Sistema de Gestión en Seguridad Informática como soporte a la toma de decisiones en respuesta a incidentes, basados en monitoreo de redes

[1]Ariel Armijos Guevara, [2]Luis VillamarLavayen, [3]Cindy Garcia, [4]Gustavo Galio
Facultad de Ingeniería en Electricidad y Computación
Licenciatura en sistemas de información gerencial
Escuela Superior Politécnica del Litoral
Campus Peñas Malecón 100 y Loja, Teléfono (593-4) 2 530271, Guayaquil, Ecuador
arielarmijos@hotmail.com, lvillamar@hotmail.com,cgarciam_25@hotmail.com

Resumen

NetSolution empresa especializada en el área de networking la cual brindara servicios de consultoría, implementación, capacitación y soportes de herramientas con políticas de seguridad basados en los servicios de red.

Los problemas más comunes que las empresas enfrentan y tienen a diario.
Uso de Internet no autorizado por usuarios, Internet fácil vía de infecciones por virus, Base de datos alta disponibilidad, Servidores de servicios de redes inseguras y desprotegidos, correo electrónico no deseado, correo electrónico alta disponibilidad, protección de ataques locales y remotos, en fallos o caídas de sistemas no existe herramientas de monitoreo y alertas.

La propuesta para solucionar los problemas que arriba se describen son los siguientes:

Contar con herramientas de monitoreo alertas en eventos que rompan las políticas de seguridad y continuidad del negocio, asegurar las políticas de seguridad de los accesos y restricciones en el uso de los servicios de red de los clientes y las empresas, crear políticas de acceso a internet por horarios y grupos de clientes, contar con software antivirus para los servidores para protección de la información,
Generar Reportes de Incidentes, riesgos y fallos, asegurar la disponibilidad de los servicios de red como internet, base de datos, correo electrónico de la organización..
Palabras claves:
Networking; Recurso que ayuda a grupos humanos afines a compartir servicios o información.
Internet: Es un conjunto descentralizado de redes de comunicación interconectadas.
Seguridad :En el area informática proteje la información contenida dentro y fuera de la red.
Monitoreo:Realizar controles periódicos para conocer futuros incidentes en la red.

Abstract

NetSolutioncompany specializing in the networking area which will provide consulting, implementation, training and tool holders with security policies based on network services.

The most common problems companies face and have every day. Internet use by unauthorized users, Internet easily via virus infections, high availability database, network services servers insecure and unprotected, spam, email high availability, protection of local and remote attacks, in failure or system down there monitoring tools and alerts.

The proposal to solve the problems described above are: Have monitoring tools alert on events that break the security policies and business continuity, ensuring the security policies and access restrictions on the use of network services and business customers, create Internet access policies by schedules and customer groups, have antivirus software for servers to protect information. Generate Incident Reports, risks and failures, ensuring the availability of network services such as internet, database, e-mail of the organization.
Keywords:
Networking; It's a resource that helps to human groups to share servicer or information.
Internet: It's a decentralized set of interconnected communication networks.
Security: In the informatica area protects the information contained inside or outside the network
Monitoring: Make regurarly controls to know futures incidents in the network

1. Introducción

El uso de sistemas de información y de redes electrónicas, incluida la Internet, ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia.

En el Ecuador,se ha incrementado el número de empresas que utilizan sistemas computacionales, correo corporativo, así como también el uso de servidores(web, de base de datos, etc), donde día a día se logra ver el esfuerzo constante por brindar accesos seguros y confiables a la información.

Después de haber realizado estudios como la observación directa a algunas empresas como Comerciales Hidromecanica, Chiriboga y Jara,Romero y Reyes,Seguros Hispana de Seguros, Bolivar, SulAmerica, Salud Hospitales Kennedy.
Se puede determinar que las empresas no tiene sistemas o herramientas de seguridad robustas que le permitan monitorear y gestionar de manera rápida y oportuna cuando estas reciban ataques por agentes externos que buscar llevarse información valiosa de la empresa.

