Implementación de buenas prácticas en el bastionado de sistemas y redes

Juan Carlos Ramos Moll *Bastionado de redes*

Índice

Escenario:....3
Analisis y posibles soluciones a los puntos presentados al CEO:....4
Punto 01: Con el fin de reducir costes tanto el programa gestor como la página web corporativa se ubican el mismo servidor....4
Análisis:....4
Posible solución:....4
Punto 02: La herramienta que gestiona informes, nóminas y proveedores ha sido desarrollada exprofeso para Venus SA....4
Análisis:....4
Punto 03: Para la página web corporativa se ha utilizado un gestor de contenidos o CMS de código abierto....4
Análisis:....4
Punto 04: El servidor se alojará en el cuarto destinado a guardar los productos y herramientas de limpieza....5
Análisis:....5
Posible solución:....5
Punto 05: Como personal de mantenimiento de la herramienta y la página web se dará una formación al recepcionista de clínica....5
Análisis:....5
Posible solución:....5
Punto 06: Todos los equipos serán conigurados para que los usuarios puedan ser adminstrados por los popios usuarios....5
Análisis:....5
Posible solución:....6
Punto 07: 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....6
Análisis:....6
Conclusión:....6

Escenario:

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 pagina web corporativa de carácter informativo.
- Adquirir un nuevo servidor para alojar la herramienta.
- Reducira 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.

“A partir de este punto voy a ir enumerando cada uno de los puntos tratados y comentando mis impresiones y recomendaciones”.

Analisis y posibles soluciones a los puntos presentados al CEO:

Punto 01: Con el fin de reducir costes tanto el programa gestor como la página web corporativa se ubican el mismo servidor

Análisis:

Este punto claramente es erróneo, ya que la herramienta de gestión interna tendría que estar separada de la Web corporativa. Con esta configuración estaríamos dando un punto de entrada a los atacantes.

Posible solución:

En mi opinión, se debería disponer de un servidor local solo por red interna (sin conexión a internet) para la aplicación de gestión y desplegar la web en algún sevicio de hosting gratuïto para no incrementar el coste en el presupuesto. De esta manera se reduciría ampliamente la vulneravilidad del sistema gestor.

Punto 02: La herramienta que gestiona informes, nóminas y proveedores ha sido desarrollada exprofeso para Venus SA.

Análisis:

Este punto lo encuentro correcto, ya que un software a medida, siempre va a garantizar un sistema de roles, autenticación y autorización mas adecuado para la organización.

Punto 03: Para la página web corporativa se ha utilizado un gestor de contenidos o CMS de código abierto.

Análisis:

Lo veo correcto siempre que la web se utilice solamente a modo de información y no de gestión.

Un CMS facilita mucho la labor de subuida de contenidos de plante del cliente, así como abarata el desarrollo de la misma, por lo que en un presupuesto reducido considero que es ideal.

Juan Carlos Ramos Moll *Bastionado de redes*

Punto 04: El servidor se alojará en el cuarto destinado a guardar los productos y herramientas de limpieza.

Análisis:

Otro punto claramente erróneo, un servidor en el que se guarda la información (activo más valioso de la organización) nunca debe situarse en una sala en la que se van a alojar materiales de limpieza que pueden ser: corrosivos, inflamables, etc…

Estariamos exponiendo a la organización a una perdida total de la información lo que supondría un gran coste económico para la misma.

Posible solución:

Trasladar los servidores a otra sala en la que se cuente con una buena ventilación y acondicionamiento térmico. Convencer al CEO de que este es el activo más importante de su empresa y que el coste de un desastre con los servidores sería mucho mayor que el pequeño incremento de acondicionar una sala solo para alojar el servidor.

Punto 05: Como personal de mantenimiento de la herramienta y la página web se dará una formación al recepcionista de clínica.

Análisis:

Este punto lo considero semi correcto, ya que el recepcionista por ejemplo tiene que tener acceso a la creación de nuevos clientes, pero no a la información de los historiales médicos ni a las nóminas de los empleados.

Posible solución:

Disponer de un sistema de autenticaión y autorización el cual jerarquice el acceso a las distintas secciones de la aplicación de gestión.

Punto 06: Todos los equipos serán conigurados para que los usuarios puedan ser adminstrados por los popios usuarios.

Análisis:

Erroneo al 100%, es parecido al punto anterior, nunca todos los empleados de una organización deben tener acceso a todos los recursos del software de gestión, ya que como es conocido el principal punto de entrada de los atacantes son los propios empleados. Si configuráramos así los accesos el atacante tendría multiples puntos puntos de acceso a los activos de la empresa.

Posible solución:

Disponer de un sistema de autenticaión y autorización el cual jerarquice el acceso a las distintas secciones de la aplicación de gestión.

Punto 07: 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.

Análisis:

Este punto lo considero correcto, ya que en mi opinión es el recepcionista el que tiene que realizar esta labor. Siempre y cuando se le de un acceso especial temporal a los recursos de creación y modificación de la información del Software Gestor.

Conclusión:

El caso presentado considero que es el típico en el que se intenta abaratar costes comprometiendo por completo la seguridad de los activos de la organización, hay que concienciar a las organizaciones, para que entiendan que su activo más importante es la información y que el coste de su pérdida sería mucho mayor que la inversión de tener un sistema robusto de seguridad.

Juan Carlos Ramos Moll *Bastionado de redes*