(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 558 740**

(51) Int. CI.:

H04L 12/58 (2006.01)
G06Q 10/06 (2012.01)
G06Q 10/10 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.02.2007 E 07004097 (7)**

(97) Fecha y número de publicación de la concesión europea: **07.10.2015 EP 1965547**

(54) Título: **Sistema implementado en ordenador y procedimiento para detectar el uso indebido de una infraestructura de correo electrónico en una red informática**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.02.2016

(73) Titular/es:

STRATO AG (100.0%)
Pascalstr. 10
10587 Berlin, DE

(72) Inventor/es:

BICKEL, STEFFEN DIPL.-WIRTSCHAFTSINFORM.;
HAIDER, PETER DIPL.-INFORM.;
SCHEFFER, TOBIAS PROF. DR. y
WIENHOLTZ, RENE

(74) Agente/Representante:

TORNER LASALLE, Elisabet

DESCRIPCIÓN

Sistema implementado en ordenador y procedimiento para detectar el uso indebido de una infraestructura de correo electrónico en una red informática.

La presente invención versa acerca de técnicas para detectar el uso indebido de una infraestructura de correo electrónico en una red informática.

Antecedentes de la invención

Los servicios comerciales que proporcionan ancho de banda de Internet y recursos de cálculo son usados indebidamente con frecuencia por atacantes para enviar grandes cantidades de correo electrónico masivo no solicitado. Por ejemplo, una tienda de Internet que resida bien en servidores del operador o bien en servidores proporcionados por un tercero expone a Internet secuencias de ejecución. Estas secuencias de ejecución son accesibles en conexiones de HTTP que tienen capacidad de enviar automáticamente correos electrónicos, a menudo a destinatarios predefinidos —por ejemplo, a un cliente de la tienda— para entrar en contacto con el operador. Dado que muchos de esas secuencias de ejecución son propensas a contener agujeros de seguridad y, de hecho, son frecuentemente vulnerables, los atacantes pueden hacer un uso indebido de ellas para enviar correos electrónicos masivos a destinatarios de su elección, con contenido arbitrario y en cantidades que tienen como resultado graves consecuencias para el operador del sitio con el programa vulnerable de ejecución y/o el proveedor de la infraestructura de correo electrónico. En primer lugar, se consumen los recursos de cálculo y el ancho de banda, lo que causa costes. En segundo lugar, la sobrecarga de las transmisiones de correo electrónico puede interrumpir la operación regular de la página Web y tener como resultado, por ejemplo, una pérdida de ingresos para el operador. En tercer lugar, es probable que los destinatarios de los correos electrónicos no solicitados denuncien los servidores remitentes a sus proveedores de servicio de correo electrónico y/o a organismos independientes de control de correo basura. Esto tiene como resultado, frecuentemente, que las direcciones de IP de los servidores remitentes sean bloqueadas respectivamente por otros proveedores de servicio de correo electrónico, con el resultado de que los correos electrónicos legítimos enviados desde el anfitrión atacado dejen de llegar a sus destinatarios.

Los anteriores enfoques para evitar tal envío masivo de salida de correos electrónicos basura comprenden sobre todo una pasarela separada para los correos electrónicos de salida, que filtra todo el tráfico de correo electrónico de salida y bloquea los correos electrónicos que se considera que son de uso indebido. Hay varias desventajas en este enfoque. En primer lugar, surgen problemas legales cuando se bloquean o borran correos electrónicos de salida, especialmente cuando el correo electrónico se origina en una cuenta de usuario que pertenece a un tercero. En segundo lugar, no hay forma de proporcionar información de retorno a la secuencia de ejecución vulnerable de origen, dado que en el punto de filtrado se pierde toda la información acerca de la secuencia de ejecución de origen. Esto también está relacionado con la tercera desventaja, que es la falta de información adicional para clasificar los correos electrónicos de salida, tal como el nombre y parámetros de la secuencia de ejecución de inicio.

En el documento US 7.054.907 B1 se dan a conocer sistemas y procedimientos para bloquear la entrega de una comunicación electrónica. En una realización, un procedimiento incluye la recepción de al menos una porción de una primera comunicación electrónica que incluye una primera dirección remitente de la comunicación electrónica y una primera dirección del destinatario de la comunicación electrónica. Se accede a los datos del perfil de bloqueo de comunicación electrónica de usuarios, incluyendo los datos del perfil de bloqueo de comunicación electrónica de usuarios una pluralidad de registros de bloqueo de la comunicación electrónica de usuarios. Cada registro de bloqueo de la comunicación electrónica de usuarios de al menos un subconjunto de la pluralidad de registros de bloqueo de la comunicación electrónica de usuarios incluye un campo identificador del destinatario para almacenar un identificador del destinatario y un campo identificador del remitente para almacenar un identificador del remitente. Se selecciona un primer registro de bloqueo de la comunicación electrónica de usuarios en función de, al menos en parte, la primera dirección remitente de la comunicación electrónica y la primera dirección del destinatario de la comunicación electrónica. Se bloquea la entrega de la primera comunicación electrónica a la primera dirección del destinatario de comunicación electrónica en función, al menos en parte, del primer registro seleccionado de bloqueo de la comunicación electrónica de usuarios.

El documento US 6.789.203 B1 da a conocer un procedimiento, un aparato y un medio legible por un ordenador para evitar un ataque DoS sin notificar al atacante DoS. En una realización, en un entorno de cliente/servidor, un módulo de defensa de DoS determina una tasa de solicitud de conexión para un cliente particular. Se bloquea al cliente si se determina que la tasa de solicitud de conexión se encuentra por encima de un primer umbral predeterminado. Sin embargo, si la tasa de solicitud de conexión se encuentra por debajo del primer umbral pero por encima de un segundo umbral, entonces se ralentiza, o reduce , la tasa de solicitud de conexión del cliente hasta una tasa coherente con un intervalo de retraso de la conexión que está basado en un factor de reducción.

El documento US 6.434.601 B1 da a conocer un procedimiento y un aparato que operan completamente en segundo plano (es decir, de forma transparente al usuario) para verificar la validez de la dirección de correo electrónico de Internet del destinatario. Se intenta evitar la entrega de un mensaje de correo electrónico a una dirección de correo electrónico de Internet del destinatario que tenga un nombre de usuario, un nombre de servidor incorrectos o errores

ortográficos en cualquiera o en ambos. Si se detecta un error, se presenta a la atención del remitente, pudiendo ser corregido antes de que se envíe el mensaje.

El documento WO 2006/088915 A1 da a conocer un sistema que permite a los remitentes gestionar el contenido de la mensajería electrónica en el punto de origen. El sistema está integrado con la aplicación cliente que está siendo utilizada para preparar el mensaje para ser enviado. Se intercepta una solicitud de envío aún dentro del cliente y se lleva a cabo una serie de etapas de análisis de mensaje que analizan el remitente, el destinatario, el mensaje, cualquier archivo adjunto al mensaje y/o contenido e información relacionados. Se pone la salida del análisis de mensajes a disposición de los usuarios con reglas especificadas por el desempeño de varias acciones. Las etapas de análisis del contenido y las acciones tomadas pueden ser determinadas por el remitente o pueden ser gestionadas centralmente y determinadas por la organización del remitente.

El documento US 2005/0198175 A1 da a conocer procedimientos y sistemas para crear y generar correos masivos dinámicos con un contenido estático y dinámico. Se establecen filtros para determinar el contenido dinámico.

En el documento WO 2005/081109 A1 se da a conocer un sistema de gestión de correo electrónico.

Sumario de la invención

El objeto de la invención es proporcionar técnicas mejoradas para detectar el uso indebido de una infraestructura de correo electrónico en una red informática.

Según un aspecto de la invención, se proporciona un sistema implementado en ordenador según la reivindicación 1.

Según un aspecto adicional de la invención, se proporciona un procedimiento para detectar el uso indebido de una infraestructura de correo electrónico en una red informática según la reivindicación 13.

La presente invención proporciona un sistema y un procedimiento para detectar y evitar el uso indebido de recursos de comunicaciones en forma de envío de correo electrónico masivo no solicitado a través de vulnerabilidades aprovechadas del soporte lógico. Se lleva a cabo un filtrado no dentro de una pasarela en una capa externa, sino directamente en el sistema anfitrión que puede ejecutar una secuencia de ejecución, y no después de que haya acabado el procedimiento de envío y el correo electrónico está de camino a la red informática, preferentemente Internet, sino durante el procedimiento de envío.

La colocación del componente de monitorización de correo electrónico directamente en el sistema anfitrión remitente permite las consideraciones de información valiosa adicional para una clasificación de correo electrónico. Por ejemplo, información acerca de un usuario, una secuencia de ejecución o programa y/o hay disponible una sesión de inicio para la detección de un uso potencial indebido, pero se pierde en cuanto el correo electrónico abandona el sistema anfitrión. De forma alternativa, también se denomina al correo electrónico mensaje electrónico o comunicación electrónica.

En una realización preferente, el sistema y el procedimiento incluyen componentes para aplicar filtros estadísticos a todos los correos electrónicos de salida en un servidor. Estos incluyen, preferentemente, correos electrónicos enviados a través de un agente de transferencia de correo electrónico en el servidor, al igual que correos electrónicos transmitidos directamente por SMTP. SMTP es un acrónimo de protocolo de transferencia simple de correo. Es un estándar de Internet descrito por el Internet Engineering Task Force (IETF) para ser utilizado para enviar mensajes de correo electrónico. En la actualidad, la mayoría de proveedores de Internet utilizan este protocolo para enviar correo electrónico.

En una realización preferente, el sistema anfitrión comprende, además, un componente de agente de transferencia de correo electrónico. En general, las secuencias de ejecución más ejecutables no están dotadas de un componente de agente de transferencia de correo, sino que, en vez de ello, retransmiten correos electrónicos invocando un agente de transferencia de correo como sendmail. Por lo tanto, el agente de transferencia de correo debería ser un componente del sistema.

En una realización preferente adicional, el componente de monitorización de correo electrónico está integrado con el componente de agente de transferencia de correo electrónico. Por lo tanto, el componente de monitorización goza del beneficio de poder acceder a los parámetros internos del agente de transferencia de correo y para influir en el procedimiento de envío de mensajes electrónicos.

Aún en una realización preferente adicional, se proporciona el componente de monitorización de correo electrónico como un filtro en una conexión de transmisión de datos entre el componente de programa de aplicación y el componente de agente de transferencia de correo electrónico. Esta realización es beneficiosa en particular cuando un agente de transferencia de correo de código cerrado está integrado, de manera que no pueda modificarse a sí mismo.

En una realización preferente de la invención, se proporciona el componente de monitorización de correo electrónico en una conexión de transmisión de datos entre el componente de programa de aplicación y el componente de

agente de transferencia de correo electrónico. De nuevo, tal realización es beneficiosa, en particular, cuando hay integrado un agente de transferencia de correo de código cerrado que no puede modificarse a sí mismo.

En una realización preferente, el componente de monitorización de correo electrónico está integrado con la interfaz de red. El soporte lógico, tal como secuencias de ejecución ejecutables, puede estar dotado de un agente de transferencia de correo. Tal integración garantiza que la comunicación que se origina en tal soporte lógico pueda seguir siendo monitorizada.

Se proporciona al menos una conexión de SMTP en el sistema anfitrión.

Se proporciona un componente adicional de monitorización de correo electrónico en la al menos una conexión de SMTP, en el que el componente adicional de monitorización de correo electrónico está configurado para interceptar correos electrónicos en el sistema anfitrión generados por medio del componente de programa de aplicación para enviarlos a la red informática por medio de al menos una conexión de SMTP y la interfaz de red. Esto es beneficioso en un caso de un motor de SMTP.

En una realización preferente adicional, se proporcionan como un componente transparente al menos uno del componente de monitorización de correo electrónico y del componente adicional de monitorización de correo electrónico.

En otra realización preferente adicional, el sistema anfitrión comprende, además, un componente de clasificación estadística conectado a al menos uno del componente de monitorización de correo electrónico y del componente adicional de monitorización de correo electrónico.

En otra realización preferente adicional, el componente de clasificación estadística está integrado con al menos uno del componente de monitorización de correo electrónico y del componente adicional de monitorización de correo electrónico.

