Fundamentos de ciberseguridad

La **seguridad de la información** (InfoSec) es la protección de la información importante contra el acceso, la divulgación, el uso, la alteración o la interrupción no autorizados.

La **seguridad informática** es la práctica de proteger el activo informático de una organización, ya sea: sistemas informáticos, redes, dispositivos digitales o datos de accesos no autorizados, filtración de datos, ciberataques y otras actividades maliciosas.

La **ciberseguridad** es la práctica de proteger los sistemas, las redes y los programas de ataques digitales. Son todos los procesos, tecnologías y medidas de seguridad aplicadas para proteger la información y los sistemas en entornos digitales o conectados, como redes e internet, frente a amenazas lógicas.

Vulnerabilidades y tipos

Una vulnerabilidad es un fallo, punto débil o defecto de seguridad en activos físicos, lógicos o humanos que pueden ser explotados para comprometer la confidencialidad, integridad o disponibilidad de los sistemas, datos o servicios. Algunos ejemplos de las vulnerabilidades más comunes son:

- **Naturales:** Son aquellas vulnerabilidades causadas por fenómenos naturales o condiciones ambientales, que pueden comprometer la infraestructura de la empresa.
- **Físicas:** Se refiere a debilidades en la protección de los espacios donde se almacenan o procesan datos, como falta de controles de acceso, equipos expuestos al público o instalaciones mal protegidas.
- **En Software:** Son errores de programación, configuraciones incorrectas o ausencia de actualizaciones en sistemas operativos, aplicaciones y servicios, que pueden ser explotadas para comprometer la seguridad.
- **En Hardware:** Son defectos en los componentes físicos de un sistema, como fallos de diseño, fabricación o mantenimiento.
- **En conexión:** Afectan la seguridad de los datos durante su transmisión a través de redes o medios de comunicación.
- **Humanas:** Son errores o comportamientos que los atacantes pueden explotar, como contraseñas débiles, falta de capacitación o susceptibilidad a técnicas de ingeniería social.

Malware y tipos

El malware es un conjunto de programas o códigos maliciosos diseñados para causar daño, obtener beneficios ilícitos para su creador o comprometer dispositivos, sistemas o redes. Puede manifestarse de diversas formas, dependiendo de su propósito y comportamiento, algunos ejemplos son:

- **Virus:** Todos los virus son un tipo de malware, pero no todos los malwares son un virus. Los virus son programas diseñados para infectar archivos legítimos, replicarse y propagarse a otros dispositivos.
- **Gusano:** Es un malware que puede replicarse y propagarse de manera autónoma, a menudo explotando vulnerabilidades en redes
- **Troyano:** Es un tipo de malware que se presenta como un programa legítimo o inofensivo para engañar al usuario y lograr su ejecución. Una vez activado, permite al atacante realizar acciones maliciosas.
- **Spyware:** Esta diseñado para recopilar información del usuario sin su consentimiento. Esta información puede incluir hábitos de navegación, credenciales o datos sensibles, en ocasiones es utilizada para espionaje o vendida a terceros.
- **Adware:** Genera y muestra anuncios no deseados en el dispositivos infectado, a menudo con el objetivo de generar ingresos para el atacante o redirigir al usuario a sitios peligrosos.
- **Ransomware:** Cifra los datos de los dispositivos infectado y exige un rescate, generalmente en criptomonedas, a cambio de la clave de descifrado.
- **Rogue:** Se presenta como un software legítimo de seguridad, engañando al usuario con alertas de infecciones inexistentes para que compre licencias falsas o descargue otros malwares.
  El malware tiene diferentes formas de funcionamiento, pero la mayoría consta de dos elementos esenciales para su ejecución:
- **Exploit**: Es un conjunto de instrucciones, código o herramientas diseñadas para aprovechar una vulnerabilidad específica y comprometer un sistema o activo, ejecutando acciones no autorizadas.
- **Payload**: Es la carga maliciosa que se ejecuta una vez que el exploit ha tenido éxito. Puede incluir acciones como la instalación de malware, robo de datos o la creación de puertas traseras.

