Abuso en el correo electrónico (ACE)

1. Introducción

Definimos ACE (Abuso en Correo Electrónico) como las diversas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios. Algunos de los términos habitualmente asociados en Internet a estos tipos de abuso son *spamming*, *mail bombing*, *unsolicited bulk email* (UBE), *unsolicited commercial email* (UCE), *junk mail*, etc., abarcando un amplio abanico de formas de difusión.

De los tipos de abuso englobados en ACE, el que más destaca es el conocido como *spam* que es un término aplicado a mensajes distribuidos a una gran cantidad de destinatarios de forma indiscriminada. En la mayoría de los casos el emisor de estos mensajes es desconocido y generalmente es imposible responderlo (*reply*) de la forma habitual o incluso llegar a identificar una dirección de retorno correcta.

2. Definición de términos

El correo en Internet es procesado por máquinas o servidores de origen, de encaminamiento y de destino utilizando el estándar de correo SMTP. Los agentes implicados en la transferencia de correo son:

- **Operador de Origen**: Es la organización responsable de la máquina que encamina el mensaje de correo hacia Internet.
- **Operador de Encaminamiento**: Es la organización responsable de las máquinas que encaminan el mensaje de correo entre el operador de origen y el operador de destino).
- **Operador de Destino**: Es la organización o responsable de la máquina que mantiene el control de los buzones de los destinatarios.
- **Emisor**: Es la persona origen del mensaje. Incluso cuando el emisor es un programa o sistema operativo, habrá una o más personas que sea(n) responsable(s) del mismo.
- **Receptor**: Es la persona que recibe el mensaje. Al igual que en el caso del receptor, puede no tratarse de una persona física, pero siempre habrá al menos un responsable más o menos directo de cada dirección de destino.
- **Listas de correo**: Son receptores de correo que actuan distribuyendo el mensaje a un número de destinatarios. Se las puede considerar como una especie de encaminadoras de correo. Estas listas pueden ser gestionadas por una persona o por un proceso automático.

No se les considera emisores ni receptores propiamente dichos, ya que la lista no es ni el origen ni el destinatario final de los mensajes. Sin embargo, pueden considerarse como tal en algunos casos: por ejemplo, los mensajes de control enviados para darse de alta o baja de una lista, y las respuestas del servidor a dichas acciones. Incluso en esos casos hay una persona detrás del servidor: el administrador del mismo.

3. Tipos de abuso

Las actividades catalogadas como ACE se pueden clasificar en cuatro grandes grupos:

- **Difusión de contenido inadecuado.**

  Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: apología del terrorismo, programas piratas, pornografía infantil, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.

  Contenido fuera de contexto en un foro temático. Pueden definir lo que es admisible: el moderador del foro, si existe; su administrador o propietario, en caso contrario, o los usuarios del mismo en condiciones definidas previamente al establecerlo (por ejemplo, mayoría simple en una lista de correo).

- **Difusión a través de canales no autorizados.**

  Uso no autorizado de una estafeta ajena para reenviar correo propio. Aunque el mensaje en sí sea legítimo, se están utilizando recursos ajenos sin su consentimiento (nada que objetar cuando se trata de una estafeta de uso público, declarada como tal).

- **Difusión masiva no autorizada.**

  El uso de estafetas propias o ajenas para enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado se considera inadecuado por varios motivos, pero principalmente éste: el anunciante descarga en transmisores y destinatarios el coste de sus operaciones publicitarias, tanto si quieren como si no.

- **Ataques con objeto de imposibilitar o dificultar el servicio.**

  Dirigido a un usuario o al propio sistema de correo. En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga el objetivo neto de paralizar el servicio por saturación de las líneas, de la capacidad de CPU del servidor, o del espacio en disco de servidor o usuario. Se puede considerar como una inversión del concepto de difusión masiva (1->n),en el sentido de que es un ataque (n->1).

  En inglés estos ataques se conocen como mail bombing, y son un caso particular de *denial of service* (DoS). En castellano podemos llamarlos bomba de correo o saturación, siendo un caso particular de denegación de servicio.

  Suscripción indiscriminada a listas de correo. Es una versión del ataque anterior, en la que de forma automatizada se suscribe a la víctima a miles de listas de correo. Dado que en este caso los ataques no vienen de una sola dirección, sino varias, son mucho más difíciles de atajar.

4. Problemas ocasionados

- **Efectos en los receptores.**

  Los usuarios afectados por el ACE lo son en dos aspectos: costes económicos y costes sociales. También se debe considerar la pérdida de tiempo que suponen, y que puede entenderse como un coste económico indirecto.

  Si se multiplica el coste de un mensaje a un receptor por los millones de mensajes distribuidos puede hacerse una idea de la magnitud económica, y del porcentaje mínimo de la misma que es asumido por el emisor. En lo que respecta a los costes sociales del ACE debe considerarse, aparte de la molestia u ofensa asociada a determinados contenidos, la inhibición del derecho a publicar la propia dirección en medios como News o Web por miedo a que sea capturada.

- **Efectos en los operadores.**

  Los operadores de destino y encaminamiento acarrean su parte del coste: tiempo de proceso, espacio en disco, ancho de banda, y sobre todo tiempo adicional de personal dedicado a solucionar estos problemas en situaciones de saturación.