Gestión de la seguridad informática

Estudio de Caso: “Simón: Parte I”

Dickson Arley Garcia Rincon

SENA

Servicio Nacional de aprendizaje

**Estudio de Caso: “Simón: Parte I”**

Simón junto con 3 (tres) amigos iniciaron con un negocio de consultoría para llevar la contabilidad de microempresas, su trabajo ha tenido tan buena aceptación que otras empresas mucho más grandes los han contactado para contratar sus servicios, Simón y sus socios ven que su negocio está creciendo y que todo lo que hacían manualmente necesitan de apoyo tecnológico, el problema es que ellos no entienden de tecnología, ni de software y tampoco saben en qué tipo de modelo de negocio están.

Decidieron averiguar e invertir en infraestructura tecnológica. Para el personal que piensan contratar, compraron 6 (seis) equipos de cómputo tipo escritorio. Cuando les llegó la tecnología, muy contentos empezaron a destapar las cajas pero se encontraron con unos equipos que no sabían cómo instalarlos, unos CD con unos aplicativos del cual no entendían cuál sería la función que cumplirían dentro de su negocio y adicional a esto, debían hacer la instalación de una red para conectar sus ordenadores, navegar en la Internet y estar en contacto con los clientes.

Con base en lo anterior ¿Cómo le ayudarías a Simón a organizar su infraestructura tecnológica, asumiendo los riesgos reales en la instalación de la red de acuerdo con el modelo de negocio identificado?

**Desarrollo de actividad:**

De acuerdo al aprendizaje y la información disponible en el material de estudio. Se debe instalar un red PAN (Red de Área Personal): Estas redes se caracterizan por ser personales y pequeñas, ya que el máximo de equipos conectados a este tipo de red son 8 (ocho). Podríamos también definirla como una red de área local (LAN), pero apegado al material de estudio se denomina PAN.

Para la instalación de esta red se necesita utilizar un switch con 8 o más puerto para la conexión de los equipos, un router para conexiones inalámbricas.Tambiénn la contratación con un servidor de servicios de Internet (ISP: Es una empresa que brinda la conexión a Internet a sus clientes). La estructura de la red quedaría de la siguiente manera:



PC 1

PC 2

PC 3

PC 4

PC 5

PC 6

Switch

Firewall

Ethernet

Router

Smart Phone

Web Service

Impresora

La tipología de red utilizada es de estrella. La tipología de estrella, una de las tipologías más comunes, consiste en un switch (conmutador) central mediante el cual se transfieren todos los datos, junto con todos los nodos periféricos conectados a ese nodo central. Las tipologías de estrella tienden a ser confiables porque los equipos individuales pueden averiarse sin afectar al resto de la red. Pero si el switch central falla, ninguno de los nodos conectados podrá acceder al mismo. Los costos de cable para las redes en estrella también tienden a ser más altos.

Para la configuración de red se utilizaría Red basada en el protocolo IP: Las redes basadas en el Protocolo de Internet (IP) en la actualidad son muy importantes. Los datos en una red basada en IP son enviados en bloques conocidos como paquetes (Saucedo, A.). IP define las reglas a través de las cuales fluye la información en la red, donde cada computador debe ser identificado en esta, por medio de un numero IP, dicho número debe ser único. Y el rango de la IP estaría en la Clase C: Es el direccionamiento más común, se utilizan tres bytes para la red y el ultimo para los equipos. Este tipo de direccionamiento, tiene 2.097.152 redes y 254 equipos. Su rango es: 192.0.0.0 hasta el 223.255.255.255.



192.168.0.11

255.255.255.0

192.168.0.12

255.255.255.0

192.168.0.2 255.255.255.0

192.168.0.1 255.255.255.0

192.168.0.3 255.255.255.0

192.168.0.17 255.255.255.0

192.168.0.13 255.255.255.0

192.168.0.14 255.255.255.0

192.168.0.15 255.255.255.0

192.168.0.16 255.255.255.0

192.168.0.18 255.255.255.0

En cuanto a la configuracion del software, teniendo encuenta el enunciado del problema propuesto. Se debe instalar el sistema operativo y software de aplicación.

Software básico o sistema operativo. Es un conjunto de programas que controlan los trabajos del ordenador o computadora. Se encarga de administrar y asignar los recursos de hardware. Estos software son: Sistemas operativos, Controladores de dispositivos, Herramientas de diagnóstico, Herramientas de corrección y optimización, Servidores, Utilidades, BIOS, Gestores de arranque.

