SEGURIDAD FISICA Y LOGICA EN REDES

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

INTRODUCCIÓN

- A continuación, abordaremos a detalle como y cuales elementos podemos utilizer para protejer nuestras redes, o computadores personales de personas inescrupulosas que quieren atacarnos para extraer información clave personal o táctica de la empresa, cuales combinaciones de hadware y software debemos realizar para asegurarnos de poner un alto al delito, también se van a nombrar los tipos de hardware y como deben ser utilizados.

Características de PXI y de una PMI

¿Cómo empezó todo?

Todo da inicios con el uso de la tecnologia y sobretodo con la actividad de comercio internacional y los procedimientos de transferencia de fondos de las instituciones bancarias los cuales siempre habían existido y se daban de una forma lenta aunque muy seguros, luego para los 90´s se inicia con el comercio internacional globalizado, tratados de libre comercio las empresas, las empresas de tecnología estaban en pleno desarrollo y no estaban preparadas para intervenir y ser el motor que detonara el comercio internacional mas intenso, para ellos se debía de agilizar las formas de pago internacionales entre las empresas con todos los protocolos de Seguridad necesarios, sin dejar de lado las operaciones locales, o sea había que hacer una estandarización, dicha estandarización. Para ello la ITU-T trabajó con urgencia en la estandarización de las Telecomunicaciones. Por lo anterior, la ITU-T, como parte de sus trabajos de normalización internacional, desarrolló una serie de conceptos y herramientas informáticas, cuya función es sustituir todas aquellas actividades que realiza la persona detrás de la ventanilla de un banco o aquellas funciones que ejecuta un cajero automático para otorgar dinero al poseedor de una tarjeta de crédito o débito.

Definición de conceptos

¿Qué es un certificado?

Un certificado es una confirmación de identidad y contiene información que se utiliza para proteger datos o establecer conexiones seguras de red. De este modo, el almacén de certificados, como su nombre lo indica, es el área del sistema donde se guardan los certificados.

Los propósitos que tiene la emisión de un certificado se listan a continuación:

- Asegurar la identidad de un equipo remoto.
- Probar su identidad ante un equipo remoto.
- Proteger los mensajes enviados por Internet (correos).
- Confirmar que el software procede de un editor de software.
- Proteger al software de alteraciones después de su publicación.
- Permitir que se cifren los datos en el disco.

Un certificaco debe contener (version, número de serie, algoritmo de firma, algoritmo hash, period de validez, clave pública, uso, adlgoritmo de identificación, huella digital, nombre descriptive, autenticación del servidor).

Existen varios tipos de certificados: personal, empresa, representante, persona jurídica, de atributo, de servidor seguro, de firma de código.

Para enviar un certificado están disponibles varios formatos de exportación de archivos, algunos de los más usados son:

- Estándar de sintaxis de cifrado de mensajes, certificado PKCS No. 7.P7B.
- X.509 codificado base 64 (.CER).
- DER binario codificado X.509 (.CER).

¿Cómo se obtiene un certificado de identidad?

Los servicios de autorización para emitir certificados tienen una extensa demanda en una Infraestructura de Clave Pública (PKI, por sus siglas en inglés). Normalmente, los certificados de identidad tienen un periodo de vigencia mayor al que tienen los derechos de acceso o los privilegios del usuario. Al vencerse la vigencia de un certificado, éste se revoca, es decir ya no puede utilizarse, lo cual provoca un incremento enorme en la demanda de los servicios de autorización. (Ver páginas 114 – 122 del libro de lectura.)

Atributos

Un atributo es la información que describe a un usuario o al medio ambiente de redes o digital, pueden almacenar pares de valores. La autoridad de atribuos es un almacen, es la autoridad que firma los certificados para asignar los privilegios, La infraestructura de administración de privilegios es la que gestiona los atributos y los privilegios de usuarios, algunos de los dispositivos que se pueden configurar como autoridades de atributos son bases de datos MySql, directories LDAP y algunos servidios de la WEB.

