Inicio y Evolución de la Seguridad Informática en el Mundo

Fernando Antonio Rentería Echeverry
Universidad Piloto de Colombia
Correo Electrónico:
Fernando190879@gmail.com

Abstract - For a long time he has been talking about computer security, but has certain where and in what year this word or phrase Computer Security is born and this whole concept, if we go a little to the origin of this story the year 1980 appeared the first manifestation of SI, James P Anderson writes the document Segurity Computer Threat Monitoring and Surveillance (Computer Security and Threat Monitoring and Surveillance).

In this paper the author expresses the main agents of the threats that will be some of the pillars for what today is known as information security, hence the different companies in the world began to implement software to detect computer crime and these different types infectious files and start protecting systems in their companies.

Index Terms - SI, hacker, Flaws, Breaches.

Resumen - Desde hace mucho tiempo se ha venido hablando de seguridad informática, pero que tiene de cierto donde y en qué año nace esta palabra o frase de Seguridad Informática y sobre todo este concepto, si nos vamos un poco a el origen de esta historia en el año de 1980 apareció la primera manifestación sobre **SI, James P Anderson** escribe el documento **Computer Segurity Threat Monitoring and Surveillance** (Seguridad en Computadores y Monitoreo de Amenazas y Vigilancia)[1].

En este documento el autor expresa los principales agentes de las amenazas informáticas que serán algunos de los pilares para lo que hoy se conoce como seguridad informática, de ahí que las diferentes empresas del mundo comenzaron a implementar software para detectar los delitos informáticos y estos diferentes tipos de archivos infecciosos y empezar a proteger sus sistemas en sus empresas.

Palabras Clave: SI, hacker, Flaws, Breaches.

I. INTRODUCCIÓN

Hablar de seguridad informática, es un concepto básico que tiene importancia y es necesario para todos los que nos dedicamos a el área de la informática o área de las Tic´s, dando inicio a toda duda y riesgo que presenta cualquier persona o entidad que maneje los sistemas informáticos; el concepto de ¨seguridad¨ es la calidad de seguro, y seguro es algo libre y exentó de todo peligro o riesgo. De ahí la pregunta la seguridad informática es un sistema exentó de peligro?, la seguridad informática en su concepto es un conjunto de métodos y herramientas destinados a garantizar la confidencialidad, integridad y disponibilidad de la información, y por ende proteger los sistemas informáticos ante cualquier amenaza, y además en este proceso tenemos mucha participación los seres humano. Los riesgos en términos de seguridad, se caracterizan mediante la siguiente ecuación:

$$RISQUE = \frac{MENACE \times VULNERABILITE}{CONTRE\text{-}MESURE}$$

Fig. 1 Introducción a la seguridad informática. Tomado de es.kioskea.net

La amenaza es el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad, conocida como falencias (flaws) o brechas (breaches) es el grado de exposición a las amenazas y por último la contramedida representa, las acciones que se está implementando en cuanto al riesgo de prevenir las amenazas[2].

[1] http://csrc.nist.gov/publications/history/ande80.pdf
[2] http://willy-houze.infographie-heaj.eu/Syllabus/securite/

II. LA SEGURIDAD INFORMÁTICA EN EL MUNDO

La seguridad informática es la disciplina que se encarga de proteger la integridad y la privacidad de la información, esta disciplina se ocupa de diseñar las normas, procedimientos métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Cuando hablamos de seguridad, este concepto se asocia a la certeza, falta de riesgo o contingencia. No es posible la certeza absoluta, si el elemento de riesgo siempre está presente, independientemente de las medidas que se tomen, significa tenerlo presente para seguimiento y evaluación de niveles de seguridad. También se entiende la seguridad informática como un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos, lo que se requiere también un nivel organizativo.

En la seguridad informática otro aspecto importante corresponde con los servicios de seguridad, ya que mejoran en un buen porcentaje la seguridad de un sistema y el flujo de información de una organización, estos servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio.

Fig. 2 Que es la seguridad informática. Tomado de g3ekarmy.

Cuáles servicios?
disponibilidad, autenticación, integridad, no repudio, control de acceso y disponibilidad.

a) Disponibilidad

Es la capacidad de asegurar el acceso de algún tipo de información a las personas autorizadas para mantenerla secreta y proteger los recursos de una información contra el descubrimiento internacional o accidental por personas no autorizadas a el sistema de información, es decir, protección de datos transmitidos de ataques pasivos por cualquier medio de fusión.