En una realización preferente adicional, el componente de clasificación estadística está configurado para asignar al correo electrónico interceptado una puntuación de clasificación estadística en función de al menos uno de un análisis de propiedades del correo electrónico interceptado y de un análisis de información relacional que indica la relación del correo electrónico interceptado con al menos otro correo electrónico generado en el sistema anfitrión para su envío a la red informática por medio de la interfaz de red, y estando comprendida la puntuación de clasificación estadística en la información de clasificación electrónica. De ese modo, se puede mejorar la precisión de la clasificación.

En otra realización preferente, el componente de clasificación estadística está configurado para analizar al menos una propiedad del correo electrónico interceptado seleccionado del siguiente grupo de propiedades del correo electrónico interceptado: identificación del remitente, dirección de la red asignada a la identificación del remitente, información del destinatario, dirección de la red asignada a la información del destinatario, información de la línea de asunto, información de la hora de envío e información de la fecha de envío. La precisión del análisis puede mejorarse adicionalmente utilizando todas las propiedades mencionadas anteriormente.

En otra realización preferente adicional, la puntuación de clasificación estadística asignada al correo electrónico interceptado es indicativa de que el correo electrónico interceptado es al menos uno de un correo electrónico de uso indebido y de un correo electrónico masivo no solicitado.

A continuación, se dan a conocer realizaciones preferentes del procedimiento para detectar el uso indebido de la infraestructura de correo electrónico en la red informática.

En una realización preferente adicional de la invención, el correo electrónico es interceptado en un componente de agente de transferencia de correo electrónico.

En una realización preferente adicional, el correo electrónico interceptado es interceptado en el componente de agente de transferencia de correo electrónico antes de que se complete el procedimiento de transmisión. Esto permite que el sistema interrumpa el procedimiento de envío del correo electrónico antes de que el correo electrónico haya pasado desde una aplicación de soporte lógico invocadora a una infraestructura que es responsable de entregar el mensaje. Una vez que el soporte lógico invocador ha hecho pasar con éxito el correo electrónico al agente de transferencia de correo, no se puede borrar el correo electrónico sin implicaciones legales y sin la pérdida desapercibida del mensaje.

En una realización adicional, el correo electrónico es interceptado en un filtro proporcionado como componente de monitorización de correo electrónico en una conexión de transmisión de datos entre el componente de programa de aplicación y el componente de agente de transferencia de correo electrónico.

El correo electrónico es interceptado en la interfaz de red.

El correo electrónico es interceptado en una conexión de SMTP establecida en el sistema anfitrión.

En otra realización, el correo electrónico es interceptado antes del fin de una sesión de SMTP asignada al correo electrónico interceptado, proporcionando, de ese modo, la opción de seguir dando fin a la conexión.

En otra realización, se proporcionan las siguientes etapas:

- el sistema anfitrión comprende, además, un componente de clasificación estadística conectado al componente de monitorización de correo electrónico,

- en la etapa de proporcionar la información de clasificación electrónica, el componente de clasificación estadística asigna una puntuación de clasificación estadística al correo electrónico interceptado en función de al menos uno del análisis de las propiedades del correo electrónico interceptado y del análisis de la información relacional que indica la relación del correo electrónico interceptado con al menos otro correo electrónico generado en el sistema anfitrión para su envío a la red informática por medio de la interfaz de red, y

- la puntuación de clasificación estadística está comprendida en la información de clasificación estadística.

En otra realización preferente adicional, el componente de clasificación estadística analiza al menos una propiedad seleccionada del siguiente grupo de propiedades del correo electrónico interceptado: identificación del remitente, dirección de la red asignada a la identificación del remitente, información del destinatario, dirección de la red asignada a la información del destinatario, información de la línea de asunto, información de la hora de envío e información de la fecha de envío.

En una realización adicional, la puntuación de clasificación estadística asignada al correo electrónico interceptado es indicativa de que el correo electrónico interceptado es al menos uno de un correo electrónico de uso indebido y un correo electrónico masivo no solicitado.

En otra realización preferente adicional, la etapa de análisis de la información relacional comprende analizar al menos una de la información relacional que indica una distribución horaria de una pluralidad de correos electrónicos generados por el componente de programa de aplicación y de la información relacional adicional que indica propiedades de similitud entre la pluralidad de correos electrónicos.

En una realización preferente adicional de la invención, para una pluralidad de correos electrónicos proporcionada en representación de una cuenta de usuario o de un grupo de cuentas de usuario se suma una puntuación respectiva de componentes de clasificación estadística para proporcionar una puntuación de la suma de componentes de clasificación estadística que es utilizada para determinar si al menos uno del comportamiento de envío de correo electrónico de la cuenta de usuario y del comportamiento de envío de correo electrónico del grupo de cuentas de usuario es de uso indebido.

Descripción de realizaciones preferentes de la invención

A continuación se describirá la invención con más detalle, a modo de ejemplo, con referencia a distintas realizaciones. En las Figuras:

La Fig. 1 muestra una representación esquemática de un sistema de correo electrónico,

La Fig. 2 muestra realizaciones alternativas para integrar un componente de monitorización de correo electrónico en un sistema anfitrión proporcionado en el sistema de correo electrónico de la Fig. 1, y

La Fig. 3 muestra un diagrama de flujo de un procedimiento llevado a cabo por medio de un componente de monitorización de correo electrónico entre el inicio y el fin de la transmisión de un correo electrónico.

Con referencia a las figuras, la Fig. 1 muestra una representación esquemática de un sistema 1 de correo electrónico. El sistema 1 de correo electrónico es un ordenador de red en el que se puede implementar la presente invención. El sistema proporcionado 1 de correo electrónico contiene una red 2, que es el medio usado para proporcionar enlaces de comunicaciones entre diversos dispositivos y ordenadores conectados entre sí en el sistema 1 de correo electrónico. La red 2 puede incluir conexiones, tales como enlaces de comunicaciones alámbricos o inalámbricos o cables de fibra óptica.

