“SEGURIDAD” UNA REALIDAD INMEDIATA

Mongui Baquero Wilmer Camilo
wilmercamilo@gmail.com
UNIVERSIDAD PILOTO DE COLOMBIA - DIRECCIÓN DE POSTGRADOS

Abstract **-** This article aims to show a link on safety in their various fields, taking an approach in the field of computer and use models applied to solve a design suitable for every situation present. Next to this the various ways to exploit a vulnerability on computer networks as in some way a need to invest in solutions that can ensure the information in each of the companies is generated is shown. Each of the situations and examples presented reflect the reality in which every day we are exposed to every new situation presented validates the need for continuous improvement and new methodologies in which we are being subjected to an end

Resumen **-** Este articulo tiene como fin mostrar un enlace sobre la seguridad en sus diversos campos, tomando un enfoque en la rama de la informatica y sus modelos aplicados para poder emplear un diseño adecuado para solventar cada situacion presente. Junto a esto se muestra las diversas maneras de aprovechar una vulnerabilidad sobre las redes informáticas y como de cierta manera se genera una necesidad de invertir en soluciones que puedan asegurar la información presente en cada una de las empresas.Cada uno de las situaciones y ejemplos presentados, reflejan la realidad en la cual día a día estamos expuestos, cada nueva situación presentada valida la necesidad del mejoramiento continuo y las nuevas metodologias en las cuales estamos siendo objeto para su fin.

Índice de Términos **-** Hacking, Vulnerabilidad, Exploits, Malware, Redes computacionales.

I. INTRODUCCIÓN

La seguridad como término global, cubre aspectos relevantes en los cuales brindan un mismo enfoque “Asegurar algo o alguien” teniendo un nivel de confianza óptimo que se pueda brindar. A lo largo del tiempo este enfoque ha tenido una tendencia o mayor precedencia sobre la evolución tecnológica la cual estamos viviendo. Así fue sobre los años ´80 con el documento nombrado “***Computer Security Threat Monitoring and Surveillance***” por su autor en inglés, **James P. Anderson,** publica lo que parece ser la primer indagación sobre el tema de la seguridad informática, en la cual podemos identificar términos y primero pilares que afectan nuestra seguridad a nivel de la informática.

El mundo va de la mano de las tendencias, y sin ser indiferente, la Tecnología no es la excepción. Cada auge presente y demanda que se va acogiendo sobre los productos de la innovación presente, permite tener un nuevo enfoque sobre los riesgos adherentes a la necesidad frente a su demanda. Si adquirimos un nuevo producto es importante tener un nivel de prudencia adecuado para evitar ser el objetivo de varios frentes.

La evolución que hemos presenciado tecnológicamente, ha contado con una visión en la cual podamos contar con un conjunto funcional a nivel lógico y físico que permitan tener una experiencia a nivel de usuario final ideal, que a su vez permita aumentar el uso y generar una dependencia para tener un nivel de demanda amplio. Junto a esto vemos su evolución a nivel de Malware[1], que busca tener un beneficio sobre las acciones ejecutadas en los equipos que presentan vulnerabilidades[2]

II. INFORMÁTICA E INFORMACIÓN

Dos conceptos por los cuales es necesario

1. Definición de Malware - http://seguridadinformati.ca/articulos/malware
2. Definición de Vulnerabilidad - http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#sthash.UGBX5WjB.dpbs

profundizar para validar su aplicabilidad en el término "seguridad", y su relación conjunta en dicho ámbito, permite al lector conocer el manejo sugerido y su diferencia.

Tomando referentes para dar una definición precisa, identificamos los siguientes conceptos dados:

- Informática:

"Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores"[1].

"El término informática proviene del francés informatique, implementado por el ingeniero Philippe Dreyfus a comienzos de la década del '60. La palabra es, a su vez, un acrónimo de information y automatique. De esta forma, la informática se refiere al procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales"[2].

- Información:

"Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada"[3].

"La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento"[4].

