Certificado de Profesionalidad en Seguridad Informática IronHack - SOC

Aplicación Práctica 2 Seguridad en Equipos Informáticos

Alumno: Julián Gordon

Índice

Introducción

En el contexto empresarial actual, la gestión de riesgos es esencial para asegurar la continuidad del negocio. En esta práctica, nos enfocaremos en una empresa de desarrollo web donde la disponibilidad de servicios es crucial. La organización utiliza una infraestructura compleja con servicios de hosting externos y aplicaciones en la nube. El objetivo es identificar, caracterizar y mitigar riesgos que puedan afectar la disponibilidad del servicio, como cortes de suministro eléctrico, ataques de virus y averías de hardware. Se empleará una metodología de análisis cualitativo para priorizar activos críticos y amenazas. Además se desarrollará un plan de acción para fortalecer la resiliencia de la empresa y garantizar la continuidad operativa, sugiriendo distintas salvaguardas que puedan mitigar los riesgos a los que se enfrenta la organización.

Práctica Análisis de riesgos

La organización para la que trabaja tiene como principal producto el desarrollo de páginas web. Para ello utiliza los servicios de hosting de distintas empresas, en las que contrata espacio web a nombre del cliente sobre los cuales lleva a cabo la instalación del software CMS, plantillas, personalización, etc. De forma adicional, gestiona el contenido de muchos de sus clientes, con compromisos de tiempo de respuesta ante sus solicitudes, recogidos en un SLA. La garantía contractual de disponibilidad con los proveedores es del 99,99%, que se considera suficientemente disponible y no entrará en el análisis de riesgos. El acceso a Internet se hace desde las oficinas que disponen en Málaga, mediante una línea FTTH, que se encuentra conectada al router del operador, a un firewall propio y de ahí a la LAN que da servicio a los puestos del personal de diseño. Estos acceden mediante un navegador a la aplicación de gestión. La principal vía de comunicación es el correo electrónico, por dónde reciben todo el contenido que los clientes les hacen llegar. Este servicio se encuentra en cloud, con el servicio de Microsoft Office 365 que ofrece una disponibilidad del 99%, la cual se considera suficientemente disponible y no entrará en el análisis de riesgos.

Como responsable de seguridad, la empresa le muestra su preocupación por la disponibilidad del servicio de actualización de contenidos frente a las amenazas de un corte de suministro eléctrico, de un virus que afecte a los equipos de la red y frente a averías de hardware, ya que las penalizaciones por no cumplimiento de los acuerdos con sus clientes son importantes, y le pide que haga un plan para reducir los riesgos de disponibilidad del servicio, con el criterio de reducir el mayor riesgos en esta dimensión. Realizando un análisis de forma cualitativa, ¿sobre qué riesgo y activo actuaría?

La metodología es libre, pudiendo usar MAGERIT de forma completa o parcial. En todo caso, limite a un max. de activos a 8 y el número de amenazas a las tres indicadas. PASOS:

- Identificar activos.
- Realizar el diagrama con las relaciones de activos y obtener su valor en la dimensión de disponibilidad.
- Caracterizar amenazas.
- Calcular el riesgo en base a la probabilidad de la amenaza y el valor (impacto) del activo.
- Proponer salvaguardas que reduzcan el/los riesgos mayores.

El primer paso que realizaremos para este análisis será la identificación de Activos:

- Servicio desarrollo páginas web
- Software CMS, Plantillas, Aplicación de gestión, navegador
- Contenido del cliente
- Conexión a internet FTTH – LAN
- Router, Firewall, Equipos
- Desarrolladores
- Instalaciones (Málaga)
- Electricidad

A continuación mostramos un diagrama con los activos y su valor en la dimensión de la disponibilidad junto con una tabla de valoración cualitativa y cuantitativa:

Activos	Dimensión (Disponibilidad)	Clasificación Magerit
Servicio desarrollo paginas web	Muy Alto 4	2.5. [S] Servicios
Software CMS, Plantillas, Aplicación de gestión, navegador	Alto 3	2.6. [SW] Software - Aplicaciones informáticas
Contenido del cliente	Muy Alto 4	2.3. [D] Datos / Información
Conexión a internet FTTH – LAN	Alto (3)	2.8 [COM] Redes de comunicaciones
Router, Firewall, Equipos	Alto (3)	2.7. [HW] Equipamiento informático (hardware)
Desarrolladores	Medio (2)	2.12. [P] Personal
Instalaciones (Málaga)	Medio (2)	2.11. [L] Instalaciones
Electricidad	Alto (3)	2.10. [AUX] Equipamiento auxiliar

Nivel de Disponibilidad	Descripción (Cualitativa)	Valor Numérico (Cuantitativo)
Muy Alto	El activo está disponible en todo momento y su ausencia es crítica.	4
Alto	El activo está disponible la mayor parte del tiempo.	3
Medio	El activo está disponible en momentos específicos o bajo condiciones.	2
Bajo	El activo experimenta interrupciones frecuentes.	1

En el siguiente diagrama, nos enfocaremos en caracterizar las amenazas en distintos factores, por la dimensión afectada, la clasificación Magerit y el activo afectado. Luego en las siguientes imágenes, mostramos un cuadro cualitativo y cuantitativo del Impacto de estas amenazas.

