2005:5

STATSKONTORET

Myndigheternas spamhantering

en vägledning kring rättsliga frågor

Förord

Den offentliga sektorn måste slå vakt om medborgarnas möjligheter att via e-post på Internet kunna sätta sig i förbindelse med myndigheterna. Under senare år har emellertid andelen s.k. spam (skräppost) i den internationella e-posttrafiken antagit alarmerande proportioner och låg under 2004 på 70-80 procent – och med en stadig ökningstakt.

Myndigheterna har att hantera balansgången mellan att vara tillgängliga via e-post men inte så tillgängliga att man dränks och därmed inte längre kan upprätthålla öppenheten. Stor osäkerhet råder om vilka åtgärder som kan och bör vidtas i den rådande situationen. Statskontoret startade därför på initiativ från Statens e-forum sommaren 2004 projektet ”Myndigheternas Spamhantering”.

I projektet har en juristgrupp uppbackad av en teknikergrupp – med representanter från totalt tio myndigheter – strävat efter att göra en heltäckande genomgång av åtgärder som är tänkbara i ett rättsligt perspektiv.

De slutsatser som redovisas i föreliggande vägledning är baserade på grundprincipen att myndighetens egen säkerhet är en förutsättning för säker kommunikation med omvärlden. Att en viss lösning för spamhantering redovisas innebär därmed inte att den rekommenderas. Varje myndighet måste utifrån sina respektive verksamheter göra egna rimlighetsbedömningar av vilka spamhanteringsåtgärder som ska tillämpas.

Generaldirektör Knut Rexed har beslutat i detta ärende. Direktör Jenny Birkestad, organisationsdirektör Olov Östberg, föredragande, och avdelningsdirektör Per-Erik Wejshammar var närvarande vid den slutliga handläggningen.

Enligt Statskontorets beslut
Olov Östberg

Innehållsförteckning

Bilagor

Sammanfattning

Problemen med spam/skräppost blir allt större. Ungefär 70 procent av all e-post hör i dag till denna kategori, och den i särklass största andelen skickas via falskskyltade servrar eller infekterade (”förslavade”) hemdatorer.

I syfte att underlätta myndigheternas spamhantering har Statskontoret i samarbete med jurister och tekniker från ett tiotal myndigheter utarbetat föreliggande vägledning avseende de åtgärder som är tänkbara ur ett rättsligt perspektiv. Vägledningen syftar till att ge en grund för de bedömningar som varje myndighet har att göra utifrån den egna verksamhetens förutsättningar. Varje myndighet bör ta i bruk de lösningar som bäst tillgodoser den egna verksamhetens krav. Ytterst är det varje myndighet som själv avgör hur lagstiftningen i fråga skall tillämpas på den egna myndighetens förhållanden.

Det för myndigheterna grundläggande problemet är att göra en avvägning mellan å ena sidan skyldigheten att vara öppen för e-postkommunikation från medborgare och företag (5 § förvaltningslagen 1986:223) och å andra sidan att inte visa sådan öppenhet att kanalen e-post slammas igen av allt skräp.

Det är t.ex. inte förenligt med öppenhetsprincipen att rutinmässigt stänga ute e-post från en ”svartlistad” server med notoriskt rykte som spridare av spam. I akuta situationer kan det emellertid vara befogat att åtminstone tillfälligt avvisa e-post från en viss server.

Med vissa undantag har det hittills varit regel att spam och virus skickas via förfalskade avsändaradresser. Den juristgrupp som ställt sig bakom vägledningen bedömer att det är en acceptabel skyddsåtgärd att avvisa sådana meddelanden med hänvisning till att det internationellt standardiserade protokollet för e-post (SMTP; RFC 2821) anger att sändande e-postserver vid kontakt med mottagande e-postserver måste presentera sig med korrekt namn som går att kontrollera i domännamnsystemet.

I alla de fall där e-post inte avvisas utanför myndighetsgränsen blir e-posten en inkommen handling, som emellertid för kategorin spam är en handling ”av tillfällig eller ringa betydelse för myndighetens verksamhet” och därför oproblematiskt kan gallras (Riksarkivets föreskrifter och allmänna råd 1991:6, ändrad 1997:6). Hur gallringen ska gå till och vilka kriterier som då skall gälla måste dock framgå av ett särskilt beslut av myndigheten i fråga.

För att underlätta hanteringen av icke avvisad spam kan myndigheten använda olika tekniker för att bedöma sannolikheten av att det rör sig om handling av tillfällig eller ringa betydelse för myndighetens verksamhet. Låg sannolikhet kan medföra att meddelandet skickas vidare till mottagande tjänsteman, medan hög sannolikhet kan medföra att myndigheten väljer att korttidslagra meddelandet inför en senare mer rationell gallring.

Vid all spamhantering är det viktigt att varje myndighet väljer hanteringsmetoder utifrån den egna verksamhetens förutsättningar. Oavsett metodval är det viktigt att myndigheten har ett dynamiskt förhållningssätt och löpande uppdaterar metoder och kriterier i takt med att spammarna ändrar sina intrångsmetoder. Exempel på generella åtgärder som kan minska mottagen spam är användning av funktionsadresser och webbformulär som officiella kontaktvägar för allmänheten istället för att exponera varje enskild tjänstemans e-postadress.

1 Projektet ”Myndigheternas spamhantering”

1.1 Spamproblemet

Möjligheten att via Internet globalt och lokalt sända och ta emot e-post har på ett genomgripande sätt förändrat samhällets kommunikationsmönster. Användandet av e-post har dock successivt blivit ett problem genom att mottagna e-postmeddelanden i allt större omfattning innehåller olika typer av virus och spam. Internationella mätningar visar att andelen av sådana skadliga och/eller förorenande e-postförsändelser hösten 2004 uppgick till cirka 70 procent av den totala e-posttrafiken.[1]

”Virus” är det för gemene man samlande begreppet på skadeframkallande och saboterande e-post. Det i Sverige dominerande otyget under november 2004 var masken ”Sober.I”, som sprider sig som en e-postbilaga och har förmågan att leta reda på alla e-postadresser i besökta datorer.

”Spam” är lite mer svårdefinierat men utgörs i regel av massutskick av påträngande och obeställda och/eller oönskade erbjudanden om tjänster och produkter av typ läkemedel, pornografi och piratkopierad programvara. Att spam existerar beror på att sändkostnaden är nära nog obefintlig och att spammaren gör bra vinster om så bara var tiotusende mottagare nappar på erbjudandena.[2] I realiteten är det en avsevärt högre andel erbjudandebrev som resulterar i beställningar – uppemot 20 procent av spammottagarna säger sig någon gång ha nappat på ett erbjudande.[3]

---

[1] MessageLabs Intelligence Annual Email Security Report 2004

[2] Leung, A., Spam – The Current State. (Tellus Corporation, August, 2003)

[3] På *http://www.bsa.org/uk/press/newsreleases/online-shopping-tips.cfm* redovisades den 9 december 2004 en internationell enkät till 1000 spammottagare i sex olika länder (”1 in 5 British Consumers Buy Software from Spam”).

”DoS-attack” (Denial of Services) är en överbelastningsattack där en enskild e-postserver bombarderas med e-post – s.k. mail-bombning – i syfte att dränka mottagarens möjligheter att upprätthålla service mot omgivningen.

Ett annat fenomen är den typ av e-post som innehåller fällor och förslag av illegal natur. Ett sådant exempel är företeelsen "phishing" (private data fishing), som innebär att e-postmottagaren luras att uppge exempelvis kreditkortsnummer.

Internetsamfundet, inklusive de stora internationella tjänsteoperatörerna för e-post, arbetar sedan många år på möjligheterna att stoppa virus och spam. Sedan ett par år tillbaka har också ett stort antal nationer instiftat antispam-lagar och utpekat övervakande myndigheter.

Den svenska lagstiftningen är baserad på ett EU-direktiv och är knutet till marknadsföringslagen (1995:450) och med Konsumentverket som övervakande myndighet. Post- och telestyrelsen har ansvar för att skadeframkallande och saboterande e-post – ”farlig spam” – hålls i schack.

I Sverige såväl som i andra länder är emellertid erfarenheterna inte speciellt goda från lagstiftningsinsatserna. I USA anses lagarna (”CAN-SPAM; opt-out”) t.o.m. ha legitimerat spammarnas verksamhet. Spamvolymen har under alla omständigheter ökat markant under senare år.

1.2 Behov av vägledning för myndigheternas spamhantering

Den offentliga sektorn måste slå vakt om medborgarnas möjlighet att via e-post kunna sätta sig i förbindelse med myndigheterna. Detta innebär bl.a. att myndigheter inte rutinmässigt kan avvisa e-postmeddelanden som med viss sannolikhet kan bedömas vara ”spam”. Å andra sidan är det en stor teknisk, ekonomisk och arbetsmiljömässig belastning att manuellt granska all anländande e-post.

Myndigheterna ska vara öppna för e-post men inte så öppna att man dränks och därmed inte längre kan upprätthålla öppenheten.

Hur ska myndigheterna hantera den uppkomna situationen? Stor osäkerhet råder rörande vilka åtgärder som får vidtas för att hindra spam, vilka säkerhetsfunktioner som får tillämpas och hur mottagen spam skall hanteras.

I syfte att underlätta myndigheternas spamhantering startade Statskontoret sommaren 2004 projektet ”Myndigheternas Spamhantering”. Projektets målsättning har varit att en juristgrupp med uppbackning av en teknikergrupp strävat efter att göra en heltäckande genomgång av åtgärder som är tänkbara ur ett rättsligt perspektiv. Att en viss lösning redovisas i föreliggande vägledning innebär därmed inte att den rekommenderas. En del av de lösningar som kommit fram vid inventeringen och som har bedömts vara mindre ändamålsenliga har begränsats till en juridisk genomlysning.

Vägledningen syftar till att ge en grund för de bedömningar som varje myndighet har att göra utifrån den egna verksamhetens förutsättningar. En sammanställning, i form av ett s.k. mind-map diagram över samtliga frågeställningar som behandlas i finns i Bilaga 1. Varje myndighet bör ta i bruk de lösningar som bäst tillgodoser den egna verksamhetens krav.

Deltagare i den för vägledningen primärt ansvariga juristgruppen har varit Hans Sundström (ordförande), Anna Björklöf och Per-Erik Wejshammar, Statskontoret, Ulla Ahlqvist, Riksarkivet, Christina Lindencrona, Konsumentverket, Elisabeth Herder, Lantmäteriverket, Jaan Entson, Försäkringskassan, Johan Bålman, Skatteverket, Per Bergstrand, Post- och telestyrelsen, Per Holmstrand, Patent- och registreringsverket, samt Fredrik Roos (sekreterare), Setterwalls Advokatbyrå.