El papel de los protocolos en PKI y PMI

Los protocolos son importantes para el interncambio de información confidencial y de forma segura, por lo tanto se require de un protocolo que me lo permita, dicho protocol es un conjunto definido de procedimientos que se adoptan para asegurar la comunicación entre dos conjuntos de procesos que existen dentro de una misma capa dentro de una jerarquía de capas. (Ver páginas 130 – 135 del libro de lectura)

La seguridad fisica y lógica en redes

Riesgos fisicos de los centros de cómputo y de las redes

Dentro de éste tipo de riesgo no interesa tanto entender los desastres naturales sino entender que en las grandes empresas se almacena una copia de la información en línea en otra localidad donde, los cuales se ubican en lugares desconcidos y lejos de oficinas centrales, con fachadas que no aparentan ser lo que son, esto es una idea del por que la información es tan valiosa, por tanto deben tener la certeza total de que la información esta salvo, para el año 2005 la ANSI publica el estandar para la infraestructura de la Telecomunicaciones en los centros de datos, y para ellos define cuatro niveles que describen la disponibilidad de datos que pueden tomarse o consultarse del hardware de una instalación de cómputo. A mayor nivel, mayor confiabilidad en que los datos estarán disponibles cuando se necesiten.

La ingeniería social

Es una práctica para obtener la información confidencial de la persona atacada, ya sea que se trate de manipular o que se le engañe con sutileza para obtener la información deseada, está enfocada a la manipulación o al engaño de personas ingenuas o de Buena voluntad, para obtener información que al final sirve para cometer un delito de fraude.

La seguridad lógica en las redes

Es un término que hace mensión a la lógica matemática y a la logística que priva en cualquier computadora, a continuación veremos sobre los ataques más comunes que se tienen registrados.

Suplantación de la direccion IP

Esta técnica consiste en suplantar una dirección IP de un paquete IP de la computadora que envía dicho paquete por la dirección IP de otra computadora, lo que le permite al atacante enviar paquetes de manera anónima, tambien implica modificar el campo Dirección IP origen, para simular que el paquete proviene de otra dirección IP.

Uso de rastreadores de red

Un analizador de red, o un atrapador de información de la red, como también se le conoce, permite supervisar toda la información que pasa a través de una tarjeta de red, sobre todo si esta tarjeta es inalámbrica. Debido a que los analizadores de red son de uso cotidiano para los verdaderos administradores de redes, éstos también son accesibles y pueden ser utilizados por personas con malas intenciones; como contraparte, se desarrollaron los sistemas de detección de intrusos. Casi todos los protocolos de Internet no están cifrados, por lo que cuando se navega por una red sin utilizar un protocolo HTTPS (recuérdese que la S indica que se trata de un protocolo seguro) es posible interceptar la información que se envía o se recibe, como contraseñas o números de cuentas bancarias; esto lo logra un atacante con rastreadores de puertos

Medidas preventivas

A continuación algunas de las medidas que se recomiendan:

Contar con un buen antivirus instalado y actualizado en la computadora, no abrir los archivos adjuntos en correos de remitentes desconocidos, o de sitios web no confiables.

Siempre tener presente cuando se aabre una dirección URL que sea segura o sea HTTPS, ya que cuenta con certificado de Seguridad.
No proporcionar información personal a un sitio web que la solicite para accesar.
No utilizer antivirus piratas o falsos.

Sistema de prevención de intrusiones

Conocido tambien como IPS (Intruder Prevention System) es un software que controla el acceso de información en una red de cómputo, vigilando y detectando anormalidades en las vías por donde transita la información, dicho software tiene una serie de reglas o políticas de seguridad que le permiten tomar decisions, y proteje al equipo antes de que suceda la intrusion, en lugar de hacer las del antivirus que trata de eliminar o cambatir al intruso que ya se a alojado en la computadora.

CONCLUSIONES Y RECOMENDACIONES

En cuanto al tema de seguridad física y lógica de las redes, pudimos ver los distintos dispositivos de hardware o software que nos van a permitir evitar el fraude o incluso ue intrusos ingresen a nuestras redes o computadoras a realizar algún tipo de hecho malintencionado, y hacernos daño. Para ellos se ven los tipos de cortafuegos que existen y las recomendaciones que se nos hacen para aplicarlas a nivel físico como es la seguridad de las redes, edificios, datos entre otros, se recomienda incursionar en la investigación de temas que se han visto muy superficialmente como son las normas ISO.

REFERENCIAS BIBLIOGRÁFICAS

- Baca, G. (2016). *Introducción a la Seguridad informática* (1a. ed.). Grupo editorial Patria.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica