SEGURIDAD EN LA WEB.

Un efecto secundario del crecimiento exponencial que ha tenido el Internet es la privacidad de información tanto personal como profesional. En Internet encontramos funcionando tiendas en línea, negocios que mueven grandes cantidades de dinero, redes de los servicios que habilitan el comercio a nivel internacional así como sitios de redes sociales que contienen información muy delicada de la vida privada de sus miembros.

Mientras más se conecta el mundo, la necesidad de seguridad en los procedimientos usados para compartir la información se vuelve más importante. Desde muchos puntos de vista, podemos creer sin dudar que el punto más crítico de la seguridad del Internet, lo tienen las piezas que intervienen de forma directa con las masas de usuarios y los servidores web.

Por tal motivo **FUTURE SOLUTIONS DEVELOPMENT S.A.S** como proveedor del servicio de TELECOMUNICACIONES pone a disposición de todos sus clientes y de la comunidad en general, conceptos teórico - prácticos de la seguridad en internet que pueden evitar o reducir los riesgos a que se está expuesto cuando se interactúa con el mismo y sus elementos asociados.

¿Por qué requiere atención especial la seguridad en el Web?

- Internet es una red de dos sentidos. Así como hace posible que los servidores Web divulguen información a millones de usuarios, permite a los hackers, crackers, criminales y otros, irrumpir en las mismas computadoras donde se ejecutan los servidores Web.
- Las empresas, instituciones y los gobiernos utilizan cada vez más el Word Wide Web para distribuir información importante y realizar transacciones comerciales. Al violar servidores Web se pueden dañar reputaciones y perder dinero.
- Aunque la Web es fácil de utilizar, los servidores son piezas de software extremadamente complicadas y tienen diversas fallas de seguridad potenciales.
- Es mucho más onerosa y tardada la recuperación de un incidente de seguridad que implementar medidas preventivas.

OBJETIVOS DE LA SEGURIDAD EN LA WEB

La seguridad en la web es el conjunto de procedimientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información de una persona u organización.

- ***Integridad:*** Es necesario asegurar que los datos no sufran cambios no autorizados, la pérdida de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques. El sistema contiene información que debe se protegida de modificaciones imprevistas, no autorizas o accidentales, como información de censo o sistemas de transacciones financieras.

- ***Disponibilidad:*** Se refiere a la continuidad operativa de la entidad, la pérdida de disponibilidad puede implicar, la pérdida de productividad o de credibilidad de la entidad. El sistema contiene información o proporciona servicios que deben estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes, como sistemas esenciales de seguridad y protección de la vida.
- ***Confidencialidad:*** Se refiere a la protección de datos frente a la difusión no autorizada, la pérdida de confidencialidad puede resultar en problemas legales, pérdida del negocio o de credibilidad. El sistema contiene información que necesita protección contra la divulgación no autorizada, como información parcial de informes, información personal o información comercial patentada .

Estos aspectos además de lidiar con el riesgo que representan los atacantes remotos, se ven amenazados también por los riesgos por desastres naturales, empleados desleales, virus y sabotaje, entre otros.

VULNERABILIDADES Y AMENAZAS

La vulnerabilidad es la exposición latente a un riesgo, en la internet existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

ELEMENTOS DE PROTECCIÓN:

- ***Cortafuegos (Firewall):*** Básicamente los firewall son elementos de protección que se encargan de bloquear o filtrar paquetes de información entre dos redes, que puede ser Internet o una Intranet. 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:
- ***Antivirus prenventores:*** Estos antivirus se caracterizan por avisar antes de que se presente la infección. Este tipo, por lo general, permanece en la memoria del computador, monitoreando las acciones y funciones del sistema.
- ***Antivirus identificadores:*** Este tipo de antivirus tiene objetivo identificar programas infecciosos que pueden afectar el sistema. Además, rastrean secuencias de códigos

específicos vinculados con dichos virus.

- ***Antivirus descontaminadores:*** Tienen características similares a los identificadores. Sin embargo, se diferencian en que estos antivirus se especializan en descontaminar un sistema que fue infectado, a través de la eliminación de programas malignos. El objetivo principal de este tipo de virus es que el sistema vuelva a estar como en un inicio.
- ***Anti-spam:*** Programas capaz de detectar, controlar y eliminar correos spam.
- ***Criptografía:*** Es el arte 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 éstos.

AMENAZAS TÉCNICAS DE SEGURIDAD:

- ***Spam:*** Los spam son correos basura que se deben al envío de cualquier cualquier tipo de mensaje masivo o no, a personas a través correo electrónico que incluyen temas tales como pornografía, bromas, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).
- ***Ingeniería social:*** Es la manipulación de las personas para convencerlas de que ejecuten acciones, actos o divulguen información que normalmente no realizan, entregando al atacante la información necesario para superar las barreras de seguridad.
- ***Código Malicioso:*** Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Ejemplo: Troyanos, Works, Spyware, Rootkits, Adware, Backdoor, Cookies, Dialers, Exploit, Hijacker, keyloggers, Pornware, etc.
- ***Hoax:*** Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena, aparte de ser molesto, congestiona las redes y los servidores de correo, pueden ser intencionales para la obtención de direcciones de correo para posteriormente ser utilizadas como spam. Algunos de los Hoax más conocidos son correos con mensajes sobre virus incurables, temática religiosa, cadenas de solidaridad, cadenas de la suerte, Regalos de grandes compañías, entre otros.
- ***Suplantación*****:** Hacerse pasar por algo o alguien, técnicamente el atacante se hace pasar por un servicio o correo original.