Privacidad/Anonimato

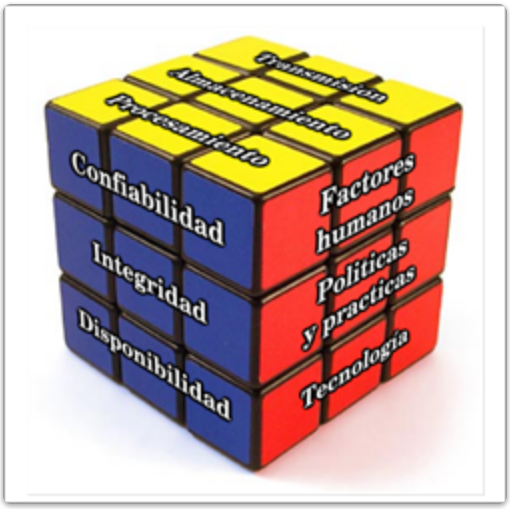
- **Privacidad:** Se refiere al control que una persona o entidad tiene sobre su información personal. Esto implica la capacidad de decidir qué datos compartir, con quién compartirlos y en qué condiciones.
  Ejemplo: Un usuario de redes sociales configura su perfil para que únicamente sus amigos puedan ver sus publicaciones.
- **Anonimato:** Es la capacidad de actuar o comunicarse sin que se revele la identidad de la persona. Su objetivo es proteger al individuo de la identidad personal, ya sea por medio de su nombre, dirección IP, huella digital o cualquier otra información identificable.
  Ejemplo: Un activista utiliza la red Tor para publicar un blog sobre corrupción sin revelar su identidad, protegiéndose de represalias

Arquitectura Zero Trust

Se basa en el principio fundamental de **"nunca confíes, siempre verifica"**. A diferencia de los modelos de seguridad tradicionales que se centraban en proteger el perímetro de la red, Zero Trust asume que las amenazas pueden originarse tanto desde fuera como desde dentro de la red. Algunos puntos clave de esta arquitectura son:

- **Verificación constante:** Requiere que todos los usuarios, ya estén dentro o fuera de la red de la organización, sean autenticados, autorizados y validados continuamente antes de concederles o mantener el acceso a aplicaciones y datos.
- **Privilegio mínimo:** Se asegura que empleados, equipos y terceros tengan acceso solo a los recursos de TI que estrictamente necesitan.

Cubo de McCumber



Principios de seguridad

- **Confidencialidad:** Se refiere a la protección contra el acceso no autorizado a la información. Asegura que los datos sean accesibles por personas, procesos o sistemas autorizados, minimizando el riesgo de filtración de información sensible
  Ejemplo: Encripta la información de clientes durante su transmisión (SSL/TLS en sitios web).
- **Integridad:** Asegura que la información se mantenga precisa, completa y confiable a lo largo del tiempo, evitando alteraciones no autorizadas o daños durante el almacenamiento, transmisión o procesamiento de los datos.
  Ejemplo: Utilizar firmas digitales para asegurarse de que los documentos enviados no han sido alterados.
- **Disponibilidad:** Busca que los usuarios autorizados puedan acceder a los datos y sistemas cuando sea necesario, minimizando tiempos de inactividad o interrupciones debido a fallos técnicos, ataques o desastres.
  Ejemplo: Sistemas de respaldo y failover permiten mantener los servicios accesibles, incluso durante fallos.

Estado de datos

- **Datos en tránsito:** Son aquellos que se están enviando de una lugar a otro, ya sea dentro de la misma red, entre redes o a través de Internet. Durante este estado, los datos son vulnerables a intercepciones y manipulaciones.
- **Datos almacenados:** Son aquellos que están guardados en dispositivos locales o en almacenamiento remoto. Durante este estado, los datos no están siendo procesados o

transmitidos, pero deben estar protegido contra accesos no autorizados mediante cifrado y controles de acceso.

