ATAQUES INFORMÁTICOS, ETHICAL HACKING Y CONCIENCIA DE SEGURIDAD INFORMÁTICA EN NIÑOS.

Lady Johana Cañón Parada
joicelady8563@gmail.com
Universidad Piloto De Colombia

Resumen: *En los tiempos actuales la tecnología es la que mueve a toda la humanidad, no hay hogar donde no se cuente con un dispositivo tecnológico sea computador, tablet o teléfono celular entre otros, y es allí donde nos volvemos más propensos a que nuestra información y datos sean vulnerables a personas malintencionadas y aun peor es cuando vemos que día a día nuestras nuevas generaciones optan por permanecer en línea desde muy pequeños y para los adultos se convierte en algo normal, sin percibir todos aquellos peligros en la red y desinformación que ellos pueden obtener de está, es por esta problemática que se realiza un informe detallado de los ataques informáticos más usuales a los que no solo nuestros niños si no nosotros mismos estamos propensos a caer.*

Abstrac: At the present time the technology is moving to all mankind, no home where there is counted with a technological device is computer, tablet or mobile phone among others, and that is where we become more prone to our information and data they are vulnerable to malicious individuals and even worse is when we see that every day our new generations choose to stay online very young and for adults becomes normal, without perceive all those dangers on the net and misinformation that they can get of it is, it is for this issue to a detailed report of the most common computer attacks that not only our children if we ourselves are not likely to fall is done.

Palabras clave: Seguridad, Informática, Ataques, Malware, Phishing.

INTRODUCCIÓN

La seguridad informática es una necesidad que debemos poner en práctica en nuestra vida cotidiana, somos vulnerables ante cualquier tipo de ataque informático el cual pone en riesgo la confidencialidad , integridad y disponibilidad de la información, debemos ser conscientes que el avance del desarrollo tecnológico cada día es mejor donde la comodidad y el confort que nos brinda la tecnología es seductora, pero la pregunta es ¿hasta dónde podemos aceptar que nuestra información privada sea expuesta ante la sociedad o aún más la de algún ser querido?.

La respuesta es negativa, ya que es importante considerar que cada una de las personas tiene algo que proteger; sus bienes, su privacidad e información por tal razón el manejo de seguridad que le demos es responsabilidad de cada uno.

Hoy en día las empresas colombianas están invirtiendo en el campo de la seguridad informática, podemos observar el sector financiero como un ejemplo ya que ellos deben proveer a sus clientes seguridad en sus transacciones y en sus datos con el fin de dar una continuidad de negocio a su organización.

Del otro lado, la seguridad en el hogar es fundamental especialmente en los niños, ya que ellos están siendo cautivados por los dispositivos, aplicaciones y herramientas que la tecnología les ofrece día a día , con el uso de internet el cual está disponible las 24 horas los 7 días de la semana, por tal razón se encuentran vulnerables a métodos de ataque como la ingeniería social.

Por lo anterior es importante que se genere un ambiente de concientización sobre la seguridad de

la información, ¿será que sí estaremos tomando las medidas necesarias para no estar expuestos

ante ataques informáticos?, estos están siendo más comunes hoy en día, en este artículo conoceremos algunos de los ataques más usados, la importancia del ethical hacking en organizaciones y se dará a conocer unas recomendaciones de seguridad informática en niños.

1. Los ataques informáticos más comunes:

Ilustración 1. Tomado de: Terra Perú. (29 de 09 de 2010). Terra. Recuperado el 06 de 06 de 2015, de Terra: http://www.terra.com.pe/noticias/noticias/act2532901/piratas-peruanos-ataques-informaticos-mas-sonados.html[1]

1.1 Malware:

Se cataloga como un código malicioso compuesto por gusanos, worms, spyware, troyanos, virus o script malintencionados que tiene como propósito infiltrarse y dañar un computador o sistema de información sin el consentimiento de los propietarios.

1.2 Hacking Ethico Carlos Tori:

Generalmente los virus y gusanos son los tipos más conocidos de software maligno que existen, se distinguen por la manera en que se propagan ya que al ser ejecutados en un ordenador infecta otro software que este contenga, con el fin de realizar acciones maliciosas como borrado de archivos adicionalmente explotan vulnerabilidades su objetivo es infectar la mayor cantidad de usuarios que se encuentran en una red con el fin de ocasionar un impacto malicioso.

Como protegerse de este ataque:

- Tenga actualizado el sistema operativo y los navegadores web que utiliza.
- Instale el antivirus y active el firewall y configúrelos para que se actualicen automáticamente.
- Utilice contraseñas de alta seguridad.
- Instale un programa antimalware que le proporcione protección en tiempo real.

