ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
Facultad de Ingeniera en Electricidad y Computación

Tema:

Diseño de una Infraestructura Tecnológica y Políticas de Uso que permitan alojar Aplicaciones Web de una Manera Segura.

Integrantes:

Erica Paola Sojos Briones [1]

Edwin Daniel López Montesdeoca [2]

Ignacio Abel Zambrano López [3]

Ing. Albert Espinal Santana[4]

[1]Licenciado en Sistemas de información 2004.

[2]Licenciado en Sistemas de información 2004.

[3]Licenciado en Sistemas de información 2004.

[4]Director de Tópico, Título de Pregrado: Ingeniero Eléctrico en Computación, ESPOL, Enero 1990. Título de Postgrado: Magister en Sistemas de Información Gerencial, ESPOL, Enero 2000. Profesor de la ESPOL desde: Mayo 1995

RESUMEN

Esta tesis propone el diseño de una infraestructura tecnológica con sus políticas de uso, de privacidad y de confidencialidad para los usuarios, alojando aplicaciones Web seguras, ya que reconocemos la importancia del manejo discreto y confidencial de toda información proporcionada por los usuarios al momento de realizar diversas tareas. Aparte del desarrollo de las políticas de seguridad, se consideran también los esquemas de respaldo, los planes de contingencias, autenticación de los usuarios y administración de la red.

En el desarrollo de esta infraestructura se ha pensando también en las necesidades de la empresa, en su ahorro y en su funcionabilidad sin dejar a un lado su eficiencia ya que para toda empresa es importante la protección y resguardo de la información privada y personal de cada uno de sus clientes.

Consideremos que la tecnología puede aumentar espectacularmente la eficiencia, la productividad y la satisfacción de los clientes en cuanto a servicios, ayudando así a obtener una Ventaja Competitiva; para esto se debe estar al día con respecto a las últimas tendencias y tecnologías, las cuales las indicamos en el contenido dependiendo de las necesidades de cada tipo de empresa.

INTRODUCCIÓN

El siguiente trabajo propone el diseño de una infraestructura tecnológica conjuntamente con la definición de sus políticas de uso para los usuarios, que permitan alojar aplicaciones Web de una manera totalmente segura, para esto se ha considerando tanto las infraestructuras físicas como las lógicas, y que a su vez pueda ser aplicado a cualquier tipo de empresa sin importar el tamaño de esta, simplemente adaptarlo dependiendo a sus necesidades.

Para el desarrollo de este tema también hemos tomado en consideración los factores claves de éxito como son la provisión de un sistema tecnológico de próxima generación a bajo costo, con alta eficiencia y escalable para redes multiservicio de tal manera que se pueda atender de forma efectiva los requerimientos de los clientes, gestionados no solo por una buena infraestructura sino también por un personal comprometido.

Tomado en consideración muy aparte de los posibles requerimientos de los diferentes tipos de empresa, el beneficio y la calidad del servicio brindado al cliente para que ambas partes (empresa - usuario) se sientan bien.

CONTENIDO

1. Seguridad A Nivel De Software.

La intención de contar con un sistema completamente seguro es prácticamente un imposible, de modo que el enfoque usado con mayor frecuencia en lo que a seguridad se refiere, es uno que busque el balance adecuado entre riesgo y funcionalidad. Si cada variable enviada por un usuario requiriera de dos formas de validación biométrica (como rastreo de retinas y análisis dactilar), contaríamos con un nivel extremadamente alto de confiabilidad.

También implicaría que llenar los datos de un formulario razonablemente complejo podría tomar media hora, cosa que podría incentivar a los usuarios a buscar métodos para esquivar los mecanismos de seguridad. La mejor seguridad con frecuencia es lo suficientemente razonable como para suplir los requerimientos dados sin prevenir que el usuario realice su labor de forma natural, y sin sobrecargar al autor del código con una complejidad excesiva. De hecho, algunos ataques de seguridad son simples recursos que aprovechan las vulnerabilidades de este tipo de seguridad sobrecargada, que tiende a erosionarse con el tiempo.

Una frase que vale la pena recordar: Un sistema es apenas tan bueno como el eslabón más débil de una cadena. Si todas las transacciones son registradas copiosamente basándose en la fecha/hora, ubicación, tipo de transacción, etc., pero la verificación

del usuario se realiza únicamente mediante una cookie sencilla, la validez de atar a los usuarios al registro de transacciones es mermada severamente.

Cuando realicemos pruebas, tengamos en mente que no seremos capaces de probar todas las diferentes posibilidades, incluso para las páginas más simples. Los datos de entrada que podemos esperar en nuestras aplicaciones no necesariamente tendrán relación alguna con el tipo de información que podría ingresar un empleado disgustado, un cracker con meses de tiempo entre sus manos, o un gato doméstico caminando sobre el teclado. Es por esto que es mejor observar el código desde una perspectiva lógica, para determinar en dónde podrían introducirse datos inesperados, y luego hacer un seguimiento de cómo esta información es modificada, reducida o amplificada. Internet está repleto de personas que tratan de crearse fama al romper la seguridad de su código, bloquear su sitio, publicar contenido inapropiado, y por lo demás haciendo que sus días sean más interesantes. No importa si usted administra un sitio pequeño o grande, usted es un objetivo por el simple hecho de estar en línea, por tener un servidor al cual es posible conectarse. Muchas aplicaciones de cracking no hacen distinciones por tamaños, simplemente recorren bloques masivos de direcciones IP en busca de víctimas.

