SEGURIDAD INFORMATICA Y LA PREVENCION DE AMENAZAS INFORMATICAS DEL FUTURO.

En la actualidad los ataques cibernéticos, son un problema que amenaza a la mayoría de las personas en todo el mundo, ahora vemos como países espían o otros países, organizaciones o instituciones privadas hackean cuentas de altos funcionarios de gobiernos extranjeros, ajenos a su país.

Los fraudes por internet cada vez son más frecuentes y más fáciles de realizar, todo esto, catalogado como amenazas informáticas o ataques cibernéticos. Ya sean los llamados “piratas cibernéticos o hackers” o por medio de virus troyanos o espías o por cualquier medio estas amenazas encontraran la forma de penetrar en el sistema e invadir, robar, o cambiar la información. Lo cual acarrea problemas muy grandes.

Es por esto que creemos que las medidas que toma la S.I. no son suficientes o mejor dicho no son 100% efectivas contra los problemas o los ataques cibernéticos que se presentan.

ANTIVIRUS

Las amenazas informáticas cada vez van tomando mayor importancia en el desarrollo de la sociedad y en la vida personal de cada individuo, ya que estas pueden ir desde el simple hackeo de una cuenta de correo red social. Hasta el fraude en cuentas de banco o problemas mayores como ataques informáticos terroristas a gobiernos o ejércitos.

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas, es decir a base de troyanos o malware infectar un ordenador, eliminar información y propagarse rápidamente por la web, después esto evoluciono con los llamados crimeware, programas que se presentaban como virus y reunían información para poder obtener dinero, siempre utilizando troyanos u otro tipo de virus. Ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los certificados que contienen la información digital. Se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

En un inicio se creía que con el lanzamiento de los antivirus estos problemas de troyanos y demás virus quedarían en el olvido pero con el transcurso del tiempo y la vida diaria, las experiencias nos hemos dado cuenta de que estos softwares o programas no solucionan el problema por completo.

Los programas para la protección de ordenadores en mi opinión son insuficientes para combatir los ataques virtuales a los que se enfrentan las organizaciones, ordenadores personales, sistemas organizacionales, etc.

Las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

Hablando en términos sencillos y de bajo riesgo, si no tenemos amplios conocimientos en este tema entonces creemos que si contamos con un antivirus nuestro ordenador, o nuestra computadora estará protegida de amenazas, virus, ataques, etc. Porque sabemos que los antivirus están diseñados precisamente para eliminar los virus, es decir, estos softwares están diseñados para proteger nuestra información personal y nuestro ordenador en general.

Pero no es hasta que tenemos una relación con estos softwares y ponemos a prueba ante diversas circunstancias su funcionabilidad y nos damos cuenta, es decir, es hasta ese momento cuando conocemos los alcances de de ese programa, conocemos cual es el mejor antivirus, o ante que ataques nos protege cada uno, etc.

Aunque no podemos dejar de mencionar que esto está sujeto a las experiencias de cada quien ya que no todos nos enfrentamos a las mismas amenazas.

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

La Seguridad de la Información (S-I) es algo más que un antivirus, cortafuego o cifrado de datos, la S-I es el resultado de operaciones realizadas por personas y que son soportadas por la tecnología[1]

Como podemos ver si la seguridad informática no se limita únicamente a antivirus, cortafuegos, etc. Entonces las amenazas no se limitan solo a virus, malware, crimeware, etc. Existen amenazas físicas como hackers los cuales son aun mas peligrosos porque pueden llegar a lograr evadir cualquier filtro que exista en un determinado sistema.

Ahora sabemos que los antivirus no eliminan el problema de los virus por completo, sería exagerado decir que con la llegada de los antivirus se eliminarían por completo todos los virus que existen y que las computadoras se encontrarían libres de amenazas pero no es asi. Haciendo una comparación seria como decir que con la llegada de las vacunas y los antibióticos las enfermedades se acabarían.

