Practica Nº2

Nombre: Rafael Antonio Patricio Ayllon **CI:** 10473854 **RU:** 108771

Análisis de Riesgos

Producto del análisis realizado a la financiera la caridad, se identificaron los siguientes puntos:

- la comunicación entre el edificio principal y su única sucursal se realiza mediante fibra óptica, además que se encuentra con un segundo proveedor de servicios ISP, para evitar cortes de servicio.
- Producto de algunos inconvenientes con la generación de reportes, se optó por comprar una solución de pago incluyendo el soporte para esta generación de reportes en tiempos y formas óptimas, dicho software agilizo de gran forma este proceso en la institución.
- Para la administración remota de todos los switches de la red interna, se tiene habilitado el protocolo telnet para hacer modificaciones de manera rápida.
- 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.
- Debido a la presión de la alta dirección, la aplicación móvil fue lanzada producción, únicamente siendo testeada con pruebas de caja blanca y caja negra.
- Ninguna de las PCs permite la utilización de memorias USB, DVDs, o cualquier tipo de medio removible sin la habilitación y revisión por el oficial de seguridad información.
- Recientemente finalizó 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.
- Para asignar un activo de información (PC) a un nuevo funcionario, primeramente, se procede a realizar la eliminación segura de toda la información que se almacenaba anteriormente en dicha PC (formato en bajo nivel).

TAREAS

Seleccionando únicamente los puntos donde se puede suscitar un incidente, identifique las amenazas, vulnerabilidades para poder realizar un análisis de riesgo siguiendo un enfoque metódico. (Utilice los 6 pasos aprendidos en clase).

Determinar el alcance

El Dpto. de Informática de la financiera “La Caridad” y los procesos que se desarrollan en esta unidad.

Identificar y valorar los activos

ACTIVO	IMPORTANCIA
Dispositivos	
(Switches de red interna D=5+I=4+C=3=>12)->12/3=4	**ALTA**
(Servidor web D=5+I=4+C=5=>14)->14/3=4.66->5	**MUY ALTA**
(PCs corporativas D=3+I=4+C=3=>10)->10/3=3.33->3	**MEDIA**
Software y aplicaciones	
(Aplicación móvil D=3+I=4+C=3=>10)->10/3=3.33->3	**MEDIA**
(Software de generación de reportes D=3+I=4+C=4=>11)->11/3=3.66->4	**ALTA**
(Software DLP D=5+I=5+C=3=>13)->13/3=4.33->4	**ALTA**
Telecomunicaciones	
(Comunicación por fibra óptica y enlace de respaldo ISP D=4+I=3+C=2=>9)->9/3=3	**MEDIA**
(Administración remota vía Telnet D=5+I=5+C=4=>14)->14/3=4.66->5	**MUY ALTA**
Personal	
(Oficial de seguridad de la información D=5+I=4+C=4=>13)->13/3=4.33->4	**ALTA**
Instalaciones	
(Edificio principal D=4+I=3+C=3=>10)->10/3=3.33->3	**MEDIA**
(Sucursal D=4+I=3+C=3=>10)->10/3=3.33->3	**MEDIA**

Dispositivos

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_01	Switches	Switches de red interna	Jefe del Dept. Inf. Sistemas	Switch (Físico)	Edificio principal y sucursal	Alta
ID_02	Servidor	Servidor web	Jefe del Dept. Inf. Sistemas	Servidor (Físico)	Edificio principal	Muy alta

ID_03	PCs	PCs de los corporativos	Jefe del Dept. Inf. Sistemas	Dispositivos (Físico)	Edificio principal	Media

Software y aplicaciones

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_04	App	Aplicación móvil	Jefe del Dept. Inf. Sistemas	Sistema (Lógico)	Servidor	Media
ID_05	Generador de reportes	Software para generación de reportes	Jefe del Dept. Inf. Sistemas	Sistema (Lógico)	Servidor	Alta
ID_06	DLP	Software para prevenir perdida de datos	Jefe del Dept. Inf. Sistemas	Sistema (Lógico)	Servidor	Alta

Telecomunicaciones

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_07	Fibra óptica	Canal de comunicaciones con la sucursal	Jefe del Dept. Inf. Sistemas	Cable (Físico)	Calle 1,2,3	Media
ID_08	TELNET	Software para conexiones remotas	Jefe del Dept. Inf. Sistemas	Sistema (Lógico)	CPD	Muy alta

Personal

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_09	Juan Perez	Responsable de la seguridad de información	Jefe del Dept. Inf. Sistemas	Consultor	Dept. Inf. Sistemas	Alta

Instalaciones

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_10	Edificio principal	Instalaciones primarias	Jefe de seguridad	Inmueble	Calle 1	Media

ID_11	Sucursal	Instalaciones de respaldo	Jefe de seguridad	Inmueble	Calle 5	Media

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. (AMENZA: ATAQUES INTENCIONADOS) -> acceso no autorizado (I, C), análisis de tráfico (C), conexiones sospechosas detectadas desde IPs de otros países.

