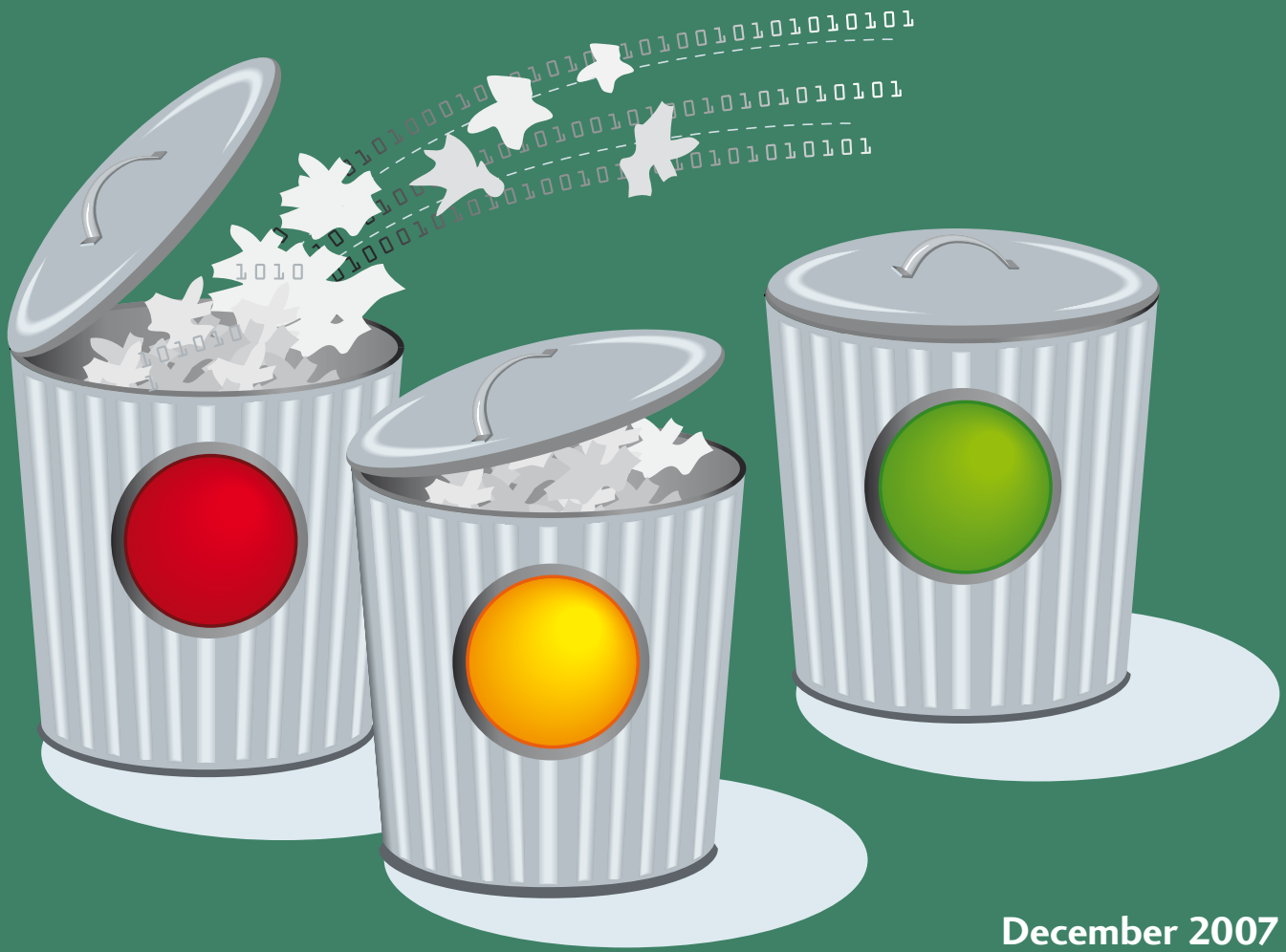
Sveriges Kommuner och Landsting

Digital sopsortering

Att hantera skräppost i kommuner och landsting



December 2007

Innehåll

Denna skrift är framtagen av IT-sektionen på Sveriges Kommuner och Landsting. I arbetet har följande personer ingått från Sveriges Kommuner och Landsting Mats Östling IT-strateg, Anders Nordh IT-strateg, Staffan Wikell förbundsjurist och Ulrika Gustafsson, arkivarie. Dessutom har Thomas Nilsson, oberoende säkerhetsexpert, Certezza AB medverkat.

ISBN: 978-91-7164-296-7
form: Ordförrådet, Stockholm
tryck: åtta.45, Solna

Inledning

Den moderna e-förvaltningen inom offentlig sektor kännetecknas av ett stort antal kommunikationskanaler och ett effektivt nyttjande av teknik.

En förutsättning för att få full effekt av IT-baserad kommunikation är att alla som berörs känner ett stort förtroende för de nya kanalerna. E-post är en etablerad och för de flesta välkänd teknik som ingår naturligt i e-förvaltningsarbetet. E-posten är dessvärre också drabbad av en hel del problem – skräppost (spam), skadlig kod (virus, trojaner, maskar, root-kit etc.) och bedrägerier (t.ex. phising). Att bekämpa skräppost och annan skadlig kod är därför ett nödvändigt men trist inslag i arbetet med att modernisera den offentliga förvaltningen.

Insatser behöver sättas in på flera olika områden. Utbildning av personal är viktig både för att minska risken att utsättas för skräppost men också för att förbättra hanteringen av skräppost i syfte att minimera problemen med att skadlig kod kommer in i IT-systemen samt att öka rättsäkerheten. Andra lösningar är en säkrare exponering av e-postadresser, nya och mer effektiva kommunikationskanaler som till stor del kan ersätta e-post samt naturligtvis tekniska lösningar för att filtrera och hantera den skräppost som strömmar in. En effektiv bekämpning av skräppost bygger på en kombination av tekniska metoder, policydokument, regelverk och personalens kunskap och medvetenhet.

Skräpposten fyller våra bredband och e-postsystem. Kostnaderna för att hantera skräppost är betydande. Trots försök med hårdare lagstiftning visar mängden skräppost inga tendenser att avta. Risken att bli åtalad för brottslighet som kan vara kopplad till skräppost är försvinnande liten och vinsterna betydande. I Sverige och inom EU är det inte tillåtet att skicka obeställd e-post till privatpersoner och i USA finns det strikta regler för massbrev (13b § Marknadsföringslagen CAN-SPAM Act). Andelen skräppost i världen har i snitt legat kring 2/3 av det totala e-postflödet det senaste året och huvuddelen, upp till 80 procent, genereras av en liten grupp professionella skräppostavsändare.

Statskontoret (numera Verva) gav i mars 2005 ut vägledningen ”Myndigheternas spamhantering 2005:5”. Vägledningen ger en bra översikt över området och en slutsats av rapporten är att varje myndighet måste göra sina egna bedömningar av vilka åtgärder och beslut som är nödvändiga mot bakgrund av myndigheternas egna förhållanden.

Varje enskild kommun och varje landsting måste därför själv ta beslut kring policy, organisation, metoder, verktyg och ansvarsfördelning.

