CLASIFICACIÓN DE LAS MEDIDAS DE PROTECCIÓN

MEDIDAS PASIVAS

Escanear y desinfectar de malwares

Todos los equipos informáticos que se hayan visto afectados por esta intromisión en la seguridad.

Recuperar las copias de seguridad

Guardar toda nuestra información guardada y en buen estado.

Particiones de discos duros

Para almacenar las copias y evitar que el malware se extienda a más equipos.

Usar algún almacenamiento en la nube

Es sencillo, es barato y puede salvarnos la vida ante un ataque contra nuestros sistemas.

Escanear y desinfectar de malwares

Todos los equipos informáticos que se hayan visto afectados por esta intromisión en la seguridad.

Recuperar las copias de seguridad

Guardar toda nuestra información guardada y en buen estado.

Particiones de discos duros

Para almacenar las copias y evitar que el malware se extienda a más equipos.

Usar algún almacenamiento en la nube

Es sencillo, es barato y puede salvarnos la vida ante un ataque contra nuestros sistemas.

Medidas activas

Sistemas de detección y prevención de intrusiones (IDS/IPS)

Herramientas que monitorean y analizan el tráfico de la red, alertando sobre actividades sospechosas y bloqueando posibles ataques en tiempo real.

Autenticación multifactor (MFA)

Requiere varios métodos de verificación (contraseña, código en el móvil, huella dactilar) para asegurar el acceso a sistemas o aplicaciones.

Firewall

Un sistema que filtra el tráfico de red, permitiendo o bloqueando el acceso a diferentes recursos en función de reglas predefinidas, evitando ataques como el acceso no autorizado.

Respuesta ante incidentes

Planes y acciones diseñados para responder rápidamente ante un ataque cibernético, minimizar su impacto y restaurar los sistemas afectados.

Monitoreo continuo de redes

Uso de herramientas para observar en tiempo real las actividades en la red, detectando anomalías o comportamientos inusuales que puedan indicar un ataque.

Cifrado de datos en tránsito

Proteger los datos que se transmiten entre dispositivos y redes mediante el uso de protocolos seguros, como TLS, para evitar que sean interceptados o modificados.

Segmentación de red

Dividir una red en partes más pequeñas y seguras, lo que limita el acceso entre secciones y evita que un ataque en una parte afecte a toda la red.

Honeypots

sistemas de seguridad que actúan como carnada o señuelo para atraer a posibles atacantes y estudiar sus tácticas sin que comprometan los sistemas reales. Aquí te detallo qué hacen:

Medidas preventivas

Educación y concienciación del personal

Capacitar a los empleados sobre buenas prácticas de ciberseguridad, como evitar correos de phishing, crear contraseñas seguras y reconocer comportamientos sospechosos.

Políticas de gestión de contraseñas

Implementar reglas estrictas para la creación, uso y caducidad de contraseñas, como el uso de combinaciones complejas y el cambio regular de las mismas.

Análisis de vulnerabilidades

Realizar auditorías y escaneos periódicos en la infraestructura para detectar posibles vulnerabilidades antes de que los atacantes puedan explotarlas.

Cifrado de datos en reposo

Aplicar cifrado a los datos almacenados en discos duros, bases de datos o dispositivos, protegiéndolos en caso de acceso no autorizado o robo.

Control de acceso basado en roles (RBAC)

Restringir el acceso a sistemas y datos sensibles solo a aquellos empleados que realmente lo necesitan para cumplir con sus funciones.

Restricción de dispositivos externos

Limitar el uso de dispositivos externos como memorias USB o discos duros portátiles en los sistemas corporativos para evitar la propagación de malware o el robo de datos.

Política de acceso remoto seguro

Implementar conexiones seguras para el acceso remoto a los sistemas corporativos, como el uso de redes privadas virtuales (VPN) y autenticación multifactor (MFA), para proteger a los empleados que trabajan desde fuera de la oficina.

Bloqueo automático de cuentas tras intentos fallidos

Configurar los sistemas para que bloqueen automáticamente las cuentas de usuario después de varios intentos fallidos

Medidas detectivas

detección de intrusiones (IDS)

Un sistema de detección de intrusiones (IDS) es una herramienta de seguridad de red que monitoriza el tráfico y los dispositivos de la red en busca de actividades maliciosas conocidas, actividades sospechosas o infracciones de las políticas de seguridad.

Prevención de intrusiones (IPS)

Un sistema de prevención de intrusiones (IPS) supervisa el tráfico de red en busca de amenazas potenciales y las bloquea automáticamente mediante alertas al equipo de seguridad, la terminación de conexiones peligrosas, la eliminación de contenidos maliciosos o la activación de otros dispositivos de seguridad.

Monitoreo de logs

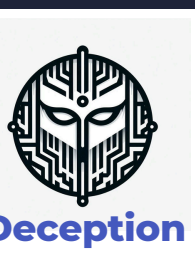
El monitoreo de logs es el proceso de recopilar, analizar y utilizar datos de distintas fuentes. Esto puede incluir aplicaciones e infraestructura; procesamiento, red y almacenamiento.

Análisis de Comportamiento

Estas técnicas se centran en identificar patrones inusuales o sospechosos en el tráfico de red, actividades de usuarios y otros datos relacionados con la seguridad informática.

Sistemas de Información y Gestión de Eventos de Seguridad (SIEM)

Es una solución de seguridad que ayuda a las organizaciones a detectar y analizar amenazas y responder a ellas antes de que afecten a las operaciones del negocio.



Deception Technology

La tecnología de engaño es una categoría de soluciones de ciberseguridad que detectan amenazas tempranas con tasas bajas de falsos positivos.

Auditorías de seguridad

Revisiones periódicas que evalúan el cumplimiento de las políticas de seguridad y la presencia de vulnerabilidades en los sistemas de una organización

Sistemas de Monitoreo de Integridad de Archivos (FIM)

Verifican los cambios en archivos críticos del sistema o configuraciones. Cualquier alteración no autorizada o inesperada genera una alerta