Christer Wilsby

# E-post att lita på

En guide om hur man skyddar sin e-post mot olika hot

**E-post att lita på**

.SE:s Internetguide, nr 18
Version 1.0 2010



Författare: Christer Wilsby
Redaktör: Lennart Bonnevier
Formgivning, layout och redigering: Gunnel Olausson/FGO AB
Illustrationer: © Camilla Laghammar

ISBN: 978-91-978350-8-4

.SE (Stiftelsen för Internetinfrastruktur) ansvarar för Internets svenska toppdomän. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige.

Besöksadress: Ringvägen 100 A, 9 tr, Stockholm
Brevledes på .SE Box 7399, 103 91 Stockholm
Telefon: +46 8 452 35 00
Fax: +46 8 452 35 02
E-post: info@iis.se
Organisationsnummer: 802405-0190
www.iis.se

**Förord** 5

**Vi behöver kunna lita på e-posten** 7

**Så rör sig e-posten** 9
Företag med egen e-postserver ..... 9
En första filtrering hos operatören ..... 10
Enskild användare ..... 11

**Hoten mot e-posten** 13
Skadliga meddelanden ..... 14
Falska avsändare ..... 15
Avlyssning ..... 17
Förvanskat innehåll ..... 17
Angrepp på katalogtjänsten ..... 18
Säkerhetskultur ..... 19
Kommersiella produkter och gratissäkerhet ..... 19

**Skyddsmekanismer och hur de fungerar** 21
PGP ..... 21
TLS ..... 23
DKIM ..... 24
ADSP ..... 27
SPF ..... 28
DNSSEC ..... 29
Antispam ..... 33

**Kom igång med säkerhetsarbetet** 35
MailCheck kollar e-postservern ..... 35
DNSCheck kontrollerar att DNS fungerar ..... 36
Undvik svartlistning och att fastna i spamfilter ..... 37

**Ordlista** 39

**Länkar till referenser och källor** 41

# Förord

Internet och e-post har hamnat i samhällets huvudfåra på ett så diskret och självklart sätt att de flesta inte kan säga när och hur det hände. Det betyder bland annat att kraven på att e-posten går att lita på har ökat snabbt.

Guiden vänder sig i första hand till den eller de som ansvarar för e-posten på små och medelstora företag men som inte har som affärsidé att själva arbeta med Internetsäkerhet. Guiden går igenom olika hot och visar vad man kan göra för att skydda sin e-post. Även intresserade användare bör ha behållning av guiden och kanske kan ett stort företag som har kompetensen i huset se den som en checklista på att det gjort hela läxan.

Tillförlitlig e-post går inte att bygga på en enda produkt eller tjänst. Det handlar om att balansera innehållet i verktygslådan så att man har flera lager av säkerhet och även om att arbeta med säkerhetsmedvetandet i den egna organisationen.

Författaren riktar ett stort tack till Rickard Bellgrim, .SE, Alex Bergvall, Gatorhole, Anne-Marie Eklund Löwinder, .SE, Patrik Wallström, .SE och Jörgen Eriksson, .SE som alla bidragit med sina insikter. Till källorna hör även Wikipedia, andra publikationer från .SE och webbsajter specialiserade på de olika säkerhetstekniker som beskrivs, flertalet drivna av de organisationer som förvaltar respektive säkerhetsteknik. För slutresultatet och det urval som gjorts ansvarar dock författaren.

Bromma i februari 2010
Christer Wilsby

**Hjälp oss att förbättra**
Om du hittat fel eller har synpunkter på denna guide kan du sända dem till publikationer@iis.se

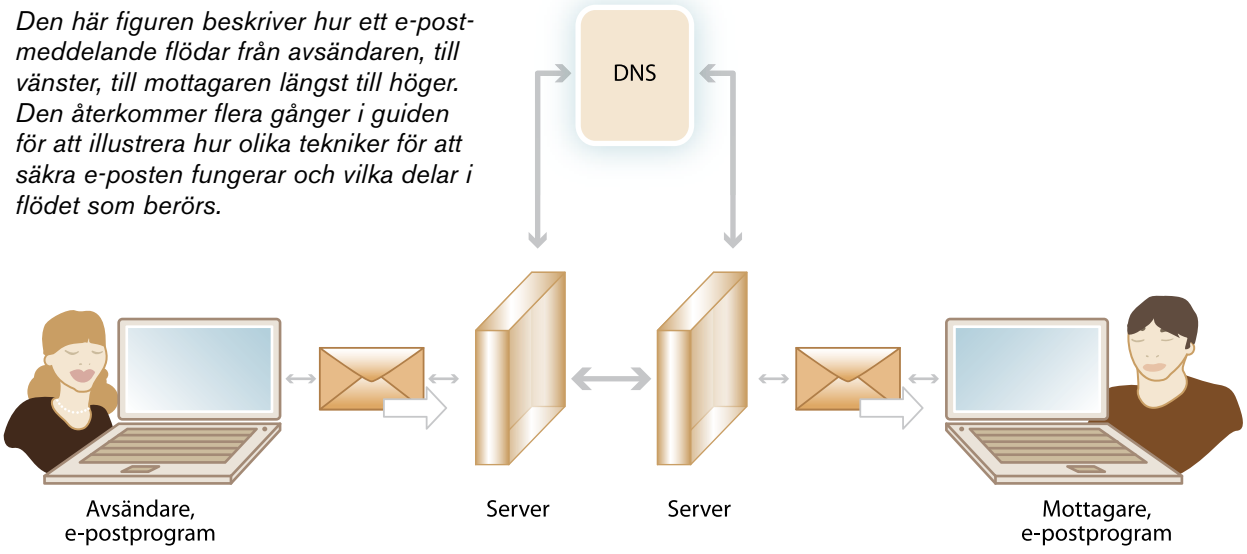
# Vi behöver kunna lita på e-posten

På bara ett par decennier har Internet som plattform för kommunikation, handel, myndighetskontakter och bankaffärer gått från ömsom hyllad, ömsom utskrattad vision till att vara en realitet för företag och individer. Internet har ofta fått en större roll i våra dagliga liv än vad de mest utstuderade Internetvisionärerna gissade när den så kallade bubblan var som störst. Mycket av innovationsarbetet sker på webben, men i botten finns alltid e-posten. ”Blev något fel? Skicka ett mejl!”

Lite grand i skuggan av utvecklingen av allt mer spektakulära och funktionella kommunikationstekniker har e-posten gradvis tagit över rollen från pappersposten. Vill man vara säker på att budskapet når fram skickar man e-post. Det är snabbt, enkelt och billigt.

Det betyder att förväntningarna på e-posten hela tiden ökar. Den behöver vara tillförlitlig. Tillförlitlig i meningen att vi vet vem

*Den här figuren beskriver hur ett e-postmeddelande flödar från avsändaren, till vänster, till mottagaren längst till höger. Den återkommer flera gånger i guiden för att illustrera hur olika tekniker för att säkra e-posten fungerar och vilka delar i flödet som berörs.*



*”Tillförlitlig i meningen att vi vet vem som har skickat ett meddelande, … att den inte innehåller virus eller försöker lura av oss känslig information och … att vi kan vara säkra på att den alltid når fram till den avsedda mottagaren.”*

som har skickat ett meddelande, tillförlitlig i meningen att den inte innehåller virus eller försöker lura av oss känslig information och tillförlitlig i meningen att vi kan vara säkra på att den alltid når fram till den avsedda mottagaren. Dessutom utan att ändras eller tjuvläsas på vägen.

Viktiga orsaker till e-postens framgång är de låga kostnaderna och enkelheten, både när vi vill nå en enda individ och när vi skickar e-post till många mottagare. Tyvärr gäller dessa fördelar även för individer och organisationer som inte vill oss så väl. Skräppost (spam), försök att lura av oss lösenord, kontonummer och annan känslig information (*phishing*), skadliga program som gömmer sig i bilagor och bakom länkar och även avlyssning av meddelanden har blivit vardagliga verktyg för de individer som fiskar i grumliga vatten.

Det finns domedagsprofetior som spår e-postens undergång under trycket av all skräppost och alla tvivelaktiga aktörer som skickar e-post till oss. Men det behöver inte bli så. Tvärtom, det finns etablerade och ofta lättanvända tekniker som gör e-posten tillförlitligare. Utan att göra anspråk på att redovisa alla tekniker och produkter som finns tillgängliga ger den här guiden en verktygslåda för att bygga ett balanserat skydd för företagets e-post.

# Så rör sig e-posten

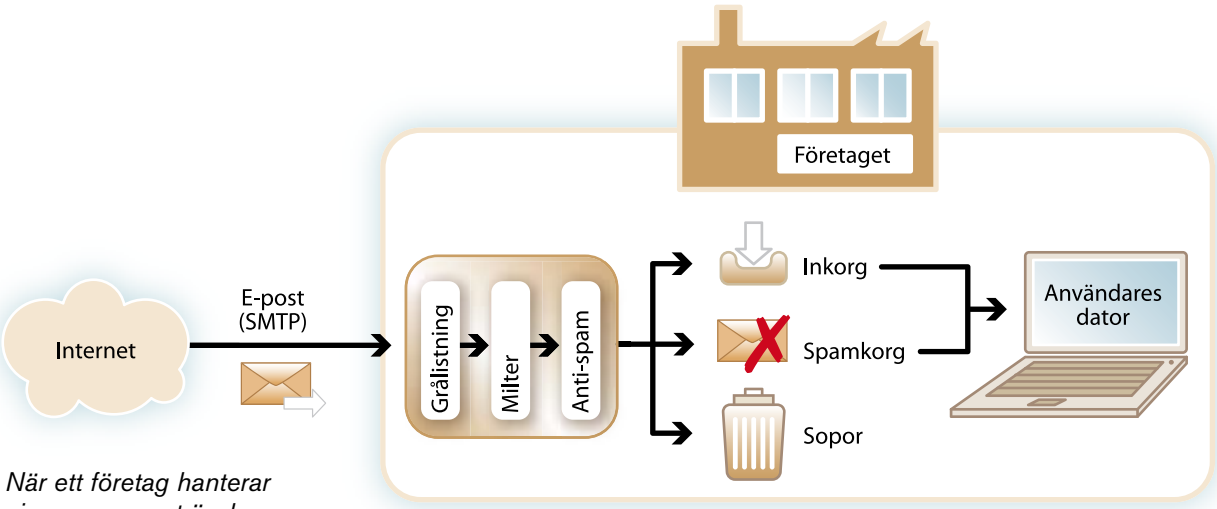
## Företag med egen e-postserver

Låt oss titta på hur ett företags e-post är uppbyggd. Mellan olika e-postservrar på Internet används protokollet SMTP (*Simple Mail Transfer Protocol*) för att skicka och ta emot e-post. Vilken server som tar emot e-posten för en viss domän (till exempel iis.se) finns beskrivet i katalogtjänsten DNS. När ett e-postmeddelande tagits emot av servern kan det behandlas i flera steg innan det levereras till mottagaren. Det första steget är ofta något som kallas grålistning. Det innebär att meddelanden från en avsändare som man inte tagit emot e-post från tidigare sätts i karantän i väntan på att avsändaren visar att den menar allvar genom att skicka meddelandet en gång till.