Skräppost måste bekämpas med alla tänkbara medel utan att medborgarens möjlighet och rättighet att kommunicera via e-post med myndigheten åsidosätts. Med ett strukturerat och uthålligt arbete och ett ökat samarbete mellan olika organisationer går det att uppnå goda resultat.

I de fall där myndigheten är minst 99,99 procent säker (1 fel på 10 000) kan det vara rimligt att automatiskt avvisa skräppost förutsatt att det sker innan e-posten har inkommit och att avsändaren informeras om att e-posten avvisats och rekommenderas en alternativ kontaktväg.

Granskningen av den mottagna e-posten bör ske på samma sätt som övriga inkomna handlingar och kanske också av samma funktion inom myndigheten. Detta arbete måste underlättas med tekniska filter och automatisk sortering då en helt manuell granskning av stora mängder e-post dels blir ohanterlig dels har en betydligt större felmarginal än ett effektivt skräppostfilter. Med ett filter installerat finns också möjligheten att logga åtgärder och beslut kring gallring.

Felaktig eller skadlig e-post kan avvisas med automatik. Det gäller dels sådan e-post som inte uppfyller krav enligt SMTP-protokollet (RFC2821), dels e-post som innehåller virus, maskar, trojaner eller annat innehåll som bedöms kunna åsamka skada i myndigheternas system.

För både medborgare och personalen är det av största vikt att skräppostbekämpningen sker på ett förutsägbart och rättssäkert sätt. Ingen ska behöva känna oro över att e-post försvinner på grund av felaktig hantering.

Att bekämpa skräppost effektivt och korrekt är nödvändigt för att upprätthålla förtroendet för den offentliga förvaltningen och användningen av digitala kommunikationsformer.

Lagrummet

Offentlig sektor har att ta hänsyn till flera lagar och förordningar i bekämpningen av skräppost, vilket avhandlas grundligt i Statskontorets ovan nämnda rapport varför vi väljer att bara belysa några viktiga aspekter.

Hantering av bifogade filer

Förändringen av 5 § i förvaltningslagen (1986:223; FL) innebär att medborgaren skall kunna kontakta myndigheten med e-post. Förarbetena (proposition 2002/03:62) säger att:

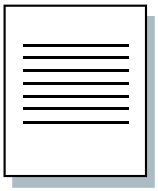
Det bör framhållas att den skyldighet som myndigheterna nu åläggs avser hantering av textmeddelanden som sänds med hjälp av e-postprogram. Någon allmän skyldighet att ta del av innehållet i bilagor till sådana meddelanden kan inte anses gälla.

- *Sådana bilagor kan nämligen förekomma i en mängd olika format.*
- *Det är inte rimligt att kräva att en enskild myndighet skall kunna hantera alla dessa.*

Kan en myndighet inte ta del av innehållet i en bilaga skall den om det är möjligt givetvis underrätta avsändaren om detta så att denne får möjlighet att sända bilagan på nytt i ett format som myndigheten kan hantera.

Begreppet textmeddelande saknar en tydlig definition. E-post kan innehålla enbart text men ofta utformas e-postbrevet med hjälp av HTML (kod som används på webbsidor) för att ge innehållet ett mer attraktivt utseende. De flesta e-postprogram kan ställas in för att antingen bara ta emot och skicka text eller för att också kunna använda HTML-formatering.

Skräppost är utformade så att de alltid innehåller mer än bara text, men det finns idag inte något stöd för att neka e-post som innehåller annat än bara ren text. Däremot kan naturligtvis ett filter ställas in så att e-post i form av rena textmeddelande släpps igenom utan kontroll, detta för att minska belastningen på filtret.



Bifogade filer kan vara av en mängd olika format. För att underlätta kommunikationen med medborgarna när det gäller bifogade filer bedömer vi att det är rimligt att kommuner och landsting kan ta emot dokumentformat som följer erkända standarder som ISO (ODF och PDF/A) och andra format som är fastställda eller rekommenderade av ansvariga myndigheter. Vartefter kan det bli aktuellt att komplettera med nya format som garanterat kan tas emot. Även ett antal vanliga bildformat liksom olika typer av textformat bör kunna hanteras. Vilka format som kommunen eller landstinget väljer att ta emot är upp till respektive organisation att avgöra. Information om vilka format som är lämpliga vid kommunikationen bör tydligt anges på kommunens och landstingets webbplats och i annat informationsmaterial. Om ett e-postmeddelande avvisas som en följd av att bilagan inte kan tas emot bör avsändaren meddelas och anvisas ett alternativ.

Det är inte acceptabelt att kommuner, landsting eller myndigheter begränsar formaten till att vara så applikationsspecifika att det behövs en viss produkt för att kunna kommunicera med myndigheten. Oavsett vilka program som används inom organisationen bör kommunikationen med medborgarna ske på medborgarens villkor så långt det är möjligt.

Gallringsbeslut

E-post som inkommer till myndigheten är i de allra flesta fall att betrakta som allmänna handlingar. För att få gallra (förstöra) en handling krävs ett beslut av varje kommunal/landstingskommunal myndighet (nämnd) som e-posten inkommer till. Man kan även välja att fatta ett generellt gallringsbeslut rörande handlingar av tillfällig eller ringa betydelse för myndigheten. Ett sådant generellt beslut skulle kunna fattas av varje kommuns/landstings arkivmyndighet. Som underlag till ett sådant beslut kan man t.ex. använda sig av bilagan till en av Riksarkivets föreskrifter (RA-FS 1997:6).

Verkställandet av gallringen ska utföras manuellt av myndigheten. Den får inte vara automatiserad, då det är en bedömningsfråga vad som ska gallras eller inte. Om IT-enheten centralt får i uppgift att verkställa beslutad gallring ställer det höga krav på förmåga att bedöma en inkommen handling och tillämpa gallringsbeslutets innehåll. Gallringsbeslutet kan även vara riktat till samtliga medarbetare som då har att bedöma om gallring av handlingar som genom sitt informationsinnehåll eller sin funktion är av tillfällig eller ringa betydelse.

Exempel på sådana handlingar:

- Inkomna eller expedierade framställningar, förfrågningar och meddelanden av tillfällig betydelse eller rutinmässig karaktär.
- Handlingar som har inkommit för kännedom och som inte har föranlett någon åtgärd, om de även i övrigt är av ringa betydelse.
- Inkomna handlingar som inte berör myndighetens verksamhetsområde, eller som är meningslösa eller obegripliga, om handlingarna inte kräver vidarebefordran till annan myndighet eller enskild för åtgärd.
- Förteckningar över avsända och mottagna e-postmeddelanden (postloggar) och fax under förutsättning att de inte längre behövs för kontroll av överföringen, och att de inte heller behövs för återsökning av de handlingar som inkommit till eller utgått från myndigheten och som skall bevaras.
- Olika former av elektroniska spår (t.ex. cookiefiler, historikfiler) som inkommit till eller upprättats hos myndigheten via Internetuppkoppling.

När gallringsbeslutet väl är fattat kan man efter granskning löpande gallra ovanstående handlingar. Granskningen kan ske på olika sätt beroende på handlingens art. E-post som med stor sannolikhet klassats som skräppost kan granskas genom att gå igenom rubriken eller ärenderaden, vid osäkerhet öppnas brevet. Handlingar där sannolikheten inte är lika stor granskas genom att brevet öppnas.

