UNIVERSIDAD DEL CENTRO DEL BAJIO.

LICENCIATURA EN SISTEMAS COMPUTACIONALES.

TÍTULO:

“AMENAZAS Y BULNERABILIDADES”.

MATERIA:

SEGURIDAD INFORMATICA.

DOCENTE:

FILIBERTO DURAN GARCIA.

PRESENTA

PABLO SÁNCHEZ UGALDE.

Celaya, Guanajuato , 16 de Febrero del año 2019.

Amenazas.

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información.

Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales.

Tipos de amenazas

Las amenazas pueden clasificarse en dos tipos:

Intencionales, en caso de que deliberadamente se intente producir un daño (por ejemplo el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).

No intencionales, en donde se producen acciones u omisiones de acciones que si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales).

Vulnerabilidad.

Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas. Podemos diferenciar tres tipos de vulnerabilidades según cómo afectan a nuestro sistema:

• Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados. Son vulnerabilidades de las que ya tienen conocimiento las empresas que desarrollan el programa al que afecta y para las cuales ya existe una solución, que se publica en forma de parche.

Existen listas de correo relacionadas con las noticias oficiales de seguridad que informan de la detección de esas vulnerabilidades y las publicaciones de los parches a las que podemos suscribirnos.

• Vulnerabilidades conocidas sobre aplicaciones no instaladas. Estas vulnerabilidades también son conocidas por las empresas desarrolladores de la aplicación, pero puesto que nosotros no tenemos dicha aplicación instalada no tendremos que actuar.

• Vulnerabilidades aún no conocidas. Estas vulnerabilidades aún no han sido detectadas por la empresa que desarrolla el programa, por lo que si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tienen instalado este programa.

Lograr que los sistemas y redes operen con seguridad resulta primordial para cualquier empresa y organismo. Para ello clasifica las vulnerabilidades en función de su gravedad, lo que nos da una idea de los efectos que pueden tener en los sistemas.

En la siguiente tabla puedes ver dicha clasificación de gravedad de vulnerabilidades:

Calificación	Definición
Crítica	Vulnerabilidad que puede permitir la propagación de un gusano de Internet sin la acción del usuario.
Importante	Vulnerabilidad que puede poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento.
Moderada	El impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacar partido a la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

Referencias.

VULNERABILIDADES | SEGURIDAD INFORMÁTICA

En el texto: ("Vulnerabilidades | Seguridad Informática", 2019)

Bibliografía: Vulnerabilidades | Seguridad Informática. (2019). Retrieved from https://infosegur.wordpress.com/tag/vulnerabilidades/