Deltagare i den uppbackande teknikergruppen har varit Olov Östberg (ordförande och projektledare) och Wiggo Öberg, Statskontoret, Mattias Amnefelt, Kungliga Tekniska Högskolan, Åke Andersson och Bo Magnusson, Arbetsmarknadsstyrelsen,

Roger Antimon och Bengt Hägglund, Skatteverket, Ingemar Ericson, Länsstyrelsen i Västra Götaland, Mats Forsman och Ulf Lennahl, Tullverket, Björn Linderoth, Kriminalvårdsstyrelsen, Mikael Sköld och Mats-Olov Söderman, Lantmäteriverket, samt Mats Thorman, Konsumentverket.

1.3 Spamhantering som en del i en övergripande policy för e-post

Denna vägledning är fokuserad på de juridiska frågeställningarna kring hanteringen av inkommande e-post klassificerad som ”spam”. Det är uppenbart att detta område är en del av en mer övergripande policy för en myndighets användande av e-post-funktioner. En övergripande e-postpolicy kan exempelvis innehålla rutiner för:

- tilldelning och användning av e-postadresser.
- publicering av e-postadresser.
- e-post till frånvarande/semestrande tjänsteman.
- spamklassificerad[4] e-post levererad till mottagande tjänsteman.
- spamkontroll av utgående e-post.
- arkivering och diarieföring.
- e-postens integrering i ärendehanteringsprocesserna.

[4] Det är en klar tendens att spam i allt högre utsträckning skickas från äkta men ovetande sändaradresser – adresser som genom tidigare datorintrång blivit förslavade. Detta betyder att spam i allt lägre utsträckning kan stoppas med hänvisning till att avsändaren är ”falskskyltad”. Spamklassificering kan då bli det viktigaste spamhanteringsinstrumentet.

2 Särskild reglering av e-post

För myndigheterna kompliceras spamhanteringen av att reglerna om inkommande handlingar, handläggning av mål och ärenden, offentlighetsinsyn, samt arkivering och gallring, inte kan tillämpas i IT-miljö på samma enkla sätt som när reklam översänds på papper. De skyddsmekanismer som räcker i traditionell miljö är inte tillräckliga i IT-miljö. En anledning är att vanliga reklamförsändelser och liknande inte anländer i miljontal till varje myndighet. De är oftast inte heller direktadresserade till vissa tjänstemän eller adresserade till påhittade namn på handläggare. Traditionella brev med skadligt innehåll, t.ex. brevbomber, är dessutom mycket ovanliga och resulterar i betydande polisiära insatser, till skillnad från motsvarande angrepp på IT-infrastrukturen där t.ex. virus kan slå ut samhällsviktiga kommunikationer och hela myndigheters IT-miljö.

Den särskilda regleringen av e-post, virus och spam har begränsats till

1. en regel i 5 § förvaltningslagen (1986:223; FL) om att myndigheterna skall se till att det är möjligt för enskilda att kontakta dem med hjälp av e-post och att svar kan lämnas på samma sätt,
2. vissa marknadsrättsliga åtgärder för att införa ett EU-direktiv om spam i svensk rätt (se 13 b § marknadsföringslagen, 1995:450), och
3. en anpassning år 2001 av reglerna om förberedelse till brott så att vissa i 23 kap. 2 § brottsbalken (BrB) angivna förfarandena kriminaliserats även med avseende på skadlig kod.[5]

Enligt motiven till regeln i 5 § FL om skyldighet att kommunicera via e-post framstår det som angeläget att det införs en otvetydig skyldighet för myndigheterna att erbjuda medborgarna en kontaktmöjlighet med hjälp av moderna kommuni-

[5] Ang. förberedelse, se prop. 2000/01:85 s. 41 och 92.

kationsmedel och att detta bör ske genom ett ”uttryckligt åliggande för förvaltningsmyndigheterna och domstolarna”.[6]

Åläggandet för myndigheter att låta sig kontaktas via e-post har haft avsedd verkan; myndigheterna följer lagen. Någon gynnsam effekt av de andra lagstiftningsåtgärderna, som syftade till att hindra spam och virus, har däremot inte märkts. Missbruket har i stället ökat så att det vuxit fram en ”miljardindustri” för filtrering m.m. Utan de programvaror och tjänster som nu finns på området skulle missbruket av e-post sannolikt helt slå ut denna kanal som kommunikationsväg för seriösa aktörer.

[6] Se prop. 2002/03:62 s. 11.

3 Hantering av e-post och spam

3.1 Förutsättningar

För att resonemanget i denna vägledning skall bli enklare att följa behandlas frågorna i detta avsnitt huvudsakligen utifrån två förutsättningar nämligen

- att e-posten är adresserad till en myndighet eller till någon enskild anställd på dennes myndighetsadress, och
- att åtgärderna för att motverka spam vidtas med hjälp av en dator i myndighetens lokaler, av myndighetens egen personal.

Dessutom görs en åtskillnad mellan de åtgärder som

1. hindrar mottagande av e-post (så att e-posten aldrig *överförs* till myndighetens e-postserver), respektive
2. hanterar e-post som nått fram till myndighetens e-postserver (så att inkomna spam gallras på ett effektivt sätt).

Skillnaden mellan meddelanden som inte överförs (1) respektive överförs (2) blir betydelsefull om gällande rätt, i det förra fallet, generellt kan tolkas så att meddelandena inte har kommit in till myndigheten; varken enligt FL eller enligt tryckfrihetsförordningen (TF). Rättsläget belyses i avsnitt 3.2 Tidpunkt för inkommande.

3.2 Tidpunkt för inkommande

3.2.1 Inkommande handlingar enligt Tryckfrihetsförordningen

TF innehåller bestämmelser rörande inkommandetidpunkten vid prövningen av en fråga om offentlighetsinsyn. TF:s regler om

förvaring och inkommande är avgörande även för tillämpningen av sekretesslagen (1980:100; SekrL) och arkivlagen (1990:782).

Enligt huvudregeln för *pappers*miljö anses en handling vara inkommen när den har ”anlänt till myndigheten” (2 kap. 6 § TF), vilket normalt innebär att den skall ha kommit till myndighetens lokaler, dvs. befinna sig inom myndighetens väggar. Denna förvaringsprincip är emellertid i IT-miljön modifierad med en tillgänglighetsprincip, enligt vilken en upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel anses inkommen till myndighet när annan har gjort den tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (2 kap. 6 § jämförd med 3 § TF).[7]

Enligt TF är det alltså möjligheten att läsa, avlyssna eller på annat sätt uppfatta en upptagnings informationsinnehåll som avgör om den skall anses förvarad och inkommen i TF:s mening.[8]

Vid ett införande av hinder mot överföring av e-post som inte följer standard för format eller som stoppas till följd av att de innehåller skadlig kod och liknande aktualiseras frågan om

- sådana meddelanden skall anses tillgängliga för adressaten i TF:s mening, även om en överföring till mottagarens e-postserver hindrats, och
- ett införande av hinder mot överföring av meddelanden står i strid med 2 kap. TF.

Dessa frågor gäller hur myndigheternas ”yttre gränser” skall bestämmas från offentlighetssynpunkt. Några uttalanden i motiv eller doktrin som tar sikte på skyddsrutiner rörande virus eller spam i detta sammanhang torde inte finnas.

---

[7] En sammanställning av uppgifter ur en upptagning anses dock förvarad hos myndigheten endast om myndigheten kan göra sammanställningen tillgänglig med rutinbetonade åtgärder.

[8] Se SOU 2001:13 s. 153 samt prop. 2001/02:70 s. 25.

Det är upp till varje myndighet att utifrån sina egna förutsättningar bestämma vilka tekniska begränsningar som skall finnas i myndighetens system, t.ex. med avseende på skydd mot intrång och andra missbruk. De hinder och men som uppkommer för myndigheterna till följd av floder av spam och brottsliga angrepp, som stöds av manipulerade domänadresser och skadlig kod, utgör skäl för tekniska begränsningar av tillgängligheten.

Juristgruppen har ansett att det skulle föra med sig orimliga konsekvenser för det allmänna om offentlighetsprincipen skulle anses hindra nödvändiga åtgärder för att skapa och vidmakthålla fungerande och säkra e-postsystem. Detta blir särskilt påtagligt i fall där avsändarna vidtar aktiva åtgärder för att genomföra otillåtna utskick eller brottsliga angrepp. Här bör även beaktas att TF:s bestämmelser om allmänna handlingars offentlighet har utformats med tanke på pappersbaserade försändelser.

Som juristgruppen ser det innebär reglerna i 2 kap. TF att e-post inte anses inkommen till en myndighet om meddelandet inte är tillgängligt för myndigheten till följd av sakligt motiverade skydds- och kontrollåtgärder. Meddelandet blir nämligen inte tillgängligt för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att det kan läsas, avlyssnas eller på annat sätt uppfattas. I enlighet med denna bedömning blir reglerna i arkivlagen om bevarande och gallring, se vidare avsnitt 5.1 Allmänt nedan, inte tillämpliga på sådana meddelanden.

3.2.2 Inkommande handlingar enligt förvaltningslagen

Reglerna om inkommande handlingar i 33 kap. 3 § rättegångsbalken (RB), 44 § lag (1996:242) om domstolsärenden (ärendelagen), 44 § förvaltningsprocesslagen (1971:291; FPL) och 10 § FL är i sak samordnade. Huvudregeln enligt nämnda bestämmelser är att en handling skall anses inkommen den dag då ”handlingen anländer till myndigheten”. Av hänsyn till arbetets behöriga gång behöver dessa regler kunna tolkas enkelt och snabbt.

Olika lösningar tas upp i lagmotiv och doktrin. Rättsläget är oklart. Här bör beaktas att bestämmelserna har tillkommit med tanke på vanliga pappersbaserade försändelser.

En ”Vägledning för service och hantering av inkommande handlingar, m.m.” har i det s.k. SAMSET-projektet[9] utarbetats i samverkan mellan Skatteverket, Riksförsäkringsverket, Patent- och registreringsverket, Bolagsverket och Statskontoret. Vägledningen har överlämnats till Nämnden för elektronisk förvaltning (e-nämnden) för ställningstagande och publicering. I den utarbetade vägledningen har regeln om inkommande handlingar tolkats så att en elektronisk handling skall anses ha kommit in när den har nått den funktion för automatiserad behandling som myndigheten har anvisat som mottagningsställe (mottagningsfunktionen)[10]. Den tolkningen innebär att ett meddelande inte bör anses inkommet om meddelandet

1. sänts till
   a. fel elektronisk adress,
   b. rätt adress men med fel anrop eller format,[11] eller

2. hindrats till följd av sådana skydds- och kontrollåtgärder som behandlingar i brandväggar, virusprogram eller intrångsdetekteringssystem.[12]

En förutsättning för denna bedömning är emellertid att myndigheternas system verkligen har konfigurerats så att meddelandena inte når fram till den funktion för automatiserad behandling som

---

[9] SAMSET-projektet har haft ett regeringsuppdrag att under ett inledningsskede ansvara för administrationen av elektroniska ID-handlingar (e-legitimationer) för elektronisk identifiering och elektroniska underskrifter inom statsförvaltningen. Här ingår såväl juridiska som tekniska och ekonomiska frågor. De senare handlar främst om hur medborgare och företag kan förses med e-legitimationer och om hur dessa finansieras.