Debido a la presión de la alta dirección, la aplicación móvil fue lanzada producción, únicamente siendo testeada con pruebas de caja blanca y caja negra. (AMENZA: ERRORES Y FALLOS NO INTENCIONADOS) -> vulnerabilidades de los programas (D, I, C), (AMENZA: ATAQUES INTENCIONADOS) -> manipulación de programas (D, I, C), lanzamiento con pruebas limitadas (solo caja blanca y caja negra) y fallas de seguridad explotables en producción.

Recientemente finalizó 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. (AMENZA: ERRORES Y FALLOS NO INTENCIONADOS) -> fugas de datos (C), (AMENZA: ATAQUES INTENCIONADOS) -> divulgación de información (C), pérdida de control sobre documentos confidenciales por expiración de la licencia del software DLP.

Telecomunicaciones

Para la administración remota de todos los switches de la red interna, se tiene habilitado el protocolo telnet para hacer modificaciones de manera rápida. (AMENZA: ATAQUES INTENCIONADOS) -> acceso no autorizado (I, C), intercepción de información (C), uso inseguro de Telnet para administración remota.

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 PISTAS DE AUDITORIA, MONITORIE INSUFICIENTE, No aplicación de filtros geográficos ni WAF (firewall de aplicaciones web).

Debido a la presión de la alta dirección, la aplicación móvil fue lanzada producción, únicamente siendo testeada con pruebas de caja blanca y caja negra. SOFTWARE NUEVO O INMADURO, ESPECIFICACIONES INCOMPLETAS, publicación apresurada sin pruebas de seguridad profundas.

Recientemente finalizó 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. AUSENCIA DE CONTROL DE CAMBIOS EFICAZ, GESTIÓN INADECUADA, falta de herramienta de monitoreo de datos sensibles.

Telecomunicaciones

Para la administración remota de todos los switches de la red interna, se tiene habilitado el protocolo telnet para hacer modificaciones de manera rápida. TRANSFERENCIA DE CONTRASEÑAS EN CLARO, ARQUITECTURA INSEGURA DE LA RED, uso de protocolo no cifrado susceptible a sniffing.

Evaluar el riesgo

Software y aplicaciones

Nº	DESCRIPCION DEL RIESGO	Probabilidad	Impacto				Riesgo
			Financiero	Imagen	Operativo	Total	
1	Conexiones sospechosas detectadas desde IPs de otros países.	4.66	3	4	4	3.66	17.05
2	Lanzamiento con pruebas limitadas y fallas de seguridad explotables en producción.	3.33	4	4	4	4	13.32
3	Pérdida de control sobre documentos confidenciales por expiración de la licencia del software DLP.	4.33	4	4	4	4	17.32
Riesgo promedio							47.69

Telecomunicaciones

Nº	DESCRIPCION DEL RIESGO	Probabilidad	Impacto				Riesgo
			Financiero	Imagen	Operativo	Total	
4	Uso inseguro de Telnet para administración remota.	4.66	4	4	5	4.33	20.17
Riesgo promedio							20.17

Tratar el riesgo

		Probabilidad	Impacto	Activo
1	Conexiones sospechosas detectadas desde IPs de otros países.	5	4	Software y aplicaciones
2	Lanzamiento con pruebas limitadas y fallas de seguridad explotables en producción.	3	4	Software y aplicaciones
3	Pérdida de control sobre documentos confidenciales por expiración de la licencia del software DLP.	3	4	Software y aplicaciones
4	Uso inseguro de Telnet para administración remota.	5	4	Telecomunicaciones

Matriz de riesgos

Muy Alto (5)	Medio	Medio	Alto	Muy alto	Muy alto
Alto (4)	Bajo	Medio	2, 3	Alto	1, 4
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)**

Descripción de contramedidas

Activo	Riesgo Identificado	Contramedida
Software y aplicaciones	Conexiones sospechosas detectadas desde IPs de otros países.	Configurar reglas de firewall para bloquear tráfico no autorizado. Mejorar logs y auditoría.
Software y aplicaciones	Lanzamiento con pruebas limitadas y fallas de seguridad explotables en producción.	Aplicar pruebas de seguridad (pentesting) y correcciones inmediatas post-lanzamiento.
Software y aplicaciones	Pérdida de control sobre documentos confidenciales por expiración de la licencia del software DLP.	Renovar contrato de DLP o implementar nueva solución de monitoreo de información sensible.
Telecomunicaciones	Uso inseguro de Telnet para administración remota.	Deshabilitar Telnet y habilitar administración por SSH (cifrado seguro).