Hälsoläget i .se 2012

– nåbarhet på nätet

Innehåll

1 Introduktion

Detta är den sjätte rapporten i ordningen från .SE:s undersökning av nåbarhet på nätet och hälsoläget i .se med de senaste resultaten från 2012.

Årets undersökning är precis som tidigare år till stora delar men inte fullständigt en uppföljning av de tidigare undersökningar som genomförts under åren 2007-2011.

Rent statistiskt finns det vissa mindre avvikelser på grund av förändringar i domännamnssystemet för undersökningsgruppen. Det är viktigt att förstå att vi tar en ögonblicksbild av hur det ser ut vid en viss tidpunkt. Den bilden kan ändras väldigt fort om till exempel någon förändrar sin miljö. Vi har däremot inte ändrat i kategorierna, dessa är desamma som förra året.

Syftet med undersökningen är liksom tidigare att kartlägga och analysera kvaliteten och nåbarheten i framför allt domännamnssystemet (DNS) i .se-zonen och några andra viktiga funktioner för domäner registrerade i .se. Genom att undersökningen har genomförts flera år i rad kan vi också visa på utveckling och trender inom de undersökta områdena. Undersökningen har som vanligt gjorts på både ett urval av domäner som representerar viktiga funktioner i samhället och ett slumpmässigt urval motsvarande en procent av samtliga domäner i .se.

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

Undersökningen ingår som en del i ett större satsningsområde som kommer att ta form 2013 och gå under benämningen Internets ekosystem. Syftet med satsningsområdet är att övervaka kvaliteten på Internets infrastruktur i Sverige, och i enlighet med vår urkund bidra till en positiv utveckling genom att peka på områden för förbättringar och genom att förse marknaden med verktyg där man själv kan kontrollera status – egen eller andras - i olika avseenden.

.SE:s ambition är att genom insamling och analys av fakta samt spridning av resultaten bidra till att infrastrukturen har god funktionalitet och hög tillgänglighet.

Hälsolägetrapporten finansieras av .SE. Resultaten av årets undersökning har analyserats och rapporten har sammanställts av Anne-Marie Eklund Löwinder, säkerhetschef på .SE. Det operationella ansvaret för de verktyg som används har Patrik Wallström, projektledare på .SE. Granskningen av den statistiska analysen samt diagram och tabeller har gjorts 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 tekniken bakom undersökningen kan man få från Patrik Wallström. Honom når man på patrik.wallstrom@iis.se.

2 Sammanfattning

Årets undersökning har genomförts under oktober 2012. Liksom tidigare år ligger undersökningens fokus på DNS-kvalitet. Utvecklingen av IPv6 och DNSSEC är viktiga parametrar, inte minst som en uppföljning av utvecklingen av både IPv6 och DNSSEC eftersom dessa faktorer uppmärksammades särskilt i regeringens strategi för det IT-politiska området ”It i människans tjänst - en digital agenda för Sverige”.[1]

I årets undersökning kan vi konstatera att vi äntligen har hamnat under 20 procent i andel fel för undersökningsgruppen som helhet, närmare bestämt ligger den på 18 procent. Även andelen varningar har minskat rejält, från 37 till 30 procent.

2.1 Om undersökningsgruppen

I årets undersökning testas totalt 913 domäner fördelade på 1 445 unika namnservrar (både IPv4 och IPv6). Med ”unik” menas här servrar med unika IP-adresser. En namnserver hos en operatör kan härbärgera flera domäner. Vilka kategorier vi använt och hur många domäner som finns i varje kategori redovisas i avsnitt 0.

Dessutom har en jämförelse gjorts med en kontrollgrupp som utgör en procent av hela .se-zonen, det vill säga 11 806 slumpmässigt utvalda .se-domäner som redovisas i avsnitt 0.

För att vi ska kunna följa utvecklingen år från år försöker vi i allmänhet hålla oss till ungefär samma parametrar och undersökningsgrupp som använts tidigare. I år har vi inte genomfört några radikala förändringar förutom sådana som föranleds av att verksamheter tillkommit, ändrat namn eller upphört.

I fjol undersöktes till exempel 912 domäner mot årets 913, alltså en minimal skillnad.

Resultaten från undersökningsgruppen har också jämförts med en mätning på ett urval motsvarande en procent av alla domäner i hela .se-zonen, 11 806 domäner.

2.2 Fortsatt minskning av mängden allvarliga fel

2007 var det första året undersökningen genomfördes. 2008 års undersökning gav oss en fingervisning om att det hade skett en viss positiv utveckling på området jämfört med året innan. När vi 2009 började se trender kunde vi bara konstatera att förändringarna var blygsamma och att det fortfarande fanns stora brister som vi pekade på och vi föreslog också konkreta åtgärder för att komma tillrätta med dessa. Åtgärdsförslagen överlämnades till den dåvarande infrastrukturministern. 2010 kunde vi tyvärr inte se någon större förändring till det bättre. Resultaten för 2011 var positiva i flera avseenden. Så, hur ser det då ut 2012?

Den totala andelen allvarliga fel och varningar har minskat ytterligare, och för första gången har felprocenten hamnat under 20 procent för majoriteten av de undersökta domänerna. Situationen har förbättrats avsevärt sedan förra året både när det gäller andelen allvarliga fel och mängden varningar.

[1] http://www.regeringen.se/content/1/c6/17/72/56/99284160.pdf

2.3 Skillnader i undersökningen sedan förra året

Vårt syfte med att publicera resultaten från undersökningen av domännamnssystemet 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.

Resultaten genom åren bekräftar 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 definitionen av ”hög kvalitet”.

I detta sammanhang är det vi själva som har definierat vad vi anser vara hög kvalitet och definitionen har utgått från vad som rekommenderas som praxis, eller branschstandard, internationellt, *Best Common Practice*.

2.4 Dominerande aktörer ökar riskerna

Spridningen bland operatörer till vilka man ansluter namnservrar är i princip oförändrad från 2011. De stora Internetoperatörerna blir allt större och de mindre för en allt mer tynande tillvaro. Ett undantag är Telenor som har ökat sin andel från sex till nio procent. Risken med att många aktörer är anslutna till en och samma operatör är att om en enskild operatör dominerar inom en viss kategori kan konsekvensen bli att en hel sektor drabbas om den operatören får problem. Därför är det viktigt att ha flera namnservrar utplacerade hos olika operatörer.

2.5 Bristande kompetens hos konsulter och tjänsteleverantörer

Tidigare års undersökningsresultat har lett till slutsatsen att det finns brister i kunskaperna om vad som krävs för att hålla en hög kvalitet på domännamnssystemet (DNS). Den slutsatsen har förstärkts i och med kraven på införande av DNSSEC. Med DNSSEC följer krav på bland annat nyckelhantering. Det finns också skäl att göra en analys av vem som kan göra vad i en DNS-infrastruktur. Ompekning av en domän är en tämligen drastisk åtgärd som kan få stora konsekvenser om det sker på ett felaktigt sätt, vare sig det är oavsiktligt eller avsiktligt.

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 radikalt från tidigare undersökningar. Vi vill betona behovet av att olika verksamheter vässar sin beställarkompetens och ställer relevanta krav på både konsulter, registrarer och de leverantörer som driver exempelvis namnservertjänster, e-posttjänster och webbtjänster. För den offentliga förvaltningens vidkommande bör stöd till sådan kravställning komma från centralt håll.

2.6 Fortfarande namnservrar med rekursion påslaget

Mellan 2007 och 2012 har andelen namnservrar med rekursion påslaget minskat mycket kraftigt, från 40 procent till årets 10 procent. Sedan förra undersökningen har vi haft en minskning med ytterligare en procent. Kategorin

Kommuner är den som står för den största kvarvarande andelen rekursiva namnservrar, 16 procent. Myndigheter ligger också relativt högt med 11 procent. I kategorierna Landsting och ISP är det nere på 0 procent! Öppna rekursiva namnservrar kan missbrukas av andra och användas i överbelastningsattacker.

2.7 Fler använder IPv6

När det gäller införande av IPv6 ser vi en ökning över hela linjen, bland samtliga kategorier, från 19 till 24 procent. Den största ökningen har skett inom kategorin Registrarer där det gått från 19 procent som använde IPv6 2011 till 37 procent 2012. Universitet och högskolor är den kategori där det är allra vanligast, 73 procent använder IPv6. .SE driver ett mycket aktivt arbete för att påskynda spridningen av IPv6.

2.8 Fler DNSSEC-signerade domäner

Som resultat av en omfattande kampanj från .SE som genomfördes i december 2011 har vi sett en kraftig ökning av DNSSEC-signerade domäner. Vid årets undersökning har antalet signerade domäner i undersökningsgruppen (913 domäner) ökat till 100 domäner, motsvarande 11 procent.

Kontrollgruppen (ett urval av en procent av hela .se-zonen) har vid den nu genomförda mätningen 1 182 signerade domäner, eller 10 procent. Detta ska jämföras med undersökningen 2011 där endast 0,45 procent eller totalt 50 domäner i kontrollgruppen hade signerats.

Myndigheten för samhällskydd och beredskap, MSB, har varje år möjlighet att bevilja medel ur anslaget 2:4 Krisberedskap som kan sökas av utpekade statliga myndigheter. För 2012 prioriterades området robusthetshöjande åtgärder med inriktning mot att säkerställa adressuppslagningar på Internet, det som sker via domännamnssystemet DNS. Myndigheten har bland annat tryckt på att det är mycket angeläget att domäner för offentliga webbplatser signeras med DNSSEC, något som vi på .SE förstås tycker är utmärkt.

.SE som på olika sätt stödjer och uppmuntrar införandet av DNSSEC har därför i ett samarbete med MSB, PTS, och Sveriges Kommuner och Landsting (SKL), arbetat med att ta fram en paketlösning som kommunerna kan använda sig av. 2011 beviljades 86 kommuner medel för ett införande av DNSSEC.

2.9 Fler e-postservrar i Sverige

Årets mätning visar att hela 42 procent av de IPv4-adresserade e-postservrarna är placerade i Sverige mot fjolårets 24 procent, en relativt kraftig ökning.

2.10 Användningen av kakor ökar starkt

Vi har med anledning av förändringen i lagen om elektronisk kommunikation (2003:389) beträffande kakor (cookies) följt upp utvecklingen även på detta område. Trots den nya skärpta regleringen ser användningen av kakor ut att öka i alla kategorier. Den kraftigaste ökningen ser vi bland kommuner och statliga myndigheter.

PTS har fått i uppdrag av regeringen att undersöka om den nyligen införda ”kaklagen” har försämrat tillväxten på eller tilliten till Internet. Deras uppdrag kommer att redovisas i slutet av 2012.

