POLITICAS DE SEGURIDAD

Internet es una red de ordenadores que fue diseñada en los años 70 partiendo de recursos bastante limitados, comparados con los disponibles en la actualidad en cualquier organización. En un principio el objetivo fundamental era facilitar el intercambio de información entre los profesores e investigadores de distintas instituciones universitarias: básicamente, envío de mensajes de correo electrónicos en formato de texto, así como la difusión de algunos documentos de texto con resultados de los estudios y trabajos de investigación. Hoy en dia su auge ha crecido de manera exponencial y las vulnerabilidades a las que se encuentra expuesto cualquier usuario tambien, Por este motivo JEFFERSON-AFE S.A.S, pone a disposicion de sus clientes informacion y tips basicos con los cules pueden protegerse y proteger sus equipos cuando navegan en internet.

Tipos de amenazas a la seguridad en las redes de ordenadores

Desde el 22 de noviembre de 1988, cuando Robert Morris protagonizó el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en un famoso “worn” o gusano de Internet y con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos ante ciertos tipos de ataques a los cuales se encuentra expuesto si navega en Internet, han evolucionado, asi mismo, las empresas deben enfrentarse a muchas amenazas combinadas que exploran las diferentes vulnerabilidades con el fin de crear un ataque tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya, Crackers, hackers, ataques de denegacion de servicios, fuerza bruta y golpeo de puertos, entre otros. Por esta razon muchas agencias contra ataques informaticos comenzaron a crearse y su misión principal es facilitar una respuesta rápida a los problemas de seguridad que afectaran a redes de ordenadores conectados a Internet, no obstante, usted como cliente puede proteger sus equipos utilizando cualquiera de los siguientes elementos:

- Cortafuegos (Firewall): Básicamente los firewall son elementos de protección entre internet y una red local, los cuales se encargan de

bloquear o filtrar paquetes de información autorizando o desautorizando su ingreso o salida de una red. Existen firewall de software o hardware. Este filtrado se hace a través de reglas, donde es posible bloquear direcciones (URL), puertos, protocolos, entre otros.

- Anti-virus: Son programas capaz de detectar, controlar y eliminar virus informáticos y algunos códigos maliciosos (Troyanos, Works, Rootkits, Adware, Backdoor, entre otros). En el mercado existen los siguientes tipos de antivirus:
- Anti-spam: Programas capaz de detectar, controlar y eliminar correos spam.
- Criptografía: programas capaces de cifrar y descifrar información con claves secretas, donde los mensajes o archivos sólo puedan ser leídos por las personas a quienes van dirigidos, evitando la interceptación de éste.

Los fraudes y estafas financieras a través de Internet se han hecho muy frecuentes en los últimos años, las siguientes son amenazas tecnicas que podrian ser utilizadas.

- **Phishing:** Se referiere al tipo de ataques que tratan de obtener los números de cuentas y claves de accesos de servicios bancarios para realizar con ellos operaciones comerciales fraudulentas que perjudiquen a los legítimos propietarios. Normalmente se utilizan páginas web falsas que imitan las originales.
- **Pharming:** Es una variante del phishing en la que los atacantes utilizan un virus que conecta a las víctimas desde su ordenador a paginas falsas, en lugar de las legitimas de sus bancos para capturar números de cuentas, usuar ios y claves de accesos.
- **Ransom ware:** Es software malicioso que busca el lucro por medio de rescates - es un tipo de extorsión. Un caso famoso fue el PGPcoder en mayo de 2005 que pretendía dinero a cambio de que los usuarios afectados pudiesen restaurar su información de ficheros.

¿Cómo se puede evitar?

Siempre que observe este tipo de mensajes, aga caso omiso a ellos y ingrese directamente al sitio oficial desde s navegador, nunca desde el enlace enunciado en el correo, ni dando clic a dicho enlace. Evite el envío de mensajes cadena, pornografía, mensajes no solicitados, bromas a otros remitentes de correo. Cuando ingrese al sitio, valide que la seguridad que se indica a través de certificados digitales, si estén respaldados, de doble clic el icono de seguridad, que debe estar ubicado en la parte inferior derecha del navegador (no dentro de la página).