Sobre las redes de comunicación informáticas en la pequeña y mediana empresas ecuatorianas, mediante visitas efectuadas a empresas (comerciales ,Hidromecanicas, Hospitales, Empresas del sector Publico,etc.),se detectaron una serie de problemas que con frecuencia se presentan y muchas veces son ignorados, descuidados o no planificados en la infraestructura de red por los administradores de los sistemas IT.

2. Producto y Mercado

Las tecnologías de seguridad de redes, ha tomado un gran auge en las empresas, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles en la actualidad.

La pequeña y mediana empresas por lo general no prestan o toman las medidas necesariaspara proteger su red de ataques externos que buscan robar información valiosas de la organización. [1]
En algunos casos podrían suponerpérdidas económicas importantes para la empresa.

NetSolution es una empresa de servicios especializada en el área de networking, la cual se dedica a implementar medidas de seguridad a las redes de datos de las pequeñas y medianas empresas.
Netsolution brinda los siguientes servicios. Configuración de servidores de correo electrónico, Configuración de redes Lan, Configuración de Firewall, Configuración de proxy, Administración y Monitoreo de la red.

Estrategias Utilizadas

Con el objetivo de captar las pequeñas y medianas empresas que utilizan redes informáticas en el día a día para operar, hemos planteado las siguientes estrategias.[2]

2.1 Estrategia de lanzamiento

El objetivo principal de la empresa es posicionar el producto en las empresas que usan redes informáticas

Los recursos que forman parte del plan táctico son los siguientes.

- Correo electrónico
- Brosurs
- Tarjetas de presentación
- Base de datos de clientes conocidos
- Base de datos actualizadas de medianas y pequeñas empresas
- Pagina web de la empresa

2.2 Estrategia comunicacional

El objetivo principal de nuestra estrategia comunicacional es dar a conocer la página web de la empresa www.netsolution.net con la información de la empresa y los servicios que se brinda a los clientes, así como los casos de éxito de empresas que implementaron normas de seguridad de manera exitosa.

Los recursos que forman parte del plan táctico para alcanzar esos objetivos son los siguientes.

- Internet
- Banner estacionarios
- Central telefónica
- Medios impresos

2.3 Estrategia Promocional

El principal objetivo de la estrategia promocional es captar clientes a los cuales le vamos a obsequiar vouchers para cursos de capacitación, tickets de descuentos para que lo hagan efectivo en su próxima compra, CD con información de las nuevas utilidades de la solución, así como gorras, plumas, llaveros,etc.

3. Implementación

En este capítulo vamos a tomar una empresa real, a la cual se le realizo una encuesta con la finalidad de determinar las brechas de seguridad que actualmente tiene la red de la organización.

La entrevista se la realizo al personal de tecnología de Movilway, en el mismo se pudo determinar las siguientes falencias.

1. Problema para controlar el acceso a internet a usuarios.
2. La organización no cuenta con un firewall
3. No cuentan con un sistema de monitoreo de red.
4. Antivirus con protección básica.
5. Acceso remoto a los equipos de la empresa.

El personal técnico de la organización nos levanto los siguientes requerimientos:

Reglas de acceso a los servicios.

a. Restringir el uso de Messenger en horarios de oficina 09:00 a 18:00
b. Restringir el uso de correos electrónicos Hotmail, Yahoo, Gmail, etc.
c. Restringir en el correo local que no lleguen mails de correos como Hotmail, Yahoo,Gmail.
d. Restringir páginas web cuyo contenido no es de beneficio para la organización
e. Restringir sitios de juegos, música, sociales (facebook, hi5, twitter) y descargas
f. Restringir el acceso desde equipos remotos a equipos de la organización
g. Restringir el acceso a departamentos sensibles de la organización
h. Restringir el acceso a determinados equipos Servidor de Base de Datos, Servidor de aplicaciones, Servidor de correo.
i. Restringir el ancho de banda a determinados equipos