- **Datos en proceso:** Son aquellos que están siendo activamente manipulados, como durante la entrada, modificación, cálculo o análisis. Este estado representa el momento en que los datos son más susceptibles a errores, alteraciones maliciosas o pérdidas.

Medidas de seguridad

Están diseñadas para proteger los datos y la infraestructura de una organización. para ello, deben basarse en varios pilares fundamentales que abordan distintos aspectos de la protección: **Factor humano, Tecnología, Políticas y Procedimientos**. Estos pilares aseguran que todos los elementos de seguridad estén integrados y sean manejados de forma efectiva.

Controles de seguridad

Controles físicos

Están diseñados para proteger los activos físicos de la organización y prevenir accesos no autorizados a áreas sensibles. Estos incluyen el uso de dispositivos de hardware como lectores de tarjetas, controles de acceso biométricos, cámaras de vigilancia, cercas perimetrales y características arquitectónicas específicas de los edificios, como puertas blindadas o sistemas de acceso restringido. Además, las acciones de seguridad deben ser realizadas por el personal autorizado, que debe estar capacitado para manejar las medidas de seguridad de forma adecuada.

Controles técnicos

Son medidas de seguridad implementadas directamente en los sistemas informáticos y redes de la organización. Estos incluyen mecanismos automáticos de protección como firewalls, sistemas de detección de intrusiones (IDS), cifrado de datos, control de acceso basado en roles (RBAC), autenticación multifactor (MFA), y políticas de gestión de parches. Además, facilitan la detección de incidentes de seguridad, permiten auditar accesos y actividades y aseguran la protección de aplicaciones y datos sensibles, tanto en reposo como en tránsito.

Controles administrativos

Son políticas, procedimientos y directivas que regulan el comportamiento de las personas dentro de la organización, así como las interacciones con partes externas. Estos controles incluyen la implementación de políticas de seguridad, formación continua en ciberseguridad para empleados, normativas para el manejo adecuado de datos sensibles, políticas de respuesta ante incidentes, y auditorías regulares para asegurar el cumplimiento.

Defensa en profundidad

Security Onion

Es un modelo que esta basado en la idea de múltiples capas de seguridad. Cada una de las capas representa una medida de protección (Firewall, IDS, MFA, segmentación de red) que un atacante debe de superar para comprometer el sistema. La ventaja de este modelo es la redundancia en las defensas, lo que aumenta a probabilidad de detectar un posible ataque.
Ejemplo: Un atacante intenta acceder a un servidor corporativo. Pero primero deberá de enfrentar un firewall, luego un detector de intrusiones (IDS) y por ultimo, la autenticación multifactor (MFA). Estas capas deben de ser superadas para comprometer el sistema.

Security Artichoke

En este modelo cada una de las capas de defensa puede contener información sensible, lo que implica que no es necesario llegar hasta el núcleo del sistema para extraer datos valiosos. Esto evidencia la importancia de asegurar cada capa adecuadamente, evitando fugas de información en puntos superficiales.
Ejemplo: Un empleado descuida proteger algunos datos en un sistema compartido. Aunque el atacante solo compromete una capa, este puede acceder a datos relevante de la empresa sin necesidad de evadir otros sistemas de seguridad.

Gestión de riesgos

Es un proceso estratégico esencial para las organizaciones que buscan proteger sus activos digitales y garantizar la continuidad de sus operaciones. Consiste en identificar, analizar, evaluar y mitigar las amenazas que acechan a los sistemas de información. El objetivo principal es establecer controles preventivos y reducir la exposición a posibles incidentes de seguridad.

Etapas clave en la gestión de riesgos de ciberseguridad

1. **Identificación de riesgos:** El primer paso es reconocer y documentar las posibles amenazas y vulnerabilidades que podrían afectar a la organización. Esto implica un conocimiento profundo de los activos de información y los posibles puntos débiles en la infraestructura de ciberseguridad.
2. **Análisis y Evaluación:** Una vez identificados los riesgos, se procede a analizarlos para comprender su posible impacto en la organización. Se evalúa la probabilidad de que ocurran y el daño potencial que podrían causar a los activos digitales y las operaciones del negocio.
3. **Gestión y Mitigación:** En esta etapa, se definen y aplican las estrategias para tratar los riesgos identificados. Esto puede incluir la implementación de controles de seguridad, la transferencia del

riesgo (como seguros cibernéticos) o la aceptación del riesgo cuando el costo de mitigación es demasiado alto en comparación con el impacto potencial.

