Caso de Éxito

Usuario/Cliente: **Universitat de Barcelona**
Apoyado por: **Iron Port**

SOLUCIÓN AVANZADA PARA TRATAR EL CORREO NO DESEADO EN LA UB

INTRODUCCION

La Universidad de Barcelona, como otras tantas organizaciones de nuestro país, no es ajena al problema de la recepción de volúmenes crecientes de correo no solicitado (Spam) y al coste cada vez mayor que supone poder extraer de forma eficiente y efectiva el correo lícito para poder entregarlo, sin acumular importantes retrasos, a los destinatarios de los mensajes. El volumen de correo no deseado ha crecido de forma espectacular en los últimos años lo que significa que hay que procesar cada vez mayor cantidad de correo para acabar extrayendo una proporción cada vez menor de correo legítimo. En la actualidad el 95% del correo corresponde a correo no deseado y tan solo el 5% a correo legítimo. No resulta difícil imaginar el aumento de carga que ello ha supuesto para la pasarela de correo existente. La solución convencional a este problema pasa por incrementar los anchos de banda, aumentar la capacidad de proceso de las pasarelas, aumentar el espacio de almacenamiento y aumentar la dedicación, en este caso de los usuarios, a repasar su carpeta de correos clasificados como Spam. Esta solución se convierte en insostenible cuando el volumen de correo no deseado sigue creciendo de forma incontrolada. Es necesario recurrir a soluciones que de algún modo sean capaces de detener la mayor parte del correo no deseado en origen. El gran reto es hacerlo sin crear el efecto contrario; el de los falsos positivos.

PRINCIPALES SOCIOS TECNOLÓGICOS

Para resolver el problema del correo no deseado, la Universidad ha apostado por la tecnología de Ironport de la mano del integrador Ingelan.
Ingelan lleva tres años trabajando con Ironport en España y ha acometido con éxito un importante número de proyectos en empresas de sectores muy diversos. La problemática en todos los casos, la misma; mejorar la eficiencia y la eficacia en el tratamiento del correo no deseado. En algunos sectores como el Financiero, objetivo continuado de ataques de phishing y de las consecuencias de este tipo de ataques (DoS), también han tenido su peso otros factores tecnológicos que forman parte de las soluciones de Ironport.,

PROBLEMÁTICA A RESOLVER

Tal como se ha indicado en la introducción el reto de la Universidad era el de dotarse de una solución que le permitiera atajar el problema del correo no deseado con un enfoque distinto del utilizado hasta entonces. Dotarse de más infraestructura y recursos solo serviría para resolver momentáneamente una parte del problema y convertirlo con el tiempo en un problema de mayor envergadura y más difícil de gestionar. Con el paso del tiempo la solución existente se había convertido en algo inmanejable, poco eficiente, el tiempo de entrega de un correo podía alcanzar las 2 horas, y la eficacia/exactitud de la solución había dejado de ser la que fue en el momento de su implantación.

Hasta el momento se ha hecho referencia al volumen creciente de correo, como principal causa del problema, pero este también ha venido acompañado de importantes avances en las soluciones y tecnologías utilizadas por los 'spamers' para conseguir burlar las soluciones Antispam basadas en el análisis de la construcción y el contenido de los mensajes recibidos. Ejemplo de ello han sido las epidemias de spam gráfico que se iniciaron en el 2006 y perduran hasta hoy, la capacidad de proceso necesaria para detectar spam gráfico es muy superior a la necesaria para realizar un análisis textual, en definitiva, otro factor que sirve para poner de manifiesto la no viabilidad de la aproximación clásica.

En el escenario descrito resulta indispensable pensar en una solución capaz de contener el problema en origen de forma que ya no se dependa de la infraestructura y recursos disponibles en destino para atajar el problema, y la única forma de hacerlo es en base a la reputación de quién intenta enviar el correo. De igual forma que se valida la reputación de una tarjeta de crédito antes de completar una transacción y si la tarjeta de crédito está en una lista negra se deniega la transacción, en el caso del correo se acepta o rechaza el correo en función de la reputación del origen del mismo. Si bien esta aproximación no es en si novedosa, de hecho hace mucho que existe el concepto de lista negra (RBL, RBL+, ...), y hace tiempo que muchos fabricantes de productos de Antispam han incorporado el concepto de reputación a sus soluciones, la forma de funcionar de estas soluciones, muy efectivas en el bloqueo, pero con un comportamiento binario, si estás en una lista negra rechazo tu correo y en caso contrario lo acepto, ha sido una fuente de falsos positivos tal que han convertido la solución en un problema mayor que el propio problema a resolver.