Ejemplo: Conozca de antemano cual es la dirección o URL del sitio real y valide este nombre cada que ingrese a realizar un proceso donde deba ingresar sus datos. Recuerde que el atacante utiliza técnicas que pueden engañar la percepción del sitio cuando se lee. Si usted es un usuario frecuente portales donde se ingresan datos personales, manténgase actualizado, consultando en la página de la policía nacional (http://www.policia.gov.co/), CAI virtual, los últimos eventos, recomendaciones y consultas en línea.

Tips de seguridad

• Evite Alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma implicita o explicita contengas informacion de actividades sexuales con menores de edad, o que atenten contra los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquella que la aclare, modifique o adicione o todas las leyes que lo prohíban.

•Mantenga siempre su antivirus actualizado en su equipo(s), si estos trabajan bajo windows o en lo posible trate de trabajar en dispositivos con disposiciones linux, a su vez, procure correr el antivirus periódicamente, de la misma manera, tenga en su equipo elementos como anti-spyware y bloqueadores de pop-up (ventanas emergentes).

•Evite visitar páginas no confiables o instalar software de dudosa procedencia. La mayoría de las aplicaciones peer-to-peer contiene programas espías que se instalan sin usted darse cuenta. Asegúrese que se

aplican las actualizaciones en sistemas operativos y navegadores Web de manera regular.

•Si sus programas o el trabajo que realiza en su computador no requieren de popup, Java support, ActiveX, Multimedia Autoplay o auto ejecución de programas, deshabilite estos. Si asívlo requiere, obtenga y configure el firewall personal, esto reducirá el riesgo de exposición.

•No preste su cuenta de correo ya que cualquier acción será su responsabilidad ni divulgue información confidencial o personal a través del mismo.

•Si recibe un correo con una advertencia sobre su cuenta bancaria, no debe contestarlo. Nunca responda a un correo HTML con formularios embebidos.

• Si ingresa la clave en un sitio no confiable, procure cambiarla en forma inmediata para su seguridad y en cumplimiento del deber de diligencia que le asiste como titular de la misma.

•Nunca hacer click en enlaces dentro del correo electrónico aun si parecen legítimos. Digite directamente la URL del sitio en una nueva ventana del navegador.

•Para los sitios que indican ser seguros, revise su certificado SSL.

•No reenvié los correos cadenas, esto evita congestiones en las redes y el correo, además el robo de información contenidos en los encabezados.

•No divulgue información confidencial suya o de las personas que lo rodean.

•No hable con personas extrañas de asuntos laborales o personales que puedan comprometer información.

•Utilice los canales de comunicación adecuados para divulgar la información.

• Valide con la entidad con quien posee un servicio, si el mensaje recibido por correo es válido.

•Cambie sus contraseñas frecuentemente, mínimo cada 30 días, a su vez, use contraseñas fuertes: Fácil de recordar pero difícil de adivinar.

•No envié información de claves a través del correo u otro medio que no esté encriptado.

Medios de seguridad JEFFERSON-AFE S.A.S

La salida de trafico de cada uno de nuestros clientes hacia internet se da a travez de una direccion IP proporcionada al equipo de borde del mismo y que sirve como identificacion para cada paquetes que intente atravezar nuestra red, cada uno de estos paquetes son minuciosamente filtrados por puerto, procolo o URL en un Firewall ubicado dentro de nuestro servidor principal, el cual autoriza o desautoriza el transito de dicho paquete. Este firewall cuenta con las siguientes capacidades:

- Antispam.
- Filtrado e URL, el objetivo de ellas es filtrar trafico con contenido de pornografia infantil.
- Bloqueo de ataques DoS, DDos, fuerza bruta, port knocking, entre otros.
- Bloqueo de puertos.

Por otra parte en el lado del cliente se cuenta con dispositivos CPE que permiten el filtraje y autoriacion de diferentes servicios y usuarios a la red, proporcionando una conexión a internet mas segura.