**SEGURIDAD**

Capacidad del sistema para proteger los datos y la información del acceso no autorizado, sin dejar de ofrecer acceso a personas y sistemas que si están autorizadas

Una acción contra un sistema informático con la intensión de hacer daño se llama un ataque, que puede tomar varias formas:

* Un intento no autorizado para acceder a los datos o servicios
* Modificar los datos
* Negar servicios a los usuarios legitimos

**CARACTERISTICAS**

Confidencialidad

Sub atributo que determina la capacidad de que los datos o servicios están protegidos contra el acceso no autorizado

Integridad

Sub atributo que determina que los datos o servicios no están sujetos a la manipulación no autorizada

Disponibilidad

Sub atributo que determina que el sistema estará disponible para su uso legitimo

Autenticidad

Verifica la identidad en una transacción y comprueba si son realmente quienes dicen ser

No repudio

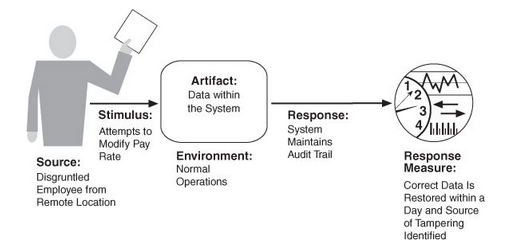
Garantiza que el remitente de un mensaje no puede negar haber enviado el mensaje y que el receptor no puede negar haberlo recibido

Autorización

Otorga al usuario los privilegios para realizar una tarea

ESCENARIO GENERAL

Un ataque es un intento de romper la CIA (Confidencialidad, integridad, disponibilidad), las hojas del árbol son el estímulo. La respuesta al ataque es preservar el CIA o disuadir a los atacantes a través del seguimiento de sus actividades



• Fuente de estímulo.

La fuente del ataque puede ser un ser humano u otro sistema . Puede que haya sido identificado previamente ( ya sea correcta o incorrectamente ) o puede ser actualmente desconocido . Un atacante humano puede ser de fuera de la organización o desde dentro de la organización.

• Estímulo .

El estímulo es un ataque. Caracterizamos esto como un intento no autorizado para mostrar, cambiar o eliminar datos, acceder a los servicios del sistema , cambie el comportamiento del sistema , o reducir la disponibilidad.

• Artefacto .

El objetivo del ataque puede ser cualquiera de los servicios del sistema, los datos dentro de la misma, o de los datos producidos o consumidos por el sistema. Algunos ataques se realizan en los componentes particulares del sistema conocido por ser vulnerables.

• Medio ambiente

El ataque puede venir cuando el sistema esté en línea o fuera de línea, ya sea conectado o desconectado de la red, ya sea detrás de un firewall o abierto a una red, en pleno funcionamiento, funciona parcialmente, o no operativa.

• Respuesta

El sistema debe asegurar que las operaciones se lleven a cabo de tal manera que los datos o servicios están protegidos contra accesos no autorizados, de datos o servicios que no están siendo manipulados sin autorización; dar garantía de las transacciones, las transacciones no pueden repudiar sus relaciones, y los datos, recursos y servicios del sistema estarán disponibles para su uso legítimo.

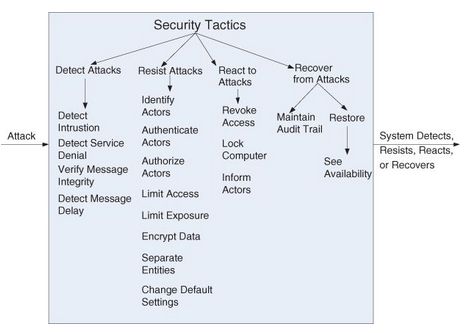
El sistema también debe seguir las actividades en su interior por el acceso de grabación o modificación; intenta acceder a datos, recursos y servicios , y notificar a las entidades correspondientes ( personas o sistemas ) cuando un aparente ataque está ocurriendo.

