Modelos de Seguridad (Internet)

INGETTEL LTDA

Ingeniería Tecnología y Telecomunicaciones

JUSTIFICACION

Internet, que se creó como iniciativa gubernamental, se ha extendido por todo el mundo con un crecimiento notable durante los últimos 30 años. Expertos en tecnología y medios de comunicación califican de revolucionaria esta transición de internet, de unos pocos académicos a impregnar prácticamente todos los aspectos de la vida personal y profesional, pero la disponibilidad de este recurso no se ha librado de complicaciones y retos, ya que, han aparecido métodos numerosos para cometer ilícitos a través de la Internet, es por esta razón que se deben implementar sistemas de seguridad que garantice un uso seguro de Internet.

La seguridad en internet son todas aquellas precauciones que se toman para proteger todos los elementos que hacen parte de la red como infraestructura e información, la mas afectada por delincuentes cibernéticos. La seguridad informática se encarga de crear métodos, procedimientos y normas que logren identificar y eliminar vulnerabilidades en la información y equipos físicos, como los computadores.

Los delincuentes cibernéticos usan varios modos para atacar a una víctima en la red como los virus con los que logran vulnerar sistemas y alterar el funcionamiento de los dispositivos electrónicos; el phishing, que consiste en que un cibercriminal se hace pasar por una persona diferente por medio de correos electrónicos, mensajería instantánea o redes sociales para adquirir información confidencial como contraseñas, tarjetas de crédito, entre otros. Por esta razón se deben implementar modelos de seguridad que contrarresten estos ataques.

OBJETIVO

- Conocer las distintas vulnerabilidades y ataques a los usuarios en la red.

- Implementar modelos de seguridad que contrarresten las diferentes modalidades de ataques cibernéticos a los usuarios de la red.

TERMINOLOGIA

- **Antivirus**

Software diseñado para la detección, prevención y eliminación de Software mal intencionado o dañino para los sistemas.

- **Ataque de Fuerza Bruta**

Es un tipo de ataque que consiste en que el atacante intenta con todas las posibles combinaciones de letras, números y caracteres para acertar la contraseña, PIN o phassphrace.

- **Firewall**

Dispositivo o programa que controla el flujo de tráfico entre redes.

- **Firewall de Aplicaciones**

Un Firewall que inspecciona la capa 7 del Modelo OSI (aplicación) con el objetivo de bloquear contenido malicioso antes de que alcancé o abandone el Servidor de Aplicaciones (portal web, base de datos, etc).

- **Malware**

son programas diseñados para infiltrarse en un sistema con el fin de dañar o robar datos e información.

- **Phishing**

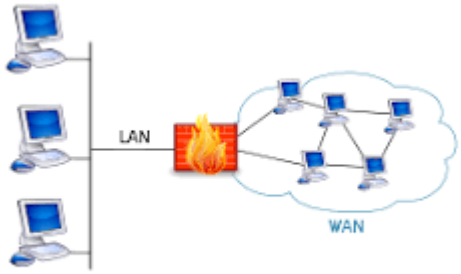
métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

- **Spam**

Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

MODELOS DE SEGURIDAD PARA INTERNET SEGURO

1. Uso De Firewall.



Un firewall o cortafuegos es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una misma red. Si el tráfico entrante o saliente cumple con una serie de Reglas que nosotros podemos especificar, entonces el tráfico podrá acceder o salir de nuestra red u ordenador sin restricción alguna. En caso de no cumplir las reglas el tráfico entrante o saliente será bloqueado.

El tipo de reglas y funcionalidades que se pueden construir en un firewall son las siguientes:

1. Administrar los accesos de los usuarios a los servicios privados de la red como por ejemplo aplicaciones de un servidor.

2. Registrar todos los intentos de entrada y salida de una red. Los intentos de entrada y salida se almacenan en logs.

3. Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como filtro de direcciones.