[10] Mottagningsfunktionen utgör en form av elektronisk brevlåda hos myndigheten för att ta emot elektronisk post.

[11] Se Vägledning för service och hantering av inkommande handlingar, m.m. avsnitt 3.5.

[12] Se Vägledning för service och hantering av inkommande handlingar, m.m. avsnitt 3.6.

myndigheten har anvisat som mottagningsställe (mottagningsfunktionen). Utgångspunkten för detta resonemang har varit en *förvaringsprincip* som i korthet innebär att data som representerar meddelandet anses inkomna när de har nått mottagningsfunktionen.

Med anledning av de komplikationer som kan uppkomma vid kontroller som utförs av säkerhetsskäl anförs följande i en kommentar till vägledningen:

”Låter en myndighet ”intelligenta” brandväggar, t.ex. s.k. intrångsdetekteringssystem ”öppna” meddelanden av systemsäkerhetsskäl, bör meddelandet inte anses inkommet redan till följd av denna åtgärd. Detta bör gälla även om åtgärden sker i den dator där myndighetens mottagningsfunktion körs, om meddelandet stoppas eller behandlingarna fallerar på annat sätt, innan handlingen registreras i mottagningsfunktionen. Meddelanden som t.ex. har felaktigt format eller innehåller ett virus och därför ”fastnar” eller ”rensas bort” genom de automatiska skydds- eller kontrollåtgärderna skall därför inte ses som inkomna, även om de faktiskt har lagrats i myndighetens system, t.ex. i en logg över intrång eller en ”karantän” för virusinfekterade meddelanden. Detta synsätt kan jämföras med vissa typer av kontroller av vanlig post som sker innan en försändelse når fram – t.ex. ett s.k. hundsök för att finna narkotika, sprängämnen eller andra skadliga eller otillåtna ämnen i brev och paket. Detsamma bör gälla för virussmittade elektroniska försändelser som stoppas eller raderas. I den mån det kan ske med rutinbetonade åtgärder bör enskildas rättssäkerhet dock tillgodoses och myndighetens serviceskyldighet uppfyllas genom tydliga felmeddelanden och uteblivna kvittenser.”

SAMSET menar således att ett e-postmeddelande inte är att anse som inkommet om det av säkerhetsskäl stoppas under sändningen. Juristgruppen delar denna uppfattning. Eftersom de kontroller som sker av e-post och den kontroll som sker av brev och paket båda utförs av säkerhetsskäl torde samma synsätt kunna tillämpas på e-postmeddelanden. Dagens genomdatoriserade myndighetsvärld, med e-tjänster och kommunikation via nät

av handlingar som aldrig skrivs ut, förutsätter att en handling inte skall behöva skrivas ut för att anses som inkommen.[13]

Oklara eller otidsenliga bedömningar kan bli kännbara för användare som önskar ta tillvara sin rätt och för myndigheter som skall bygga sina system så att de blir förenliga med regler om service, inkommande och handläggning av mål och ärenden. För ingivarna är det ett självklart rättssäkerhetskrav att myndigheterna inte i enskilda fall skall kunna förfoga över inkommandetidpunkten genom att t.ex. vänta med att läsa eller skriva ut en elektronisk inlaga och såväl ingivare som myndighet behöver veta i vilka delar befordran sker på avsändarens respektive mottagarens risk.

En förvaringsprincip synes vidare bäst kunna uppfylla kraven på förutsägbarhet och rättssäkerhet i rättstillämpningen. Enligt en genomgång av doktrinen på området synes det även finnas tolkningsteorier som kan beskrivas som en tillgänglighetsprincip, en utskriftsprincip och en läs- eller omhändertagandeprincip. Dessa synsätt är dock inte anpassade till dagens användning av e-post, bl.a. eftersom de kan göra det möjligt för myndigheten att i enskilda fall förfoga över vilken tidpunkt som en handling skall anses som inkommen.

3.3 Tekniska förutsättningar för kommunikation genom e-post

Internet och e-post har på ett genomgripande sätt förändrat vårt sätt att kommunicera. Genom att ange en adress kan användare över hela världen sända och hämta meddelanden. För detta ändamål tilldelas varje e-postserver en adress för sin s.k. *domän*. Denna adress består av ett s.k. IP-nummer.[14] Till IP-numret

[13] Jfr annorlunda uppfattning Hellners, Trygve; Malmqvist, Bo, Förvaltningslagen med kommentarer s. 122, 2003.

[14] En IP-adress (även kallat IP-nummer) är i likhet med telefonnummer en numerisk adress som används av Internet-protokollet (IP). IP version 4, som dominerar idag, använder IP-adresser som består av 32 bitar eller 4 oktetter.

kopplas ett domännamn (t.ex. ”myndigheten.se”) för att Internet skall kunna ges en användarvänlig utformning.[15] När denna domänadress kompletteras, så att en viss elektronisk brevlåda pekas ut, blir det en e-postadress (t.ex. registrator@myndigheten.se).

Den generellt tillämpade standarden för e-post, Simple Mail Transfer Protocol (SMTP), innehåller ett flertal standardiserade funktioner som innebär att ett e-postmeddelande inte sänds förrän vissa kontroller har utförts och utfallit positivt. Om dessa funktioner tillämpas och det uppträder brister stannar det vid en s.k. handskakning[16] mellan sändande och mottagande dator och tillhörande kontroll av de tekniska förutsättningarna för själva överföringen. En närmare genomgång och rättlig analys av de tekniska leden följer nedan i avsnitt 4 Åtgärder för att hindra mottagande av spam.

Som exempel kan nämnas att det visar sig att den sändande serverns adress och/eller den avsändande e-postadressen förfalskats; något som är vanligt vid spam och virussmittade meddelanden. Åtgärder i enlighet med standardiserade rutiner för att hindra sådana fel i försändelser bör inte, enligt det synsätt som redovisats i föregående avsnitt, leda till att försändelsen anses inkommen enligt 10 § FL (förvaltningsärenden eller annan förvaltningsverksamhet).

Dessa brukar skrivas decimalt, oktett för oktett, med punkter emellan, till exempel 193.15.191.196.

[15] Vanliga namn på personer och organisationer kan därmed användas för adressering, i stället för långa sifferkombinationer. Översättningen mellan domännamn och IP-nummer hanteras av det s.k. domännamnssystemet (DNS). Domännamnen registreras genom ett särskilt förfarande och består – såvitt avser hanteringen av e-post – av det som står efter @-tecknet i en e-postadress; t.ex. ”@myndigheten.se”.

[16] Med handskakning avses en funktion som innebär att sändande och mottagande utrustning utbyter styrsignaler för att anpassa sig till varandra och underrätta varandra om att de är redo att sända respektive att ta emot.

3.4 Serviceskyldigheten enligt 5 § förvaltningslagen

Den serviceskyldighet som åläggs myndigheterna genom 5 § andra stycket FL kan enligt juristgruppens mening inte innebära att det finns en skyldighet för myndigheter att utforma sina system så att de är vidöppna, dvs. att samtliga försändelser måste tas emot, om meddelandena t.ex. utformats i strid mot funktioner i standarden för e-post (SMTP) och kan antas utgöra farliga försändelser. Det kan inte rimligen ha varit lagstiftarens avsikt att kräva att myndigheterna skall åsidosätta befogade säkerhets- och kontrollåtgärder och därigenom medverka till en försämring av anställdas arbetsmiljö.[17] Myndigheten bör alltjämt anses tillgänglig via e-post så länge de standardiserade rutinerna för sådan kommunikation följs.

Av motiven till bestämmelsen i 5 § FL framgår dessutom att det åligger myndigheterna att vidta de åtgärder som erfordras från säkerhetssynpunkt för att myndigheterna skall kunna uppfylla sin skyldighet att vara tillgängliga för allmänheten per e-post.[18] Saknas virusskydd eller hindras myndigheterna från att skydda sina system från intrång, genom meddelanden med falska uppgifter om avsändardomän, är risken uppenbar att den föreskrivna tillgängligheten via e-post inte kan upprätthållas för icke-manipulerade försändelser som innehåller handlingar som rör myndighetsärenden.

Det är vidare en grundläggande princip att försändelser till myndigheter går på avsändarens risk. Det torde inte ens av rättssäkerhetsskäl kunna krävas att en myndighet skall ta emot farliga försändelser. Myndigheterna skall vidta de åtgärder som erfordras från säkerhetssynpunkt. Sker inte det är risken uppenbar att de inte kommer att kunna uppfylla sin skyldighet att vara tillgängliga via e-post.[19]

---

[17] Här bör även beaktas att problemet och diskussionen kring spam inte var aktuell vid tidpunkten för lagstiftningsarbetet.

[18] Se Ds 2001:25 s. 20 och prop. 2002/03:62 s. 10-14 och 19f.

[19] Jfr Ds 2001:25 s. 20.

4 Åtgärder för att hindra mottagande av spam

4.1 Allmänt

Det har vuxit fram en ”miljardindustri” för filtrering och klassificering av virus och spam. Utan de programvaror och tjänster som nu finns på området skulle missbruket av e-post sannolikt helt slå ut denna kanal som kommunikationsväg för seriösa aktörer. Kriterierna för filtrering och klassificering kan gälla form, innehåll och transportvägar, och måste uppdateras i takt med att attackerare och spammare ändrar taktik. Sådana kontrolltekniker är värdefulla men måste användas med urskiljning.

Leder motiverade tekniska åtgärder till att överföringen av en försändelse hindras eller stoppas är försändelsen – enligt den bedömning som redovisats i avsnitt 3.2.1 Inkommande handlingar enligt Tryckfrihetsförordningen och avsnitt 3.2.2 Inkommande handlingar enligt förvaltningslagen – inte att anse som inkommen till myndigheten enligt TF och inte heller enligt FL. Åtgärderna får emellertid inte strida mot serviceskyldigheten i 5 § FL eller utgöra en risk för att e-postmeddelanden från enskilda rörande myndighetsärenden stoppas.

Bilaga 2 innehåller en närmare redovisning för möjligheterna att med hänvisning till e-postprotokollet SMTP hindra mottagande av spam.