Grålistningen eliminerar en hel del oseriösa meddelanden eftersom de flesta som skickar spam tycker att det är alldeles för resurskrävande att hålla reda på vilka meddelanden som gått fram och vilka som kan behöva sändas om. För legitima avsändare är det inte så svårt men för spammare som skickar miljontals e-postmeddelanden, ofta från kapade datorer, är det inte värt besväret att försöka följa upp vilka som når fram.

När meddelandet passerat grålistningen går ett filter in och hanterar signaturer, kryptering och säkerhetsprotokoll som installerats på servern. Därefter tar oftast ett antispam-program över och skapar sig en helhetsbild av meddelandet som summeras i ett samlat betyg. Är betyget tillräckligt bra går meddelandet till adressatens inkorg, är det riktigt dåligt kastas det direkt och om betyget ligger mellan dessa värden går det till mottagarens mapp för skräppost. Det är också vanligt att antivirusprogram körs på det här stadiet. Det är också vanligt att mottagarens e-postprogram har skydd av olika slag som gör ytterligare tester på meddelandet innan mottagaren kan öppna det.

Förutom grålistning finns det svartlistning, det vill säga en




*När ett företag hanterar sin egen e-post är den första uppgiften för e-postservern att grovsortera inkommande meddelanden i tre högar: definitivt skräp (slängs), troligen skräp (märks som skräppost/spam) samt riktiga meddelanden (levereras till mottagarens inkorg).*

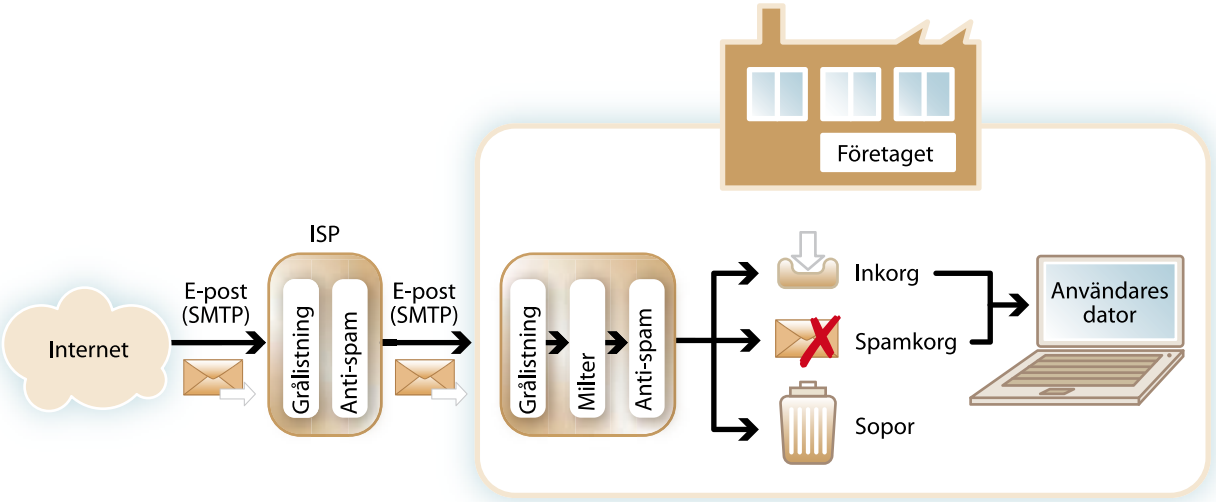
spärrlista för avsändare, och vitlistning, det vill säga en lista på avsändare som man uttryckligen godkänt som legitima avsändare.

Men det sista och avgörande testet gör människan av kött och blod som fått e-posten. Litar jag på avsändaren, ska jag klicka på länken, eller ska jag öppna bilagan? Om det verkar skumt kan det vara bäst att låta bli, oavsett hur många säkerhetskontroller som lagts på innan det når mottagarens brevlåda.

## En första filtrering hos operatören

När ett företag väljer att gå via en operatör i stället för att koppla upp sig direkt mot Internet blir bilden i stort sett som två eller flera seriekopplade e-postservrar. Principuppbyggnaden är densamma för e-postservrar men detaljerna varierar. Variationerna har ett värde i sig, eftersom spammare och andra oönskade avsändare aldrig vet riktigt vad de har att förhålla sig till. Den stora skillnaden för företagets e-postansvarige när man använder en ISP (*Internet Service Provider*) för e-posthantering är att den största volymen skräppost tas

bort redan hos operatören, men man måste fortfarande skydda sig mot det som slipper igenom operatörens filter.




*I de flesta fall filtrerar också Internetleverantören e-posten. Den tvätten tar bort 80–90 procent av meddelandena redan innan e-posten når mottagande företags e-postservrar, men som mottagare måste man ändå se till att ta hand om det skräp som slipper igenom operatörens filter.*

## Enskild användare

Enskilda användare som driver sin egen e-postserver finns naturligtvis men om du hör till den gruppen behöver du antagligen inte den här Internetguiden. Resten av oss sitter och läser e-post på våra egna datorer och vill sannolikt se så lite som möjligt av vad som görs bakom kulisserna för att hålla skräpposten borta.

Oavsett om man kopplar upp sig direkt mot en operatör eller har företagets e-postserver mellan sig och Internet får man grovsorterad e-post utan det värsta skräpet. Även webbaserade e-posttjänster som Yahoo och Gmail levererar filtrerad e-post till användaren. Men man kan fortfarande behöva skydda sig med till exempel lokala spamfilter och antivirusprogram, och som alltid tänka själv och inte öppna eller klicka på vad som helst. Som användare kan man även lokalt svart- och vitlista återkommande avsändare så att man är säker på att de stoppas respektive släpps igenom.

# Hoten mot e-posten

Hoten på Internet i allmänhet och mot e-posten i synnerhet tar sig många tekniska uttryck och skurkarna förnyar sig hela tiden. Men attackerna faller ändå i några typiska kategorier som är förhållandevis statiska.

- Det finns de som tjänar pengar på att lura till sig lösenord och kontouppgifter för att till exempel tömma ett bankkonto. Det sker genom att de utger sig för att vara någon annan och frågar efter uppgifterna, genom att leta efter informationen i informationsströmmen och genom att via e-post installera mjukvara i användarnas datorer som letar efter och skickar iväg de uppgifter som de kriminella behöver. Företeelsen kallas *phishing*, eller nätfiske på svenska.
- Andra vill avlyssna informationsflödet eller förvanska det. Det kan till exempel handla om att söka information för att göra fördelaktiga aktieaffärer eller genom att skicka falsk information för att lura andra att göra dåliga affärer som avsändaren tjänar på.
- Ytterligare andra vill installera program på klientdatorerna för att ta kontroll över dem. Här är motivet oftast att kunna skicka ytterligare spam men det kan även användas till att göra attacker mot banker och liknande. Ett nät av sådana kapade datorer kallas botnet.
- Många skickar oönskad massreklam för produkter och tjänster som kan vara legitima, men oftast är det frågan om bondfångeri.
- Ytterligare en kategori är bara ute för att ställa till oreda i största allmänhet.

Många attacker är en kombination av kategorierna ovan.

## Skadliga meddelanden

Innehållet i själva e-postmeddelandena är det som många förknippar med skadlig e-post. Det kan handla om spam, det vill säga oönskade massutskick som på grund av sin stora volym fyller inkorgarna om de inte filtrerats bort tidigare. Spam är ofta relativt harmlöst om man tittar på enskilda meddelanden, men blotta mängden spam gör det ändå till ett allvarligt hot mot e-postens funktion. Spammare gömmer sig ofta bakom andra identiteter och skickar inte sällan via infekterade datorer, men här handlar det mest om att slippa igenom spamfilter och bara ibland om att få mottagaren att tro att meddelandet verkligen kommer från den som står som avsändare.

Phishing, eller nätfiske, är en elakare form av oönskad e-post. Avsändaren försöker lura av mottagaren lösenord och annan känslig information, oftast genom att utge sig för att vara någon annan, och då gärna en avsändare som mottagaren kan antas ha förtroende för. Phishing-attacker måste inte skickas i gigantiska volymer, men oftast gör man det ändå för att öka chansen att åtminstone någon luras. Här handlar det alltså både om att luras i meddelandet och att försöka se ut som om man är någon annan, mer pålitlig avsändare, för att mottagaren ska göra som man säger.

