

Productos y Servicios en el área de Seguridad

Análisis de Vulnerabilidad

El Centro de Tecnología NWEB, C.A., es una empresa joven que participa en el mercado tecnológico como Integrador de Soluciones en las distintas áreas de negocio, manteniendo siempre el reconocimiento de cada empresa a la que le ha prestado servicio, así como el nivel de calidad de las soluciones entregadas.

En estas distintas áreas se ha caracterizado por ofrecer soluciones de última tecnología orientadas a satisfacer los requerimientos generales y específicos de cada empresa, de acuerdo a sus políticas y basadas en estándares del mercado.



Dentro de las soluciones que mercadea están Centrales de VoIP, Call Center, Help_desk, Software para Evaluación de la Seguridad de Redes, Encriptado de Discos, Archivos, etc. dispositivos de redes y seguridad, servidores y estaciones de trabajo, servicios profesionales y entrenamiento, entre otras.

La cartera de productos y/o servicios en el área de Seguridad es una de las más amplias, cubriendo todas las subáreas que se definen dentro del tema.



Considerando que la información es el activo más importante para las empresas, su seguridad viene a ser la pieza fundamental del negocio.

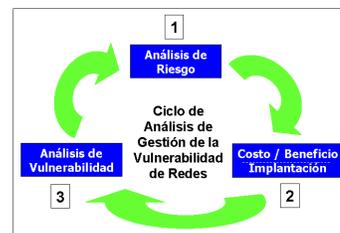
Se ofrecen productos y servicios profesionales en seguridad y planificación para ayudar a las distintas organizaciones a proteger su activo crítico de información, como es el caso, entre otros, del Análisis de Vulnerabilidad.

Análisis de Vulnerabilidad

Actualmente las organizaciones en todos los niveles tienen cada día mayor dependencia de la Tecnología de la Información (TI), para realizar las operaciones propias del negocio, esta realidad hace necesario que ellas tomen las medidas conducentes a resguardar su información crítica.

El Análisis de Vulnerabilidad consiste en un estudio técnico detallado de las debilidades de los controles de seguridad en el ambiente computacional de las organizaciones.

El servicio de Análisis de Vulnerabilidades provee auditorías de seguridad precisas, exhaustivas, con reportes detallados sobre las vulnerabilidades encontradas, incluyendo niveles de severidad, impacto en el negocio, tiempo estimado de corrección y análisis de tendencias.



A través del monitoreo continuo y proactivo de todos los puntos de accesos a las redes, nuestro servicio reduce dramáticamente los tiempos de investigación, escaneo y reparación de exposiciones de las redes, por parte de los grupos de seguridad, habilitando a las empresas a eliminar las vulnerabilidades de sus redes antes que las mismas sean explotadas por los atacantes.

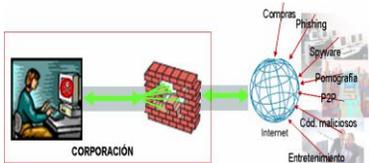
El conjunto de herramientas que se utilizan en este tipo de análisis son bastante seguras, empleando las mejores prácticas existentes en el mercado, técnicas de detección abiertas basadas en software libre y referencias de la base de datos de conocimiento sobre vulnerabilidades más completa en la industria de la seguridad informática.

Este tipo de análisis, de acuerdo a los estándares internacionales de seguridad, se realizan en períodos trimestrales, con una recomendación de

revisiones mensuales con fines de prepararse para el próximo período.

El Análisis de Vulnerabilidad comprende, entre otros, los siguientes aspectos:

- ❖ Técnico: test de vulnerabilidad, con el cual se generará una imagen de cómo está la plataforma tecnológica de la empresa. Se requiere de la información más actualizada de la arquitectura de la red con todos sus componentes representados. Este comprende: test de acceso externo a servidores, acceso interno, acceso wireless/LAN, accesos telefónicos, acceso a estaciones de trabajo, acceso a infraestructura de redes (switches, routers, otros).



Adicionalmente se ofrece: análisis del estado del cuarto de cableado y del diseño de la red, así como de la seguridad física de la red y el acceso a las áreas críticas.

- ❖ Gestión: análisis de cómo se realiza la administración de seguridad en la organización, lo cual comprende: organización de tecnología según lo que establece ISO27001 y 17799.

Pasos en la realización de un Análisis de Vulnerabilidad

Cuando se realiza este tipo de análisis, se ejecutan las siguientes actividades:

- ❖ Descubrimiento: identificación en tiempo real de todos los elementos dentro de la red, como son routers, switches, concentradores, estaciones, servidores, firewalls, sistemas operativos, etc.
- ❖ Exploración: de todos los niveles de seguridad de la red.
- ❖ Análisis de vulnerabilidades
- ❖ Reportar: generar reportes precisos donde se representen análisis de tendencias. Estos pueden ser tanto técnicos, como ejecutivos.
- ❖ Recomendaciones: se indican una serie de observaciones para que se implementen como

soluciones a determinadas vulnerabilidades, de tal manera que el tiempo de exposición a la misma sea el menor posible.

- ❖ Implantación: si la organización lo desea, se puede realizar la implantación de las recomendaciones.

Beneficios de este tipo de Servicios

Los beneficios de contratar este tipo de Servicios se resumen en los siguientes puntos:

- ❖ Incrementa el valor de los sistemas de detección de virus, firewalls e IDS a través del descubrimiento automático de debilidades en las configuraciones.
- ❖ Acelera la velocidad de reparación de vulnerabilidades y mejora la eficiencia del personal de seguridad.
- ❖ Provee ahorros dramáticos en costos operacionales y reducción del Costo Total de Tenencia.
- ❖ Escalable a todo tipo de redes IP.

Personal Certificado

Los servicios de consultoría en seguridad y en general, serán tan efectivos como lo sea la capacitación del personal que los realice.

Una de las mayores fortalezas del Centro de Tecnología NWEB, C.A., es la de contar con personal altamente preparado con certificaciones internacionales y cursos avanzados realizados en instituciones de educación superior o especializada, además de contar con amplia experiencia basada en los distintos proyectos que se han implantado en las áreas respectivas.

Instalaciones

El Centro de Tecnología NWEB, C.A., cuenta con instalaciones de primer nivel para la realización de los entrenamientos en las distintas áreas, considerando la existencia de laboratorios para la implementación de ambientes prácticos.