Cabe destacar que la mayor concentración de virus son programados para el sistema operativo Windows, debido a su amplia libertad para que los usuarios puedan crear aplicaciones propias de manera muy fácil, a diferencia de IOS de MAC y Ubuntu, GNU Linux y UNIX en general además que Windows tiene un alto nivel de comercialización, es decir, es uno de los sistemas operativos mas utilizados tanto en hogares como en organizaciones.

FIREWALL

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

Los Firewalls están diseñados para proteger una red interna contra los accesos no autorizados. En efecto, un firewall es un Gateway con un bloqueo, estos aparatos solo lo utilizan las grandes corporaciones.[2]

---

[1] Baldeón Garzón, Mauricio Javier Coronel Guerrero, Christian Alfredo; en el articulo “Plan maestro de Seguridad Informática para la UTIC de la ESPE con lineamientos de la Norma ISO/IEC 27002” en la dirección electrónica **http://repositorio.espe.edu.ec/handle/21000/6026**

Los firewalls pueden ser lógicos, es decir, un programa que protege tu ordenador y que no necesariamente es un antivirus, es un protector de red. Y físicos los cuales tienen una eficacia sumamente mayor en comparación a los lógicos.

Esta tecnología en su forma física adquiere precios muy altos por lo cual son utilizados comúnmente en las organizaciones y representan una barrera de seguridad muy buena, pero al igual que los antivirus no son la solución a los problemas de seguridad informática.

Estos sistemas tienen como ventajas que permiten el monitoreo de dos la red, es una barrera entre una red segura, por ejemplo una red local o casera y una no segura como lo es internet. Su filtro puede ser de muchas maneras, por dirección IP, por paquetes de datos, etc. Pero siempre trabajan sobre parámetros establecidos por el programador o el administrador de red.

Como desventajas encontramos que al no ser un programa inteligente y manejarse por parámetros tiene inconsistencias que permite a los intrusos ingresar a la red por medio de los huecos que se encuentran en este. También algo importante es que el firewall no protege contra amenazas humanas, es decir, si un intruso logra entrar y extraer información de la red el firewall no se dará cuenta, así, como tampoco identificara aquellos paquetes de datos infectados que el usuario ingrese en su ordenador.

Una vez que un usuario instale algún programa en su computadora, este le esta otorgando una serie de permisos que el firewall detecta como buenos, es decir, que los tiene que dejar pasar. si en algún momento el programa instalado trae virus el firewall no lo detectara debido a que el usuario indico que el conocía la procedencia de todos esos datos, y por esta razón no impedirá su ejecución o las modificaciones que estos llegaran a hacer dentro del sistema operativo o la computadora en general.

Ahora sabemos que los firewalls son una herramienta protección muy potente, pero aun así no es impenetrable, hasta cierto punto llega a ser vulnerable ante

---

[2] Baldeón Garzón, Mauricio Javier Coronel Guerrero, Christian Alfredo; en el articulo "Plan maestro de Seguridad Informática para la UTIC de la ESPE con lineamientos de la Norma ISO/IEC 27002" en la dirección electrónica **http://repositorio.espe.edu.ec/handle/21000/6026**

amenazas mayores. Tiene enormes ventajas al proteger la red nos da una capa mas de protección ante las amenazas, pero sigue teniendo cierta vulnerabilidad ante amenazas de otro tipo como las humanas. No podríamos compararlo con un antivirus, porque tienen funciones muy distintas podemos decir que un antivirus protege una computadora y un firewall protege una red.

ENCRIPTACIÓN

Otro método o concepto de la seguridad informática es la encriptación o el cifrado de la información. La encriptación o cifrado es el método pór el cual un mensaje o una información es cambiada en su modo de escritura, para que solo la persona a la que está destinada pueda leerla.

