INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 002 GTSI

"ANTI SPAM"

1. Nombre del Área

El área encargada de la evaluación técnica para la implementación de software Anti Spam es la Gerencia de Tecnologías y Sistemas de Información (GTSI) de la Contraloría General de la República.

2. Nombre y Cargo del Responsable de la Evaluación

El encargado de realizar la evaluación es el Sr. Leoncio Rodríguez Manyari, Jefe de Soporte Técnico de la Gerencia de Tecnologías y Sistemas de Información.

3. Fecha

La fecha del presente informe es el 07 de Septiembre de 2006.

4. JUSTIFICACIÓN

El Spam hoy día es un problema, se estima que el 70% del tráfico internacional de e-mail es Spam, el correo basura cuesta dinero, tanto por el tiempo que se pierde examinándolo, como por los recursos de *hardware* y *software* necesarios para manejarlo (ancho de banda, servidores de correo más potentes, software de filtrado, etc.), costes que deben ser soportados por las organizaciones (CGR) en forma de inversiones y horas de trabajo de sus empleados, y que en el caso de los proveedores de acceso a Internet, acabarán repercutiendo a los clientes.

La mayor parte del Spam que recibimos consiste en:

- Cadenas de mensajes.
- Esquemas piramidales (incluyendo las de marketing multinivel).
- Otros esquemas de "hágase rico fácilmente" o "gane plata rápidamente".
- Avisos de servicios y/o sitios pornográficos.
- Avisos de servicios de envío masivo de e-mails publicitarios (Spam).
- Avisos de software y bases de datos para hacer Spam.
- Ofertas de hosting (muchos de ellos toleran y/o hacen del Spam su negocio).
- Avisos de acciones de empresas nuevas "que van a subir hasta el cielo".

C.G.R. GERENCIA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN V°B°

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 002 GTSI

"ANTI SPAM"

- Productos milagrosos y remedios de muy dudoso efecto y origen.
- Software ilegal, películas y/o música pirateada.

El Spam está basado en el robo de servicios, el fraude y el engaño, además de la transferencia de costos de quien lo envía a quien lo recibe

Spam son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de Spam incluyen grupos de noticias usenet, motores de búsqueda, wikis y blogs. El Spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.

Consecuencias del Spam y afectados: Usuario, servidor, todos

El usuario que lo recibe:

- Pierde tiempo y dinero al descargar mensajes que no solicitó.
- Es molestado permanentemente con publicidad de cosas que no le interesan.
- Puede llegar un momento en que reciba más Spam que mensajes que realmente le interesan.

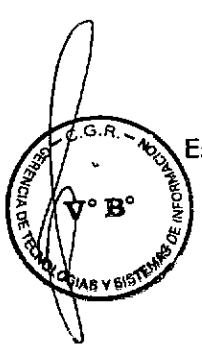
El servidor al que pertenece la empresa o persona que lo envía:

- Saturación del servidor.
- Ingreso del servidor a listas negras.

Todos los usuarios de Internet:

- Según una nota publicada en Terra "500 millones de avisos personalizados bombardean cada día las casillas de email de todo el mundo, según un estudio de la Comisión Europea. Esto significa un costo de unos 9,360 millones de dólares al año para los usuarios, en función del tiempo de conexión utilizado".

Esto nos da una idea de cómo esta práctica afecta el rendimiento de toda la red.



INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 002 GTSI

"ANTI SPAM"

5. ALTERNATIVAS

Para combatir el problema se pueden plantear distintas alternativas en función de los requisitos de ésta:

-Filtrar (se puede hacer en múltiples puntos).

-Desplegar una solución de anti-Spam basada en reglas (heurísticos)

-Desplegar una solución de anti-Spam basada en aprendizaje estadístico.

-Controlar (debe hacerse en la entrada y salida)

-Implementar gestión y control del ancho de banda (revisión periódica).

Estas alternativas pueden utilizarse de forma conjunta o separada para reducir el problema derivado del Spam.

Soluciones basadas en reglas

Una de las implementaciones iniciales de control de Spam es la introducción de sistemas basados en reglas que determinan qué es Spam y qué no lo es. Habitualmente las reglas están basadas en:

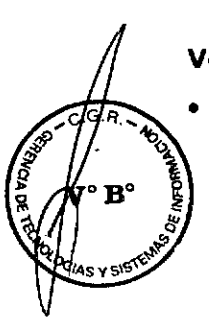
- Análisis del origen del Spam (direcciones IP o direcciones) para determinar si es lícito:
- Listas negras: Real-Time Block Lists (RBLS), DNS Block Lists (DNSBLS) y XBLs (Xploit bot lists)
- Origen del correo (validar el dominio: SPF, Yahoo! Domain Keys)
- Análisis del contenido:
    - De las cabeceras (permite rechazar antes de encolar)
    - En el cuerpo del mensaje (una vez encolado)

Básicamente, si cumple un número suficiente de las reglas se califica como Spam.