La disponibilidad se encarga de asegurar que nadie pueda Leer, Copiar, Descubrir o Modificar la información sin autorización y por consiguiente que ninguna persona pueda interceptar las comunicaciones o los mensajes entre entidades de diferentes organizaciones mundiales.

b) Autenticación

Estos servicios son más fáciles de comprender, este sistema de autentificación se encarga de verificar la identidad de algo o alguien, como puede ser la autentificación individual como la firma o si lo preferimos la contraseña.

La autenticación es utilizada para proporcionar la prueba a un sistema en realidad es la identidad de quien se pretende ser, y así mismo verificar la autenticación de la misma y acceder a dicha información, como medida principal a través de **algo que se sabe** (una contraseña o un numero personal de identificación, algo que se sabe, verifica la copia que está en el sistema de almacenamiento y determina si la autentificación es exitosa o no). **algo que se tiene (**una tarjeta o un pasaporte, es algo que se tiene y también el sistema verifica su autentificación); y a**lgo que se es** (la voz, la retina, la huella digital o la imagen del rostro, que pueden identificar de quien se trata y la veracidad de la información en cuanto a lo que se trata de autentificación.

c) Integridad

Este servicio verifica y garantiza, que la información trasmitida por cualquier medio no sufra cambios o modificaciones de forma no autorizada.

d) No repudio

Previene tanto al emisor como al receptor de negar un mensaje transmitido, el receptor del mensaje prueba la veracidad del mensaje que fue enviado por el presunto emisor y viceversa y confirma el recibido del receptor, el no repudio ofrece protección a un usuario frente a otro que niegue el mensaje y posteriormente la comunicación o

recepción del mensaje enviado, por ejemplo la firma digital.

e) Control de acceso

Controla el acceso de los sistemas y aplicaciones mediantes los medios de comunicación, el cual al tratar de ganar acceso, debe identificarse primero o autenticarse, con el fin que un usuario sea identificado y autenticado de manera exitosa y permitir el acceso a la información relacionada. La lista de control de acceso LCA permite los permisos que determina quién puede tener acceso a los recursos de la red, esta lista le permite al propietario que dé acceso o deniegue el ingreso a los recursos a una entidad o un grupo de entidades.

f) Disponibilidad

Este último servicio verifica que las personas autorizadas accedan a la información deseada cuando lo requieran y tantas veces como sea necesario, esto no significa que siempre se va tener este acceso, sino cuando sea requerido o necesario[3].

III. AHORA LA PREGUNTA POR QUÉ LA SEGURIDAD INFORMÁTICA

Cuando hablamos de seguridad informática, también nos tenemos que preguntar sobre el robo de datos a entidades nacionales e internacionales y personas del común en ser víctimas de robo, virus informáticos, gusanos maliciosos, los ciberataques como pueden ser en línea, y muchas de las infiltraciones de los teléfonos inteligentes, estas serían algunas de las amenazas más grandes y consideradas las más peligrosas. De ahí la inquietud sobre como la seguridad informática se ha convertido en una preocupación constante ante el creciente uso de la tecnología.

Y como podría la humanidad lidiar con estos problemas de la era digital.

Y propongo la utilización del siguiente formulario a estas inquietudes, que relaciono a continuación:

Fig. 3 Todo lo que usted quería saber sobre seguridad informática. Tomado de noticias BBC mundo.

1) Que es un virus informático?

En términos informáticos un virus es un pequeño programa de computación que se reproduce así mismo e infecta una o más computadores estando en red o localmente ya que existen diferentes tipos de medios de comunicación para trasmitirlo y dado su capacidad de reproducción al infectar un archivo se ejecutan cada vez que se utiliza la maquina o se manipula cierta información por medios extraíbles creando una cadena de contagios infecciosos.

2) Que es un software malicioso o malware?

Este dispositivo se diseñó para acceder a cualquier tipo de usuario sin su consentimiento con el fin de robar información, para ingresar códigos maliciosos o dañar el sistema operativo, este software malicioso se reconoce son los mismos que se instalan en las barras de los navegadores, anuncios publicitarios, o en su defecto se descargan programas sin que el usuario se dé cuenta y son los más utilizados por las redes criminales en internet. Los países que poseen un alto grado de programas maliciosos están referenciados en China y Rumania.