4.2 Kontroll av förfalskade adresser

Cirka 200 ”spamgäng” bedöms svara för 80 procent av dagens spam.[20] Delstaten Virginia, USA, dömde i november 2004 en av

[20] Databasen The Register of Known Spam Operations (ROKSO) listar professionella spammare som till följd av överträdelser mot spamförbud minst tre gånger har förbjudits använda tjänsterna hos Internet Service Providers.

de värsta spammarna till 9 års fängelse. Av bevisningen framgick att spammaren ifråga rutinmässigt förfalskade information om vem som var spamavsändare och vilka vägar spammet skickats till mottagarna.[21]

Förfalskade avsändaradresser har i många år varit ett av kännetecknen för spam. En åtgärd för att hindra mottagande av sådan spam kan utgöras av t.ex. kontroller i enlighet med den internationella standarden för sändande och mottagande av e-post (SMTP; RFC 2821, [22] "Protokollet").

Kommunikationen med e-postservern skall, om systemen är konfigurerade i enlighet med Protokollet, begränsas till en handskakning mellan sändande och mottagande dator samt kontroller av de tekniska förutsättningarna för överföringen. Dessa kontroller leder till att e-postmeddelanden inte överförs om fel föreligger.

Här bör uppmärksammas att Protokollet – om överföringen stoppas – ålägger den sändande e-postservern att skicka ett felmeddelande till angiven avsändare och att möjligheter finns för en myndighet att till ett sådant felmeddelande lägga anvisningar om alternativa vägar att ge in en handling elektroniskt.

Därmed återstår den ovan i avsnitt 3.4 Serviceskyldighet enligt 5 § förvaltningslagen berörda diskussionen om sådana begränsningar är förenliga med 5 § andra stycket FL och motsvarande syn på service och rättssäker kommunikation. Som exempel på kontroller enligt Protokollet, som bör kunna godtas även om brister leder till att ett meddelande inte överförs, kan nämnas granskning av huruvida uppgiften om den avsändande serverns adress är falsk. Sådana manipulationer sker regelmässigt vid attacker mot informationssäkerheten och vid spridning av spam. Risken är att en myndighet som hindras från att skydda sina system från angrepp genom meddelanden med falska uppgifter

[21] ”Spammer Sentenced to Nine Years in Jail”, Computerworld, November 05, 2004.

[22] RFC2821; dvs. Request For Comments. Ett RFC-dokument utgör en standard som beskriver protokoll, systems eller procedurer för Internet.

om avsändande server inte tillräckligt effektivt kan värna sig från angrepp och därmed, i vart fall periodvis, kan mista sin förmåga att ta emot icke-manipulerad e-post. Åtgärder för att hindra e-postmeddelanden bör därför i många fall anses motiverade av säkerhetsskäl på samma sätt som åtgärder som hindrar mottagande av t.ex. virus.

Ett mer svårhanterligt problem är att virus och spam i allt större utsträckning skickas från ovetande ”förslavade datorer”, varvid avsändaradressen visserligen är manipulerad men ändå inte falsk.

4.3 Okänd mottagare

Som en följd av rutinerna för vanlig postgång kommer ”pappers-post” fram till myndigheten så länge rätt boxnummer är ifyllt, oavsett om den handläggare som posten är adresserad till existerar eller inte. En sådan analogi är dock inte lämplig för e-post, dels på grund av att möjligheten finns att kontrollera om den adresserade mottagaren existerar innan e-posten kommit in, dels på grund av väl övervägda och internationellt förankrade tekniska regler och rutiner för behandlingen av e-post. Dessa regler finns i Protokollet (se Bilaga 2). En konsekvens av reglerna i Protokollet är t.ex. att den e-postserver som tagit emot ett meddelande (från en e-postklient i det egna nätverket eller från en annan e-postserver) och inte lyckats sända det vidare är skyldig att kontakta avsändaren.

Denna regel utnyttjas av spammare genom att med en förfalskad avsändaradress sända spam till en förfalskad mottagaradress, t.ex. påhittatnamn@myn-digheten.se. Om den e-postserver myndigheten använder skulle ta emot e-post-meddelandet och därefter upptäcka att det inte går att leverera meddelandet till en e-postklient måste e-postmeddelandet sändas tillbaka till avsändaren. Eftersom avsändarens adress också är förfalskad innebär detta då att e-postmeddelandet inte sänds tillbaka till avsändaren utan att myndighetens e-postserver sprider spam till en tredje part. Dessutom skulle e-postmeddelandet vara att anses som inkommet hos myndigheten.

Någon skyldighet att ta emot feladresserade e-postmeddelanden följer inte av 5 § FL och inte heller av Protokollet. Åtgärder för att hindra sådana e-postmeddelanden torde kunna anses motiverade av säkerhetsskäl innan de anses inkomna enligt FL eller TF.

Risken att en enskild vid försök att ge in en handling till myndigheten stavar fel på handläggarens namn eller försöker skicka e-post till en handläggare som slutat vid myndigheten bör naturligtvis beaktas. Det bör dock uppmärksammas att den enskilde då, i enlighet med Protokollet, skall få ett felmeddelande från den sändande e-postservern eftersom e-postmeddelandet aldrig går fram; jfr det fallet att den enskilde stavar myndighetens domännamn felaktigt eller att en enskild ger in en handling via fax men slår fel nummer (då är det inte ens säkert att något felmeddelande genereras). I praktiken är många myndigheters e-postservrar redan idag uppsatta så att sådana meddelanden studsar tillbaka. En ändring skulle innebära att problemet med spam förvärrades ytterligare.

Myndigheten bör överväga att upprätta rutiner för hur e-postmeddelanden som är adresserade till handläggare som slutat eller är tjänstlediga, eller till namn som är snarlika med vid myndigheten anställda handläggare, skall tas emot.

4.4 Till mottagare med annan domän

Vid sändande av spam är det vanligt att inte bara sändande utan även mottagande adress är förfalskad, dvs. den uppgivna mottagarens e-post skall rätteligen sändas till en annan domän. Det är då uppenbart att uppgiften om mottagare är förfalskad, t.ex. om e-postmeddelandet är adresserad till tjansteman@påhittaddomän.se men den sändande e-postservern ändå anropar myndighetens e-postserver och försöker leverera det till tjansteman@myndigheten.se. E-post-meddelandet bör då anses utgöra en säkerhetsrisk.

4.5 Kontroll av teckenuppsättning

I samband med handskakningsprocessen mellan sändande och mottagande e-postserver är det möjligt att kontrollera vilken teckenuppsättning som används i e-postmeddelandet – innehållet i datadelen anges av ett underliggande protokoll ”MIME-protokollet” som talar om vilket format data i e-postmeddelandet har.

Det varierar mellan olika sändande e-postservrar när i handskakningsprocessen denna information sänds. Informationen från MIME-protokollet torde dock i vilket fall tas emot innan e-postmeddelandet anses inkommet till myndigheten enligt TF och FL enligt resonemanget ovan. Myndigheten bör under åberopande av säkerhetsskäl kunna stoppa e-postmeddelanden om MIME-protokollet anger att e-postmeddelandet bygger på ett format som är klassat som en säkerhetsrisk, exempelvis om ett e-postmeddelande innehåller en teckenuppsättning som är oläsbar för myndigheten och känd för att innehålla virus.

4.6 Svartlistning

4.6.1 Spärr av vissa avsändare

Flertalet kommersiella spamfilter erbjuder möjligheten att stänga ute e-postmeddelanden som sänts från vissa e-postadresser, även om dessa inte är felaktiga på det sätt som beskrivits ovan. Mot denna typ av åtgärd, s.k. ”svartlistning”, kan ett uttalande i lagmotiven till 5 § andra stycket FL åberopas. Där uttalas (prop. 2002/03:62 s. 12) att:

”*I sammanhanget skall också framhållas att den ökande användningen av e-post förstärker behovet av att myndigheterna anpassar sina säkerhetssystem så att de kan skydda sig mot s.k. datavirus och andra systemangrepp. Även riskerna för s.k. mailbombning måste beaktas. Det skall dock framhållas att de åtgärder som vidtas givetvis inte får innebära att särskilda katego-*

rier av e-post spärras, så att t.ex. meddelanden från en viss avsändare inte alls tas emot."

Regeringen torde härigenom dock inte ha avsett att förbjuda myndigheterna att stoppa överföringen i samband med pågående angrepp, utan endast att generella stopp utan en aktuell hotbild inte godtas. Det torde därför inte finnas hinder mot att tillfälligt stänga av en viss sändande e-postadress *under ett pågående angrepp*. Om en myndighet blev utsatt för försök att sätta eld på byggnaden, genom att någon stoppar in brinnande föremål genom brevinkastet, skulle myndigheten kunna stänga brevinkastet till dess skyddsåtgärder vidtagits eller hotet annars avvärjts, utan att detta skulle anses strida mot serviceskyldigheten eller den processuella regleringen. På motsvarande sätt måste en myndighet kunna hindra meddelanden som innehåller skadegörande program eller sänds i sådan omfattning att systemet kan bli obrukbart eller allvarligt störas genom överbelastning.

Det får bedömas från fall till fall hur länge en spärr av en IP-adress kan anses motiverad av säkerhetsskäl.

4.6.2 Spärr av vissa e-postservrar

En s.k. "svartlistning" kan även användas för att stänga ute e-postmeddelanden som sänds från en viss e-postserver (som kan betjäna många användare). En följd av motivuttalandet till 5 § andra stycket FL är att "svartlistning" som används av traditionella spamfilter för att hindra mottagande av e-post inte får användas. Genom ett sådant förfarande blockeras servrar som tidigare sänt stora mängder spam mer eller mindre permanent. Anledningen till att en sådan åtgärd skulle strida mot 5 § FL är att en e-postserver som klassats som spamsändande kan användas av många olika användare och att en permanent blockering av en sådan server hindrar e-postmeddelanden även från den som försöker kontakta myndigheten i mål och ärenden. Enligt ett ut-

talande av JO bedöms det vara olämpligt att rutinmässigt använda marknadens svartlistningstjänster.[23]

Enligt juristgruppen torde däremot, på motsvarande sätt som enligt resonemanget för spärr av e-postmeddelanden från vissa e-postadresser, en sändande e-postserver[24] kunna spärras tillfälligt för att – när angrepp sker – stänga ute meddelanden. En förutsättning är att angreppet är sådant att det inte räcker att stänga ute en viss e-postadress och att en aktuell hotbild och säkerhetsrisk föreligger.

4.7 Orimligt stora e-postmeddelanden

I traditionell miljö är det en självklarhet att paket och brev som är för stora inte kan läggas i myndighetens brevinkast. Ställs sådana utanför myndighetens dörr och kommer de bort innan de omhändertagits av myndighetens personal och förts in i lokalerna[25] anses de inte vara inkomna och myndigheten har heller inte förfarit felaktigt.