Inkommen handling

I Statskontorets rapport användes SAMSET-projektets vägledning för när en elektronisk handling skall anses vara inkommen. Elektronisk handling skall anses ha kommit in när den har nått den funktion för automatiserad behandling som myndigheten har anvisat som mottagningsställe. En elektronisk brevlåda utgör en sådan mottagningsfunktion för elektronisk post och när meddelandet har tagits emot av e-postsystemet är det inkommet, oavsett när mottagaren öppnar och läser själva brevet.

Detta synsätt ligger också till grund för denna text.

SMTP-protokollet som används för överföring av e-post har en mycket tydlig gräns för när meddelandet kan anses vara mottaget. Detta inträffar när mot-

tagarens e-postserver svarar ”250 OK” och därefter avslutar dialogen med den avsändande servern. Den e-postserver som avses är den eller de som pekats ut för den aktuella domänen och som har lägst referensnummer.

E-postmeddelande som har nekats genom sakligt motiverade skydds- och kontrollåtgärder innan den avslutande delen av SMTP-dialogen kan därför inte anses vara inkommet. Regler om bevarande och gallring enligt arkivlagen ska därmed inte tillämpas.

SMTP-dialogen och andra tekniska strukturer beskrivs senare i texten.

Avvisning av skräppost

När e-post inte tas emot bör avsändaren informeras. Om e-posten stoppas innan den betraktas som inkommen handling bör denna information ske inom ramen för SMTP-protokollet. I stället för att acceptera e-post med ”250 OK”, avbryter den mottagande e-postservern dialogen med en 5yz-kod (Permanent Negative Completion reply) till avsändarservern. I svaret går det att med automatik lägga till information om varför meddelandet inte togs emot och också hänvisa till alternativa kontaktvägar.

När det gäller bilagor som inte kan tas emot bör avsändaren meddelas och ges möjlighet att inkomma med ett annat format eller anvisas andra kontaktvägar.

Policy

En policy som beskriver hur e-post skall hanteras inom organisationen är en viktig del i arbetet. Att ta fram en policy är relativt enkelt men att få alla att omfatta och använda den är som alltid betydligt svårare. Information och uppföljning är ett långsiktigt och kontinuerligt arbete.

Exempel på frågor som en policy kan belysa:

- Exponering av e-postadresser
- Funktionsbrevlådor
- Privat e-post
- Användarens ansvar.

Dessa frågeställningar kan med fördel ingå i en mer övergripande policy för e-post och andra elektroniska kommunikationskanaler.

Exponering av e-postadresser

Kommuner och landsting har omfattande kontakter med medborgarna och har ett behov av att vara så tillgängliga som möjligt. När man av det skälet exponerar e-postadresser på sin webbplats ökar risken för att drabbas av skräppost. Det finns flera sätt att försvåra för dem som med hjälp av dataprogram samlar in e-postadresser från webbsidor. Användningen av ”mailto” funktionen bör undvikas. Mailto innebär att det i koden för webbsidan tydligt anges att det är en e-postadress, vilket gör det lätt för sökprogram att hitta och samla ihop e-postadresserna. E-postadresser kan istället beskrivas generellt genom att på webbplatsen ange att alla e-postadresser skrivs på ett visst sätt (fornamn. efternamn och sedan @organisationen.se) och att namnen finns i en lista för sig. Med hjälp av namnet på den man vill ha kontakt med kan man förstå hur e-postadressen ska skrivas. Dubbelnamn kan ibland ställa till svårigheter, så de behöver beskrivas extra tydligt.

Andra metoder är att göra om hela eller delar av e-postadressen till en bild (@ kan vara en liten bild) eller att på andra sätt göra så att e-postadresser kan tolkas av människor men är svårlästa för ett sökprogram.

En sökfunktion för e-postadresser är ytterligare ett alternativ, det underlättar för medborgarna att hitta den de söker, men gör det svårt för program som samlar in e-postadresser.

Personalen måste vara medveten om riskerna med att lämna ut e-postadress om det finns en osäkerhet kring hur mottagaren kommer att hantera dem och att inte i onödan skicka ut stora delar av sina arbetskamraters e-postadresser vid grupputskick. Personer som ofta behöver lämna ut sin e-postadress vid registrering på webbsidor skaffar ofta ett eget e-postkonto som inte används till något annat än just registrering till t.ex. nyhetsutskick, nedladdning av information och medlemskap i olika communities.

Funktionsbrevlådor

En funktionsbrevlåda är inte personlig utan kan användas av en avdelning, grupp eller en hel förvaltning/myndighet. De kan underlätta för medborgare som kan kontakta en förvaltning utan att känna till vilken person som har hand om deras ärende, men de kan också vara till hjälp när det gäller skräppost. Funktionsbrevlådor av typen forvaltning@kommun.se eller kansli@landsting.se kan minska exponeringen av e-postadresser och därmed minska den totala mängden skräppost. Funktionsbrevlådor kräver säkra rutiner för att se till att den bevakas kontinuerligt. Utan ett tydligt ansvar riskerar de att glömmas bort.

Webbformulär

Webbformulär är ett bra sätt att minskar kommunikationen med medborgarna samtidigt som det minskar skräppostarbetet. Det innebär att den som vill komma i kontakt med kommunen eller landstinget fyller i ett antal färdiga fält direkt på webbsidan (textfält, kryssrutor eller färdiga svarsalternativ) och sedan skicka in formuläret. Det gör det möjligt att kontakta organisationen från en valfri Internetuppkopplad dator utan att behöva använda ett e-postkonto. Webbformulär kan ibland vara besvärligt att använda för personer med olika funktionsnedsättningar, vilket innebär att de måste utformas så att de är tillgängliga för så många som möjligt. Om det av olika skäl inte går att använda webbformuläret bör därför alternativa kanaler anges.

Privat e-post

Den e-postfunktion som kommuner och landsting tillhandahåller till sin personal är avsedd för att användas i arbetet. Om de anställda ges möjlighet att använda sin e-postadress i begränsad omfattning för privata ändamål är det desto viktigare att de är medvetna om hur de ska använda den.

Användarens ansvar

Beroende på hur arbetet är organiserat kan användaren ibland få ta ett större ansvar för det praktiska arbetet med gallring och hantering av skräpposten. Även om det finns filter som kan sortera skräppost och lägga den i särskilda mappar innebär det inte att de kan raderas utan kontroll. Skräppost som tar sig förbi filter och hamnar i den vanliga e-postlådan ska vid gallring skickas till den som är ansvarig för filtret så att detta kan uppdateras och vartefter bli allt effektivare.

Personalen måste också vara medveten om vad skräppost är och motiven bakom utskicken. Idag står skräppost för en stor del av spridningen av virus och annan skadlig kod, så det handlar inte bara om oönskad reklam. Professionella organisationer med ekonomiska drivkrafter vill på olika sätt komma åt datorer och personliga uppgifter. Detta är ett hot mot både individen och organisationen.

Besked om varför e-post inte kommer fram

När ett e-postmeddelande eller en bifogad fil inte kan tas emot bör avsändaren informeras om detta och få reda på vilka andra sätt det finns att kontakta myndigheten. Detta svarsmeddelande skickas antingen automatiskt om skräpposten stoppas under SMTP-dialogen, eller via e-post efter det att e-posten gallrats. Automatiska e-postutskick som svar på all skräppost skulle översvämma e-postsystemet.