Con estos antecedentes cuando menos uno se cuestiona la efectividad de una solución basada en reputación.

DETALLE DE LA SOLUCION:

(Tecnologías, Arquitecturas, Base Tecnológica)
Sensible al problema la Universidad evaluó las soluciones disponibles en el mercado y decidió confiar en la solución que le proponía Ingelan utilizando tecnología de Ironport. La solución de Ironport está basada en una plataforma tecnológica (MTA) pensada y diseñada para afrontar con éxito todos los retos que plantea la utilización del correo electrónico en el contexto actual. Son muchas las soluciones incorporadas en la plataforma tanto desde el punto de vista de la efectividad y eficiencia, en el tratamiento del Spam, como desde el punto de vista de la protección frente a otro tipo de amenazas como los Directory Harvest Attacks, ataques de negación de Servicio DoS, ataques de phishing etc... , pero lo que en este caso concreto fue el aspecto más valorado de la solución fue la tecnología de Reputación de Ironport. La Reputación de Ironport se basa en un modelo matemático que computa un elevado número de parametros de comportamiento de las IPs de origen de un correo: aspectos como el tiempo que hace que una IP envía correo en Internet, los volúmenes de correo, las variaciones de estos volúmenes, si la IP es estática o dinámica, si la IP está en una o varias listas negras, etc son parámetros que influyen en que una IP tenga una reputación positiva o negativa pero ninguno de ellos es, en si mismo, determinante como ocurre con los sistemas basados en listas negras. El valor de la reputación es un número comprendido entre -10 y +10, cuanto más negativo peor es la reputación y menor la probabilidad de que alguien envíe un correo lícito desde ese origen. El segundo aspecto diferencial de la tecnología de reputación de Ironport es la forma en que se determina el punto de corte porque al final será necesario establecer dónde se sitúa la frontera entre los orígenes desde los que se va a aceptar correo y los orígenes de los que no. Situar la línea de separación en un punto u otro implicará tener mayor efectividad a costa de mayor número de falsos positivos o menor efectividad con menor número de falsos positivos. El corte en Ironport no es una línea sino una franja, llamada zona gris en la que el objetivo que se persigue es doble; no perder ni un solo correo legítimo enviado desde una IP de reputación dudosa y evitar que desde una de estas IPs se pueda bombardear indiscriminadamente con correo ilegítimo. El mecanismo utilizado para conseguir este doble objetivo es el de limitar el número de correos que se aceptan desde dicha IP durante una hora.

Además de la reputación la plataforma valida los recipientes de correo contra diversos servidores LDAP, descartando el correo dirigido a usuarios que no existen, y aplica una segunda capa de seguridad reactiva basada en el Antispam de Ironport y un Antivirus convencional.
La solución implantada en la Universidad de Barcelona se compone de dos equipos Ironport C350, en configuración de alta disponibilidad. La alta disponibilidad se consigue mediante la utilización de una pareja de balanceadores de red. Los Ironport C350 están configurados para implementar las funcionalidades de Reputación, validación LDAP, Antispam y Antivirus descritas, además de otras funciones de control y de seguridad como la protección frente a ataques de DoS o DHA (Directory Harvest Attacks).

CONCLUSIONES

La experiencia próxima al año de utilización de la tecnología seleccionada ha resultado ser un éxito absoluto. La tecnología de Ironport ha estado a la altura de las expectativas generadas, la Reputación se ha mostrado tremendamente efectiva con cero falsos positivos, y la experiencia aportada por Ingelan en la implantación de este tipo de soluciones ha sido clave para alcanzar los resultados deseados desde el primer momento en el que los Ironport C350 empezaron a recibir el correo dirigido a los dominios de la Universidad de Barcelona.

El gráfico que sigue muestra la pantalla principal de monitorización de la entrada de correo con los resultados del último mes, los datos hablan por si solos.

Incoming Mail Summary

Message Category	%	Messages
Stopped by Reputation Filtering	91.9%	22.4M
Stopped as Invalid Recipients	0.0%	1,530
Spam Detected	2.2%	532.3k
Virus Detected	0.0%	1,120
Stopped by Content Filter	0.0%	0
Total Threat Messages:	**94.1%**	**22.9M**
Clean Messages	5.9%	1.4M
Total Attempted Messages:		**24.3M**