Estos dos términos influyen bastante en el método o la manera en la cual son aplicadas medidas de seguridad. En el primero de ellos "Informática" vemos una inclinación al manejo de "datos" a través de medios electrónicos y/o dispositivos que cumplan dicha función. Este enfoque tiene una connotación más técnica, permitiendo el manejo en la aplicación de soluciones para dicho fin. En el segundo de estos "Información" es un término que influye en el ámbito informático por el manejo dado de este tipo de datos que manejan un contenido lógico frente a su composición. Aunque va de la mano con la Informática, su manejo contiene parámetros adicionales que requiere contar para dar un correcto tratamiento frente a su aplicabilidad con la seguridad.

A. Ámbito Técnico

El manejo realizado de la seguridad en el ámbito técnico, teniendo en cuenta las definiciones anteriores, se identifica como "Seguridad Informática". Esta aplicabilidad va inclinada sobre la estructura lógica de la red corporativa, en la cual identificamos varios factores que influyen en un adecuado manejo de la información. Desde este punto comenzamos a identificar términos que derivan del enfoque realizado, Malware, Ataques de Denegación de Servicio, Suplantaciones, CriptoMalware, Hackers, entre otros, son algunos términos.

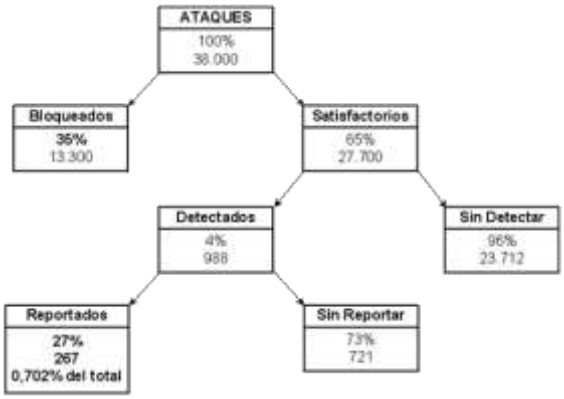

Gráfico 1. Ataques realizados de 1992 a 1995 fuente: www.disa.mil

1. RAE informática - http://lema.rae.es/drae/?val=informatica
2. Deficinión Informática - http://definicion.de/informatica/
3. RAE Información - http://lema.rae.es/drae/?val=informaci%C3%B3n
4. Definición Información - http://definicion.de/informacion/
5. Ataques reportados por DISA

En el Gráfico 1, se evidencia el resultado de 38 mil ataques realizados a entidades gubernamentales entre el periodo de 1992 a 1995. En dicha época no se tenía una tendencia tan fuerte como la que manejamos hoy en día, por ende vemos cifras más altas pero que reflejan el manejo dado. Se identifica que más del 50% de los ataques fueron satisfactorios, de los cuales únicamente fueron identificados el 4%, dichas cifras brindan un conocimiento en el cual permite identificar la falta de visibilidad y de protección aplicada en las redes corporativas. Cada uno de los ataques mencionados fue ejecutado y logrado sin que algunas entidades se enterarán de lo que estaban presentando.

Al 2013 estas cifras han aumentado de manera considerable, según **Kaspersky LAB**[1], "*En los dos últimos años la cantidad de ataques informáticos graves detectados ha crecido tanto, que cada nuevo ataque ya no suele causar sorpresa. Los informes de las compañías antivirus sobre el descubrimiento de una nueva botnet o un nuevo refinado ejemplar de malware que roba datos aparecen con regularidad.*"

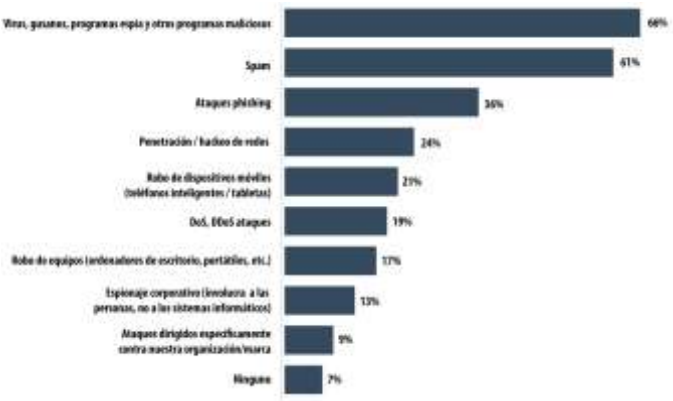

Gráfico 2. Ataques selectivos realizados a organizaciones empresariales Fuente: http://www.viruslist.com/sp/analysis?pubid=207271238

Cada cifra reflejada aumenta al transcurrir el tiempo, pero de la misma manera podemos encontrar un sinfín de soluciones de seguridad informática empleadas y diseñadas específicamente para garantizar un nivel de seguridad mayor y reducir cada brecha presente en organizaciones que son el blanco deseado.