Många privata datorer har ofta ett sämre skydd mot virus och andra angrepp och risken är stor att legitima e-postbrev stoppas och raderas av virusskyddet utan att avsändaren är medveten om detta. Detta problem är svårare att hantera, då skadlig kod måste hindras från att nå in i verksamheten och därför stoppas eller förstörs direkt. Om e-postmeddelandet ändå når fram till mottagaren med besked att bilagan tagits bort som en följd av virussmitta, bör avsändaren om möjligt uppmärksammas på detta.

Framtidens kommunikation med medborgare och företag

E-post är bara en del av den digitala kommunikationen mellan medborgare, företag och den offentliga sektorn. Webbsidor, webbformulär, digitala blanketter och SMS är andra exempel. Nästa steg i utvecklingen av den elektroniska förvaltningen är att skapa mer sammanhållna webbfunktioner, ett slags personliga webbsidor. Genom att identifiera dig kan du som medborgare och företagare komma åt information som rör dig och ditt ärende. Hur identifieringen går till är beroende av vilken information det handlar om. E-posten spelar fortfarande en roll, kanske framför allt för att påminna dig och hålla dig uppdaterad om hur ditt ärende behandlas. Detta scenario kan öka kvaliteten på kommunikationen samtidigt som det minskar e-postanvändningen och därmed minskar risken att legitim e-post försvinner bland skräpposten. Det finns därför alla skäl att ta de steg som krävs för att förbättra dialogen med medborgarna med hjälp av moderna webblösningar.

… och så var det tekniken

RÖD: bör ej användas

GUL: tveksamt, måste kombineras med annan teknik

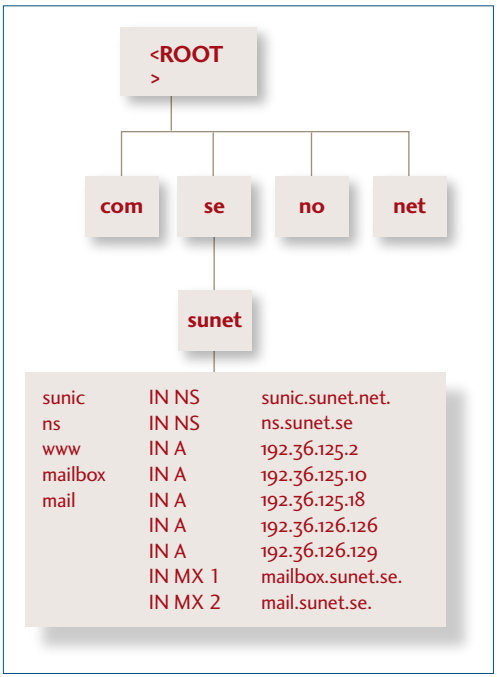
GRÖN: bör användas, åtgärder kan behöva vidtas innan användning.

DNS och SMTP

Internet och e-post vilar på ett antal tekniska byggstenar: DNS, den gigantiska databasen som håller koll på alla domäner, SMTP som är själva protokollet för att överföra e-post och MIME för att formatera breven, bifoga filer och inte minst för att hantera ÅÄÖ. Dessa byggstenar finns definierade i så kallade RFC (Request for Comments), dokument som beskriver olika standarder.

DNS (Domain Name System, RFC1034/RFC1035)

För att kunna hitta fram till rätt adress på Internet används domäner och IP-adresser. Varje domän har ett namn som är begripligt (eller åtminstone läsbart) för människor. När vi berättar för andra om webbplatser eller via länkar får reda på en webbadress är oftast domännamnet vi använder, t.ex. *skl.se*. IP-adressen är en unik sifferkombination som pekar på en viss server. IP-adressen används för att se till att e-post och alla annan Internettrafik kom fram till rätt mottagare. För att koppla ihop rätt domän med rätt IP-adress används DNS. DNS översätter domännamn till IP-adresser och viceversa. DNS bygger på en hierarkisk struktur med ett fåtal domäner i toppen och ett delegerat ansvar till underliggande domäner. De flesta toppdomäner är nationella – Sverige har tilldelats domänen .se – men det finns även ett antal allmänna toppdomäner, t.ex. *.com .org* och *.net*.



Så här ser DNS-strukturen ut för Swedish University Network (SUNET), som tillhandahåller möjlighet till datakommunikation för universitet och högskolor.

För att hitta rätt i DNS-databasen utgår man normalt från toppen och letar sig ner, tills att man når rätt namnserver (NS).

Högst upp finns ett antal root-servrar som håller reda på var namnservrarna finns för de olika toppdomänerna, exempelvis *.se*, *.com* och *.net*. Dessa har i sin tur delegerat ansvaret till

respektive underliggande domän, exempelvis *sunet.se*. Denna domän kan i sin tur innehålla ett antal underdomäner.

För leveransen av e-post är det speciellt viktig att domänen som e-brevet skall levereras till har MX-pekare (*mail exchanger*). MX-pekaren anger till vilken e-postserver som e-brevet ska levereras. Om en domän har flera MX-pekare så sker leveransen i första hand till den e-postserver som har det lägsta värdet.

Nedan är ett exempel på en domän med två olika MX-pekare. Leverans av e-brev sker i första hand till server1.domain.se

domain.se MX 2 server1.domain.se
domain.se MX 4 server2.domain.se

Det är inget krav att ha flera MX-pekare, men om man har flera ska samtliga har ett fullgott skräppostskydd.

Kontrollera den egna domänen

Det är av största vikt att er egen domän är i bästa skick. För se-domäner kontrolleras detta enklast på *http://www.dnscheck.se/*. Kontrollen ger en bild av domänen och om det behövs några åtgärder för att förbättra säkerheten.

SMTP (Simple Mail Transfer Protocol, RFC2821)

Innan ett e-postmeddelande tas emot av e-postsystemet sker en kommunikationen mellan den sändande och mottagande servern. Genom att analysera kommunikationen går det att avslöja felaktigheter som visar att e-postmeddelandet innehåller skräppost eller annan skadlig kod. Om analysen visar att e-posten innehåller skräppost eller annan skadlig kod kan transaktionen avbrytas och istället för att svara med 250 OK så skickas ett meddelande om att transaktionen har avbrutits till den avsändande servern. Det finns flera sådana kontrollstationer under dialogen. Svarsmeddelandet kan anpassas efter lokala krav och ge tydligare information om varför e-brevet inte togs emot samt vart man skall vända sig för att få mer information.

En stor del av den information som handlar om själva brevet visas inte för dig som mottagare.

1. Det första avsnittet visar envelope-delen av e-brevet (kuvertet). Här kontrolleras avsändande servers IP-adress eller namn. Även kontroller av avsändar- eller mottagaradress görs i denna del.

Envelopedelen visas normalt inte, men det kan finnas en inställning i e-postklienten för att visa den. Primärt används denna information för att e-postservrarna skall kunna skicka e-brevet vidare. Det innehåller enbart till- och frånfält för leveransändamål. Kontroller av dessa kan göras i den mottagande servern.

2. Det andra avsnittet visar header-delen (meddelande-huvudet). Här görs fler kontroller av avsändar- och mottagaradresser, dessa presenteras för mottagaren i själva e-postklienten.