Crear la siguiente regla para bloquear todos los sitios de internet a excepto de los siguientes dominios que son de interés para el trabajo.

a. www.sri.gov.ec
b. www.bp.fin.ec
c. www.bolivariano.com
d. www.bancoguayaquil.com
e. www.pichincha.com
f. www.iess.gov.ec

3.1 Implementación de zentyal

Para cubrir con todos los requerimientos de la organización, se instalara los siguientes módulos que permite gestionar y configurarlos servicios que requieren la organización.[3]

a) Zentyal Gateway
b) ZentyalInfrastructure
c) Zentyal Office
d) Zentyal Unified Communications

Zentyal Gateway

Permite que tu red sea más fiable, optimiza el ancho de banda así como ayuda a controlar lo que entra a tu red. No pierdas más tiempo con redes ineficientes

ZentyalInfrastructure

Gestiona y optimiza el tráfico interno de tu red, incluyendo la configuración del servidor de dominio y la gestión de máquinas y de los certificados digitales.

Características Objetos de Red

Puedes elegir hasta qué nivel quieres gestionar tu red con Zentyal. Puedes cambiar la configuración de toda tu red, de un departamento o de un solo ordenador.

Servidor DNS (Domain Name System)

Puedes asignar una dirección y un nombre fijo a cada equipo de tu red para facilitar la navegación por Intranet. Es más fácil recordar erp.miempresa.es que 10.0.13.27

Servidor Web

Zentyal viene con el servidor web Apache, el servidor web utilizado por más de la mitad de los sitios web conocidos. Es una base perfecta para todas las aplicaciones de tu Intranet.

SSL (Secure Sockets Layer) Profesional

Es posible que necesites una autoridad de certificación externa con tus clientes. Pero internamente, no es necesario pagar por seguridad. Zentyal te permite crear tus propios certificados SSL y usarlos para correo electrónico o sitios webs internos.

Zentyal Office

Comparte tus recursos de oficina

Zentyal Office permite gestionar y compartir recursos de oficina, incluyendo perfiles de usuarios y grupos, ficheros, impresoras, calendarios, contactos, tareas y backup de datos.

Características de Zentyal Office
Servicio de Directorio

Tus usuarios en un sitio.Zentyal Office permite la gestión de todos tus usuarios y recursos desde un punto central. Decide quién tiene acceso y a qué datos. Zentyal se basa en estándares abiertos como LDAP así que es fácil integrarlo con otras aplicaciones y servicios.

Compartición de Ficheros e Impresoras

Es una solución, pero un repositorio para documentos compartidos es más eficiente. Puedes compartir fácilmente archivos con Zentyal y usarlos independientemente de tu sistema operativo.

Backup de Datos

El almacenamiento y la compartición centralizados de documentos pueden ser muy útiles, pero también presentan un único punto de fallo. Puedes automatizar los backups de datos para no tener que preocuparte de discos que fallan o de usuarios que borran un fichero por accidente.

ZentyalUnifiedCommunications

Zentyal servidor de comunicaciones unificadas gestiona todas tus comunicaciones, incluyendo correo electrónico, mensajería instántanea y Voz IP.

Gestión de Usuarios

Gestiona todos los usuarios y recursos desde un punto central. Ellos no tienen que recordar distintos usuarios y contraseñas para cada servicio. Además, es fácil y rápido proporcionar correo electrónico, una cuenta de IM y Voz IP a los usuarios.

Correo electrónico

Zentyal viene con una solución de correo electrónico integrado, con tecnologías antispam y antivirus. Esta característica soporta todos los estándares habituales para que puedas seguir utilizando tus clientes de correo electrónico favoritos.

