Nåbarhet på nätet

Hälsoläget i .se 2010

.se

1 Introduktion

I den fjärde rapporten från .SE:s undersökning av nåbarhet på nätet och hälsoläget i .SE redovisar vi resultaten från 2010. Syftet med undersökningen är att kartlägga och analysera kvaliteten och nåbarheten i domännamnssystemet (DNS) i .se-zonen och en del andra viktiga funktioner för domäner registrerade i .se, både ett urval av domäner som representerar viktiga funktioner i samhället och ett slumpmässigt urval ur samtliga domäner i .se.

Årets undersökning är precis som tidigare år till stora delar, men inte fullständigt, en uppföljning av de tidigare undersökningar som genomförts 2007, 2008 respektive 2009. I år har vi alltså material som gör det möjligt att jämföra resultat över en fyraårsperiod.

Rapporten riktar sig främst till IT-strateger och IT-chefer, men givetvis också till alla andra med ansvar för drift och förvaltning av en verksamhets IT- och informationssystem. Den bör kunna läsas med behållning även av den mer tekniskt intresserade.

Undersökningen ingår i ett av .SE:s satsningsområden, Hälsoläget. Syftet med satsningsområdet är att övervaka kvaliteten på Internets infrastruktur i Sverige. .SE har som ambition att bidra till att infrastrukturen har god funktionalitet och hög tillgänglighet. Syftet är också att vid behov uppmärksamma brister och missförhållanden. Målsättningen för 2010 har varit att genomföra vidareutveckling och förbättringar både vad avser metodstöd och undersökningsområden.

Hälsoläget finansieras av .SE och drivs av projektledaren Patrik Wallström. Resultaten av årets undersökning har analyserats och rapporten har sammanställts av Anne-Marie Eklund Löwinder, kvalitets- och säkerhetschef på .SE. Granskningen av den statistiska analysen har genomförts av Anders Örtengren, Mistat AB.

Mer information om innehållet i rapporten kan erhållas från Anne-Marie Eklund Löwinder, och henne når man på anne-marie.eklund-lowinder@iis.se. Mer information om Hälsoläget kan man få från Patrik Wallström. Honom når man på patrik.wallstrom@iis.se.

2 Sammanfattning

Liksom tidigare år har vi i årets undersökning i första hand fokuserat på DNS-kvalitet. Vi har också granskat andra viktiga parametrar för exempelvis e-post och webb. Vi har i år dessutom tittat lite extra på utvecklingen av IPv6 och DNSSEC. Undersökningen är genomförd under oktober 2010.

2.1 670 undersökta domäner

Testerna har omfattat totalt 670 domäner fördelade på 908 unika namnservrar. Med ”unik” menas här servrar med unika IP-adresser. En namnserver hos en operatör kan härbärgera flera domäner. En jämförelse görs även med .se-zonen i sin helhet.

Vi har försökt hålla oss till ungefär samma undersökningsgrupp som den som undersöktes förra året, men förändringar har skett, vilket ger en inte hundraprocentigt jämförbar bild över åren. I fjol undersöktes till exempel 663 domäner mot årets 670. De främsta orsakerna till det förändrade antalet domäner är förändringar bland statliga myndigheter där myndigheter har lagts ner, slagits ihop eller kommit till och att vi utökat kategorin Bank och försäkring så att den i år omfattar alla registrerade företag som står under Finansinspektionens tillsyn, vilket gör att den kategorin ökat från 21 till 67 domäner. Dessutom kan en domän förekomma i flera kategorier, men de förekommer bara en gång i den sammanlagda gruppen. Det betyder att summan av alla domäner i de olika kategorierna blir 689, det finns alltså 19 dubbletter.

2.2 Mer än en fjärdedel har allvarliga fel

2007 genomförde vi den första mätningen för att få en uppfattning om hur det såg ut i .se-zonen. 2008 års undersökning gav oss en fingervisning om det hade skett en viss positiv utveckling på området. När vi 2009 började se trender kunde vi bara konstatera att förändringarna var blygsamma och att det fortfarande fanns stora problem som vi pekade på och föreslog åtgärder mot. Dessa överlämnades bl.a. till den dåvarande infrastrukturministern och Hälsoläget-rapporten har också tagits upp under en debatt i Riksdagen.

2010 kan vi, trots att vi rapporterat allvarliga brister under flera år, inte se någon större förändring till det bättre. Av de 670 domäner som ingått i undersökningsgruppen hade 25,4 procent allvarliga fel som bör åtgärdas snarast och 43,4 procent brister av en karaktär som genererar varning, vilka också bör åtgärdas även om det inte är lika akuta problem som de allvarliga felen. År 2009 var dessa siffror 23 respektive 34 procent.

Två domäner hade vid undersökningstillfället så pass allvarliga fel att de inte ens gick att testa. De fungerade så till vida att det gick att surfa till domänernas webbplatser, men sannolikt går det inte att nå dem med e-post. Vad vi kan se används dock inte dessa domäner för e-post, bara för webbtrafik, vilket kan vara en orsak till att innehavarna av dessa domäner inte ens märker att de har problem med nåbarheten. Skulle de använda DNSCheck för att testa sina domäner skulle svaret bli att domänen inte existerar.

Den totala andelen allvarliga fel och varningar har tyvärr ökat sedan förra undersökningen. Möjligen kan det till en viss del förklaras av förändringar i undersökningsgruppen, men inte helt. Slutsatsen är att vi inte ser några väsentliga förbättringar.

Vi blir egentligen inte kloka på varför det är så; om det är nonchalans, okunskap, bristande resurser eller något annat. DNS-systemet med sina namnservrar är kritiska för normal funktion hos Internet. Det behöver få komma in i finrummet och tas på allvar.

2.3 Ingen förbättring sedan förra året

Våra observationer för 2010 tyder alltså på att det inte sker några egentliga förbättringar på området över huvud taget, trots allt prat om vikten av robust infrastruktur och krav på hög tillgänglighet för till exempelvis den offentliga förvaltningens e-tjänster.

Syftet med att publicera resultaten från undersökningen en gång per år är att skapa uppmärksamhet kring de problem och brister som en hel del domäner i .se-zonen lider av. Att genomföra undersökningen flera år i följd ger dessutom möjlighet att se utvecklingstrender, om det går att spåra effekten av några av de råd och rekommendationer som vi delar med oss av och om det har föranlett åtgärder bland de undersökta verksamheterna.

Redan den första undersökningen 2007 bekräftade vår hypotes om att det generellt brister i kunskaper om vad som krävs för att hålla en hög kvalitet på till exempel domännamnssystemet (DNS), även om det alltid går att diskutera vad som är definitionen på ”hög kvalitet”. I det här fallet är det vi själva som har definierat vad vi anser vara hög kvalitet men vi har definierat nivån efter vad som rekommenderas som praxis internationellt, *Best Common Practice*. Det finns också anledning att tro att kunskapsbristen visar sig i brister när det gäller både drift och operativt ansvar.

2.4 Dominerande aktörer ökar riskerna

Spridningen av operatörer till vilka man ansluter namnservrar minskar. De stora Internetoperatörerna blir allt större och de mindre för en allt mer tynande tillvaro. En risk med detta är om en enskild operatör dominerar inom en viss kategori. Konsekvensen kan i värsta fall bli att en hel sektor drabbas om den enskilda operatören får problem.

2.5 Bristande kompetens hos namnserveroperatörer

Tidigare års undersökningsresultat har lett till slutsatsen att det finns bristande kunskaper om vad som krävs för att hålla en hög kvalitet på domännamnssystemet (DNS). Det finns anledning att tro att dessa bristande kunskaper sannolikt också omfattar drift och operativt ansvar. Det faktum att några av de grövsta felen fortfarande är relativt vanligt förekommande ger oss också svart på vitt på att situationen inte har förbättrats nämnvärt från tidigare undersökningar, snarare tvärtom. Det kan finnas skäl för ansvariga myndigheter att börja ställa relevanta krav på den som driver namnservertjänst t.ex. för offentlig förvaltning.

2.6 Bristande certifikatshantering

Hanteringen av certifikat i undersökningsgruppens webbmiljö håller fortfarande mycket dålig kvalitet i alla avseenden som undersökningen tar upp. Hos de organisationer som ingår i undersökningen hade vi förväntat oss bättre resultat, framför allt med avseende på att använda giltiga, aktuella certifikat utgivna av trovärdiga utgivare.

3 Kontrollpunkter

I undersökningen har vi bl.a. tagit reda på fakta för följande kontrollpunkter:

- Hur hanterar verksamheten sin egen DNS? Vem har hand om DNS för verksamheten, hur är det uppsatt (i relation till vad som är att betrakta som branschstandard eller Best Common Practice, BCP), vilka är de allvarligaste bristerna och inom vilka kategorier är de vanligast?

- Hur hanterar verksamheten sin e-post? Står servrarna i eller utanför Sverige, accepteras TLS/SSL (transportskydd), hur utbredd är användningen av SPF (teknik för att minska mängden skräppost).

- Hur ansluter verksamheterna sina webbplatser till Internet? Var står servrarna, vilken serverprogramvara används, använder de servercertifikat, det vill säga har de stöd för TLS/SSL (transportskydd). Hur är certifikaten beskaffade?

I årets undersökning har vi tagit bort ett test om man har namnservrarna stående hos flera operatörer (olika AS) eftersom resultatet blev för osäkert, det är helt enkelt för svårt att avgöra med tillräckligt god tillförlitlighet. Några av de stora operatörerna bygger dessutom nät idag där man använder Anycast eller på annat sätt är så robust byggda att detta med att ha namnservrarna hos en och samma operatör inte är ett problem. Det förefaller också vara en trend att ISP:erna själva tar hem driften av namnservrar inom sitt eget nät.

Testerna har genomförts på domäner och namnservrar för ett stort antal viktiga verksamheter i samhället; affärsverk och statliga bolag, börsnoterade företag, banker, försäkrings- och finansföretag, Internetoperatörer, kommuner, landsting, medieföretag och statliga myndigheter inklusive länsstyrelser samt universitet och högskolor, totalt 670 domäner. Hur de fördelar sig per kategori framgår i avsnitt 5.

Datainsamlingen har skett helt automatiskt och har omfattat tester av de allra vanligaste felen och bristerna som vi förknippar med DNS-drift, e-post och webbhantering.

Med dessa tester har vi undersökt hur väl verksamheternas system fungerar i olika avseenden, var de allvarligaste felen finns och genomfört analyser av vad det kan få för konsekvenser. I år har vi också förbättrat möjligheterna att jämföra med tidigare undersökningar då vi nu har tillgång till sammanlagt fyra års undersökningsresultat, vilket gör det möjligt att dra slutsatser om utvecklingstrender på området.

Till detta knyter vi också rekommendationer om hur vi skulle vilja att det såg ut i DNS-infrastrukturen mer generellt. Slutligen lämnar vi några råd och rekommendationer om frågeställningar för ansvariga myndigheter, lämpliga att gå vidare med och utreda mer i detalj. Vi låter dessa stå kvar i princip oförändrade från förra årets undersökning eftersom resultaten av undersökningen talar sitt tydliga språk, nämligen att inget radikalt har skett som förbättrar situationen. Vi skulle dock gärna se att myndigheter och individer i beslutande ställning tar emot förslagen och vidtar lämpliga åtgärder, inom områdena DNS, DNSSEC och IPv6.

4 DNS-tjänst med kvalitet

Domännamnssystemet är en av hörnstenarna på Internet och är till för att förenkla adressering av resurser på Internet. Varje ansluten enhet har en egen IP-adress som med hjälp av DNS kan kopplas till en adress i en form som är lättare att hantera för oss människor. Vi har använt nedanstående definition av kvalitet i DNS-tjänsten även för detta undersökningstillfälle.

Att ha en DNS-tjänst med hög kvalitet innebär i korthet:

- Att ha en robust DNS-infrastruktur med god nåbarhet.
- Att alla inblandade namnservrar svarar på frågor korrekt.
- Att domäner och servrar är korrekt uppsatta.
- Att data i domännamnssystemet om enskilda domäner är korrekta och äkta.
- Att verksamheten uppfyller de krav som ställs i relevanta Internet- och andra standarder.

Det är viktigt att den egna DNS-infrastrukturen ansluter till aktuell standard och att den är konstruerad på ett sätt som gör att den tillhandahåller en robust tjänst med god nåbarhet vare sig man driver sina namnservrar för DNS själv eller har lagt ut driften på någon extern partner.

I undersökningen utgår vi från en erfarenhetsmässigt uppbyggd branschstandard eller Best Common Practice (BCP) av vad som är att betrakta som en bra DNS-infrastruktur.

Tidigare års undersökningsresultat har lett till slutsatsen att det finns bristande kunskaper om vad som krävs för att hålla en hög kvalitet på domännamnssystemet (DNS). Det finns anledning att tro att dessa bristande kunskaper sannolikt också omfattar drift och operativt ansvar. Det faktum att några av de grövsta felen fortfarande är relativt vanligt förekommande ger oss också svart på vitt på att situationen inte har förbättrats nämnvärt från tidigare undersökningar, snarare tvärtom.

I bilaga 4 redovisar vi de viktigaste åtgärderna som behöver genomföras för att sammantaget skapa en DNS-infrastruktur med hög kvalitet.

5 Tester 2010

De genomförda testerna 2010 har omfattat både domänernas konfiguration och de namnservrar som svarar på frågor om domänen. De har också omfattat några av de enligt vår bedömning viktigaste parametrarna för e-post och webb. Vid testerna används en programvara som automatiskt kontrollerar de olika kontrollpunkter som angivits i branschstandarden för samtliga domäner som ingått i undersökningen, både för gruppen som helhet och per kategori. Detta har kompletterats med frågor bland annat om hantering av elektronisk post och webb. En del av undersökningen har dessutom genomförts för att tränga djupare in i frågor kring säkrare, mer tillgängliga och robusta e-post- respektive webbtjänster.

Testerna har omfattat totalt 670 domäner på 908 unika namnservrar. Testobjekten har grupperats i kategorier på följande sätt:

- Affärsdrivande verk och statliga bolag (40)
- Banker och försäkring (67)
- Internetoperatörer (ISP) (20)
- Kommuner (290)
- Landsting (21)
- Medieföretag (24)
- Statliga myndigheter, inklusive länsstyrelser (exkl. myndigheter under Riksdagen) (40)
- OMX30-listan (20)
- Universitet och högskolor (35)

19 domäner är dubbletter som förekommer i mer än en kategori. Alla länsstyrelser ligger under en och samma domän.

Vi rapporterar två olika typer av problem, och kategoriserar dem som antingen fel eller varningar.

Fel: Det som markeras som fel i undersökningen är sådant som direkt påverkar driften och snarast bör åtgärdas för att verksamheten ska kunna förvissa sig om god tillgänglighet och nåbarhet till DNS och andra resurser.

Varningar: Varningar är också fel som kan påverka driften, även om åtgärder inte bedöms vara lika akuta, men de skulle givetvis höja kvaliteten och nåbarheten.

6 Observationer 2010

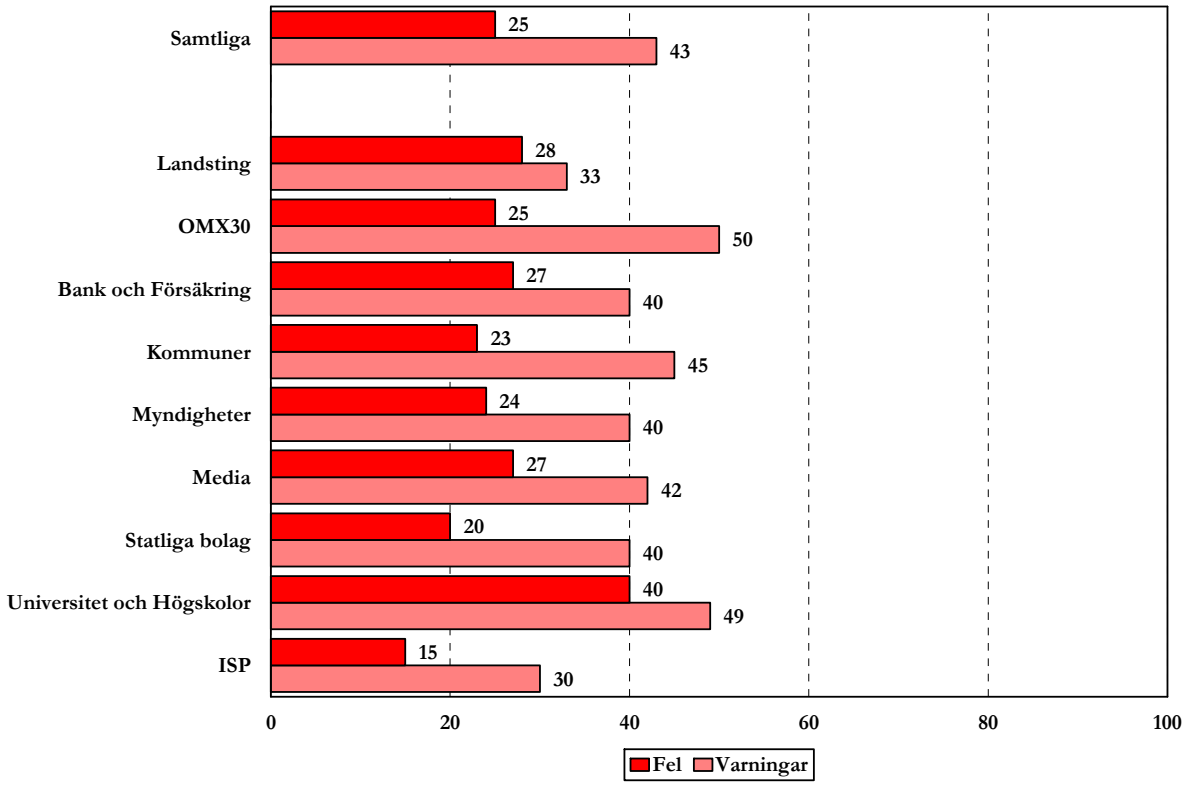
2007 genomförde vi den första mätningen för att få en uppfattning om hur det såg ut i .se-zonen. 2008 års undersökning gav oss en fingervisning om det hade skett någon positiv utveckling på området. När vi 2009 började se trender kunde vi bara konstatera att förändringarna var blygsamma och att det fortfarande fanns stora problem som vi pekade på och föreslog åtgärder mot. Dessa överlämnades bl.a. till den dåvarande infrastrukturministern och Hälsoläget-rapporten har också tagits upp under en debatt i Riksdagen samt under Trafik- och Försvarsutskottens offentliga utfrågning om IT-säkerhet 2008.

