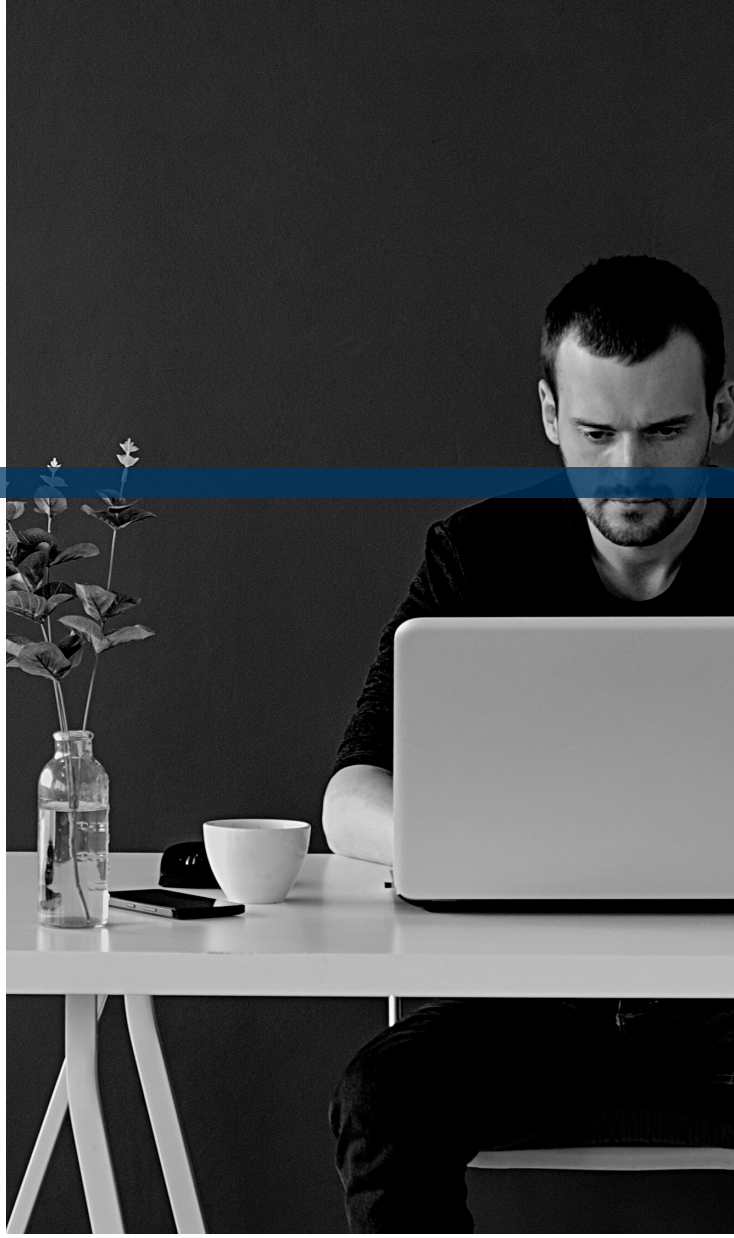
Fiscalía General de Justicia
Ciudad de México

ASPECTOS DE SEGURIDAD

POLÍTICAS DE USO DE INTERNET | MESA DE AYUDA

9911, 9912, 9977

ASPECTOS DE SEGURIDAD



En un entorno empresarial globalizado y competitivo como el existente en la actualidad, las empresas dependen cada vez más de sus sistemas de información y de la información que estos administran, pues se ha demostrado que tienen una enorme influencia en la toma de dediciones estratégicas para aumentar su nivel de competitividad.
El problema de la seguridad de la información se caracteriza por la complejidad y la interdependencia. La gestión de la seguridad contiene un número importante de factores y elementos que se interrelacionan entre sí. Las instituciones suelen tener una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridades olvidadas. De ahí la gran importancia de divulgar y conocer los siguientes conceptos como guía al interior de nuestras oficinas.

