Nuevos enfoques para las infraestructuras de correo electrónico

Modelo de infraestructura común para el Servicio de correo electrónico en la comunidad RedIRIS

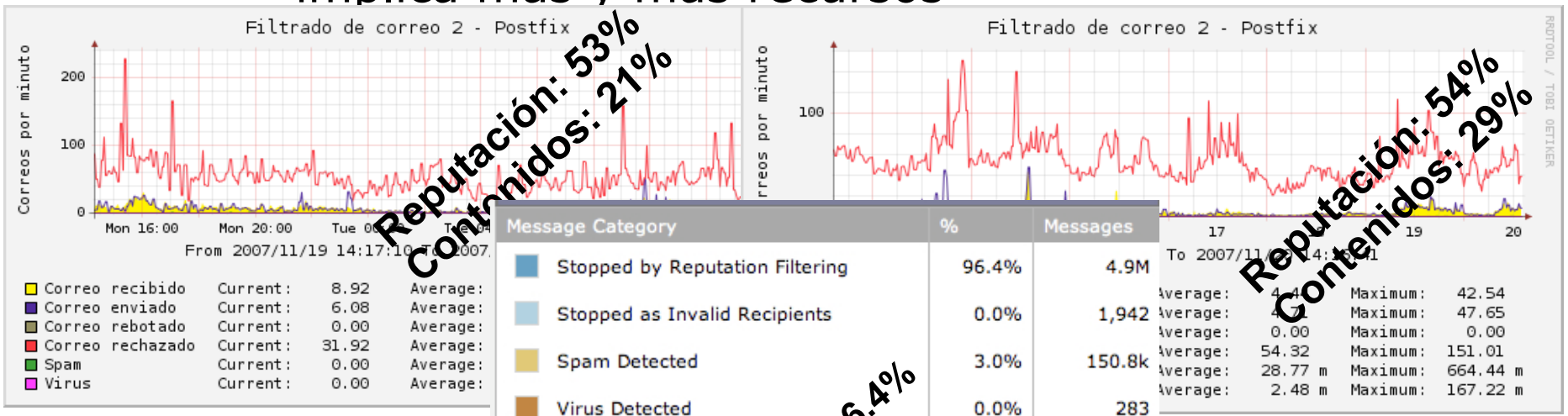
Alcalá de Henares, 17 Noviembre

Situación actual (1)

- Actualmente los servicios de correo electrónico:
  - Son infraestructura crítica
  - Requieren muchos recursos para su mantenimiento:
    - Actualizaciones y reconfiguraciones de software
    - Aumento de recursos hardware
    - Reconfiguración de nuevos tecnologías, plugins etc
    - Licencias de Antivirus y/o Antispam
  - El correo electrónico es una tecnología estable cuya gestión y recursos continua incrementándose
  - Usurpa recursos para mejorar o implementar nuevos servicios

Situación actual (2)

- A pesar de los esfuerzos los resultados no son los esperados, por lo que…
  - Los usuarios migran a soluciones externas
  - Siguen aumentando los niveles de spam lo que implica mas y mas recursos



Message Category	%	Messages
Stopped by Reputation Filtering	96.4%	4.9M
Stopped as Invalid Recipients	0.0%	1,942
Spam Detected	3.0%	150.8k
Virus Detected	0.0%	283
Stopped by Content Filter	0.0%	0
Total Threat Messages:	**99.4%**	**5.0M**
Clean Messages	0.6%	28.2k
Total Attempted Messages:		**5.0M**

Reputación: 96.4%
Contenidos: 3%

Situación actual (y3)

- Los porcentajes de spam bloqueado en el primer nivel de protección son espectaculares: 60-90%
- Según previsiones lejos de mejorar la situación empeorará

- Se destinan recursos para:
  - Bloquear cantidades enormes de basura
  - Buscar algunos mensajes buenos entre la basura

- No se destinan recursos para:
  - Mejorar las interfaces Webmail y servicios de valor añadido
  - Aumentar el almacenamiento en buzones
  - Dispositivos móviles

Estrategia

- 1ª Fase "La Idea" Mayo 2008 (Valencia)
  - Se presentó la idea en bruto
  - Idea no rechazada
  - Debate positivos

- 2ª Fase "La propuesta" Noviembre 2008 (Alcalá)
  - Se presenta una propuesta mas concreta
  - Se debate...