Amenazas	Dimensión Afectada	Clasificación Magerit	Activo Afectado
Corte suministro eléctrico	Disponibilidad	5.2.7. [I.6] Corte del suministro eléctrico	[HW] Equipos informáticos (hardware) [AUX] equipamiento auxiliar
Software dañino	D, I, C	5.4.6. [A.8] Difusión de software dañino	[SW] Aplicaciones (software)
Averías de Hardware	Disponibilidad	5.2.6. [I.5] Avería de origen físico o lógico	[SW] Aplicaciones (software) [HW] equipos informáticos (hardware) [AUX] equipamiento auxiliar

Impacto		
Descripcion	**Cuantitativo**	**Cualitativo**
Crítico al servicio o activo	4	Muy Alto
Significativo para el servicio ó activo	3	Alto
Moderado para el servicio ó activo	2	Medio
Bajo o nulo para el servicio o activo	1	Bajo

Impacto de las Amenazas		
Descripcion	**Cuantitativo**	**Cualitativo**
Corte Suministro Eléctrico	3	Alto
Software dañino (Malware)	4	Muy Alto
Averías de Hardware	2	Medio

Nivel de Impacto de Amenazas	Descripción
Muy Alto	La interrupción del servicio o el daño a los activos tendría consecuencias catastróficas y graves para la organización.
Alto	La interrupción del servicio o el daño a los activos tendría consecuencias críticas para la organización.
Medio	La interrupción del servicio o el daño a los activos tendría consecuencias moderadas para la organización.
Bajo	La interrupción del servicio o el daño a los activos tendría consecuencias menores o insignificantes para la organización.

Ahora analizamos la frecuencia de las amenazas.

Frequencia		
Descripcion	**Cuantitativo**	**Cualitativo**
Probable que suceda entre 1 y 2 años	4	Muy Alto
Probable que suceda en los próximos 3 a 5 años	3	Alto
Probabilidad moderada en los próximos 3 a 5 años	2	Medio
Probabilidad de ocurrencia baja en los proximos 5 años	1	Bajo

Frequencia		
Descripcion	**Cuantitativo**	**Cualitativo**
Corte Suministro Eléctrico	2	Medio
Software dañino (Malware)	3	Alto
Averías de Hardware	1	Bajo

Nivel de Probabilidad de Ocurrencia	Descripción
Muy Alta	La probabilidad de que ocurra la amenaza es extremadamente alta, y es probable que suceda dentro de los próximos 1-2 años.
Alta	La probabilidad de que ocurra la amenaza es alta, y es probable que suceda dentro de los próximos 3-5 años.
Media	Existe una probabilidad moderada de que la amenaza ocurra, y podría suceder en un plazo de 3 a 5 años.
Baja	La probabilidad de ocurrencia de la amenaza es baja, y es poco probable que suceda en los próximos 5 años o más.

En base a esto podemos determinar una relación del riesgo de estas amenazas en la organización. En la siguiente tabla, calculamos el riesgo en base a la probabilidad de la amenaza y el valor (impacto) del activo.

Tabla de Riesgo				
Frequencia / Impacto	**Muy Alto (4)**	**Alto (3)**	**Medio (2)**	**Bajo (1)**
Muy Alto (4)	**Muy Alto (16)**	**Alto (12)**	**Medio (8)**	**Bajo (4)**
Alto (3)	**Alto (12)**	**Alto (9)**	**Medio (6)**	**Bajo (3)**
Medio (2)	**Medio (8)**	**Medio (6)**	**Bajo (4)**	**Bajo (2)**
Bajo (1)	**Bajo (4)**	**Bajo (3)**	**Bajo (2)**	**Bajo (1)**

Ya en el siguiente cuadro podemos observar los resultados del riesgo, en un análisis cualitativo y cuantitativo.

Resultado	Descripción
Muy Alto	Resultado cuantitativo: 13-16
Alto	Resultado cuantitativo: 9-12
Medio	Resultado cuantitativo: 5-8
Bajo	Resultado cuantitativo: 1-4

El objetivo consiste en medir el grado de riesgo, para poder realizar una evaluación comparativa entre los diversos activos. A través de las relaciones establecidas, vemos a continuación un mapa de riesgos que facilitará la identificación de los activos con mayores riesgos y las amenazas que están generando dichos riesgos.

