Fundamentos de la Ciberseguridad

CIB

ALBERTO MÉNDEZ NÚÑEZ

Contenido

1. Conceptos básicos de seguridad

Amenaza: es todo aquello que puede poner en peligro nuestra información.

Vulnerabilidad: es una debilidad o un fallo en nuestro sistema que puede ser explotada por un atacante.

Confidencialidad: garantizar que la información solo sea accesible a las personas autorizadas.

Integridad: asegurar que la información no sea alterada de manera no autorizada.

Disponibilidad: que la información esté disponible y utilizable cuando los usuarios autorizados la necesiten.

Datos sensibles: Información que, por su naturaleza, requiere mayor protección debido a su carácter personal o confidencial.

Ciclo de vida de la información: Conjunto de etapas por las que pasa la información desde su creación hasta su destrucción.

2. Tipos de ataques y malware

Malware: software malicioso diseñado para dañar, robar información o tomar el control de sistemas.

Ransomware: tipo de malware que cifra los archivos del usuario y exige un pago para liberarlos.

Ingeniería social: manipulación psicológica de personas para obtener acceso a información o sistemas.

DoS: ataque de denegación de servicio que busca hacer que un servicio no esté disponible saturándolo con peticiones falsas desde un mismo dispositivo.

DDoS: ataque de denegación de servicio distribuido que busca hacer que un servicio no esté disponible saturándolo con peticiones falsas desde varios dispositivos.

Man-in-the-Middle: ataque en el que un intruso intercepta y manipula la comunicación entre dos partes sin que lo sepan.

Exploit: código o técnica que aprovecha una vulnerabilidad en un sistema para comprometerlo.

Inyección SQL: ataque que inserta código SQL malicioso en una consulta para acceder o modificar bases de datos.

Cross-Site-Scripting: ataque que inyecta scripts maliciosos en páginas web vistas por otros usuarios.

3. Protección de la información y acceso

Cifrar: transformar datos con un algoritmo de cifrado para proteger la información.

Autenticación Multifactor: método de verificación que requiere más de un factor.

Roles: responsabilidades asignadas a un usuario dentro de un sistema.

Permisos: autorizaciones que se le otorgan a un usuario que controlan las cosas que puede o no hacer en un sistema.

Políticas de acceso: Normas y reglas que determinan quién puede acceder a qué información o recursos dentro de un sistema o red.

4. Dispositivos y control de red

Router: dispositivo que dirige el tráfico entre diferentes redes y aplica medidas básicas de seguridad.

Proxy: Es un servidor intermediario que actúa como puente entre tu dispositivo y internet.

Regla de firewall: instrucción de seguridad que controla qué tráfico de red está permitido o bloqueado.

Filtrado de puertos: técnica para permitir o bloquear el tráfico que usa ciertos puertos de red.

Filtrado de protocolos: control del tráfico según el tipo de protocolo.

Cortafuegos: Dispositivo o software que controla el tráfico de red según reglas predefinidas, permitiendo o bloqueando conexiones.

Cortafuegos basado en red: Firewall que protege toda la red y filtra tráfico entre segmentos, aplicando políticas centralizadas.

Cortafuegos basado en host: Firewall instalado en un equipo individual (servidor, PC o dispositivo) para protegerlo del tráfico no autorizado.

5. Sistemas de seguridad y software

Antivirus: Software que detecta, bloquea y elimina malware en sistemas y dispositivos.

Antimalware: Software diseñado para detectar, prevenir y eliminar todo tipo de malware (virus, troyanos, ransomware, spyware, etc.).

IDS: Sistema de detección de intrusiones que monitorea la red o sistemas para identificar actividad sospechosa o ataques.

IPS: Sistema de prevención de intrusiones que detecta y bloquea automáticamente actividad maliciosa en tiempo real.

Herramientas de monitoreo: Software o sistemas que supervisan continuamente la red, servidores, aplicaciones o dispositivos para detectar cambios, problemas de rendimiento o actividad sospechosa.

Herramientas de auditoría: Sistemas que permiten revisar y evaluar la seguridad, configuraciones y cumplimiento de políticas.

6. Gestión de incidentes y respuesta

Incidentes de seguridad: Eventos o series de eventos que comprometen la confidencialidad, integridad o disponibilidad de la información o los sistemas.

Detección: Proceso de identificar eventos de seguridad o actividad sospechosa en la red o sistemas.

Análisis: Etapa donde se investigan los incidentes detectados para entender el alcance, la causa y el impacto.

Contención: Acciones para limitar la propagación o el impacto de un incidente mientras se desarrolla la respuesta.

Erradicación: Eliminar completamente la causa raíz del incidente.

Recuperación: Restaurar los sistemas a su estado normal de funcionamiento tras un incidente de seguridad.

Aprendizaje: Revisión posterior al incidente para identificar mejoras en procesos, políticas y herramientas, reduciendo riesgos futuros.

Indicadores de compromiso: Evidencias que muestran que un sistema ha sido comprometido o atacado.

Estrategias proactivas: Medidas preventivas para reducir la probabilidad de incidentes de seguridad.

Análisis forense: Investigación detallada de un incidente de seguridad para descubrir cómo ocurrió, quién lo causó y qué se vio afectado.

Diagnóstico de fallos: Proceso de identificación y análisis de problemas o errores en sistemas, redes o aplicaciones.

Propuesta de mejora: Sugerencia o plan para optimizar procesos, sistemas o controles de seguridad basándose en el diagnóstico o auditoría realizada.

Registro de incidencias: Documento o sistema que documenta todos los incidentes ocurridos, incluyendo detalles, responsables, acciones tomadas y resultados.

7. Normativas y cumplimiento

RGPD: Normativa europea que regula la protección de datos personales de ciudadanos de la UE.

ENS: Marco normativo español que establece medidas de seguridad para los sistemas de información del sector público.