3 Kontrollpunkter

I årets undersökning har vi bland annat tagit reda på fakta om följande kontrollpunkter:

- Hur hanterar verksamheten sin 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), vilka är de allvarligaste bristerna och inom vilka kategorier är de vanligast?
- Hur vanligt förekommande är det med namnservrar som är öppna för rekursion?
- Hur hanterar verksamheten sin e-post? Står servrarna i eller utanför Sverige, används TLS/SSL (transportskydd)?
- Hur ansluter verksamheterna sina webbplatser till Internet? Vilken serverprogramvara används? Hur används kakor?
- Har man infört IPv6 i verksamhetens IT-miljö?

Testerna har genomförts på domäner och namnservrar för ett stort antal viktiga verksamheter i samhället; affärsverk och statliga bolag, banker, försäkrings- och finansföretag, Internetoperatörer, kommuner, landsting, medieföretag och statliga myndigheter inklusive länsstyrelser, universitet och högskolor samt .SE:s registrarer totalt 913 domäner. Hur de fördelar sig per kategori framgår i avsnitt 0.

Datainsamlingen har skett automatiskt och har omfattat tester av de allra vanligaste felen och bristerna som vi förknippar med DNS-drift, e-post och webbhantering i förhållande till vad som bedöms vara praxis.

Med dessa tester har vi undersökt hur väl verksamheternas system fungerar i olika avseenden, var de allvarligaste felen finns och genomfört analyser av vad detta kan få för konsekvenser. Rapporten gör det möjligt att jämföra med samtliga tidigare undersökningar, det vill säga sammanlagt fem-sex års undersökningsresultat.

Till detta knyter vi också generella rekommendationer om hur vi anser att det borde se ut i den svenska DNS-infrastrukturen. Slutligen – med en dåres envishet – upprepar vi råd och rekommendationer om olika frågeställningar att ta tag i för ansvariga myndigheter, åtgärder som det kan vara lämpligt att gå vidare med och utreda mer i detalj.

Vi låter dessa stå kvar i princip oförändrade från förra årets undersökning eftersom resultaten från undersökningen talar sitt tydliga språk, nämligen att det finns brister som både behöver och enkelt kan åtgärdas.

Genom att bearbeta strategiska partners som PTS och MSB har .SE medverkat till att kommuner kan ansöka om anslag för att driva projekt för införande av DNSSEC även för nästa år. Dessa medel kommer att beviljas och kunna tas i anspråk från och med 2013. Vi ser gärna att myndigheter och individer i beslutande ställning använder våra råd och rekommendationer och vidtar åtgärder för förbättringar inom samtliga berörda områden; DNS, DNSSEC och IPv6, men även för skydd av kommunikation via e-post och webb.

4 DNS-tjänst med kvalitet

Domännamnssystemet (DNS) är en av hörnstenarna på Internet och har till uppgift att förenkla adressering av resurser på Internet. .SE har ansvaret för Sveriges nationella toppdomän på Internet, en uppgift som anses så viktig att den regleras av en särskild lag, lag (2006:24) om nationella toppdomäner för Sverige på Internet[2]. Varje Internetansluten enhet har en egen IP-adress som med hjälp av domännamnssystemet kan kopplas till en adress i en form som är lättare att hantera för oss människor, det vill säga domännamn.

Vi ser till att de omkring 1 250 000 domännamn som slutar med .se kan peka ut rätt resurser på Internet genom att vi för ett register över dem och dirigerar alla frågor och svar som ställs i domännamnssystemet. På så vis går det som regel blixtsnabbt att hitta fram till exempelvis rätt webb- eller e-postserver.

Dygnet runt, året om, övervakar vi att DNS-frågor om .se-domäner besvaras på Internet. .SE:s namnservrar besvarar i genomsnitt 5 000 frågor per sekund, med toppar som ibland ger mångdubbelt fler frågor.

Vi har använt nedanstående definition av en DNS-tjänst med kvalitet för årets liksom för tidigare års undersökningstillfällen, där hög kvalitet för oss innebär:

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

Det är viktigt att den egna infrastrukturen för DNS ansluter till aktuell standard och praxis 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) med vad som är att betrakta som en bra infrastruktur för DNS.

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 radikalt från tidigare undersökningar. Vi vill än en gång betona behovet av att olika verksamheter vässar sin beställarkompetens och ställer relevanta krav på både konsulter, registrarer och de leverantörer som driver namnservertjänster, e-posttjänster och webbtjänster. För den offentliga förvaltningens vidkommande bör det underlätta om stöd för sådan kravställning kommer från centralt håll.

I bilaga 4 redovisar vi för den mer tekniskt bevandrade läsaren vad branschstandarden för att skapa en infrastruktur för DNS i Sverige med hög kvalitet innefattar i termer av rekommendationer.

[2] https://lagen.nu/2006:24

5 Tester 2012

2012 års tester har som vanligt omfattat både domänernas konfiguration och status för de namnservrar som svarar på frågor om domänen samt några av de enligt vår bedömning viktigaste parametrarna för e-post och webb. I år har vi dock inte tittat på certifikatshantering i webb. Anledningen är att det är svårt att få fram tillförlitliga data, för det krävs andra verktyg än de vi har tillgång till just nu. Det är dock ett område som vi har för avsikt att dyka djupare i under nästa år, på samma sätt som vi i år dykt djupare i DNSSEC (rapport[3] publicerad i mars 2012) och kommer att dyka djupare i e-post (med en mer detaljerad rapport som kommer att publiceras i november 2012).

Vid de tester som ligger till grund för den här rapporten används programvara som automatiskt går igenom de olika kontrollpunkter som angivits i branschstandarden för samtliga domäner som ingått i undersökningen, både för undersökningsgruppen som helhet och separat för varje kategori. Detta har kompletterats med vissa frågor bland annat om hantering av elektronisk post och webb.

Årets tester har genomförts vid samma tidpunkt som tidigare år och har omfattat totalt 913 domäner på 1 445 unika namnservrar. Testobjekten har grupperats i kategorier på följande sätt (inom parentes redovisas det antal verksamheter som ingick i respektive kategori förra året):

- 57 affärsdrivande verk och statliga bolag (60).
- 81 banker, finansinstitut och försäkringsbolag (79).
- 21 Internetoperatörer (ISP) (22).
- 290 kommuner (290).
- 20 landsting (21).
- 36 medieföretag (34).
- 229 statliga myndigheter, inklusive länsstyrelser (exkl. myndigheter under Riksdagen) (228).
- 37 universitet och högskolor (39).
- 151 registrarer (146).

Kategorin registrarer, det vill säga återförsäljare av .se-domäner, är många gånger också tillhandahållare av namnserver- och andra tjänster till domäninnehavare. Hur många ackrediterade registrarer som finns för .se ändrar sig kontinuerligt.

Precis som tidigare år rapporterar vi två olika typer av problem, och kategoriserar dem som fel respektive varningar.

[3] https://www.iis.se/docs/Halsolaget-DNS-och-DNSSEC1.pdf

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, men de bedöms inte vara lika akuta och åtgärder inte lika angelägna. Det skulle givetvis höja kvaliteten och nåbarheten om dessa fel eliminerades.

6 Observationer 2012

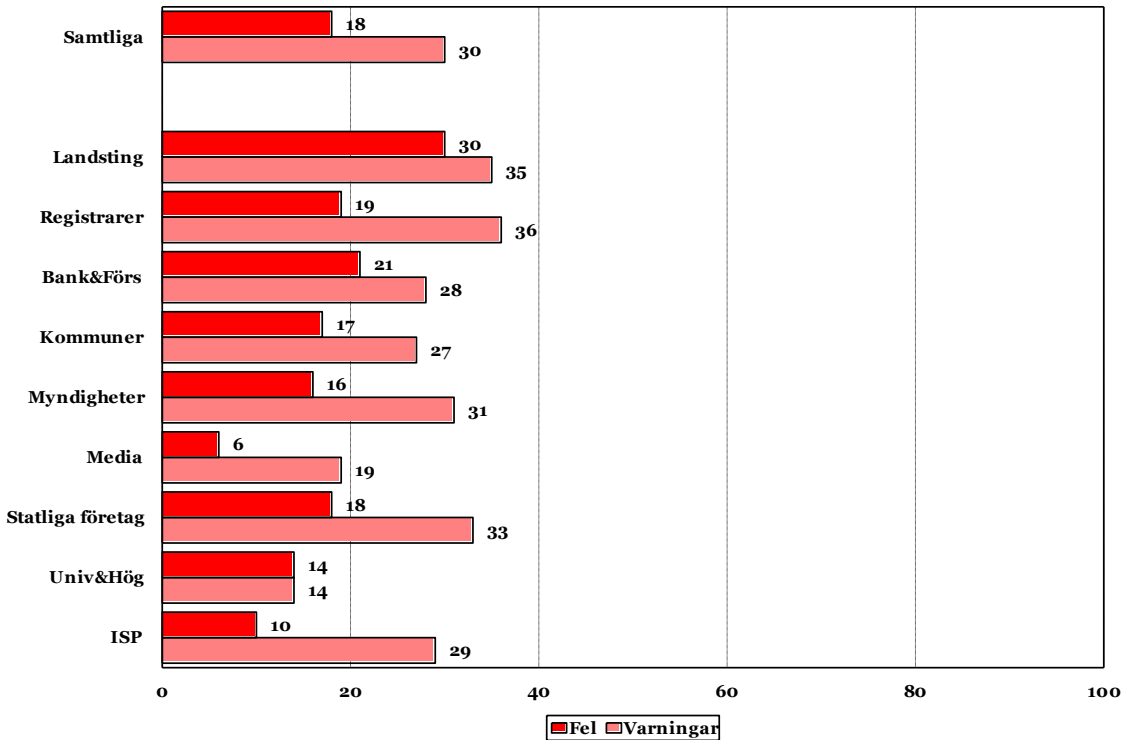
2007 genomförde vi den första mätningen för att få en uppfattning om hur det såg ut i .se-zonen. 2008 års undersökning gav oss en fingervisning om att det hade skett en positiv utveckling på området. När vi 2009 började se trender kunde vi bara konstatera att förändringarna var blygsamma och att det fortfarande fanns stora problem som vi pekade på och föreslog åtgärder mot. 2010 fanns det fortfarande allvarliga brister och vi kunde inte se någon förändring till det bättre, snarare tvärtom. Av de testade domänerna 2010 hade 25,4 procent allvarliga fel och 43,4 procent brister av en karaktär som genererade varning. I undersökningen 2011 var motsvarande siffror 21 procent domäner med allvarliga fel och 37 procent med brister av en karaktär som genererade varning.