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

Modelo de infraestructura común para el Servicio de correo electrónico en la comunidad RedIRIS

2º Asalto "La Propuesta"

Alcalá de Henares, 17 Noviembre

RedIRIS

Modelo de infraestructura común para el Servicio de correo electrónico en la comunidad RedIRIS

Objetivos

Alcalá de Henares, 17 Noviembre

Objetivos de La Propuesta

- Ambiciosos y trasgresores
- Desplegar una plataforma que recoja el correo de todas las instituciones RedIRIS que lo soliciten
- Una plataforma común, distribuida por la comunidad y una única gestión
- Actuar como MX principal

Modelo de infraestructura común para el Servicio de correo electrónico en la comunidad RedIRIS

Ventajas

Alcalá de Henares, 17 Noviembre

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

Universidad de Alcalá

Ventajas de La Propuesta (1)

- Reducir en las instituciones los recursos necesarios para frenar el spam
- Mejorar la efectividad de las medidas anti-spam
- Ofrecer un modelo viable:
  - Económico
  - Gestión
  - operación

Ventajas de La Propuesta (2)

- Disponer de políticas comunes en RedIRIS para:
  - Presentar una línea única y coherente de actuación frente al spam
  - Mejorar y simplificar el soporte
  - Mejorar la experiencia del usuario final ante incidencias relativas al filtrado de mensajes.
  - Ajustar los requisitos a los requerimientos de las instituciones

Ventajas de La Propuesta (y 3)

- Definir un plataforma tecnológica avanzada cuya definición y experiencia sería pionera en Europa

- Establecer colaboración tecnológica con la industria española del sector

Modelo de infraestructura común para el Servicio de correo electrónico en la comunidad RedIRIS

Requisitos

Alcalá de Henares, 17 Noviembre

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

Universidad de Alcalá

Requisitos de La Propuesta (1)

- Ubicado en las instalaciones de RedIRIS
- Hardware necesario para soportar gran carga de conexiones SMTP y tiempos de respuesta eficientes
- Módulos de reputación eficientes
- Módulos de análisis de contenidos (opcional)
- Interface de gestión para cada institución.

Requisitos de La Propuesta (2)

- Que la plataforma sea igual o mas efectiva que las individuales
- Soporte a *postmaster*
- Debe implicar una disminución de recursos económicos, hardware y software por parte de las instituciones así como una mejora de la efectividad

Requisitos de La Propuesta (y3)

- Escalable hacia un modelo distribuido
- Integración y desarrollo por parte de alguna empresa
- Que sea viable económicamente

Modelo de infraestructura común para el Servicio de correo electrónico en la comunidad RedIRIS

Propuesta

Alcalá de Henares, 17 Noviembre

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

Universidad de Alcalá

Modelo

- Modelo basado en tres niveles de Servicio
  - Nivel 1. Filtros de Reputación gratuito
  - Nivel 2. Filtros de Contenidos facturado
  - Nivel 3. Almacenamiento facturado

Internet

Servicio

Nivel 1

Nivel 2

Nivel 3

Panel de control

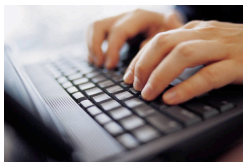
100%

Conexiones SMTP : reputación

IRISRBL | Greylist | SPF | Listas Blancas

20%

Institución A



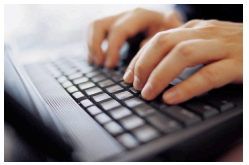
Análisis contenidos

AntiVirus

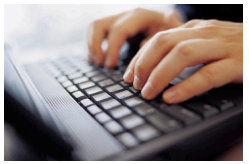
AntiSpam: Bogofilter + Spamassassin

15%

Institución B



Almacén y cuarentena



MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

Universidad de Alcalá

- ¿Qué ofrecería?
  1. Gestión de flujos SMTP
  2. Análisis de reputación IP basado en:
     - Listas negras, blancas y grises
     - Chequeos SPF, DKIM
  3. Panel de control vía web:
     - Logs, estadísticas, configuración(bloqueo,marcado)
  4. Personalización de chequeos
  5. Soporte a *postmaster*
  6. Chequeo de usuarios vía LDAP u otro
  7. Almacenamiento en caída del servidor destino
  8. Cobertura de política homogénea: acciones, errores tamaño mensaje etc