1.3 Troyanos:

Permite la administración remota de un ordenador de forma oculta sin la autorización del usuario, por lo general son enviados en mensajes llamativos que inducen al usuario a ver el mensaje y ejecutarlo sin que el usuario se dé cuenta, por lo general su objetivo es causar daño y borrado de archivos.

Como protegerse de este ataque:

- Evite conectarse a una red WIFI abierta.
- Active los controles de integridad de los archivos de sistemas.
- Separe las cuentas de usuario de las cuentas administrador.
- Use programas especializados para detectar posibles intrusiones.
- Utilice cifrado de disco.

1.4 Phishing

Su objetivo es intentar obtener datos como usuarios , contraseñas, información de cuentas bancarias , e identidad del usuario mediante correos electrónicos y llamadas telefónicas usando la técnica de suplantación de portales bancarios haciendo creer al usuario ,que se está conectando al sitio oficial del banco , sin saber que está siendo víctima de un portal falso donde luego utilizan la información con el fin de generar transacciones no autorizadas donde se genera hurto.

Como protegerse de este ataque:

- No responda ningún correo electrónico o llamadas donde le soliciten información personal.
- Teclee la dirección o URL para realizar visitas en sitios web y más si consulta entidades bancarias por la red.

Ataques informáticos a sitios web y servidores:

1.5 SQL Injection:

Es uno de los ataques más usados, actualmente con este ataque pueden tener acceso a las tablas de bases de datos, donde incluye información del usuario con su contraseña; este tipo de ataque es más común en organizaciones y negocios de comercio electrónico donde los crackers observan grandes bases de datos, con el fin de extraer información sensible, este ataque se caracteriza por ser fácil de ejecutar, ya que utiliza una técnica que modifica la cadena de consulta en base de datos donde se encuentra una inyección de código en la consulta.

Como protegerse:

- No utilice sentencias SQL construidas dinámicamente.
- No utilice cuentas con privilegios administrativos.
- No proporcione mayor información de la necesaria.
- Verifique el tamaño como el tipo de datos de las entradas del usuario.

1.6 DDOS:

Es un ataque muy común donde su objetivo principal es denegar el funcionamiento de sitios web, donde se vulnera la disponibilidad del servicio ya que cuando un usuario trata de ingresar al sitio este se encuentra fuera de servicio cumpliendo con el objetivo propuesto.

Hay variedades de ataques DDoS

- Ataques por volumen: donde se intentan desbordar el ancho de banda de un sitio web.
- Ataques de protocolo: donde los paquetes intentan consumir servicios de red.
- Ataques de aplicaciones: donde las peticiones se hacen con el fin de explotar un servidor web mediante la capa de aplicación.

Como protegerse del ataque DDoS:

- Restrinja el uso de ancho de banda a los hosts que cometan violaciones.
- Realice un monitoreo de las conexiones TCP/UDP que lleve a cabo el servidor.
- Limite el número de conexiones concurrentes en el servidor.

1.7 Fuerza bruta:

El principal objetivo de este ataque es intentar romper todas las combinaciones posibles de nombre usuario y contraseña, estos ataques buscan contraseñas débiles para ser descifradas y tener acceso de forma fácil.

Como protegerse del ataque:

- Bloquee el número de intentos fallidos al introducir el usuario y la contraseña.
- Utilice una contraseña segura de más de 8 caracteres realizando combinación de mayúsculas, minúsculas, letras y números.
- Evite un nombre de usuario como admin, administrador.

1.8 Cross site Scripting:

Los atacantes utilizan (XXS) con el fin de inyectar scripts maliciosos en sitios web inofensivos, es utilizado para obtener acceso a una cuenta de usuario.

Como protegerse del ataque:

- No confié en datos que vengan de usuarios externos.

1.9 Man in the middle:

Se utiliza para supervisar la comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellas , este ataque es realizado utilizando la técnica de rastreo de puertos.

Como protegerse del ataque:

- Utilice un sistema de cifrado fuerte entre cliente servidor mediante un certificado digital.
- Evite que los usuarios puedan conectarse a una red wifi abierta.

1.10 Ataque de día cero.

Este tipo de ataque afecta directamente al ordenador, donde tratan de explotar las vulnerabilidades que no han sido detectadas e informadas a la audiencia, por lo anterior son vulnerabilidades desconocidas y que se presentan si aún no se cuenta con una actualización o parche que lo proteja de la vulnerabilidad.

Como protegerse de este ataque:

- Elimine del sistema aplicaciones que no utilice.
- Mantenga actualizado los parches de los proveedores de los programas.
- Utilice un sistema de prevención contra intrusos HIPS con el fin de detener otra amenaza.