Mensajería Instantánea

A veces necesitas conversaciones más fluidas. Zentyal ofrece mensajería instantánea basada en el protocolo Jabber/XMPP, así que puedes utilizar cualquiera de los clientes existentes en cualquier plataforma, incluso en los teléfonos móviles.

Voz IP

Zentyal puedes ofrecer a tus empleados su propia extensión y realizar llamadas internas y conferencias con facilidad. Con un proveedor puedes también obtener números de teléfono reales y dirigirlos a tu servidor Zentyal para hacer y recibir llamadas a un coste muy bajo.

4. Análisis Financiero

Se desarrolla el análisis financiero del proyecto de acuerdo al alcance y al mercado donde se quiere introducir el servicio, de esta manera se realiza el análisis financiero que involucra inversiones de Capital, Gastos de constitución, Gastos operativos, Flujos de Caja de cada año, Ventas estimadas por año y finalmente el retorno y la rentabilidad recibida por la inversión efectuada al principio de la operación de la empresa.

En este capítulo analizamos las proyecciones que la empresa tendría en crecimiento en los tres primeros años de operaciones, donde nos damos cuenta si es rentable o no prestar este tipo de servicios a las pequeñas y medianas empresas que tienen redes de datos.

Ingresos por ventas solución

	Año 1	**Año 2**	**Año 3**	**Total**
Pequeña Empresas	14400	18000	22000	54400
Mediana Empresas	14400	21000	27000	62400
Personas Naturales	2100	3500	5250	10850
	30900	**42500**	**54250**	**127650**

Tabla1 .Ingresos por ventas solución

Se logra visulizar en los tres años que en las medianas empresas es decir 48% de los ingresos totales, frente al 52% de ingresos repartidos en pequeñas empresas y personas naturales.

Ingresos por Soporte

	Año 1	Año 2	Año 3
Pequeña Empresas	3600	4500	5500
Mediana Empresas	2880	4200	5400
Personas Naturales	720	1200	1800
	7200	9900	12700

Tabla2 .Ingresos por Soporte

Se logra visulizaren en los tres años que en las medianas empresas tiene la representación del 43% de los ingresos totales, frente al 57% de ingresos totales repartidos en pequeñas empresas y personas naturales

Ingresos Totales

	Año 1	Año 2	Año 3
Venta Solución Tecnológica	30900	42500	54250
Soportes	7200	9900	12700
Capacitación	8750	11250	13750
Total	46850	63650	80700

Tabla3 .Ingresos por Soporte

Se logra visulizar en los tres años la venta de una solución tecnológica representa e 67% de los ingresos totales, ante el soporte representado por el 16%y la capacitación que representa el 17% de los ingresos totales.

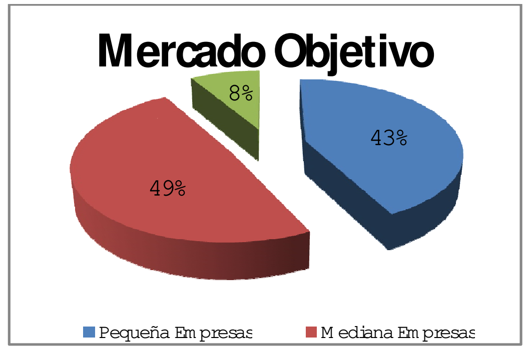

Grafico1 .Mercado Objetivo

El mercado Objetivo esta representado pot rl 49% dirigido a las medianas empresas, y el 51% dividido entre las pequeñas empresas y las personas naturales