FRAUDES

Phishing: Es la capacidad de duplicar una página Web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada. Se tienen dos variantes de esta amenaza:

- ***Vishing:*** Utilización de técnicas de phishing pero para servicios asociados con voz sobre IP (VoIP).

- ***Smishing:*** Utilización de técnicas de phishing en los mensajes de texto de teléfonos móviles.

1.¿Cómo funciona?

A través de Sitio Web En primera instancia los atacantes crean un sitio Web similar al original, trascribiendo textos, pegando las mismas imágenes y los mismos formularios para digitar los datos. Una vez creado el sitio, lo publican en la Web con un alias parecido al sitio original.

Ej: Reemplazando un simple de caracteres, usando un dominio real como prefijo:

- Sitio oficial: www.sitioReal.com
- Sitio falsos: www.sitioReal.com.sitio.com
- Variaciones: www.sitioReal-account.com www.sitioReal.actualiza.com
- Jugar con la percepción y la lectura del usuario:

  www.sitiio.Real.com

  www.sitio.Rea1,com

  www.sitio.Real.com/bin/actualiza

Adicional a esto, fijan una imagen simulando ser un sitio seguro (con certificados digitales) que a simple vista, da mucha confianza pero son FALSOS:

Una vez realizado esta labor y utilizando mecanismos masivos de comunicación como el spam, envían correos indicando a los “posibles” clientes o usuarios del portal a que actualicen sus datos, invocando la posibilidad de dar obsequios o premios si hacen esta acción.

- **A través de Correo electrónico:** Esta modalidad es realizada enviando correos masivos a las personas solicitando informen sus datos personales, lo correos engañosos pueden indicar que existe un problema técnico y es necesario restablecer las contraseñas. Los correos llegan a nombre de una empresa o razón social, donde el atacante suplanta el nombre de dicha empresa

2. ¿A quién le puede pasar?

A cualquier usuario que tenga un correo electrónico y acceso a Internet, donde periódicamente haga consultas y/o actualizaciones en portales que le presten servicios: Tiendas virtuales, Bancos, portal de correo, pago de servicios públicos, etc.

3. ¿Dónde está el peligro y cómo podemos ser víctimas?

El peligro radica en que, al ser una página falta, inducen a los usuarios a que ingresen los datos personales, como cuantas de correo, número de tarjetas de crédito, claves, etc. y estos datos son

recogidos por el atacante en bases de datos ajenas a las entidades oficiales de los sitios. Al sitio Web “similar” al original, es difícil que el usuario se percate, en primera instancia, de que se trata de un engaño. Cuando llega un correo indicando sean actualizados los datos, los usuarios validan las bondades de estar actualizados e ingresan desde el enlace o link del correo, directamente a la página falsa. Al ser un spam “atractivo”, los usuarios hacen un reenvió de este a más usuario, formándose una cadena o Hoax para capturar más y más personas. Y si es a través del correo, los usuarios enviarían los datos personales (usuario y contraseña) a un correo desconocido.

4. ¿Cuáles son las consecuencias?

Una vez se ingresen los datos personales, son almacenados en bases de datos del atacante, que posteriormente utilizará en beneficio propio para realizar estafas o robos de dinero, dado que tiene en número de la cuenta bancaria y la clave de acceso (si el sitio falso es una entidad bancaria).

5. ¿Cómo se puede evitar?

Siempre que llegue este tipo de mensajes, ingrese directamente al sitio oficial desde el browser o navegador, nunca desde el enlace l link 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.

INTERNET SANO

Internet sano es una iniciativa del Gobierno nacional, que en cabeza del Ministerio de Comunicaciones, busca ponerle control a la red. Ahora, los padres de Colombia contarán con el apoyo de las autoridades para denunciar las actividades sospechosas en internet. La imagen de la campaña está representada por SUSY90, una niña que conoce muy bien www, es decir, la red mundial de información y le da consejos a todos sobre cómo navegar en internet de manera sana.

Muchos padres de familia se atemorizan porque saben que sus hijos están expuestos diariamente a los peligros que hay en las redes de información, por donde pasan todo tipo de mensajes, nocivos o

didácticos. ¿Pero quién establece ese control?

Navegar en la red de forma sana significa consultar información, encontrarse con amigos en el chat, divertirse jugando, hacer parte de algún foro o de redes de aprendizaje. Pero no es sano que personas desconocidas contacten a sus hijos en algún chat pidiéndoles información personal. Tampoco es sano establecer citas a ciegas con propósitos desconocidos.

Lo que la campaña Internet Sano busca es que sus hijos no corran riesgos al navegar y además proteger la dignidad infantil.