Skadlig kod kan ha samma syfte som phishing, att lura till sig känslig information, men i det här fallet inte genom att be mottagaren om den utan genom att installera skadlig kod som letar rätt på informationen och skickar tillbaka den till den som är det verkliga upphovet till attacken. Det kan också handla om att ta kontroll över en dator för att kunna skicka mera spam från den. Syftet kan också vara att helt enkelt ställa till oreda genom att göra mottagarens dator helt eller delvis obrukbar. Virus, trojaner och maskar är tre vanliga former av skadlig kod. Man blir oftast infekterad genom att klicka på en länk eller genom att öppna en bilaga.

Som enskild användare med en sofistikerad operatör mellan sig och Internet ser det nog ut som om mängden spam minskar eller i alla fall är konstant. Men de som lagt sin e-postserver direkt på Internet vet att volymen i själva verket ökar och att de stora operatörerna tvingas lägga stora resurser på att blockera den värsta spammen.

Det är viktigt att göra skillnad på spammare som bara köper en billig kanal för tvivelaktig reklam och mer organiserade aktörer som driver gigantiska så kallade botnets av kapade datorer. De senare agerar ofta underleverantörer till spammare och säljer tjänsten ”spridning av spam”. Spammarna är irriterande medan underleverantörerna är stora, mer eller mindre kriminella organisationer som använder den absolut senaste tekniken för att ta kontroll över oskyldiga datorer och det är dessa som myndigheterna måste försöka stoppa.

Om man genom dålig säkerhet har släppt in botnets i sin dator bidrar man inte bara till spridningen av spam, man kommer också se sitt rykte som e-postavsändare förstöras till den grad att det blir svårt att skicka legitim e-post till legitima mottagare.

## Falska avsändare

Ett vanligt sätt att lura mottagaren att lita på e-post som han inte ens borde öppna är att avsändaren låtsas vara en annan, betrodd källa (så kallad spoofing). Om man kan få mottagaren att tro att e-posten verkligen kommer från banken ökar chansen att han gör som man ber honom om i meddelandet. De vanligaste sätten är att skriva ett annat mer trovärdigt namn som avsändare eller att kapa datorer för att skicka spam. I det senare fallet skickas e-posten verkligen från en oskyldig användares dator fast meddelandet kommer naturligtvis ursprungligen från en allt annat än oskyldig avsändare.

Lyckligtvis finns det motmedel. Det går att skydda sin e-post med signaturer och nycklar. Ju fler mekanismer man inför desto större blir chansen att man kan avslöja bedragare i den inkommande e-posten. Men det handlar också om att skydda sitt rykte som avsändare. Dels hindrar man andra att solka ned sin domän, och dels ger det poäng i antispam-program om man använder olika skyddsmekanismer.

Men att signera sin e-post har bara ett begränsat värde om man inte samtidigt talar om för omvärlden vilka signeringsrutiner man har, vilka servrar man skickar från och vad mottagaren rekommenderas att göra med e-post som inte uppfyller de krav som ställts upp.

Det finns nämligen en rätt stor gråzon där signaturer och checksummor kan brytas av att en server på vägen gör någon liten oavsiktlig ändring i till exempel hur adressen skrivs i e-postmeddelandet. Det förekommer även en del slarv på den sändande sidan så det är inte givet att man ska kasta all signerad e-post som inte är perfekt.

Man kan till exempel publicera en regel som säger att alla mottagande e-postservrar också får skicka e-post, namnge andra servrar som får skicka e-post, att allt som anses legitimt av en stor tjänst som Gmail är legitimt för oss, och att e-post från alla andra avsändare är att anse som falsk.

Det finns sedan några år en fungerande standard, SPF (*Sender Policy Framework*), för att beskriva den här typen av policyregler men den används fortfarande i alltför liten omfattning.

Man kan signera och ta ansvar för sin utgående e-post med *Domain Key Identified Mail* (DKIM). DKIM hanterar problemet att spammare och nätfiskare utger sig för att vara någon annan än de är, och används även för att verifiera att meddelandet inte ändrats på vägen.

Signering med DKIM är en användbar teknik för tunga avsändare av e-post som vet om att deras kunder och användare utsätts för phishing. Det kan även vara anledning för en mottagare att vitlista domänen, det vill säga att sätta upp den på en lista över godkända avsändare, vilket drastiskt ökar chanserna att e-posten kommer fram till den mottagaren. Flera stora e-postoperatörer som Yahoo och Gmail signerar all sin e-post enligt DKIM. Men för e-post som kommer andra vägar är det svårt att veta om man som mottagare ska förvänta sig en signatur, och vad man ska göra om den inte finns där.

Man behöver även kunna hantera problemet att någon kan ta bort signaturer från signerad e-post utan att mottagaren vet om det. För om man inte vet om att något saknas kan ett förvanskat meddelande som i själva verket kommer från en annan källa tas som legitimt. Med ADSP (*Author Domain Signing Practices*) talar avsändaren om vad den har för regler för signering av e-post (till exempel alltid) och vad mottagaren rekommenderas att göra om något inte stämmer.

En svaghet i DKIM är att vanlig DNS inte ger tillräckligt skydd för de publika nycklarna som lagras där, se avsnittet An-

grepp på katalogtjänsten nedan. Säker DNS, DNSSEC, löser det problemet och som i så många andra fall är det kombinationer av säkerhetsåtgärder som ger ett tillräckligt skydd utan uppenbara svagheter.

## Avlyssning

FRA-debatten har lyft fram integritetsfrågorna på nätet. Det står numera klart för de flesta att kommunikation på Internet kan avlyssnas, och även om man väljer att lita på FRA finns det många grupperingar inom och utanför landets gränser som inte förtjänar ett sådant förtroende. Med ökande användning av tjänster för spamtvätt av e-posten finns det också en högst reell möjlighet att e-post från en svensk avsändare till en svensk mottagare har varit utomlands på vägen. Då har inte bara FRA utan även andra länders underrättelsetjänster och mindre nogräknade organisationer haft möjlighet att avlyssna trafiken. Om man sysslar med produktutveckling, gör känsliga affärer eller har någon annan verksamhet där man behöver skydda sina hemligheter är det naturligtvis inte tillfredsställande.

*”Då har inte bara FRA utan även andra länders underrättelsetjänster och mindre nogräknade organisationer haft möjlighet att avlyssna trafiken.”*

## Förvanskat innehåll

Förvanskning av innehåll använder ungefär samma svagheter i e-postsystemen som gör avlyssning möjlig. Men syftet är vanligen ett annat – avlyssnare vill komma åt hemligheter helst utan att det märks medan de som förvanskar innehåll vill åstadkomma någon form av skada genom att stoppa in felaktig information i flödet. Avlyssning görs ofta av en stor ström av information och i sin mest renodlade form är det underrättelsetjänster som kartlägger samhällets medborgare genom att lyssna på det mesta och försöka avgöra vad som är signifikant information. De som ändrar information är ofta ute efter en mer riktad attack. Denna typ av hot är kanske inte vanlig mot gemene man eller mindre företag men högst reell för storföretag.

Om man vill skydda sig mot avlyssning och förvanskning av informationen i e-posten måste man skydda transportlagret med kryptering. Det finns minst två etablerade sätt att kryptera e-posten. Båda kräver att både sändare och mottagare installerar skyddet. Den ena, PGP (*Pretty Good Privacy*), hanteras på individnivå och den andra, TLS (*Transport Layer Security*), hanteras av IT-avdelningen eller motsvarande.

## Angrepp på katalogtjänsten

I stort sett all Internetanvändning bygger på domännamn i e-postadresser och URL:er, som går att komma ihåg och i sin tur kan översättas till IP-adresser. IP-adresser är siffror som saknar mening för de flesta människor, men är det som datorer och nätverk använder som ”telefonnummer”. Katalogen som översätter domännamn till IP-adresser kallas DNS (*Domain Name System*) och ligger distribuerat på DNS-servrar.

Denna katalog är helt livsviktig för e-postens funktion, och den ansågs länge vara tillräckligt säker. Den uppfattade säkerheten och den universella täckningen har gjort att katalogen även används för att lagra certifikat och policyer för olika säkerhetssystem. Men för ett par år sedan visade forskaren Dan Kaminsky att det var förvånansvärt enkelt att lura DNS-systemet. Bland möjliga attacker på DNS kan nämnas att peka till felaktiga IP-adresser, lägga in felaktiga DKIM-nycklar eller korrumpera SPF-data i DNS.

*”Tyvärr är DNS lågt prioriterat i många organisationer. Kunskaperna brister, DNS går på uttjänta servrar och säkerhetsmedvetandet motsvarar inte DNS kritiska roll.”*

Tyvärr är DNS lågt prioriterat i många organisationer. Kunskaperna brister, DNS går på uttjänta servrar och säkerhetsmedvetandet motsvarar inte DNS kritiska roll. För om DNS är nere, någon lyckats föra in falsk information eller om den är avstängd så får man ingen e-post. Kaminsky visade hur lätt det är att lura DNS men det går långsamt att förändra attityderna ute i företagen.

Men allt är inte svart. DNSSEC inför säkerhet i DNS och i Sverige har vi haft möjlighet att utnyttja detta under flera år.

## Säkerhetskultur

Inga lås och larm i världen hjälper om man aningslöst öppnar när det ringer på dörren när som helst på dygnet eller om man går hemifrån utan att låsa sina fina lås. Internetsäkerhet fungerar likadant. Utan en väl utvecklad säkerhetskultur i hela organisationen kan sofistikerade verktyg till och med få omvänd effekt när användarna känner sig säkra och börjar svara på e-post och klicka på länkar de inte borde. Därför måste varje säkerhetsstrategi för e-posten ta ansvar för säkerhetskulturen bland alla anställda som har tillgång till datorer.

## Kommersiella produkter och gratissäkerhet

Alla vill kunna lita på sin e-post och det finns två skolor med olika filosofi om hur målet ska uppnås. Den ena ser Internet som en öppen transportmekanism som inte ska förändra information, bara förflytta den. All logik och alla skyddsmekanismer ligger i ändarna och är avsändarens och mottagarens ansvar. Lösningar som distribueras som öppen källkod och en stark känsla av *community* för kunskap och support är grundpelaren för den här inriktningen. Den andra skolan ser sig som pragmatiker som gärna köper nyckelfärdiga lösningar. Det finns många säkerhetsföretag som bygger kommersiella produkter på etablerade standarder och som tillhandahåller certifikatstjänster och annat stöd.