A.1 Razones

La ejecución de ataques informáticos y amenazas presentes en la red, no siempre fueron con fines lucrativos, dicho pensamiento ha ido evolucionando de igual forma que todo converge. Las razones iniciales van ligadas a la reputación de los atacantes, el ego juega un rol importante en el cual, quien ejecutara de cierta manera el mejor ataque tenía una posición y reputación mayor. Hacer indisponer el usuario ante sus funciones en el ordenador, era un objetivo inicial para ellos. Hoy en día vemos un cambio total en su función.
Las razones asociadas a este tipo de ataques en la actualidad pueden clasificarse de cierta manera según su fin:

- Fines Lucrativos: es comúnmente mencionado el tipo de ataque en el cual el atacante, genera un código que permite obtener el control sobre cierto tipo de información de nivel crítica de los usuarios. Términos como el de CryptoMalware[2], se están popularizando debido a que se genera un cifrado de la información de los usuarios, que para permitirla usar requiere un pago para permitir el acceso. El uso de Botnet, el uso de backdoor, son algunos ejemplos presentes en este grupo.

- Robo de Información: Este grupo de ataques van enfocados a la exposición de información confidencial de las compañías. En ocasiones se refleja este tipo de ataques en las cuales en ambientes de competencia buscan conocer información sensible de sus competidores para poder tener una ventaja frente a estos.

1. En 1999, Kaspersky Lab fue la primera compañía en introducir software antivirus integrado para estaciones de trabajo, servidores de archivos y servidores de aplicaciones que se ejecutan en sistemas operativos Linux/FreeBSD. Fuente. http://latam.kaspersky.com/sobre-kaspersky/sobre-la-compania
2. Definicion de CrytoMalware - http://support.kaspersky.com/viruses/common/10646

- Falla en funcionamiento: Afectando la operación de la compañía, se busca eliminar los datos donde puedan alojarse el código malicioso, impidiendo la recuperación de estos. Lo anterior ocasiona que la compañía quede por fuera de su operación.

- Afectación de Servicio: Comúnmente conocidos como ataque de denegación de servicio (DoS, DDoS por sus siglas en inglés), generan accesos a los servicios públicos de las compañías, como páginas web, portales transaccionales, de manera errónea en las cuales por su número elevado de solicitudes genera carga excesiva en el servicio afectando su disponibilidad por un tiempo determinado.

Cada uno de los grupos mencionados anteriormente, buscan un fin en común, generar una marca, una huella en la cual afecte la reputación de las compañías y su credibilidad en el manejo adecuado y seguro en la información de sus clientes.

B. Ámbito Administrativo

El manejo aplicado sobre este ámbito, y según las definiciones identificadas anteriormente, se conoce como "Seguridad en la Información". Según ***ISO/IEC*** 27001 la Seguridad en la Información, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización

A este nivel podemos manejar un conjunto de reglas o mejores prácticas aplicables a la información y sus diversos medios de manejo y transmisión de esta. Hoy en día conocemos varios modelos aplicables al manejo adecuado de la información que permiten entre muchas otras tener el respaldo frente a entes que garantizar el manejo de la seguridad en la información ante sus clientes.
A diferencia de la Seguridad Informática en la cual se identificaba el tipo de Ataque normalmente manejado, en este punto podemos validar como es el manejo estructurado para generar le mitigación de dicho tipo de ataques. Generalmente este tipo de amenazas los empleados en dos grandes tipos: Intencionales y no Intencionales.

¿Es posible validar la importancia de la Seguridad en la Información frente al volumen de información manejada en cada una de las compañías?, es importante generar un nivel de conciencia amplio en el cual se logre identificar cada uno de los factores que puedan involucrar la seguridad de la información. Hemos identificado hasta el momento que la información es un activo valioso sobre las compañías, sobre muchas de ellas es el más importante. Partiendo de este punto, es necesario mostrar el daño frente a una posible amenaza, en el cual puede generar pérdidas numerosas a nivel económico e incluso llevar al cierre de compañías por el desprestigio que se pueda generar.