El software de aplicación, son programas que controlan y dirigen las distintas tareas que realizan las computadoras, creando un ambiente amigable entre el PC y el usuario. Llevan a cabo tareas de tratamiento de textos, gestión de bases de datos, documentos, imágenes y videos además para el envío y distribución de información. Entre ellas encontramos: Procesadores de texto (block de notas), Editores (Photoshop para el diseño gráfico), Hojas de cálculo (MS Excel), Sistemas gestores de bases de datos (MySql, postgress, Access), Programas de comunicación (MSN Messenger, Skype), Paquetes integrados (Ofimática: Word, Excel, Power Point), Programas de diseño asistido por computador (Autocad).

Por ultimo cabe resaltar que el resguardo de informacion y la seguridad de la misma depende de los niveles de seguridad que se mantengan. Para esto es importante inplementar buenas politicas de seguridad informatica asi como tambien el uso de ativirus y antispam, los cuales previenen la pérdida de informaciony garantizan la integridad de la informacion almacenada en los computadores y cuentas de correo electronico.

Además para garantizar la seguridad de la red, se debe tener en cuenta lo siguiente:

* Evitar los enlaces sospechosos: Uno de los medios más utilizados paradireccionar a las víctimas a sitios maliciosos son los hipervínculos o enlaces. Evitar hacer clic en éstos previene el acceso a páginas web que posean amenazas capaces de infectar al usuario. Los enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social: la clave está en analizar si son ofrecidos en alguna situación sospechosa (una invitación a ver una foto en un idioma distinto al propio, por ejemplo), provienen de un remitente desconocido o remiten a un sitio web poco confiable.
* No acceder a sitios web de dudosa reputación: A través de técnicas de Ingeniería Social, muchos sitios web suelen promocionarse con datos que pueden llamar la atención del usuario – como descuentos en la compra de productos (o incluso ofrecimientos gratuitos), primicias o materiales exclusivos de noticias de actualidad, material multimedia, etc. Es recomendable para una navegación segura que el usuario esté atento a estos mensajes y evite acceder a páginas web con estas características.
* Actualizar el sistema operativo y aplicaciones: El usuario debe mantener actualizados con los últimos parches de seguridad no sólo el sistema operativo, sino también el software instalado en el sistema a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.
* Descargar aplicaciones desde sitios web oficiales: Muchos sitios simulan ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso al momento que el usuario lo instala en el sistema. Por eso, es recomendable que al momento de descargar aplicaciones lo haga siempre desde las páginas web oficiales.
* Utilizar tecnologías de seguridad: Las soluciones antivirus, firewall y antispam representan las aplicaciones más importantes para la protección del equipo ante la principales amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante amenazas.
* Evitar el ingreso de información personal en formularios dudosos: Cuando el usuario se enfrente a un formulario web que contenga campos con información sensible (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del sitio. Una buena estrategia es corroborar el dominio y la utilización del protocolo HTTPS para garantizar la confidencialidad de la información. De esta forma, se pueden prevenir ataques de phishing que intentan obtener información sensible a través de la simulación de una entidad de confianza.
* Tener precaución con los resultados arrojados por buscadores web: A través de técnicas de Black Hat SEO , los atacantes suelen posicionar sus sitios web entre los primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público, como temas de actualidad, noticias extravagantes o temáticas populares (como por ejemplo, el deporte y el sexo). Ante cualquiera de estas búsquedas, el usuario debe estar atento a los resultados y verificar a qué sitios web está siendo enlazado.
* Aceptar sólo contactos conocidos: Tanto en los clientes de mensajería instantánea como en redes sociales, es recomendable aceptar e interactuar sólo con contactos conocidos. De esta manera se evita acceder a los perfiles creados por los atacantes para comunicarse con las víctimas y exponerlas a diversas amenazas como malware, phishing, cyberbullying u otras.
* Evitar la ejecución de archivos sospechosos: La propagación de malware suele realizarse a través de archivos ejecutables. Es recomendable evitar la ejecución de archivos a menos que se conozca la seguridad del mismo y su procedencia sea confiable (tanto si proviene de un contacto en la mensajería instantánea, un correo electrónico o un sitio web). Cuando se descargan archivos de redes P2P, se sugiere analizarlos de modo previo a su ejecución con una solución de seguridad.
* Utilizar contraseñas fuertes: Muchos servicios en Internet están protegidos con una clave de acceso, de forma de resguardar la privacidad de la información. Si esta contraseña fuera sencilla o común (muy utilizada entre los usuarios) un atacante podría adivinarla y por lo tanto acceder indebidamente como si fuera el usuario verdadero. Por este motivo se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud de al menos 8 caracteres. Como siempre, las buenas prácticas sirven para aumentar el nivel de protección y son el mejor acompañamiento para las tecnologías de seguridad. Mientras estas últimas se encargan de prevenir ante la probabilidad de algún tipo de incidente, la educación del usuario logrará que este se exponga menos a las amenazas existentes, algo que de seguro cualquier lector deseará en su uso cotidiano de Internet.