Det ligger en del i att ”Internet som öppen plattform” har sina flesta vänner i akademiska kretsar, men det är inte fullt så enkelt som att företag köper motsvarande tjänster och får vad de vill ha. De flesta som erbjuder säkerhetslösningar erbjuder gärna innehållsrika sviter till höga kostnader och då måste man ändå komplettera med andra lösningar för att få ett fullgott skydd och även dessa leverantörer har tilläggsprodukter i prislistan och så vidare. Till slut tar även den största säkerhetsbudget slut och det är svårt att veta exakt vilket skydd man har fått för pengarna.

Resonemanget är även tillämpligt på hur mycket operatörerna

ska göra med e-posten som passerar dem. Om man lägger mycket ansvar på operatörerna finns risken att de använder alltför fyrkantiga skyddsverktyg som stör andra funktioner. Det kan vara bättre att separera olika tjänster och ta ett eget ansvar för säkerheten, både på individnivå och i företaget.

Med större ansvarstagande i ändarna av e-postkonversationen blir det också lättare att upprätthålla en rimlig säkerhetskultur. Människor som vill komma åt något är som barn – de hittar en väg runt tekniska hinder. Som användare måste man tänka själv. Inte klicka på länkar utan eftertanke och googla länkar först om man misstänker att något är fel.

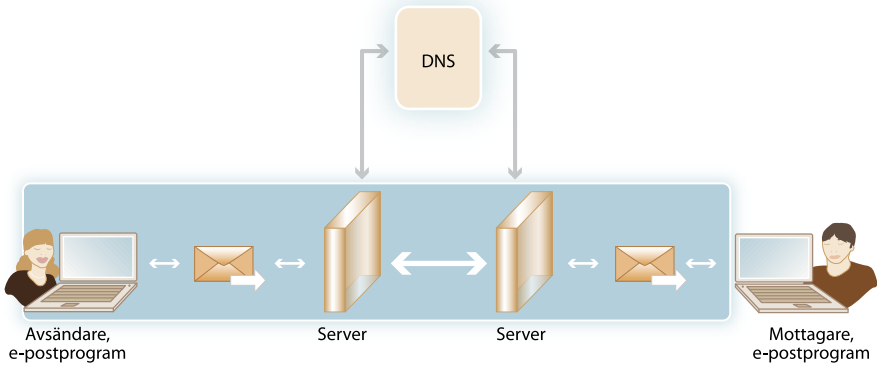
Så inget ont i att köpa teknik och tjänster, men i slutändan är det ändå klokt att själv ta kontroll över sin e-postsäkerhet för att få optimal nytta av sin budget. På köpet får man en god förståelse för vilket skydd man egentligen har och vad som händer och inte händer med känslig information, och det har även kommersiella organisationer ett intresse av.

# Skyddsmekanismer och hur de fungerar

## PGP

PGP står för *Pretty Good Privacy* och kan skydda innehållet i e-posten med både kryptering och signaturer. Mjukvaran installeras på klienten och två användare som båda har PGP kan skicka e-post mellan sig utan att någon utomstående kan läsa eller förvanska den. Signaturer tillför *non-repudiating*, eller icke-förnekande, vilket ska tolkas som att man både kan fastställa vem avsändaren är och verifiera att innehållet inte förvanskats. Dessutom är PGP ett uttryck för *end-to-end*-filosofin för Internet, där nätet bara förmedlar det råa meddelandet och alla kontroller och säkerhetsåtgärder görs hos avsändare och mottagare.

PGP skapades 1991 av amerikanen Philip Zimmerman som en reaktion på ett lagförslag om att kryptoprodukter skulle tvingas ha bakdörrar tillgängliga för amerikanska myndigheter. Kryptoprodukter betraktades dessutom som krigsmateriel och omgärdades av exportrestriktioner. Det löste Zimmerman genom att bygga PGP med öppen källkod som han sedan publicerade som en bok. Böcker skyddas av tryckfriheten och kan därför exporteras utan påföljd, hävdade Zimmerman. Det gjorde honom till folkhjälte men ledde




*Det krävs förkunskaper och en del eget arbete om man vill använda PGP till att skydda sin e-post. Belöningen är att PGP kan både signera meddelanden (skydda mot förvanskning) och kryptera dem hela vägen fram till mottagarens inkorg.*

också till en lång juridisk strid med både myndigheter som hävdade att han bröt mot exportregler och med företaget RSA som hävdade äganderätt till krypteringssystemet han använde. Zimmerman vann till slut men risken för ett långvarigt fängelsestraff hängde över honom under den fleråriga processen.

Nu när nästan två decennier gått sedan kontroversen bröt ut är det inget politiskt ställningstagande att använda PGP och det innebär inga juridiska risker. Men ursprunget i kretsar som misstror myndigheter och företag syns fortfarande i PGP:s uppbyggnad.

PGP använder en kombination av asymmetrisk och symmetrisk kryptering för att skydda innehållet i e-posten och även signera meddelanden. Det är ett vanligt missförstånd att asymmetrisk kryptering har ersatt symmetrisk kryptering. I själva verket lever båda och har hälsan och används parallellt av PGP. Symmetrisk kryptering är effektivt för stora informationsmängder och kan byggas in i hårdvara, medan asymmetrisk kryptering ofta används för att starta kommunikationen och föra över nyckeln för symmetrisk kryptering.

Den asymmetriska krypteringen i PGP använder Diffie-Hellman-algoritmen. Kärnan i den är att man kan använda en publik nyckel för att kryptera och en privat för att dekryptera, och vice versa för signaturer. Man kan alltså starta en skyddad informationsöverföring med en öppen oskyddad nyckel. Det används i sin tur för att överföra en tillfällig, symmetrisk så kallad sessionsnyckel som skapas av PGP vid varje tillfälle när e-post ska skickas.

PGP använder en så kallad Web of Trust för att verifiera den publika nyckeln med ett identitetscertifikat. *Web of Trust* innebär att andra användare, gärna sådana som är relativt kända och har ett gott anseende i Internetkretsar, går i god för det egna nycklar. Tanken är att om mottagaren känner igen och litar på en eller flera av de personer som går i god för mitt certifikat så kan de även lita på mig som avsändare. Det går även att använda andra sätt att verifiera nycklar, till exempel med en vanlig svensk e-legitimation. Däremot finns det inget standardiserat sätt att använda DNS för att lagra publika nycklar för PGP, vilket av en del uppfattas som en svaghet hos PGP.

PGP är verktyget för individer som vill kryptera sin e-post utan att en IT-avdelning behöver blandas in. PGP ger ett bra skydd men

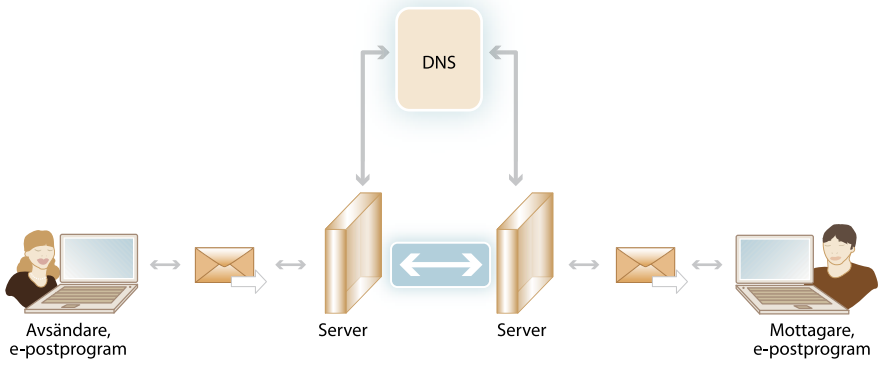
kräver att program installeras hos både avsändare och mottagare, och båda parter behöver vara förhållandevis kunniga och engagerade. En påtaglig nackdel är att om en PGP-användare skickar ett meddelande till någon som inte använder PGP kommer det eventuellt att synas svårbegripliga teckensträngar i meddelandet.

Idag förvaltas PGP som en IETF-standard under namnet OpenPGP och kan laddas ned från http://www.pgpi.org. Det finns även kommersiella tjänster och produkter baserade på PGP från PGP Corporation, se http://www.pgp.com.

## TLS

TLS (*Transport Layer Security*) skyddar mot att FRA eller andra lyssnar på kommunikationen eller förvanskar data på vägen. TLS-protokollet ger konfidentiell kommunikation med hjälp av kryptering. Som namnet säger är det transportlagret, själva kommunikationen på Internet, som skyddas. TLS kan endera vara unilateral, där servern autentiseras av klienten medan klienten är anonym mot servern, eller bilateral vilket ger bättre säkerhet. I den senare kan båda ändarna i en kommunikation vara säkra på vem de pratar med.

TLS är liksom PGP en *end-to-end*-lösning. En skillnad är att TLS-protokollet typiskt införs av IT-avdelningen och är transparent för användaren. Det innebär lägre kompetenskrav för enskilda användare.




*TLS skyddar transporten av e-post via det öppna Internet, från sändande till mottagande server.*

TLS används förutom för att skydda e-postprotokollet SMTP även för säker webbtrafik med HTTPS och kan även vara en del i en VPN-lösning. En nackdel med TLS är att till skillnad från till exempel PGP kan inte användaren få bekräftat om meddelandet verkligen var krypterat eller inte.

TLS kan användas med flera olika säkerhetsfunktioner och det förekommer minst tre olika former av handskakning för att initiera förbindelsen.