2010 kan vi konstatera att det fortfarande finns allvarliga brister och att vi inte kan se någon förändring till det bättre. Av de testade domänerna har 25,4 procent allvarliga fel som bör åtgärdas snarast och 43,4 procent brister av en karaktär som genererar varning.

6.1 Tester av DNS – fel och varningar

Hur fel och varningar fördelar sig mellan de olika kategorier som ingår i undersökningen framgår av nedanstående tabell.

Tabell 1: Fel och varningar



Tabellen visar procentandelarna fel respektive varningar för hela undersökningsgruppen (Samtliga), och för varje enskild kategori. Staplarna läses alltså så att av de 670 verksamheter som ingår i undersökningen är 25 procent behäftade med fel av allvarligare karaktär och 43 procent med fel som genererar en varning. Det är alltså en ökning från föregående års undersökning. Av de 21 undersökta landstingen är det alltså 28 procent som har allvarligare fel och 33 procent som har fel som genererar varningar, osv.

Situationen för undersökningsgruppen som helhet har försämrats sedan förra året. Myndigheter, medieföretag, universitet och högskolor samt ISP:er har fler fel i år än förra året. Universitet och högskolorna till och med väldigt många fler. Landstingen, OMX30, bank och försäkring samt statliga bolag har däremot färre fel än förra året.

Andelen varningar har dock ökat kraftigt för gruppen OMX30, och även ökat i grupperna bank och försäkring, kommuner, myndigheter och statliga bolag. Andelen varningar är oförändrad för landstingen medan den har minskat i grupperna medieföretag, universitet och högskolor samt ISP:er.

Vi kan av tabellen utläsa att det i år är universiteten och högskolorna som är den grupp som har den procentuellt största andelen fel. Inom den gruppen är närmare 40 procent av alla namnservrar behäftade med någon typ av fel som betraktas som allvarligt vilket innebär en ökning med hela 25 procent, alltså ett mycket sämre resultat än förra året. Sannolikt är alltså tillgängligheten till information och tjänster i verksamheter inom samtliga kategorier lika påverkad av fel och varningar som förra året, om inte mer. För att fördelningen fel och varningar per kategori och år, se avsnitt 6.3.

6.2 De vanligaste felen

Felkonfigurationer som utförs hos någon av de större namnserveroperatörna och som de tillämpar på alla de domäner som de hanterar får stort genomslag i resultaten från undersökningen. Värt att nämna är att .SE:s tre största återförsäljare (registrarer) har 50 procent av marknaden och de 7 största motsvarar 75 procent av marknaden. Bland namnserveroperatörerna så har de två största 36,6 procent av marknaden och de 5 största 50 procent av marknaden. Samtidigt finns det bland namnserveroperatörerna en väldigt lång svans, dvs. väldigt många små operatörer.

De vanligaste felen i DNS bland undersökta domäner och namnservrar är:

- Namnservern svarade inte på anrop via TCP. Detta beror troligtvis på att DNS-servern inte är korrekt uppsatt eller på en felaktigt konfigurerad brandvägg. Det är en ganska utbredd missuppfattning att DNS inte behöver kunna kommunicera enligt TCP-protokollet (om den inte tillhandahåller zonöverföringar). Sanningen är emellertid att TCP är ett krav enligt standard (RFC 5966, *DNS transport over TCP implementation requirements*), och trenden är att behovet av TCP ökar då nya protokoll leder till att det används i större omfattning än tidigare. Felet är en indikation på att den som har konfigurerat namnservern inte har tillräckligt aktuella kunskaper om DNS.

- Verksamheten har en inkonsekvent namnserveruppsättning (NS). De namnservrar som listats med NS-poster i en barnzon skiljer sig från den information som finns i DNS i föräldrazonen, och därmed kan namnservrarna inte svara auktoritativt och korrekt för domänen. Om informationen inte är konsekvent påverkar det tillgängligheten för domänen negativt och tyder på brister i den interna DNS-hanteringen. Följande är exempel på sådan inkonsekvens:

  - IP-adressen för en DNS-server är inte samma hos barnzonen som föräldrazonen i nivån ovanför. Detta är ett konfigurationsfel och bör korrigeras så snart som möjligt. Sannolikt har administratören för domänen glömt att göra en uppdatering vid förändring.

  - En DNS-server finns listad i föräldrazonen men inte i barnzonen. Det här är troligtvis ett administrationsfel. Föräldrazonen behöver snarast uppdateras så att den listar samma DNS-servrar som finns listade hos barnzonen. Konsekvensen av ett sådant

fel är att den redundans som någon har försökt åstadkomma i praktiken inte existerar.

- Namnservern saknar stöd för EDNS. Detta är en utökning av DNS-protokollet för att hantera DNS-svar som överstiger UDP-protokollets begränsning på 512 bytes. EDNS möjliggör större DNS-svar än så, vilket också blir allt vanligare med utökad användning av DNS med t.ex. DNSSEC och IPv6.

- DNS-servern svarade inte på anrop via UDP. Detta beror troligtvis på att DNS-servern inte är korrekt uppsatt eller på en felaktigt konfigurerad brandvägg. En namnserver som varken svarar på TCP eller UDP är inte nåbar över huvudtaget, och då kan felet stå att finna någon annanstans, till exempel i förbindelsen till namnservern eller att servern inte har en korrekt angiven IP-adress. Numera avslutas testerna på namnservern om båda dessa tillstånd har konstaterats.

- Endast en DNS-server hittades för domänen. Det bör alltid finnas minst två DNS-servrar för en domän för att kunna hantera tillfälliga problem med förbindelserna. Om den enda servern eller förbindelsen till servern skulle sluta fungera blir tjänsterna som pekas ut från namnservern också otillgängliga. Vi räknar separat för IPv4 och IPv6. Att ha för få servrar anser vi vara allvarligare för IPv4 (ger fel) medan vi i nuläget betraktar det som mindre allvarligt för IPv6 (ger varning).

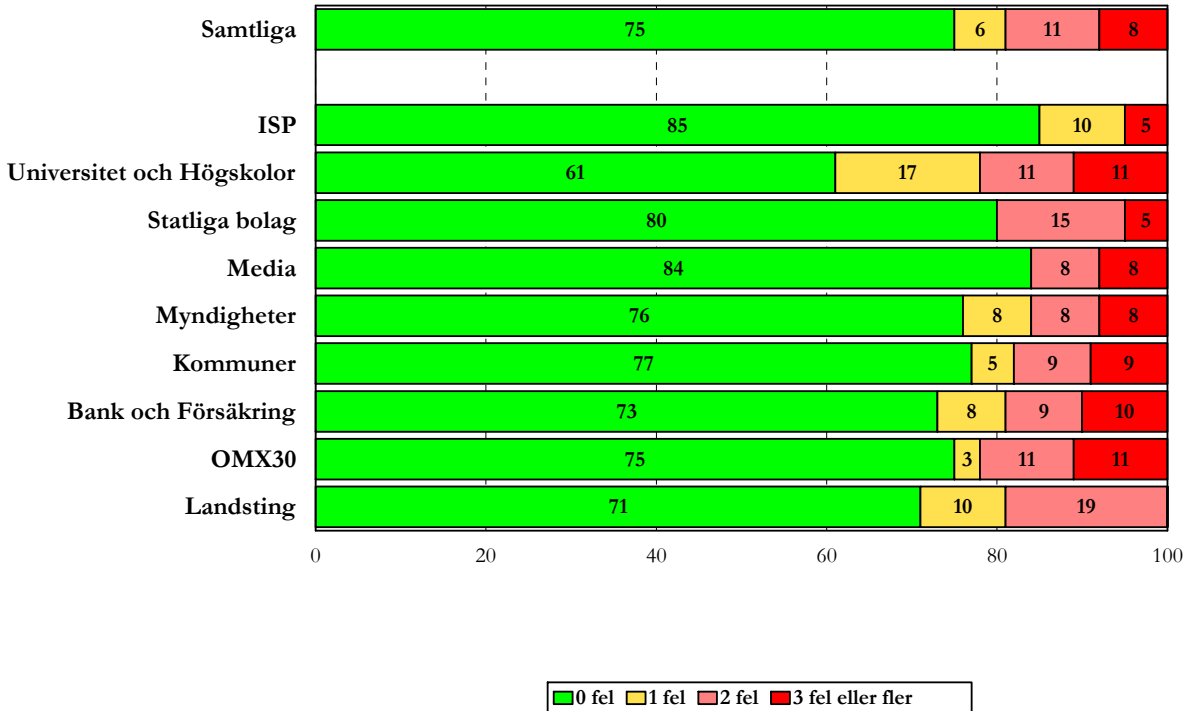
- DNS-servern är rekursiv. DNS-servern svarar på rekursiva anrop från tredje part (så som DNSCheck). Det är väldigt lätt att utnyttja öppna rekursiva resolvrar i överbelastningsattacker (s.k. DDOS-attacker), eftersom man med en väldigt liten DNS-fråga kan skapa en hävstångseffekt med ett mångdubbelt större svar. I DNS är det möjligt att förfalska avsändaradressen, och den som vill attackera ett system skapar frågor med falsk avsändaradress som genererar stora DNS-svar som går till den förmodade avsändaren och som är en tredje part vars tjänster kan bli mer eller mindre blockerade. (Se bilaga 6).

- SOA-serienumret är inte detsamma på alla DNS-servrar. Detta beror vanligtvis på en felkonfiguration, men kan ibland bero på långsam spridning av zonen till sekundära DNS-servrar. Det innebär att den som frågar efter resurser under en domän kan få olika svar beroende på vilken namnserver som får frågan.

6.2.1 MÄNGDEN FEL PER KATEGORI

Det är givetvis skillnad på om en domän har ett fel eller flera fel som många gånger dessutom samverkar. Därför har vi liksom tidigare år också tittat på spridningen av mängden fel i antal och mellan de olika kategorierna.

Tabell 2: Procentuell fördelning av mängden fel per kategori



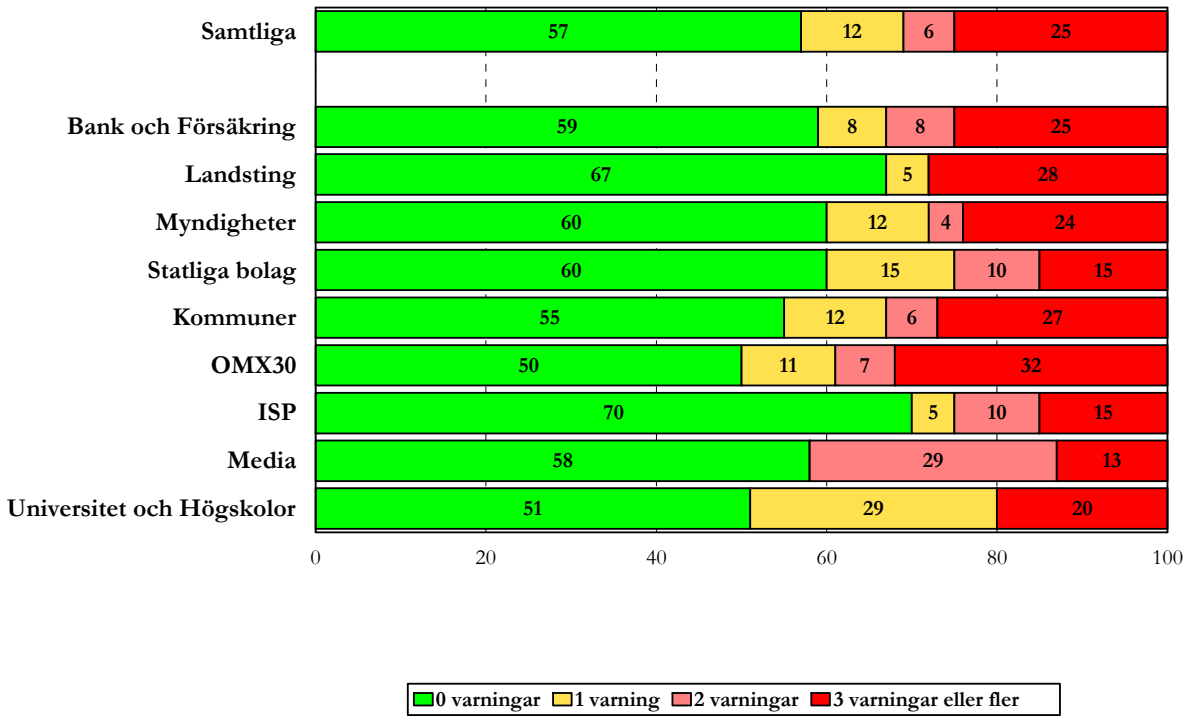
Internetoperatörerna har den lägsta felprocenten, medan universitet och högskolor i år har den högsta. Där skulle man ändå kunna förvänta sig att kunskapen och kompetensen kring DNS finns, och också erfarenhet av hur det drivs och administreras. I kategorin Universitet och högskolor verkar det ha skett en förändring som har lett till en kraftig försämring.

I år har kategorin landsting en minskad andel fel, 29 procent mot fjolårets 33. Kategorin OMX30 har också de färre fel, 25 procent mot fjolårets 30. Det är bara kategorierna ISP och Media som kommer under 20 procent fel, vilket borde vara ribban för samtliga kategorier. Under 20 procent fel kan alla komma utan ansträngning. För att komma under 15 procent krävs det lite mer.

6.2.2 MÄNGDEN VARNINGAR PER KATEGORI

Vi har också undersökt motsvarande fördelning av antalet varningar i antal och inom respektive kategori. Resultatet visas i tabellen på nästa sida.

Tabell 3: Procentuell fördelning av mängden varningar per kategori



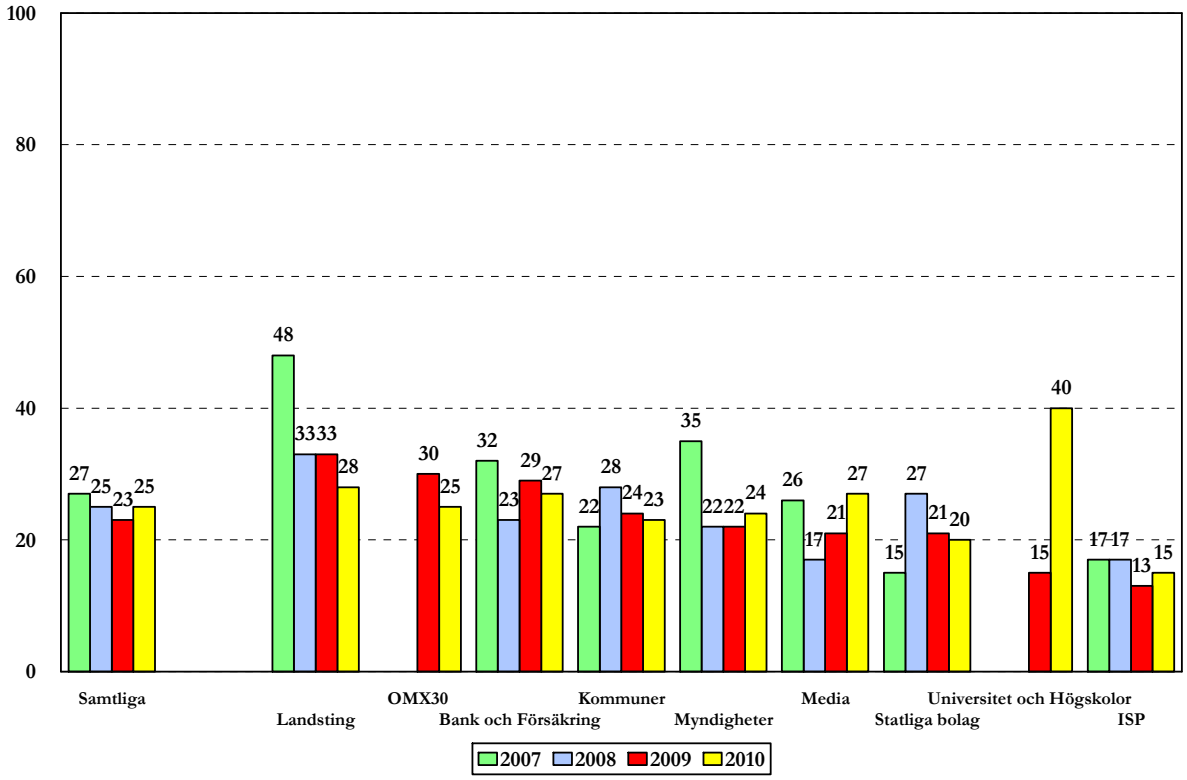
Kategorin OMX30 har flest varningar både i andel och antal, följt av universitet och högskolor. Bland kommuner och landsting har 27 respektive 28 procent tre eller fler varningar. Vår bedömning är att detta framför allt beror på administrativa brister, som till exempel att e-postadresser som anges i DNS inte fungerar. Det är generellt också mycket vanligare med varningar än med fel. Båda påverkar emellertid nåbarheten negativt.