Det går även att kontrollera rubrik/ärenderad eller mer avancerad information som exempelvis mottagningstider eller vilka servrar som passerats på vägen.

Meddelandehuvudet i e-brevet visas heller inte i sin helhet för användaren. Vissa valda fält som Till, Från, Datum och Rubrik presenteras i e-postklienten. Information om vilka e-postservrar som varit inblandade i leveransen av e-brevet finns i meddelandehuvudet men visas normalt inte. Informationen gör det möjligt att spåra vilken väg ett e-brev tagit för att nå fram.

Meddelandehuvudet skiljs från meddelandekroppen genom en tom rad.

3. Det tredje avsnittet visar body-delen (meddelandekroppen). Här kontrolleras innehållet i brevet och bifogade filer. Om brevet är i HTML-format är det i meddelandekroppen som själva HTML-koden ligger.

Meddelandekroppen kan formateras på olika sätt och i sin enklaste form är det bara ren text som inte innefattar de svenska tecknen Å, Ä eller Ö. För att lösa detta används MIME (Multipurpose Internet Mail Extensions). MIME bygger ut möjligheterna med meddelandekroppen så att den kan innehålla svenska teckenupsättningar men även bilagor som t.ex. multimedia.

KLIENT	SERVER
1	
	220 mail.skl.se ESMTP
ehlo testhost.skl.se	
	250-mail.skl.se 250-PIPELINING 250-SIZE 90240000 250-ETRN 250-STARTTLS 250 8BITMIME
mail from:<thomas@certezza.net>	
	250 Ok
rcpt to:<mats@skl.se>	
	250 Ok
2	
data	
	354 End data with
from: Thomas <thomas@certezza.net> to: Mats <mats@skl.se> subject: SMTP demo	
3	
Visar hur SMTP-dialogen ser ut.	
	250 Ok: queued as
quit	
	221 Bye

Automatisk hantering

Mängden skräppost kan bli helt ohanterlig för de organisationer som inte använder någon form av tekniska hjälpmedel och filter. Åtgärderna kan delas in i två steg:

1. Avvisa felaktig och skadlig e-post inom ramen för SMTP-dialogen. Denna e-post anses inte inkommen till myndigheten och behöver inte något gallringsbeslut.
2. Sortera inkommen e-post för att underlätta det fortsatta arbetet. Genom att använda olika filtertekniker kan e-posten sorteras i olika kategorier utifrån en maskinmässig värdering av sannolikheten för att det är skräppost. Denna sortering gör det möjligt att effektivisera den manuella gallringen. Målet är att på ett enkelt sätt gallra bort största möjliga mängd skräppost utan att äventyra den relevanta e-posten.

Ett flertal olika metoder måste kombineras för att ge en säker hantering

Följande beskrivning är inte heltäckande men tar upp ett antal viktiga metoder för att kunna avvisa eller sortera skräppost. Till varje metod finns det en kommentar kring lämplighet och vilka åtgärder som kan behöva vidtas för att ytterligare förbättra arbetet. Beslut om vilka metoder som kommuner och landsting tillämpar är upp till varje organisation.

Giltig SMTP-dialog

Skräppostavsändare har ofta så bråttom att få ut en så stor mängd skräppost som möjligt att de struntar i att sätta upp e-postsessionerna på ett korrekt sätt. Detta slarv kan användas för att filtrera oseriösa avsändare genom att bara acceptera tekniskt korrekt e-post.

FÖRDELAR: Mycket enkelt att införa och kräver inget underhåll.

NACKDELAR: Avsändare som använder felaktigt konfigurerade e-postservrar kan komma att påverkas.

REKOMMENDATION: Åtgärden bör kompletteras med ett felmeddelande som går till avsändaren, som därmed ges möjlighet åtgärda felaktigheterna.

Giltig avsändardomän

Kontroll av om avsändardomänen är en existerande domän. Detta görs som en del av SMTP-dialogen.

FÖRDELAR: Mycket enkelt att införa och kräver inget underhåll.

NACKDELAR: Avsändare som använder felaktigt konfigurerade e-postservrar kan komma att påverkas.

REKOMMENDATION: Åtgärden bör kompletteras med ett felmeddelande som går till avsändaren, som därmed ges möjlighet åtgärda felaktigheterna.

Giltig avsändaradress

Kontroll av om avsändaradressen följer gällande standard för utformning av e-postadresser.

FÖRDELAR: Mycket enkelt att införa och kräver inget underhåll.

NACKDELAR: Avsändare som använder felaktigt konfigurerade e-postservrar kan komma att påverkas.

REKOMMENDATION: Åtgärden bör kompletteras med ett felmeddelande som går till avsändaren, som därmed ges möjlighet åtgärda felaktigheterna.

Giltig mottagaradress

En mycket stor del av skräpposten har påhittade mottagare (eller bara en mängd slumpvisa tecken) men med korrekt domän. Kontroll kan göras av att mottagaren faktiskt existerar inom det mottagande e-postsystemet. Detta kan ske genom att använda exempelvis LDAP för att kommunicera med de aktuella kataloger som innehåller giltiga mottagaradresserna.

FÖRDELAR: Relativt enkelt att införa och kräver inget manuellt underhåll.

NACKDELAR: Vissa kataloger lagrar endast personliga e-postadresser vilket gör att e-post till funktionsbrevlådor avvisas. Viss reservation måste göras för felstavning och personer som nyligen avslutat sin anställning.

REKOMMENDATION: Metoden förutsätter att alla e-postadresser finns tillgängliga för kontroll. Undvik att använda en standardadress som tar emot all e-post som kommer till domänen.

Giltigt e-posthuvud

Utformningen av e-posthuvudet kan kontrolleras mot gällande SMTP-standard för att hitta avvikelser som tyder på att e-brevet är ogiltigt.

FÖRDELAR: Mycket enkelt att införa och kräver inget underhåll.

NACKDELAR: Tyvärr finns det ”riktiga” avsändare som har ett felaktigt e-posthuvud.

REKOMMENDATION: Med ett felmeddelande som går till avsändaren kan dessa uppmärksammas på felaktigheter och därmed åtgärda dessa.

Giltig e-postkropp

Denna kontroll söker efter avvikelser från gällande SMTP-standard i e-postkroppen.

FÖRDELAR: Mycket enkelt att införa och kräver inget underhåll.

NACKDELAR: Tyvärr finns det ”riktiga” avsändare som har felaktig e-postkropp.

REKOMMENDATION: Med ett felmeddelande som går till avsändaren kan dessa uppmärksammas på felaktigheter och därmed åtgärda dessa.

Svartlistning (blacklisting)

Svartlistning bygger på någon typ av lista med e-postservrar som inte är önskvärda. Motsatsen är vitlistning.

En enskild administratör kan underhålla en svartlista manuellt och specificera servrar som skickar stora mängder skräppost. Detta är inte speciellt effektivt utan i stället används någon eller några av de publika listor som finns. Det finns ett flertal svartlistor som är fria att använda för allmänheten och en del leverantörer av säkerhetsprodukter erbjuder prenumerationer på listor som de själva underhåller. De kommersiella svartlistorna har ofta större träffsäkerhet än de ideella.

FÖRDELAR: Stora mängder skräppost kan nekas utan att förbruka några större resurser i den mottagande servern.

NACKDELAR: Vissa e-postservrar används av så väl legitima avsändare som skräppostavsändare och båda nekas konsekvent.