4. Filtrar determinados tipos de tráfico en nuestra red u ordenador personal. Esto también se conoce como filtrado de protocolo. El filtro de protocolo permite aceptar o rechazar el tráfico en función del protocolo utilizado. Distintos tipos de protocolos que se pueden utilizar son http, https, Telnet, TCP, UDP, SSH, FTP, etc.

5. Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que superen un determinado límite. De este modo es posible evitar algunos ataques de denegación de servicio.

6. Controlar las aplicaciones que pueden acceder a Internet.

7. Detección de puertos que están en escucha y en principio no deberían estarlo. Así por lo tanto el firewall nos puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

- **Sistema de Firewall Implementado en la Red de Ingettel Ltda**

La red de Ingettel Ltda se alimenta con un servicio de conexión a internet a través de Fibra Óptica, el servicio es entregado sobre un Router de Frontera marca Mikrotik de altas capacidades de procesamiento de tráfico, este Router se encarga de distribuir el ancho de banda, y permite el uso de Reglas de Firewall, provee funciones de seguridad que son usadas para el manejo del flujo de datos desde y hacia el Router, adicionalmente con el NAT, previene el acceso no autorizado a una red conectada directamente.

El modelo de seguridad implementado en la red para brindar seguridad a los usuarios es la aplicación de Reglas de Firewall en el Router de Frontera. Estas reglas nos permiten:

- Bloquear accesos no autorizados.

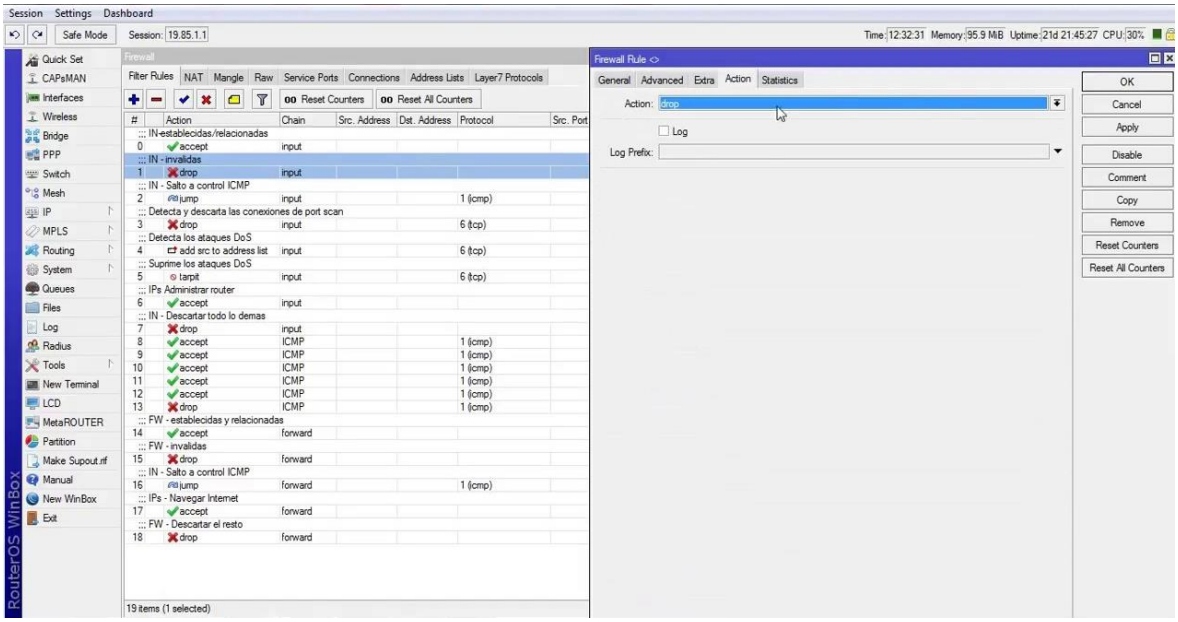
- Bloqueo de escaneo de puertos.

- Bloquear ataque DoS.

- Evita acceso entre equipos terminales (Clientes).

- Evita entrada de trafico no solicitado (por parte de los clientes).