6.3 Jämförelse över tiden - fel och varningar

I och med att vi har sparat data från tidigare undersökningar har vi möjlighet att jämföra resultaten mellan årets och tre tidigare undersökningar för de kategorier som finns med i undersökningarna för alla fyra år. Några kategorier kom till för första gången 2009 och därför kan vi för dessa kategorier bara redovisa resultat från de två senaste undersökningarna.

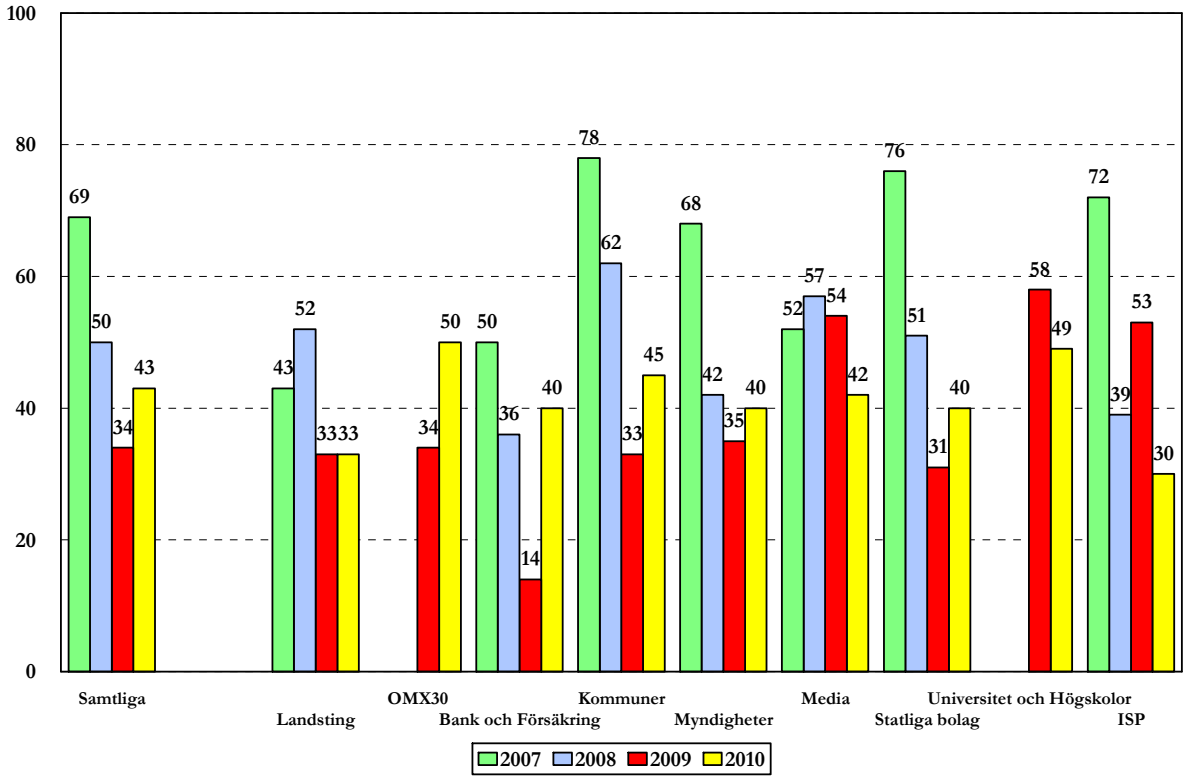
I nästa tabell jämför vi andelen fel över tiden, från 2007 till 2010 (med undantag för Universitet och högskolor respektive OMX30 som tillkom i fjol och där vi bara kan jämföra 2009 till 2010).

Tabell 4: Andel fel över tiden



Av tabellen kan vi se att situationen har förbättrats något jämfört med den första undersökningen. Däremot är årets resultat sämre än fjolårets för kategorin Samtliga. Andelen fel har ökat i kategorierna Myndigheter, Media, Universitet och högskolor samt ISP. Den har emellertid minskat sedan förra året för kategorierna OMX30, Bank och försäkring, Kommuner, Statliga bolag respektive Landsting som dessutom visar en trend med förbättrat resultat över tiden.

Tabell 5: Andel varningar över tiden

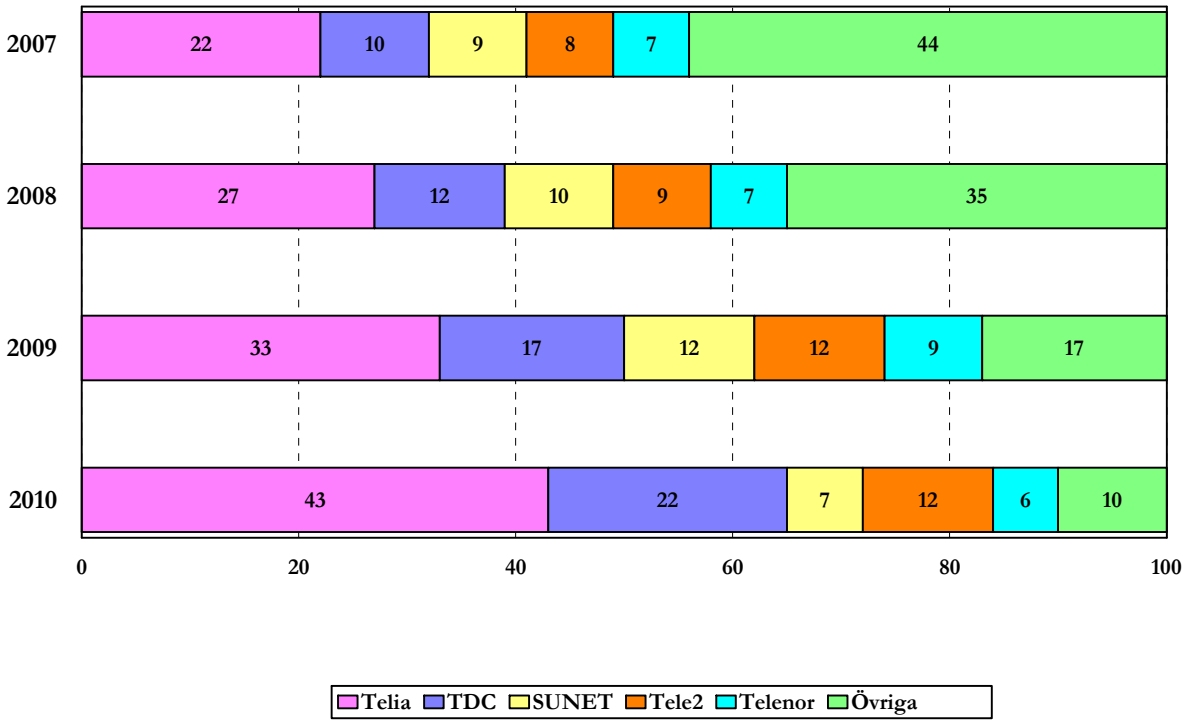


När det gäller varningar har dessa minskat kraftigt mellan 2007 och 2009. Årets ganska kraftiga ökning är ett trendbrott - åt fel håll. OMX30, Bank och försäkring och Kommuner ökar kraftigt. Även Myndigheter och Statliga bolag uppvisar en ökning. Landstingen ligger oförändrat på 33 procent medan andelen varningar minskat i Media, Universitet och högskolor samt ISP.

6.4 Anslutning av namnserver till Internet

Liksom tidigare år har vi tittat närmare på vilka operatörer som namnservrarna ansluts till för de olika verksamheterna. **Tabellen på nästa sida visar alltså inte vilken operatör som driver namnserver för domänerna, utan enbart via vilken operatör namnservern är ansluten till Internet.**

Tabell 6: Operatörsvis fördelning – anslutning av namnservrar till Internet



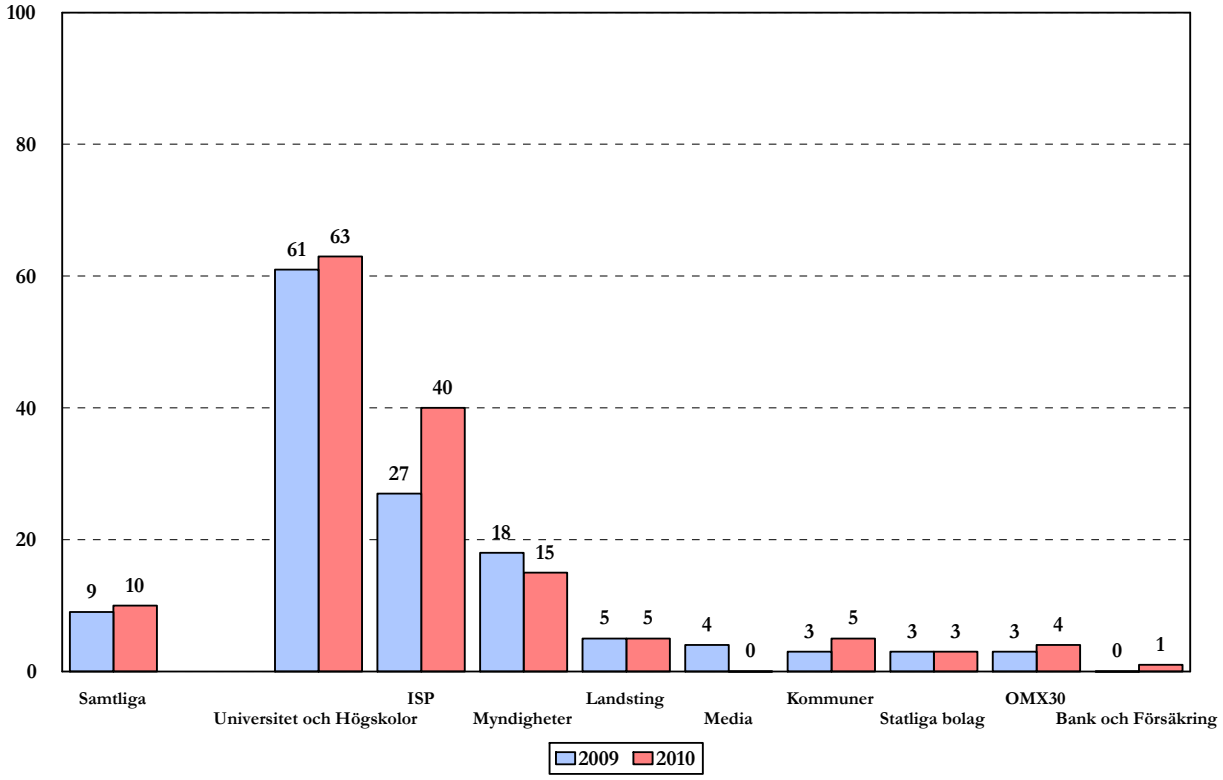
Vi konstaterar att spridningen bland operatörer när det gäller anslutning av namnservrar till Internet minskar från år till år om man tittar på den totala mängden domäner. Andelen ”Övriga” har minskat kraftigt även i år, och har gått från 44 procent 2007 till 10 procent i år. Vi ser en ökning överlag hos de största operatörerna där i synnerhet Telia ser ut att allt mer dominera marknaden och i år ökat sin andel till 43 procent jämfört med 33 procent förra året. Även TDC har ökat medan Tele 2 är oförändrat med sina 12 procent. Sunet och Telenor har minskat påtagligt. Förändringarna jämfört med förra året är betydande.

Vi kan alltså se hur spridningen av drift av namnservrar minskar bland operatörerna. De stora blir allt större och de mindre verkar föra en tynande tillvaro. En risk med detta är om en enskild operatör dominerar inom en viss kategori. Konsekvensen av detta blir i värsta fall att en hel sektor drabbas om den operatören får problem. Vi har tittat djupare i databasen för att försöka svara på frågan hur det ser ut. Det ser dock i nuläget inte ut att finnas något fall där en hel grupp domäner är beroende av enbart en leverantör, och i de fall där vi kommer närmast är leverantören i fråga Telia. Där vet vi redan att om Telia får problem så får det stora konsekvenser på många områden.

6.5 Namnservrar med IPv6

Trenden med en ökad aktivitet på IPv6-området håller i sig även om den är alldeles för blygsam. De enda som sticker ut är kategorierna Universitet och högskolor samt ISP.

Tabell 7: Använder IPv6 på namnservrar



Totalt 10 procent av de undersökta domänerna har någon namnserver som går att nå via IPv6, jämfört med 9 procent 2009. Trots att den svenska regeringen har tagit initiativ genom att kräva IPv6-stöd vid offentliga upphandlingar ser vi ingen positiv förändring i kategorin Myndigheter och en mycket blygsam sådan i kategorin Kommuner.

Adressbristen blir snart mycket akut och det är hög tid att skifta till IPv6. Det är viktigt att förstå att en sådan övergång kräver förberedelser och arbete på omkring 12-18 månader.

Att gå över till IPv6 är det enda sättet att garantera en stabil framtida Internetinfrastruktur. .SE tar en aktiv roll för att underlätta samarbete och samordning kring övergången. Av den anledningen har vi startat en webbplats för att kontinuerligt rapportera om IPv6 i Sverige. Den finns på http://ipv6.iis.se/.

6.6 Operatörer för drift av namnservrar

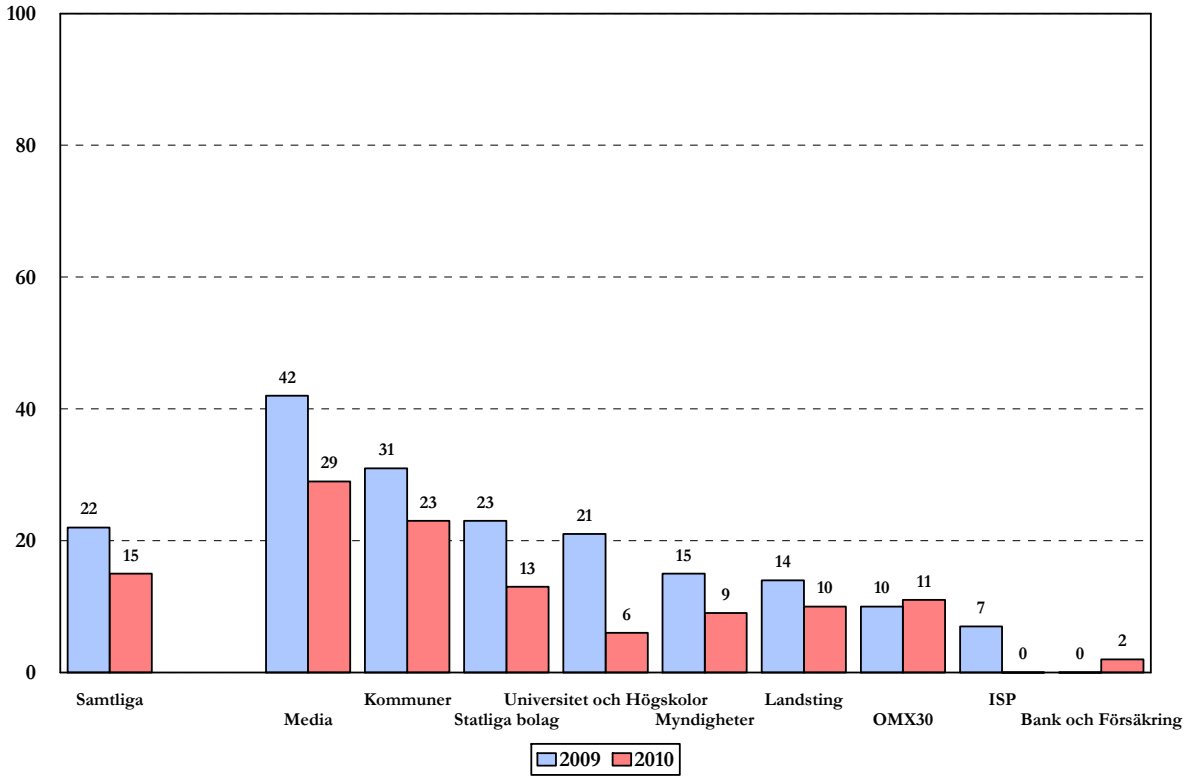
I normalfallet är det en registrar som också svarar för driften av namnservrar för en domän. De sju största registrarerna hanterar 75 procent av domänerna i se-zonen.

6.7 Namnservrar med rekursion påslaget

Öppna rekursiva namnservrar har mycket få legitima användningsområden och kan komma att utnyttjas i samband med överbelastningsattacker. En stark rekommendation är därför att eliminera möjligheten att missbruka öppna rekursiva resolvrar med hjälp av de tekniker som beskrivs i de referenser som anges i bilaga 6.