3) Que es el phishing?

Brevemente la definición de esta pregunta es la suplantación de páginas que el usuario frecuenta diariamente, para adquirir las claves y contraseñas, este nombre Phishing es conocido

[3] http://www.g3ekarmy.com/%C2%BFque-es-la-seguridad-informatica/

como la mezcla de Password (contraseña en inglés) y Phishing (pescando en inglés), unidas estas palabras el significado es pescando contraseñas

4) *Como darnos cuenta si un vínculo es seguro?*

La conexión que utiliza para navegar es segura, como saber eso, por el prefijo de https en vez de http común, en donde la S significa seguro; una de las diferencias de las conexiones abiertas, es que el canal de las https establece una conexión segura de internet donde se comprueba la autenticidad de un sitio web, y el https es importante en sitios de comercio electrónico y bancos en línea.

5) *Son efectivos los antivirus?*

Los antivirus son la mejor herramienta para combatir este tipo de problemas expuestos, de ahí su eficacia para mitigar y controlar la seguridad en su organización y supervisar los archivos maliciosos con el fin de eliminarlos del sistema, existen versiones gratuitas como medio de pagos, igual las gratuitas tienen cierto grado de eficiencia, el virus no te puede indicar que no hagas clic sobre algún vínculo o que instales programas que contengan características maliciosas, muy importante es mantenerlos actualizados para estar atentos con las amenazas tecnológicas que día a día es el problema de los sistemas y la tecnología.

6) *Que es un troyano?*

Este tipo de daño informático aparenta tener un fin con algún propósito, pero en realidad oculta acciones maliciosas que se van ejecutando sin consentimiento que el usuario se dé cuenta, y su nombre de troyano es referido a Caballo de Troya. Un consejo para los usuarios es descargar programas en sitios confiables en ocasiones se dicen que son antivirus y en realidad son programas que propagan los virus.

7) *Existe una ciberguerra informática?*

Existe un debate sobre si el termino ciberguerra es preciso o no, debido a las cantidades de ataques informáticos que desestabilizan los sitios de internet y paginas gubernamentales como del estado por cuestiones ideológicas, ejemplo Anonymous o el caso Wikileaks, es de ahí que muchas asociaciones en el mundo sugirieron que se creen mecanismos como las propuestas en la convención de Ginebra para el Ciberespacio. Al final de cuenta la palabra guerra es (lucha o combate) aunque sea en un sentido moral.

Sería un buen complemento que los diferentes países subdesarrollados que poseen las más altas tecnologías para resolver casos delictivos, seguridad en las empresas y cada una de las personas, establecieran un solo vinculo para combatir esta plaga de ataques que cada vez avanza con más fuerza y vulnera las diferentes herramientas que día a día se implementan para estar al margen de la seguridad informática en el mundo.

IV. CUÁL ES EL ALCANCE Y HASTA DONDE LLEGARA LA SEGURIDAD INFORMÁTICA EN EL MUNDO

El alcance de la seguridad informática se centra en proteger las infraestructuras tecnológicas y de comunicación de una organización donde básicamente comprende el hardware y software que son las utilizadas en todas las organizaciones mundiales, su análisis de riesgo se centra en la vulnerabilidad de estos requerimientos y llevar el nivel de riesgo a niveles aceptables por la organización.

La seguridad informática, como todo deseo de una organización o persona natural se orienta a mitigar los ataques de los ciberdelincuentes o ciberdelitos, pero cuanto le cuesta esto al mundo, las cifras superan los USD$ 110.000 millones, una empresa reconocida por todos en la parte de seguridad informática es ¨NORTON¨ que cada año entrega un informe sobre las víctimas de los delitos informáticos y el año pasado en promedio tienen 18 víctimas por cada segundo, sumando más de un millón y medio de victimas al día y 556 millones de víctimas al año.