Retorno de la inversión

Inversión Inicial	Año 1	Año 2	Año 3
-13800	4.694,84	12.008,94	36.867,30

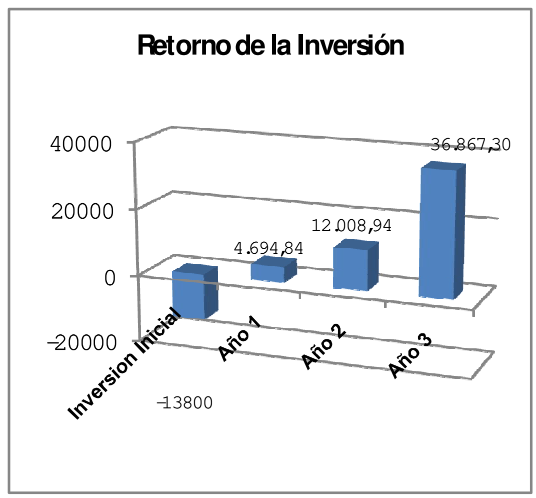

Grafico1 Retorno Inversiòn

La inversión retornna en el año 3 36.867,30, frente una inversión inicial de-13800, es decir 37% de lo invertido.

5. Conclusiones

El uso de sistemas de información y de redes electrónicas, incluida la Internet, ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia.

En el Ecuador, se ha incrementado el número de empresas que utilizan sistemas computacionales, usan correo corporativo, así como también el uso de servidores (web, de base de datos, etc.), donde día a día se logra ver el esfuerzo constante por brindar accesos seguros y confiables a la información, convirtiéndose la misma en las redes de telecomunicaciones que ha facilitado el acceso a la información desde sitios muy distantes a las organizaciones.

Las pequeñas y medianas empresas que utilizan sistemas de información conectados a redes informáticas, están expuestas a robo de información tanto de agentes externos como internos.
Por tal motivo las organizaciones están en la necesidad de tener un sistema informático protegido de estos ataques, para lo cual es una buena oportunidad de negocio brindar el servicio de seguridad basado en el monitoreo de redes.

6.Recomendaciones

Las organizaciones están en la necesidad de tener un sistema informático protegido y con un nivel de seguridad aceptable que cubra los aspectos mínimos de seguridad ante posibles ataques.
Zentyal es un servidor de código abierto y soluciones de gestión de redes, que les permite a las pequeñas y medianas empresas alcanzar un nivel de seguridad aceptable para proteger la información de la organización.
Algunos consejos necesarios para mantener un nivel se seguridad aceptable.

Actualice regularmente su sistema operativo y el software instalado en su equipo, poniendo especial atención a las actualizaciones de su navegador web. A veces, los sistemas operativos presentan fallos, que pueden ser aprovechados por delincuentes informáticos. Frecuentemente aparecen actualizaciones que solucionan dichos fallos. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, le ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.

Instale un Antivirus y actualícelo con frecuencia. Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.

Instale un Firewall o Cortafuegos con el fin de restringir accesos no autorizados de Internet. Es recomendable tener instalado en su equipo algún tipo de software anti-spyware, para evitar que se introduzcan en su equipo programas espías destinados a recopilar información confidencial sobre el usuario.

7. Bibliografía.

[1] Observación directa a las pequeñas y medianas empresas.
Información de las empresas Ecuatorianas [En Línea]
http://www.supercias.gov.ec/consultas/inicio.html
Hispana de Seguros
www.hispanadeseguros.com
Seguros Bolívar
www.seguros-bolivar.com
SulAmerica
Hospitales Kennedy
http://www.hospikennedy.med.ec/
[2]Dr. Gustavo GalioEspol.
Marketing para DesarrolladoresPdf2010
[3]Envió de mail publicitarios usando el estándar IAB ,[En Línea],
http://www.iab.org/
[4] Documentación de la solución, [En Línea],
http://www.zentyal.com/es/
[5]Documentación técnica ubuntu,[En Línea],
http://doc.ubuntu-es.org
[6] Documentación técnica de modulos de Zentyal, ZentyalInfrastructure, Zentyal Gateway, Zentyal Office,ZentyalUnifiedCommunications[En Línea]
http://doc.zentyal.org

M.Sc. Gustavo Galio
Director de Tópico
Fecha: Enero16/2011