En este punto se tiene una posición en la cual se pueden generar pruebas controladas sobre la red, para poder evidenciar y generar un impacto que en ambientes reales podría significar pérdidas significativas.

III. CASOS DE ESTUDIO

Aunque se ha generado un nivel de maduración en el tratamiento y manejo de incidentes, se han presentado situaciones en las cuales han evidenciado un impacto en muchas organizaciones afectando su estado y funcionamiento. A continuación se mencionan algunos casos de estudio que reflejan el mejoramiento de la seguridad y en algunos no tan efectivos su realidad de cierre ante el mercado de sus clientes activos. Sobre estos es importante visualizar algunas estadísticas adicionales sobre este tipo de amenazas:

Gráfico 3. Reporte Cibercrimen Fuente: http://es.norton.com/cybercrimereport

Gráfico 5. DoS Apple **Fuente:** http://daily.bhaskar.com/

- Más de 9 mil ataques realizados por día a sitios Web

- Nuevas vulnerabilidades presentes en Sistemas que afectan la seguridad en la en la presencia de ataques en personas.

Junto a esto se suman algunas situaciones que reflejan a continuación:

- Blackberry sufre de perdida de servicio en Europa, oriente medio y África. Más de 70 millones de suscriptores con navegación, correo electrónico y el servicio de mensajes personales de Blackberry, fueron afectadas 50% de estas en Europa.

Gráfico 4. DoS Blackberry **Fuente**: http://www.zdnet.com/article/widespread-disruption-in-blackberry-crash-across-europe-middle-east-africa/

- El sistema de descarga de actualizaciones de Apple colapsa cuando sus usuarios intentan descargar la versión iOS5. Los usuarios presentaron caídas del servicio y lentitud.

- **Datos obtenidos de cada uno de lo portales mencionados en los graficos inlucidos**

- Hackers manipulan los sistemas de cómputo de los trenes. (El alcance de estos ataques no tiene límite, todos estamos en riesgo, incluso vidas humanas está en juego). Dicho sistema fue afectado sobre dos días en el mes de Diciembre, afectando los tiempos en llegada de trenes ocasionando un colapso en usuarios.

Gráfico 6. Cibercrimen **Fuente:** http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/

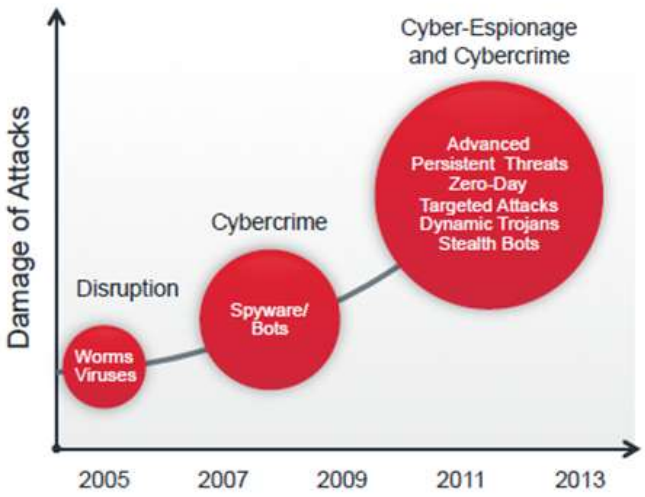

Gráfico 7. Evolución de amenazas **Fuente**: http://www.viruslist.com/

Algunos números reflejan las situaciones presentadas ante la falla de controles que permitan tener una efectividad en la prestación del servicio. Ante casos como BlackBerry, Apple, Sistemas públicos de Servicios, se generaron optimizaciones de controles, que permitieron reforzar índices de seguridad y de esta manera tener una disponibilidad del servicio continua para sus clientes y aumentar la calidad del servicio. Es importante identificar que aunque se tuvieron medidas tecnológicas que brindaban un nivel de seguridad, tal vez no fue la mejor aplicación en su ambiente corporativo, o faltaban algunos factores adicionales que pudieran reforzar aún más este nivel ofrecido.