En el ejemplo mostrado, hay conectado un servidor 3 a la red 2 junto con una unidad 4 de almacenamiento. Además, hay conectados clientes 5, 6 y 7 a la red 2. Estos clientes 5, 6, 7 que también pueden ser denominados estaciones de red pueden ser, por ejemplo, ordenadores personales u ordenadores de red, teniendo cada uno la capacidad de gestionar correos electrónicos, como al menos uno de un remitente configurado para enviar correos electrónicos y un destinatario configurado para recibir correos electrónicos.

La Fig. 2 muestra realizaciones alternativas para integrar un componente 20 de monitorización de correo electrónico en un sistema anfitrión 21. El sistema anfitrión 21 se proporciona en el servidor 3 del sistema 1 de correo electrónico de la Fig. 1. Mediante el cliente respectivo 5, 6, 7 un usuario puede acceder al sistema anfitrión 21 para una gestión de correo electrónico.

Se proporciona el componente 20 de monitorización encima de una interfaz 22 de red del sistema anfitrión 21 de una forma que es transparente para un usuario del sistema anfitrión 21, de forma que sean necesarios cambios a un soporte lógico de usuario. El componente 20 de monitorización monitoriza todas las conexiones 23 de salida de SMTP en el sistema anfitrión 21.

Se puede integrar, opcionalmente, un componente adicional de monitorización implementado similar al componente 20 de monitorización en el agente 24 de transferencia de correo electrónico (MTA) del sistema anfitrión, por ejemplo sendmail, o puede construirse sobre el mismo, de nuevo de forma transparente al usuario: El componente adicional de monitorización monitoriza todas las llamadas de un programa 25 de usuario o secuencia de ejecución al MTA 24 que intenta llevar a cabo una transmisión de correo electrónico. La razón de esta monitorización doble es que, en algunos casos, las secuencias de ejecución o los programas de usuario utilizan el MTA 24 proporcionado por el anfitrión para enviar correos electrónicos, lo que es sencillo de implementar. El componente 20 de monitorización en el MTA 24, o encima del mismo, tiene acceso a todos los parámetros con los que se invoca al MTA 24. En otros casos, las secuencias de ejecución o los programas de usuario circunvalan el MTA 24 del sistema anfitrión implementando su propio motor de SMTP. Para poder monitorizar correos electrónicos enviados también desde estas secuencias de ejecución, se necesita el componente adicional de monitorización en la interfaz de red, que tiene entonces acceso a las propiedades de los correos electrónicos y de las conexiones durante el procedimiento de envío.

A continuación, con referencia a la Fig. 3, un procedimiento que es ejecutado por el componente 20 de monitorización de correo electrónico entre el inicio y el fin de la transmisión de un correo electrónico también es denominado mensaje electrónico.

Se activa un componente de monitorización de correo electrónico por cada intento de un programa o secuencia de ejecución de enviar un correo electrónico bien a través del MTA del sistema anfitrión o bien directamente con su propia conexión de SMTP en una etapa 200. El componente de monitorización de correo electrónico analiza el contenido del correo electrónico interceptado en una etapa 201, sus nombres y direcciones de destinatarios, su nombre y dirección de remitente, su línea de asunto, su fecha y su hora de envío, la secuencia de ejecución o programa que invoca el procedimiento de envío y los parámetros de la invocación, las propiedades de la sesión de usuario que dieron lugar a la invocación (por ejemplo, la sesión de HTTP que accedió a la secuencia de ejecución), y todas estas propiedades de todos los correos electrónicos enviados anteriormente desde la misma cuenta de usuario y/o anfitrión.

Con un clasificador estadístico 300 basado en el contenido del correo electrónico interceptado, sus atributos externos, los atributos de la invocación de envío y su relación con los casos anteriores 301, en una etapa 202 se calcula una puntuación de correo basura del correo electrónico actual. La puntuación de correo basura es un indicador de que el correo electrónico interceptado sea correo electrónico masivo no solicitado. Junto con las puntuaciones de correo basura de todos los correos electrónicos enviados recientemente por el mismo usuario o grupo de usuarios y la aplicación de un umbral predefinido, el componente de monitorización estima si el uso del programa o secuencia de ejecución es de uso indebido.

En una realización preferente, se puede deducir la puntuación de correo basura calculando una suma de puntuaciones específicas al término en una lista predefinida de términos, y añadiendo una puntuación específica para el usuario. Se deduce una puntuación específica para el término multiplicando el número de apariciones del término en el correo electrónico con un peso específico para el término. Se puede determinar el peso específico de término para cada término procesando una colección de correos electrónicos de entrenamiento con un procedimiento de aprendizaje estadístico que es conocido como tal. Se puede derivar la puntuación específica para el usuario del contenido o de la puntuación de correo basura de todos los mensajes que ha enviado el usuario en un intervalo de tiempo reciente. Además, se puede influir en la puntuación de correo basura por medio de una puntuación que se deriva de la línea de asunto del mensaje, de las imágenes adjuntas y de otros elementos del mensaje. La presente invención no depende del procedimiento específico para el cálculo de la puntuación. Se conocen varios procedimientos en la técnica que pueden ser implementados junto con el sistema dado a conocer en la presente solicitud. Por ejemplo, se pueden encontrar tales procedimientos en la bibliografía (Drucker y otros.: “Support Vector Machines for Spam. Categorization”, IEEE Transactions on Neural Networks, Volumen: 10, número: 5, páginas 1048-1054, IEEE Computational Intelligence Society, 1999; Sahami y otros.: “A Bayesian Approach to Filtering Junk E-mail”, AAAI-98 Workshop on Learning for Text Categorization. Tech. Rep. WS-98-05, AAAI Press, 1998; Siefkes y otros.: “Combining Winnow and orthogonal sparse bigrams for incremental, spam filtering”, Proceedings of the 8th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD 2004), volumen 3202 de Lecture Notes in Artificial Intelligence, páginas 410-421. Springer, 2004).

Se clasifica el correo electrónico como correo basura cuando la puntuación de correo basura supera un umbral predefinido. En una posible realización, se puede ajustar el umbral, de forma que se reduzca el riesgo de una clasificación errónea de un mensaje como correo basura por debajo de un valor deseado.

En la realización mostrada, el componente de monitorización comprende un componente de reconocimiento que reconoce el inicio de una transmisión de un mensaje o correo electrónico, en función de protocolos apropiados tales

como SMTP. Un componente adicional del componente de monitorización, en concreto un componente extractor, extrae del correo electrónico el contenido y un conjunto de características que se requieren para calcular la puntuación de correo basura.