4. **Monitoreo y Revisión:** La gestión de riesgos es un proceso continuo. Es fundamental monitorear constantemente el panorama de amenazas, revisar la efectividad de los controles implementados y ajustar las estrategias de gestión de riesgos según sea necesario para adaptarse a los nuevos desafíos y vulnerabilidades.

Respuesta a incidentes

Es el conjunto de procesos y acciones que una organización debe llevar a cabo para detectar, contener, erradicar y recuperarse de un incidente de seguridad informática. Es una función crítica para minimizar el daño y restaurar las operaciones normales lo más rápido posible tras un ciberataque.

Fases clave en la respuesta a incidentes

1. **Preparación:** Antes de que ocurra un incidente, es fundamental establecer un plan de respuesta a incidentes. Esto incluye definir roles y responsabilidades, establecer procedimientos de comunicación, identificar los activos críticos y configurar las herramientas y tecnologías necesarias para la detección y respuesta.
2. **Detección y Análisis:** Esta fase se centra en identificar la ocurrencia de un incidente de seguridad. Implica la monitorización continua de los sistemas y redes, el análisis de alertas de seguridad y la evaluación de posibles eventos sospechosos para confirmar si se trata de un incidente real y determinar su alcance y naturaleza.
3. **Contención:** Una vez confirmado un incidente, el objetivo principal es evitar que se propague y minimizar su impacto. Las acciones de contención pueden incluir el aislamiento de sistemas afectados, la segmentación de redes, la deshabilitación de servicios comprometidos o la modificación de reglas de firewall.
4. **Erradicación:** Esta fase se enfoca en eliminar la causa raíz del incidente y restaurar los sistemas a un estado seguro. Puede implicar la eliminación de malware, la corrección de vulnerabilidades, la reconstrucción de sistemas comprometidos o la restauración de datos desde copias de seguridad.
5. **Recuperación:** El objetivo de esta fase es restaurar las operaciones normales de la organización lo más rápido posible. Incluye la recuperación de sistemas y datos, la validación de la seguridad de los sistemas restaurados y la reanudación gradual de los servicios afectados.
6. **Lecciones Aprendidas (Post-incidente):** Después de resolver el incidente, es crucial realizar una revisión post-incidente para analizar lo sucedido, identificar las causas raíz, evaluar la efectividad de la respuesta y documentar las lecciones aprendidas. Estas lecciones deben utilizarse para mejorar el plan de respuesta a incidentes y fortalecer la postura de seguridad de la organización.

Modelos de control de acceso

Control de acceso discrecional (DAC)

Es el modelo menos restrictivo y permite a los usuarios controlar el acceso a sus datos como si fueran propietarios de esos datos, puede utilizar una ACL u otros métodos para especificar que usuarios o grupos de usuarios tienen acceso a la información.

Control de acceso obligatorio (MAC)

Se aplica el más estricto control de acceso y suele utilizarse en aplicaciones militares o fundamentales para la misión, asigna etiquetas del nivel de seguridad a la información y habilita el acceso de los usuarios en función del nivel de autorización.

Control de acceso basado en roles (RBAC)

Las decisiones de acceso se basan en los roles y las responsabilidades del individuo dentro de la organización, se asignan privilegios de seguridad a diferentes roles y se asignan personas al perfil RBAC para el rol. Las funciones pueden incluir diferentes puestos, clasificaciones de puestos o grupos de clasificaciones de puestos.

Control de acceso basado en atributos (ABAC)

Permite el acceso según los atributos del objeto (recurso) al que se tendrá acceso, el sujeto (usuario) que tendrá acceso al recurso y los factores del entorno respecto de cómo se tendrá acceso al objeto.

