirus y Antimalwares gratuitos

CONTRAMEDIDAS
Controlar, supervisar y limitar todas las instalaciones realizadas en las computadoras
Adquirir Antivirus de paga o empresariales para asegurar la seguridad