2. Ingeniería social:

Es el arte de engañar a las personas, las amenazas de la ingeniería social son más peligrosas, ya que es más difícil protegerse frente a ellas, debido a que el objetivo principal no solamente el sistema si no la víctima.

Es una técnica de hackeo utilizada para extraer información a otras personas, teniendo como base la interacción social, donde la persona que está siendo atacada no se da cuenta cuando suministra información personal que puede terminar en manos de un atacante.

En la ingeniería social se encuentra 4 formas de actuar:

- La primera consiste en una técnica pasiva que se basa en la observación y el análisis de donde se logra conseguir un perfil psicológico de la víctima.
- La segunda técnica utilizada es la no presencial donde se recurre a los medios de comunicación como el teléfono, los correos electrónicos con el fin de obtener información personal y útil para el atacante.
- La tercera técnica es la presencial no agresiva, se inicia con un procedimiento de investigador, donde incluye seguimiento de la víctima , vigilancia de su domicilio, hasta buscar información dentro de la basura con el fin de recolectar la mayor cantidad de información.

La combinación de las tres técnicas nombradas anteriormente resulta ser más común y a la vez la más efectiva, ya que se compromete una serie de actividades que generan un ambiente de confianza al atacante con el fin de tener un acercamiento más real con su víctima con el propósito de estafarlo mediante engaños.

Como protegerse de este ataque:

- No revele datos confidenciales por ningún medio (llamadas telefónicas, personal desconocido o correos electrónicos no confiables).
- Nunca ingrese a links de páginas web que lleguen por medio de email desconocidos donde le soliciten información confidencial y siempre digite la url de los sitios web al que desea ingresar.
- Clasifique su información confidencial y destruya información que usted no utilice.

- Sea reservado con su información , recuerde que es un activo propio que solo le pertenece al responsable.

3. Ethical Hacking

Ilustración 2. Tomado de: Aula Nueva. (2011). Aulanueva.org. Recuperado el 2015 de 06 de 01, de Aulanueva.org: cursosonline.aulanueva.org [2]

Es una metodología utilizada para simular un ataque malicioso sin causar daño con el fin de analizar las brechas de seguridad que contiene una red , esta práctica tiene como fin poder identificar los riesgos a los que se encuentran expuesta la red de una organización.

El ethical hacking se basa en procedimientos basados en una investigación preliminar de análisis de vulnerabilidades, donde la acción inicia en el momento de identificar vulnerabilidades criticas del sistema, después de realizar la identificación se realiza la explotación de vulnerabilidades, donde se evidencia los puntos sensibles que se encuentran expuestos, se procede a realizar un análisis con el fin de dar las respectivas recomendaciones de como mitigar las brechas de seguridad encontradas.

Esta práctica es recomendada en las organizaciones con una periocidad concurrente ,en las entidades financieras el ethical hacking es una práctica obligatoria debido a los controles de PCI que se deben implementar con el fin de proteger los datos personales y cuentas bancarias de sus usuarios.

Seguridad informática en los niños:

Ilustración 3. Tomado de: Seguridad al día. (03 de 03 de 2013). Ligasuper sec caricaturas de seguridad informatica para niños. Bogota, Bogota, Colombia. [3]

La comunicación abierta que se tenga con los niños es muy importante ya que cumple un rol en la seguridad de la información, se debe explicar a los niños que toda la información que proviene de la web no es cien por ciento confiable y que deben ser muy cuidadosos con las páginas que visitan, ya que se encuentran expuestos a muchas trampas contenidas en la red es importante que acompañemos a nuestros niños y se fomente el uso responsable de la mensajería instantánea , las redes sociales y las búsquedas ON-LINE.

Actualmente existen métodos como el control parental que permiten a los padres poder establecer límites en la navegación de internet como bloqueo de páginas web, restricciones por categoría de contenido, control de descargas y envío de datos personales.

Pero es importante que se contemplen las siguientes recomendaciones con el fin de brindar protección en ellos:

- Explique al niño(a) no abrir enlaces sospechosos que puedan ser enviados a los correos electrónicos de ellos.
- No permitan que hablen con personas desconocidas en la WEB, explíqueles los riesgos a los que se pueden encontrar expuestos.
- No permitan que descarguen archivos de procedencias desconocidas.
- Realice acompañamientos de navegación con ellos.
- No permita que permanezcan bastante tiempo en la red.

Si sigue estas recomendaciones muy seguramente protegerá a los niños del cyberbullying, pornografía infantil, robo de información y trata de personas, ya que al hacer uso de las redes sociales u otros medios de comunicación los niños se exponen a los peligros mencionados del hostigamiento y el acoso.

