UNIVERSIDAD POLITÉCNICA DE VICTORIA

**TAREA. AMENAZAS INFORMÁTICAS**



ALUMNA: DANIELA LIZETH GUZMÁN VÁZQUEZ

MATRÍCULA: 1930007

FECHA DE ENTREGA: 29 DE SEPTIEMBRE DE 2019

*Ser capaz de superar la seguridad no te convierte en un hacker, de la misma forma que hacer un puente a un coche no te convierte en ingeniero mecánico.*

*(Raymond)*

Actualmente las grandes empresas informáticas, ya sean privadas o públicas, cuentan con casi el doble de la seguridad con la que contaban hace 20 años y, la razón de esto es que debido al mencionado avance tecnológico las personas que dominan demasiado las tecnologías han creado los llamados *virus*, una de las numerables formas de dañar la información que tiene resguardada la computadora, normal mente se debe a la vulnerabilidad que tienen.

En este documento te enseñaré un poco de lo que son las amenazas actuales y principales que la informática tiene, junto con algunos ejemplos.

Para comenzar, las amenazas, en general, se definen como “peligro o anuncio de un mal”, por lo que, en la informática se podría decir que es una amenaza que representa la acción que tiende a causar daño a los dispositivos o sistemas en donde se encuentra almacenada la información, invadiendo la integridad de las personas.

Como mencioné anteriormente lo virus son un ejemplo algo vago de lo que son las amenazas, pero, entre estas, podemos encontrar los virus creados específicamente para espiar a las personas, para divulgar su información, para alterar información específica, para suplantar a las personas, para robarle la identidad a una persona, etc.

Desde una vista más general, las amenazas las podemos encontrar clasificadas como: Factores Humanos (Humanas), Fallas del Sistema de Procesamiento de Información (Lógicas). Desastres Naturales (Físicos) y, por último los Actos malintencionados.

* FALLAS POR FACTORES HUMANOS:

Estos ataques vienen de las personas que ya sea que les paguen o lo hagan por ellas mismas causan enormes problemas a las empresas o a persona partiendo se l vulnerabilidad que tienen sus equipos.

A este tipo de personas se les conoce como:

* Hacker: estas personas no son para nada lo que imaginamos. Los hackers son las personas que

se encargan de crear programas, se dedican a estudiar y aprender lo más que se pueda ya que para ellos todo lo que tenga que ver con la informática es un reto.

* Cracker: Aquí si entraríamos con las personas que solo manejan las tecnologías con el fin de hacer malicia, la habilidad que tienen la emplean para perjudicar a cualquiera (por su cuenta por algún trabajo).
* Phreakers: Son las personas que su habilidad se concentra en las líneas telefónicas. Emplean dicho conocimiento para realizar llamadas sin costo.
* FALLAS DEL SISTEMA DE PROCESAMIENTO DE LA INFORMACIÓN:

En esta clasificación podemos encontrar los programas que dañan de manera intencionada (malware) o simplemente por errores lógicos, un sistema.

Algunas de las amenazas más comunes que podemos encontrar aquí son:

* Backdoor: Estos aparecen cuando los programadores están creando grandes sistemas operativos y quieren insertar atajos (puertas traseras) en los sistemas de autenticación. Aunque, con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.
* Bombas Lógicas: solo ciertos programas lo tienen, permanecen sin realizar ninguna función hasta que son activadas. Su función a realizar no son las mismas que las del programa original, sino que generalmente se tratan de una acción perjudicial.
* Caballos de Troya: programa que se hace pasar por uno válido cuando en realidad es uno malicioso. Es llamado así por la semejanza del Caballo de Troya que utilizaron los griegos.

Así los usuarios pueden descargar algo de un sitio web como música cuando en realidad es un troyano que instala en el quipo un Keylogger o programa que captura todo lo que el usuario escribe desde el teclado.

* Gusanos (Worms): programas que se propagan por si mismos a través de las redes, tomando ventaja de alguna falla de seguridad en los sistemas operativos con el propósito de realizar alguna malicia.
* Malware: proviene de la agrupación de las palabras “**Mal**icious Soft**ware**”. Está diseñado para insertar virus, gusanos, troyanos, spyware o bots (tipo de troyano que cumple con una función

específica), intentando conseguir información sobre el usuario o algún documento ubicado en la PC.

* Spyware: también conocido como programa espía. Este se refiere a las aplicaciones que recopilan información sobre una persona o empresa e instalan y se ejecutan sin el conocimiento del usuario. Su principal objetivo es recolectar información sobre el usuario y distribuirla empresas publicitarias o algunas otras empresas interesadas en la información.
* Virus: son los programas que tienen como objetivo alterar el funcionamiento de la computadora y en ciertos casos alterar la información, se propaga sin el computador y en ciertos casos altera la información del usuario en la PC
* DESASTRES NATURALES (FÍSICOS )

Estos ataques están enfocados a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en el cual se encentra ubicado los centros de cómputo de cada organización o individuo. Entre las principales amenazas que se pueden prevenir en la seguridad física encontramos:

* Incendios: generalmente son causados por el uso inadecuado de combustibles, fallas de instalación eléctricas defectuosas y el inadecuado almacenamiento y traslado se sustancias peligrosas. Es el enemigo número uno ya que puede destruir fácilmente los archivos de información y programas.
* Inundaciones: se le conoce como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, generalmente por falta de drenaje (natural o artificial).
* Señales de radar: estas señales pueden interferir en el procesamiento de la información; únicamente si la señal que alcanza el equipo es de 5 volts/Metro o mayor.
* Instalaciones eléctricas: cuando realizas instalaciones eléctricas debes de tener muy en cuenta los siguientes aspectos: picos y ruidos electromagnéticos, buen cableado, piso de placas extraíbles, un buen sistema de aire acondicionado y emisiones electromagnéticas.

