pimec
Micro, petita i mitjana empresa de Catalunya

DTE – DIAGNÓSTICO TÉCNICO EXTERIOR

SERVICIO INTEGRAL DE CIBERSEGURETAT PARA COMPRENDER Y MITIGAR LOS RIESGOS ASOCIADOS A SU PRESENCIA EN INTERNET

Mediante un enfoque exhaustivo, el DTE evalúa la exposición pública de la organización, identificando vulnerabilidades en sus servicios web, dominios, subdominios y direcciones IP conocidas. Este servicio no solo proporciona una evaluación detallada y proactiva de la seguridad externa de una empresa, sino que también ofrece las herramientas y el conocimiento necesarios para ir un paso por delante de las amenazas cibernéticas.

¿QUÉ INCLUYE?

1. Evaluación de la Exposición de Dominios y Subdominios:
- Análisis detallado de todos los dominios y subdominios registrados de la empresa para identificar configuraciones erróneas, vulnerabilidades conocidas y potenciales brechas de seguridad.

2. Análisis de Vulnerabilidades en Servicios Web:
- Escaneo de todos los servicios web expuestos en Internet para detectar vulnerabilidades como SQL injection, XSS y fallos de configuración de seguridad.
- Pruebas de penetración ligera para evaluar la resistencia de los sistemas ante ataques simulados.

3. Inspección de IP Conocidas:
- Escaneo de todas las direcciones IP asociadas a la empresa para evaluar los servicios que están expuestos y analizar sus configuraciones de seguridad.
- Identificación de puertos abiertos, servicios innecesarios existentes en las IP y potenciales puntos de entrada para atacantes.

4. Informe de Correcciones y Recomendaciones:
- Entrega de un informe detallado que incluye un resumen ejecutivo de los hallazgos, detalles técnicos de las vulnerabilidades detectadas y un plan de acción prioritaria para ponerles solución.
- Recomendaciones basadas en las mejores prácticas de la industria para reforzar la seguridad y reducir la superficie de ataque de la organización.

¿CÓMO AYUDA ESTO A MI EMPRESA?

- **Visibilidad Completa: O**btener una visión clara de su superficie de ataque externo y comprender mejor de qué manera los atacantes podrían ver su infraestructura desde el exterior.
- **Priorización de Riesgos:** Priorizar las vulnerabilidades a partir del nivel de riesgo, permitiendo una asignación efectiva de recursos para mitigar en primer lugar las amenazas más críticas.
- **Mejora Continua:** con recomendaciones prácticas y estratégicas, su empresa puede mejorar continuamente su posición de seguridad ante un panorama de amenazas en evolución.

¿A QUIÉN VA DIRIGIDO?

- Pequeñas y medianas empresas que buscan mejorar su posición de seguridad externa.
- Las organizaciones que necesitan cumplir con las regulaciones y estándares de seguridad informática.
- Negocios que deben prevenir brechas de seguridad y proteger sus activos críticos de información.

Contacto
Departamento de Tecnología e innovación
Imma Navarra
inavarra@pimec.org | Tel. 93 496 45 00

Clica aquí para acceder al servicio