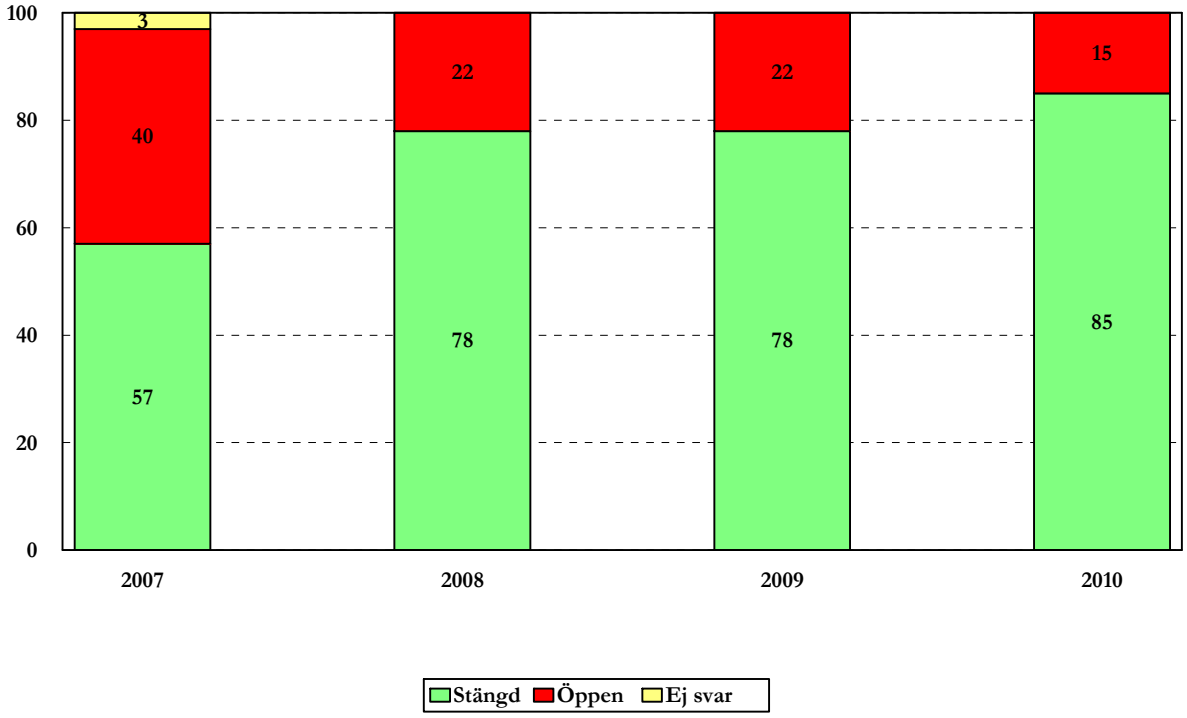
Andelen namnservrar som är öppna för rekursion minskar även i år och är nu nere i 15 procent. Det är mycket positivt, med tanke på de risker det innebär. Vanligast förekommande är det inom kategorierna Kommuner och Media även om det minskat också inom dessa kategorier jämfört med förra året, vilket framgår av tabellen nedan.

Tabell 8: Namnservrar öppna för rekursion per kategori



Öppna rekursiva namnservrar har minskat i samtliga kategorier, förutom OMX30 samt Bank och Försäkring där det faktiskt finns en liten ökning. Det mest anmärkningsvärda är kanske att kategorin ISP minskat från 7 till 0 procent, vilket tyder på att dessa har förbättrat sin infrastruktur kanske genom bättre separation mellan auktoritativa namnservrar och resolvrar.

Tabell 9: Namnservrar öppna för rekursion 2007-2009



Mellan 2007 och 2010 har andelen namnservrar med rekursion påslaget minskat kraftigt, från 40 till 15 procent. Sedan förra undersökningen har vi alltså haft en minskning med ytterligare sju procent. Detta resultat är ett av de riktigt glädjande resultaten från årets undersökning.

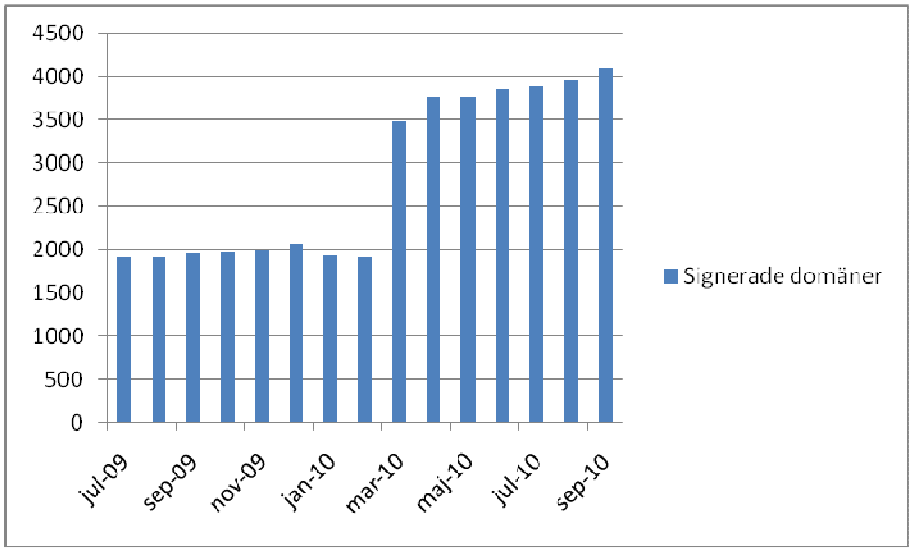
6.8 Användning av DNSSEC

För första året särredovisar vi hur många domäner som är signerade med DNSSEC. Vi har också gjort vissa ändringar i mätverktyget eftersom DNSSEC inte längre är på experiment-stadiet utan i full drift. Det innebär att vi har skärpt kraven något och därmed har ändrat nivån för vad som är fel respektive varningar i några olika avseenden. Detta är inget som påverkar resultaten i redovisningarna för övrigt eftersom vi inte har haft med DNSSEC under tidigare år.

6.8.1 Hur utbredd är användningen av DNSSEC?

Bland domänerna i undersökningsgruppen 2010 är 3,88 procent signerade med DNSSEC. Det är kommuner, myndigheter, landsting och ISP:er som har börjat anamma den säkrare tekniken. Som jämförelse kan vi nämna att i hela .se-zonen finns det för närvarande totalt knappt 4 000 domäner som har infört DNSSEC, dvs. dubbelt så många som förra året men ändå bara 0,4 procent av det totala antalet domäner. Vi ser en tillväxt, men kanske inte i den takt vi skulle önska oss. I tabellen nedan redovisas tillväxten för DNSSEC-signerade domäner i hela .se-zonen.

Tabell 10: Tillväxt – domäner med DNSSEC i hela .se-zonen



Källa: .SE:s webbplats

Hittills i år har exempelvis tre kommuner signerat sina domäner, och om tillväxten fortsätter i den takten kommer det att ta 80 år innan alla 290 kommuner är signerade.

E-delegationen har nyligen börjat publicera en lista över de myndigheter som infört IPv6 och DNSSEC. Syftet med publiceringen är att lyfta fram de myndigheter som infört IPv6 och DNSSEC som goda exempel och förebilder och därmed få fler myndigheter att följa efter. E-delegationen säger på sin webbplats att DNSSEC på myndigheterna bör införas senast sommaren 2011.

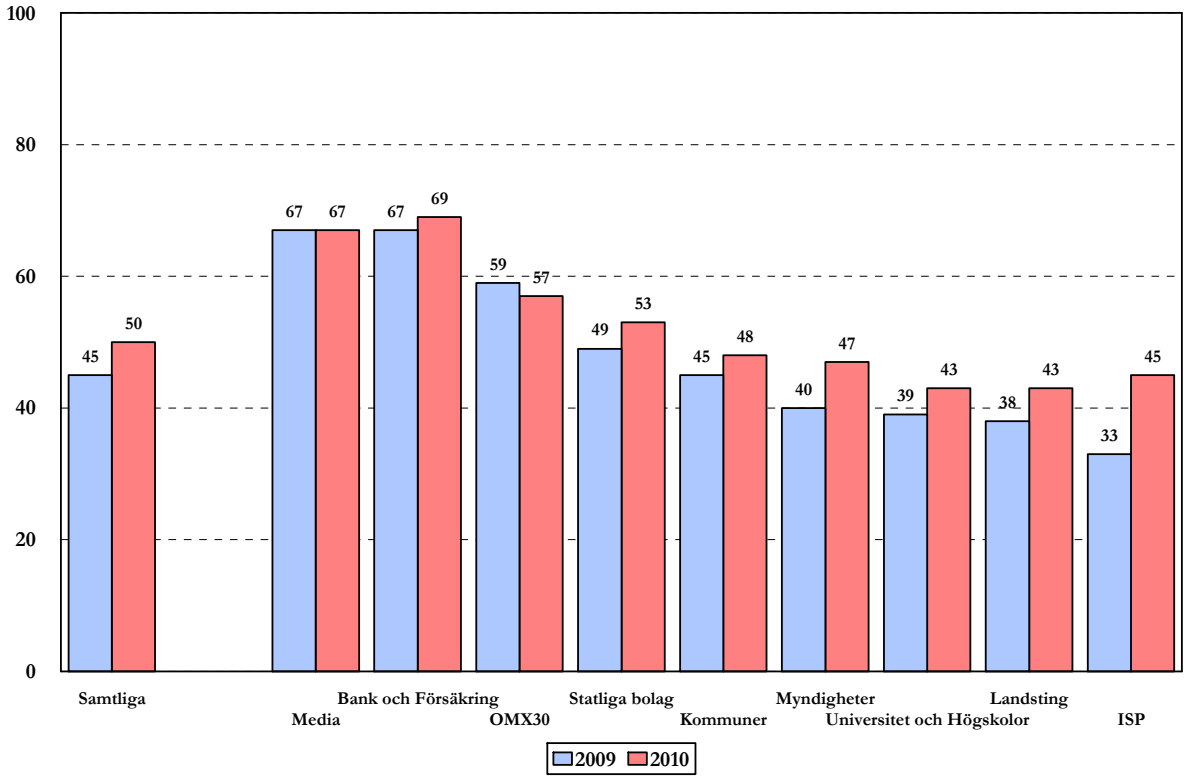
Spridningen av DNSSEC har också tagit fart bland toppdomänerna efter signeringen av rotzonen. Bara de senaste veckorna har ett antal nya toppdomäner signerats. Mer information om DNSSEC finns i bilaga 5.

7 Viktiga parametrar för e-post

7.1 Stöd för transportskydd (TLS)

För att säkert utbyta information mellan e-postservrar bör ett transportskydd läggas på kommunikationen. Av de undersökta verksamheterna 2010 har knappt hälften, eller 49,5 procent, stöd för TLS/SSL i sina e-postservrar. Det är visserligen en liten ökning från förra året (44,5), men det betyder att många inte vidtar tillräckliga åtgärder för att skydda e-posttrafiken från insyn även om situationen blivit aningen bättre. Alla programvaror har idag inbyggt stöd för det idag.

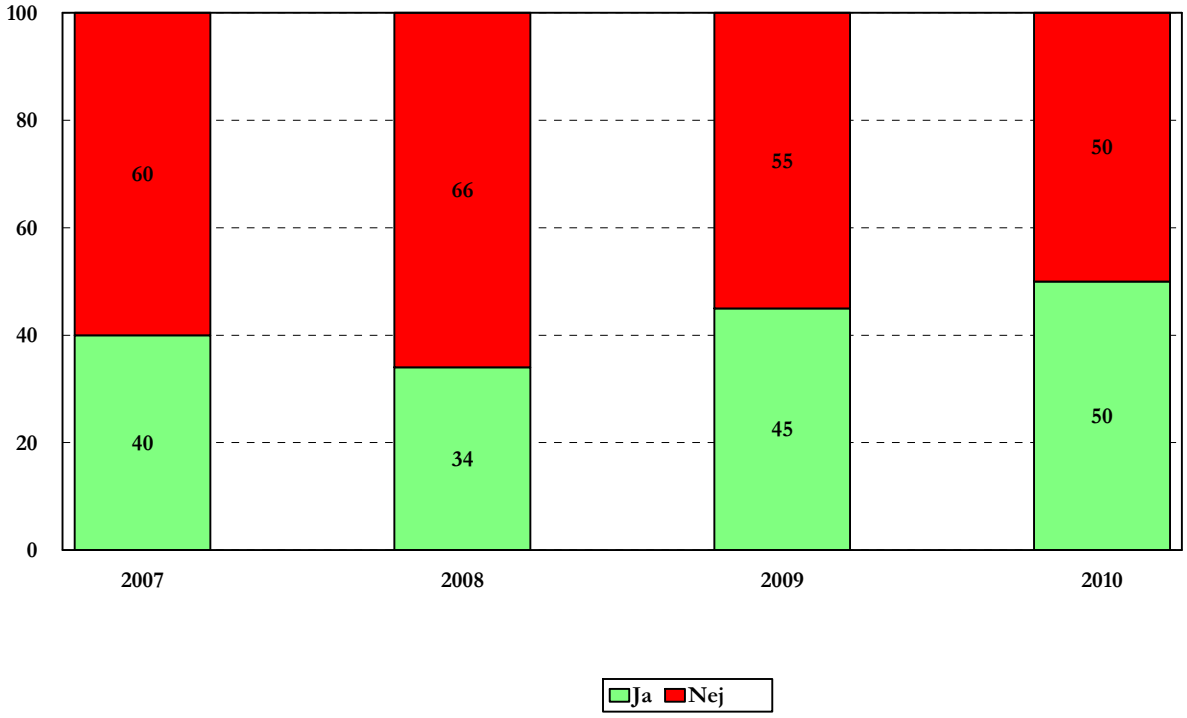
Tabell 11: E-postservrar med stöd för TLS



Användningen av StartTLS har ökat i samtliga kategorier förutom Media där det är oförändrat respektive OMX30 där det har minskat något. Vi har ingen information om orsaken till varför det är så.

Tabellen nedan visar utvecklingen de fyra senaste åren. Vi kan se att andelen e-postservrar med stöd för TLS har ökat under perioden, men det går mycket långsamt.

Tabell 12: E-postservrar med stöd för TLS 2007-2010



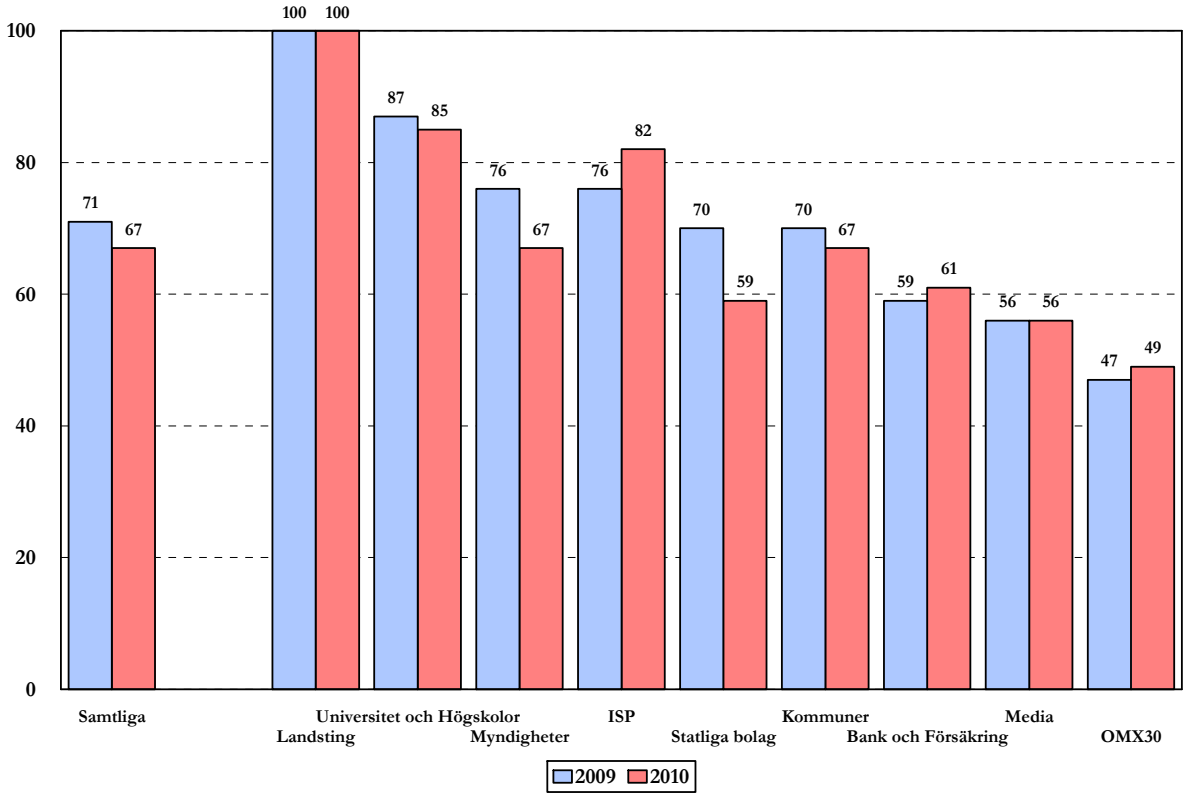
Transport Layer Security (TLS) är en öppen standard för säkert utbyte av information. TLS erbjuder konfidentialitet (kryptering) och riktighet (dataintegritet), samt beroende på användning även äkthetsskydd (källskydd). Äldre versioner av metoden benämns Secure Socket Layer (SSL). TLS/SSL kan bland annat användas för överföring av elektronisk post (SMTP). För mer information, se bilaga 9.

7.2 Placering av e-postservrar

För 2010 och de undersökta verksamheterna har 67 procent sina e-postservrar placerade i Sverige vilket är något färre än förra året. Det är viktigt att påpeka att då vi inte har någon möjlighet att avgöra var IPv6-adresserade e-postservrar står rent geografiskt så hamnar dessa i kategorin ”utanför Sverige”. I undersökningsgruppen har 1 procent av domänerna e-postservrar som är IPv6-adresserade.

Nedanstående tabell visar procentandelen e-postservrar placerade inom landet fördelat per kategori.