Säkerhetsarbete är en ständigt pågående katt-och-råtta-lek mellan dem som gör intrång och dem som vill skydda sig. I augusti 2009 upptäcktes ett säkerhetshål som möjliggör en så kallad man-in-the-middle-attack. Sårbarheten finns i ett flertal leverantörers implementation av TLS och visar sig när en TLS-session ska omförhandlas. En angripare som placerar sig mellan en användare och en TLS-skyddad tjänst kan skicka med godtycklig text i en pågående kommunikationssession som för användaren till synes är skyddad av TLS. Detta kan utnyttjas för att till exempel injicera en godtycklig HTTP-förfrågan. Angriparen kan dock inte dekryptera själva kommunikationen och ta del av innehållet.

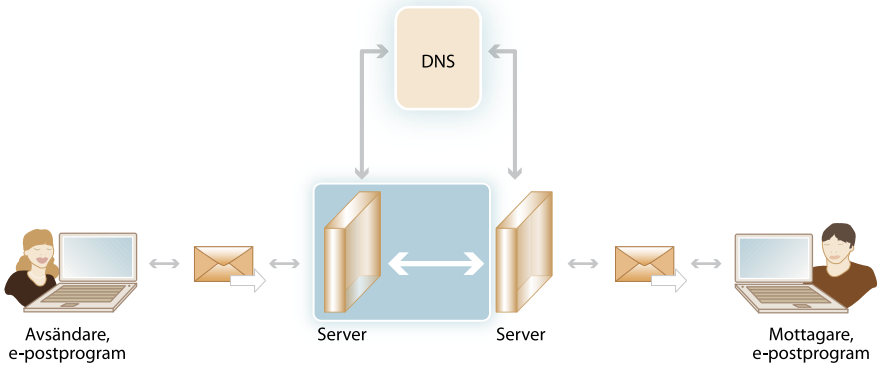
Den snabba lösningen är att stänga av omförhandling av TLS-sessioner medan en långsiktig lösning föreslagits i form striktare regler för hur omförhandling av TLS ska gå till.

En grundlig genomgång av TLS finns på http://en.wikipedia.org/wiki/Transport_Layer_Security.

## DKIM

DKIM står för *DomainKeys Identified Mail*. Det grundläggande syftet med DKIM är att den mottagande parten kan verifiera att den sändande parten verkligen är den som den utger sig för att vara och därigenom öka chansen att meddelandet tar sig genom spamfilter. DKIM skyddar normalt sett information i meddelandets huvud men kan också skydda själva innehållet.

Huvudsyftet med DKIM är att komma tillrätta med spam och phishing som utger sig vara från en legitim avsändare för att lura




*Med DKIM kan en mottagande e-postserver verifiera att meddelandet kommer från rätt sändande server och att innehållet inte har förvanskats på vägen. Det är möjligt tack vare att sändande server lagrar sin publika kryptonyckel i DNS-katalogen.*

mottagaren att öppna ett skadligt e-postmeddelande. Det ligger i både mottagarens och den förespeglade avsändarens intresse att avslöja sådan e-post.

Även DKIM är ett utryck för *end-to-end*-filosofin som ser Internet som ett renodlat transportlager där operatörer i princip inte ska göra någonting med informationen på vägen, bara skicka den från avsändare till mottagare. Men till skillnad från PGP hanteras DKIM typiskt av sändande och mottagande organisationer i stället för på individnivå. Därav *domain* i namnet. DKIM används inte bara av företag och organisationer med egen e-postserver utan även av stora e-postoperatörer som till exempel Yahoo och Gmail.

E-posten signeras av DKIM med en öppen nyckel som lagras i och hämtas från DNS. Det betyder att ingen extra infrastruktur eller tredjepartstjänst behövs för nyckelhanteringen eftersom DNS redan finns, och alla potentiella avsändare och mottagare finns också där eftersom de har e-postservrar som måste finnas i DNS för att e-posten ska fungera över huvud taget. När ett meddelande ska skickas räknar DKIM ut en checksumma för de delar avsändaren valt att skydda. Checksumman hjälper mottagaren att verifiera att meddelandet inte ändrats.

Det är dock inte ovanligt att något händer på vägen, till exempel att en mellanliggande e-postserver gör en liten förändring i till exempel hur adressen skrivs, vilket gör checksumman felaktig och

signaturen blir ogiltig. Dock är det inte självklart att ett sådant meddelande ska kastas, utan felet rapporteras framåt i leveranskedjan och mottagaren får bestämma vad som ska göras med meddelandet. Det är troligt att sådana oavsiktliga ändringar utan ont uppsåt kommer att minska genom att produktutvecklare och systemadministratörer blir mer uppmärksamma i takt med att spridningen av DKIM ökar, men för närvarande måste de hanteras. En viktig uppgift för den som sätter upp DKIM är att fastställa regler för hur e-post som saknar signatur eller där signaturen är ogiltig ska hanteras.

DKIM är transparent för enskilda användare eftersom ingenting läggs till själva meddelandet. Signaturen lägger istället till information i brevhuvudet vilket har två fördelar. De som inte har DKIM ser inga konstiga extratecken i meddelandet och andra signaturer från till exempel PGP påverkas inte.

För att få bästa kompatibilitet med andra skyddstekniker är det lämpligt att signera med DKIM som sista steg innan meddelandet skickas och att validering görs vid mottagandet som första steg eller möjligen andra efter en kontroll mot eventuella svarta listor.

DKIM har en inbyggd begränsning genom att de publika nycklarna som lagras i DNS inte är skyddade. Det hanteras genom att använda DKIM tillsammans med DNSSEC. I kombination med DNSSEC är DKIM ett robust sätt att verifiera att ett e-postmeddelande verkligen kommer från den avsändare som påstås och att innehållet inte ändrats under överföringen.

Ett intressant specialfall är när någon skickar e-post till en stor organisation och utger sig för att vara från samma domän. Om organisationen bestämt att all e-post signeras och det kommer meddelanden med en intern avsändaradress men som saknar signatur så vet man med säkerhet att det är en attack.

Det är viktigt att förstå att en giltig DKIM-signatur inte i sig är en garanti för att meddelandet inte är spam, eller att avsändardomänen har rent mjöl i påsen. Även spammare kan signera sin e-post och signaturen visar bara att meddelandet kommer från samma domän som signerat det, inte om detta är en god eller ond domän.

En giltig DKIM-signatur visar egentligen bara två saker: Att meddelandet är detsamma som avsändaren signerade eftersom

checksumman stämmer, och att den som sköter domänen godkänt signaturen eftersom det finns en valideringsnyckel i domänens DNS.

Det verkliga värdet av DKIM visar sig när man har en ström av signerade meddelanden från samma domän. Om domänen är känd för att signera ”bra” meddelanden, där det är upp till varje mottagare att hitta sin egen definition av vad som är ”bra”, kan man förutsätta att ytterligare ett signerat e-postmeddelande från samma domän även det är ”bra”.

Som avsändare av stora mängder e-post i marknadsföringssyfte kan man anta att DKIM ökar chansen att meddelandena passerar mottagarens filter, men variationen är stor eftersom användaren bestämmer reglerna och även valet av filter påverkar.

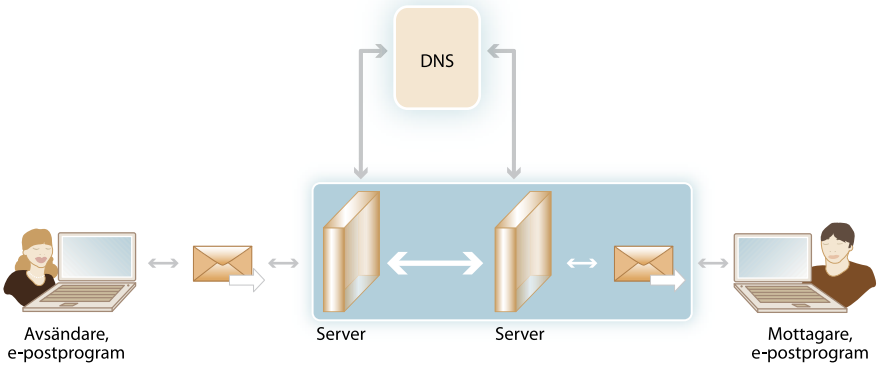
Det finns en inbyggd möjlighet att använda mer än en nyckel i en domän. Fördelen med det är att olika avdelningar under en organisations gemensamma domän kan ha sin egen signaturhantering. Det ger också möjlighet att överlåta delar av signaturhanteringen till en tredjepart som arbetar för domäninnehavaren.

DKIM togs fram av ett branschkonsortium 2004 och är idag en IETF-standard. DKIM är tillgängligt för implementation nu och körs på servern utan ingrepp i klienterna. Signering och validering med DKIM kan även outsourcas utan större tekniska problem.

## ADSP

ADSP uttyds *Author Domain Signing Practices* och är ett frivilligt tillägg till DKIM. ADSP låter en domänägare publicera en policy för hur domänen använder DKIM-signaturer. ADSP kan också informera om vilka rekommendationer avsändaren har om en signatur skulle vara felaktig. En bank eller annan organisation som har högt anseende och skickar mycket e-post kan meddela att den alltid signerar sin e-post. Avsändaren kan även rekommendera mottagaren att kasta meddelandet om det saknar korrekt DKIM-signatur. Om en mottagare då får e-post som utger sig för att komma från banken men som saknar DKIM-signatur kan man utgå från att meddelandet

*ADSP kompletterar DKIM (se sid 24) med regler för hur mottagaren ska hantera e-post med ofullständiga eller felaktiga signaturer. På sikt kommer ADSP troligen att bakas in i DKIM-standarden.*




kommer från en falsk källa och att rätt åtgärd är att kasta det.