APÉNDICE

Comunicación Virtual: Abraca las comunicaciones en que los intervinientes prese4rvan su identidad de una relación física mediante una forma telemática que evita el compromiso expreso de la propia personalidad.[4]

Software: Programas, detalles del diseño escritos en un lenguaje de descripción de programas, diseño de la arquitectura, especificaciones escritas en lenguaje formal, requerimientos del sistema, etc.[5]

Redes Sociales: Las redes sociales son sitios de internet que permiten a las personas conectarse con sus amigos e incluso realizar nuevas amistades, de manera virtual, y compartir contenidos, interactuar, crear comunidades sobre intereses similares: trabajo, lecturas, juegos, amistad, relaciones amorosas, relaciones comerciales, etc.[6]

Acoso cibernético: consiste en utilizar la tecnología para amenazar, avergonzar, intimidar o criticar a otra persona.[7]

CONCLUSIONES

Es indispensable generar un ambiente de concientización sobre la seguridad de la información y así llegar a minimizar la exposición de ataques informáticos.

Es prioridad brindar conocimiento a los adultos en especial a los padres, de métodos como el control parental para establecer límites en la navegación de internet en sus hijos.

REFERENCIAS

[1] Terra Perú. (29 de 09 de 2010). *Terra*. Recuperado el 06 de 06 de 2015, de Terra: http://www.terra.com.pe/noticias/noticias/act2532901/piratas-peruanos-ataques-informaticos-mas-sonados.html

[2] Aula Nueva. (2011). *Aulanueva.org*. Recuperado el 2015 de 06 de 01, de Aulanueva.org: cursosonline.aulanueva.org

[3] Seguridad al día. (03 de 03 de 2013). Ligasuper sec caricaturas de seguridad informatica para niños. Bogota, Bogota, Colombia.

[4] Botella, J. (01 de 10 de 2012). Papeles para el progreso.

[5] Alegsa. (s.f.). *http://www.alegsa.com.ar/Dic/software.php*. Recuperado el 01 de 06 de 2015, de http://www.alegsa.com.ar/Dic/software.php

[6] Escritorios familias. (2008). Escritorios familias. Recuperado el 01 de 06 de 2015, de http://escritoriofamilias.educ.ar/datos/redes-sociales.htm

[7] Arbelaez, A. (2014). Ingenieria Social:El hackeo silencioso. Colombia.

[8] Asociación de Internautas. (28 de 05 de 2005). *Asociación de Internautas.* Recuperado el 01 de 06 de 2015, de Asociación de Internautas: http://seguridad.internautas.org/html/451.html

[9] Catoira, F. (28 de 03 de 2012). welivesecurity. Recuperado el 01 de 06 de 2015, de welivesecurity: http://www.welivesecurity.com/la-es/2012/03/28/consejos-ataque-denegacion-servicio/

[10] Colombia. (2008). Colombia Tecnologia. Recuperado el 01 de 06 de 2015, de Colombia Tecnologia:

http://www.colombia.com/tecnologia/informatica/sdi/57401/consejos-de-seguridad-informatica-para-ninos-y-jovenes

[11] El Hacker. (s.f.). Wiki. Recuperado el 01 de 06 de 2015, de Wiki: http://wiki.elhacker.net/bugs-y-exploits/nivel-web/inyeccion-sql/proteccion

[12] HostDime. (s.f.). Tipos De Ataques Más Comunes A Sitios Web Y Servidores. Recuperado el 01 de 06 de 2015, de Tipos De Ataques Más Comunes A Sitios Web Y Servidores: http://www.hostdime.com.co/web-hosting/compartido/linux/

[13] Julian, G. (05 de 06 de 2013). ¿Qué es un troyano, cómo funciona y cómo podemos protegernos? Bogota, Colombia.

[14] Kidshealth. (2006). Kidshealth. Recuperado el 01 de 06 de 2015, de http://kidshealth.org/teen/en_espanol/seguridad/cyberbullying_esp.html

[15] Laguna, A. (15 de 10 de 2012). Entiende los ataques XSS y aprende a prevenirlos en PHP. Sevilla, España.

[16] Malenkovich, S. (10 de 04 de 2013). Que es un ataque man-in-tehe-middle?

[17] Minimalware. (01 de 11 de 2011). blogspot Como protegernos del malware. España.

[18] Rl, D. (09 de 01 de 2015). Guía para Prevenir Ataques por Fuerza Bruta en WordPress.

[19] Sophos. (s.f.). Amenazas de día cero. Recuperado el 01 de 06 de 2015, de Amenazas de día cero: https://www.sophos.com/es-es/security-news-trends/security-trends/zeroday-threats.asp