På motsvarande sätt bör gällande rätt tolkas så i IT-miljö att en myndighet inte är skyldig att ta emot orimligt stora försändelser. Något exempel har inte uppmärksammats där de skyddsintressen som åberopas till stöd för att e-post skall kunna tas emot kan anses omfatta försändelser som är osedvanligt stora. Riskerna från informationssäkerhetssynpunkt skulle bli betydande om myndigheterna tvingades att ha mottagningsfunktioner som snabbt, genom en enda försändelse, kunde fyllas så att andra meddelanden inte kan tas emot eller så att systemet upphör att fungera. Det bör vara upp till varje myndighet att, utifrån sina egna förutsättningar, avgöra hur stora e-postmeddelanden som

[23] Anmälan mot Uppsala läns allmänna försäkringskassa om att en försäkrad har nekats möjligheten att kommunicera med kassan med e-post (JO Dnr 4804-2003)

[24] Den sändande e-postservern identifieras och spärras genom sin IP-adress, vilken den mottagande e postservern kan kontrollera och som inte heller går att förfalska.

[25] Eller från den tidpunkt försändelsen omhändertas för den händelse den som utför åtgärden är en behörig handläggare.

skall tas emot. En sådan gräns får dock inte sättas alltför lågt, det är rimligt att medborgare skall kunna bifoga försändelser som t.ex. skannade dokument. Myndigheten bör informera om sådana begränsningar, t.ex. på sin webbplats.

Det bör även i detta sammanhang uppmärksammas att sändande e-postserver i enlighet med Protokollet har en skyldighet att meddela avsändaren att meddelandet inte gick fram och att myndigheten har möjlighet att, utan att svara avsändaren med ett e-postmeddelande, under handskakningsprocessen med den sändande servern informera avsändaren om varför meddelandet inte kunde komma fram och ge förslag till alternativa vägar att kontakta myndigheten.

4.8 Farliga försändelser

Brevbomber är farliga, men lyckligtvis mycket ovanliga. Skadlig kod och mailbombning har däremot blivit allt vanligare och kan slå ut samhällsviktiga kommunikationer och hela myndigheters IT-miljö. En brevbomb tas naturligtvis inte in för bevaring hos en myndighet, även om risken är begränsad att någon skulle råka aktivera den. Detta gäller även om ett meddelande finns i brevet. Sannolikt spränger polisen försändelsen och meddelandet.

På motsvarande sätt kan en myndighet inte rimligen behöva ta emot och bevara försändelser som är farliga för myndighetens informationssystem. Problemet är hur det skall kunna säkerställas att endast meddelanden som innehåller datavirus eller andra farliga komponenter raderas. Kan en sådan avgränsning göras på ett fungerande sätt bör berörda försändelser omedelbart få destrueras (jfr prop. 2002/03:62 s. 12). Visserligen kan undantagsvis en försändelse med virus innehålla ett meddelande som rör t.ex. en myndighets verksamhet. Avsändaren kan till och med vara ovetande om att han eller hon skickat virus. På samma sätt som det inte kan krävas att en myndighet botaniserar bland brevbombsförsändelser för att säkerställa att inget meddelande går förlorat bör avsändaren dock stå risken för att försändelsen stoppas. Detta bör gälla även om virusangreppet sker av oakt-

samhet, till följd av bristande tillsyn eller bristande skydd av sändarens utrustning; jfr att en myndighet inte hanterar en brevbomb ens när någon annan än avsändaren apterat den.

Juristgruppen anser att samma synsätt är tillämpligt vid mailbombning, dvs. när stora volymer e-post vid en given tidpunkt sänds till en myndighet så att en säkerhetsrisk uppstår för myndighetens IT-miljö.

Här bör också erinras om att de objektiva rekvisiten för dataintrång – *”olovligen ändrar eller utplånar eller i register för in ...*” – torde uppfyllas om myndigheten förmås att exekvera den skadliga koden så att uppgifter i myndighetens informationssystem drabbas. I dessa fall bör skyddet för avsändarens intressen få vika för behovet av att skydda myndighetens IT-miljö från angrepp.

Frågan blir hur den myndighet som meddelandena är ställda till skall kunna skilja virusmeddelanden från e-post eller spam som inte utgör en säkerhetsrisk. För denna hantering finns s.k. virusprogram. De kan med relativt hög grad av träffsäkerhet finna och ta bort ”smittade” meddelanden. Hur en myndighet rent praktiskt bör genomföra åtgärder av detta slag är både en teknisk och en juridisk fråga.

Vad som bör bedömas från juridiska utgångspunkter är om en hundraprocentig träffsäkerhet är en förutsättning för att myndigheten skall anses ha uppfyllt sin serviceskyldighet. På samma sätt som en misstänkt brevbomb kräver åtgärder, även om det inte är helt visst att försändelsen är farlig, krävs balanserade avvägningar i IT-miljö mellan motstående intressen av informationssäkerhet och rättssäkerhet.

Det är viktigt att allmänheten kan ha tillit till myndigheternas system för elektronisk kommunikation. En del i denna tillit är att systemen inte enkelt får slås ut vid ett angrepp. Skulle denna avvägning i något fall leda till att ”fel” meddelanden sorteras bort kan bestämmelserna om resning och återställande av försutten tid

bli tillämpliga.[26] Under dessa förutsättningar kan därmed, på motsvarande sätt som i traditionell miljö, vissa misstag repareras i efterhand.

[26] Se 11 kap. 11 § regeringsformen (RF), 58 kap. RB och 37 b och 37 c §§ FPL.

5 Myndigheternas hantering av inkommande handlingar

5.1 Allmänt

I den mån myndighetens skyddsåtgärder leder till att e-postmeddelanden som utgör t.ex. angrepp mot informationssystem hindras från mottagande innan de har kommit in enligt TF behövs inga ytterligare åtgärder av myndigheten.[27] Det finns i sådana fall inget hos myndigheten att registrera eller gallra. E-postmeddelanden, inklusive spam, som inte hindras blir däremot vid anländande till myndighetens IT-miljö vid någon punkt i processen tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas.[28] Meddelandet blir därmed att anse som en inkommen allmän handling, jfr 2 kap. 3 och 6 §§ TF.[29] TF:s regler om förvaring och inkommande är avgörande även vid tillämpningen av reglerna i 15 kap. 1 § SekrL om registrering och reglerna i arkivlagen om bevarande och gallring (se bl.a. 6 § 4 arkivlagen).

Huvudregeln i arkivlagen är att allmänna handlingar skall bevaras. De får emellertid gallras om åtgärden har stöd i författning eller ett beslut om gallring.[30] En statlig myndighet får bara gallra allmänna handlingar enligt lag, förordning eller föreskrift,[31]

---

[27] Jfr. dock möjligheten att förmedla felmeddelande till avsändaren, se Bilaga 2.

[28] Förutsatt att meddelandet har en sådan form att det kan läsas av myndigheten. I sammanhanget kan uppmärksammas att det av motivuttalandet till 5 § FL följer att en myndighet inte har någon skyldighet att skaffa sig program för att kunna läsa bilagor i olika filformat.

[29] Det kan visserligen i många fall vara så att en handling inte är att anse som allmän till följd av undantaget i 2 kap. 4 § TF. Vid den masshantering det här blir fråga om kan emellertid en utsortering, s.k. rensning, av sådant material som är irrelevant för myndigheten, antas kräva omfattande insatser jämfört med att endast gallra.

[30] Se 2 kap. 18 § TF och 10 § arkivlagen.

[31] Jfr. 14 § arkivförordningen (1991:446).

medan kommunerna har egna arkivmyndigheter och fastställer sina egna regler för när gallring kan ske. Exempel på lagar och förordningar som innehåller speciella regler om gallring är de s.k. databasförfattningarna, som i många fall föreskriver att person-uppgifter skall gallras inom viss tid.

I många fall finns inga speciella regler om gallring. Den föreskrift som dock kan tillämpas på gallring av spam är i första hand Riksarkivets föreskrifter och allmänna råd (RA-FS 1991:6, ändrad 1997:6) om gallring av handlingar av tillfällig eller ringa betydelse, som gäller för de flesta statliga myndigheter.[32] Enligt denna föreskrift skall en myndighet gallra allmänna handlingar av tillfällig eller ringa betydelse för myndighetens verksamhet, under förutsättning att allmänhetens rätt till insyn inte åsidosätts och att handlingarna bedöms sakna värde för rättskipning, förvaltning och forskning[33]. Som exempel på handlingar som genom sitt informationsinnehåll eller sin funktion är av tillfällig eller ringa betydelse anges i en bilaga bl.a. inkomna handlingar som inte berör myndighetens verksamhetsområde, eller som är meningslösa eller obegripliga, se vidare avsnitt 5.5.2 Registrering behövs inte – däremot ett gallringsbeslut, samt avsnitt 5.5.3 Skilj mellan olika typer av beslut och åtgärder nedan.

Med stöd av denna föreskrift gallras en stor mängd handlingar varje dag. De flesta myndigheter gallrar t.ex. reklam som saknar intresse för den egna verksamheten direkt vid postöppningen. Reklam som sänds med vanlig post till en myndighet uppfyller reglerna i TF för att vara allmän handling och kan gallras då myndigheten i RA-FS 1991:6 har stöd för att omedelbart gallra en reklamtidskrift och förpassa den till pappersåtervinning.

Respektive myndighet skall enligt föreskriften besluta hur reglerna skall tillämpas av den egna myndigheten. Reklam gallras vanligen omedelbart medan andra typer av handlingar har längre gallringsfrist. Beslutet bör dokumenteras i plan eller förteckning med angivande av gallringstidpunkt för respektive handlingsslag. En myndighet kan förslagsvis ange i planen att ”reklam som inte

[32] Se 1 § RA-FS 1991:6.

[33] Se 7 § RA-FS 1991:6.

behövs i verksamheten gallras vid postöppningen". Samma regler kan tillämpas på spam och en myndighet bör således i sin plan eller förteckning över handlingar som skall gallras ange också hur spam skall behandlas. Som en säkerhetsåtgärd kan spam eller loggar sparas viss tid innan gallring sker.

5.2 Lagring av spam

Möjligheten att lagra spam i stället för att direkt gallra den har diskuterats. Som nämnts innan är huvudregeln enligt arkivlagen att allmänna handlingar skall bevaras. I 9 § första stycket i personuppgiftslagen (1998:204; PUL) stadgas dock att personuppgifter inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen av personuppgifterna. Ett undantag i 8 § andra stycket PUL innebär emellertid att arkivlagens bestämmelse om att allmänna handlingar skall bevaras går före 9 § PUL. En myndighet får arkivera och bevara allmänna handlingar om det inte finns någon annan författning som säger att handlingarna skall gallras. Inget hindrar således en myndighet att lagra mottagen e-post för att i efterhand kunna rätta till ett misstag om ett e-postmeddelande felaktigt ansetts utgöra spam (jfr Bilaga 3). Lång lagring av allmänna handlingar har dock andra nackdelar förutom att det tar utrymme. Så länge som handlingarna finns kvar har allmänheten rätt till insyn och kan begära utdrag enligt 26 § PUL vilket kan medföra merarbete.