Activos	Clasificación Magerit	Riesgo de las Amenazas		
		Suministro Electrico	Malware	Averías HW
Servicio desarrollo paginas web	2.5. [S] Servicios			
Software CMS, Plantillas, Aplicación de gestión, navegador	2.6. [SW] Software - Aplicaciones informáticas		Alto	Bajo
Contenido del cliente	2.3. [D] Datos / Información			
Conexión a internet FTTH – LAN	2.8 [COM] Redes de comunicaciones			
Router, Firewall, Equipos	2.7. [HW] Equipamiento informático (hardware)	Medio		Bajo
Desarrolladores	2.12. [P] Personal			
Instalaciones (Málaga)	2.11. [L] Instalaciones			
Electricidad	2.10. [AUX] Equipamiento auxiliar	Medio		Bajo

Salvaguardas

Por último, nos queda proponer salvaguardas para mitigar los posibles riesgos dentro de la organización. Una vez que ya identificamos los activos, las amenazas a las que están sometidos y hecha la valoración de los riesgos, podemos concluir que el mayor riesgo, al que se enfrenta la organización, es el Malware. Por lo que el activo que tiene mayor riesgo es el Software y propondremos salvaguardas para intentar protegerlo.

La primer salvaguarda que proponemos es la implementación de un Software Antivirus y AntiMalware de calidad y se recomienda actualizarlo regularmente, configurarlo para realizar análisis programados y automáticos, así como mantener activas las funcionalidades de detección en tiempo real para una protección continua y proactiva contra posibles ataques de malware.

La segunda salvaguarda propuesta, es la implementación de programas de educación y concienciación del personal. Estos programas incluirían capacitaciones regulares sobre prácticas seguras en el uso de la tecnología, identificación de posibles amenazas y cómo reportar actividades sospechosas. Promover una cultura de conciencia en seguridad informática, entre los empleados y dueños de la organización, puede fortalecer las defensas de la empresa, disminuyendo así el riesgo asociado a la ingeniería social y a los errores humanos que puedan resultar en vulnerabilidades de seguridad.

La tercera salvaguarda propuesta implica la implementación de políticas de seguridad de Tecnologías de la Información (TI). Estas políticas establecerían directrices claras y procedimientos específicos para proteger los activos de la organización contra posibles amenazas cibernéticas. Se podrían incluir medidas como el uso de contraseñas robustas, la restricción de acceso a información confidencial según roles y la implementación de cifrado de datos.

Se pueden emplear sistemas de autenticación como contraseñas, tokens o autenticación de dos factores para garantizar que solo personas autorizadas puedan acceder a sistemas y datos críticos. Asimismo, estas políticas podrían abordar la gestión adecuada de dispositivos y software, así como la realización regular de copias de seguridad para garantizar la disponibilidad y la integridad de los datos. Además, es importante que estas políticas se actualicen y revisen periódicamente para adaptarse a las cambiantes amenazas y tecnologías. Finalmente, se debería asegurar la capacitación del personal en cuanto a la comprensión y el cumplimiento de estas políticas para una implementación efectiva y consistente en toda la organización.

Con las salvaguardas propuestas, disminuiría significativamente el riesgo de que el software sea comprometido por malware. Una vez que se hayan implementado las salvaguardas, es necesario llevar un seguimiento de estas y evaluar su impacto en los activos de manera regular.

Conclusiones

En esta práctica de análisis de riesgos en una empresa de desarrollo web, hemos identificado varios elementos cruciales para garantizar la disponibilidad y seguridad de los servicios ofrecidos. La gestión de riesgos es esencial en un entorno empresarial actualmente marcado por la dependencia de la tecnología y la conectividad en línea.

Hemos utilizado una metodología cualitativa para priorizar activos críticos y amenazas, permitiéndonos enfocarnos en las áreas de mayor riesgo para la organización. La identificación de activos clave, como el software, la conexión a Internet y los recursos humanos, nos ha permitido comprender mejor los posibles puntos vulnerables en la infraestructura de la empresa.

Tras caracterizar las amenazas potenciales, como cortes de suministro eléctrico, ataques de malware y averías de hardware, hemos calculado el riesgo en base a la probabilidad de la amenaza y el impacto en los activos.

Esto nos ha permitido identificar el malware como el mayor riesgo, especialmente para el software, y hemos propuesto salvaguardas específicas, como la implementación de software antivirus y antimalware de calidad, así como programas de educación y concienciación del personal.

Además, hemos sugerido la implementación de políticas de seguridad de TI para proteger los activos de la organización contra posibles amenazas informáticas. Estas políticas incluirían medidas como el uso de contraseñas robustas, la restricción de acceso según roles y la realización de copias de seguridad regulares. Con la implementación de las salvaguardas propuestas, la empresa puede reducir significativamente su riesgo de enfrentar problemas de disponibilidad y seguridad en sus servicios de desarrollo web. Es esencial que se realice un seguimiento continuo de estas medidas y se evalúe su impacto en los activos de la organización para garantizar la efectividad a largo plazo en la mitigación de riesgos.