I årets undersökning kan vi konstatera att vi äntligen har hamnat under 20 procent i andel fel för undersökningsgruppen som helhet, närmare bestämt ligger den på 18 procent. Även andelen varningar har minskat rejält, från 37 till 30 procent.

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 på föregående sida visar procentandelarna fel respektive varningar för de 913 domänerna i hela undersökningsgruppen (Samtliga) och för varje enskild kategori. Staplarna ska alltså läsas så att av de 913 verksamheter som ingår i undersökningen är 18 procent behäftade med fel av allvarligare karaktär och 30 procent med brister som genererar en varning. Detta är en klar förbättring från föregående års undersökning.

För en mer detaljerad beskrivning av fördelningen fel och varningar per kategori och år, se avsnitt 6.3.

6.2 De vanligaste felen

De vanligaste felen i DNS bland undersökta domäner och namnservrar som genererar antingen fel eller varning enligt vår definition har under samtliga år då vi genomfört undersökningen i princip varit desamma:

- Namnservern svarar inte på anrop via TCP. Detta beror troligtvis på att DNS-servern inte är korrekt uppsatt eller på en felaktigt konfigurerad brandvägg. Den höga andelen av just detta fel inom kategorin landsting försöker vi härleda men vi har ännu inget klart besked.
  Det är en ganska utbredd missuppfattning att DNS inte behöver kunna kommunicera enligt TCP-protokollet (om den inte tillhandahåller zonöverföringar). TCP är emellertid ett krav enligt standard (RFC 5966, *DNS transport over TCP implementation requirements*), och trenden är att behovet av TCP ökar då nya protokoll som IPv6 och DNSSEC leder till att det används i större omfattning än tidigare. Felet är en indikation på att den som har konfigurerat namnserver eller brandvägg inte har tillräckligt aktuella kunskaper om DNS.

- Verksamheten har ingen konsekvent 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 namnserver är inte samma hos barnzonen som hos 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 namnserver finns listad i föräldrazonen men inte i barnzonen. Det här är troligtvis ett administrationsfel. Föräldrazonen behöver snarast uppdateras så att den listar samma namnservrar som finns listade hos barnzonen. Konsekvensen av ett sådant fel är att den redundans som någon har försökt åstadkomma i praktiken inte finns.

- 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 är något som blir allt vanligare med utökad användning av DNS för exempelvis 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 ligger felet sannolikt någon annanstans, till exempel i förbindelsen till namnservern eller att servern inte har en korrekt angiven IP-adress. Våra tester på namnservern avslutas direkt om båda dessa tillstånd har konstaterats.

- Endast en namnserver hittades för domänen. Det bör alltid finnas minst två namnservrar för en domän för att kunna hantera tillfälliga problem med förbindelserna. Om denna enda server eller förbindelsen till servern slutar fungera blir tjänsterna som pekas ut från namnservern också onåbara. Vi räknar namnservrar 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 en notifiering) eftersom det är under införande. Det är givetvis bättre att ha en ensam namnserver som kommunicerar via IPv6 än att inte ha någon alls.

- Namnservern är rekursiv. Namnservern svarar på rekursiva anrop från tredje part (så som DNSCheck). Det är väldigt lätt att utnyttja öppna rekursiva resolvrar i överbelastningsattacker (så kallade DDOS-attacker, Distributed Denial of Service), eftersom man med användning av en väldigt liten DNS-fråga kan skapa en hävstångseffekt med ett mångdubbelt större svar (förstärkningsattack, *amplification attack*). I DNS är det också möjligt att förfalska avsändaradressen, så att den som vill attackera ett system kan skapa frågor med falsk avsändaradress som går till en tredje part. Frågorna ställs på ett sätt som genererar stora DNS-svar vilka går till den förmodade avsändaren vilken alltså är en tredje part vars tjänster kan bli mer eller mindre blockerade. (Se bilaga 6).

- SOA-serienumret (Start of Authority) 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 eftersom de då innehåller olika versioner av information om domäner.

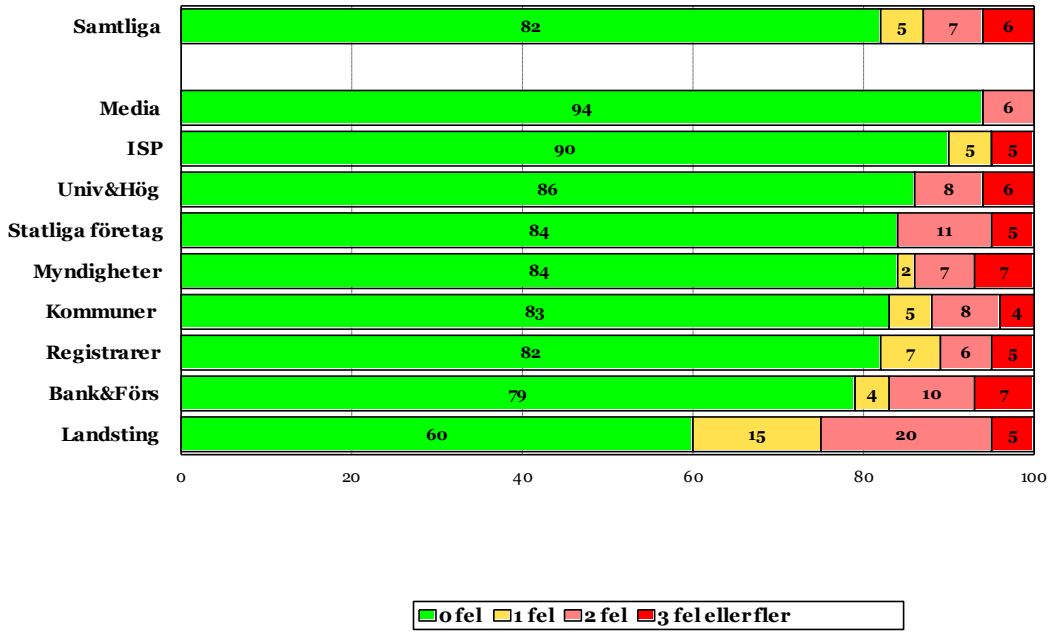
Felkonfigurationer som utförs av en och samma konsult hos många verksamheter eller av någon av de större namnserveroperatörna fortplantar sig till alla domäner som de hanterar och kan, om de är många till antalet, givetvis få stort genomslag i resultaten från undersökningen. Framför allt om dessa fel uppträder inom en och samma kategori.

Värt att nämna är att .SE:s tre största registrarer har cirka 50 procent av marknaden och tar vi de sju största har dessa nästan 60 procent av marknaden. Bland namnserveroperatörerna så har de två största ungefär 36 procent av marknaden och de fem största 50 procent av marknaden. Samtidigt finns det bland namnserveroperatörerna en väldigt lång svans, det vill säga väldigt många mycket små operatörer.

6.2.1 Mängden fel per kategori

Det är en viss skillnad om en domän bara har ett fel eller om den har flera olika fel som många gånger kanske dessutom samverkar. Av det skälet tittar vi också på spridningen av mängden fel både i antal och per kategori.

Tabell 2: Procentuell fördelning av mängden fel per kategori



Fördelningen mellan 1, 2 och 3 eller fler fel är jämn i hela undersökningsgruppen (Samtliga). Kategorin Media har gått om kategorin ISP:er, det vill säga Internetoperatörerna, och har i år den lägsta felprocenten, tätt följt av ISP. Kategorierna Bank och Försäkring samt Myndigheter är de som har flest fel, tre eller flera. Kategorin Landsting har den sammantaget högsta felprocenten med relativt många som har fler än ett fel.

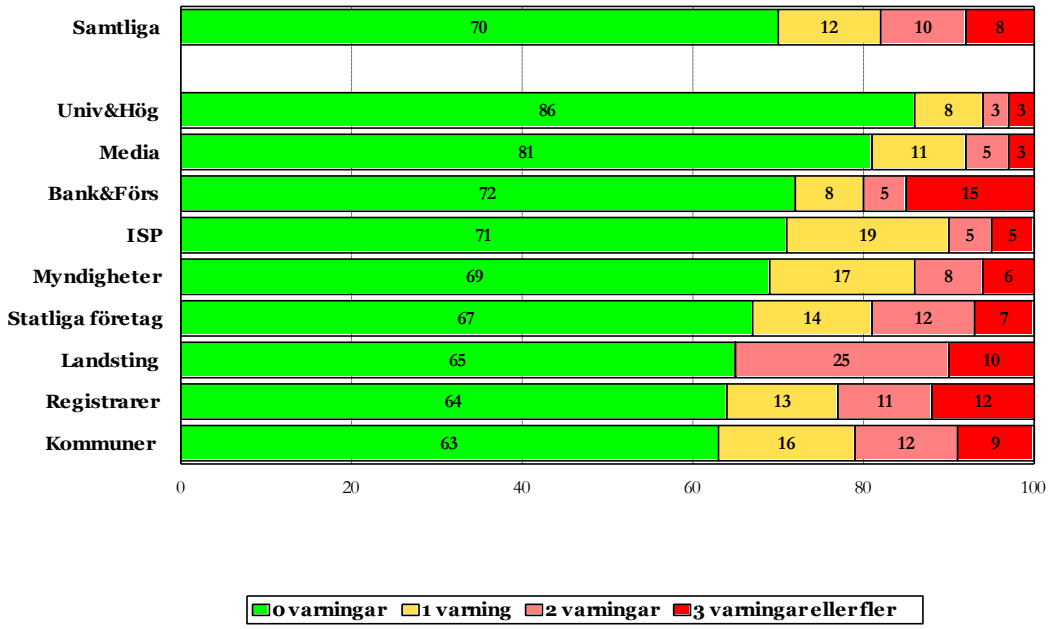
Via våra kontakter har vi nyligen uppmärksammat landstingen på årets resultat. Orsakerna till felen har varit av lite varierande slag, men det viktiga är att de jobbar på att lösa problemen. Eftersom vår undersökning är en ögonblicksbild av hur det ser ut just då mätningarna görs kan saker och ting förändras väldigt snabbt.

Vi har ju tidigare hävdat att alla kan komma under 20 procent fel utan större ansträngningar. I årets mätning ser det ut som om det målet har uppnåtts för alla kategorier förutom Landsting samt Bank och försäkring. För att komma under 15 procent krävs det lite mer än att bara rätta till grundläggande hygienfaktorer, men det är absolut ingen omöjlighet.

6.2.2 Mängden varningar per kategori

Vi har också detta år undersökt motsvarande fördelning av antalet varningar i antal och inom respektive kategori. Resultatet visas i följande tabell.