IV. MODELOS A APLICAR

Existe diversidad de modelos aplicables sobre los cuales se pueden presentar en ambientes corporativos y de esta manera generar la reducción de este tipo de ataque efectivos. En un ambiente ideal de la red corporativa se pueden presentar ataques o comportamientos que son conocidos y de la misma manera se debe ser consciente de la presencia en la red, de esta manera podemos tener un control y respuesta rápida ante algún incidente.

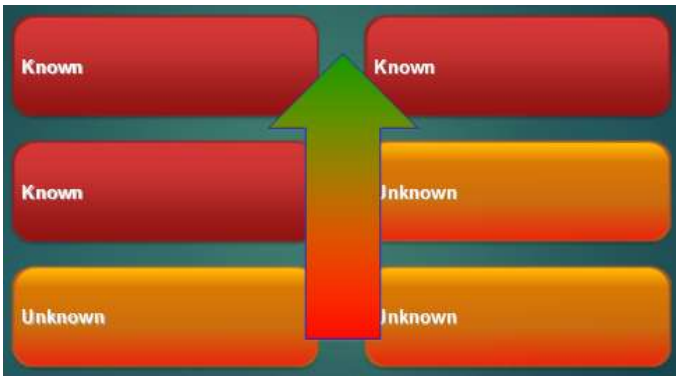

Gráfico 8. Modelo de Ataques frente a conocimiento de estos **Fuente:** Autoría Propia

Junto a esto es importante aplicar algunas metodologías que incluyan:

- Modelos de sensibilización de la seguridad en las entidades corporativas, para los funcionarios
- Protección con soluciones tecnológicas que permitan tener una visibilidad de las amenazas conocidas como las nuevas día tras día.
- Implementar Modelos de manejo de la seguridad de la información (ISO, etc)
- Generar pruebas de penetración controladas y enfocadas al descubrimiento de vulnerabilidades presentes en la red.

CONCLUSIONES

La realidad presente en la actualidad permite ampliar los conocimientos, la necesidad y conciencia en el avance que tenemos frente a las amenazas que fluyen sobre las redes a través del tiempo, cada una de estas frente su intensión brindaron la necesidad y la concientización que debe aplicarse para las personas, (Ambiente corporativo y Hogar), de la misma manera su aplicabilidad y seguimiento que debemos realizar sobre cada una de estas. Cada uno de los puntos analizados permite generar un punto clave de conocimiento explorando ítems claves como:

1. Reconocimiento en la necesidad de renovación de plataformas tecnológicas y de igual manera una revisión continua de nuestros modelos de seguridad implementados para contar con un nivel óptimo y de la misma manera reducir estos riesgos presentes.

2. El manejo de prudencia y conciencia es importante para poder tener un adecuado tratamiento ante situaciones que podemos prevenir para ataques como es el tipo Ingeniería Social.

3. El impacto de conocer la evolución de las amenazas, permite generar un nivel de protección mayor ante las nuevas amenazas que puedan presentarse, así mismo conocer la tendencia presente en la historia de cambio tecnológico y nuevas maneras de modo de operación y su protección a aplicar.

4. Finalmente se visualiza que día a día se presentan diversos casos en los cuales se reportan el robo de información, afectación en la reputación y demás puntos que afectan cada una de las compañías, en lo cual renace nuevas formas de protección ante cada reporte realizado. Generación de conciencias frente al impacto permite la inversión de soluciones que permitan aumentar la protección en las redes corporativas.

REFERENCIAS

[1] Wikipedia. [en línea]. Wikipedia, La enciclopedia libre, http://es.wikipedia.org.
[2] Diccionario de la Real Academia Española http://www.rae.es/
[3] James P Anderson, “Computer Security Threat Monitoring and Surveillance”
[4] Kaspersky LAB
[5] Virus TOTAL
[6] Portales de Diarios externos
http://www.nextgov.com/
http://daily.bhaskar.com/
http://www.zdnet.com/
[7] Norton Security
http://es.norton.com/cybercrimereport

AUTOR

Wilmer Camilo Mongui Baquero
Ingeniero de Sistemas
Universidad Piloto de Colombia
Especialización en Seguridad Informática