2. Diseño De Red.

La seguridad en las redes se está tornando una preocupación cada vez más importante para las pequeñas y medianas empresas. Una violación interna o externa a la seguridad puede dañar gravemente las operaciones más importantes de una empresa,

afectando la productividad, poniendo en peligro la integridad de los datos, reduciendo la confianza de los clientes, interrumpiendo el flujo de ingresos y deteniendo las comunicaciones.

Este capítulo tiene el objetivo de dar enfoque modular para la definición de la seguridad de red. Sus componentes claves incluyen:

- Protección contra intrusiones para defender a la red contra ataques y uso indebido con sistemas de detección de intrusiones en tiempo real (IDS)
- Conectividad segura para empresas que dependen de la conectividad a Internet, y empleados que trabajan a distancia.
- Seguridad perimetral para controlar el acceso a las aplicaciones, servicios y datos críticos de modo que sólo los usuarios autorizados pueden atravesar la red y acceder a la información abierta para ellos.
- Administración de la seguridad para brindar a los administradores la capacidad de manejar desde dispositivos individuales hasta sistemas completos.
- Evaluar el hardware requerido, para que de una manera segura haya disponibilidad, funcionalidad, y operatividad en la red.

Sin embargo, con el avance de Internet y la generalización del uso de las redes inalámbricas, las redes de las empresas han cambiado de un modo que presenta nuevos y grandes desafíos a la seguridad. A medida que las empresas abren sus infraestructuras para admitir conectividad a Internet, trabajo remoto, movilidad inalámbrica y aplicaciones entre empresas, desaparece el perímetro de red tradicional. Las empresas han crecido tanto que desbordan los dispositivos de seguridad diseñados

para las redes heredadas y ahora son mucho más vulnerables a los ataques de hackers y otros agentes perniciosos. Un dispositivo de seguridad individual ya no resulta adecuado como protección de redes abiertas - se necesita una solución de seguridad profunda.

3. Políticas De Seguridad.

La privacidad de los usuarios de nuestro Sitio Web es de gran importancia, para esto la Empresa se debe comprometer a mantener las políticas de confidencialidad, con el objeto de proteger la privacidad de la información personal de sus usuarios, obtenida a través de sus servicios en línea.

Las políticas a establecer para el uso y mantenimiento del sitio web, deberán estar dentro de los siguientes parámetros:

- Tipo de Información que se Obtiene
- Finalidad que se le Dará a la Información
- Confidencialidad de la Información
- Modificación / Actualización de la Información Personal
- Protección de la Información Personal
- Aceptación de los Términos

CONCLUSIONES

Las preocupaciones de las empresas que basan sus operaciones sobre la plataforma del Internet buscan la manera de evitar intrusiones no autorizadas mientras los clientes están conectados, el desafío real es encontrar un equilibrio entre la facilidad de acceso y uso, y la exclusión de intrusos, sin olvidar que la seguridad perfecta no existe pero con los puntos tratados en este trabajo, podemos concluir que las principales falencias de la seguridad se basan en la mala implementación de los recursos o la subestimación de los posibles intrusos, ya que hemos demostrado con pequeños ejemplos como una programación poco concienzuda puede ser fácilmente burlada.

Los diseños de redes pueden variar mucho de una empresa a otra, a medida de que las necesidades y requerimientos lo ameriten; lo importante es tener presente el propósito del diseño a implementar, ya que una red puede estar sobredimensionada en donde los recursos no se utilicen en todo su potencial, así mismo podemos encontrar redes en las que los componentes no tengan los recursos suficientes, por este motivo hemos elaborados 3 modelos de redes, en los cuales se pueden basar para la implantación de sitios web seguros demostrando lo más claramente posible la confidencialidad y seguridad del proceso en todos los niveles. El principal factor que subyace al problema es simplemente la novedad de Internet como canal de ventas y comercialización, por lo que la seguridad será siempre una prioridad.

No obstante, el sentido común y la vigilancia evitarán prácticamente todos los ataques no autorizados, tratando de establecer límites, reglas y políticas que procuren mantener la estabilidad y seguridad en la misma, pero siempre pensando en el

crecimiento de la empresa, por esa razón es bueno disponer de un esquema de red que permita la expansión, flexibilidad y que sobretodo cumpla con requisitos tecnológicos cambiantes, actuales y a largo plazo.

Otra de las maneras de prevenir los posibles ataques o intrusiones de personas no autorizadas, es la correcta implementación de normas y políticas de seguridad; tanto para el personal como para los procesos. Pero esto de nada serviría sin una constante supervisión del cumplimiento de las mismas y tener como lema que la seguridad depende de todos.

REFERENCIAS

a) Documentación sobre el Análisis, Diseño e Implementación de un Sitio Web para pago de servicios

1. http://www.desarrolloweb.com, pp 32-50
2. http://www.microsoft.com, pp 66-72
3. http://www.cisco.com, pp 94-168
4. http://www.monografias.com, pp 180-200

b) Documentación sobre Seguridad De Redes Informáticas

1. Ing. Albert Espinal, "Tópico de Graduación – Seguridad de Redes Informáticas", (Material utilizado y estudiado durante el desarrollo del Tópico, 2004).

_____

Ing. Albert Espinal, M.S.I.G

Director de Tesis