Un componente de determinación invocado subsiguientemente determina en una etapa 202 un sumando de la puntuación de correo basura que está basado en el propio correo electrónico. En la etapa 203, el componente de monitorización recupera el historial de correos (mensajes) electrónicos enviados por el propietario o por la empresa explotadora de la aplicación de soporte lógico y calcula una puntuación de correo basura específica para el usuario. El componente de monitorización determina la etapa final de correo basura (etapa 204), la compara con el valor umbral y decide qué acción tomar.

Si la puntuación derivada de correo basura supera un valor predefinido, el componente de monitorización puede desencadenar cualquiera de las acciones siguientes:

- Contactar con el administrador, el proveedor o la empresa explotadora de la infraestructura en la etapa 207 y enviarles una notificación, posiblemente por medio de mensajes electrónicos.

- Contactar con el propietario o la empresa explotadora del soporte lógico (usuario), posiblemente por medio de mensajes electrónicos.

- Interrumpir el procedimiento de comunicación, suministrar un código de error al soporte lógico que ha invocado el componente de monitorización. Por lo tanto, se notifica al remitente del mensaje de que ha fallado el procedimiento de entrega del mensaje.

- Suministrar un código de retorno al invocar un soporte lógico que indica una entrega con éxito del mensaje. Por lo tanto, se mantiene al remitente del mensaje desinformado del fallo en la entrega del mensaje.

- Bloquear el acceso del usuario a la infraestructura de comunicaciones.

- Almacenar información acerca del mensaje electrónico y del procedimiento.

Cuando la puntuación de correo basura no supera el umbral, se procesa normalmente el correo electrónico interceptado. En caso de que no se detecte un uso potencial indebido, el envío del correo electrónico interceptado se lleva a cabo en una etapa 205. Se proporciona un informe acerca del envío con éxito.

Sin embargo, en caso de un probable uso indebido de la infraestructura (204) de correo electrónico, el componente de monitorización de correo electrónico inicia al menos una de las siguientes acciones en una etapa 206:

- Enviar una notificación al administrador del anfitrión (etapa 207), incluyendo información acerca del usuario, el correo electrónico y las puntuaciones de correo basura de los correos electrónicos enviados recientemente.

- Enviar una notificación al propietario de la cuenta de usuario (etapa 209), incluyendo información acerca del correo electrónico y el patrón de uso de la secuencia de ejecución afectada, y aconsejar posiblemente acerca de la subsanación de los agujeros de seguridad.

- Abortar la transmisión del correo electrónico (etapa 208), y bloquear todos los intentos ulteriores de transmisión de correo electrónico por medio de la misma secuencia de ejecución o programa.

- Abortar la transmisión del correo electrónico interceptado, y bloquear todos los intentos ulteriores de transmisión de correo electrónico por parte del mismo usuario o grupo de usuarios.

- Abortar la transmisión del correo electrónico interceptado (etapa 208), y añadir una entrada acerca del correo electrónico y su puntuación de correo basura en la base de datos almacenada de correos electrónicos recientes.

- Informar de un mensaje de error a la secuencia de ejecución de envío o al programa de aplicación (etapa 211).

- Abortar la transmisión del correo electrónico interceptado (etapa 208), pero informar un éxito a la secuencia de ejecución de envío o programa (etapa 210), simulando, por lo tanto, una finalización con éxito de la transmisión para no dar al atacante una pista de la detección.

- Retrasar la transmisión del correo electrónico interceptado (etapa 212), para reducir la cantidad de correos electrónicos que pueden ser enviados por el usuario, reduciendo, de esta manera, el daño potencial causado por los correos electrónicos de uso indebido.

La presente invención proporciona una forma de eludir problemas legales con el bloqueo de correos electrónicos de salida. El filtrado tiene lugar antes de terminar el procedimiento de envío y, por lo tanto, el correo electrónico puede

ser bloqueado antes de que la secuencia de ejecución o programa de inicio obtenga información de retorno acerca del éxito de la transmisión y, por lo tanto, no proceden necesariamente las complicaciones legales.

Además, el componente de monitorización puede proporcionar una información de retorno directamente a la secuencia de ejecución o programa de envío, incluso antes de terminar la transmisión.

Las características dadas a conocer en la presente memoria, en las reivindicaciones y/o en las figuras pueden ser el material para la implementación de la invención en sus diversas realizaciones, tomadas de forma aislada o en diversas combinaciones de las mismas.

REIVINDICACIONES

1. Un sistema implementado en ordenador para detectar el uso indebido de una infraestructura de correo electrónico, que comprende:

- un sistema anfitrión (21),

- un componente (25) de programa de aplicación implementado en el sistema anfitrión (21),

- una interfaz (22) de red proporcionada como parte del sistema anfitrión (21) y configurada para gestionar un intercambio de datos electrónicos entre el sistema anfitrión (21) y una red informática,

- un componente (20) de monitorización de correo electrónico proporcionado en el sistema anfitrión (21) y transparente a un usuario del sistema anfitrión (21), en el que el componente (20) de monitorización de correo electrónico está configurado para interceptar dentro del sistema anfitrión (21) correos electrónicos generados por el componente (25) de programa de aplicación para enviar a la red informática por medio de la interfaz (22) de red y para proporcionar información de clasificación electrónica acerca de un estado de uso indebido del correo electrónico interceptado, y

- un cliente (5, 6, 7) conectado a la red informática y configurado para gestionar correo electrónico como al menos uno de un remitente configurado para enviar correo electrónico y un destinatario configurado para recibir correo electrónico,

en el que se proporciona el sistema anfitrión (21) en un servidor (3) de un sistema (1) de correo electrónico, de forma que se puede acceder al sistema anfitrión (21) por medio del cliente (5, 6, 7) para una gestión de correo electrónico,

caracterizado porque se proporciona al menos una conexión (23) de SMTP en el sistema anfitrión (21) y se proporciona un componente adicional (20) de monitorización de correo electrónico en la al menos una conexión (23) de SMTP, en el que el componente adicional de monitorización de correo electrónico está configurado para interceptar dentro del sistema anfitrión (21) correos electrónicos generados por medio del componente (25) de programa de aplicación para enviarlos a la red informática por medio de la al menos una conexión (23) de SMTP y la interfaz (22) de red.