Control de acceso basado en reglas (RuBAC)

El personal de seguridad de red especifica conjuntos de reglas o condiciones asociadas con el acceso a datos o sistemas. Estas reglas pueden especificar direcciones IP permitidas o denegadas, o ciertos protocolos y otras condiciones.

Control de acceso basado en tiempo (TAC)

Permite el acceso a los recursos de red en función de la hora y el día.

Protocolos de autenticación

Protocolo de autenticación extensible (EAP)

La contraseña del cliente se envía mediante un hash al servidor de autenticación. El servidor de autenticación tiene un certificado.

Protocolo de autenticación de contraseña (PAP)

Un nombre de usuario y una contraseña se envían a un servidor de acceso remoto en texto plano. La mayoría de los servidores de sistemas operativos de red admiten PAP. Es un protocolo inseguro ya que transmite la información en texto plano

Protocolo de confirmación de aceptación de la autenticación (CHAP)

CHAP valida la identidad de clientes remotos mediante una función de hash unidireccional creada por el cliente. El servicio también calcula el valor hash esperado. El servidor compara los 2 valores, si ambos coinciden, la transmisión continúa. Este mismo también verifica periódicamente la identidad del cliente durante la transmisión.

Tecnologías de autenticación

802.1x

Una organización autentica su identidad y autoriza el acceso a la res. Su identidad se determina en función de las credenciales o de un certificado confirmado por un servidor RADIUS.

RADIUS

Cuando se necesita una autenticación de nombres de usuario/contraseña, se utiliza RADIUs para aceptar o denegar el acceso. Este servicio solo encripta la contraseña del usuario desde el cliente RADIUS al servidor RADIUS. El nombre de usuario, registro de uso y los servicios autorizados se transmiten en texto plano. Cuando se implementa esta tecnología solo son necesarios medidas de seguridad que protejan contra los ataques de repetición.

TACACS+

Utiliza TCP como protocolo de transporte. Esta cifra todos los datos entre el cliente y servidor. Dado que los administradores de red pueden definir listas ACLs, filtros y privilegios de usuarios, es la mejor opción para las redes corporativas que requieren pasos de autenticación más sofisticados y control sobre las actividades de autorización.

Kerberos

Kerberos utiliza un cifrado fuerte, solicitando a un cliente que demuestre su identidad a un servidor, y el servidor a su vez se autentica ante el cliente.
El servidor Kerberos contiene ID de usuario y contraseñas con hash para todos los usuarios que tendrán autorizaciones para los servicios del dominio. El servidor Kerberos también tiene claves secretas compartidas con todos los servidores a los que concederá tickets de acceso. El primer ticket es un ticket de concesión de tickets emitido por el servicio de autenticación a un cliente solicitante. El cliente puede presentar este ticket al servidor Kerberos con una solicitud de ticket para acceder a un servidor específico.
Al poder cifrar toda la sesión se elimina la transmisión intrínsecamente insegura de elementos que pueden ser interceptados en la red. Los tickets tienen fecha de caducidad, por lo que cualquier intento de reutilización de un ticket no tendrá éxito.

Funcionamiento de AAA

El protocolo de autenticación, autorización y auditoría (AAA) proporciona el marco de trabajo necesario para habilitar la seguridad de acceso escalable

Authentication/Autenticación

Los usuarios y administradores deben probar que son quienes dicen ser, la autenticación se puede establecer utilizando combinaciones de nombre de usuario y contraseñas, preguntas de desafío y respuestas, tarjetas de token y otros métodos.
La autenticación proporciona una forma centralizada de controlar el acceso a la red.

Authorization/Autorización

Una vez autenticado el usuario, los servicios de autorización determinan a qué recursos puede acceder el usuario y que operación está habilitado para realizar.

Accounting/Contabilidad

Los registros de contabilidad tienen también la función de registrar lo que hace el usuario, incluidos los elementos a los que accede, la cantidad de tiempo que accede al recurso y todos los cambios que se realizaron. La contabilidad realiza un seguimiento de la forma en que se utilizan los recursos de red.

By JPablo13