Servicio: Reordenamiento de Infraestructura Digital

Precio: CUP: $63312.00

Exportable: No
Calificación: 0.0
Comentarios: 0
Vistas: 516

Descripción:

Una de las principales problemáticas que tienen las empresas, con el empleo de tecnologías de la información y las comunicaciones en sus procesos, es la actualización constante de la infraestructura tecnológica y con ello, el uso ineficiente de los recursos, dado por una inadecuada planificación de crecimiento y actualizaciones paulatinas. Después de tener funcionando toda una infraestructura tecnológica que asegura servicios para el trabajo diario, es complejo acometer tareas de reorganización de los recursos con el objetico de optimizar su uso.

La implementación de nuevos servicios telemáticos, el despliegue de plataformas para videoconferencias y otros sistemas que contribuyen directamente a la informatización de los procesos claves en su organizacion, no siempre van acompañados de mejoras en la gestión de la seguridad de la información y la ciberseguridad, ambas ramas vitales de la **SEGURIDAD INFORMATICA.** Uno de los pilares fundamentales del servicio es la implementacion del paradigma de seguridad por oscuridad en los servicios, apoyandonos en el modelo Zero Trust (Cero Confianza) para cohesionar la seguridad en sistemas.

El paradigma de ciberseguridad “Zero Trust” o sea Confianza Cero explícitamente plantea el tratamiento a todas las redes a las cuales se les brinda acceso a los servicios como redes de internet. La implementación de este paradigma se reforzó con un modelo desarrollado por los especialistas de la División, que se basa

en el modelo de seguridad por oscuridad que se emplea por los desarrolladores de software para la protección de sus sistemas, pero adaptado a la teleinformática de manera que a través de los procesos de NAT y PAT los usuarios de los diferentes tipos de redes asociados a nuestra red de servicios solo conocen el dirección IP del cortafuegos como punto de acceso a cualquier servicio.

Características:

Sistemas de Nombre de Dominio

Implementacion de Listas de Control de Acceso (ACL) por subredes, reforzado con múltiples vistas de las zonas de dominio donde solo se brinda a las subredes la información necesaria para el trabajo de los usuarios.

Sistemas de Proxy Inverso

Si visita páginas HTTP simples mientras está conectado, su sesión puede ser secuestrada, y ni siquiera la autenticación de dos factores lo protegerá. Para proteger toda la información enviada entre usted y su servidor web, redirigiremos todas las solicitudes que lleguen a través de HTTP simple al equivalente seguro HTTPS, interceptando las conexiones cliente - servidor y garantizando la seguridad de las comunicaciones mediante la encriptación usando certificados seguros.

Sistemas Cortafuegos y de Deteccion de Intrusos

Un firewall o cortafuegos es un dispositivo hardware o software que permite filtrar el tráfico tanto entrante como saliente de una red. El uso de procedimientos de Traducción de Direcciones de Red (NAT) y Traducción de Direcciones de Puertos (PAT) en el cortafuegos, es un mecanismo que además de enmascarar el tráfico garantiza que el único punto de acceso a la subred de servicios o Zona Desmilitarizada (DMZ) sea el cortafuegos.

Este servicio pertenece a la empresa Xetid División Territorial Holguín
https://empresascubanas.xutil.net/xetidhlg