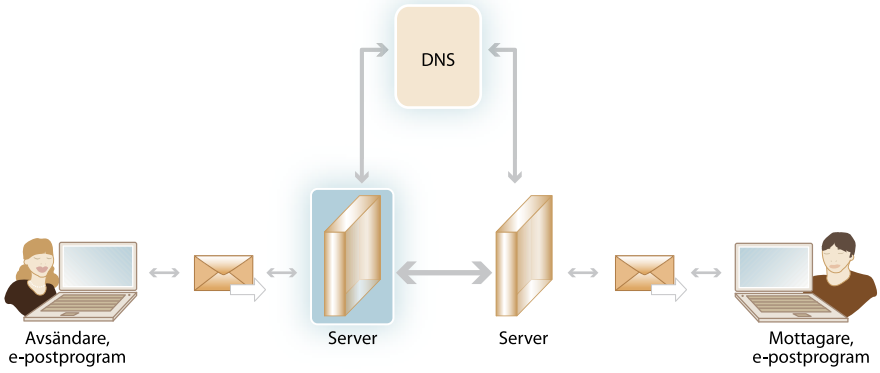
ADSP använder DNS för att lagra uppgifterna. För att skydda sin ADSP-information i DNS använder man med fördel DNSSEC. ADSP väntas bli en fullvärdig del av DKIM-standarden relativt snart.

## SPF

SPF (*Sender Policy Framework*) bygger liksom ADSP på att avsändardomänen publicerar uppgifter om hur man skickar e-post på ett sätt som mottagaren kan kontrollera och agera på. Man talar om vilka servrar som ska få skicka e-post och hur det bör tolkas ifall en annan server använts.

En stor del av den illasinnade e-posten har falska avsändaradresser. Spammare vill undvika e-post som returneras, bedragare vill sopa igen spåren, en mask vill bara skapa förvirring och bryr sig inte om avsändaradresser och de som nätfiskar låtsas vara en betrodd avsändare för att kunna stjäla inloggningsuppgifter från användare.

De flesta har väl fått meddelanden om att e-post man påstås ha sänt själv inte kommit fram. Det kan vara ett tecken på att någon annan använder ens e-postadress och därmed utnyttjar ens goda rykte.




*Med hjälp av SPF kan den som skickar e-post annonsera för omvärlden vilken eller vilka servrar som används för utgående meddelanden. Mottagande server kan då kasta meddelanden där avsändaradress och server inte stämmer överens. Liksom DKIM publiceras SPF-regler i DNS-katalogen.*

Precis som de flesta pappersbrev har e-postmeddelanden två adresser. En returadress som i pappersvärlden står på kuvertet, och en *header sender address* i e-posthuvudet som motsvarar brevhuvudet på det brevpapper som ligger i kuvertet. Det är den senare som syns som avsändare i e-postprogrammen, medan e-postservern normalt bara bryr sig om adressen som står ”på kuvertet”.

SPF skyddar adressen ”på kuvertet”. För att det ska fungera måste ägaren till den sändande domänen publicera sin SPF-information i DNS och mottagaren måste kontrollera att e-postmeddelandet stämmer med de angivna uppgifterna, till exempel vilka e-postservrar som har rätt att skicka från den angivna adressen. Det finns även planer på att framtida versioner av SPF ska kunna specificera andra regler, till exempel att avsändaren signerar med PGP.

De flesta e-postservrar stöder kontroll av SPF, eller kan fås att göra det med tilläggsprogram.

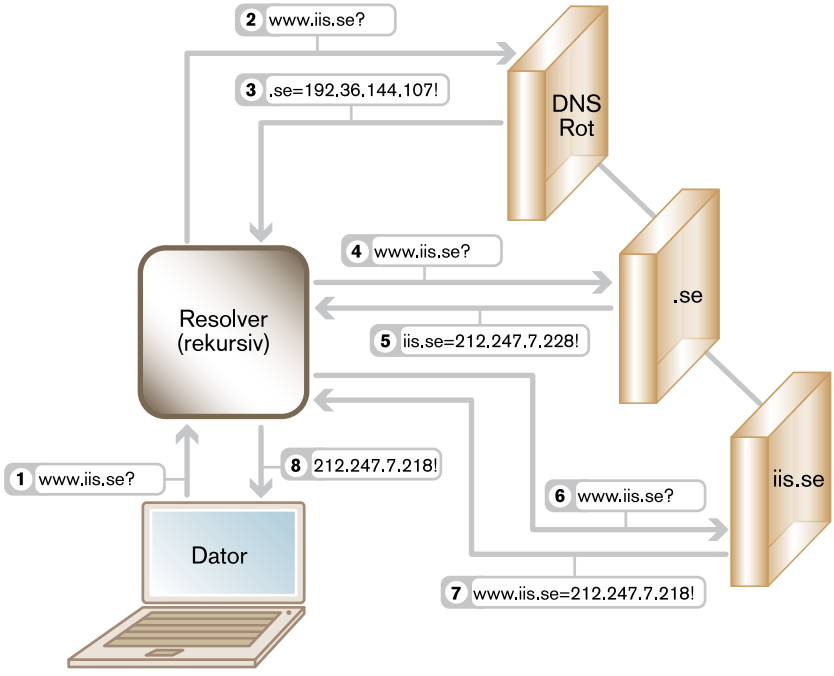
SPF är en IETF-standard. Mer finns att läsa på http://www.openspf.org.

## DNSSEC

DNSSEC (*DNS Security Extensions*) är den säkra varianten av katalogtjänsten DNS. DNS är en global, hierarkisk men distribuerad katalog

som bland annat översätter domännamn till IP-adresser. Flera sätt att kompromettera DNS har varit kända länge, men betraktades som mer eller mindre hypotetiska eftersom konsensus var att det var allför krävande att utnyttja svagheterna. Sedan kom Dan Kaminsky och chockerade världen 2008 genom att visa att det närmast var löjligt enkelt att lura DNS.

Den så kallade Kaminsky-buggen satte fart på säkerhetsarbetet




*Resolvern får fram IP-adressen för ett domännamn genom att slå i den hierarkiska och distribuerade katalogtjänsten DNS (Domain Name System). Resolvern är ett program som ofta är uppdelat på två, en så kallad stubb-resolver som är installerad på den lokala datorn och en rekursiv resolver som finns hos en Internetleverantör. Stubbresolvern ställer frågan till den rekursiva resolvern som sedan letar igenom DNS-trädet och återkommer med rätt IP-adress. Den rekursiva resolvern lagrar nyligen gjorda slag-ningar i ett cacheminne för att slippa göra om hela sökningen nästa gång någon frågar efter samma domännamn.*

inom DNS och resulterade i ett uppsving för DNSSEC. Sverige har varit och fortsätter vara en drivande kraft i införandet av DNSSEC och .SE har drivit ett pionjärarbete och signerade .se-zonen redan 2005.

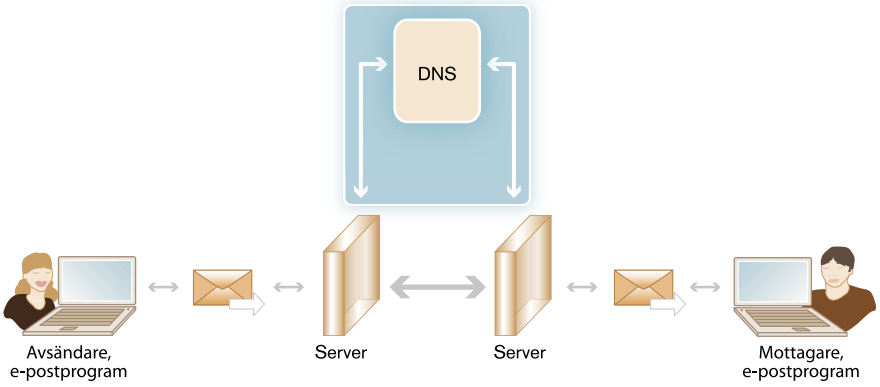
Under 2010 kommer mycket att hända och bland annat kommer rotzonen (startpunkten för DNS) införa DNSSEC. Ett antal andra toppdomäner, bland annat .org, .th och .fi är också på väg att införa DNSSEC. Det är mycket troligt att införandet kommer att accelerera betydligt i och med införandet i rot-zonen.

Med DNSSEC kan man lita på översättningen mellan domäner och IP-adresser så att e-posten går dit den ska och att den verkligen kommer från den angivna avsändardomänen. Dessutom får man en säker distributionsmetod för certifikat och nycklar som används av andra säkerhetssystem.

Funktionen i DNS bygger på den hierarkiska strukturen där en nivå hänvisar till närmast lägre nivå tills man hittat den IP-adress som motsvarar ett domännamn. DNS, med eller utan DNSSEC, består av en distribuerad katalog som innehåller de IP-adresser som är de verkliga adresserna bakom URL:er och e-postadresser och annan information. Den del som ställer frågor till DNS-systemet är en program som kallas resolver. Två svagheter i hur man programmerat resolvrar utgjorde förutsättningarna för Kaminsky-buggen. Resolvrar är *stateless* (tillståndslösa på svenska) vilket ska uttydas som att de inte håller reda på om de till exempel ställt en fråga. Det innebär bland annat att man kan skicka svar till en resolver utan att den frågat något och den kommer ändå att agera på svaret. Den andra svagheten är att svarspaketet till resolvern i och för sig innehåller många fält, men tyvärr är de flesta fält i praktiken tomma så det är ändå lätt att gissa vad som ska stå i dem. Det tar bara en bråkdels sekund att skicka ett svar så en angripare kan försöka många gånger utan ansträngning. Detta är något förenklat mekanismen för att lura en användare att använda en falsk IP-adress istället för den som verkligen tillhör en domän.

Med DNSSEC sätter man en signatur på svarspaketet så att mottagaren kan se om paketet är äkta eller inte. Säkerhetskedjan bygger bland annat på att närmast högre nivå går i god för underliggande nivå i DNS.