Solución basada en reglas

Ventajas

- La tasa de falsos positivos es relativamente baja (aunque no cero)



- Pueden adaptarse manualmente al Spam recibido.

Desventajas

- Las reglas deben actualizarse de forma periódica.
- Los Spammers siempre intentarán saltárselas.
- Los bloqueos con RBLS pueden bloquear sistemas legítimos (pero mal configurados) ¿quién los gestiona?

Soluciones basadas en aprendizaje estadístico

Para solventar algunas de las desventajas de los sistemas basados en reglas fijas se han diseñado sistemas basados en aprendizaje estadístico:

- Habitualmente basados en filtros bayesianos.
- Generan reglas basadas en mensajes previamente clasificados como Spam.
- Aplican probabilidades para determinar si un mensaje es o no Spam.
- Son muy fáciles de implementar en los MUAs y se están incluyendo de "serie" en muchos clientes de correo (Mozilla Thunderbird, Outlook, etc..)

Ventajas

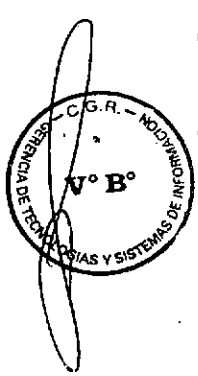
- Permite una adaptabilidad mayor al Spam que recibe la organización.
- Puede detectar características "no evidentes" en el Spam.
- Puede detectar Spam para el que no exista una regla definida.
- La adaptación de los filtros puede hacerse de forma automática y sin intervención.

Desventajas

- Se deben alimentar con una "buena" fuente de Spam.
- Habitualmente tienen sólo en cuenta el contenido de los mensajes.
- Puede ser difícil generar reglas para mensajes basados en contenido no analizable (imágenes embedidas, JavaScript...)
- También es posible contaminarlas.

Gestión del ancho de banda

En último término el Spam es un problema que consume recursos (spool de disco, comunicaciones, etc.) y, aunque se corte en la pasarela un Spammer puede



colapsar la organización consumiendo todos sus recursos. La única solución en este escenario es introducir sistemas de gestión de ancho de banda:

- Priorizar las comunicaciones de los servidores de correo de la organización con otros "habituales".
- Controlar el tráfico de correo y detectar fácilmente un consumo excesivo de recursos.
- Dos posibilidades: sistema genérico de gestión o throttling de correo.

Ventajas

- Permite controlar en tiempo real el consumo de recursos y actuar en consecuencia.
- Puede utilizarse para gestionar otros servicios.
- Permite identificar rápidamente los servidores con los que la organización se comunica habitualmente (proveedores de servicio)
- Puede ralentizar los ataques y evitar así el consumo de recursos

Desventajas

- La revisión del consumo debe ser permanente, aunque se pueden definir políticas.
- Se trata de un recurso más orientado a la gestión de comunicaciones que a la gestión del servicio (distintas personas).

6. ANALISIS COMPARATIVO TÉCNICO Y DE COSTO-BENEFICIO

Para realizar este análisis comparativo técnico, se eligieron los siguientes productos, todo ellos líderes en su área:

Sistema de protección de correo electrónico Anti-Spam:

- Symantec Mail Security
- InterScan Messaging Security suite

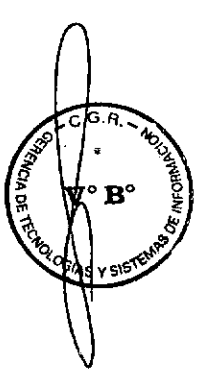
INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 002 GTSI

"ANTI SPAM"

Así, se han evaluado las características técnicas de los productos mencionados, cada uno de los cuales es de fácil implementación, uso y mantenimiento, no siendo necesario realizar modificaciones o cambios en la plataforma actualmente en uso. Los productos evaluados cumplen las especificaciones técnicas que se detallan a continuación:

CARACTERÍSTICAS

- Appliance antiSpam.
- Debe detectar y bloquear de ataques a nivel de SMTP (ataques de Directorio, Ataques de virus, ataques de SPAM) y Phising.
- Capacidad para crear reglas diferenciadas para el tráfico entrante o el saliente.
- Debe usar tecnologías heurísticas para la detección de SPAM.
- Actualización de filtros heurísticas anti-Spam automáticamente.
- Debe contener filtros de reputación actualizables. (listas negras, proxys que permiten relay, listas seguras y dominios confiables)
- Debe tener Bases de Datos de URLs que generalmente vienen en correos SPAM.
- Debe tener Integración con Service Policy Framwork (SPF)
- Capacidad para detectar el idioma del correo (7 idiomas como mínimo) y reconocer el tipo de Spam en basera esto.
- Capacidad para elegir los idiomas en que los correos están permitidos de ingresar a la red.
- Creación de Políticas independientes por dominio, por usuario o por grupo.
- Eliminación automática de correos infectados con gusanos.
- El software debe permitir bloquear servidores, direcciones IP y dominios de correos Spammers y permitir al administrador bloquear correos según el nombre de dominio.
- Opciones de creación de reglas de filtrado de contenido por: destinatario, remitente, copia de carbón, encabezados del correo, cuerpo, tamaño, cabecera MIME.
- El producto debe tener cuarentena web para poder almacenar SPAM o MENSAJES SOSPECHOSOS



INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 002 GTSI

"ANTI SPAM"

- Integración con LDAP (Directorio Activo)
- Notificaciones automáticas a los usuarios indicando los correos Spam que tiene almacenados en la cuarentena y la posibilidad de que ellos mismos los liberen.
- Uso de DISCLAIMERS personalizables por el usuario.
- Opciones de configuración ANTI-RELAY
- Interfaz de administración tipo Web (HTTPS)
- Alertas personalizadas ante diferentes tipos de eventos.
- Distintos tipos permisos para administradores.
- Uso de diccionarios para la búsqueda de palabras o frases en el todo el contenido correo.
- Múltiples opciones de respuesta como: eliminar adjunto, eliminar el mensaje, entregar normalmente, enviar a cuarentena, reenviar el mensaje a otra cuenta, enviar el mensaje al destinatario con copia a otra cuenta, archivar el correo en el disco duro, enviar el mensaje a la carpeta SPAM del cliente, agregar etiquetas en la línea asunto, etc.
- Reportes estadísticos por virus, Spam, ataques, filtrado de contenido, teniendo la posibilidad de personalizar el rango de tiempo en el cual se necesita obtener el reporte, pudiendo agrupar los eventos por horas, días, semanas, meses.
- Generación automática de reportes de Spam/virus y envío automático a cuentas preconfiguradas.
- Actualización de los componentes del producto previa notificación a los administradores.
- Opción para realizar backup y restore de todas las opciones de configuración.
- Características de Hardware:
    - Rack
    - Mínimo 2 x 73 GB de Disco Duro.
    - 2 Interfaces de Red (una para trafico entrante y otra para trafico saliente)
    - Redundancia de ventiladores y fuente de poder.
    - Numero de usuarios soportados como mínimos: 1000

C.G.R. – GERENCIA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN – V° B°

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 002 GTSI

"ANTI SPAM"

CONSIDERACIONES:

- El proveedor deberá acreditar ser representante de la solución ofertada y de estar en condiciones de dar mantenimiento y reparar el equipo ofertado y tener el personal técnico para ello.
- El proveedor deberá acreditar haber vendido una solución en por lo menos cinco (05) entidades del producto ofertado en magnitud similar en el último año.
- Contar con personal certificado en el producto: mínimo 2 personas
- Todas las funcionalidades solicitadas deben ser demostradas en su propuesta técnica a base de manuales del producto. No se aceptará justificaciones a base de cartas o declaraciones juradas.
- Garantía de fábrica para la solución, y garantía de buen funcionamiento de la solución instalada por el período mínimo de 01 año.
- Despliegue de la solución, actualización libre de las versiones de software de la solución adquirida que se liberen durante el período de garantía.
- Número de usuarios 1,000.
- El postor deberá considerar en su propuesta la instalación y configuración del equipo, para lo cual deberá prever todo lo necesario para ello (accesorios, cables, etc.).

Licenciamiento

Las licencias, soporte y mantenimiento será como mínimo de un año y los precios referenciales son los siguientes:

- InterScan Messaging Security $ 32,688.00
- Symantec Premium Anti-Spam $ 21,857.92

El impacto sobre la plataforma será imperceptible y los beneficios se lograrán reduciendo el ancho de banda, la pérdida de tiempo al recibir correos no deseados y la reducción del la saturación del Servidor de Correo Electrónico Lotus Domino.

7. CONCLUSIONES

GERENCIA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN – G.G.R. – V° B°

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 002 GTSI

"ANTI SPAM"

Las conclusiones de la evaluación realizada son las siguientes:

- La CGR obtendrá mayor calidad en el nivel de servicio de los recursos de red, al reducir el ancho de banda y los equipos ocupados por correos no deseados y el uso incorrecto de las herramientas Internet.

- Los servicios ofrecidos por los sistemas de la CGR son críticos y de alta importancia para las labores diarias de los usuarios, por lo que se requiere contar con una plataforma de seguridad acorde con las tecnologías y amenazas actuales existentes, que asegure a su vez el correcto funcionamiento de los sistemas institucionales.

- Por las razones expuestas anteriormente, se recomiendan adquirir e implementar las soluciones propuestas a fin de mejorar el nivel de seguridad de la información de la institución.

8. Firmas

C.G.R. – GERENCIA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN
V° B°

Jesús León Lamas
Gerente
Gerencia de Tecnologías y Sistemas de Información

Leoncio Rodríguez Manyari
Jefe Soporte Técnico
Gerencia de Tecnologías y Sistemas de Información