ANEXO 1: Abuso no correo electrónico

1. Introdución

Definimos **ACE (Abuso no Correo Electrónico)** como as diversas actividades que trascenden os obxectivos habituais do servizo de correo e ocasionan prexuízos directa ou indirectamente aos usuarios. Algúns dos termos habitualmente asociados en Internet a estes tipos de abuso son spamming, mail bombing, unsolicited bulk email (UBE), unsolicited commercial email (UCE), junk mail, etc., abarcando un amplo abano de formas de difusión.

Dos tipos de abuso englobados no ACE, o que máis destaca é o coñecido como spam que é un termo aplicado a mensaxes distribuídas a unha gran cantidade de destinatarios de forma indiscriminada. Na maioría dos casos o emisor destas mensaxes é descoñecido e xeralmente é imposible responderlle (reply) da forma habitual ou incluso chegar a identificar unha dirección de retorno correcta.

2. Definición dos termos

O correo en Internet é procesado por máquinas ou servidores de orixe, de encamiñamento e de destino utilizando o estándar de correo SMTP. Os axentes implicados na transferencia de correo son:

1- Operador de Orixe: É a organización responsable da máquina que encamiña a mensaxe de correo cara Internet.

2- Operador de Encamiñamento: É a organización responsable das máquinas que encamiñan a mensaxe de correo entre o operador de orixe e o operador de destino.

3- Operador de Destino: É a organización ou responsable da máquina que mantén o control dos buzóns dos destinatarios.

4- Emisor: É a persoa orixe da mensaxe. Incluso cando o emisor é un programa ou sistema operativo, haberá unha ou máis persoas que sexa(n) responsable(s) do mesmo.

5- Receptor: É a persoa que recibe a mensaxe. Ao igual que no caso do receptor, pode non tratarse dunha persoa física, pero sempre haberá polo menos un responsable máis ou menos directo de cada dirección de destino.

6- Listas de correo: Son receptores de correo que actúan distribuíndo a mensaxe a un número de destinatarios. Pódense considerar como unha especie de encamiñadoras de correo. Estas listas poden ser xestionadas por unha persoa ou por un proceso automático.

Non se lles considera emisores nin receptores propiamente ditos, xa que a lista non é nin a orixe nin o destinatario final das mensaxes. Sen embargo, poden considerarse como tales nalgúns casos: por exemplo, as mensaxes de control enviadas para darse de alta ou baixa dunha lista, e as respostas do servidor a estas accións. Incluso neses casos hai unha persoa detrás do servidor: o administrador do mesmo.

ANEXO 2: Tipos de abuso

As **actividades** catalogadas como **ACE** pódense clasificar en catro grandes grupos:

1- Difusión de contido inadecuado: Contido ilegal por natureza (todo o que constitúa complicidade con feitos delictivos). Exemplos: apoloxía do terrorismo, programas piratas, pornografía infantil, ameazas, estafas, esquemas de enriquecemento piramidal, virus ou código hostil en xeral... Máis información sobre estos temas na área de información legal.

2- Contido fóra de contexto nun foro temático: Poden definir o que é admisible: o moderador do foro, se existe; o seu administrador ou propietario, en caso contrario, os usuarios do mesmo en condicións definidas previamente ao establecelo (por exemplo, maioría simple nunha lista de correo).

3- Difusión a través de canles non autorizadas: Uso non autorizado dunha estafeta allea para reenviar correo propio. Aínda que a mensaxe en si sexa lexítima, estanse utilizando recursos alleos sen o seu consentimento (nada que obxectar cando se trata dunha estafeta de uso público, declarada como tal).

4- Difusión masiva non autorizada: O uso de estafetas propias ou alleas para enviar de forma masiva publicidade ou calquera outro tipo de correo non solicitado considérase inadecuado por varios motivos, pero principalmente este: o anunciante descarga en transmisores e destinatarios o custo das súas operacións publicitarias, tanto se queren coma se non.

5- Ataques con obxecto de imposibilitar ou dificultar o servizo: Dirixido a un usuario ou ao propio sistema de correo. En ambos os dous casos o ataque consiste no envío dun número alto de mensaxes por segundo, ou calquera variante, que teña o obxectivo neto de paralizar o servizo por saturación das liñas, da capacidade de CPU do servidor, ou do espazo en disco do servidor ou usuario. Pódese considerar como unha inversión do concepto de difusión masiva (1->n), no senso de que é un ataque (n->1).

   En inglés estos ataques coñécense como *mail bombing*, e son un caso particular de *denial of service* (DoS). En galego podemos chamalos bomba de correo ou saturación, sendo un caso particular de denegación do servizo.

6- Suscrición indiscriminada a listas de correo: É unha versión do ataque anterior, na que de forma automatizada se susbcribe á víctima a miles de listas de correo. Dado que neste caso os ataques non veñen dunha soa dirección, senón de varias, son moito máis difíciles de atallar.

ANEXO 3: Problemas ocasionados

1- Efectos nos receptores: Os usuarios afectados polo Abuso no Correo Electrónico sono en dous aspectos: custos económicos e custos sociais. Tamén se debe considerar a perda de tempo que supoñen, e que pode entenderse como un custo económico indirecto. Se se multiplica o custo dunha mensaxe a un receptor polos millóns de mensaxes distribuídas, é posible facerse unha idea da magnitude económica e da porcentaxe mínima da mesma que é asumida polo emisor. No que respecta aos custos sociais de ACE débense considerar, aparte da molestia ou ofensa asociada a determinados contidos, a inhibición do dereito a publicar a propia dirección en medios como News ou Web por medo a que sexa capturada.

2- Efectos nos operadores: Os operadores de destino e encamiñamento acarrean a súa parte do custo: tempo de proceso, espazo en disco, ancho de banda, e sobre todo, tempo adicional de persoal dedicado a solucionar estos problemas en situacións de saturación.