Tabell 3: Procentuell fördelning av mängden varningar per kategori



Kategorin Kommuner har störst andel varningar, följt av Registrarer, Landsting och Statliga företag. Bank och försäkring samt Registrarer har dessutom väldigt många varningar, det vill säga hög andel med 3 eller fler varningar.

Vår bedömning är att detta i de allra flesta fall 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. Både fel och varningar påverkar emellertid nåbarheten negativt.

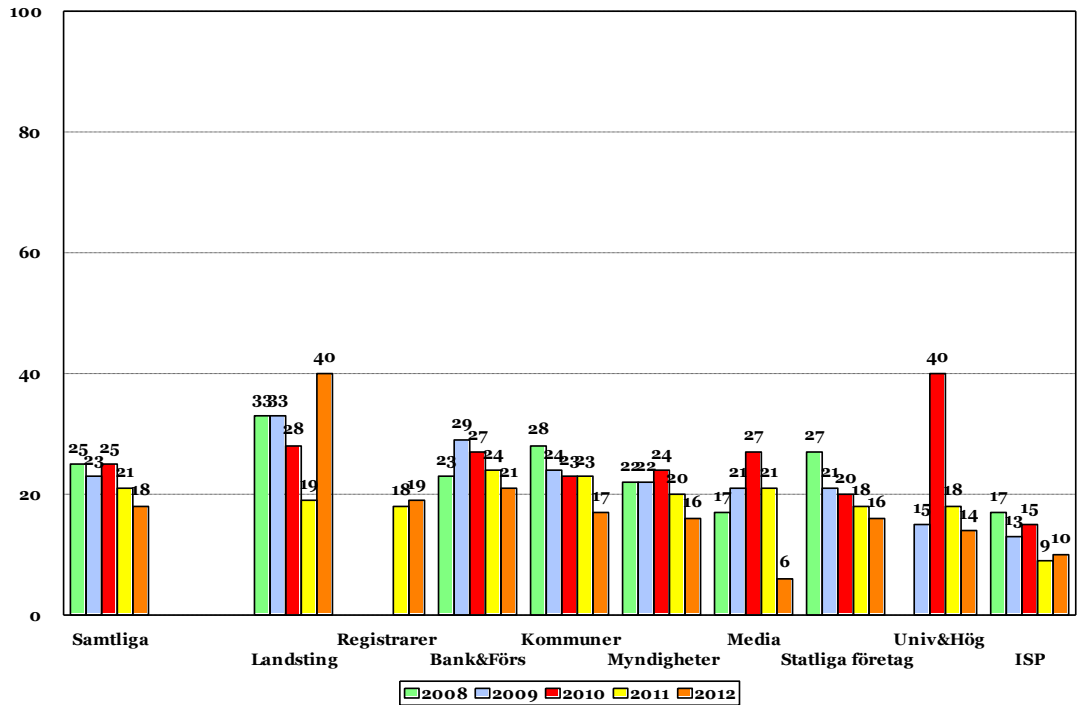
6.3 Jämförelse över tiden - fel och varningar

I och med att vi har sparat data från tidigare undersökningar har vi också möjlighet att jämföra resultaten mellan årets och tidigare undersökningar för de kategorier som finns med i undersökningarna för alla fem åren. Några kategorier kom till för första gången 2009 och därför kan vi för dessa kategorier

bara redovisa resultat från de tre senaste undersökningarna. Kategorin Registrarer är ny sedan 2011.

I tabellen nedan jämför vi andelen fel över tiden från 2008 till 2012 (med undantag för Universitet och högskolor respektive Registrarer som tillkom 2009 respektive 2011).

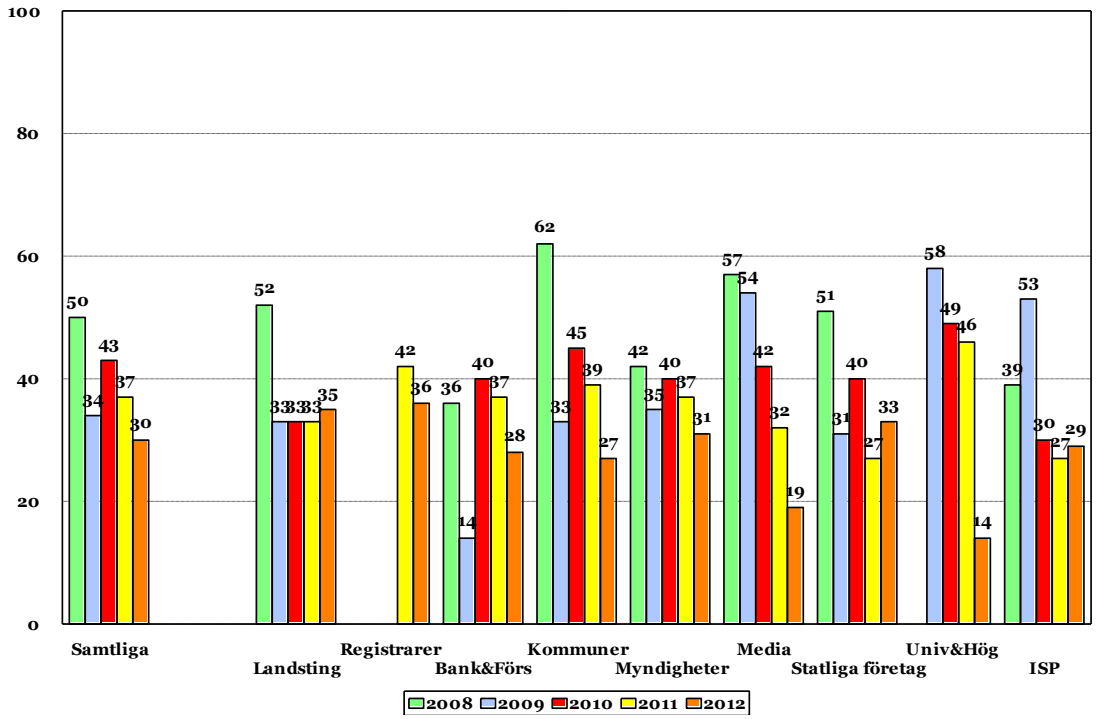
Tabell 4: Andel fel över tiden



Av tabellen kan vi se att situationen har förbättrats väsentligt inom i princip alla kategorier jämfört med föregående år. Kategorin Media har minskat från 21 procent fel till endast 6 procent i år.

Kategorin Landsting utgör det stora undantaget med en ökning från 19 till 40 procent fel, något som vi alltså gjort dem uppmärksamma på och där vi har en förhoppning att det kommer att ändras relativt snabbt. Kategorierna Registrarer och ISP:er visar en marginell ökning, men ingenting som är alarmerande.

Tabell 5: Andel varningar över tiden

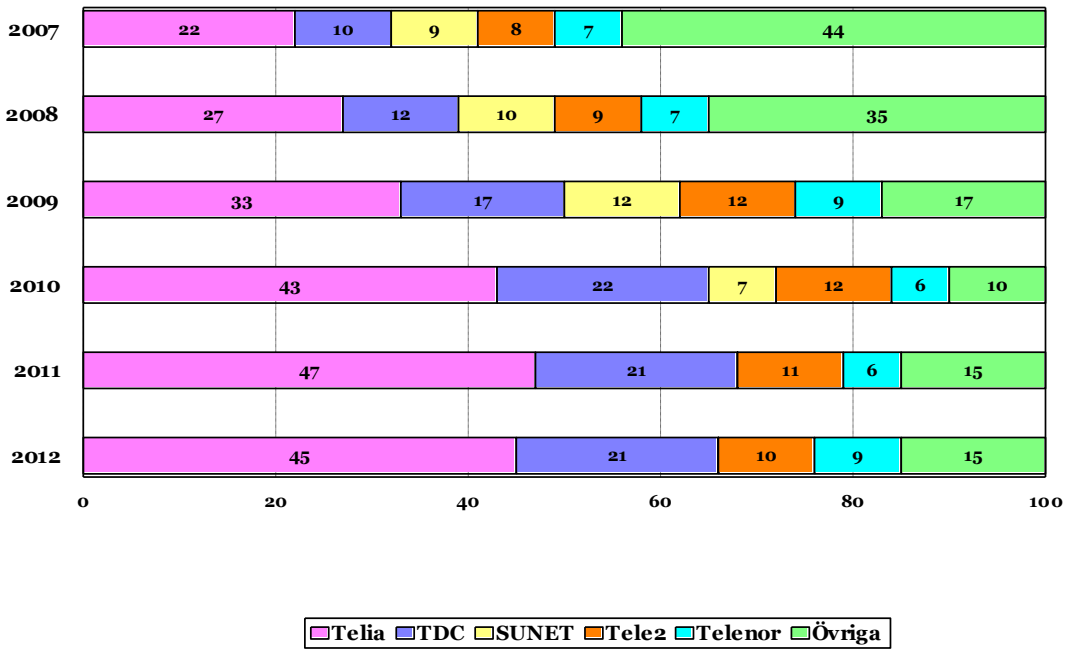


När det gäller varningar har andelen sådana också minskat, från 37 till 30 procent för samtliga i undersökningsgruppen. Den allra största minskningen har skett inom kategorin Universitet och högskolor, från 46 till 14 procent. Minskningen är utspridd i alla kategorier förutom kategorierna Landsting, Statliga företag och 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: Fördelning operatörsvis – anslutning av namnservrar till Internet



Vi konstaterar att spridningen bland operatörer när det gäller anslutning av namnservrar till Internet minskat från år till år om man tittar på den totala mängden domäner.

Vi ser överlag små förändringar hos de största operatörerna där i synnerhet Telia och Tele 2 ser ut att ha förlorat någon procent till förmån för Telenor som förefaller ha ökat från 6 till 9 procent. Förändringarna jämfört med förra året är alltså relativt små. Andelen ”Övriga” ligger kvar på 15 procent även i år.

Spridningen av drift av namnservrar av olika operatörer fortsätter alltså att utvecklas på samma sätt som tidigare. De stora blir allt större. En risk med den utvecklingen är om en enskild operatör skulle dominera inom en viss kategori. Konsekvensen av en sådan dominans blir i värsta fall att en hel sektor drabbas om den dominerande operatören får problem.

Det ökar redundansen om namnservrarna är anslutna till olika operatörer.