2. El sistema según la reivindicación 1, en el que el sistema anfitrión (21) comprende, además, un componente (24) de agente de transferencia de correo electrónico.

3. El sistema según la reivindicación 2, en el que el componente (20) de monitorización de correo electrónico está integrado con el componente (24) de agente de transferencia de correo electrónico.

4. El sistema según la reivindicación 2, en el que se proporciona el componente (20) de monitorización de correo electrónico como un filtro en una conexión de transmisión de datos entre el componente (25) de programa de aplicación y el componente (24) de agente de transferencia de correo electrónico.

5. El sistema según la reivindicación 1 o 2, en el que se proporciona el componente (20) de monitorización de correo electrónico en una conexión de transmisión de datos entre el componente (25) de programa de aplicación y el componente (24) de agente de transferencia de correo electrónico.

6. El sistema según la reivindicación 1 o 2, en el que el componente (20) de monitorización de correo electrónico está integrado con la interfaz (22) de red.

7. El sistema según una de las reivindicaciones precedentes, en el que el componente adicional de monitorización de correo electrónico es proporcionado como un componente transparente.

8. El sistema según una de las reivindicaciones precedentes, en el que el sistema anfitrión (21) comprende, además, un componente de clasificación estadística conectado a al menos uno del componente (20) de monitorización de correo electrónico y del componente adicional de monitorización de correo electrónico.

9. El sistema según la reivindicación 8, en el que el componente de clasificación estadística está integrado con al menos uno del componente (20) de monitorización de correo electrónico y del componente adicional de monitorización de correo electrónico.

10. El sistema según la reivindicación 8 o 9, en el que el componente de clasificación estadística está configurado para asignar al correo electrónico interceptado una puntuación de clasificación estadística en función de al menos uno de un análisis de propiedades del correo electrónico interceptado y de un análisis de información relacional que indica la relación del correo electrónico interceptado con al menos otro correo electrónico generado en el sistema anfitrión (21) para enviarla a la red informática por medio de la interfaz (22) de red, y en el que la puntuación de clasificación estadística está comprendida en la información de clasificación electrónica.

11. El sistema según una de las reivindicaciones 8 a 10, en el que el componente de clasificación estadística está configurado para analizar al menos una propiedad del correo electrónico interceptado seleccionada del siguiente grupo de propiedades del correo electrónico interceptado:

identificación del remitente, dirección de la red asignada a la identificación del remitente, información del destinatario, dirección de la red asignada a la información del destinatario, información de la línea de asunto, información de la hora de envío e información de la fecha de envío.

12. El sistema según la reivindicación 10 u 11, en el que la puntuación de clasificación estadística asignada al correo electrónico interceptado es indicativa de que el correo electrónico interceptado es al menos uno de correo electrónico de uso indebido y de correo electrónico masivo no solicitado.

13. Un procedimiento para detectar un uso indebido de una infraestructura de correo electrónico en una red informática, en el que un sistema implementado en ordenador conectable a la red informática comprende

- un sistema anfitrión (21),

- un componente (25) de programa de aplicación implementado en el sistema anfitrión (21),

- una interfaz (22) de red proporcionada como parte del sistema anfitrión (21) y configurada para gestionar un intercambio de datos electrónicos entre el sistema anfitrión (21) y la red informática, y

- un cliente (5, 6, 7) conectado a la red informática y que tiene la capacidad de gestionar correo electrónico como al menos uno de un remitente configurado para enviar correo electrónico y un destinatario configurado para recibir correo electrónico,

comprendiendo el procedimiento las etapas de:

- generar un correo electrónico por medio del componente (25) de programa de aplicación para enviar el correo electrónico a la red informática por medio de la interfaz (22) de red,

- en el sistema anfitrión (21), interceptar el correo electrónico por medio de un componente (20) de monitorización de correo electrónico proporcionado en el sistema anfitrión (21), siendo transparente dicho componente de monitorización de correo electrónico a un usuario del sistema anfitrión (21), y

- mediante el componente (20) de monitorización de correo electrónico, proporcionar información de clasificación electrónica acerca de un estado de uso indebido del correo electrónico interceptado,

en el que se proporciona el sistema anfitrión (21) en un servidor (3) de un sistema (1) de correo electrónico, de forma que el sistema anfitrión (21) es accesible por medio del cliente (5, 6, 7) para una gestión de correo electrónico,

caracterizado porque se proporciona al menos una conexión (23) de SMTP en el sistema anfitrión (21) y se proporciona un componente adicional (20) de monitorización de correo electrónico en la al menos una conexión (23) de SMTP, en el que el correo electrónico es interceptado en una conexión (23) de SMTP establecida en el sistema anfitrión (21) o en la interfaz (22) de red por medio del componente adicional de monitorización de correo electrónico.

14. El procedimiento según la reivindicación 13, en el que el correo electrónico es interceptado en un componente (24) de agente de transferencia de correo electrónico.

15. El procedimiento según la reivindicación 14, en el que el correo electrónico interceptado es interceptado antes del inicio de un procedimiento de transmisión dentro del componente (24) de agente de transferencia de correo electrónico.

16. El procedimiento según la reivindicación 13, en el que el correo electrónico es interceptado en un filtro proporcionado como el componente (20) de monitorización de correo electrónico en una conexión de transmisión de datos entre el componente (25) de programa de aplicación y el componente (24) de agente de transferencia de correo electrónico.

17. El procedimiento según la reivindicación 13, en el que el correo electrónico es interceptado antes del fin de una sesión de SMTP asignada al correo electrónico interceptado.

18. El procedimiento según una de las reivindicaciones 13 a 17, en el que:

- el sistema anfitrión (21) comprende, además, un componente de clasificación estadística conectado al componente (20) de monitorización de correo electrónico,

- en la etapa de proporcionar la información de clasificación electrónica, el componente de clasificación estadística asigna una puntuación de clasificación estadística al correo electrónico interceptado en función de al menos uno del análisis de las propiedades del correo electrónico interceptado y del análisis de la información relacional que indica la relación del correo electrónico interceptado con al menos otro correo electrónico generado en el sistema anfitrión (21) para enviarlo a la red informática por medio de la interfaz (22) de red, y

- la puntuación de clasificación estadística está comprendida en la información de clasificación electrónica.