Es de considerar que la tecnología avanza a pasos agigantados, pero también los delitos informáticos, queda el dilema de cómo se podrá llegar al final de poder estar tranquilos en sus organizaciones y saber que pueden dormir tranquilos y no esperando que la información se va desaparecer o que pueden ser víctimas de un virus informático que les destruya todo el sistema operativo es

algo que tenemos que tener en cuenta y vivir con ello hasta no llegar al fondo de establecer una cura para este daño mundial.

V. EL DESAFÍO DE INVERTIR EN LA SEGURIDAD INFORMÁTICA Y AÑADIR UN VALOR A LA EMPRESA

También existen muchas formas y métodos de realizar ataques informáticos que dependen directamente del delincuente que va realizar tal acción para esto necesita reconocer qué sistema es el que en riesgo de ser vulnerado para establecer las acciones pertinente. Es así como la ingeniería social es el método de engañar a otros para conseguir algo, los ¨Hackers¨ son expertos en lo que se trata de ingeniería social y cualquier organización o persona que para ellos vean vulnerables van a realizar las acciones que sean para infiltrarse y obtener información o saqueo ya que somos el eslabón más débil de la seguridad informática.

Uno de los Hackers más famosos del mundo, el norteamericano **Kevin Mitnick,** ha escrito diversos libros sobre la materia. La ingeniería social está basada en 4 principios básicos de pura psicología: todos queremos ayudar, siempre tendemos a confiar de entrada en el otro, no nos gusta decir que no y si nos gusta que nos alaben. Y al tratar de engañar a una organización o persona es bueno documentarse a fondo sobre dicha persona, especialmente cuando la víctima es un experto, supuestamente inteligente, de una compañía de telecomunicaciones o un agente de seguridad[4].

Muchas de las empresas en el ámbito mundial aplican la seguridad informática solo cuando les pasa algo y cubrirse de un eventual riesgo, es donde les resulta más caro que manejar los intereses de su propia empresa; no pensaron desde el comienzo de la organización, cuando se asume la conveniencia de estar más protegido y convencer a la organización o empresario;, antes de informarle el costo, es conveniente y sobre todo convencerlo del beneficio que el producto que se le oferta va mejorar toda su productividad organizacional.

VI. CONCLUSIÓN

El desafío de invertir en la seguridad informática en las organizaciones, significa pensar en el problema que tienen latente y a corto plazo; muchos dicen ¨a mí no me va a pasar¨ y así asumen el riesgo. La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional de la organización, incluyendo la información contenida, a medida de esto existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes para minimizar los posibles ataques o riesgos de la información estructural de la organización.

La seguridad informática también comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore como un activo y que de manera simultánea significa un riesgo; la información como privilegiada o confidencial de la organización, puede llegar a manos de personas mal intencionadas.

Para nadie es un secreto que los ataques a las grandes organizaciones y personas que poseen alguna forma de ataque cibernético o que poseen alguna información importante, siempre van a ser vulnerables para los Ciberdelincuentes o Hackers, ahora bien, en el mundo estamos totalmente preparados para luchar contra este fenómeno de la SEGURIDAD INFORMÁTICA.

REFERENCIAS BIBLIOGRAFICAS

[1] Fraude Online, “El mundo del e-crimen en Internet convertido en disciplina,” Informatica64 Mikel Gastesi, Daniel Creus

[2] Hacking y Seguridad en Internet Rústica, 2nd ed. Año 2011, García-Moran, J Paul, Fernández Hansen Yago, Martínez Sánchez Rubén, Ochoa Martin Ángel. Ra-Ma Editorial. N Páginas 577.

[3] Formato IEEE para presentar artículos. ITSA, Marzo 2006. Disponible en internet: < http://www.itsa.edu.co/ciit2010/Formato_Articulos_IEEE.pdf >.

[4] http://www.bbc.co.uk/mundo/noticias/2011/03/110324_1458_guia_preguntas_seguridad_informatica_virus_tlquqssynsaap_dc.shtml

Autor

Fernando A. Rentería Echeverry. Nació en Quibdó – Chocó, el 19 de Agosto de 1979. Obtuvo el título de Ingeniero de Sistemas en la Universidad Manuela Beltrán en el año 2006. En la actualidad, termino la Especialización en Seguridad Informática y está cursando el Diplomado en Informática Forense en la Universidad Piloto de Colombia. Su experiencia laboral se ha desarrollado en entidades públicas como privadas en el área de sistemas.