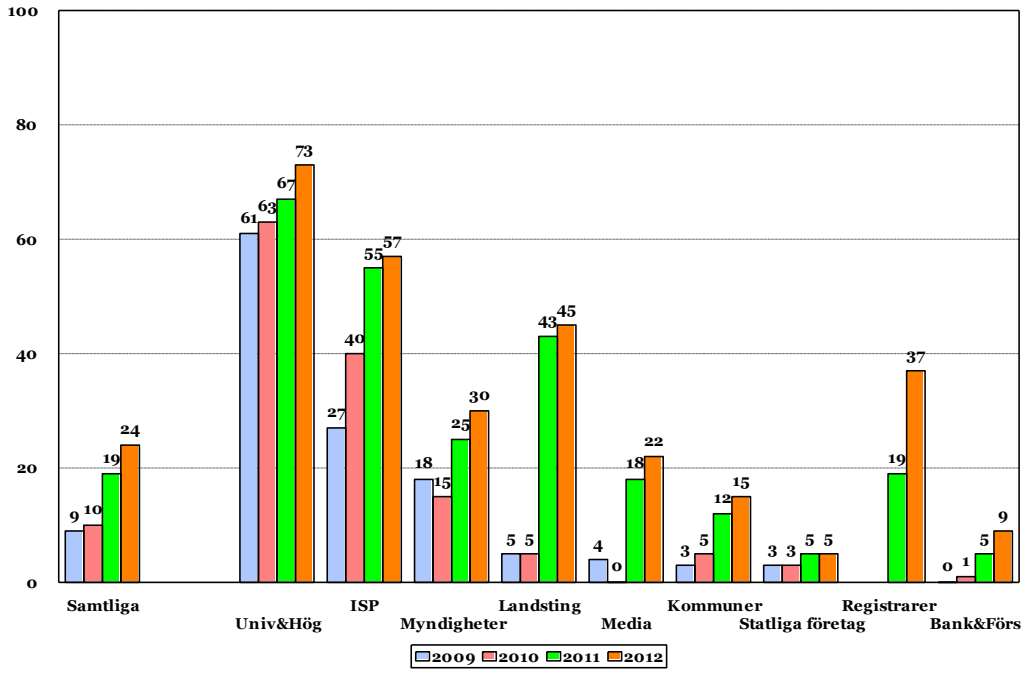
6.5 Namnservrar med IPv6

Att införa IPv6 som gemensamt kommunikationsprotokoll är det enda sättet att garantera en stabil framtida Internetinfrastruktur.

Trenden med en ökad aktivitet på IPv6-området håller i sig och fortsätter uppåt även i år. Universitet och högskolor toppar inte oväntat utvecklingen, men samtliga kategorier utom en visar på en ökning. Den allra största ökningen finns inom kategorin Registrarer, från 19 till 37 procent. Det är endast inom kategorin

Statliga företag som det fortfarande går väldigt långsamt. Det har i själva verket inte ändrat sig alls sedan förra årets mätning.

Tabell 7: Andel som använder namnservrar som går att nå med IPv6



Totalt 24 procent av de undersökta domänerna har någon namnserver som går att nå via IPv6, jämfört med 19 procent 2011. I dag pågår arbetet med att införa det nya protokollet för fullt hos Internetleverantörerna. Nu måste även företag och organisationer följa efter. IPv6 införs parallellt med IPv4 och det gamla protokollet kommer inte att fasas ut förrän efter en övergångstid på flera år. .SE verkar på olika sätt för att underlätta och stödja införandet av IPv6 i Sverige.[4]

Adressbristen är redan ett faktum och det är mer än hög tid att införa IPv6. Regeringen gav i fjol Post- och telestyrelsen (PTS) i uppdrag att beskriva hur IPv6 kan införas på myndighetsnivå med avseende på tillgänglighet, säkerhet och ekonomi. Syftet med beskrivningen var att den ska kunna fungera som stöd till myndigheter, kommuner och andra organisationer i offentlig sektor i deras införande av IPv6. Uppdraget har avrapporterats och rapporten finns att läsa på http://www.pts.se/upload/Rapporter/Internet/2011/2011-18_Att_infora_internetprotokollet_IPv6.pdf.

Post- och telestyrelsen (PTS) har fått ännu ett regeringsuppdrag att följa upp myndigheternas införande av IPv6. I samband med det har PTS lanserat webbsidan ”Myndigheter med IPv6”[5]. Där man kan följa IPv6-införandet i det offentliga Sverige.

[4] https://www.iis.se/lar-dig-mer/ipv6/om/
[5] http://e-tjanster.pts.se/internet/ipv6

Det är viktigt att förstå att en övergång av det här slaget kräver förberedelser och arbete på omkring 12-18 månader. Det finns en risk för att vi är på väg in i ett nytt Y2K-scenario. Alla kommer att vilja göra anspråk på en begränsad mängd resurser i form av utbildning och erfarna konsulter. Vårt råd är att planera i förväg, långt i förväg. Vänta inte heller på Dagen D, låt era tekniker börja testa redan nu, de kommer långt med en brandvägg och en dator. .SE tillhandahåller en omfattande e-utbildning för IPv6 där vi precis har lagt till fem nya avsnitt: https://www.iis.se/lar-dig-mer/ipv6/e-utbildning/.

6.6 Operatörer för drift av namnservrar

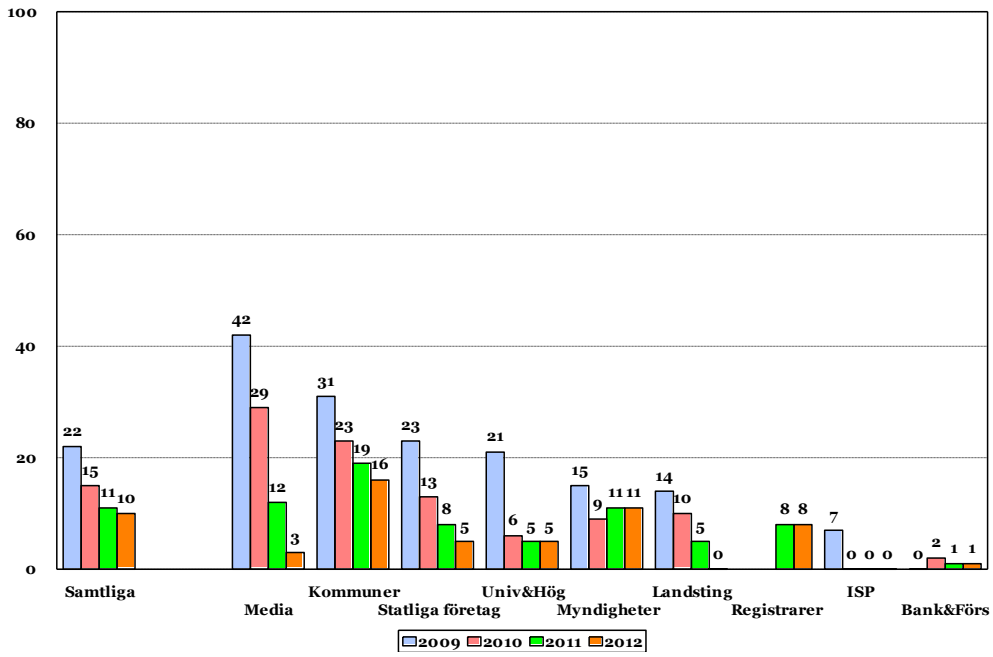
I normalfallet är det en registrar som också svarar för driften av namnservrar för en domän. Som vi tidigare nämnt har .SE:s tre största registrarer cirka 50 procent av marknaden och tar vi de sju största har dessa nästan 60 procent av marknaden. Bland namnserveroperatörerna hanterar de två största ungefär 36 procent och de fem största 50 procent av domänerna i .se-zonen. Allvarliga felkonfigurationer hos någon av dessa registrarer som också driver namnservrar för sina kunder blir givetvis mycket märkbara.

6.7 Namnservrar med rekursion påslaget

Vi upprepar även i år budskapet från tidigare år: Öppna rekursiva namnservrar har mycket få legitima användningsområden och kan komma att utnyttjas bland annat i samband med överbelastningsattacker. En stark rekommendation är därför att eliminera möjligheten att utnyttja öppna rekursiva resolvrar med hjälp av tillgängliga tekniker som beskrivs i de referenser som anges i bilaga 6.

Andelen namnservrar som är öppna för rekursion har minskat ännu lite till i år och är nere i 10 procent jämfört med 11 procent 2011. Det är mycket positivt, med tanke på vilka risker öppna rekursiva namnservrar innebär.

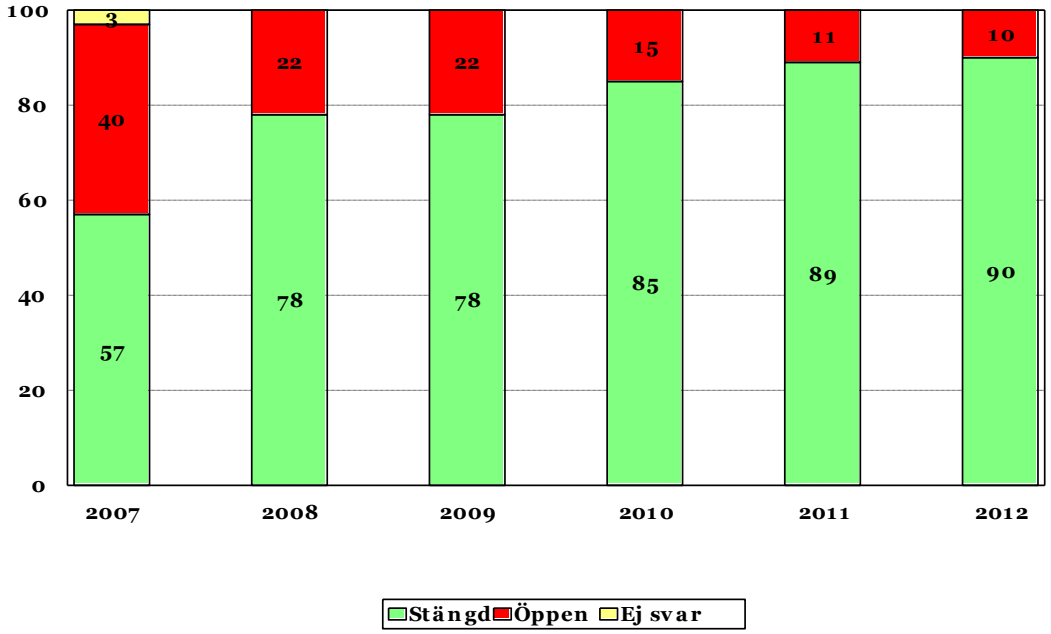
Tabell 8: Namnservrar öppna för rekursion per kategori



Vi ser en fortsatt förbättring, och en av förklaringarna till dessa förbättringar att namnservrar idag levereras med rekursion avslaget som grundinställning. Vi tror också att de som ansvarar för DNS-infrastruktur har blivit bättre på att införa separation mellan auktoritativa namnservrar (de som faktiskt ska svara på frågor) och resolvrar (de som bara förmedlar frågor och svar). Kategorin Kommuner är den som står för den största andelen rekursiva namnservrar, 16 procent. Myndigheter ligger också relativt högt med 11 procent. I kategorierna Landsting och ISP är det nere på 0 procent!