REKOMMENDATION: I förarbetet till förändringen 5 § i förvaltningslagen (1986:223; FL), proposition 2002/03:62, framhålls att de åtgärder som vidtas inte får innebära att

meddelanden från en viss avsändare inte alls tas emot. Statskontorets rapport pekade ut svartlistor som en sådan åtgärd. Metoden bör inte användas av offentliga verksamheter.

Grålistning (greylisting)

Grålistning innebär att den mottagande e-postservern temporärt nekar att ta emot e-post från en okänd e-postserver. Den avsändande servern fortsätter att försöka sända brevet som efter en förutbestämd tid accepteras av mottagande server. Avsändare av skräppost brukar oftast inte vänta tills att den mottagande servern accepterar brevet, vilket medför ett visst skydd. Grålistning är en teknik som vuxit i popularitet hos skolor och universitet.

FÖRDELAR: Mycket enkelt att införa och kräver inget underhåll.

NACKDELAR: Tekniken har varit föremål för en hel del kritik eftersom avsändarna av skräppost kan modifiera sina program till att ta hänsyn till eventuell grålistning vilket får betraktas som en nackdel. Det kan också vara tveksamt att stoppa legitima brev, även om det är för en kortare tid, då förutsägbarhet är en viktig del av den offentliga verksamheten. Frågan kan komma att uppstå om när brevet egentligen inkom till en myndighet, vid första försöket eller när det släpptes igenom.

REKOMMENDATION: Metoden bör inte användas av offentliga verksamheter.

Vitlistning (whitelisting)

Vitlistning innebär att den mottagande e-postservern släpper igenom all e-post vars avsändare finns med på listan utan andra kontroller än av virus. E-post som inte finns med på listan kontrolleras och behandlas enligt uppsatta rutiner. Både användare och administratörer kan lägga till godkända avsändare till listan. Vitlistning är ett sätt att minska belastningen på skräppostfiltret. Det gör också att godkända e-postbrev kommer fram till mottagaren utan fördröjning.

FÖRDELAR: Mycket enkelt att införa och kräver litet underhåll.

NACKDELAR: Tekniken minskar inte mängden skräppost, men minskar belastningen på servrar och filter. Ställer krav på att användarna aktivt tillför avsändare till listan.

REKOMMENDATION: Metoden behöver kompletteras med åtgärder för att kontrollera e-post i övrigt.

Distributed Checksum Clearinghouse (DCC)

DCC innebär att den mottagande e-postservern granskar innehållet i ett e-postbrev och utifrån det räknar ut en kontrollsumma. Innan e-brevet levereras till den slutgiltiga mottagarens brevlåda så skickas kontrollsumman till en DCC-server. Om ett flertal andra e-postservrar har skickat in identiska eller snarlika kontrollsummor innebär det att e-brevet är ett massutskick, vilket kan indikera att det är skräppost.

FÖRDELAR: Enkel teknik för att fånga massutskick som ofta är synonymt med skräppost.

NACKDELAR: Det finns en risk att stora utskick från legitim part klassas som skräppost. E-post från större leverantörer, prenumerationer och nyhetsbrev är exempel på massutskick som några vill ha, andra inte. Dessa måste således undantas från filtrering (vitlistas) innan denna teknik tas i bruk. Skräppostavsändare kan också göra stora slumpvisa förändringar i varje enskilt meddelande som försvårar detektering.

REKOMMENDATION: Metoden måste kombineras med andra tekniker.

Bayesiansk logik

Detta är ett matematiskt teorem som med hjälp av tidigare kända faktorer kan förutse framtida händelser. Detta teorem har visat sig ge bra resultat inom skräppostbekämpning eftersom skräppostmeddelanden har en hel del gemensamma kännetecken som inte förändras över tid.

Ofta samlas ett antal ord eller teckenföljder in och klassificeras antingen positivt eller negativt. Det är en pågående process och nya teckenföljder samlas in kontinuerligt och sparas i databaser. Genom att jämföra innehållet i ett e-brev med innehållet i databaserna går det att räkna ut ett värde för sannolikheten att e-brevet är skräppost. Denna självlärande teknik kan tillämpas antingen på servernivå eller på användarnivå. En implementation på användarnivå innebär att varje användare får egna databaser med positivt och negativt innehåll beroende på vad den enskilde användaren anser vara skräppost. Detta lämpar sig bäst inom organisationer där användare har olika uppfattningar om vad som är skräppost. Användarna blir mer utsatta för skräppost under den tid det tar att träna upp varje enskild instans av filtret. En central funktion har fördelen att man inte behöver acceptera brevet ända in till användarna innan det nekas och filtret lärs upp betydligt snabbare.

FÖRDELAR: Kräver oftast minimal administration och underhållet sker automatiskt.

NACKDELAR: Olika uppfattning om vad som anses vara skräppost kan medföra att de teckenföljder som betecknas som negativa blir så många att antalet ”false positives” ökar. En implementering på servernivå kan få oönskade följder om verksamheter från flera olika branscher använder samma filter.

REKOMMENDATION: Metoden behöver kombineras med andra tekniker.

Regelbaserade filter (Heuristic filters)

Varje inkommet meddelande matchas mot vanliga kännetecken för skräppost. Det kan vara exempelvis felaktiga datum eller vissa ord eller konstiga stavningar som m0rtgage eller vlagra. Skräppostavsändare lär sig dock fort vilka kännetecken som de bör undvika vilket innebär att reglerna måste uppdateras ofta.

FÖRDELAR: Ger mycket hög träffsäkerhet för de e-brev som inte är önskvärda utifrån regelverket.

NACKDELAR: Kan kräva en omfattande administration och uppdatering och är inte speciellt effektiv.

REKOMMENDATION: Metoden är en av de sämre metoderna och måste kombineras med andra tekniker.

Signaturbaserade filter (Signature based filters)

Signaturbaserade filter prenumererar på signaturer från kända skräppostbrev. Ofta samlas dessa in av servrar på Internet som tillsammans bildar s.k. honeynets. I dessa nät behandlas flera miljoner e-brev om dagen.

FÖRDELAR: Denna typ av filter ger en minimal mängd ”false positives” dvs. e-brev som felaktigt klassas som skräppost.

NACKDELAR: Precis som med uppdateringar av anti-virusprogram kan det dröja innan nya signaturer når ut till prenumeranterna, vilket kan medföra att en del skräppost hinner slinka igenom filtret.

REKOMMENDATION: Metoden bör användas.

Fråga-svar filter (Challenge-reponse filters)

När ett e-brev inkommer från en okänd avsändare skickar e-postservern ett svar till avsändaren att denne måste registrera sig. Detta sker oftast på organisationens webbplats. När det är utfört så släpps e-brevet igenom filtret. Denna procedur behöver utföras en gång per avsändare. Avsändare av hundratusentals skräppostbrev har naturligtvis ingen möjlighet att registrera sig manuellt, de tar dessutom inte överhuvudtaget emot svarsbrev. En e-postadministratör kan genom att vitlista vissa avsändare kringgå filtret. Detta kan vara nödvändigt för t.ex. nyhetsbrev eller andra prenumerationsbrev.

FÖRDELAR: Ger ett väldigt bra skydd, det är näst intill omöjligt att få in skräppost med denna typ av filter.