*DNSSEC, det vill säga säker DNS-uppslagning, kan användas till att höja säkerheten för väldigt mycket av det som sker på Internet. I e-postsammanhang utnyttjas DNSSEC bland annat till att skydda DKIM- och SPF-information som lagras i DNS-katalogen.*




Fullt utbyggt kommer DNS-roten att gå i god för alla toppdomäner som infört DNSSEC, och en hundraprocentig täckning för toppdomänerna är målet. Större organisationer som har många domäner under sin huvuddomän kan på motsvarande sätt säkra underdomänerna så länge kedjan från toppdomänen är obruten. Det är viktigt med stor täckning eftersom skyddet för en mottagare kräver att avsändaren använder DNSSEC.

En domänägare under toppdomänen .se kan beställa DNSSEC från ett urval av .SE:s ombud. Startavgiften fastställs av ombudet och varierar.

DNSSEC är en tjänst som inte ställer några särskilda tekniska krav varken hos domännamnsinnehavaren eller hos Internetanvändaren. Dock måste DNS- och resolver-operatören, vanligen ett ombud eller en Internetleverantör, kunna hantera DNSSEC.

Man kan även administrera sin egen DNS men det är då viktigt att ha tillräcklig kompetens även på DNSSEC eftersom misstag i administrationen kan leda till att domännamnet, och därmed både webbplats och e-post, försvinner från Internet.

Oavsett om man gör det själv eller outsourcar DNS-hanteringen måste den som administrerar domänens DNSSEC-nycklar ha ett certifikat från en av .SE godkänd certifikatsutfärdare CA (*Certificate Authority*) för att identifiera sig i användargränssnittet.

## Antispam

Det finns ett stort antal kommersiella produkter för att motverka spam, för många för att lista i denna guide. Dessutom förändras fältet hela tiden i försöken att hålla jämna steg med spammarna. Det finns också väl fungerande gratisprogram för att städa bort spammen. Ett sådant öppen källkod-program är SpamAssassin. SpamAssassin sätter liksom de flesta andra alternativen ett betyg på varje e-postmeddelande. Administratören har i förväg bestämt vilka betygsnivåer som gäller för att släppa igenom meddelandet, lägga det i spam-foldern eller ta bort det innan adressaten ser det.

Spam filtreras bort på flera nivåer. Som användare ser man spamfiltret i sitt e-postverktyg men dessförinnan har företagets e-postserver sorterat bort spam och om man är kund hos en Internetoperatör så har denne tagit bort det värsta skräpet redan innan e-posten når företagets e-postserver.

Det finns olika åsikter om var spamfiltreringen bör ligga. Många är glada och nöjda nu när operatörerna har blivit mycket bättre på att filtrera och släpper igenom allt mindre spam trots att volymen faktiskt ökar därute. Andra anser att det sanna Internet ska vara en öppen kanal från punkt till punkt och att operatörerna ska göra så lite som möjligt. Filosofiskt är det lätt att hålla med om att kända och okända aktörer ska göra så lite som möjligt med den information de förmedlar och att sändare och mottagare ska få göra sina egna val. Men i praktiken tycker många att det är bra att slippa grovjobbet. Ytterligare en skola väljer att skicka företagets inkommande e-post på spamtvättning hos något fristående företag som erbjuder den tjänsten.

Om man väljer att sätta sin e-postserver direkt på Internet utan att utnyttja en tjänsteoperatör tvingas man själv ta ansvar för sin spamfiltrering. Även i andra änden av spektrumet måste man ta ställning, eftersom en outsourcingpartner som tvättar e-post har svårt att dra en skarp gräns mellan legitim e-post och sådant som ska kastas. Det som hamnar i gråzonen kanske man ändå måste ta ställning till hos mottagaren.

Oavsett vilket antispam-program man väljer fungerar de snarlikt.

Första steget är ofta att kontrollera mot en eller flera kända svarta listor. Dessa listor uppdateras i realtid när någon domän plötsligt börjar skicka stora mängder suspekt e-post. Genom att kolla mot en eller flera sådana listor kan man sortera bort det värsta. En annan åtgärd som är vanlig på företag som tar emot stora mängder e-post är att jämföra med tidigare e-post. Om man aldrig tidigare fått meddelanden från avsändaren släpper man inte igenom meddelandet direkt, så kallad grålistning. Om det är en spammare är det troligt att de inte försöker igen, men om det är en legitim avsändare kommer den skickande e-postservern att försöka igen och först då tittar man på meddelandet hos mottagaren. Man kan även upprätta vitlistor, som helt enkelt är listor med avsändare man litar på.

När sedan själva spamfiltret går igång tittar det på ett antal faktorer som viktas olika. Resultatet blir ett betyg i form av en siffra, och förutbestämda regler säger om betyget är tillräckligt bra för att ta emot e-posten, lägga det i spamfoldern eller kasta det innan någon får möjlighet att öppna det. Exakt vad som betygsätts och hur viktningen ser ut vill man inte avslöja för spammare men man vet att det är en variation på känt tema.

Signaturer och certifikat (PGP, DKIM, ADSP, SPF) enligt den tidigare genomgången är bra, vissa avsändarländer är dåligt, länkar är dåligt, vissa ord och mönster i innehållet är dåligt, bilagor med exekverbar kod är dåligt och så vidare.

# Kom igång med säkerhetsarbetet

Praktiskt säkerhetsarbete handlar om att hitta en balans mellan skydd och kostnad samt mellan säkerhet och den börda man lägger på användare genom restriktioner och resurskrävande säkerhetsåtgärder. Ett balanserat angreppssätt innehåller lagom många säkerhetsåtgärder enligt en väl avvägd prioritering. Flera av säkerhetsmekanismerna beskrivna i den här guiden överlappar varandra. Det är då frestande att välja en som täcker det viktigaste men eftersom det är svårt att veta vilka säkerhetsmekanismer domänen i andra änden använder kan det ändå vara motiverat att införa flera skydd som överlappar. På så sätt kan man kommunicera med god säkerhet med flera avsändare och mottagare därute.

Den mänskliga faktorn är en del av ekvationen. Att lita för mycket på en säkerhetsmekanik kan invagga användarna i en känsla av falsk säkerhet som ökar riskbeteenden. *Social engineering*, där angriparen samlar information om användaren genom att vara allmänt trevlig och ställa förment oskyldiga frågor, har fungerat sedan långt innan Internet och fortsätter att vara ett effektivt arbetssätt. Därför bör alltid användarutbildning ingå i en säkerhetsstrategi.

Det är också viktigt att veta säkerhetsstatus för den egna e-posten innan man planerar åtgärder. .SE tillhandahåller särskilt två gratistjänster som testar säkerhetsnivån och hur professionellt man satt upp sin e-post. MailCheck testar den e-postserver som finns bakom en e-postadress medan DNSCheck kollar hur DNS är inställd och hur väl den fungerar.

## MailCheck kollar e-postservern

MailCheck är en ny tjänst från .SE som ger ett samlat grepp om hur en e-postserver är inställd. Den mäter faktorer som påverkar säkerhet, snabbhet och tillförlitlighet för en e-postserver. Tjänsten är fram-

tagen för att operatörer och IT-avdelningar, men även intresserade användare, på ett enkelt sätt ska kunna testa sina e-postservar.

MailCheck är en gratis nättjänst från .SE och hittas på http://mailcheck.iis.se. Den aktuella e-postadressen skrivs in i ett enkelt användargränssnitt och sen startar man testen med ett klick.

Servern bakom MailCheck gör ett antal tester på katalogtjänsten DNS och e-postservern som hanterar det angivna e-postkontot. Grön prick vid ett deltest betyder att resultatet är bra och ingen åtgärd behövs, gul prick betyder varning och att åtgärd eventuellt behövs. Rött betyder att ett direkt fel har hittats. Dessutom betygsätter MailCheck om en e-postserver använder extra funktioner som SPF och TLS och för varje sådan tjänst utdelas en guldstjärna.

För professionella användare, som operatörer och IT-avdelningar, ger MailCheck en kontroll av det egna arbetet och en intern kvalitetsstämpel. MailCheck blir ett arbetsverktyg för organisationer som själva administrerar sina e-postservrar. En funktion där en e-postadministratör kan beställa regelbundna tester av sin server är under utveckling.

## DNSCheck kontrollerar att DNS fungerar

DNSCheck är en gratis nättjänst som hjälper företag att kontrollera, mäta och förhoppningsvis också bättre förstå hur DNS fungerar. När en domän (även kallad zon) skickas till DNSCheck kommer programmet att undersöka domänens hälsotillstånd genom att gå igenom DNS från roten (.) till toppdomänen (till exempel .se) och till slut de DNS-servrar som innehåller information om den specificerade domänen (till exempel iis.se). DNSCheck utför även en hel del andra tester, så som att kontrollera DNSSEC-signaturer, att de olika datorerna svarar på anrop och att IP-adresser är giltiga. DNSCheck finns på http://dnscheck.iis.se

## Undvik svartlistning och att fastna i spamfilter

En viktig del i det praktiska arbetet att underhålla företagets e-postmiljö är att se till att utgående e-post inte blir svartlistad. En sådan svart lista innehåller domäner som anses skicka skadlig e-post, och e-post från avsändare som finns med på listan filtreras vanligen bort i mottagande e-postservrar. Det finns några tiotal svartlistetjänster som drivs av olika organisationer som sitter mitt i ett stort flöde av e-post och därmed snabbt kan se om en domän plötsligt skickar många suspekta e-postmeddelanden. När tjänsten hittar en sådan domän förs den upp på listan. En svartlistning kan bero på att någon kapat ens e-postserver eller klientdatorer i företagsnätet och skickar stora mängder spam, men det kan också handla om att man själv gör något som uppfattas som suspekt.

Följden blir dock densamma, det blir allt svårare att få e-post att gå fram till mottagaren. Eftersom svartlistorna fungerar på snarlikt sätt och flera av dem aggregerar information från andra listor går det snabbt att hamna på så många listor att man i praktiken inte kan skicka e-post. Precis som i alla andra relationer är det lättare att behålla ett förtroende än att återskapa det om det gått förlorat. Men de flesta svarta listor går att kontakta om man anser sig orättvist behandlad och man kan även kolla om den egna domänen finns med på just den listan.

