Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Bastionado de redes y sistemas

UD02. Diseño de planes de securización.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico

El alumno debe identificar, en este supuesto, qué elementos/decisiones/acciones no cuadran con unas prácticas correctas de los planes de securización que pueden provocar problemas.

La empresa "Venus SA", dedicada a la cirugía estética y con sede en Ibiza. El grado de dependencia tecnológica es bajo ya que la mayor parte de la información que gestionan como los historiales de los pacientes se encuentran en formato físico. La empresa cuenta con 10 empleados distribuidos de la siguiente manera:

- ✓ Un CEO.
- ✓ Un empleado del departamento de RR.HH.
- ✓ Cinco doctores en cirugía estética.
- ✓ Dos empleados encargados de la limpieza y saneamiento de la clínica.
- ✓ Un recepcionista.

El CEO de la empresa ha decidido modernizar la clínica para ello se han marcado los siguientes hitos:

- ✓ Desarrollar una herramienta informática que gestione:
  - ➢ Historiales de los pacientes.
  - ➢ Nóminas.
  - ➢ Relaciones con proveedores.
- ✓ Informatizar todos los historiales.
- ✓ Adquirir nuevos equipos con los que poder utilizar la herramienta.
- ✓ Crear una página web corporativa de carácter informativo.
- ✓ Adquirir un nuevo servidor para alojar la herramienta.
- ✓ Reducir al máximo posible los costes y plazos de entrega.

Debido a que el presupuesto es reducido varias empresas con las que se han puesto en contacto se han negado a realizar el desarrollo pero finalmente una empresa local acepta los términos además garantizar costes y plazos.

Transcurrido no más de un mes la empresa desarrolladora ha terminado y deciden presentar al CEO de Venus SA. los resultados de su trabajo. Para ello pactan una reunión en la que los principales puntos tratados fueron:

- ✓ Con el fin de reducir costes tanto el programa gestor como la página web corporativa se ubican en el mismo servidor.
- ✓ La herramienta que gestiona informes, nóminas y proveedores ha sido desarrollada exprofeso para Venus SA.
- ✓ Para la página web corporativa se ha utilizado un gestor de contenidos o CMS de código abierto.
- ✓ El servidor se alojará en el cuarto destinado a guardar los productos y herramientas de limpieza.
- ✓ Como personal de mantenimiento de la herramienta y la página web se dará una formación al recepcionista de clínica.
- ✓ Todos los equipos serán configurados para que los usuarios puedan ser administrados por los propios usuarios.

- ✓ Le recomiendan que la informatización de los historiales antiguos la haga el personal interno, como el recepcionista, ya que el proceso es bastante sencillo y principalmente lo que hay que hacer es escanear documentos.

El CEO decide dar luz verde, para que la actualización sea lo menos traumática posible.

Esta se realizará durante el fin de semana así como la formación de los empleados.

Llegado el lunes, el recepcionista comienza a digitalizar todos los informes, el personal de recursos humanos hace lo propio con las nóminas y el CEO con los proveedores.

Después de una semana de arduo trabajo, sobre todo del recepcionista, el sistema está listo para ser utilizado por los doctores.

A los pocos días de uso de la herramienta esta deja de funcionar correcta y constantemente se producen caídas del servicio pese a los intentos del recepcionista-técnico de sistemas por solucionarlo. Tanto los doctores, como el personal de RR.HH. y el CEO deben volver a hacer su trabajo como lo habían estado haciendo hasta antes de la informatización de la clínica.

¿Qué te pedimos que hagas?

✓ Apartado 1: tarea de investigación

Una vez que conoces los diferentes modelos para aplicar ciberseguridad en una organización, en base al supuesto planteado deberás:

- ➢ Identificar qué elementos/decisiones/acciones no cuadran con unas prácticas correctas de los planes de securización.

La figura del CEO demuestra con sus decisiones, aunque sea por desconocimiento, no estar al 100% en este proceso, a pesar de haber tomado esa decisión.

Lo primero que podemos resaltar es la **ausencia de un análisis previo**. Toma la decisión sin hacer una **planificación de los riesgos**.

Muestra dar **prioridad a la reducción de costes y plazos de entrega**. Una decisión que habiendo cumplido la primera parte, seguramente no tomaría y que demostraría que apuesta por esa securización.

La **solución** (aunque se realice exprofeso como aseguran) **y** el **despliegue no** son los **adecuados**. Aunque no aparezca expresamente, es posible que **no** mantenga **política** alguna de **copias de seguridad.**

Utilizar un mismo servidor para la herramienta y para la web corporativa, **aumenta** no solo la **posibilidad de fallos** en cadena que afecten a ambas, sino también aumenta el **riesgo de ataque** y afectación común.

También es un riesgo que el **recepcionista** puede llegar a priori, a ser responsable del **mantenimiento** de ambas soluciones, al faltarle conocimientos y experiencia.

El cambio radical de un sistema tradicional a una solución informática **necesita de una formación adecuada**. Hacer todo en un fin de semana, alerta de la poca formación que han

recibido al respecto. El hecho de que el recepcionista (único con capacidad de acceso al sistema) no pueda corregir las incidencias, es otra prueba de ello.

Hay un **riesgo de seguridad física** en la instalación del **servidor en un cuarto** con productos **de limpieza**, donde es más fácil que pueda dañarse o que pueda robarlo.

➢ Ofrecer las mejores soluciones a los problemas previos.

Los costes de hoy pueden ser el ahorro y el beneficio del mañana. Desde esa prerrogativa inicial, habrían dado los siguientes pasos:

- **Contratar a un proveedor profesional** de servicios de ciberseguridad.
- **Análisis y planificación adecuados** a la transformación que necesita la empresa, por parte del proveedor, **evaluando e identificando necesidades** de la empresa, posibles **riesgos y amenazas** asociados a este proceso (incluyendo un procedimiento claro de **gestión de riesgos** para identificar, evaluar y mitigar en su caso los riesgos de ciberseguridad).
- **Desarrollo y despliegue** de una herramienta adecuada y diseñada en base al punto anterior, que incluya **medidas de mitigación** de riesgos, incluida una adecuada **política** de **copias de seguridad** optimizada.
- **Formar adecuadamente al personal** para la nueva herramienta informática. Esto **incluye** formar tanto al recepcionista como al resto de personal en **ciberseguridad**, concienciando, sensibilizando y adoptando **políticas de seguridad**.
- Adquirir un **servidor dedicado** y alojarlo en un **cuarto que sea seguro** y que pueda tener ciertas medidas de seguridad (alarma, control de acceso, cámaras…)