NACKDELAR: Gör organisationen mer svårtillgänglig vilket kan vara ett hinder för kommunikation med medborgare. Det finns också personer som varken kan eller vill registrera sig.

REKOMMENDATION: Metoden kan inte anses vara i harmoni med 5 § i FL och bör inte användas.

SPFv1 (Sender Policy Framework version 1)

Merparten av skräpposten har en falsk avsändaradress. Ofta kan e-brevet dessutom se ut att komma från den egna organisationen. För att råda bot på detta har SPFv1 tagits fram. SPFv1 innebär att en avsändardomän har en beskrivning i sin DNS av vilka e-postservrar som är godkända att skicka brev från denna domän. Detta görs med ett TXT-record (textsträng). Det medför att organisationer med SPF-kontroll påslagen kan kontrollera om e-brevet verkligen kommer från den angivna domänen, förutsatt att den domänen har ett korrekt TXT-record. Om inget SPF-värde existerar i den aktuella domänen ignoreras denna kontroll och brevet mottas oavsett.

Nedan är ett exempel på hur en SPFv1-sträng kan se ut.

domain.tld. IN TXT ”v=spf1 mx –all”

v=spf1 Anger versionen av SPF

mx Innebär att de angivna MX-recorden för domänen är de enda som får skicka e-post från den angivna domänen.

-all Anger att inga andra hostar än de angivna är tillåtna (Hard-fail).

Hade det i stället varit ~all, innebär det i stället att funktionen testas och den kontrollerande servern får själv avgöra (Soft-fail).

FÖRDELAR: Ger ett visst skydd mot skräppost, däremot görs kontrollen enbart på domännamnsinformationen i kuvert-delen (envelope) av sessionen. Det går fortfarande att förfalska informationen i brevhuvudet (header) som tyvärr är den del som mottagaren ser i sin e-postklient.

NACKDELAR: Det är frivilligt att införa denna textsträng i DNS-strukturen och de flesta organisationer har ännu inte genomfört denna förändring. Det kan för stora organisationer också vara svårt att identifiera alla e-postservrar som används för att skicka e-post. Det kan vara lätt att glömma exempelvis utlokaliserande webbservrar som e-postar inloggningsuppgifter.

REKOMMENDATION: Metoden bör användas.

Sender ID

Sender ID är en metod från Microsoft som påminner mycket om SPF men är mer inriktad på phishingförsök än skräppost. Kontrollen görs på envelope-from adressen som i fallet med SPF och/eller på något som Microsoft kallar för Purported Responsible Adress eller PRA. PRA bestäms genom en inbördes utvärdering av följande fält i meddelandehuvudet: From, Sender, Resent-From, Resent-Sender. Det är fält som ofta visas av användarens mailklient och kan förfalskas i phishingförsök. Den resulterande adressen är gällande PRA vilken sedan kontrolleras på samma sätt som i SPF fallet. Det råder en hel del oenigheter kring Sender ID bland annat på grund av att mailinglistor enbart kan stödja detta genom att modifiera själva meddelandehuvudet och lägga till ett Sender- eller Resent-Sender-fält vilket är emot gällande standard. Microsoft har nyligen gjort tekniken SPF-kompatibel för de som redan har ett SPF-record.

FÖRDELAR: Ger ett visst skydd mot phishing.

NACKDELAR: Tyvärr stormar det mycket kring denna teknik då flera leverantörer inte säger sig stödja denna teknik.

REKOMMENDATION: Metoden bör användas med försiktighet.

DomainKeys

DomainKeys är som SPF en metod för att kontrollera om avsändaren av ett e-brev är den faktiska avsändaren. Yahoo står bakom utvecklingen av denna teknik. Det fungerar så att domänägaren skapar ett nyckelpar bestående av en privat och en publik nyckel. Den privata nyckeln används i domänens sändande e-postservrar och den publika publiceras i de berörda DNS-servrarna. När sedan ett e-brev skickas av en tillåten användare använder den utgående servern den privata nyckeln för att generera en signatur för meddelandet. Denna signatur inkluderas sedan i header-delen av meddelandet som till sist skickas till den mottagande servern.

Den mottagande servern, som också måste stödja DomainKeys, hämtar sedan den publika nyckeln från den avsändande domänens DNS. Den publika nyckeln används sedan för att verifiera att signaturen skapats av den motsvarande privata nyckeln. Observera att detta inte innefattar någon form av kryptering av själva meddelandet, utan signaturen kan enbart påvisa att meddelandet inte ändrats på vägen.

FÖRDELAR: E-brevets integritet kan verifieras och vid den händelse att det inte stämmer, sållas det bort. Detta är ett säkert skydd mot exempelvis phishing.

NACKDELAR: Relativt komplex införa.

REKOMMENDATION: Metoden bör övervägas.

Sammanfattning

Målet är att all bekämpning av skräppost ska ske med ett modernt och effektivt teknikstöd.

I de fall man är säker på att de verktyg och metoder som används kan identifiera felaktig e-post samt skräppost och annan skadlig e-post på ett säkert sätt kan e-posten avvisas och därmed betraktas som ej inkommen. Endast den e-post som följer tillämpliga standarder för DNS, SMTP, MIME etc. bör accepteras. All annan e-post bör avvisas. E-post som befaras innehålla virus, maskar, trojaner eller på annat sätt är direkt skadlig för myndigheten skall avvisas.

Viktigt är att inom ramen för SMTP-dialogen informera anändaren om att e-posten har avvisats. I den informationen har också en alternativ e-postadress angivits som kan användas i de fall avsändaren anser att gallringen skett på felaktiga grunder. Denna e-postadress har ingen filtrering eller kontroll.

Den inkomna e-posten sorteras efter sannolikheten för att det är skräppost för att underlätta granskning och gallring. Här är det viktigt att den manuella gallringen sker på ett professionellt sätt. Gallringen skall utföras av en tjänsteman som är behörig att utföra gallringen. För att säkerställa att hanteringen är effektiv och rättssäker måste ett antal tekniker kombineras.

Det fortsatta arbetet

Nya vägar

Innan lagändringar och andra omvärldsförändringar hunnit i kapp skräppostavsändarna är vi hänvisade till tekniska hjälpmedel och vårt eget omdöme. Tyvärr verkar problemen sprida sig till andra medier än e-post. I framtiden kommer säkerligen en ökning av oönskade meddelanden att ske både inom IP-telefoni och inom andra meddelandebaserade system som exempelvis SMS och MMS. Det är möjligt att detta innebär att många skräppostavsändare byter till att använda de ”nya medierna” för att få ut sitt budskap. Om detta är fallet så kanske vi får se en ökande mängd skräppost de kommande åren.

Nya metoder?

Många av de metoder som beskrivits i texten är på kort sikt effektiva för att hantera problemet med skräppost. Dock saknas långsiktiga lösningar. En långsiktig teknik som diskuterats är att varje enskild avsändare certifieras och detta certifikat skall också kunna återkallas om avsändaren missbrukar det, exempelvis genom att skicka skräppost. En lösning av detta slag skulle kanske kunna råda bot på problemet. Det skulle också underlätta spårandet av enskilda avsändare exempelvis i brottsammanhang. Men det försvårar givetvis skapandet av anonyma e-postkonton.