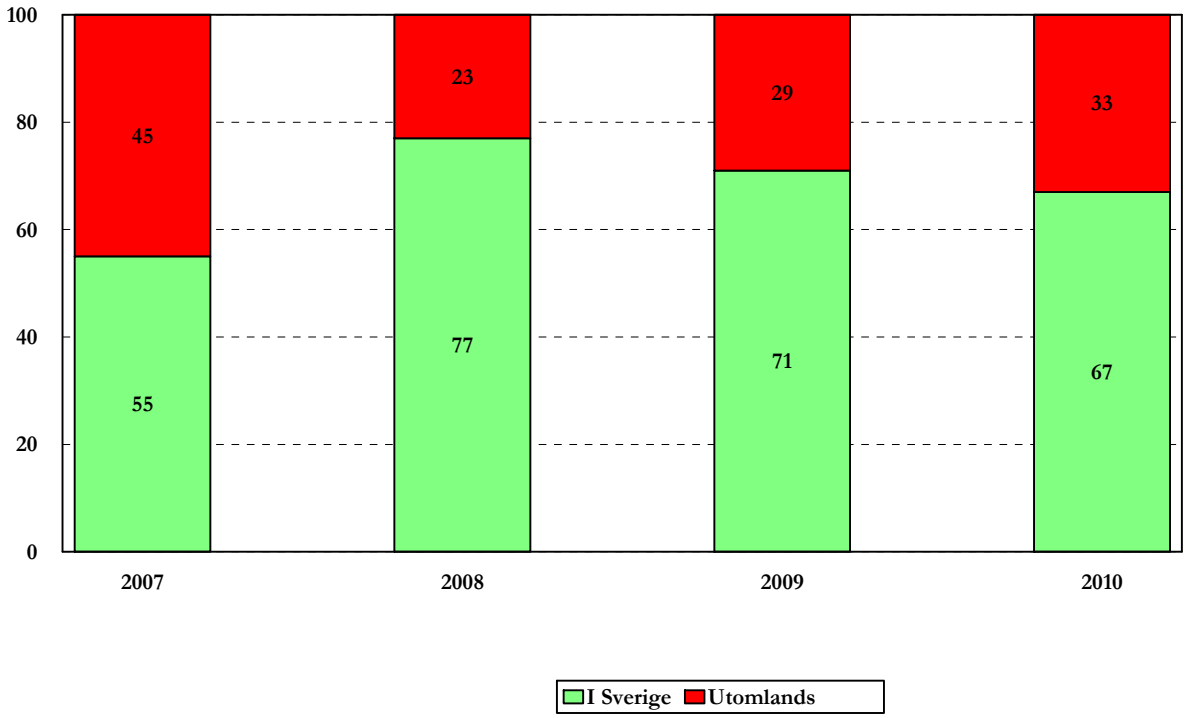
Tabell 13: Andel som har e-postservrar placerade i Sverige



Den huvudsakliga anledningen till placeringen är med största sannolikhet fortfarande densamma, dvs. att verksamheter anlitar någon tredjepartsleverantör för att sköta om filtrering av virus och skräppost (spam). För kategorin OMX30 kan det även bero på att det är multinationella verksamheter med centraliserad IT-verksamhet belägen i något annat land.

En konsekvens av att t.ex. myndigheters och kommuners e-postservrar är placerade utanför Sverige blir att en hel del av bl.a. den offentliga förvaltningens e-postkommunikation passerar ett främmande land på sin väg till mottagaren.

Tabell 14: Andel som har e-postservrar placerade i Sverige 2007-2010



Av tabellen framgår att andelen e-postservrar placerade utanför landets gränser har ökat sedan förra året. Sammanfattningsvis kan vi konstatera att det fortfarande är vanligt förekommande att verksamheter skickar sin e-post utomlands för tvätt.

Samtidigt vet vi att det fortfarande bara är hälften av de undersökta verksamheterna som använder kryptering för transportskydd av elektronisk post. Endast 50 procent av de undersökta domänerna har stöd för transportskydd med kryptering för inkommande e-post, däremot kan vi inte avgöra om de använder funktionen för utgående e-post.

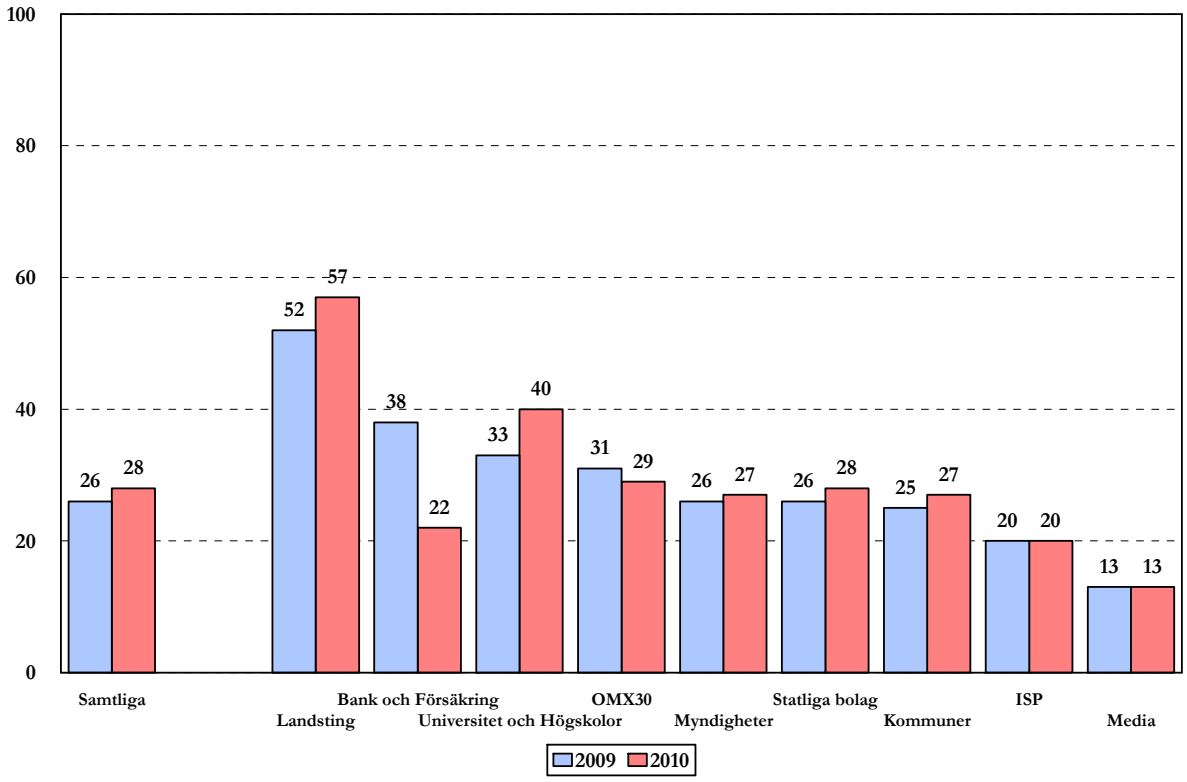
Det vi bland annat vill visa med denna del av undersökningen är att det faktum att e-post som skickas från svenska företag och myndigheter till något annat land för t.ex. spamfiltrering eller virustvätt kan få konsekvenser i Sverige med det regelverk som finns i den mycket omdebatterade FRA-lagen som riksdagen fattade beslut om 2009. Att ha e-postservrarna i utlandet innebär de facto att informationen passerar landets gränser och sedan kommer tillbaka, vilket gör det mer eller mindre omöjligt att avgöra om det är svensk trafik eller inte.

Det innebär dessutom att utländska underrättelsetjänster kan avlyssna trafiken på motsvarande sätt. Placeringen av servrar i utlandet innebär att all information passerar Sveriges gränser och att främmande stater och andra mycket enkelt kan komma åt information som kan vara känslig ur olika aspekter. Det är omöjligt att säga hur medvetna verksamhetsansvariga är om att så är fallet, och om de i så fall gjort någon konsekvensanalys.

7.3 Åtgärder mot skräppost

Standardprotokollet för att skicka e-post, SMTP, gör det möjligt att skicka meddelanden med valfri domän som avsändaradress. Det finns några olika lösningar som syftar till att begränsa framkomligheten för skräppost genom att försöka verifiera att det är legitima avsändare bakom ett meddelande. En av dessa lösningar går under benämningen Sender Policy Framework, eller SPF.

Tabell 15: Använder SPF



28 procent av de undersökta verksamheterna använder SPF. Landstingen ligger i topp, med 57 procent, medan användningen minskat kraftigt i kategorin Bank och Försäkring, vilket sannolikt förklaras av den utökade populationen i kategorin från bara de centrala bankerna till alla registrerade företag under Finansinspektionens tillsyn.

I den nu aktuella mätningen tittar vi bara på om domänen har en SPF-post publicerad eller inte. Vi gör ingen bedömning av innehållet mer än att verifiera att det är just en SPF-post.

DomainKeys Identified Mail (DKIM) är en annan teknik som skyddar valda delar av e-posthuvudet och innehållet i e-postmeddelandet mot modifiering av tredje part.

På grund av hur standarden för DKIM är utformad går det inte med exakthet att bestämma om en domän använder DKIM eller inte. I 2008 års undersökning hittade vi endast två domäner med DKIM påslaget och resultatet för 2009 var i princip lika magert. 2010 har vi

valt att inte redovisa några resultat från körningen eftersom det inte säkert går att härleda förekomsten av DKIM för en domän förrän användningen av ADSP blir mer utbredd (se bilaga 8).

Det går även att kombinera teknikerna SPF och DKIM om man vill. Vi har dock i årets undersökning inte tittat närmare på hur många som valt att göra detta.

8 Viktiga parametrar för webb

Information och tjänster som förmedlas via webbgränssnitt har kommit att bli allt vanligare, och många verksamheter är helt beroende av att deras webbtjänster fungerar och är tillgängliga för deras kunder, samarbetspartners eller för medborgare i samhället. Det finns åtgärder som kan vidtas för att se till att ha redundans även för webbtjänster. Det kan vara bra att överväga dessa om det är en kritisk funktion som tillhandahålls via webb.

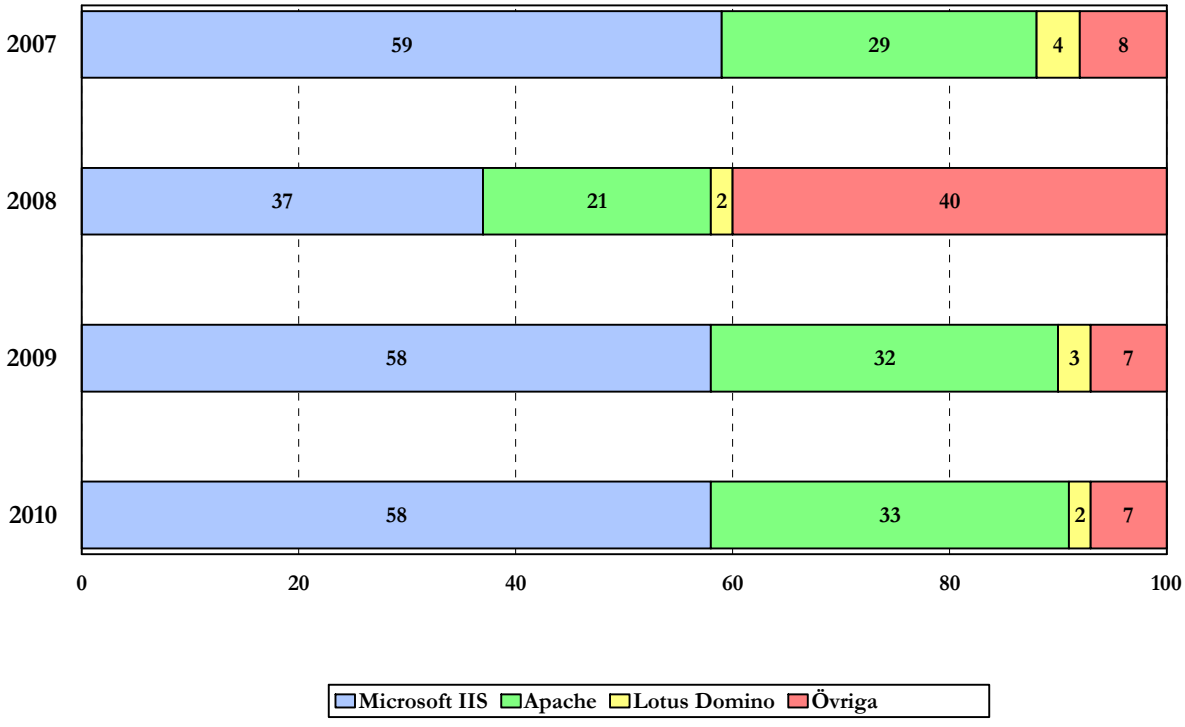
8.1 Anslutning av webbservrar

Har en verksamhet alla sina namnservrar anslutna till en och samma Internetoperatör spelar det egentligen ingen roll om man lägger webbservern där också. Får operatören problem med tillgängligheten blir inte bara namnservrarna utan också webbservern onåbar. Den som däremot har sina namnservrar placerade hos två olika operatörer kan också överväga att placera webbservern hos en tredje operatör för att uppnå största möjliga redundans.

8.2 Programvaror för webbservrar

Även i denna omgång av undersökningen har vi tittat på vilka programvaror för webbservrar som används i de undersökta verksamheterna. De klart dominerande är fortfarande Microsoft Internet Information Server (Microsoft IIS) och Apache.

Tabell 16: Programvaror som används för webbservrar



8.3 Andra intressanta iakttagelser kring webb

Genom vidareutveckling av vårt undersökningsverktyg har vi i år möjlighet att kontrollera en rad andra parametrar av intresse speciellt för webbapplikationer. Några av de mest anmärkningsvärda resultaten redovisas nedan. Många av dem blir mer intressanta nästa år, då vi faktiskt kan göra jämförelser och se om och hur det rör på sig på detta område.

En stor andel (44 procent) av de undersökta webbplatserna använder Google Analytics för insamling av besöksstatistik. Google Analytics är en mer eller mindre vedertagen branschstandard för mätning av besökare på webbplatser, och används i mycket stor utsträckning av svenska sajter för att mäta, och även jämföra besöksströmmar med andra sajter inom nätverk som t.ex. SIS-Index.

Att skicka sina besöksdata till Google Analytics innebär självklart också att man låter Google dra egna slutsatser av besöksströmmarna till exempelvis svenska myndigheters webbplatser, och det kan inte uteslutas att Google väljer att göra korsreferenser för att till exempel se vilka av besökarna till en myndighets webbplats som också besöker någon annan myndighets webbplats. Innan man väljer verktyg för besöksstatistik är det viktigt att göra en konsekvensanalys med hänsyn till var och hos vem informationen lagras.

Det överlägset mest populära publiceringssystemet (CMS) som används i undersökningen är det kommersiella systemet EPiServer, utvecklat av ett svenskt företag med samma namn. Det är förvånansvärt få som använder alternativ byggda på öppen källkod, men det är rimligt att anta att den andelen kommer att öka framöver, både på grund av minskade licenskostnader med de fria alternativen och för att mjukvara byggd på öppen källkod kan förväntas bli vanligare bland svenska myndigheter.

En majoritet, 479 (71 procent) av webbplatserna sätter själv en kaka (cookie) vid besöket. Av de 479 vet vi att också att 297 använder Google Analytics, som dessutom kräver att en tredjepartskaka sätts för att räkna besökare.

I påfallande många fall vidarebefordras besökare till en annan adress än den som användaren angett genom s.k. redirects vilket är något som påverkar prestandan för den som besöker den aktuella sidan.

En förändring är att Latin-1 (ISO 8859-1) är på stark tillbakagång till förmån för UTF-8, vilket innebär att alltfler webbplatser hanterar en starkt utökad teckenmängd för innehåll i form av text.

8.4 Stöd för transportskydd (TLS/SSL)

Med hjälp av certifikat och tillhörande krypteringsnycklar kan en webbläsare upprätta en säker, krypterad kommunikation med webbservern. Även här används TLS/SSL för upprättandet av en säker förbindelse mellan en webbläsare och en webbplats (https), se bilaga 9.

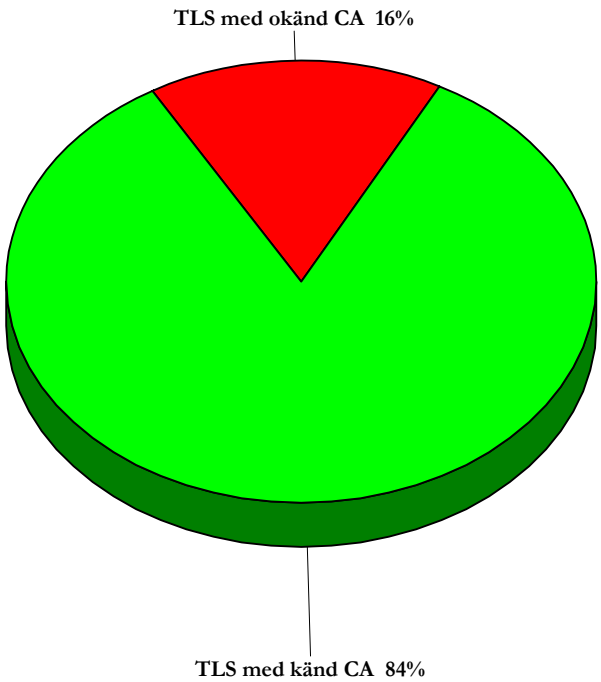
Det räcker alltså inte med att ha ett certifikat utfärdat för domänen eller webbservern, certifikatet måste också kunna betraktas som pålitligt genom att uppfylla några grundläggande krav som ska ställas på den typen av säkerhetsmekanismer, dvs. att certifikatet är giltigt, att det använder sig av säkra algoritmer, tillräckligt långa nycklar et cetera.