*”Eftersom svartlistorna fungerar på snarlikt sätt och flera av dem aggregerar information från andra listor går det snabbt att hamna på så många listor att man i praktiken inte kan skicka e-post.”*

Det ligger i sakens natur att spamfilter och organisationer som publicerar svarta listor aldrig avslöjar exakt vad de tittar på och hur allvarligt de ser på olika tecken på suspekt aktivitet. Men innan man kontaktar en svart lista för att bli återupprättad skadar det inte att fundera på om man faktiskt gör något som uppfattas som suspekt. Ju fler av säkerhetsmekanismerna, som beskrivs i kapitlet Skyddsmekanismer och hur de fungerar, och ju bättre ordning man har på sina certifikat, desto större är chansen att man betraktas som en källa till god e-post.

Man kan även arbeta proaktivt för att Internetoperatörer ska sätta upp företagets domän(er) på en lista över godkända avsändare som normalt släpps igenom, så kallad vitlistning.

Ett viktigt specialfall för dem som ansvarar för ett företags e-post

är att se till att massutskick från marknadsavdelningen kommer fram. Ju fler bilagor, länkar och grafik som finns i ett meddelande, desto mer misstänksamma blir både spamfilter och organisationer som driver svarta listor. Samtidigt vill marknadsförarna skicka så snygga meddelanden som möjligt. Men det är inte bara meddelandets innehåll som avgör om utskicken kommer fram eller inte. Listunderhåll, lämpliga domännamn, korrekt användning av IP-adresser och olika former av autentisering påverkar också hur bra man fungerar som sändare av marknadsbudskap via e-post.

En källa till information om hur man sänder marknadsutskick utan att fastna i filter och svarta listor är Messaging Anti-Abuse Working Group, MAAWG. Deras MAAWG Sender Best Communications Practices är en utmärkt källa till information för den som vill sköta sina e-postkampanjer professionellt, se http://www.maawg.org/system/files/news/MAAWG_Senders_BCP_Ver2.pdf.

En god start är att se till att man bara skickar till aktiva e-postadresser, det vill säga underhåller sina adresslistor. Internetoperatörer använder gamla e-postkonton som fällor. En sändare som skickar till icke-aktiva konton och gör gällande att dessa mottagare prenumererar på information fastnar i fällan och kan hamna på svarta listan som någon som inte är att lita på.

En stor del av listunderhållet kan göras av marknadsavdelningen men IT-avdelningen måste ha rutiner för att samla upp studsande e-post och använda den informationen till att underhålla listorna.

Andra åtgärder som höjer anseendet hos Internetleverantörerna är följa deras Acceptable Use Policies (AUP:s), där de klargör vad som krävs för att de ska släppa igenom till exempel en marknadsföringskampanj.

Vill man få ett gott e-postrykte bör man dessutom implementera så många autentiseringsrutiner som systemen orkar med, där SPF och DKIM står högt på listan. Alla domännamn som används bör ha något att göra med företaget och dess verksamhet och man bör hålla sig till en serie av IP-adresser. Man bör även sätta upp sin DNS så att det är lätt att matcha domännamn och IP-adresser i båda riktingarna.

# Ordlista

**ADSP** – *Author Domain Signing Practices*, ett frivilligt tillägg till DKIM

**Autentisera** – verifiera en identitet

**Botnet** – ett nät av kapade datorer som används för att skicka spam och andra oönskade meddelanden eller för överbelastningsattacker på nätet

**DKIM** – *DomainKeys Identified Mail*. Gör det möjligt att verifiera varifrån ett e-postmeddelande kommer och att skydda själva innehållet från manipulation

**DNS** – *Domain Name System*, katalogtjänsten som översätter domännamn till IP-adresser och vice versa

**DNS-check** – tjänst från .SE som testar en DNS-server

**DNSSEC** – *DNS Security Extensions* ett säkerhetstillägg till katalogtjänsten DNS

**Distribuerad katalog** – en katalog som är utspridd på många sammankopplade servrar

**FRA** – Försvarets Radioanstalt, en militär underrättelseorganisation som traditionellt utför signalspaning på radiokommunikation och som nu även övervakar trafiken på Internet

**IETF** – *Internet Engineering Task Force*, ett standardiseringsorgan för Internetprotokoll

**ISP** – *Internet Service Provider*, det vill säga en leverantör av Internettjänster

**Klient** – användarsidan i ett system där en central server samarbetar med användardatorer

**Mailcheck** – tjänst från .SE som testar kvaliteten hos en e-postadress

**Mask** – en typ av självspridande program som sprider sig utan användares hjälp. Är ofta beroende av någon form av säkerhetshål för att kunna spridas

**Milter –** kortform av *Mail filter*, det vill säga ett e-postfilter

**Molntjänst** – tjänst som finns på nätet, i kontrast till program som installeras på en egen dator

**OpenPGP** – PGP som IETF-standard

**PGP** – PGP står för Pretty Good Privacy och används för att skydda innehållet i e-posten med kryptering och signering

**Phishing** – nätfiske, att försöka förmå användare att lämna ut lösenord och annan konfidentiell information

**Publik nyckel** – kryptonyckel i ett asymmetriskt system som publiceras åtkomlig för allmänheten till skillnad från den privata nyckeln

**Resolver** – program som kommunicerar med DNS för att översätta ett domännamn till ett IP-nummer

**SMTP** – *Simple Mail Transfer Protocol* är protokollet som används mellan e-postservrar för att skicka och ta emot e-post

**Spam** – oönskad e-post som sänds i stora volymer

**SPF** – *Sender Policy Framework*, avsändardomänen publicerar uppgifter om hur man skickar e-post

**TLS** – *Transport Layer Security*, ett sätt att skydda informationen som skickas över Internet

**Virus** – en typ av skadlig kod som lägger sig i andra program utan användarens vetskap

**VPN-lösning** – Virtuellt Privat Nät, ett sätt att bygga säkra kommunikationslänkar på det öppna Internet i stället för att dra egna, fysiskt säkrade nätverk

# Länkar till referenser och källor

## ADSP

http://en.wikipedia.org/wiki/Author_Domain_Signing_Practices

## DKIM

http://www.dkim.org
http://en.wikipedia.org/wiki/Domain_Keys_Identified_Mail
http://weblog.johnlevine.com/Email/threemyths.html
http://www.dkim.org/info/dkim-faq.html
http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-15899
(Rickard Bondessons uppsats om DKIM med DNSSEC)

## DNS

http://sv.wikipedia.org/wiki/DNS
http://www.iis.se/docs/dns-internets-vagvisare.pdf
(DNS – Internets vägvisare, Internetguide av Björn Raunio)
http://www.kaminskybuggen.se/

## DNSCheck

http://dnscheck.iis.se

## DNSSEC

http://www.iis.se/domaner/dnssec

## MailCheck

http://mailcheck.iis.se

## Regler för marknadsföringsutskick

http://www.maawg.org/system/files/news/MAAWG_Senders_BCP_Ver2.pdf

## PGP

http://www.pgpi.org
http://www.pgp.com
http://en.wikipedia.org/wiki/Pretty_Good_Privacy
http://mikrodatorn.idg.se/2.1030/1.80370

## SPF

www.openspf.org/Introduction

## TLS

http://en.wikipedia.org/wiki/Transport_Layer_Security

.SE (Stiftelsen för Internetinfrastruktur) är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige. Utöver att ansvara för Internets svenska toppdomän bedriver .SE ett omfattande utvecklingsarbete:

- **.SE:s Internetguider** är en skriftserie som riktar sig till intresserade lekmannaanvändare och behandlar olika Internetfrågor. Denna publikation ingår i serien. Läs mer: iis.se/se-ar-mer/ses-publikationer.
- **Webbstjärnan** är en tävling i webbpublicering för skolan. Syftet är att dra nytta av Internets möjligheter i skolarbetet, genom att bygga en webbplats kring ett valfritt skolarbete. Läs mer: webbstjärnan.se och stjärnkikarna.se.
- **Internet för alla.** .SE bidrar till olika åtgärder för att förbättra tillgängligheten till Internet för de grupper som idag inte är anslutna till nätet.
- **Pålitlig e-post**. .SE undersöker vad som kan göras för att öka säkerheten och förtroendet för e-post för både företag och privatpersoner.
- **IPv6 och DNSSEC** är två viktiga teknikprojekt som ska säkerställa att Internets infrastruktur även i fortsättningen kan vidareutvecklas och fungera säkert. Läs mer: ipv6forum.se respektive iis.se/domaner/dnssec/.
- **Bredbandskollen** är ett konsumentverktyg som hjälper bredbandskunder att utvärdera sin bredbandsuppkoppling. Läs mer: bredbandskollen.se
- **Internetstatistik** .SE har tagit initiativ för att etablera ett samarbete kring statistik och fakta om Internet, vilket bland annat resulterat i den tryckta rapporten Svenskarna och Internet. Läs mer: iis.se/se-ar-mer/ses-publikationer och internetstatistik.se.
- **Internetfonden** bidrar till Internetutvecklingen genom att finansiera fristående projekt. Bland uppdragstagarna finns organisationer, privatpersoner och akademiska institutioner. Läs mer: iis.se/se-ar-mer/internetfonden.
- **Internetdagarna** är .SE:s årligen återkommande konferens för alla som arbetar med Internet. Läs mer: internetdagarna.se

.se

Som en del i .SE:s arbete med Internetutveckling producerar .SE ett antal skrifter under produktnamnet .SE:s Internetguider. Guiderna behandlar olika Internetrelaterade områden och riktar sig i första hand till intresserade lekmannaanvändare. En guide kan vara såväl en praktisk handbok som en mer beskrivande rapport.

.se

**Stiftelsen för Internetinfrastruktur**

ISBN 978-91-978350-8-4