Pag 168

Security

Es la medida de la habilidad del sistema para proteger datos e información de accesos no autorizados, mientras que mantiene el servicio a personas autorizadas.

La acción que se toma en contra de un sistema se le llama ataque.

El enfoque más general de seguridad tiene 3 características, se conoce como CIA:

Confidencialidad

Integridad

Disponibilidad

Confidencialidad: es la propiedad de datos o servicios que están protegidos contra accesos no autorizados. Ejemplo los hackers buscando cuentas bancarias

Integridad: es la propiedad de datos o servicios que no están sujetos a manipulación no autorizada. La asignación de permisos.

Disponibilidad: es la propiedad del sistema que esté disponible para uso legítimo.

Otras caracteristicas de CIA son

Autentificación: verifica las identidades de los protagonistas de una transacción, por ejemplo validar que la solicitud venga de un banco autorizado.

Nonrepudiation: garantía que el emisor de un mensaje no cambie su status de que mando ese mensaje.

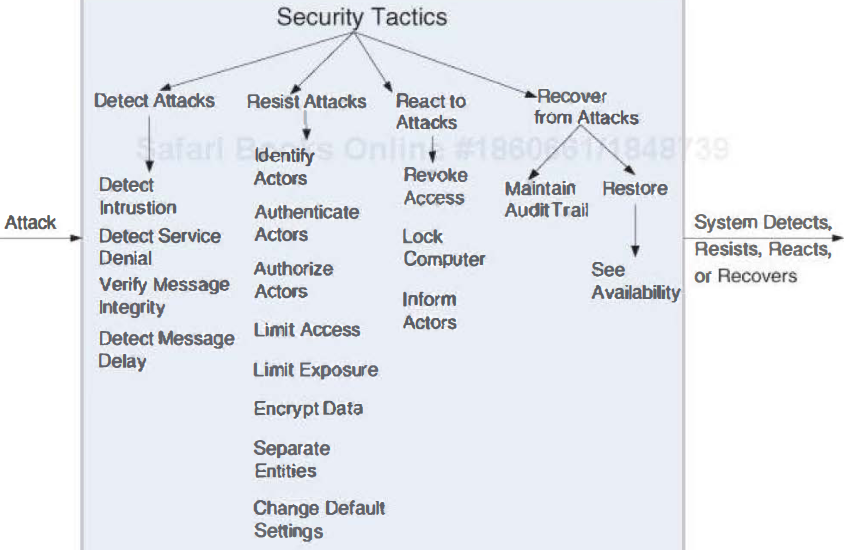
Auorizacion: asignación del permiso (privilegios) para ejecutar una tarea.

Todas las caracteristicas anteriores se usan en un escenario general de seguridad.

Escenario

|  |  |
| --- | --- |
| Fuente de estimulo | Humano o sistema que ha sido previamente identificada (correcta o incorrectamente) o desconocido. El ataque puede ser desde fuera de la organización o dentro. |
| Estimulo | Intentos no autorizados de leer, borrar o modificar información, acceder a servicios del sistema, cambiar la conducta del sistema o reducir su disponibilidad. |
| Artefacto | Servicios, datos producidos o consumidos por el sistema en modo en línea o fuera de línea. |
| Entorno | El sistema en línea, fuera de línea, conectado a red, en modo de operación total, parcial o no operacional. |
| Respuesta | Las transacciones se ejecutan en las siguientes modalidades:  -data o servicios protegidos de accesos no autorizados  -data o servicios con privilegios  -protagonistas de transacciones con autorización  -protagonistas que son nonrepudiaton  -datos, recursos y servicios que están disponibles para uso legitimo  El sistema lleva seguimiento del modo  -registrar los accesos o modificaciones  -registrar los intentos de accesar datos, recursos o servicios  -notificar a las entidades correspondientes (personas o sistemas) cuando aparentemente sucedió un ataque, |
| Medida de la respuesta | Una o varias de las siguientes  -en cuanto un sistema o componente o datos esta comprometido (en peligro)  -cuanto tiempo pasa desde el ataque  -cuantos ataques resistió el sistema  -cuanto tiempo lleva recuperarse de un ataque exitoso  -cuanto porcentaje de datos es vulnerable a un ataque en particular |

De este modo, se definen categorías de tácticas



1 detectar ataque

* 1. detect intrusión

es la comparación de trafico de la red, patrón de solicitudes u otra forma para detectar un ataque

* 1. detect service denial

la comparación de patrón o firma o historial en el trafico de la red para detectar ataques de la forma de negación de servicio.

* 1. verify message integration

técnica que usa checksums o hash values para verificar la integridad de mensajes, recursos, archivos, configuraciones.