I tabellen på nästa sida kan vi följa utvecklingstrenden från 2007 och fram till årets mätning.

Tabell 9: Namnservrar öppna för rekursion 2007-2012



Mellan 2007 och 2012 har andelen namnservrar med rekursion påslaget alltså minskat mycket kraftigt, från 40 till 10 procent. Sedan förra undersökningen har vi haft en liten minskning med ytterligare en procent. Vi ser mycket positivt på den trenden och hoppas på att den ska fortsätta. Framför allt bör kommuner och statliga myndigheter se över sin infrastruktur i detta avseende.

6.8 Användning av DNSSEC

Säker DNS (DNSSEC) är ett tillägg till DNS-protokollet som bygger på kryptografiska nycklar och används för att signera innehållet i zonfilen för en domän, både toppdomäner och huvuddomäner.

.SE:s lansering 2005 av DNSSEC för säkrare DNS bidrog till att ett ökat fokus hamnade 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.

Vi är särskilt intresserade av att ta reda på hur väl förberedda domäner i .se är för DNSSEC, inte minst för att DNSSEC fått stor uppmärksamhet i regeringens IT-politiska strategi ”IT i människans tjänst – En digital agenda för Sverige”[6], i aktiviteter från PTS och i MSB:s handlingsplan ”Samhällets informationssäkerhet – Nationell handlingsplan 2012”[7].

[6] http://www.regeringen.se/sb/d/14216/a/177256
[7] https://www.msb.se/RibData/Filer/pdf/26290.pdf

MSB anger i sin handlingsplan att målet är att DNSSEC ska vara infört hos merparten av de offentliga verksamheterna vid utgången av 2014. Åtgärder som myndigheten kommer att vidta är att följa upp de insatser som gjordes 2011 och också fortsätta arbetet med att införa DNSSEC för återstående domäner i samverkan med .SE, PTS och SKL.

Det - och det faktum att .SE ansvarar för den svenska toppdomänen - är de viktigaste skälen till varför vi fokuserar våra tester på just kvalitet i DNS. Att Internets så kallade rotzon signerades sommaren 2010 satte än mer fart på spridningen av DNSSEC. Eftersom rotzonen är toppen av DNS-hierarkin blev det därmed enklare för de underliggande toppdomänerna att införa DNSSEC.

DNSSEC skyddar Internetanvändare från förfalskad eller manipulerad DNS-information såsom exempelvis genom så kallad DNS cache poisoning. Svar på DNS-frågor som säkrats med DNSSEC förses med en digital signatur och genom att verifiera signaturen kan man förvissa sig om att DNS-informationen inte har förändrats på vägen från namnservern till mottagande system.

6.9 Hur utbredd är användningen av DNSSEC?

Bland de 912 domäner som fanns i undersökningsgruppen 2011 var 6,69 procent eller 61 domäner signerade med DNSSEC. Det var framför allt kommuner, myndigheter, landsting och ISP:er som hade börjat införa den säkrare tekniken.

Som resultat av en omfattande kampanj som genomfördes i december 2011 har vi sett en mycket omfattande ökning av DNSSEC-signerade domäner. I februari 2012 gjorde vi en djupdykning i DNSSEC-mätningar vilket redovisades i en rapport[8] som publicerades i mars 2012, och som var särskilt inriktad på DNSSEC-kvalitet.

Vid den nu genomförda undersökningen har antalet signerade domäner i undersökningsgruppen (913 domäner) ökat till 100 domäner, motsvarande 11 procent.

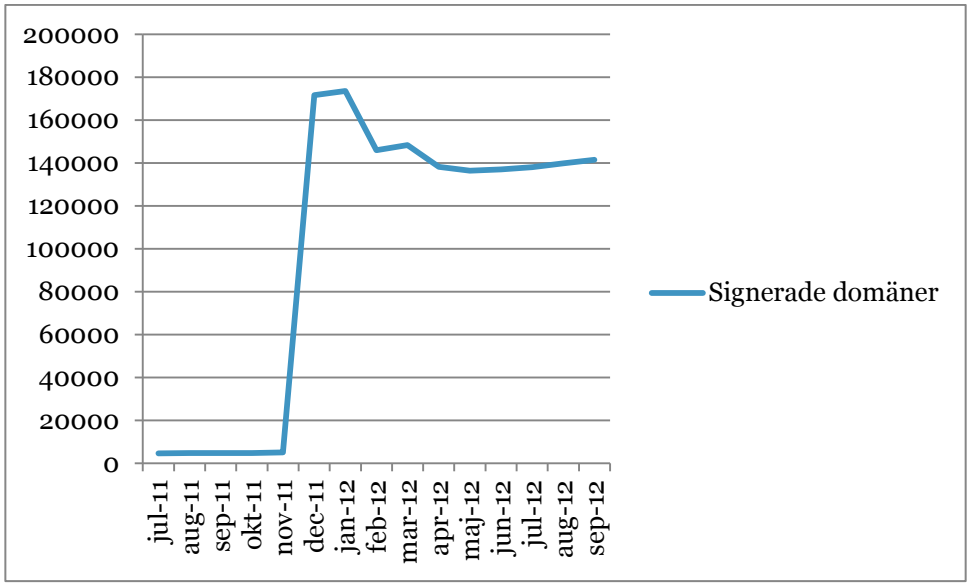
Kontrollgruppen (ett urval av en procent av hela .se-zonen) har vid den nu genomförda mätningen 1 182 signerade domäner, eller 10 procent. Detta ska jämföras med undersökningen 2011 där knappt en halv procent eller totalt 50 domäner av kontrollgruppens drygt 10 000 domäner hade signerats.

Jämfört med rapporten från mars ser vi emellertid en minskning, då en del DNS-operatörer tvingats att slå av DNSSEC på grund av att de stött på problem i den tekniska miljön.

I tabellen på nästa sida redovisas tillväxten för DNSSEC-signerade domäner för hela .se-zonen, alltså inte bara undersöknings- eller jämförelsegruppen.

[8] https://www.iis.se/docs/Halsolaget-DNS-och-DNSSEC1.pdf

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



Den 6 oktober 2011 publicerade Näringsdepartementet ”IT i människans tjänst – En digital agenda för Sverige”[9], med förslag om nytt mål för IT-politiken. I den digitala agendan deklarerar ansvarig minister att:

> *”Sverige ska verka för ett tillgängligt, öppet och robust internet i Sverige och globalt. För att få en säkrare kommunikation för myndigheter behövs underlag till en internetspecifikation som kan användas vid myndigheters upphandling av internetanslutning. Senast 2013 ska det därför finnas en gemensam internetspecifikation med olika robust- och säkerhetskrav (typfall) framtagen för myndigheter. Dessutom bör alla myndigheter senast 2013 använda sig av DNSSEC och vara nåbara med IPv6.”*

.SE har tillsammans med Myndigheten för samhällsskydd och beredskap (MSB), Post- och Telestyrelsen (PTS) och Sveriges Kommuner och Landsting (SKL) bäddat för en möjlighet för kommunerna att via länsstyrelserna ansöka om medel ur anslaget 2:4 Krisberedskap. Kommunerna kunde alltså under hösten 2011 ansöka om pengar. Trots en pressad tidplan inkom ansökningar från 120 kommuner. MSB beviljade medel för 86 av dessa, vilket motsvarar cirka 71 procent av ansökningarna. Ansökningar från 35 kommuner fick avslag i den första ansökningsomgången.

I oktober 2011 hade 24 kommuner signerat sina domäner. I oktober 2012 är antalet 36, en ökning med 12 kommuner. Med tanke på att det är 290 kommuner som ska signeras, innebär det att det med nuvarande tillväxttakt kommer att ta 20 år innan samtliga kommuners domäner är signerade, men förhoppningsvis kommer det att gå fortare med hjälp av de politiska målen och det stöd kommunerna kan få från MSB.

[9] http://www.regeringen.se/sb/d/14216/a/177256

På samma sätt som för IPv6 är det viktigt att ha eller anlita rätt kompetens vid införandet av DNSSEC. Det går att göra fatala misstag om man inte förstår hur det fungerar. Så, om ni inte vet vad ni gör, låt hellre bli tills ni fått kompetent hjälp!

Exempel på sådant som kan hända är att signaturerna i DNSSEC har en viss livslängd och därför måste förnyas regelbundet. Om de inte förnyas i tid så slutar domänen att fungera, vilket betyder att alla resurser som knyts till den domänen i form av till exempel e-post och webb också slutar fungera.

Vi ser exempel på verksamheter som har en livslängd på signaturerna på under en vecka och andra parametrar som ger mycket litet utrymme för att reagera och reparera.

Den egna DNS-miljön blir inte automatiskt stabilare bara för att man inför DNSSEC, därför är det viktigt med övervakning så att man tidigt får reda på när något händer. Det är viktigt att kunna hantera olika typer av avbrott i systemen tämligen snabbt, och exempelvis under semestertid eller långhelger kan felaktigt satta parametrar bli ett problem om man inte har drift som är verksam dygnet runt, alla dagar i veckan, året om.

6.10 DNSSEC-specifika mätningar

Efter en del inkörningsproblem under december-kampanjen tittade vi närmare på hur DNS-operatörerna faktiskt gör när de signerar sina domäner. Framför allt bedömer vi det som viktigt att på ett tidigt stadium få en uppfattning om hur många domäner som inte fungerar. Vi ville också få en indikation och en förvarning om vilka domäner som ligger i riskzonen för att förlora sin tillgänglighet, därför tittade vi också på sådana parametrar i de så kallade barnzonerna (huvuddomäner under .se, som då är förälderzon) som är förknippade med DNSSEC. Det rör sig bland annat om DNSSEC-signaturers livslängd, och hur stor tidsmarginalen är innan de går ut och domänen slutar fungera.

Vårt vanliga verktyg DNSCheck är inte riktigt färdigutvecklat för att hantera dessa värden, varför vi utvecklade ett nytt verktyg som enbart tittar på DNSSEC för signerade domäner.[10] Det är framför allt resultatet från dessa mätningar vi presenterade i DNS och DNSSEC-rapporten från mars 2012. Efter den rapporten har vi upprepat vissa av dessa mätningar till den här rapporten, och resultatet från dessa mätningar redovisas i avsnitt 6.11 nedan.