Con anterioridad hablábamos de que las amenazas informáticas ocurren por la vulnerabilidad que llega a tener un equipo para ser utilizadas con el fin de dañar la información de un usuario y/o empresa que a su vez, está ligado a las personas, equipos y entorno ya que muchas de las veces son resultado de fallas o “bugs” en el diseño de un sistema.

Las vulnerabilidades también son clasificadas y, algunas de las principales a las que las organizaciones están expuestas son:

Para la realización de diagnosticar, los trabajadores tienen una buena variedad de herramientas. Estas herramientas tienen características de ser de software libre o comercial, y en la gran mayoría son las mismas que utilizan los atacantes para efectuar dicho ataque.

Algunas de las herramientas que ofrecen para el diagnóstico son las siguientes:

* BackTrack. Es una de las herramientas más populares. BackTrack es una distribución Linux en formato live-CD orientada a los profesionales de la seguridad informática, y en la cual se incluyen más de 300 herramientas para realizar diagnósticos de seguridad.
* Wireshark. Es un analizador de protocolos de red, que permite capturar cualquier paquete que circule por la red. Con este programa se puede verificar si por medio de la red se capturan datos sin cifrar, es decir, si existe la posibilidad de que determinada aplicación envíe información confidencial que puede ser fácil de interpretar por cualquier persona dentro de la red.
* Ettercap. Es una herramienta para realizar ataques sobre las redes LAN, en especial en las basadas en switches. Entre sus características se encuentra las de sniffer entre otras para el análisis de redes y equipos.
* NetStumbler. Es una herramienta en Windows que permite detectar redes inalámbricas usando 802.11a, 802.11b, 802.11g, y permite identificar la presencia de redes inalámbricas inseguras.
* Nessus. Herramienta que se utiliza para escanear uno o varios equipos de la red con el fin de encontrar sus vulnerabilidades. Con esta herramienta se puede identificar si el equipo tiene algún problema de seguridad que pueda ser aprovechado para alguien que quiera comprometer el equipo.
* Nmap. Herramienta de código abierto para la exploración de red y auditoría de la seguridad. Permite encontrar los equipos disponibles en la red, detectar que servicios ofrecen, conocer los sistemas operativos que ejecutan, y otras funciones más que ayudan a los administradores de red a encontrar fallas en la red y a los auditores a realizar las evaluaciones de seguridad.

Ya aclarado el significado de amenazas informáticas y las vulnerabilidades, así como el diagnóstico, pasaremos con el tema de los mecanismos preventivos en la informática. Estos mecanismos consisten en una serie de revisiones cada cierto tiempo algunas mejoras diferentes que pueden de hardware o software o en sí cualquier elemento en nuestra computadora.

Las revisiones dependen de los procesos de la empresa y cada una tiene diferentes procesos, lo mismo ocurre con los usuarios, cada uno cuenta con sus procedimientos y aplicaciones de prevención.

Unas de las herramientas de prevención que podemos utilizar para evitar todos los posibles ataques anteriormente mencionados, primera mente, sería actualizar en tiempo y forma el sistema operativo y todas las aplicaciones que el usuario tenga en la computadora.

La mayoría de los ataques informáticos se pueden evitar o por lo menos podemos disminuir el impacto que tendrían. En los elementos que se pueden aplicar en los mecanismos preventivos se pueden mencionar los siguientes:

1. Respaldo de información: es uno de los procesos más comunes que se pueden realizar en las compañías y que gozan de cierta aceptación general.
2. Horario de respaldo: puede llegar a ser un reto ya que es muy común que los usuarios pongan horarios “pico” o bien, de menor trafico provocando que no le prestemos mucha atención.
3. Control de los medios: el tener acceso a los respaldos es algo de alto riesgo, se puede robar la información, manipular, perder, así que, el respaldo es una solución, pero también es otro problema que se debe resolver.
4. La comprensión de la información: no toda la información se puede comprimir, pero existe alguna que, si lo necesita, así que se deben hacer las valoraciones respectivas.

Otros ejemplos de proceso que se tienen en el mecanismo preventivo son:

* Actualización de sistemas
* Antivirus
* Firewall
* Navegación por internet
* Contraseña
* Accesos remotos

Con lo detallado anteriormente, podemos decir que cada uno de los aparatos como las computadoras, laptops, tablets al comprarlos pueden tener fallos de hardware, software que pueden volverlo vulnerable ante cualquier ataque informático provocando así que personas violen nuestra seguridad con el fin de robar nuestra identidad o en algunas ocasiones simplemente para espiarnos con un fin específico, pero ejemplo, hay personas que aseguran que el que Donald Trump ganó las elecciones por la manipulación electrónica. Con este ejemplo podemos ver que los ataques informáticos pueden o no tener un fin específico.

Lo que nos deja como enseñanza que debemos de tener protegido nuestros equipos con aplicaciones oficiales y tener cuidado con las páginas web ya que últimamente es ahí donde publican los archivos “contaminados”.

FUENTES DE INFORMACIÓN:

* <https://pdfs.semanticscholar.org/60c7/dbe2abab31a25422c92ead74085fd7093715.pdf>
* <https://www.tecnoxxi.com/blog/seguridad-informatica/amenazas-informaticas/>
* <https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf>
* <https://www.regus.com.mx/work-mexico/cybersecurity-threats-where-do-they-come-from-and-whats-at-risk/>
* [file:///C:/Users/Daniela/Downloads/965-Texto%20del%20art%C3%ADculo-3375-2-10-20180126.pdf](file:///C:\Users\Daniela\Downloads\965-Texto%20del%20art%C3%ADculo-3375-2-10-20180126.pdf)
* <https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/>