• Medida de respuesta

Las medidas de la respuesta de un sistema incluyen la porción del sistema que se ve comprometido cuando un valor de componente o de datos en particular se ve comprometida, cuánto tiempo pasó antes de que se detecta un ataque , el número de ataques que se han resistido , cuánto tiempo se tardó en recuperarse de un ataque con éxito , y la cantidad de datos que fueron vulnerables a un ataque en particular .

**TACTICAS DE SEGURIDAD**

Un método para pensar en cómo lograr la seguridad en un sistema es pensar en la seguridad física. Instalaciones seguras tienen un acceso limitado (por ejemplo, mediante el uso de los controles de seguridad), disponer de medios de detección de intrusos (por ejemplo, al exigir a los visitantes legítimos a llevar insignias), disponer de mecanismos de disuasión como guardias armados, tienen mecanismos de reacción, tales como el bloqueo automático de las puertas, y contar con mecanismos de recuperación tales como copia de seguridad fuera del sitio. Esto lleva a los cuatro tipos de tácticas: detectar, resistir, reaccionar y recuperarse.



**DETECTAR ATAQUES**

*DETECT INTRUSTION* – DETECCION DE INTRUSOS

Es la comparación de los patrones de tráfico de red o de solicitud de servicio dentro de un sistema a un conjunto de firmas o patrones conocidos de comportamiento malicioso, almacenados en una base de datos . Las firmas se pueden basar en el protocolo , indicadores TCP , tamaños de carga útil , aplicaciones, dirección de origen o de destino , o número de puerto .

*DETECT SERVICE DENIAL* – DETECTAR LA NEGACION DE SERVICIOS

Es la comparación del patrón o la firma de tráfico de red que entra en un sistema de perfiles históricos de ataques de negación de servicio conocidas

*VERIFY MESSAGE INTEGRATY* – VERIFICAR LA INTEGRIDAD DEL MENSAJE

Emplea técnicas como la comprobación o valores hash para comprobar la integridad de los mensajes, archivos de recursos , archivos de implementación, y archivos de configuración .

Una suma de control (checksum) es un mecanismo de validación en el que el sistema mantiene la información redundante para los archivos de configuración y mensajes , y utiliza esta información redundante para verificar el archivo de configuración o un mensaje cuando se utiliza . Un valor hash es una cadena única generada por una función hash cuya entrada podrían ser archivos de configuración o mensajes. Incluso un ligero cambio en los archivos originales o mensajes de resultados es un cambio significativo en el valor hash .

*DETECT MESSAGE DELAY* – DETECTAR RETRAZO DE MENSAJES

Está destinado a detectar posibles ataques man-in - the-middle , cuando una persona maliciosa está interceptando (y posiblemente modificando ) mensajes. Al marcar el tiempo que se tarda en entregar un mensaje, es posible detectar el comportamiento sospechoso de temporización, donde el tiempo que se tarda en entregar un mensaje es muy variable

**RESIST ATTACK** – RESISTIR ATAQUES

*IDENTITY ACTORS*– IDENTIFICAR ACTORES

Identificación de la fuente de cualquier entrada externa al sistema. Los usuarios se identifican típicamente a través de los ID de usuario. Otros sistemas pueden ser "identificados" a través de los códigos de acceso, direcciones IP, protocolos, puertos, etc.

AUTHENTICATE ACTORS

Autenticación significa asegurar que un actor (un usuario o un equipo remoto) es en realidad quién pretende ser. Contraseñas, contraseñas de un solo uso, certificados digitales y la identificación biométrica proporcionan un medio para la autenticación.

*AUTHORIZE* *ACTORS* - AUTORIZAR ACTORES

Autorización significa asegurar que un actor autenticado tiene los derechos para acceder y modificar los datos o servicios. Este mecanismo está habilitado normalmente proporcionando algunos mecanismos de control de acceso dentro de un sistema. El control de acceso puede ser por un actor o una clase de actor. Clases de actores pueden ser definidos por grupos de actores, por los roles de los actores, o por listas de personas.

