Charter del Proyecto

Seguridad Informática- Tonantzintla Fonda

Especialistas en Comercio Electrónico, S.A. de C.V.

Versión 1.0

Seguridad Informática

En beneficio del Cliente y principalmente de los consumidores, el portal Tonantzintla fonda, contará con sistemas de seguridad muy avanzados, los cuales proporcionarán una amplia gama de dispositivos, programas, aplicaciones y sistemas de aseguramiento de los datos, identidades, información y todo aquello que el Cliente considera como su patrimonio informático.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran:

La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

Sistema Operativo

Se tiene considerado que el sistema operativo del servidor donde se aloje el portal sea el denominado Apache. Este tipo de sistemas operativos proporcionan amplios rangos de seguridad y tienen una muy baja vulnerabilidad.

El servidor HTTP Apache es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.12 y la noción de sitio virtual.

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado.

Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios

web en el mundo.

La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas tan sólo pueden ser aprovechadas por usuarios locales y no remotamente. Sin embargo, algunas se pueden accionar remotamente en ciertas situaciones, o explotar por los usuarios locales malévolos en las disposiciones de recibimiento compartidas que utilizan PHP como módulo de Apache.

Sistema de seguridad Firewall

Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada «zona desmilitarizada» o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Anti-virus

En informática los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Nacieron durante la década de 1980.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc.

Firewall Appliance

Un Appliance hace referencia a un aparato, es decir, un implemento físico que servirá en este caso como firewall, nos ayudará a filtrar el tráfico no deseado, el spam y código malicioso que pueda poner el riesgo la integridad de la información del cliente.

Se ha seleccionado a CheckPoint para realizar este trabajo, Check Point Software Technologies Ltd. (NASDAQ: CHKP) es un proveedor global de soluciones de seguridad IT. Conocido por sus productos Firewall y VPN, Check Point fue el pionero en la industria con el FireWall-1 y su tecnología patentada de inspección de estado. Hoy en día la compañía desarrolla, comercializa y soporta una amplia gama de software y hardware combinados y productos de software que cubren todos los aspectos de seguridad de IT , incluyendo seguridad de red, seguridad endpoint, seguridad de datos y gestión de seguridad.

Fundada en 1993 en Ramat-Gan, Israel, Check Point cuenta hoy con aproximadamente 2.200 empleados en todo el mundo. Los Centros de desarrollo de la compañía se encuentran en Israel, California (ZoneAlarm), Suecia (ex centro de desarrollo de Protección de Datos) y en Bielorrusia.

La empresa también tiene oficinas en los Estados Unidos, en Redwood City, California y en Dallas, Texas, así como en Canadá en Ottawa, Ontario.

Respaldos de Información

Se llevará a cabo la elaboración de respaldos frecuentes, estos respaldos deberán estar cifrados para evitar que cualquiera tenga acceso a la información y serán resguardados conforme al siguiente:

Plan de Respaldos:

Frecuencia	**Tipo**	**Hora**	**Almacenamiento**
Respaldo Diario	Incremental	00:00 horas	Site
Semanal (Lunes)	Total	02:00 horas	Caja fuerte de dirección
Mensual (día 1º)	Total	02:00 horas	Custodia externa

Certificación del Site

Para aumentar la seguridad de las transacciones en la red, se recurre al servicio de las "Autoridades Certificadoras", que son las que certifican la identidad de las partes emitiendo un "certificado".

"Un certificado es un documento electrónico que se utiliza para identificar a un individuo o a una compañía. Las Autoridades Certificadoras son entidades que validan identidades y proporcionan certificados. Los métodos empleados para la validación de identidades dependen de las políticas de cada CA.

Un certificado es como el pasaporte de una persona. Incluye una clave pública [que sirve para la encriptación], el nombre de la entidad a quien identifica, una fecha de expiración, el nombre de la CA que ha proporcionado el certificado y un número de serie.

Lo más importante de todo, es que el certificado viene firmado digitalmente por la CA, de esta manera es como si la Autoridad Certificadora presentase a la entidad a la que identifica, asegurándonos que confía en la identidad del propietario del certificado".

La documentación que solicitan antes de otorgar un certificado es bastante exhaustiva y los antecedentes obtenidos son verificados de diferentes maneras (verificación de domicilio, control de antecedentes comerciales, etc.).

Nosotros elegiremos las siguientes empresas certificadoras:

VERISIGN (http://www.verisign.com): proporciona firmas para cualquier servidor SSL (servidor seguro) y efectúa estrictas comprobaciones de identidad (Es la más conocida. Los certificados cuestan entre US$ 349 y 995);

BelSign
BelSign (http://www.belsign.be) con oficinas de registro en Bélgica, para la Unión Europea (certificados desde US$ 20 sólo para e-mail y US$ 187 para servidores de web);

IPS
Internet Publishing Services (http://www.ips.es): CA española que entrega certificados basados en SSL en 24 horas.