TÉRMINOS Y DEFINICIONES EN SEGURIDAD

Activo
En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Amenazas
Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo
Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría
Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Adware
Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Advertencia
Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la pérdida de datos del sistema del usuario.

Alarma
Sonido o señal visual que se activa cuando se produce una condición de error.

Alerta
Notificación automática de un suceso o un error.

Amenaza
Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Amenazas polimorfas
Las amenazas polimorfas son aquellas que tienen la capacidad de mutar y en las cuales cada instancia del malware es ligeramente diferente al anterior a este. Los cambios automatizados en el código realizados a cada instancia no alteran la funcionalidad del malware, sino que prácticamente inutilizan las tecnologías tradicionales de detección antivirus contra estos ataques.

Amenaza Externa
Amenaza que se origina fuera de una organización.

Amenaza Interna
Amenaza que se origina en una organización.

Analizador
Herramienta de configuración automatizada que analiza una red en busca de sistemas activos y actúa como guía durante el proceso de definición de los sistemas que desea supervisar y de las firmas de ataques que desea asociar con cada sistema.

Antispam
Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus
Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas
Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

Arquitectura de Seguridad
Conjunto de principios que describe los servicios de seguridad que debe proporcionar un sistema para ajustarse a las necesidades de sus usuarios, los elementos de sistema necesarios para implementar tales servicios y los niveles de rendimiento que se necesitan en los elementos para hacer frente a las posibles amenazas.

Ataques multi-etapas

Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware.

Ataques Web

Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Autenticación

Garantía de que una parte de una transacción informática no es falsa. La autenticación normalmente lleva consigo el uso de una contraseña, un certificado, un número de identificación personal u otra información que se pueda utilizar para validar la identidad en una red de equipos.

Blacklisting o Lista Negra

La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Bot

Un bot es una computadora individual infectada con malware, la cual forma parte de una red de bots (botnet).

Certificado

Los sistemas criptográficos utilizan este archivo como prueba de identidad. Contiene el nombre del usuario y la clave pública.

Botnet

Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.

Caballo de Troya

Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Crimeware
Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.

Ciberdelito
El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Contraseña
Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

Cuarentena
Aislar archivos sospechosos de contener algún virus, de modo que no se pueden abrir ni ejecutar. Encriptación La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

Exploits o Programas intrusos
Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Filtración de datos
Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados.

Firewall
Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Grooming
Es una nueva forma de acoso y abuso hacia niños y jóvenes que se ha venido popularizando con el auge de las TIC, principalmente los chats y redes sociales. Inicia con una simple conversación virtual, en la que el adulto se hace pasar por otra persona, normalmente, por una de la misma edad de víctima con el fin de Gusanos Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, a diferencia de un Virus.

Ingeniería Social

Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Keystroke Logger o Programa de captura de teclado (Keylogger)

Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Malware

El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas.

Mecanismo de propagación

Un mecanismo de propagación es el método que utiliza una amenaza para infectar un sistema.

Negación de servicio (DoS)

La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o red para los usuarios. Un ataque distribuido de negación de servicio (DoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.

Pharming

Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del re direccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento.

Phishing

Método más utilizado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta, puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Redes punto a punto (P2P)

Red virtual distribuida de participantes que hacen que una parte de sus recursos informáticos estén a disposición de otros participantes de la red, todo sin necesidad de servidores centralizados. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware. Riesgo El riesgo es el efecto de la incertidumbre sobre los objetivos.

Rootkits

Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final. Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso.

Sistema de detección de intrusos

Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Sistema de prevención de intrusos

Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Spam

También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing Spyware o Software Espía El software espía consta de un paquete de software que realiza un seguimiento y envía información confidencial o personal a terceros. La información personal es información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no desearía compartir con otras, como detalles bancarios, números de tarjetas de créditos y contraseñas. Terceros puede hacer referencia a sistemas remotos o partes con acceso local.

Virus

Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios: Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa. Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red. Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos.

Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

Vulnerabilidad

Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

- Permitir que un atacante ejecute comandos como otro usuario
- Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
- Permitir a un atacante hacerse pasar por otra entidad
- Permitir a un atacante realizar una negación de servicio