Servicio de Nivel 2

- ¿Que ofrecería?
  1. Todas las del Nivel 1 (SMTP)
  2. Escaneo de contenido de mensajes con varias sistemas Antivirus y AntiSpam
  3. Bloqueo y macado de mensajes
  4. Nunca cuarentena (almacenamiento)
  5. Soporte a cargo de la empresa

  - Servicio facturado por el socio tecnológico

Servicio de Nivel 3

- ¿Qué ofrecería?
  1. Los de Nivel 1 (SMTP) y Nivel 2 (contenidos)
  2. Almacenamiento de buzones
  3. Interface de acceso al correo (Webmail)
  4. Soporte a cargo de la empresa

  - Servicio facturado por el socio tecnológico

Modelo de infraestructura común para el Servicio de correo electrónico en la comunidad RedIRIS

¿Ahora qué?

Alcalá de Henares, 17 Noviembre

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

Universidad de Alcalá

Acciones

- Debatir propuesta

- Caso afirmativo: Fase 3ª
  - Seleccionar socio tecnológico
  - Montar un plataforma piloto para probar

¿Opiniones? ¿dudas?

Actualidad IRIS-MAIL

Servicio IRISRBL
Phishing en RedIRIS

Alcalá de Henares, 17 Noviembre

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
red.es
Universidad de Alcalá

Servicio IRISRBL

- 50 instituciones
- 15millones de consultas diarias
- Efectividad total media: 75%
- 1 falso positivo por semana
- Solución instantánea

- +info: http://www.rediris.es/irisrbl/

¿Opiniones? ¿dudas?

- **Características**

  - Sucesivas avalanchas de spam/Phishing:
  - Se envían desde una sola IP
  - Utilizan el mismo contenido de mensajes
  - Enviado a unos cientos de usuarios
  - Responden (pican) unos pocos usuarios, pero es suficiente

- **Problemas sobre la infraestructura de Webmail**
  - Se conectan desde IP externas a nuestro webmail a través de las cuentas capturadas para distribuir spam
  - En algunos casos se detectó el problema de forma precoz gracias a una alarma del incremento de mensajes salientes

- **Problema del spam saliente**.
  - Servidores salientes colapsados
  - Servidores de salida de la institución entra en ListasNegras de Hotmail o genéricas

Soluciones

- **Cuando se detecta el phishing**
  - Bloquear la entrada de ese tipo de mensajes
  - Activar filtros para el correo procedente de las direcciones desde las que se realizaron los ataques.
  - Avisar a las direcciones abuse@ de los dominios que han enviado el Phishing
  - Chequear el número de mensajes enviados por usuarios autenticados. Alertas de tráfico anómalo

- **Cuando se detecta el phishing**
  - Cambiar contraseñas de todos los usuarios
  - Aviso masivo a toda Universidad
  - Incluir un captcha en la autenticación de los webmail para evitar el ataque automático

- **Problema del correo saliente**
  - Retener 2 días el correo hacia Internet para su revisión
  - Buscar patrón y limpiar colas
  - Bloquear la salida de los usuarios que han picado
  - Bloquear la dirección a la que se envían las credenciales
    - Avisar a las direcciones abuse@ de los ISP de esas direcciones

- **Problema del correo saliente**
  - Revisar las políticas y seguridad de salida del correo especialmente desde el servidor de Webmail:
    - Limpiar colas del relay de salida
    - Los mensajes de Webmail se encolan para revisión
    - Reducir temporalmente el numero máximo de destinatarios
    - Activar filtro de contenidos en el correo de salida

- **Problema del correo saliente**
  - Disponer de un sistema de alertas de flujos anormales de salida (indican en un periodo de tiempo definido el numero de mensajes por IP, destinos enviados)
  - Análisis continuo de los ficheros de Logs
  - Reconfigurar el servidor para impedir que el correo saliente tenga una dirección diferente del dominio de nuestra universidad

- **Ataque al Webmail para distribuir spam**
  - Crear una relación de rangos de bloqueo via Web. ListasNegras para web.
  - Bloquear en el router de la Universidad las IP desde las que se están conectando al Webmail
  - Cambiar claves de los usuarios que picaron