Checksum verifica la información redundante que configura archivos y mensajes

Hash value es un string que define la identidad (key) de un archivo.

* 1. detect message delay

detecta ataques potenciales llamados man-in-the-middle donde una entidad maliciosa intercepta y posiblemente modifique mensajes, se detecta por el tiempo en que se lanza un mensaje.

1. Resist Attack
   1. Identify actors

Significa identificar la fuente de cualquier intento de ataque, en general se identifican con ID o con la combinación de datos como código de acceso, dirección IP, protocolo, puerto

* 1. Authenticate actors

Autentificar significa asegurar que un actor (usuario o acceso remoto) es quien dice ser, puede ser password, certificado digital, identificación biométrica.

* 1. authorize actors

significa que el actor autentificado tiene los derechos para acceder o modificar datos o servicios

* 1. limit Access

se limita el acceso a recursos computacionales como memoria, conexión a redes, puntos de acceso

* 1. limit exposure

minimiza el ataque a un sistema, es una defensa pasiva y se realiza limitando el numero de Access point, recursos, data o servicios

* 1. encrypt data

se aplica alguna forma de encripcion de datos o comunicación

* 1. separate entities

el uso de maquinas virtuales, diferentes servers y separar los datos con prioridad

* 1. change default settings

cambiar los defaults de acceso que muchas son públicos

1. react to attacks
   1. revoke Access

si cree que un ataque esta en proceso puede limitar los accesos

* 1. lock computer

algunos sistemas puede limitar el acceso a determinada computadora o usuario

* 1. Inform actors

Si el sistema detecta una intrusión puede informar a los actores afectados (operadores, sistemas cooperativos, etc.

1. recover from attacks
   1. Auditar

Mantener un registro de usuarios, sistemas y sus efectos que ayude a rastrear las acciones e identificar al atacante.

* 1. recuperacion de los servicios

es parte de la recuperación, reiniciar el sistema y los servicios

contrastar contra las decisiones arquitecturales

|  |  |
| --- | --- |
| Localización de responsabilidades | Determinar que responsabilidades del sistema deben asegurarse  -identificar al actor  -autentificar al actor  -autorizar al actor  -dar o negar privilegios  -registrar los accesos a los datos o servicios  -encriptar datos  -reconocer la reducción de disponibilidad para avisar a las entidades correspondientes  -recuperar del ataque  -verificar checksums y hash values |

|  |  |
| --- | --- |
| Modelo de coordinación | Determinar mecanismos para comunicar y coordinar con otros sistemas.  Asegurar los mecanismos de autentificación y autorización de actores o sistemas, encripcion de datos.  Asegurar mecanismos de monitorear y reconocimientos de cambios de demanda en el sistema para detectar ataques. |

|  |  |
| --- | --- |
| Modelo de datos | Determinar los datos sensibles y abstracciones de datos que requieran mayor protección.  -asegurar que los datos sensibles sean separados y tengan mayor protección  -asegurar que se guarden en bitácora todos los accesos a datos  -asegurar que los datos sean factibles de encriptar  -asegurar que los datos puedan ser restablecidos si son modificados por entidades no autorizadas |

|  |  |
| --- | --- |
| Mapeo entre elementos arquitecturales | Determinar los mapeos alternativos por posible caso de restablecimiento de datos  Probar los mapeos alternativos  Por cada posible mapeo alternativo probar:  -identificar al actor  -autentificar al actor  -autorizar al actor  -dar o negar privilegios  -registrar los accesos a los datos o servicios  -encriptar datos  -reconocer la reducción de disponibilidad para avisar a las entidades correspondientes  -recuperar del ataque  -verificar checksums y hash values |

|  |  |
| --- | --- |
| Administrar recursos | -Determinar los recursos requeridos para identificar y monitorear un sistema o individuo (interno o externo).  -determinar los recursos para identificar al actor, autentificar al actor, autorizar al actor, dar o negar privilegios, registrar los accesos a los datos o servicios, encriptar datos, reconocer la reducción de disponibilidad para avisar a las entidades correspondientes, recuperar del ataque, verificar checksums y hash values  -asegurar que no se extienda el daño una vez detectado  -asegurar que los recursos compartidos de actores no autorizados |

|  |  |
| --- | --- |
| Binding time | -determinar casos de unión tardia donde pueda haber intrusión  -asegurar y certificar todos los actores en el caso anterior |

|  |  |
| --- | --- |
| Selección de tecnologia | Determinar que tecnología esta disponible para que el sistema pueda  -autentificar  -asignar permisos  -proteccion de recursos  -encripcion de datos |