Det kan finnas många anledningar till varför man inte kan lita på ett certifikat:

- Om kryptoalgoritmer som används är dåliga.
- Om certifikatet används innan det aktiverats.
- Om certifikatet används efter att giltighetstiden har gått ut.
- Om domänen som certifikatet är utfärdat för inte motsvarar domänen för sajten.
- Om certifikatet har revokerats (återkallats).
- Om certifikatet är självsignerat.
- Om utfärdaren inte är en välkänd CA.
- Om certifikatskedjan inte är komplett.

Vid 2007 års undersökning hade enbart en fjärdedel av de undersökta webbservrarna stöd för TLS/SSL medan motsvarande siffra för 2008 var tre fjärdedelar. Vi kan inte jämföra undersökningarna över åren då vi 2009 ändrade metoden för hur vi kontaktar webb-servrarna. Liksom förra året har vi i år bara testat vad vi får för svar på en HTTP och HTTPS GET till domännamnen i undersökningsgruppen med "www." placerat framför. 227 av 670 domäner eller 34 procent returnerar något vettigt på frågor som rör certifikat.

Av dessa 227 domäner har vi kunnat ladda ner helt korrekta certifikat från 190 utfärdade av någon känd CA, dvs. 84 procent, vilket är en ökning med 6 procent sedan förra året.



Bland de 16 procent som inte har korrekta certifikat har vi hittat följande felaktigheter:

- 12 har certifikat utställda på fel hostnamn.
- 10 har certifikat vars giltighetstid gått ut.
- 9 har självsignerade certifikat.
- 3 har certifikat signerade med en okänd root-CA.
- 2 har certifikat vars kryptografiska checksumma inte stämmer.
- 1 har ett självsignerat certifikat mellan sitt eget certifikat och root-CA-certifikatet.

Det är dessutom möjligt att de domäner som inte har korrekta certifikat har mer än ett problem.

Av de undersökta webbplatserna kan vi alltså konstatera att 10 har certifikat som är ogiltiga på grund av att de inte har förnyats inom giltighetstiden. Skräckexemplet bland dessa är ett certifikat utfärdat för ett svenskt gruvbolag och som gick ut i juli 2004, alltså för sex år och tre månader sedan. En svensk kommun har ett certifikat utfärdat som gick ut i december 2006. Dessa certifikat är fortfarande i bruk eftersom dessa de facto returnerar svar via https.

Några kommuner hade vid undersökningstillfället fyra dagar kvar till deras certifikat skulle gå ut. Alla ligger hos samma operatör, och dessa pekar dessutom på ett certifikat som inte ens är utdelat till dessa kommuner, utan till en helt annan domän. När vi gjorde en ny kontroll efter att giltighetstiden gått ut hade inget av certifikaten förnyats.

Vi kunde bland de 190 domäner som hade godkända certifikat endast hitta 27 adresser med EV-certifikat (Extended validation). Det är en variant av certifikat som medför utökat visuellt stöd i webbläsarna för att visa att certifikatet är godkänt och att utfärdarna har granskats mer noggrant än när det gäller vanliga servercertifikat.

181 sajter accepterar kryptering med svaga algoritmer och 19 sajter använde sig av osäkra signaturalgoritmer.

Ett par certifikat är konfigurerade med relativt korta RSA-nycklar, 512 bitar, medan de vanligaste nyckellängderna idag är 1024 respektive 2048 bitar.

Ett 20-tal sajter använder sig av så kallade wild card-certifikat. Ett wild card SSL-certifikat aktiverar SSL-kryptering på flera subdomäner med hjälp av ett och samma certifikat, förutsatt att domänerna kontrolleras av samma organisation och har samma huvuddomän. Vissa av de wild card-certifikat vi har tittat på är utfärdade för något webbhotell som i sin tur använder det för att utfärda certifikat för sina kunder. Det är långt ifrån riskfritt att dela certifikat mellan domäner bland annat därför att:

- Om säkerheten hos en server eller subdomän har komprometterats finns det risk för att alla subdomäner också har komprometterats.
- Om wild card-certifikatet måste bytas ut behöver också alla subdomäner ha ett nytt certifikat.

Den bästa lösningen på det problemet är att helt enkelt använda ett unikt certifikat för varje server i stället för att använda wild card-certifikat.

Hanteringen av certifikat i undersökningsgruppens webbmiljö håller alltså fortfarande mycket dålig kvalitet i alla avseenden som undersökningen visar. Denna typ av krypto-användning har funnits länge och är tämligen vanlig. Hos de organisationer som ingår i undersökningen hade vi förväntat oss bättre resultat, framför allt att de skulle ha giltiga, aktuella certifikat utgivna av trovärdiga utgivare. Vad vi vill få sagt med denna del av undersökningen är att en bristfällig användning av webbcertifikat undergräver trovärdigheten av denna typ av säkerhetslösningar.

Allt som innebär att en användare måste klicka på knappar som i praktiken innebär ”Ja, jag vet att det inte stämmer, men ta mig vidare ändå”, såsom självsignerade certifikat eller certifikat vars giltighetstid har gått ut gör att det inarbetas dålig säkerhetskultur hos Internet-användare vilket motverkar själva grundidén med servercertifikat – nämligen att helt säkert veta att man står i förbindelse med rätt server (se bilaga 9).

Alla som via sin webbplats begär någon form av information från användare, såsom inloggning, personuppgifter, användaruppgifter, betalinformation, kreditkortsnummer, telefonnummer m.m. bör använda sig av TLS/SSL med certifikat utfärdade av allmänt accepterade certifikatutfärdare som finns installerade i de vanligaste webbläsarna. Det behöver också finnas någon som internt i verksamheten ansvarar för bl.a. bevakning av när certifikat går ut och ska förnyas. Därutöver kan man tänka på att:

- Använda så långa RSA-nycklar som möjligt.
- Nyttja EV-certifikat där det är befogat.
- Undvika wild card-certifikat för webbtjänster, speciellt där driften är utlagd på webbhotell eller molntjänster där det inte finns någon egen kontroll över vare sig nyckelmaterial och certifikat.
- Använda hårdvarustöd för att spara privata nycklar för känsliga webbservrar.

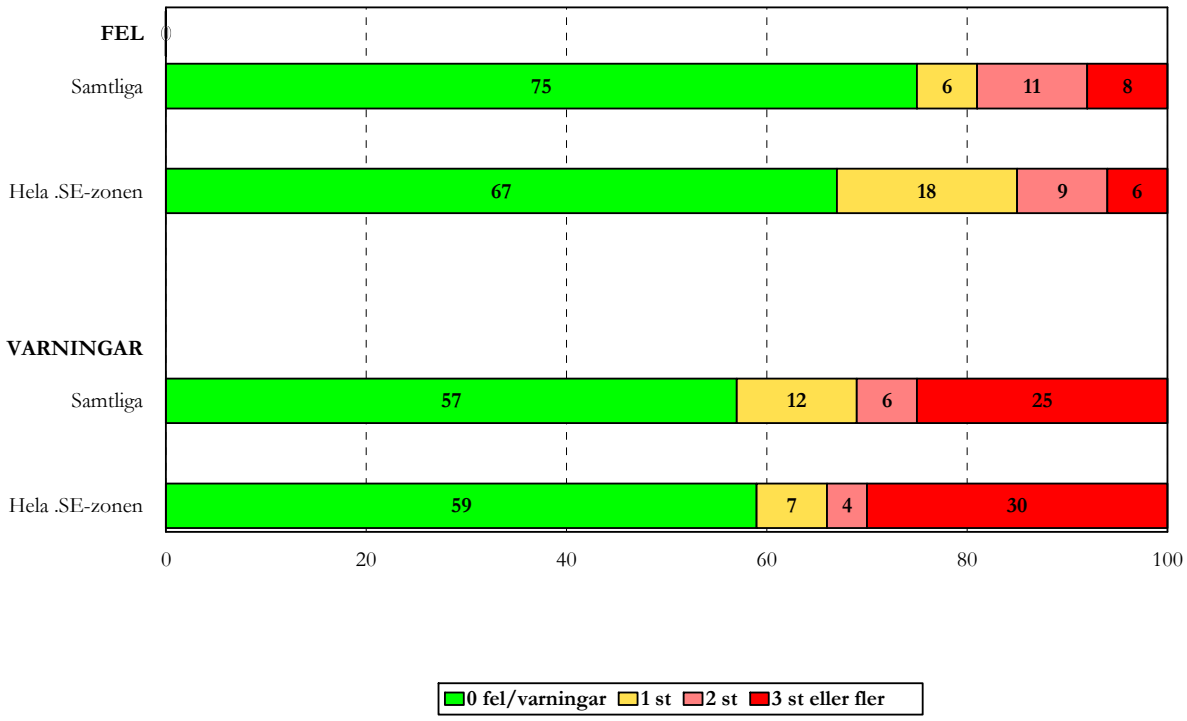
På http://www.ssllabs.com kan den som använder certifikat för att skydda webbtjänster själv testa om sajten har bra säkerhet med avseende på SSL.

9 Jämförelse med .se-zonen som helhet

För att se om vår undersökningsgrupp är bättre eller sämre än .se-zonen som helhet har vi även i årets undersökning gjort ett utsnitt av att antal slumpmässigt valda domäner ur .se-zonen för att ha som jämförelse. I tabellerna nedan representerar ”Samtliga” den aktuella undersökningsgruppen medan ”Hela .se-zonen” representerar det slumpmässiga urvalet på 10 000 domäner ur en version av zonfilen från den 7 oktober 2010.

Först och främst har vi tittat på fördelningen av fel och varningar, och hur undersökningsgruppen - som ändå innehåller en hel del kritiska funktioner och verksamheter - förhåller sig till .se-zonen som helhet.

Tabell 17: Andel fel och varningar

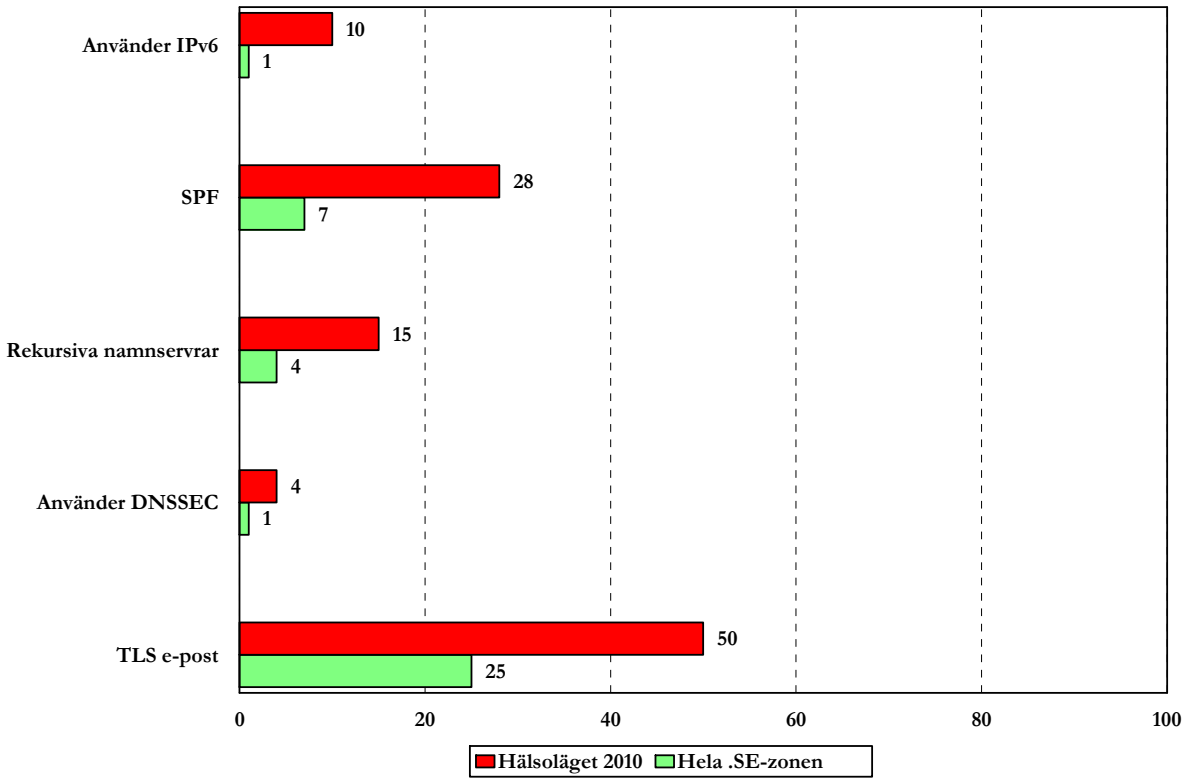


I år är det fler fel i vår undersökningsgrupp än i .se-zonen som helhet, alltså tvärtom mot förra året. Andelen varningar är ungefär lika.

De stora skillnaderna ser vi först när vi tittar på de andra specifika områden vi har granskat närmare förutom de parametrar som vi förknippar med DNS-kvalitet enligt definitionen i bilaga 4. I undersökningsgruppen är det fler som använder SPF, det är fler som har öppna rekursiva namnservrar, fler som använder DNSSEC och fler som skyddar sin e-post med TLS. Vilka slutsatser vi kan dra av det är inte alldeles uppenbart. För det behöver vi göra fler och mer specifika undersökningar.

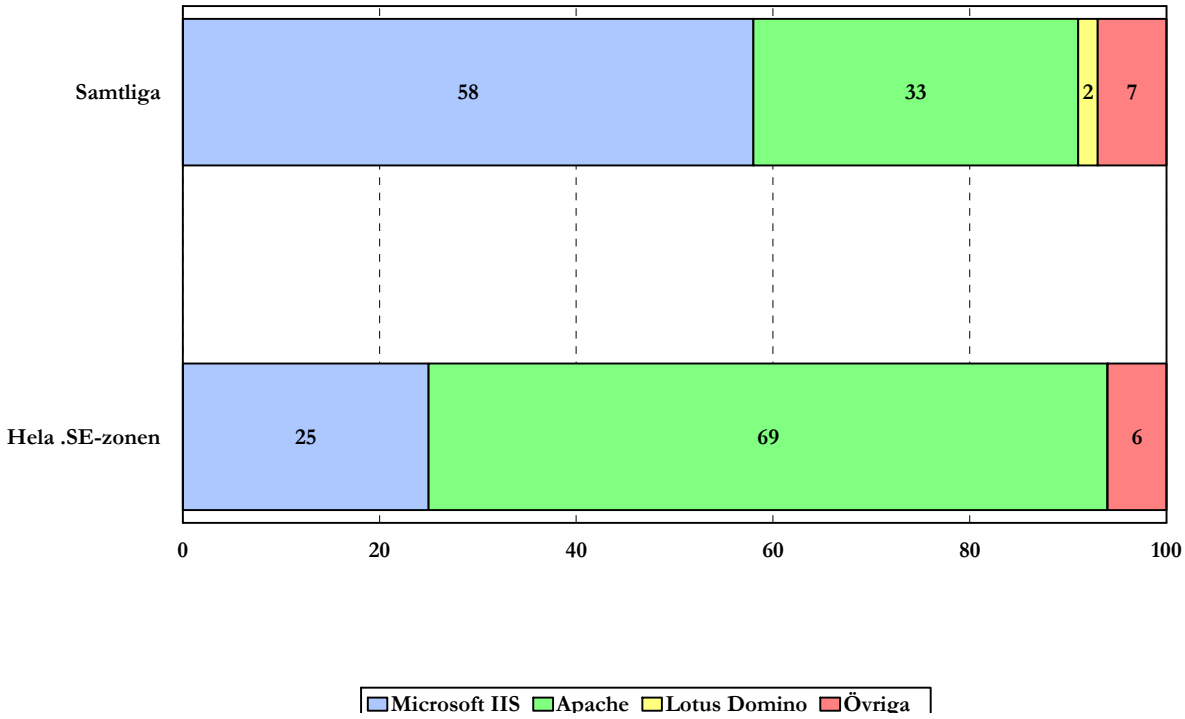
Några detaljer vi kan notera är emellertid att det är långt många fler i undersöknings-gruppen som använder IPv6 än i .se-zonen som helhet. En del av förklaringen till det är förmodligen det vi ser i tabell 8, att universitet och högskolorna har kommit längre än andra i införandet av IPv6.

Tabell 18: Använder IPv6



På samma sätt kan man förmodligen förklara den stora skillnaden mellan vilka programvaror som används för webbservrar mellan undersökningsgruppen där Microsoft IIS dominerar och .se-zonen som helhet som faktiskt mer liknar världen i övrigt, där Apache är den dominerande programvaran. Systemet med offentlig upphanding och ramavtal bidrar till en homogenisering av den offentliga förvaltningens IT-miljöer som kanske inte alltid är optimal.

Tabell 19: Programvaror för webbservrar



10 Råd och rekommendationer

Efter att ha genomfört en ny omgång tester med ett relativt likartat (och ganska dåligt) resultat jämfört med 2009 ser vi i ännu högre grad ett mycket starkt behov av större samordning mellan olika intressenter för bättre säkerhet på den svenska delen av Internet och inte minst möjligheter till mycket stora effektivitetsvinster och kostnadsbesparingar.

I första hand verksamheterna inom den offentliga förvaltningen måste kunna enas om rekommendationer och en handlingsplan för genomförandet av några viktiga aktiviteter:

- Kritiska resurser i Sverige bör ha namnservrar som är anslutna till flera operatörer samtidigt, till exempel med användning av tekniken Anycast. Det finns behov av att någon på central nivå bestämmer vad som är att betrakta som en kritisk resurs.