6.11 Fungerar, fungerar inte

För DNSSEC har vi först tittat på hela .se-zonen, det vill säga samtliga delegerade domäner. Vid den nu aktuella mätningen var 125 647 av 1 177 113 delegerade domäner signerade. (Ungefär 50 000 registrerade domäner saknar delegering (är inte utpekade) i .se-zonen och berörs därför inte av våra mätningar.)

[10] https://github.com/dotse/dnssec-analysis

Det felmeddelande man får när DNSSEC inte fungerar för en domän är SERVFAIL. Det är tyvärr också samma felmeddelande som man får när något på serversidan inte är korrekt konfigurerat, eller om namnserverprogramvaran har andra problem med att hantera frågor. Detta gör det inte alldeles enkelt att avgöra om ett fel beror på DNSSEC eller inte.

Varje domän har ett antal poster knutna till sig i DNS, det är pekare till namnservrar, till e-postservrar och liknande. En viktig post är den som förknippas med DNSSEC och kallas DS-post. DS-posten innehåller DNSSEC-specifik information för en DNSSEC-signerad domän.

Med DNSSEC-signerad domän menar vi här en domän som har en DS-post publicerad i .se-zonen, vilket innebär att zonen måste fungera med DNSSEC påslaget. En DS-post måste matcha en i zonen publicerad DNSSEC-nyckel (DNSKEY), som i sin tur genererar signaturer över alla de poster som är publicerade i zonen.

Av de totalt 125 647 signerade domänerna var det vid mätningen 112 947 som fungerade, resterande 12 700 domäner (8,9 procent) fungerade inte alls när namnservrar med DNSSEC påslaget på resolversidan försökte verifiera signaturerna. Under .SE:s DNSSEC-kampanj i december fanns stora inkörningsproblem, men i stort sett har de värsta problemen rättats till. Dock har den totala andelen DNSSEC-signerade domäner som inte fungerar alls ökat från 6 procent till 8,9 procent i den senaste mätningen.

Eftersom i stort sett alla större Internetoperatörer i Sverige har slagit på DNSSEC-validering så finner vi det lite märkligt att mängden domäner som inte fungerar för kunden faktiskt ökar i antal. Någon rimlig förklaring till detta har vi inte lyckats härleda. .SE arbetar aktivt med att försöka minska den andelen, genom dialog, mätningar och rapporter som denna.

6.12 DNSSEC i andra toppdomäner

Spridningen av DNSSEC har tagit fart bland andra toppdomäner i världen, i synnerhet efter signeringen av rotzonen som skedde 2010. Av de totalt 316 toppdomäner som annonseras i rotzonen är för närvarande 101 signerade med DNSSEC och av dessa har 94 också publicerat information om sina nycklar i rotzonen.

I samband med etablerandet av nya generiska toppdomäner (new gTLD) som ICANN arbetar med kommer antalet att öka eftersom det är ett krav på nya toppdomäner att dessa ska vara signerade med DNSSEC.

Aktuell statistik finns på http://stats.research.icann.org/dns/tld_report/.

7 Viktiga parametrar för e-post

Elektronisk post (e-post) har funnits under mycket lång tid och var en av de första både riktigt använda och användbara applikationerna. Det finns många fördelar med att använda elektronisk post som kommunikationskanal. Som så ofta beror allt på **hur** man gör det. Det är viktigt att bygga upp sina system korrekt från början och att använda funktioner som ökar säkerheten i användningen av e-post. Gör man inte det så kommer man med stor sannolikhet få både problem och kritik från frustrerade mottagare.

I 2012 års undersökning av Hälsoläget i .se har vi tittat på ett fåtal parametrar som berör e-post, dessa redovisas nedan. Vi kommer emellertid att under november publicera en fördjupad rapport om e-post där vi inte bara har genomfört en enkätundersökning bland e-postansvariga, utan också kommer att berätta historik, statistik, förklara hur det bör fungera, och också dyka djupare i en del tekniska parametrar genom mätningar med användning av vårt verktyg MailCheck[11].

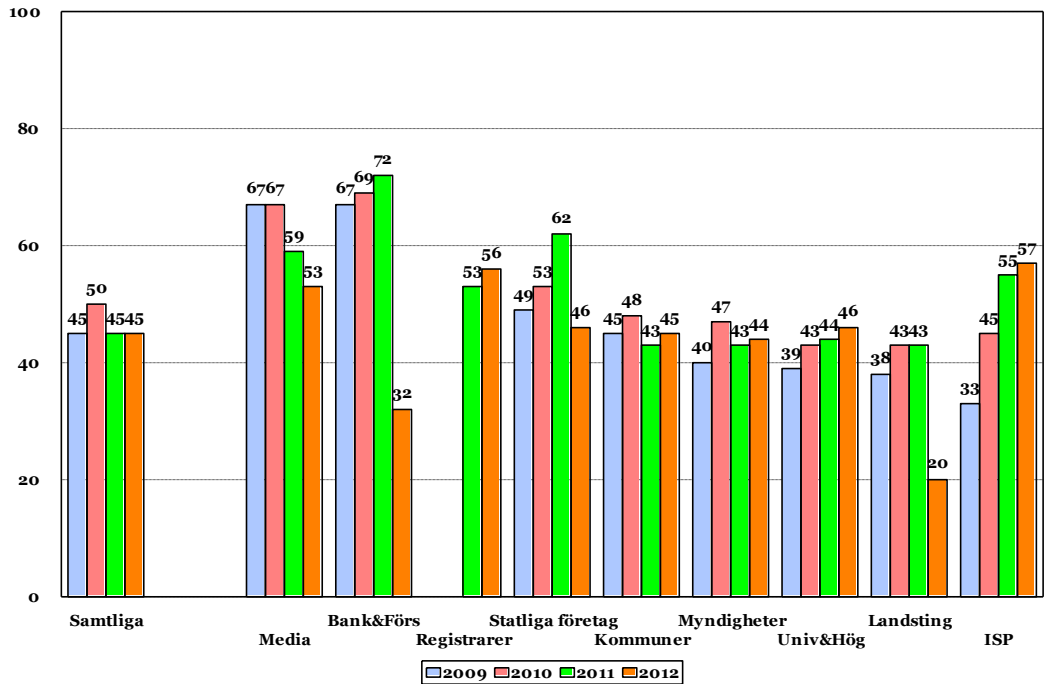
7.1 Stöd för transportskydd (TLS)

För att säkert utbyta information mellan e-postservrar bör kommunikationen skyddas under transport. TLS (akronym för engelskans Transport Layer Security, ungefär transportlagersäkerhet på svenska) är en öppen standard för säkert utbyte av krypterad information mellan datorsystem. TLS är en vidareutveckling av version 3 av SSL-protokollet, och står under IETF:s kontroll. TLS erbjuder förutom konfidentialitet (kryptering) även riktighet (dataintegritet), och beroende på hur det används dessutom äkthetsskydd (källskydd). TLS/SSL kan bland annat användas vid överföring av elektronisk post (SMTP).

Av de undersökta verksamheterna 2012 har endast 45 procent stöd för TLS/SSL i sina e-postservrar. Det är oförändrat från förra året, och det betyder att det i vart fall inte är fler som vidtar tillräckliga åtgärder för att skydda e-posttrafiken från insyn.

[11] https://mailcheck.iis.se/

Tabell 11: E-postservrar med stöd för TLS

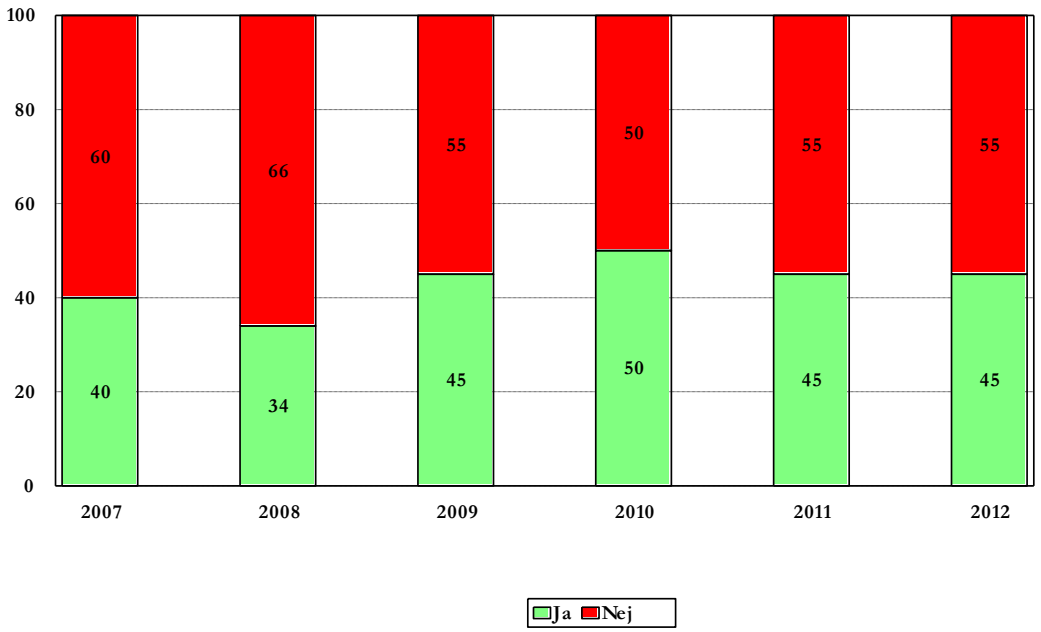


Vi ser alltså en blygsam ökning i de flesta kategorierna, men en relativt kraftig minskning i de båda kategorierna Bank och försäkring samt Landsting. Alla moderna programvaror har inbyggt stöd för det idag, och det är inte svårt att införa.

TLS används för att kryptera kommunikationen mellan två enheter, varav den ena ofta är en webbserver och den andra en webbläsare. Tanken med att skydda den information som utväxlas mellan dessa enheter är att ingen annan på nätverket, till exempel Internet, ska kunna avlyssna eller förvanska informationen. Om du handlar eller förväntas lämna känslig information hos en webbtjänst via Internet så faller det sig naturligt att man använder TLS för att kryptera exempelvis kreditkortsinformation eller personinformation.

Att det har minskat så påfallande mycket sedan denna del av undersökningen påbörjades 2009 i kategorin Media är förstås också särskilt intressant i ljuset av det så viktiga meddelarskyddet, alltså vikten av att skydda uppgiftslämnare som förser journalister med information. Vi har dessvärre inget bra svar på varför det är så. Tabellen nedan visar utvecklingen de sex senaste åren.