19. El procedimiento según la reivindicación 18, en el que el componente de clasificación estadística analiza al menos una propiedad seleccionada del siguiente grupo de propiedades del correo electrónico interceptado: identificación del remitente, dirección de la red asignada a la identificación del remitente, información del destinatario, dirección de la red asignada a la información del destinatario, información de la línea de asunto, información de la hora de envío e información de la fecha de envío.

20. El procedimiento según la reivindicación 18 o 19, en el que la puntuación de clasificación estadística asignada al correo electrónico interceptado es indicativa de que el correo electrónico interceptado es al menos uno de un correo electrónico de uso indebido y un correo electrónico masivo no solicitado.

21. El procedimiento según una de las reivindicaciones 18 a 20, en el que la etapa de análisis de la información relacional comprende analizar al menos una de la información relacional que indica una distribución horaria de una pluralidad de correos electrónicos generados por el componente (25) de programa de aplicación y la información relacional adicional que indica propiedades de similitud entre la pluralidad de correos electrónicos.

22. El procedimiento según la reivindicación 18, en el que para una pluralidad de correos electrónicos proporcionados en representación de una cuenta de usuario o de un grupo de cuentas de usuario se suma un componente respectivo de clasificación estadística para proporcionar una puntuación de suma de componentes de clasificación estadística que es utilizada para determinar si al menos uno de un comportamiento de envío de correo electrónico de la cuenta de usuario y un comportamiento de envío de correo electrónico del grupo de cuentas de usuario es de uso indebido.

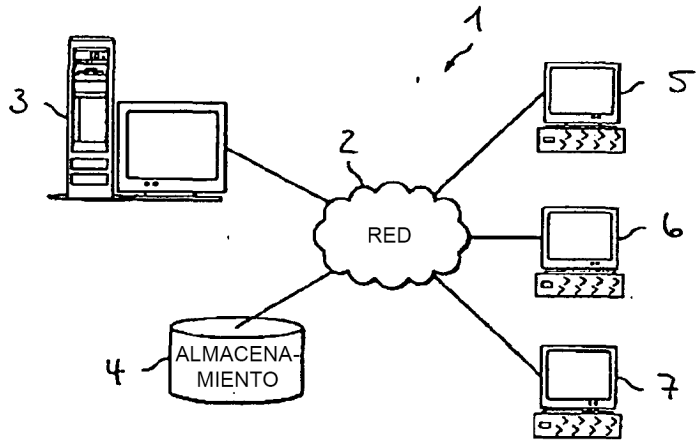

Fig. 1

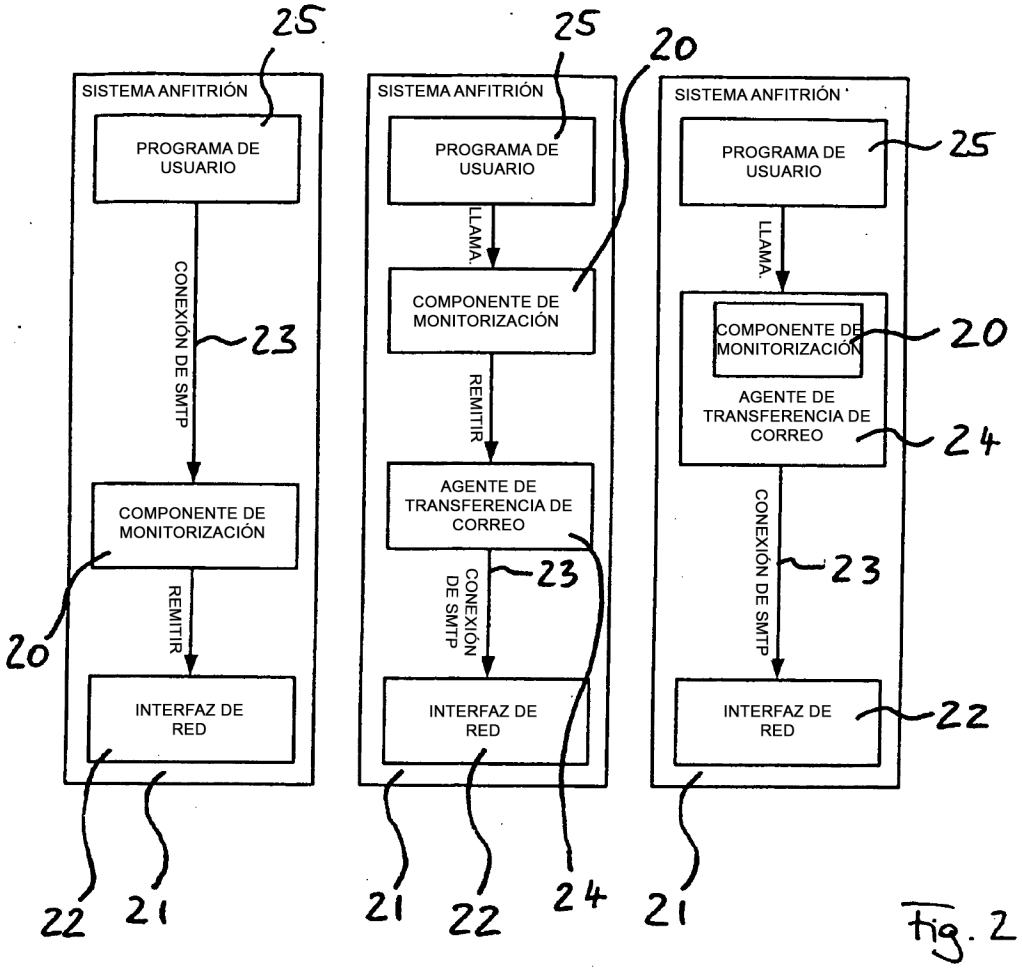
25
SISTEMA ANFITRIÓN
PROGRAMA DE USUARIO
CONEXIÓN DE SMTP
23
COMPONENTE DE MONITORIZACIÓN
REMITIR
20
INTERFAZ DE RED
22
21
25
SISTEMA ANFITRIÓN
PROGRAMA DE USUARIO
LLAMA.
20
COMPONENTE DE MONITORIZACIÓN
REMITIR
AGENTE DE TRANSFERENCIA DE CORREO
23
CONEXIÓN DE SMTP
INTERFAZ DE RED
21
22
24
SISTEMA ANFITRIÓN
PROGRAMA DE USUARIO
25
LLAMA.
COMPONENTE DE MONITORIZACIÓN
20
AGENTE DE TRANSFERENCIA DE CORREO
24
CONEXIÓN DE SMTP
23
INTERFAZ DE RED
22
21