5.3 Rutiner vid manuell gallring

Som en följd av spamfiltrens ofullständighet, begränsningar i myndigheters möjligheter att med 100 % säkerhet sortera bort all spam från e-post som kan utgöra myndighetsärenden m.m., kommer alltid en viss mängd spam, som kommer fram till den enskilde handläggaren eller fastnar i karantän, att behöva gallras manuellt. Rutiner för sådan gallring måste därför fastställas. Något uttryckligt krav i författning på att handläggaren manuellt

måste ”öppna”[34] e-posten före gallring finns inte. En jämförelse med de rutiner som tillämpas på vissa myndigheter idag talar för att det inte ansetts nödvändigt att en tjänsteman faktiskt tar del av det fullständiga innehållet i inkommen post.

På samma sätt som färgglada broschyrer med erbjudande om försäljning av varor antas utgöra reklam och gallras utan att sådana handlingar bläddras igenom (alla sidor läses inte) torde e-post meddelanden när saken framstår som uppenbar kunna gallras bort utan att allt blir genomläst av en handläggare.[35] En första bedömning kan göras utifrån den information som ges rörande ämne och avsändare. Det torde t.ex. vanligtvis stå klart att ett e-postmeddelande med ämnesraden ”WE SELL C1AL1S, V1AGRA, XANAAX & VAL1UM AT CHEAPEST PRICE.” inneåller reklam och kan gallras utan att öppnas. Rubriken har utformats särskilt för att vilseleda IT-system som med hjälp av spamfilter skall stoppa otillåten marknadskommunikation. Risken för att meddelandet utgör en handling som rör ett myndighetsärende och gallring leda till en rättsförlust för en enskild är lika begränsad som när en handläggare slänger en reklamkatalog utan att kontrollera om en inlaga skrivits i sidorna.

Ett krav på att bläddra igenom varje sida framstår som främmande i pappersmiljö. Något intresse av offentlighetsinsyn i sådant material torde normalt inte heller finnas. Motsvarande bedömning bör kunna göras i IT-miljö.

---

[34] Med begreppet ”öppna” avses i föreliggande vägledning att själva medelandet, och inte bara uppgifter om t.ex. avsändare eller rubrik, granskas av en handläggare eller ett datorprogram.

[35] Vid bedömningen av om ett dokument är en allmän handling eller inte skall innehållet av dokumentet bedömas, enbart inte dess avsändare eller fysiska lagringsmedium. Inte heller ett gallringsbeslut kan ske enkom utifrån en handlings avsändare utan skall även det ske utifrån handlingens innehåll. En tjänsteman bläddrar inte igenom möbelkatalogen eftersom han anser sig kunna avgöra att handlingen kan gallras mot bakgrund av att han av erfarenhet vet att en reklambroschyr från möbelföretaget inte innehåller något myndighetsärende. Samma typ av bedömning torde i många fall vara möjlig beträffande spam.

5.4 Manuell gallring av sorterad e-post

Den e-post som sorterats ut som handlingar av ringa betydelse för myndigheten kan gallras på olika sätt;

- av tjänsteman som angetts som adressat eller av särskild personal,
- efter manuellt öppnande och granskande av innehållet i varje meddelande, eller
- efter granskande av enbart t.ex. avsändare eller ämnesrad.

Möjligheten har diskuterats att samtidigt radera en stor mängd e-postmeddelanden, exempelvis genom att en mapp innehållande sorterad e-post raderas samtidigt utan någon individuell granskning av varje meddelande. Praktiskt skulle detta kunna genomföras genom att en ansvarig tjänsteman t.ex. en gång i veckan trycker på ”delete”-knappen för de sorterade e-postmeddelandena.

De kriterier som används vid sorteringen av inkommen e-post kan, som i traditionella spamfilter, bygga på matchning av vissa ordombinationer och utvecklas genom kontinuerlig kartläggning av mottagen e-post. E-posten kan sorteras i olika mappar där sannolikheten för att e-posten utgör handlingar av ringa betydelse är olika hög.

En tjänsteman bör med hjälp av automatiska rutiner, som elektroniskt öppnar och granskar den inkomna e-posten, kunna övertyga sig om att en mapp sorterad efter vissa kriterier enbart innehåller handlingar av ringa betydelse. Tjänstemannen bör därefter kunna tömma mappen utan att granska varje e-postmeddelande.

Varje myndighet får själv, utifrån sina förutsättningar, besluta om vilka kriterier som skall gälla för myndighetens sortering av e-post, vilka rutiner som skall tillämpas vid gallring och huruvida en manuell granskning skall krävas beträffande vissa sorterade e-postmappar. Dessa rutiner måste dock säkerställa att allmänhetens rätt till insyn inte åsidosätts.

5.5 Gallring med automatiska rutiner

5.5.1 Gallring behövs endast om handlingen kommer in

Från kostnads- och effektivitetssynpunkt är det önskvärt att kunna gallra e-post automatiskt. I prop. 2002/03:62, Några förvaltningsättsliga frågor, betonas att den ökande användningen av e-post förstärker myndigheternas behov av att anpassa sina säkerhetssystem så att de kan skyddas mot virus och andra systemangrepp. Även riskerna för överbelastningsattacker (s.k. mailbombning) nämns. I den mån skyddsåtgärder leder till att meddelanden som utgör t.ex. angrepp mot informationssystem rensas ut innan de har kommit in enligt FL och 2 kap. TF behövs inga ytterligare åtgärder av myndigheten. Det finns då inget hos myndigheten att gallra.

5.5.2 Registrering behövs inte – däremot ett gallringsbeslut

När ett meddelande har kommit in och anses utgöra allmän handling (undantagen torde inte vara relevanta i detta sammanhang) återstår det att bedöma

- om registrering enligt 15 kap. 1 § SekrL kan underlåtas för att handlingen uppenbart är av ringa betydelse för myndighetens verksamhet, och
- om arkivförfattningarna medger gallring i enlighet med ett beslut om att gallra handlingar som är av tillfällig eller ringa betydelse.

De handlingar som på denna grund i allmänhet inte behöver registreras är bl.a. pressklipp, cirkulär, reklamtryck, statistiska meddelanden och kopior av andra myndigheters yttranden samt anonyma skrifter och skrifter från enskilda med meningslöst eller obegripligt innehåll (jfr JO 1995/96 s. 485). Förutsättningar föreligger för myndigheter att meddela motsvarande gallringsbeslut

och det är uppenbart att sådan spam som myndigheterna behöver hantera hör till dessa kategorier av handlingar.

Därmed återstår frågan om hur dessa bedömningar bör göras och hur beslut bör fattas. Effektiva och träffsäkra system kan skapas som – rätt uppsatta – normalt kan fungera i huvudsak automatiskt. Avancerat IT-stöd förekommer redan i betydande omfattning i myndigheternas handläggning och beslutsfattande.

5.5.3 Skilj mellan olika typer av beslut och åtgärder

Från juridiska utgångspunkter är det viktigt att skilja mellan å ena sidan myndighetens *beslut* om regler för hur gallring ska gå till och å andra sidan praktiska *åtgärder* i enlighet med ett sådant beslut beträffande vissa handlingar.

Den typ av beslut som i praktiken aktualiseras som ett första steg är ett beslut enligt ovan om regler för gallring beträffande spam. Myndigheterna bör fatta ett sådant beslut i enlighet med 7 § Riksarkivets föreskrifter (RA-FS 1991:6; ändrad genom RA-FS 1997:6) om gallring av handlingar av tillfällig eller ringa betydelse. I denna bestämmelse föreskrivs följande:

”Myndigheten skall gallra allmänna handlingar av tillfällig eller ringa betydelse för myndighetens verksamhet. Gallring får dock endast ske under förutsättning att allmänhetens rätt till insyn inte åsidosätts och att handlingarna bedöms sakna värde för rättskipning, förvaltning och forskning.”

För tillämpningen av denna bestämmelse ger Riksarkivet följande allmänna råd:

”Vid tillämpning av dessa föreskrifter har myndigheten själv att ta ställning till vilka handlingar som är av tillfällig eller ringa betydelse med hänsyn till de bevarandemål som anges. Som stöd för övervägandena finns en bilaga som upptar sådana handlingar som kan komma ifråga för gallring.

A. Exempel på handlingar som genom sitt informationsinnehåll eller sin funktion är av tillfällig eller ringa betydelse

4.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."

Ett sådant gallringsbeslut bör naturligtvis inte fattas automatiskt utan beredas manuellt och fattas och dokumenteras på sedvanligt sätt. Av gallringsbeslutet bör framgå vilken typ av handlingar som gallras och hur gallring skall ske.

5.5.4 Åtgärder i nästa led

Därmed återstår frågan om efterföljande praktiska åtgärder för att ta bort enskilda inkomna handlingar, i enlighet med det redan fattade gallringsbeslutet, får ske automatiserat. Även här behöver en myndighets åtgärder delas in i två led så att myndigheten skiljer mellan att

1. bestämma rutiner och åtgärder för att avskilja meddelanden som omfattas av gallringsbeslutet och införa dem, respektive
2. sortera ut spam automatiserat till ett särskilt förvar och aktivera den tekniska funktionen för att förstöra de meddelanden som avskilts i enlighet med 1.

Även här är det uppenbart att åtgärderna för att bestämma rutiner och införa dem bör vidtas manuellt och att beslut i den delen inte fattas automatiserat utan manuellt och dokumenteras på sedvanligt sätt.

5.5.5 Sortering och radering

Frågan är vad som gäller för den efterföljande automatiserade sorteringen och raderingen av spam. Helt automatiska rutiner används redan i stor omfattning vid myndigheterna. Dessa

omfattar även beslutfattande. I lag finns inget uttryckligt förbud mot automatiserat beslutsfattande eller mot att automatiskt aktivera funktioner för att avskilja eller ta bort meddelanden, t.ex. handlingar som uppenbarligen saknar all relevans för eller anknytning till myndighetens verksamhet och som omfattas av gallringsbeslut.

För de uppenbara fall som här aktualiseras uppkommer frågan om det, i detta led, överhuvudtaget blir fråga om ett beslut eller ens föreligger ett ärende i FL:s mening. Även här kan en uppdelning i två led underlätta resonemanget;

1. att avskilja de handlingar som skall raderas enligt myndighetens beslut att gallra vissa typer av handlingar när de i en framtid kommer in, respektive
2. att aktivera raderingen.

FL gäller – med undantag för de regler om service som finns i 4-6 §§ – endast för handläggningen av ärenden. I nu aktuella fall har meddelandena uppenbarligen inte med myndighetens verksamhet att göra. Det är normalt inte någon som vänder sig till myndigheten utan oftast endast ett spam sänt i blindo, kanske med förfalskade uppgifter om avsändare. Själva ”hänvändelsen” sker dessutom i en form och med en metod som bär en uppenbar prägel av att inte utgöra något seriöst försök att kontakta myndigheten för att uträtta ett ärende eller att ta tillvara sin rätt. Meddelandet innehåller inte heller någon begäran om besked eller åtgärd som hör till myndighetens verksamhetsområde.