La encriptación de la información puede ser utilizada para cifrar contraseñas, cuentas bancarias, información importante, etc.

existen muchas maneras de cifrar información, utilizando matemáticas, como puede ser el caso de coordenadas o de matrices, el simple intercambio de letras u otorgando valores a determinadas letras.

Podemos creer que al encriptar un mensaje este podrá ser únicamente entendido por el destinario, la persona a la que va dirigido, pero no podemos saber si el mensaje será interceptado por alguien y este individuo tendrá la capacidad o el conocimiento para poder descifrar este mensaje.

Podemos dar un ejemplo cuando un usuario crea un perfil en una computadora y introduce una contraseña, por defecto el sistema operativo cifra esa contraseña para que no pueda ser visible a simple vista.

Pero existen maneras muy sencillas de poder descifrar esa información. esta misma mecánica es utilizada en cuentas, tarjetas de debito o crédito, bancas móviles, etc. aunque con un grado de encriptación mayor, debido a que la información es mas importante.

Aunque la encriptación de información es un método muy útil para la protección de la información es este uno de los más vulnerables y atacados de todos, debido a que al descifrar la información correcta pueden realizarse fraudes, suplantar identidades, etc.

Para ejemplificar el contenido de todo este ensayo podemos tomar como referencia dos noticias del periódico en lineal "El Economista", ya que muestran claramente la vulnerabilidad de las medidas de seguridad o del provecho que se puede sacar por medio de la seguridad informatica.

Articulo 1.

La Comisión Nacional de Seguridad (CNS) alertó por la circulación un virus cibernético que atacan principalmente a pequeñas y medianas empresas que no cuentan con la seguridad suficiente para proteger sus archivos, y sus usuarios utilizan regularmente dispositivos remotos para ingresar a los servidores de las empresas con el propósito de extorsionar.

La CNS informó en un comunicado que mediante el patrullaje en redes de Internet, los policías cibernéticos confirmaron que esta amenaza autodenominada "Anti-child Porn Spam Protection 2.0", es un intruso operado a distancia por defraudadores, quienes ingresan a los equipos mediante la función Escritorio Remoto.

"Al conseguir el acceso, el intruso deshabilita los programas antivirus que se hayan instalado para infectar el equipo y encriptar la información colocando una leyenda en un correo electrónico, donde se exige a los usuarios una cantidad de dinero a cambio de una contraseña para recuperar sus archivos", precisó.[3]

Es un ejemplo claro de cómo los virus pueden introducirse fácilmente en una computadora, robar información y posteriormente ser víctima de una extorción.

Como anteriormente mencionado, creemos que con un buen antivirus podemos estar exentos de estas amenazas, tenemos razones suficientes y objetivas para saber que con un antivirus reducimos la vulnerabilidad de nuestra información. Sin embargo, no conocemos un ataque informático, es decir, sabemos que son y lo que hacen pero no lo conocemos.

A lo que buscamos llegar es demostrar como la seguridad informática aunque cada ves mas modernizada, actualizada y mejorada, siempre los virus, hacker, y demás amenazas encontraran la forma de burlar estos filtros de seguridad que se

[3] Monroy, Jorge "alerta a PyMES por ataques cibernéticos" *el economista en la dirección http://eleconomista.com.mx/tecnociencia/2013/10/21/alertan-pymes-ataques-ciberneticos*

colocan en las organizaciones, instituciones o simplemente en las computadoras de nuestros hogares.

Articulo 2.

El presidente estadounidense tiene la potestad de ordenar ciberataques preventivos si se descubre evidencia de la preparación de un gran ataque digital contra el país, según una investigación oficial divulgada este lunes por The New York Times.

Citando responsables de la investigación, el periódico afirma que la nueva decisión también describe cómo las agencias de inteligencia pueden buscar en redes informáticas internacionales potenciales ataques contra Estados Unidos y, si es aprobado por el presidente, atacar a los adversarios con un código destructivo aunque no haya una guerra declarada.