A continuación se ilustra las reglas de Firewall implementadas para brindar seguridad en la res:



Como medida adicional los equipos de red como Radios, Routers y Swicthes actualizan automáticamente el firmware para añadir mas seguridad a sus sistemas operativos.

2. Antivirus

Un programa antivirus funciona al mantener un tipo de vigilancia dentro de una red. El programa antivirus con antispyware comprobará continuamente el sistema en busca de amenazas de malware. El usuario de la ordenadora tiene la opción de ejecutar un análisis de virus rápido, erradicando así los problemas de bajo riesgo más comunes. Para un análisis más detallado y la solución al problema, se recomienda un análisis de virus en profundidad.

Hay varios pasos involucrados en el proceso que un programa antivirus emplea para identificar una amenaza potencial a un ordenador. Considerando que hay nuevos virus, gusanos y amenazas de spyware en Internet, tener instalado antivirus no significa necesariamente que la protección es completa. Por esta razón, se cree fundamental mantener actualizaciones periódicas para la protección continua de su ordenador y todos sus ficheros.

Después de instalar y activar el antivirus, se debe realizar una prueba para asegurar que el programa se ejecuta sin problemas. Para ello debes abrir el programa en el equipo y seguir los pasos necesarios para ejecutar un análisis completo del sistema. Muchos programas antivirus vienen con un tutorial que podrás seguir si no está seguro de cómo ejecutar el software.

3. Como protegerse del Phishing

- ✓ La regla de oro, nunca le entregue sus datos por correo electrónico. Las empresas y bancos jamás le solicitaran sus datos financieros o de sus tarjetas de crédito por correo.
- ✓ Si duda de la veracidad del correo electrónico, jamás haga clic en un link incluido en el mismo.
- ✓ Si aún duda de su veracidad, llame o concurra a su banco y verifique los hechos.
- ✓ Si recibe un email de este tipo de phishing, ignórelo y jamás lo responda.
- ✓ Compruebe que la página web en la que ha entrado es una dirección segura ha de empezar con https:// y un pequeño candado cerrado debe aparecer en la barra de estado de nuestro navegador.
- ✓ Cerciórese de siempre escribir correctamente la dirección del sitio web que desea visitar ya que existen cientos de intentos de engaños de las páginas más populares con solo una o dos letras de diferencia.
- ✓ Si sospecha que fue víctima del Phishing, cambie inmediatamente todas sus contraseñas y póngase en contacto con la empresa o entidad financiera para informarles.

4. Como protegerse del Malware.

Las acciones se dividen en dos partes: mantenerse atento y utilizar herramientas de protección. Uno de los medios más populares para propagar malware es el correo electrónico, en el que el malware se puede disfrazar como un mensaje procedente de una empresa conocida, como un banco o un mensaje personal de un amigo.

Ten cuidado con los correos electrónicos que te solicitan contraseñas, así como con los correos que parecen provenir de amigos, pero contienen mensajes del tipo "¡Visita este interesante sitio web!" seguido por un enlace.

Permanecer atento es la primera capa de protección contra el malware, pero no basta con tener cuidado. Como la seguridad empresarial no es perfecta, incluso las descargas desde sitios legítimos pueden contener malware. Por consiguiente, aún el usuario más prudente está en riesgo, a menos que tome medidas adicionales.

BIBLIOGRAFIA

1. Que es la seguridad en internet. Tomado de:
https://edu.gcfglobal.org/es/seguridad-en-internet/que-es-la-seguridad-en-internet/1/

2. Terminología Seguridad Informática. Tomado de:
https://blog.cerounosoftware.com.mx/t%C3%A9rminos-de-seguridad-inform%C3%A1tica-glosario

3. Firewalls. Tomado de:

https://geekland.eu/que-es-y-para-que-sirve-un-firewall/

4. Antivirus. Tomado de:

https://www.loyvan.com/informatica/el-uso-de-los-antivirus/

5. Phishing. Tomado de:

https://www.infospyware.com/articulos/que-es-el-phishing/

6. Malware. Tomado de:

https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it