Skräppost - Spam

1 Målgrupp

Alla som är anslutna till Umeå universitets datornät.

2 Allmänt

Skräppost, populärt kallat spam, är ett problem som orsakar stora kostnader. Dels går det åt en hel del arbetstid för användarna för att gå igenom och rensa e-postlådor fulla av skräppost, dels måste administratörerna ägna mycket tid åt att rensa köer, uppdatera filter etc. på e-postservrarna.

3 Policy

Umeå universitet tar starkt avstånd från allt som har med skräppost att göra och lägger ner stora resurser på att begränsa mängden skräppost till e-postlådorna.

För att minska mängden skräppost använder universitetets centrala e-posttjänst ett system med speciella filterservrar som är placerade i datorhall resp. reservhall. Endast signaturfilerna, som styr filtreringen, hämtas från leverantörens servrar. På så vis har Umeå universitet, så långt som det är möjligt, kontrollen över e-postflödet. Av sekretesskäl har man uteslutit lösningar där e-posttrafiken filtreras av servrar utanför universitetet.

Filterservrarna använder flera olika tekniker och blockerar i genomsnitt 95% av all inkommande e-post. I de flesta fallen spärras den sändande datorns IP-adress och den får aldrig chansen att ens försöka leverera några meddelanden. Ett felmeddelande går dock tillbaka till avsändaren med information om varför sändningen blockerats och med länkar till ytterligare information. Om ingen blockering skett på IP-adressen analyseras innehållet i meddelandet. Virussmittad e-post kastas direkt medan skräppost läggs i en karantän. Användarna kan via ett webbinterface logga in och själva kontrollera de senaste tidens spamskörd. Det går också att i viss utsträckning lägga till egna filterregler.

För att förhindra att universitetets centrala e-postservrar används för spridning av skräppost är dessa konfigurerade att bara släppa igenom ett visst antal meddelanden per avsändare och dator per dygn. Undantag kan göras för de som behöver göra större utskick till studenter etc.

Det är förbjudet för anställda och studenter att göra skräppostutskick eller att upplåta resurser för andra att göra detta.

Det är ej tillåtet att sätta upp egna e-postservrar på ett sådant sätt att de kan användas av utomstående för spridning av skräppost (relaying). Om så sker brukar det inte dröja länge förrän anmälningarna börjar droppa in till IRT. Om inte servern åtgärdas omedelbart stängs den av från nätverket.

4 Regler

4.1 Anställda

Exponera inte din e-postadress i onödan. Även om universitetets spamfilter är effektiva och skyddar adressen mot inkommande skräppost så finns risken att den i stället används som falsk avsändare vid skräppostutskick vilket kan ställa till med en hel del problem.

Svara inte på skräppost. Ofta finns det en länk i brevet som man skall klicka på för att slippa få ytterligare utskick. Gör inte det! Din adress kan komma att registreras som aktiv och du riskerar att få ännu mer skräppost eller att din adress används som avsändare vid skräppostutskick.

En del epost-klienter som ex.vis Outlook har egna inbyggda spamfilter som lägger misstänkt skräppost i en separat folder. Saknar man vissa brev bör man till att börja med titta i denna folder. Ansvaret för att hantera sådana spamfilter ligger på den anställde.

Det har blivit allt vanligare med så kallade phishingmail, dvs meddelanden som fiskar efter personlig information som kontonamn och lösenord. De är ofta skrivna på svenska och utger sig komma från universitetet. Ibland uppmanas man att svara på brevet och fylla i uppgifterna, i andra fall hänvisas man till en webbsida. Svara aldrig någonsin på brev där du uppmanas lämna ut lösenord. Även om Umeå universitet ibland skickar ut varningsbrev om att ditt e-postkonto kan komma att spärras så efterfrågas aldrig några lösenord. Har du fått ett phishingmail, rapportera det genast till incidentgruppen (IRT) på abuse@umu.se och inkludera det kompletta brevhuvudet. Då kan IRT låta spärra all utgående trafik till den uppgivna svarsadressen.

4.2 Servrar

I de fall där inloggning i e-postsystemet inte är möjligt, ex.vis för kopiatorer som skickar inskannade sidor som e-post, servrar som skickar status- och felrapporter etc. finns särskilda servrar för utgående e-post som skall användas. Kontakta ITS för närmare upplysningar.

Ibland vill man låta användarna skicka e-post från en webbsida. Använd i så fall tekniker som CAS-inloggning, robotfällor (captchas) och liknande som förhindrar missbruk.

Sätter man upp diskussionsforum måste man se till att inte medlemmarnas e-postadresser exponeras för utomstående. Använd gärna universitetets distributionslistesystem (Sympa).

5 Revisionshistoria

Fastställt 2010-11-30/Einar Hillbom ITS