Fig. 2

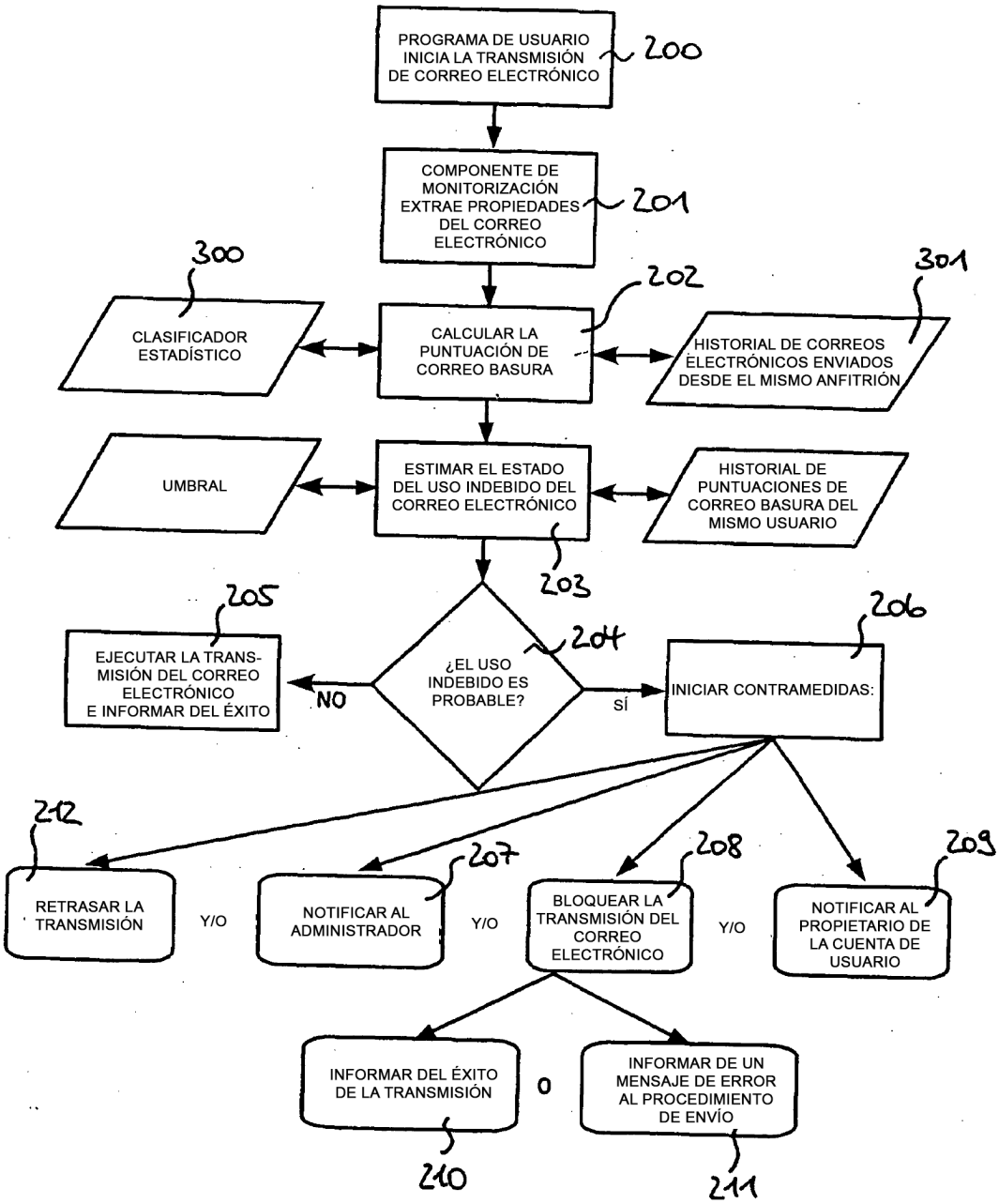
PROGRAMA DE USUARIO INICIA LA TRANSMISIÓN DE CORREO ELECTRÓNICO
200
COMPONENTE DE MONITORIZACIÓN EXTRAE PROPIEDADES DEL CORREO ELECTRÓNICO
201
300
CLASIFICADOR ESTADÍSTICO
CALCULAR LA PUNTUACIÓN DE CORREO BASURA
202
301
HISTORIAL DE CORREOS ELECTRÓNICOS ENVIADOS DESDE EL MISMO ANFITRIÓN
UMBRAL
ESTIMAR EL ESTADO DEL USO INDEBIDO DEL CORREO ELECTRÓNICO
HISTORIAL DE PUNTUACIONES DE CORREO BASURA DEL MISMO USUARIO
203
205
EJECUTAR LA TRANSMISIÓN DEL CORREO ELECTRÓNICO E INFORMAR DEL ÉXITO
NO
¿EL USO INDEBIDO ES PROBABLE?
204
SÍ
206
INICIAR CONTRAMEDIDAS:
212
RETRASAR LA TRANSMISIÓN
Y/O
207
NOTIFICAR AL ADMINISTRADOR
Y/O
208
BLOQUEAR LA TRANSMISIÓN DEL CORREO ELECTRÓNICO
Y/O
209
NOTIFICAR AL PROPIETARIO DE LA CUENTA DE USUARIO
INFORMAR DEL ÉXITO DE LA TRANSMISIÓN
O
INFORMAR DE UN MENSAJE DE ERROR AL PROCEDIMIENTO DE ENVÍO
210
211

Fig. 3