La iniciativa surge cuando el Departamento de Defensa estadounidense aprobó una expansión de su seguridad informática para los próximos años con la intención de defender redes fundamentales.

El diario The Washington Post informó que el departamento de cibercomando debe aumentar su personal de 900 a 4,900 efectivos.

La importancia de la amenaza se ha enfatizado con una serie de sabotajes, que incluye uno en el que un virus fue empleado para limpiar datos de más de 30,000 computadoras en una petrolera estatal saudita a mediados del año pasado.

Se sabe que el mandatario Barack Obama ha ordenado el uso de ciberarmas una sola vez, cuando autorizó una escalada de ataques contra instalaciones de enriquecimiento de uranio iraníes, señaló The Times.[4]

Como sabemos Estados Unidos es el país con mayor desarrollo en el ámbito de la informática, es decir que es el país que va a la cabeza en el desarrollo de las tecnologías de la información.

Este permiso que se le otorga a estados unidos para realizar ciber-ataques es un claro ejemplo del aprovechamiento de la seguridad informática para el aprovechamiento, espionaje o cualquier actividad que beneficie a un pais o una

[4] AFP "Estados Unidos con libertad para ciberataque" *El Economista* en la dirección http://eleconomista.com.mx/tecnociencia/2013/02/04/estados-unidos-libertad-ciberataques

organización, para obtener un provecho propio. Como hemos venido hablando sobre organizaciones o países que espían a otros países, pudiéndose justificar ahora con este permiso.

Queda claro que los ataques cibernéticos no están lejos de nosotros, en cualquier momento podemos ser víctimas de ellos, y sin duda podemos ver como dia a dia la seguridad informática amplia sus fronteras y por consiguiente las consecuencias de esto serán cada vez más graves.

La seguridad informática como cualquier disciplina tiene funciones principales y estas son:

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- *Integridad: garantizar que los datos sean los que se supone que son*
- *Confidencialidad: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian*
- *Disponibilidad: garantizar el correcto funcionamiento de los sistemas de información*
- *Evitar el rechazo: garantizar de que no pueda negar una operación realizada.*
- *Autenticación: asegurar que sólo los individuos autorizados tengan acceso a los recursos*[5]

La seguridad informática realizas esfuerzos desmedidos para controlar, solucionar y proteger cada uno de estos aspectos aunque en materia de seguridad informática sea mas fácil atacar que defender, o simplemente porque a pesar que estos procesos se revisan minuciosamente siempre que un bucle por donde los intrusos pueden entrar al sistema.

Después de analizar los aspectos de la seguridad informática sabemos que efectivamente las medidas de la seguridad informática aunque se van actualizando y mejorando día con día y van creciendo a la par con toda la tecnología. No son suficientes para evitar al 100% las amenazas informáticas.

[5] http://es.kioskea.net/contents/622-introduccion-a-la-seguridad-informatica#top

Sin lugar a dudas la seguridad informática crece al mismo tiempo en que crece la tecnología, debido a que los sistemas operativos y programas tienen ligeros huecos o grietas donde estos virus pueden introducirse muchas veces si ser detectados, como lo muestra la grafica anterior con datos que muestra la situación en 1995.

Haciendo referencia a que en ese entonces los antivirus o la llamada policía informática no tenía la solides que tiene en nuestros días.

BIBLIOGRAFIA

http://www.dma.eui.upm.es/conferencias/contenido/seguridad_infor.pdf

http://www.kaspersky.es/threats

http://www.segu-info.com.ar/ataques/

http://es.kioskea.net/contents/622-introduccion-a-la-seguridad-informatica#top

http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml#contrasena

http://eleconomista.com.mx/tecnociencia/2013/02/04/estados-unidos-libertad-ciberataques

http://eleconomista.com.mx/tecnociencia/2013/10/21/alertan-pymes-ataques-ciberneticos

http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml#contrasena#ixzz2lBEQoYpb