Si usted entra a la página web www.internetsano.gov.co o a través de la línea gratuita 018000 912667 encontrará formas para denunciar los sitios que contengan pornografía infantil; estas denuncias llegan al DAS o a la Policía Nacional y son verificadas. Luego, estas URL son reportadas al Ministerio de Comunicaciones.

De esta forma, el Ministerio puede exigir a los Proveedores de Acceso a Internet (ISP) el bloqueo de estas páginas en Colombia. Todo esto es un trabajo en conjunto con otros países, de hecho la mayoría de redes de pornografía infantil son extranjeras y van de la mano con la trata de blancas.

De las 45 denuncias que se producen al mes, según datos de la Unidad de Investigaciones Informáticas y Electrónicas, todas se refieren a páginas extranjeras, aunque sus participantes sean colombianas o de cualquier otro país.

Se puede encontrar mayor informacion en nuestra pagina web en el siguiente enlace http://fsdcomunicaciones.com/denuncia.html.

TIP DE SEGURIDAD

- Pornografía Infantil: Evite Alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o directa se encuentren actividades sexuales con menores de edad, en 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.
- Control de virus y códigos maliciosos: Mantenga siempre un antivirus actualizado en su equipo(s), procure correr éste 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 así lo requiere, obtenga y configure el firewall personal, esto reducirá el riesgo de exposición.

Correo electrónico:

- No publique su cuenta de correo en sitios no confiables. • No preste su cuenta de correo ya que cualquier acción será su responsabilidad.
- No divulgue información confidencial o personal a través del correo.
- Si un usuario 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.

Control de Spam y Hoax:

- Nunca hacer click en enlaces dentro del correo electrónico aun si parecen legítimos. Digite directamente la URL del sitio en una nueva ventana del browser.
- 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.
- Control de la Ingeniería social:
- 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.

Control de phishing y sus modalidades:

- Si un usuario recibe un correo, llamada o mensaje de texto con una advertencia sobre su cuenta bancaria, no debe contestarlo.
- Para los sitios que indican ser seguros, revise su certificado SSL.
- Valide con la entidad con quien posee un servicio, si el mensaje recibido por correo es válido.

Robo de contraseñas:

- Cambie sus contraseñas frecuentemente, mínimo cada 30 días.
- Use contraseñas fuertes: Fácil de recordar y difícil de adivinar.
- Evite fijar contraseñas muy pequeñas, se recomienda que sea mínimo de una longitud de 10

caracteres, combinada con números y caracteres especiales.

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

MECANISMOS DE SEGURIDAD DE FUTURE SOLUTIONS DEVELOPMENT

FSD S.A.S cuenta con sistema de autenticación y autorización por IP-MAC para controlar el acceso de los usuarios a los servicios de la red, al igual que controles de autenticación para los usuarios en los equipos terminales. Para proteger las plataformas de los servicios de Internet, FSD S.A.S ha implementado configuraciones de seguridad en los diferentes equipos de red, lo que comúnmente se llama líneas base de seguridad, además del establecimiento de medidas de seguridad a través de elementos de control y protección situados en su servidor principal como:

- ***Firewall:*** FSD S.A.S cuenta con un mecanismo de firewall que realiza un continuo análisis de todos los paquetes de datos que entran o salen de su red, creando una protección perimetral entre la internet y la red de los clientes, y creando un control que reduce el nivel de impacto ante los riesgos de seguridad.
- ***Filtrado de URLs:*** Los clientes pueden realizar filtrado de URL a través de sus navegadores Web, se sugiere instalar además sistemas parentales. FSD S.A.S cuenta con varios mecanismos capaces de realizar el bloqueo de URLs, entre ellos se encuentran los sistemas DNS y una herramienta para todo el tráfico hacia Internet, el objetivo principal de bloquear las que contengan o promuevan la pornografía infantil en Internet a través imágenes, textos, documentos y/o archivos audiovisuales.

Por otra parte se brinda *Seguridad a nivel del CPE,* donde los dispositivos de conexión final ubicados en las premisas de los clientes cuentan con elementos bases para la autenticación y autorización, además de un firewall, con ello permiten hacer una conexión a Internet de manera más segura.

REFERENCIAS

Para mayor información puede consultar los siguientes sitios:

http://www2.uah.es/etsii/master_etsii/especializacionADTIC/SI/objetivosSI.html

http://www.seguridad.unam.mx/documento/?id=17

https://es.wikipedia.org/wiki/Spam

http://www.internetsano.gob.ar/paginas.dhtml?pagina=3

http://www.colombiaaprende.edu.co/html/familia/1597/article-73583.html

http://redesysegu.blogspot.com/2010/04/vulnerabilidades-y-amenazas.html

http://es.wikihow.com/bloquear-una-p%C3%A1gina-web-en-todos-los-navegadores

http://es.ppgrefinish.com/media/869569/guia_bloqueo_navegacion_web.pdf

http://www.mediacommerce.net.co/seguridad-en-la-web

https://www.youtube.com/watch?v=Fp5TiacQHcg