Flertalet tillverkare har också börjat erbjuda distribuerade nät för att samla in information om olika typer av hot som förekommer på Internet, däribland skräppost. Denna information kan en prenumerant ta del av och använda i sin filtrering av skräppost. Problemen med dessa är att det är upp till varje tillverkare att bestämma vad som kan anses vara ett hot och skräppost. Ofta är tekniken som används proprietär och det kan vara svårt att anpassa den till lokala krav men innebär ofta en minskad administration.

Nya standarder?

En ny standard för e-postleverans förespråkas av somliga men det är inte troligt att det sker inom de närmsta åren på grund av det massiva arbete detta införande skulle innebära. Andra lösningar som diskuterats är en avgift per skickat e-brev. Denna lösning skulle innebära en enorm kostnad för en skräppostavsändare men vara hanterlig för en normal organisation. Men det är inte troligt att denna typ av lösning kommer att se dagens ljus.

Nya bedragare

Så kallad phishing har börjat bli ett allt allvarligare problem. Phishing innebär att en förövare lurar användare av t.ex. en internet-bank att gå till en falsk webbsida som ofta liknar eller är en exakt kopia av originalsidan. På webbsidan lockas besökare att lämna ifrån sig sina användaruppgifter och koder. För att få offret att besöka sidan används ofta e-postmeddelanden med en länk till den falska sidan. E-brevet är ibland snillrikt formulerat och har en förfalskad avsändaradress så att det ser ut att faktiskt har skickats från den aktuella sidans e-postdomän. Ibland uppmanas bankkunder att skicka sina uppgifter via e-post. Många phising-brev innehåller dock både stavfel och grammatikfel, vilket inte hindrar mottagarna från att lämna ifrån sig sina användaruppgifter.

Ofta är det för att komma åt kreditkorts-information eller bankuppgifter som dessa brev skickas. Men ibland kan det förekomma att ett förfalskat brev skickas till någon i organisationen för att samla in lösenord till interna system eller annan information. Utbildning och information är det bästa sättet att bekämpa phishing, men även en del tekniska hjälpmedel finns att tillgå. Flertalet av de mest uppenbara phishing-breven fastnar i ett skräppost-filter. Även tekniker som SPF och DomainKeys hjälper mot dessa attacker.

Ny lagstiftning?

Förhoppning har ibland rests på att hårdare strafflagstiftning skulle skrämma många skräppostavsändare till att upphöra med utskicken. Hittills har lagstiftning inte varit en effektiv åtgärd. Ett problem är att lagstiftningen ser olika ut i olika länder. Så länge det finns starka ekonomiska intressen bakom skräppost

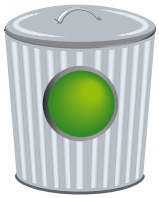
kommer det att finnas personer som är villiga att ta risken. Ska det lyckas måste sådan lagstiftning rikta sig till Internetleverantörer och andra aktörer inom infrastrukturen.

Tills vidare

Vi får alltså lita till den nuvarande tekniken och kombinera den med utbildning och information för att minska mängden skräppost och underlätta hanteringen. Så länge det finns människor som klickar på länkarna i skräpposten kommer de fortsätta att komma. Vi måste också samverka med varandra kring dessa frågor, med både informationsspridning, samverkan kring drift och gemensamma lösningar och rapportering kring olika filters effektivitet. Skräppostavsändare är påhittiga och det krävs att man håller sin filterlösning uppdaterad med den senaste tekniken från tillverkaren för att få ett fullgott skydd.

Rädslan att av misstag gallra bort viktig och relevant e-post medför att en stor andel av skräpposten hanteras manuellt. Den manuella gallringen utförs i många fall av teknisk personal som normalt inte hanterar inkomna handlingar till myndigheten. Erfarenheten pekar på att en omfattande manuell sortering inte är lika tillförlitlig som en teknisk sortering. För att uppfylla både offentlighetsprincipen och behovet av en effektiv hantering behöver därför manuell hantering kombineras med tekniska metoder.

Checklista



Att bekämpa skräpposten på ett effektivt sätt är inte enbart ett tekniskt problem, det förutsätter beslut och åtgärder på flera plan.

Beslut

Varje kommunal/landstingskommunal myndighet fattar beslut om gallring av handlingar som upprättas eller inkommer till den egna myndigheten om inte fullmäktige/landstingsfullmäktige särskilt beslutar om en annan ordning. I arkivreglementet kan man t.ex. ange att varje kommuns/landstings arkivmyndighet kan fatta generellt gällande gallringsbeslut t.ex. för handlingar av ringa betydelse.

Utbildning

Personalen utbildas så att de dels är medvetna om riskerna med e-post och vad de själva kan göra för att undvika skräppost, dels i hur de ska hantera inkommen skräppost. Förutom en korrekt gallring är det viktigt att återkoppling sker till de personer som hanterar skräppostfiltret.

Hantering

Rutiner upprättas kring hur e-post och skräppost ska hanteras. Kontroller görs kontinuerligt av att avvisning, sortering och gallring sköts på ett rättssäkert och effektivt sätt. Funktionsbrevlådor bevakas kontinuerligt.

Information

På webbplatsen finns information (t.ex. under rubriken Kontakt) om på vilka sätt man som medborgare eller företagare kan kontakta kommunen eller landstinget. Informationen beskriver olika kontaktvägar, hur mottagandet går till och på vilket sätt man kan vänta sig svar och när. När det gäller e-post kan sökfunktioner över e-postadresser eller listor över tillgänga e-postsdresser

finnas med, tillsammans med förklaringar och beskrivningar över hur man kan gå tillväga, t.ex. vilka dokumentformat som är lämpliga att använda vid e-postkommunikation.

Teknik

Ett effektivt teknikstöd är nödvändigt för att underlätta och säkerställa skräpposthanteringen. Ett antal olika tekniska lösningar behöver kombineras för att på ett säkert sätt kunna avvisa och ta emot e-post. Den inkomna e-posten filtreras för att kunna sorteras i olika kategorier så att är granskning och gallring underlättas.

Utveckling

Strategier för att flytta över e-postkommunikation till mer personliga och effektiva webbaserade lösningar tas fram. Dessa ingår i ett större arbete med att skapa ett helhetstänkande kring vilka kommunikationskanaler som ska erbjudas medborgare och företag så att alla ges möjlighet att på ett enkelt och effektivt sätt kunna kommunicera med kommunen och landstinget.

Digital sopsortering

För både medborgare och personalen är det av största vikt att skräppostbekämpningen sker på ett förutsägbart och rättssäkert sätt. Ingen ska behöva känna oro över att e-post försvinner på grund av felaktig hantering.

Att bekämpa skräppost på ett korrekt sätt är nödvändigt för att upprätthålla förtroendet för den offentliga förvaltningen och digitala kommunikationsformer.

I denna skrift belyser vi problemet samt ger ett antal råd och rekommendationer till kommuner och landsting.

Trycksaker från Sveriges Kommuner och Landsting
beställs på www.skl.se/publikationer eller på
tfn 020-31 32 30, fax 020-31 32 40.

ISBN 978-91-7164-296-7

Sveriges Kommuner och Landsting

118 82 Stockholm, *Besök* Hornsgatan 20
Tfn 08-452 70 00, *Fax* 08-452 70 50
info@skl.se, www.skl.se