

Hoy en día el funcionamiento de los negocios y proyectos basados en sistemas de información no se determinan únicamente por las facilidades de la tecnología que se usa, sino también por la disponibilidad, la confidencialidad y la seguridad de la infraestructura y los datos.

Revisar y asegurar estos factores son parte del trabajo de los responsables de sistemas de las propias empresas. Aunque la continua evolución y complejidad de los sistemas de comunicación y la creciente estadística de ataques informáticos, han priorizado esta preocupación por parte de las compañías y de sus dptos. de informática. Y es que aumentan cada día más la originalidad y la variedad de los tipos de ataques que se producen y paralelamente aumenta la incertidumbre de si los sistemas informáticos son del todo seguros.

Objetivos:

El conocimiento de nuestros técnicos especializados en sistemas de Internet, redes y comunicaciones y mediante el apoyo de una gran variedad de herramientas de software, hemos consolidado una serie de soluciones adaptadas a sus necesidades en este ámbito. Estudiamos la confidencialidad, la integridad y la disponibilidad de la información mediante el uso de diversas tecnologías en análisis de vulnerabilidades, cortafuegos, antivirus, detección de intrusos y análisis de contenidos.

En la actualidad las amenazas provienen de hackers, empleados, ex empleados, competencia, clientes, proveedores, etc. Y las realizan mediante interrupción de sistemas, destrucción o modificación de datos, robo, copia de datos, virus, caballos de troya, negación de servicios, etc. Utilizan herramientas de software que están ampliamente distribuidas por Internet, y sin ningún coste. Esto puede provocar para el cliente, pérdida de reputación, decremento de los beneficios, problemas relacionados con responsabilidades legales.

Desde 1998 en ServicioHelpDesk hemos facilitado más seguridad a aquellos clientes que necesitan una mayor confianza sobre la protección de sus sistemas, más tranquilidad para sus negocios.

Servicio:

Mediante este servicio añadimos una fase a nuestro servicio básico de detección de vulnerabilidades que se basa fundamentalmente en realizar acciones de intrusión. Estas acciones las realizamos de forma remota a la red, imitando la forma de proceder de un atacante real externo a la organización.

Se intentará penetrar en los sistemas del cliente utilizando procedimientos automatizados por software (forma pasiva), como procedimientos manuales no automatizados (Forma activa). Dependiendo de la configuración del sistema de conexión a Internet se realizarán unas acciones u otras.

Las acciones de intrusión se realizan en: Daemons, DNS, Email, Firewalls, FTP, NetBIOS, NFS, NT Usuarios y grupos y Passwords, NT Registry, Servicios de NT/2000/XP/2003, Servicios RPC, WEB Browser y zonas de seguridad, Web Server Scan, Proxy, CGI-Bin, X Windows, Terminal Server, Servidores VPN, Servicios Telnet, Servicios de impresión, etc.

Acciones que se realizan:

- Escáner de 65.535 puertos para una dirección IP.
- Test de vulnerabilidad: Búsqueda de los agujeros de seguridad.
- Testeos de Intrusión (Automatizadas).
- Acciones de Intrusión (No automatizadas).
- Fuerza bruta.
- Denegación de servicios (Bajo supervisión del cliente).
- IP Spoofing.
- Cuantificación del riesgo.
- Descripción de soluciones a adoptar.
- Indicación de qué parches hay que implantar en los softwares o servicios activos (en caso de que el fabricante lo disponga), que solventen las vulnerabilidades detectadas.
- Informe final con conclusiones.

Resultado final:

Al finalizar las pruebas oportunas, se entrega un informe completo con todas las acciones realizadas y el resultado de cada una de ellas, indicando, de ser necesario, las medidas de seguridad que recomendamos llevar a cabo para solventar dichos problemas de seguridad.