*LIMIT ACCESS* – LIMITAR ACCESO

Limitar el acceso a los recursos de computación implica limitar el acceso a recursos como la memoria, las conexiones de red o puntos de acceso. Esto se puede lograr mediante el uso de protección de la memoria, el bloqueo de un anfitrión, el cierre de un puerto, o rechazo de un protocolo.

*LIMIT EXPOSURE –* LIMITAR EXPOSICION

Minimiza la superficie de ataque de un sistema. Esta táctica se centra en la reducción de la probabilidad Y de minimizar los efectos de los daños causados ​​por una acción hostil. Se trata de una defensa pasiva, ya que no previene de forma proactiva a los atacantes hacer daño. La limitación de la exposición se realiza normalmente por tener el menor número posible de puntos de acceso para los recursos, datos o servicios y al reducir el número de conectores que pueden proporcionar la exposición imprevista.

*ENCRYPT DATA* – ENCRIPTAR LOS DATOS

Los datos deben ser protegidos contra el acceso no autorizado. La confidencialidad se logra generalmente mediante la aplicación de algún tipo de cifrado de datos y la comunicación. La encriptación proporciona una protección adicional a los datos de forma persistente mantenidos más allá de que dispone de la autorización. Los enlaces de comunicación, por otra parte, no pueden tener controles de autorización. En tales casos, el cifrado es la única protección para el paso de datos a través de enlaces de comunicación de acceso público. El enlace se puede implementar mediante una red privada virtual (VPN) o por una capa de sockets seguros (SSL) para un vínculo basado en la web. El cifrado puede ser simétrico (ambas partes utilizan la misma clave) o asimétrico (claves públicas y privadas).

SEPARATE ENTITIES

La separación de entidades diferentes dentro del sistema se pueden realizar a través de la separación física en diferentes servidores que están conectados a diferentes redes, el uso de máquinas virtuales, o una "brecha de aire", es decir, no tener conexión entre diferentes partes de un sistema. Por último, los datos sensibles se separan con frecuencia a partir de datos no sensibles para reducir las posibilidades de ataque de aquellos que tienen acceso a los datos no sensibles.

CHANGE DEFAULT SETTINGS

Muchos sistemas tienen ajustes predeterminados asignados cuando se entrega el sistema. Forzar al usuario a cambiar estos ajustes evitará que los atacantes tengan acceso al sistema a través de los ajustes que son, por lo general, a disposición del público.

**REACT TO ATTACK** – REACCIONAR A ATAQUES

*REVOKE ACCESS –* REVOCAR ACCESOS

Si el sistema o el administrador del sistema cree que un ataque está en marcha, entonces el acceso puede ser muy limitado a los recursos sensibles, incluso para los usuarios y los usos legítimos normalmente.

*LOCK COMPUTER –* BLOQUEAR EQUIPO

Repetidos intentos de conexión fallidos pueden indicar un posible ataque. Muchos sistemas limitan el acceso a una computadora en particular si se repiten los intentos fallidos de acceder a una cuenta de ese equipo. Los usuarios legítimos pueden cometer errores al intentar entrar por lo tanto, el acceso limitado sólo puede ser por un período de tiempo determinado.

*INFORM ACTORS –* INFORMAR ACTORES

Los ataques en curso pueden requerir acción de los operadores, otro personal o sistemas de cooperación. Dicho personal o sistemas - el conjunto de los agentes pertinentes - deben ser notificados cuando el sistema ha detectado un ataque.

**RECOVER FROM ATTACKS** – RECUPERARSE DE LOS ATAQUES

*MAINTAIN AUDIT TRAIL* – MANTENER PISTA DE AUDITORIA

Mantener un registro de usuario, y las acciones en el sistemas, sus efectos, para ayudar a rastrear las acciones y para identificar al atacante, el análisis de las pistas de auditoria ayudan a mejorar al defensas.

*RESTORE* - DISPONIBILIDAD