I pappersmiljö skulle det inte rimligen anses utgöra ett ”ärende” när en myndighet sorterar ut en möbelkatalog som kommit bland vanlig post till myndigheten. Motsvarande synsätt bör gälla vid utsortering till spamarkiv eller liknande i elektronisk miljö. En helt annan bedömning blir aktuell om en myndighet skulle utforma sina rutiner felaktigt så att ansökningar och andra inlagor blev bortsorterade som spam. De rättsliga komplikationerna torde emellertid härvid höra samman med fel i de manuella beslut och åtgärder som föregått de automatiska behandlingarna.

Själva aktiveringen av raderingen kan i pappersmiljö närmast jämföras med att myndighetens vaktmästare hämtar en hög med papper som redan har avskiljts för att kastas eller brännas. För sådant faktiskt handlande gäller normalt inte reglerna om handläggning av ärenden och det torde inte finnas hinder mot att i IT-miljö automatisera motsvarande åtgärder.

Det är varje myndighets eget ansvar att bedöma och besluta om hur spam skall tas om hand och hur gallringen skall utföras.

Skäl för att använda automatisk gallring enligt en på förhand bestämd programkod är att myndigheten får mycket spam, att det tar stora resurser i anspråk och att manuell hantering av spam är en arbetsmiljöfråga. Det kan vara så att om någon varje dag har till uppgift att radera spam så går det efter ett tag så mycket slentrian i hanteringen att risken att annan e-post också gallras är större än med ett väl utprovat spamfilter. En central fråga vid bedömningen är vilken risk myndigheten tar. Hur sannolikt är det att e-post som har betydelse för myndigheten eller enskild försvinner i hanteringen? Teoretiskt kan man alltid tänka sig att någon sänder ett e-postmeddelande som rör ett myndighetsärende kamouflerat som spam. Frågan är om det är sannolikt och om, förutsatt att e-postmeddelanden eller loggar sparas viss tid, någon verklig skada skulle inträffa.

Det är naturligtvis upp till varje myndighet att bedöma hur de mer i detalj planerar sin verksamhet och behandlar e-post. Det är dock på sin plats att i samband med denna redogörelse för automatisk filtrering understryka att automatiska rutiner i form av filtreringsprogram saknar det omdöme en handläggare förutsätts besitta. För det fall en myndighet väljer att använda sig av automatiska rutiner för såväl filtrering som radering är det därför viktigt att myndigheten säkerställer att de automatiska rutiner man använder sig av i princip garanterar att inga e-postmeddelanden som utgör legala förvaltningsärenden raderas. Sådana system torde regelbundet behöva ses över och utvärderas. Precis som det i ett fall där en handläggare felaktigt slänger en inkommen handling kan utkrävas ett ansvar, i det mest extrema fallet tjänstefel, kan en alltför liberal användning av automatisk

filtrering leda till att handlingar felaktigt raderas och ansvar för denna felaktiga hantering av allmänna handlingar utkrävas. Det är ytterst myndighetsledningens ansvar att verksamheten bedrivs med beaktande av myndighetens skyldigheter och en rättssäker hantering av allmänna handlingar som inkommer till myndigheten, oavsett om dessa handlingar inkommer via elektronisk väg eller traditionell post.

6 Praktiska åtgärder mot spam

6.1 Allmänt

Det förtjänar att upprepas, från avsnitt 1.3, att spamhanteringen en del i en övergripande policy för e-post. En övergripande e-postpolicy kan exempelvis innehålla rutiner för:

- tilldelning och användning av e-postadresser.
- publicering av e-postadresser.
- e-post till frånvarande/semestrande tjänsteman.
- spamklassificerad e-post levererad till mottagande tjänsteman.
- spamkontroll av utgående e-post.
- arkivering och diarieföring.
- e-postens integrering i ärendehanteringsprocesserna.

Det förtjänar också att återupprepa att föreliggande vägledning syftar till att ge en grund för de bedömningar som varje myndighet har att göra utifrån den egna verksamhetens förutsättningar. Varje myndighet bör ta i bruk de lösningar som bäst tillgodoser den egna verksamhetens krav. Bilaga 3 visar några av de praktiska spamhanteringsåtgärder som bedömts tillgodose verksamheten inom AMS.

6.2 Funktionsadresser

En praktisk åtgärd för att motverka och begränsa spam går ut på att begränsa exponeringen av e-postadresser mot Internet. Detta skulle kunna genomföras genom att myndigheten, i stället för att varje tjänsteman har en egen e-postadress, övergår till funktionsadresser, t.ex. registrator@myndigheten.se. Följden blir att endast en eller ett par e-postadresser exponeras på myndighetens webbplats. Adressen skulle inte heller spridas på Internet genom

att tjänstemän använder sina e-postadresser, t.ex. i olika diskussionsforum eller andra sammanhang.

Lösningen synes inte möta några juridiska hinder. Så länge myndigheten erbjuder enskilda att ge in handlingar till en e-postadress är serviceskyldigheten enligt 5 § FL uppfylld.

6.3 Webbformulär

Rutiner som innebär att den normala vägen för att ge in handlingar blir e-tjänster med webbformulär i stället för e-post meddelanden är en juridiskt godtagbar lösning, förutsatt att myndigheten genom sin webbservice uppfyller kravet på tillgänglighet i enlighet med 5 § FL.

7 Angränsande frågor

7.1 Filtrering utförd av operatörer

En myndighet kan inte kringgå de regler som behandlats i denna vägledning genom att ge en tredje part eller en operatör i uppdrag att vidta åtgärder mot spam. Däremot torde de regler som gäller för myndigheten inte innebära begränsningar för en operatör att på eget initiativ införa åtgärder för att stoppa spamtrafik som medför att viss e-post inte kommer fram till myndigheten. Meddelandet går på avsändarens risk och reglerna för myndighetens hantering gäller inte för åtgärder som vidtas av en privat aktör som förmedlar meddelandet. Myndigheten har dock en skyldighet att ingripa om den får klart för sig att ett orimligt stort svinn sker till följd av godtyckliga åtgärder från operatörens sida. En operatörs tekniska och juridiska möjligheter att införa denna typ av åtgärder behandlas inte närmare i denna vägledning.

7.2 Myndighetens informationsskyldighet

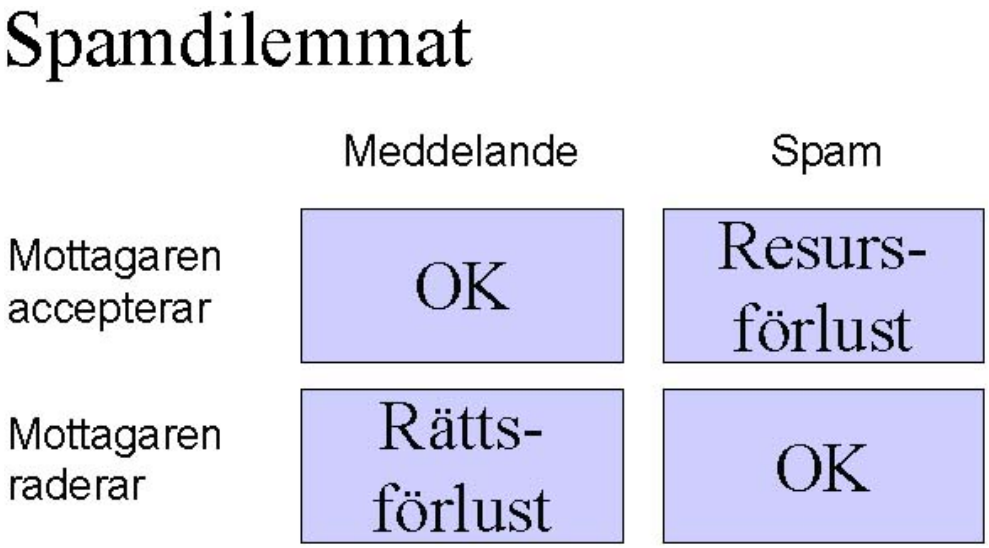
För att uppfylla sin serviceskyldighet bör varje myndighet på ett tydligt sätt informera om sina rutiner för mottagande av e-post, detta kan lämpligen göras på myndighetens webbplats.

7.3 Frågor kring outsourcing av spamhantering

Myndigheter med begränsade resurser, t.ex. små kommuner, kan pga. kostnadsskäl ha behov av att samordna och/eller lägga ut driften av åtgärder mot spam på en tredje part. En sådan samordning och outsourcing av åtgärder torde i och för sig vara möjlig. De juridiska förutsättningarna för outsourcing behandlas dock inte närmare i projektet.

8 Vart leder vägledningen?

Vägledning syftar till att ge en juridisk grund för de bedömningar som varje myndighet har att göra utifrån den egna verksamhetens förutsättningar. Varje myndighet bör ta i bruk de tekniska och administrativa lösningar som bäst tillgodoser den egna verksamhetens krav. Lösningarna skall vara resurssnåla och rättssäkra. Samtidigt gäller att myndighetens egen säkerhet är en förutsättning för säker kommunikation med omvärlden



För det fall en myndighet väljer att använda sig av automatiska rutiner för såväl filtrering som radering är det viktigt att myndigheten säkerställer att de automatiska rutiner man använder sig av i princip garanterar att inga e-postmeddelanden som utgör legala förvaltningsärenden raderas. Sådana system torde regelbundet behöva ses över och utvärderas.

Om en handläggare felaktigt slänger en inkommen handling kan utkrävas ett ansvar, i det mest extrema fallet tjänstefel. På samma sätt kan en alltför liberal användning av automatisk filtrering leda till att handlingar felaktigt raderas och ansvar för denna felaktiga hantering av allmänna handlingar utkrävas.

Det är således ytterst myndighetsledningens ansvar att verksamheten bedrivs med beaktande av myndighetens skyldigheter och en rättssäker hantering av allmänna handlingar som inkommer till myndigheten, oavsett om dessa handlingar inkommer via elektronisk väg eller traditionell post – och oavsett om spamhanteringen sker manuellt, med teknikstöd eller automatiskt.

Och arbetet måste fortsätta. Spammarna tycks redan ha lärt sig att förslava e-postoperatörer så att spam kan skickas från ISP-servrar. I ett nyhetsbrev den 3 februari 2005 kommenterades den dåliga nyheten med orden att "Spamhaus ser denna trend och den resulterande spamförändringen och -ökningen som ett seriöst hot. Med rådande tillväxtökningen kan förespås att spam vid mitten av 2006 utgör 95 % av all e-posttrafik och därmed ser vi tecken på en e-posthärdsmälta orsakad av köer i leveranssystemen och överbelastade spamfilter."[36]

[36] http://www.spamhaus.org/news.lasso?article=156 "Increasing Spam Threat from Proxy Hijackers."