- Sätt upp en gemensam sekundär DNS-drift för kritiska tjänster exempelvis via de svenska Internetknutpunkterna dit dessa kan anslutas som en extra åtgärd för att skapa redundans. En sådan funktion kan regleras genom avtal.

- Upprätta en för offentlig förvaltning gemensam funktion för virustvätt och rensning av skräppost med krav på servrar placerade i landet. Det skulle bli effektivare, förmodligen spara resurser och göra det enklare att göra revision. Samtidigt skulle det förhindra att myndighetsinformation lämnar landet.

- Utfärda riktlinjer om vad som är acceptabelt när det gäller skräpposthantering och virustvätt i offentlig förvaltning. Det borde inte vara accepterat att svenska myndigheter och kommuner skickar sin e-post utomlands, åtminstone inte utan att relevanta och enhetliga krav på transportskydd och kryptering ställs.

- Utfärda rekommendation om att e-postservrar för kritiska verksamheter hos svenska myndigheter och statliga verk fysiskt ska ligga i Sverige för att skydda spårbarheten av information mellan myndigheter och för att skydda mot de konsekvenser som följer av den s.k. FRA-lagen.

- Ställ krav på offentlig förvaltning om användning av både e-post och webb med TLS för käll- och transportskydd.

- Göra samtliga tjänster tillgängliga över IPv6 och planera omgående för en systematisk övergång till IPv6 inom hela den offentliga förvaltningen. Själva processen i sig är en operation på 12-18 månader.

- Skydda webbservrar med certifikat som är utfärdade av allmänt accepterade certifikatutfärdare och ha kontroll över deras giltighet.

- Inför DNSSEC på domäner i den offentliga förvaltningen.

För offentlig förvaltning bör flera av dessa åtgärder kunna hanteras inom ramen för e-delegationens uppdrag. Utöver ovanstående åtgärder finns det ytterligare åtgärder som behöver vidtas bl.a. på operatörsnivå för att stärka infrastrukturen för Internet. Dessa åtgärder landar huvudsakligen på Kommunikationsmyndigheten PTS, såsom tillsynsansvarig myndighet, och handlar om att ställa krav på operatörer.

Bilaga 1 - Förkortningar och ordförklaringar

ADSP Author Domain Signing Practices används för att upptäcka otillåten borttagning av signaturen i DKIM.

Barnzon Den underliggande *zonen*, till exempel är .example.se barnzon till föräldrazonen .se.

BCP Best Common Practice, branschstandard.

DKIM Domain Keys Identified Mail. DKIM gör det möjligt för e-postservrar att skicka och ta emot elektroniskt signerad e-post.

DNS Domain Name System. En internationell hierarkiskt uppbyggd distribuerad databas som används för att hitta information om tilldelade *domännamn* på Internet. Domännamnssystemet är det system som översätter domännamn (t.ex. iis.se) till IP-adress vilken används för kommunikation över IP-nät som t.ex. Internet.

DNS-data Information som lagras hos ett *Registry* där det anges vilka *namnservrar* som ska svara på förfrågningar om en viss *domän*.

DNSSEC Secure DNS. DNSSEC en internationellt standardiserad utökning av DNS som tillför säkrare namnuppslagningar, minskad risk för manipulation av information och förfalskade domännamn. Den grundläggande mekanismen i DNSSEC är kryptografisk teknik som använder digitala signaturer.

DNS-server Se *Namnserver*.

Domän Beteckning på en nivå i domännamnssystemet.

Domännamn Ett unikt namn, sammansatt av namndelar, där en i domännamns-systemet lägre placerad domän står före en högre placerad domän. Ett registrerat *domännamn* är ett *domännamn* som har tilldelats en viss *innehavare*.

Föräldrazon Den överliggande *zonen*, till exempel är .se föräldrazon till example.se. Se även *Barnzon*.

IP-adress Numerisk adress som tilldelas varje dator som ska vara nåbar via Internet.

Namnserver Dator med program som lagrar och/eller distribuerar *zoner*, samt tar emot och svarar på domännamnsfrågor.

Namnserveroperatör Den som tillhandahåller en *DNS-funktion* för Internetanvändare.

Resolver Den programvara som översätter namn till *IP-adress* eller tvärtom.

SOA Start of Authority, en pekare till var information om en zon börjar.

TLS/SSL SSL är en standard för kryptering av bland annat webbtrafik under transport. Kommunikation med http med SSL kallas https. Ersätts numera av IETF:s öppna standard TLS.

zon Avgränsning av det administrativa ansvaret för domännamnsträdet. En *zon* utgörs av en sammanhängande del av domännamnsträdet som administreras av en organisation och lagras på dess *namnservrar*.

zonfil Datafil där den information finns lagrad som behövs om en *zon* för att adressering med *DNS* ska kunna användas.

Bilaga 2 - Om DNS och om undersökningen

.SE (Stiftelsen för Internetinfrastruktur) har enligt sin urkund ”till ändamål att främja en god stabilitet i infrastrukturen för Internet i Sverige samt främja forskning, utbildning och undervisning inom data- och telekommunikation, särskilt med inriktning på Internet. Stiftelsen skall härvid prioritera områden som ökar effektiviteten i infrastrukturen för elektronisk datakommunikation, varvid stiftelsen bland annat skall sprida information om forsknings- och utvecklingsarbete, initiera och genomföra forsknings- och utvecklingsprojekt samt genomföra kvalificerade utredningar”. Säker Internetinfrastruktur är ett mycket viktigt och centralt område för oss.

Det stora intresse som har visats för resultaten från tidigare års undersökningar övertygar oss på .SE att det finns ett värde av undersökningen och vi kommer att fortsätta genomföra den, i år görs det för fjärde gången. Undersökningen ingår i ett långsiktigt projekt som går under namnet Hälsoläget.

.SE, har sedan 1997 ansvaret för teknisk drift och administration av alla namnservrar för .se-domänen och har genom åren skaffat sig gedigen erfarenhet av domännamnssystemet (DNS). På basis av våra egna och andras misstag och erfarenheter har det i branschen successivt vuxit fram en internationell Best Common Practice för DNS som kan tillämpas även i andra miljöer än på toppdomännivån. DNS är lite av en doldis med mer än 25 år på nacken. DNS har genom åren visat prov på enastående skalbarhet och robust design. Ingenting har i princip behövt ändras i de grundläggande protokollen trots den enorma tillväxt som skett på Internet. DNS har emellertid kommit att bli allt viktigare för en fungerande kommunikation mellan Internetanvändare världen över, och det ställer krav på att DNS-systemet håller hög kvalitet i alla delar.

DNSSEC

När DNS skapades på 1980-talet var huvudtanken att minimera den centrala administrationen av nätverket och göra det lätt att koppla upp nya datorer till Internet. Däremot fäste man inte någon större vikt vid säkerheten. Bristerna på detta område har öppnat för olika typer av missbruk och attacker där svaren på DNS-uppslagningar förfalskas. På så vis kan Internetanvändare ledas fel, exempelvis i syfte att lura av folk känslig information som lösenord och kreditkortsnummer.

Därför har man utvecklat säkerhetstillägg till DNS som fått beteckningen DNSSEC (DNS Security Extensions). Med DNSSEC säkras domännamnssystemet från missbruk genom att svaren på DNS-uppslagningar signeras kryptografiskt. Genom validering av signaturer går det att säkerställa att svaren verkligen kommer från rätt källa och inte har ändrats under överföringen.

.SE:s lansering 2005 av tjänsten DNSSEC för säkrare DNS har också bidragit till att ett ökat fokus hamnat på DNS och DNS-drift. Den som har för avsikt att göra sin DNS-infrastruktur säkrare genom att använda DNSSEC inser tämligen snabbt att införandet inte låter sig göras med mindre än att det först görs en översyn av den egna DNS-infrastrukturen som helhet.

Därför är vi givetvis intresserade av att ta reda på hur väl förberedda domäner i .se är för DNSSEC. Det - och det faktum att vi ansvarar för den svenska toppdomänen - är skälen till varför vi fokuserar våra tester på just kvalitet i DNS.

IPv6

För att datorer och annan utrustning ska kunna kommunicera med varandra över Internet måste de använda en gemensam kommunikationsarkitektur. Det innebär att de måste använda samma uppsättning regler för kommunikationen, eller samma protokoll. Den gemensamma kommunikationsarkitekturen samlas kring Internet Protocol som förkortas IP. Dagens Internet domineras av IPv4 (IP version 4), som togs fram redan 1981.

De så kallade IP-adresserna, det vill säga den unika nummerserie som identifierar varje ansluten enhet på Internet, består av 32 bitar. Därför finns det med IPv4 bara drygt fyra miljarder unika IP-adresser. I takt med att världen blir alltmer uppkopplad kommer vi varje dag allt närmare en adressbrist på Internet.

Lösningen för att komma tillrätta med adressbristen är att införa en ny version av IP-protokollet, IPv6, som arbetar med 128 bitar långa adresser. Med IPv6 kommer adresserna att räcka för en mycket lång tid. En riklig tillgång till IP-adresser öppnar också upp för applikationer som annars blir svåra att förverkliga i praktiken, som t.ex. intelligenta hem där all teknisk utrustning är uppkopplad med en egen IP-adress. Vi har därför tittat närmare på den aktuella utbredningen av IPv6.

Tjänster för e-post och webb

På .SE är vi också intresserade av att titta närmare på hur verksamheter hanterar sin kommunikation i övrigt, främst när det gäller säkerhet, tillgänglighet och robusthet för de vanligaste tjänsterna elektronisk post och webbtrafik. Vi arbetar kontinuerligt med vidareutveckling av mätverktyget för att kunna se mer detaljer, inte minst kring parametrar som rör webbapplikationer, men också mer detaljer kring användning av e-post. Verktyget MailCheck är det senaste tillskottet som är under utveckling och där det finns en betaversion som kan användas. Mailcheck syftar till att förbättra kvaliteten på e-postrelaterade tjänster generellt genom att peka ut möjliga konfigurationsproblem, svagheter i programvaror eller brott mot standarder för både systemadministratörer och slutanvändare.

Bilaga 3 - Om testverktyget DNSCheck

Som motor för genomförandet av undersökningen har vi använt programvaran för .SE:s tjänst DNSCheck. DNSCheck är ett program designat för att hjälpa människor att kontrollera, mäta och förhoppningsvis också bättre förstå hur domännamnssystemet fungerar. När en domän (även kallad zon) skickas till DNSCheck undersöker programmet domänens hälsotillstånd genom att gå igenom DNS från roten (.) via TLD:n (toppdomänen, till exempel .se) vidare till de namnservrar som innehåller information om den aktuella domänen (till exempel iis.se). DNSCheck utför även en hel del andra tester, som att kontrollera DNSSEC-signaturer, att de olika värddatorerna går att komma åt och att IP-adresserna är giltiga.

Verktyget finns tillgängligt för användning på http://dnscheck.iis.se. Källkoden till bl.a. detta verktyg finns att hämta på http://github.com/dotse/.

Bilaga 4 - Branschstandard för DNS-tjänst med kvalitet

För den mer tekniskt bevandrade läsaren har vi i denna bilaga redovisat mer i detalj vad branschstandarden för DNS-tjänst med kvalitet innefattar i termer av rekommendationer. Den som själv vill testa sin domän gör det enkelt på .SE:s webbplats.

.SE har vidareutvecklat verktyget DNSCheck så att det även kan utföra så kallade odelegerade domäntester. Ett odelegerat domäntest är ett test som genomförs på en domän som kan (men inte måste) vara fullständigt publicerad i DNS. Funktionen är mycket användbar t.ex. om domäninnehavaren tänker flytta en domän från en namnsserveroperatör till en annan. Låt oss ta som exempel att domänen exempel.se ska flyttas från namnservern 'ns.nic.se' till namnservern 'ns.iis.se'. I detta fall kan man genomföra ett odelegerat domäntest på domänen (exempel.se) med den namnservern domänen ska flyttas till (ns.iis.se) INNAN själva flytten genomförs. När testet visar grönt är det tämligen säkert att den nya hemvisten för domänen åtminstone vet att den ska svara på frågor om domänen. Det kan emellertid fortfarande finnas fel i zoninformationen som detta test inte känner till.

Funktionen finns tillgänglig på både svenska och engelska och hittas på:

http://dnscheck.iis.se/

1. Minst två namnservrar

Rekommendation: DNS-data för en zon bör ligga på minst två separata namnservrar. Dessa namnservrar bör av tillgänglighetsskäl vara logiskt och fysiskt separerade så att de är placerade på olika operatörsnät i olika autonoma system (AS).

Förklaring: För varje underliggande domän ska det finnas minst två fungerande namnservrar. De ska vara listade som NS-poster för domänen i fråga. De bör vara fysiskt separerade och placerade på olika nätsegment för att högsta funktionalitet ska erhållas. Det säkerställer att domänerna fortsätter att fungera även om en av de aktuella namnservrarna skulle sluta fungera.

Konsekvens: När den enda servern eller den enda operatören får ett avbrott blir DNS-tjänsten onåbar för den domän som ligger på servern eller i operatörens nät. Därmed kan man inte heller nå tjänster under domänen, även om dessa har placerats hos andra aktörer än den egna namnserveroperatören.

2. Alla namnservrar som utpekas i delegeringen ska existera i underliggande zon

Rekommendation: De NS-poster som listas i den överliggande zonen (.se eller motsvarande) för att peka ut (delegera) en viss domän ska samtliga finnas införda i den underliggande zonen.

Förklaring: I den överliggande zonen används NS-poster för att överlåta ansvaret för (delegera) en viss domän till andra servrar. Denna lista av datorer ska enligt DNS-dokumentationen finnas införd även i den zonfil som "tar emot" ansvaret, och som innehåller övriga data om zonen. Listorna måste hållas synkroniserade, så att alla NS-poster som förekommer i föräldrazonen också återfinns i barnzonen. Listan i föräldrazonen uppdateras inte automatiskt, utan endast efter "manuell" anmälan till ansvarig registreringsenhet. Vid förändring som leder till behov av ändring i överliggande zon ska underliggande zons administrativa kontaktperson utan dröjsmål se till att registreringsenheten meddelas om detta.

Konsekvens: Om föräldrazonen innehåller information om barnzonen som de facto inte existerar i barnzonen innebär det att den som ställer frågor om domänen inte kan få svar, med påföljd att tillgängligheten påverkas.

3. Auktoritet

Rekommendation: Samtliga namnservrar som listats med NS-poster i en delegerad zon ska svara auktoritativt för domänen.

Förklaring: Vid kontroll mot servrarna för underdomänen ska man kunna få konsekventa och repeterbara auktoritativa svar för SOA- och NS-poster för underdomänen. Detta gäller samtliga servrar som finns listade i den underliggande zonens DNS för domänen i fråga.

Konsekvens: DNS fungerar oftast även om detta fel existerar. Men att felet existerar i en zon tyder på bristande rutiner hos den som ansvarar för innehållet i DNS för den domänen.

4. Serienummer för zonfil

Rekommendation: Samtliga namnservrar som listats med NS-poster i den delegerade zonen ska svara med samma serienummer i SOA-posten för domänen.

Förklaring: Serienumret i SOA-posten är en sorts versionsnummer för zonen, och om servrarna har samma serienummer på sina zoner visar detta att de är synkroniserade. Det kontrolleras genom att fråga respektive server om SOA-posten och jämföra serienumren i svaren. SOA står för Start of Authority.

Konsekvens: Om namnservrarna inte är synkroniserade och inte har samma version av zonfilen riskerar den som ställer frågor om en domän att inte få något svar. Tillgängligheten påverkas.

5. Kontaktadress

Rekommendation: Zonkontaktadressen i SOA-posten ska vara nåbar.

Förklaring: I SOA-posten för en domän ingår som andra delpost en e-postadress som ska fungera som kontaktpunkt om någon behöver nå administratören för domänen i fråga. Vid en enkel kontroll ska e-postservern för e-postadressen inte ge uppenbara felmeddelanden (t.ex. ”user unknown”). Vid fördjupad kontroll ska provbrev kunna sändas till adressen och dessa ska besvaras inom tre dygn.

Konsekvens: Syftet med att ha en aktuell e-postadress för kontakter är att snabbt kunna påtala problem med nåbarheten av en domän. Om sådan inte finns kan möjligheten att lösa problem som uppstår i DNS på grund av någon enskild domän komma att minska.

6. Nåbarhet

Rekommendation: Alla NS-poster i den underliggande zonen ska vara nåbara för DNS-trafik från Internet.

Förklaring: NS-posterna för en domän är listan över de datorer som fungerar som namnserver för den domänen. Samtliga uppräknade servrar ska vara nåbara från Internet på alla de adresser som finns listade i motsvarande adressposter i DNS för datorerna i fråga.

Konsekvens: Om en namnserver inte är nåbar trots att den står i listan över namnservrar som svarar på frågor om en domän så innebär det att frågeställaren inte får svar. Tillgängligheten påverkas.

Bilaga 5 – Mer information om DNSSEC

DNSSEC står för DNS Security Extensions och är en utökning av DNS i syfte att göra säkrare uppslagningar av Internetadresser för exempelvis webb och e-post. Den ökade betydelsen av DNS har gjort att DNSSEC blivit allt mer aktuellt. Många Internetprotokoll är beroende av DNS, men DNS-information i resolvrarna har kommit att bli så sårbar för attacker att den inte går att lita på längre. Den ökade säkerhet som DNSSEC tillför gör att många attacker inte längre får någon effekt.