English summary

Managing the Spam Plague – Guidance on the Legal Issues for Swedish Government Agencies.

Governments must step up their fight against spam or risk seeing consumer and business confidence in the Internet buried under a mountain of junk e-mail. As a matter of fact, government agencies are themselves more severely plagued by spam than the average e-mail recipients. The reason is that there in many countries are legal requirements to the effects that government agencies must be accessible via e-mail and that the received e-mail must be treated as a public document and subsequently be archived or deleted.

Swedish government agencies are taking those requirements quite seriously and are as a result uncertain as to how to handle the spam flood. One extreme would be that any suspicious e-mail are treated as if containing virus and thus can be denied entrance. The other extreme would be that a non-virus e-mail must be opened and reviewed so as to allow decisions on its further handling.

As outlined in the guidelines, the most appropriate approach lies between the two extremes. Government agencies must be open for communication via e-mail, but not open to the extent that the e-mail channel becomes defunct due to a massive influx of spam.

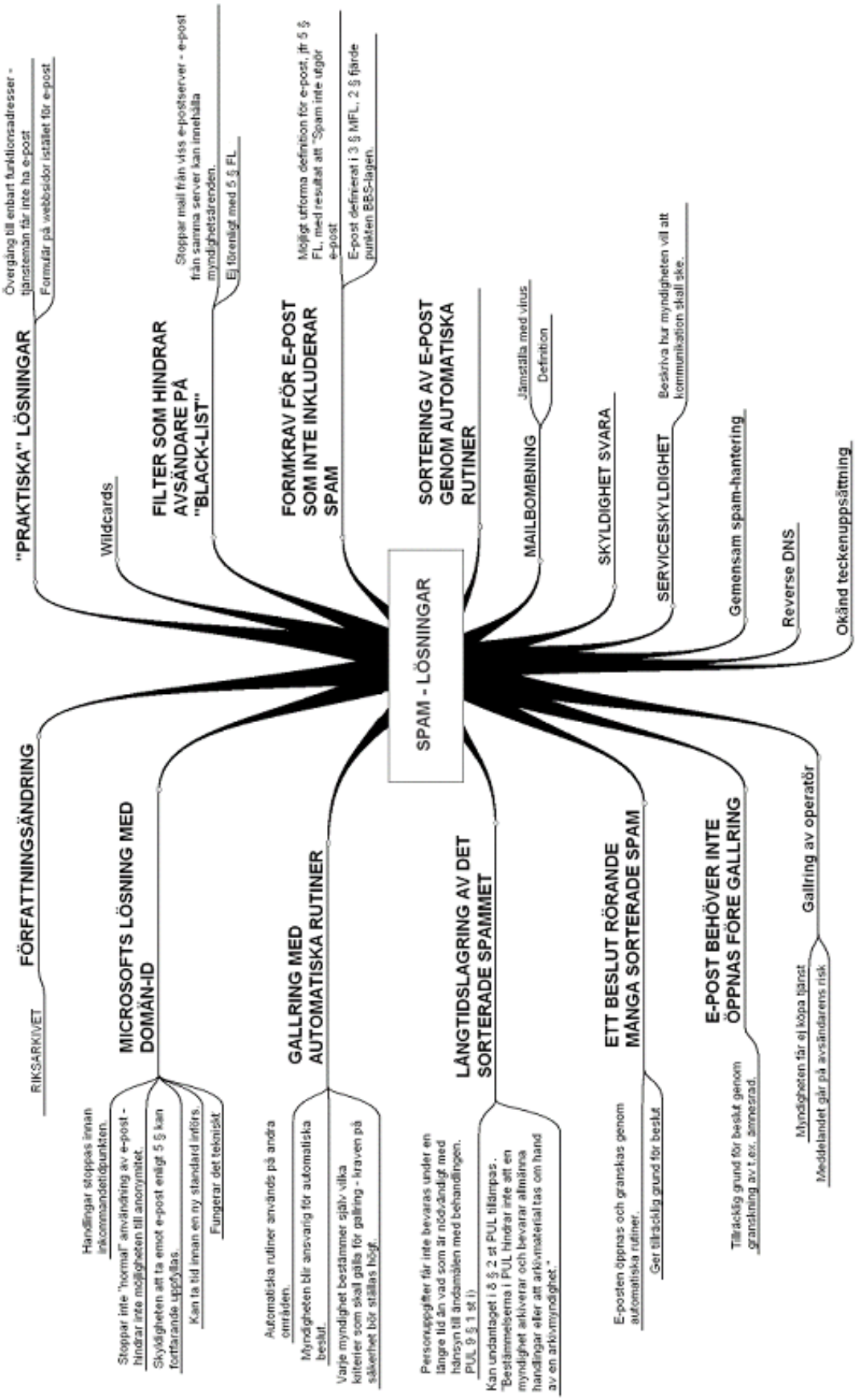
There is no "one solution fits all" - each agency will have to define its own spam handling policy and praxis. However, the group of participating agency experts collectively subscribes to the following exemplified guideline:

- Blacklists may not be used as a routine measure, but may be used in acute situations;
- Mail with forged sender-addresses may be denied access since they do violate the requirements set out in the Simple Mail Transfer Protocol (SMTP, RFC 2821);

- Mail with obviously “guessed” recipient addresses may be denied access in acute situations;
- Mail classified as “very likely spam” may temporarily be stored in a “quarantine” without being considered as received public documents;
- Mail classified as “very likely spam” may, just like virus shipments, be automatically deleted given that the system is properly supervised and meets the highest standards in order to eliminate incorrect deletion of legitimate e-mail; and
- Various methods should be used to stifle spammers' attempts at harvesting e-mail addresses.

Bilaga 1

Mind-map diagram över samtliga frågeställningar behandlade i juristgruppen.



Bilaga 2

Presentation av sändande e-postserver

Protokollet SMTP (RFC 2821)

Protokollet är utformat så att den mottagande servern formellt kan avbryta en transaktion och skicka felmeddelanden härom även om den inledande handskaningsprocessen är aktiv.[37]

Enligt Protokollet är huvudregeln att den sändande e-postservern vid kontakt med en mottagande e-postserver måste presentera sig med ett korrekt namn som går att kontrollera i domännamnssystemet.[38]

Ett exempel på ett sådant namn är ”mx.statskontoret.se”, där ”mx” anger att det är en ”mail exchangeserver” och ” stats-kontoret.se” är ett domännamn som går att slå upp i domän-namnsregistret. Den mottagande e-postservern kan alltid se vilken IP-adress den sändande e-postservern har, denna adress går inte att förfalska, och genom att slå upp domännamnet ”statskontoret.se” i domännamnsregistret och jämföra med den IP-adress som den sändande e-postservern uppgett kan den mot-tagande e-postservern kontrollera att den sändande adressen inte är ”förfalskad”, dvs. inte utges för att vara någon annan e-postserver än den som faktiskt har använts.[39]

[37] RFC 2821, section 3.1, Session initiation

[38] RFC 2821, section 3.6 första meningen anger att ”Only resolvable, fully-qualified, domain names (FQDNs) are permitted when domain names are used in SMTP.”

[39] Se mer om följderna av detta nedan.

I anslutning till kravet enligt huvudregeln på att ett korrekt namn anges, dvs. ett namn som går att kontrollera i domännamns-systemet, gäller även enligt Protokollet att "nick-names" eller okvalificerade namn inte får användas.[40]

Ett okvalificerat namn är ett namn som inte går att kontrollera genom att slå upp i domännamnsregistret, t.ex. "mx" i stället för hela "mx.statskontoret.se".[41]

Undantaget från huvudregeln anger att den sändande e-post-servern vid kontakt med en mottagande e-postserver även tillåts presentera sig med endast en IP-adress.[42]

Den mottagande e-postservern har då möjlighet att kontrollera den sändande e-postservern genom att jämföra den uppgivna IP-adress som den sändande e-postservern uppgett med den sändande e-postserverns *verkliga* IP-adress.[43]

Sammanfattningsvis kan konstateras att Protokollet ställer krav på att sändande e-postserver presenterar sig

1. med ett korrekt namn som går att kontrollera i domännamns-systemet, eller
2. med sin IP-adress

---

[40] RFC 2821, section 3.6 tredje meningen anger att "Local nicknames or unqualified names MUST NOT be used."

[41] Ett sådant namn går naturligtvis inte att slå upp annat än i en lokal katalog (DNS) på samma domän som "maskinen" står.

[42] RFC 2821, section 3.6 sista meningen anger två undantag:

(1) "The domain name given in the EHLO command MUST BE either a primary host name (a domain name that resolves to an A RR) or, if the host has no name, an address literal as described in section 4.1.1.1."

(2) "The reserved mailbox name "postmaster" may be used in a RCPT command without domain qualification (see section 4.1.1.3) and MUST be accepted if so used."

[43] Den mottagande e-postservern kan alltid se vilken IP-adress den sändande e-postservern har, denna går inte att förfalska.

Mottagande e-postserver kan kontrollera huruvida sändande e-postserver presenterat sig i enlighet med Protokollet eller uppgivit en ”falsk” adress genom att

1. jämföra uppgivet namn med information i domännamnsregistret, alternativt
2. jämföra uppgiven IP-adress med verklig IP-adress.

Kontroll av avsändarens adress

När sändande e-postserver accepterats av mottagande e-postserver överförs information om avsändarens uppgivna e-postadress. Innan mottagande e-postserver tillåter processen att fortsätta finns möjlighet att vidta kontroller av e-postadressen. När spam sänds är det vanligt att avsändaradressen är förfalskad.

Uppgiven adress finns i eget nät

Sändaren av spam använder t.ex. i vissa fall en adress som finns i den mottagande e-postserverns domän, exempelvis uppger tjansteman@myndighet.se som avsändareadressen vid sändande av spam till handlaggare@kansliet.se, troligen i syfte att lura mottagaren av e-postmeddelandet att lita på avsändaren och därför öppna och läsa e-posten.

Om en uppgiven e-postadress vid kontroll visar sig finnas i den egna domänen kan den mottagande e-postservern kontrollera den sändande e-postserverns IP-adress för att avgöra om den sändande e-postservern tillåts skicka e-post för den domänen. Om den sändande servern inte är någon av Statskontorets e-postservrar och istället finns i t.ex. Brasilien är det uppenbart att den avsändande e-postadressen är förfalskad.

Uppgiven adress finns inte

Sändare av spam använder ofta en gissad/konstruerad adress som inte finns, t.ex. tjansteman@påhittaddomän.nu. Det måste dock beaktas att en uppgiven avsändaradress, där domänen inte finns, kanske enbart är följden av att det som synes vara en ”påhittaddomän” är en ”felstavaddomän” i sändarens e-postprogram.

Bilaga 3

AMS:s hantering av e-post