På senare år har alla nya hot mot DNS gjort att DNSSEC blivit allt mer aktuellt. Några av de mest kända och största hoten mot DNS är cache poisoning och pharming. Pharming innebär att någon får själva innehållet i DNS att peka på felaktiga servrar. Rent konkret innebär det att en webbadress för exempelvis en bank kan pekas om till en helt annan server, men för besökaren ser det fortfarande i adressfältet ut som att det är rätt server han besöker.

Cache poisoning innebär att en situation skapas, antingen genom en attack eller oavsiktligt, som förser en namnserver med DNS-data som inte kommer från en auktoritativ källa. Ett av de allra färskaste exemplen på detta är den under 2008 så uppmärksammade Kaminsky-buggen.

Det råder alltså ingen tvekan om att DNS behöver bli säkrare. DNSSEC är en långsiktig lösning som skyddar mot flera olika typer av manipulering av DNS-frågor och -svar under kommunikationen mellan olika servrar i domännamnssystemet.

.SE har med åren fått stort internationellt genomslag för sitt arbete med säkrare DNS-uppslagningar. Redan hösten 2005 signerade .SE som första landstoppdomän i världen sin zon med DNSSEC och vi var även först med att 2007 erbjuda en kommersiell DNSSEC-tjänst till våra domäninnehavare. Vi har för närvarande ett tjugotal återförsäljare (registrarer) som erbjuder DNSSEC.

Till skillnad från hur det traditionella domännamnssystemet fungerar är uppslagningar med DNSSEC kryptografiskt signerade, vilket gör det möjligt att säkerställa både att de kommer från rätt avsändare och att innehållet inte har ändrats under överföringen. Syftet med funktionen är att domännamnsinnehavaren ska kunna skydda sina domäner med DNSSEC.

DNSSEC används för att säkra DNS från missbruk och man-in-the-middle-attacker som cacheförgiftning. .SE har under flera år varit en pådrivande kraft för att införa och sprida DNSSEC.

VAD DNSSEC SKYDDAR MOT

DNSSEC säkerställer innehållet i DNS med kryptografiska metoder som använder elektroniska signaturer. DNSSEC innebär att användaren genom validering av signaturer ska kunna avgöra när han gör en uppslagning i DNS, om informationen som kommer tillbaka som svar kommer från rätt källa, och om den har manipulerats på vägen. Det blir alltså svårt att förfalska information i DNS som är signerad med DNSSEC utan att det upptäcks.

För gemene man innebär DNSSEC en minskad risk för att bli utsatt för bedrägerier vid till exempel bankaffärer eller shopping på nätet, eftersom det blir lättare för användaren att fastställa att man verkligen kommunicerar med rätt bank eller butik snarare än med en bedragare.

Det är dock viktigt att notera att DNSSEC inte stoppar alla typer av bedrägerier. Funktionen är endast konstruerad för att förhindra attacker där angriparen manipulerar svar på DNS-frågor för att uppnå sitt mål.

VAD DNSSEC INTE SKYDDAR MOT

Fortfarande finns det flera andra säkerhetsbrister och problem på Internet som DNSSEC inte löser, till exempel överbelastningsattacker, så kallad Distributed denial of service (DDOS).

När det gäller såväl phishing (sidor som liknar eller är identiska med originalet för att lura till sig lösenord och personuppgifter) som pharming (omdirigering av DNS-förfrågan till fel dator) och andra liknande attacker mot DNS, så ger DNSSEC ett visst skydd mot detta. DNSSEC skyddar inte mot attacker på andra nivåer, som attacker på IP- eller nätnivå.

.SE:S ROLL I DNSSEC

Många har väntat på att rotzonen, dvs. föräldrazonen till .se, ska bli signerad och 2010 blev detta verklighet. Hittills är det .SE som haft ansvaret för att dels signera .SE:s zonfil, dels utgöra ett *trust anchor* i kedjan för den svenska delen av Internet. Ett *trust anchor* signerar de underliggande zonernas nycklar och fungerar som startpunkt i verifieringskedjan. Signeringen består av att .SE tar hand om och verifierar de underliggande zonernas DS-poster. Det är jämförbart med hanteringen av NS-poster i DNS.

.SE kommer fortfarande att signera .SE:s zonfil, men numera är det rot som utgör *trust anchor* för Internet. Detta underlättar för alla resolveroperatörer som annars blir tvungna att hålla reda på alla nycklar för alla signerade toppdomäner som är *trust anchor* för underliggande domäner. Med roten signerad behöver de bara hålla reda på rotnyckeln. Moderna standarder erbjuder dessutom enklare hantering av nyckelbyten och nya verktyg har tagits fram för att underlätta (se nedan om Open DNSSEC).

Läs mer om .SE:s DNSSEC-tjänst på http://www.iis.se/domaner/dnssec/.

. .SE tillhandahåller mer information om sårbarheter i DNS via en särskild webbplats som finns på http://www.kaminskybuggen.se.

Där finns det bland annat möjlighet att testa om den resolver som används är sårbar för Kaminskybuggen, och om DNSSEC används för en domän.

Här finns några pekare till ytterligare information:

Information om DNSSEC och utvecklingen av både användning och verktyg.
http://dnssec.net

En praktiskt inriktad guide till hur man gör för att införa DNSSEC.
http://www.nlnetlabs.nl/publications/dnssec_howto/index.html

Nyheter om DNSSEC sprids regelbundet av **DNSSEC Deployment Initiative** http://www.dnssec-deployment.org/

De har också en e-postlista som vem som helst kan prenumerera på och hålla sig uppdaterad om utvecklingen på området.

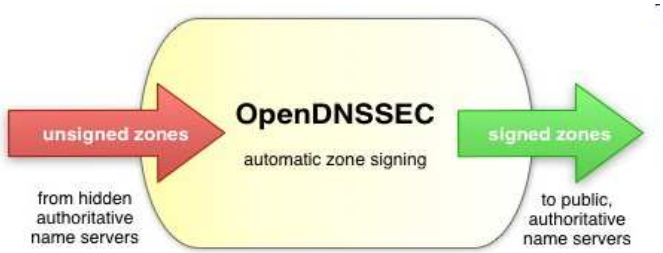
Utvecklingsprojekt – OpenDNSSEC

DNS är relativt komplicerat, och så även elektroniska signaturer, kombinationen av dessa båda i DNSSEC är givetvis också den komplicerad.

Efter att .SE noterat att bristen på bra och tillgängliga verktyg på marknaden för signering av zonfiler med DNSSEC var ett hinder för många att inleda införandet av DNSSEC påbörjades ett utvecklingsprojekt tillsammans med några av de främsta utvecklarna på området. Resultatet är OpenDNSSEC som är en nyckelfärdig programvara, eller ett verktyg för att underlätta införandet och användningen av DNSSEC. OpenDNSSEC säkrar DNS-informationen momentet innan den ska publiceras på en auktoritativ namnserver. OpenDNSSEC tar en osignerad zonfil, lägger till signaturer och andra poster för DNSSEC och skickar filen vidare till de auktoritativa namnservrarna för den aktuella zonen.

Syftet med OpenDNSSEC är att hantera dessa svårigheter och att lyfta dem från systemoperatörens axlar efter att denne väl har satt upp systemet.

Genom att delta i utvecklingen av ett nyckelfärdigt system för signering av zonfiler med DNSSEC vill .SE underlätta spridningen av DNSSEC.



OpenDNSSEC utvecklas inom ramen för ett samarbete mellan .SE, Nominet, NLNet Labs, SIDN, SURFnet, Kirei och John Dickinson. Mer information finns på http://www.opendnssec.org/

Programvaran som är öppen går också att ladda ner och testa från den webbplatsen.

Bilaga 6 - Öppna rekursiva namnservrar

En **rekursiv namnserver** svarar inte bara på frågor om DNS-poster som den själv är ansvarig för, utan går även vidare och frågar andra namnservrar för att ta reda på svaret. Frågandet kan vara både arbetskrävande (det vill säga ta datorkapacitet) och resultera i relativt stora mängder data, vilket gör att man normalt sett vill begränsa vem som får använda funktionen rekursion.

En **öppen rekursiv namnserver** svarar på alla frågor den får där rekursion har begärts. Detta gör det möjligt för utomstående att till exempel utföra tillgänglighetsattacker via den öppna namnservern genom att låta den ställa frågor som kommer att resultera i ovanligt stora svar (Amplification Attack). Detta i kombination med en falsk avsändaradress som leder till att svaret skickas någon annanstans kan utgöra en tillgänglighetsattack.

Grundproblemet är egentligen inte öppna rekursiva namnservrar, utan att operatörerna inte filtrerar trafik på avsändaradresser. Om de gjorde det så skulle öppna rekursiva resolvrar kanske inte betraktas som något problem. Eftersom sådan filtrering är relativt svår och kostsam att införa, så behöver vi under tiden försöka minska de skador som DDOS-attacker orsakar tills dess att operatörerna har klarat av att åtgärda grundproblemet. Att stänga en rekursiv resolver anser vi vara en enkel uppgift för många som det är värt att göra då det hjälper till att lindra de problem som uppstår vid DDOS-attacker.

Pekare till mer information

Nedan har vi samlat några länkar till bra och informativt material om DDOS och öppna rekursiva namnservrar.

Secure Domain Name System (DNS) Deployment Guide
http://csrc.nist.gov/publications/drafts/800-81-rev1/nist_draft_sp800-81r1-round2.pdf

DNS Amplification attacks
En bra beskrivning av hur attacken går till och vad den innebär. http://www.isotf.org/news/DNS-Amplification-Attacks.pdf

Officiellt råd från USA:s CERT
The Continuing Denial of Service Threat Posed by DNS Recursion
http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf.

ISC BIND. Här finns källkod och binärer för BIND samt länkar till mycket intressant och matnyttig information.
https://www.isc.org/downloads/all/

BIND 9 Administrator Reference Manual.
Innehåller exempel på konfigurering, praktiska tips och detaljerad beskrivning av funktioner i BIND.
http://oldwww.isc.org/index.pl?/sw/bind/arm95/index.php

Bilaga 7 - IPv6

Dagens Internet domineras av IPv4 (IP version 4), som togs fram redan 1981.

De så kallade IP-adresserna, det vill säga den unika nummerserie som identifierar varje uppkopplad enhet på Internet, består av 32 bitar. Därför kan det med IPv4 bara finnas drygt fyra miljarder unika IP-adresser. I takt med att världen blir alltmer uppkopplad uppstår det helt enkelt adressbrist på Internet.

Lösningen för att komma till rätta med adressbristen är att införa en ny version av protokollet, IPv6, med 128 bitar långa adresser. Det råder ingen som helst tvekan om att dessa IP-adresser kommer att räcka och bli över under lång tid framöver när övergången till IPv6 väl har genomförts. Med IPv6 blir IP-adresserna nämligen 128 bitar långa i stället för 32, vilket medför att det totala antalet möjliga adresser blir i det närmaste obegränsat.

Från att det med IPv4 inte ens finns en IP-adress per person i världen, skulle varje nu levande individ kunna få 5×10^{28} adresser var med IPv6. Var och en skulle alltså kunna få 50 000 000 000 000 000 000 000 000 egna IP-adresser att förfoga över. En riklig tillgång till IP-adresser öppnar också upp för applikationer som annars blir svåra att förverkliga i praktiken som t.ex. Sakernas Internet och intelligenta hem.

Bilaga 8 - Åtgärder mot skräppost

SPF

Sender Policy Framework (SPF) är en metod för att motverka att meddelanden via elektronisk post skickas med falskt domännamn i avsändaradressen, dvs. att avsändaren använder någon annan adress än sin egen som avsändaradress. Läs mer om SPF på http://www.openspf.org.

SPF ger domäninnehavaren möjlighet att i DNS publicera regler som anger från vilka datoradresser e-post från domänen ska komma. När en mottagande e-postserver får ett meddelande kontrollerar den mot SPF-informationen i DNS hur dessa regler ser ut. Om meddelandet kommer från en sändande server som inte är publicerad i reglerna tolkas det av den mottagande servern som en indikation på att allt inte står rätt till.

Den mottagande servern kan med den informationen som grund avgöra meddelandets vidare öde, till exempel vägra att ta emot meddelandet eller att sortera det som skräppost. SPF-standarden definierar inte vad som ska hända med meddelanden som inte passerar en SPF-validering.

DKIM

En annan teknik för att motverka att meddelanden via elektronisk post skickas med falskt domännamn i avsändaradressen, dvs. att användaren använder en annan adress än sin egen som avsändaradress, kallas Domain Keys Identified Mail (DKIM). DKIM bygger på kryptografi, genom att avsändarens postkontor signerar (stämplar) all utgående post. Mottagarna kan i sin tur verifiera stämpeln.

DKIM syftar till att motverka nätfiske (phishing), vilket är en sorts skräppost med falsk avsändare som har som mål att lura Internetanvändare att lämna ifrån sig känslig information.

Genom att kryptografiskt signera en kontrollsumma av dessa delar med en privat nyckel kan eventuell modifiering upptäckas av den mottagande parten. Tillsammans med den privata nyckeln finns en publik nyckel som behövs för att kunna verifiera att signaturen är korrekt. Den publika nyckeln publiceras av avsändaren i dennes DNS.

DKIM-signaturen skickas sedan med meddelandet som en del av e-posthuvudet. Den mottagande programvaran validerar det mottagna meddelandet mot signaturen och den publika DKIM-nyckeln. Därmed kan eventuella förändringar upptäckas.

För att upptäcka otillåten borttagning av signaturen används Author Domain Signing Practices (ADSP). Med ADSP kan avsändaren meddela mottagaren huruvida den aktuella domänen signerar sina meddelanden eller inte. Denna information sprids också via avsändarens DNS. ADSP är en så kallad proposed standard sedan augusti 2009. Funktionen dokumenteras i RFC 5617. I korthet definierar RFC:n en posttyp som kan annonsera huruvida en domän signerar sin utgående e-post och hur andra servrar kan komma åt och tolka den informationen.

Bilaga 9 - Åtgärder för transportskydd

Elektronisk post

Överföring av elektronisk post sker vanligen i klartext och brukar därför ofta jämföras med vykort. Sedan några år tillbaka finns en standard för hur man kan överföra e-post med transportskydd, något som närmast skulle kunna jämföras med att man visserligen fortfarande skickar vykort men faktiskt låser postvagnen under själva transporten. Detta gör att någon som försöker avlyssna e-posten på vägen mellan postkontoren inte kan se vad som skickas. Transportskydd av e-post kallas ofta STARTTLS.

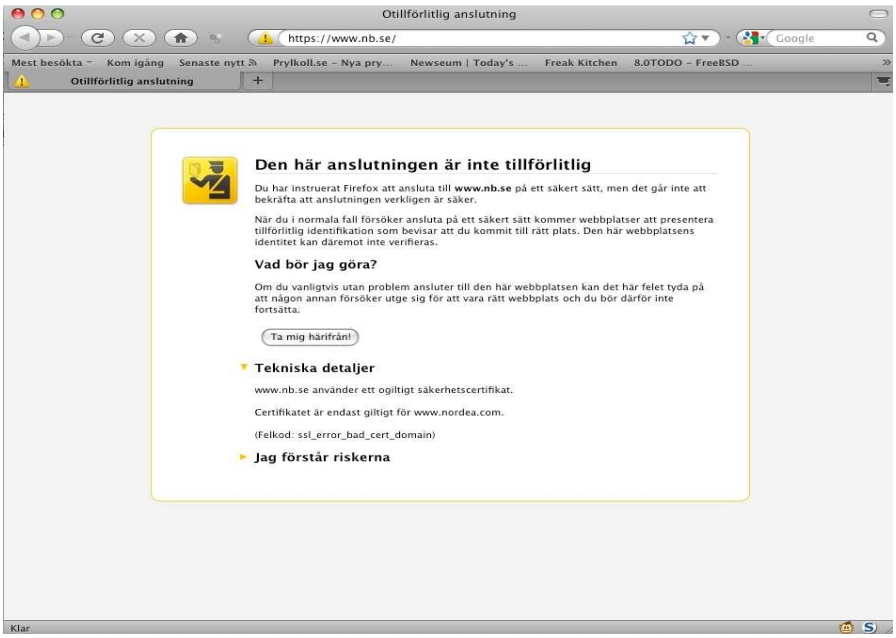
Om man vill skicka e-post som ingen annan ska kunna läsa, inte ens de som ansvarar för e-postsystemet (det vill säga "sitter på postkontoret"), behövs det ytterligare skydd. I dessa fall krypterar man hela brevet genom att man "klistrar igen kuvertet och skickar brevet rekommenderat", för att jämföra med traditionell postgång. De två vanligast förekommande metoderna för denna typ av kryptering är PGP och S/MIME.

Webbtrafik

För en användare som exempelvis vill komma i kontakt med en svensk myndighet eller med sin bank är det viktigt att veta att den server man har kontakt med är rätt server, att anslutningen av någon anledning inte har skett till fel tjänst eller server på grund av felkonfiguration eller medvetet bedrägeriförsök.

En av de tekniker som används även för detta är Transport Layer Security (TLS). TLS/SSL ger användarna möjlighet att kontrollera att man hamnat hos rätt server eller tjänst.

Webbläsaren kontrollerar adressen som uppgivits i webbläsaren med den serveradress som ingår i webbcertifikatet. Om dessa inte stämmer överens, får användaren en varning om att allt kanske inte står rätt till, som exemplet nedan.



.SE (Stiftelsen för Internetinfrastruktur) är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige. .SE ansvarar för Internets svenska toppdomän, .se, med registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret. Överskottet från registrering av domännamn finansierar initiativ som främjar Internetutvecklingen i Sverige, både genom egen verksamhet och genom finansiering av fristående projekt. Läs mer på http://www.iis.se.