Tabell 12: E-postservrar med stöd för TLS 2007-2012

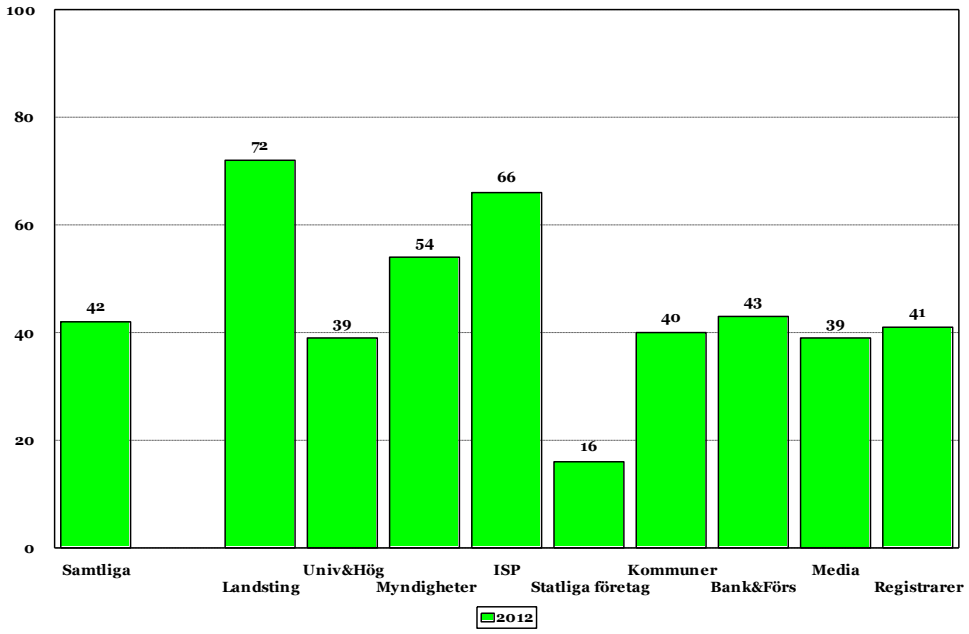


7.2 Placering av e-postservrar

Eftersom vi 2012 har en ännu större andel e-postservrar som använder IPv6-adresser än vi hade 2011, och det inte med någon visshet går att bestämma var dessa står, fortsätter vi att särredovisa resultat för endast de servrar som använder IPv4-adresser.

Tabellen på nästa sida visar procentandelen e-postservrar placerade i Sverige fördelat per kategori.

Tabell 13: Andel e-postservrar placerade i Sverige



Vad vi kan se är det alltså i år 42 procent av de IPv4-adresserade e-postservrarna som är placerade i Sverige mot fjolårets 24 procent, en relativt kraftig ökning. Den absolut största ökningen finns hos landstingen som gått från 5 procent till 72 procent. Vi ser en kraftig ökning hos i princip alla kategorier, förutom i kategorierna Registrarer och Statliga företag.

För kategorin Registrarer är en del av förklaringen till att så många har servrar utanför landets gränser att en stor del av de ackrediterade registrarerna har sin verksamhet i något annat land än Sverige. Registrarer kör också väldigt många e-postservrar eftersom de ofta levererar e-post som en tjänst till kunderna.

Det förefaller som om de statliga företagen haft ett år med outsourcing av hantering av e-post eftersom en mycket mindre andel av e-postservrarna för den kategorin är placerade i Sverige. Förra året var 35 procent av de statliga företagens e-postservrar placerade i Sverige medan resultatet från årets mätning hamnar på 16 procent.

Den huvudsakliga anledningen till placeringen av e-postservrar utanför landet är med största sannolikhet fortfarande densamma som tidigare, det vill säga att verksamheter anlitar någon tredjepartsleverantör för att hantera filtrering av virus och skräppost (spam) för deras räkning.

En konsekvens av att till exempel myndigheters och kommuners e-postservrar är placerade utanför Sverige blir att en hel del av bland annat den offentliga förvaltningens e-postkommunikation passerar ett främmande land på sin väg till mottagaren. I medias fall gäller detsamma för e-postkommunikation mellan uppgiftslämnare och journalister. Med tanke på att kommunikationen också

ofta är oskyddad innebär det en onödig risk för exponering av känslig information.

Sammanfattningsvis kan vi konstatera att det är vanligt förekommande att verksamheter skickar sin e-post utomlands för tvätt. Samtidigt vet vi att det är mindre än hälften av de undersökta verksamheterna som använder kryptering för transportskydd av elektronisk post. Endast 45 procent av de undersökta domänerna har stöd för transportskydd med kryptering för inkommande e-post.

Det innebär att inte bara den svenska utan även utländska underrättelsetjänster utan större svårighet kan avlyssna trafiken. Placeringen av servrar i utlandet medför att all information passerar Sveriges gränser och att främmande stater och andra mycket enkelt kan komma åt information som kan vara känslig på ett eller annat sätt. 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. De vanligaste lösningarna är DomainKeys Identified Mail (DKIM) respektive Sender Policy Framework (SPF) eller en kombination av båda. Båda metoderna bygger på någon form av autentisering av avsändare på server- och domännivå.

7.3.1 DKIM

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

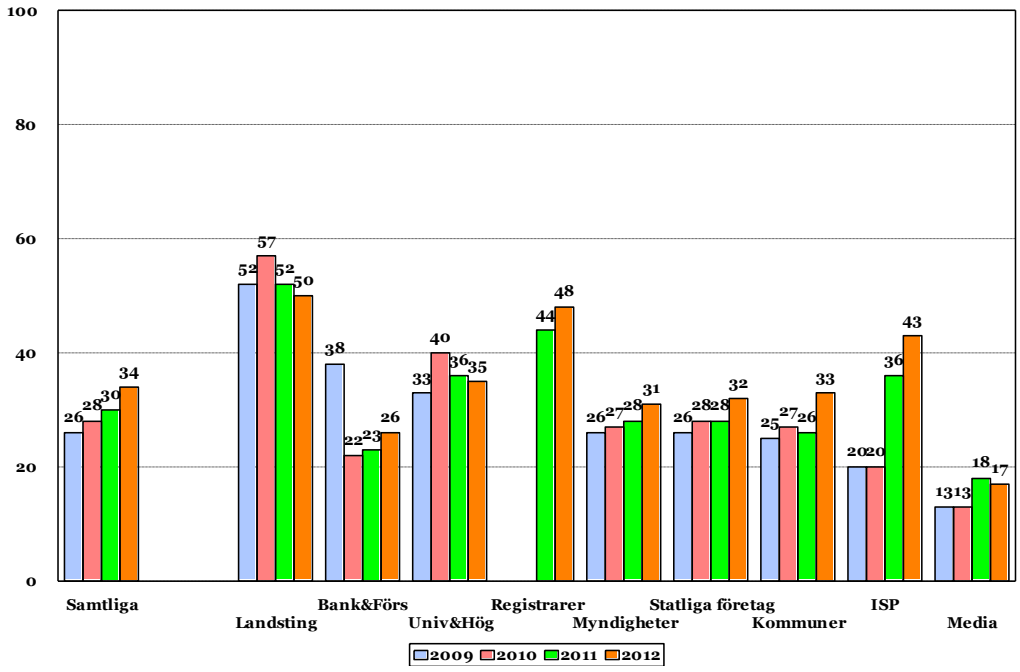
På grund av hur standarden för DKIM är utformad går det dessvärre inte med exakthet att bestämma om en domän använder DKIM eller inte. Vi kan fortfarande inte redovisa resultat om utbredningen av DKIM eftersom det inte säkert går att härleda förekomsten av DKIM för en domän förrän användningen av Author Domain Signing Practices (ADSP) blir mer vanlig. DKIM i sig hjälper inte mot skräppost om man inte kombinerar det med en ADSP-policy. I dagsläget är användningen av ADSP mycket blygsam. Vi kommer inte att redovisa förekomsten av ADSP och DKIM förrän vi har en tillförlitlig mätmetod, och vi ser att det förekommer mer än marginellt. Möjligheten att mäta finns eftersom det är information som publiceras i DNS.

7.3.2 SPF

Den andra lösningen går under benämningen Sender Policy Framework, eller SPF. SPF kan också vara effektivt mot skräppost, så länge som man är medveten om dess begränsningar. SPF klarar exempelvis inte situationer där man har automatisk vidaresändning av e-post eller där ett e-postmeddelande tar andra vägar än den som man tänkt sig. I en struktur med flera nivåer av vidaresändning och SPF-kontroller kan det bli riktigt rörigt.

Det finns kritik mot användningen av SPF, men eftersom det ändå är relativt utbrett väljer vi ändå att titta på om domänen har en SPF-post publicerad eller inte. Vi gör ingen bedömning av innehållet i övrigt.

Tabell 14: Använder SPF



Vi ser i tabellen en fortsatt ökning av användningen av SPF också i årets undersökning från 30 procent 2011 till 34 procent 2012. Användningen i kategorin Landsting fortsätter att minska, från 52 till 50 procent, men de ligger fortfarande i topp, även om kategorin Registrarer närmar sig med 48 procent, en ökning från fjolårets 44 procent. Användningen hos ISP:erna fortsätter att öka relativt kraftigt från 36 till 43 procent. Kategorierna Bank och Försäkring, Myndigheter, Statliga företag och Kommuner ökar samtliga, medan användningen minskar i kategorierna Universitet och högskolor samt Media.

8 Viktiga parametrar för webbtjänster

Idag förmedlar många verksamheter information och tjänster via webbgränssnitt och många verksamheter är helt beroende av att deras webbtjänster fungerar och är tillgängliga för kunder, samarbetspartners och för medborgare i samhället. Med den ökade användningen ställs också högre krav på tillgänglighet och nåbarhet.

Det finns konkreta åtgärder som kan vidtas för att öka redundansen även för webbtjänster. Det kan vara bra att överväga dessa om man har någon typ av kritisk funktion som tillhandahålls via webb och där man kan vänta sig starka reaktioner från användare om det inte fungerar bra. Å andra sidan kanske det är så att webbplatsen inte är en verksamhetskritisk funktion, och att det därmed inte gör något om den skulle vara nere några timmar om året. Oavsett vilket är det viktigt att de åtgärder som vidtas är resultatet av ett balanserat beslut om vilken tillgänglighet och nåbarhet som krävs.

Krav på tillgänglighet är en viktig del som aktualiseras alltmer, inte minst i ljuset av de överbelastningsattacker (DDOS-attacker) som några svenska webbplatser varit utsatta för, nu senast under hösten 2012.

8.1 Anslutning av webbservrar till Internet

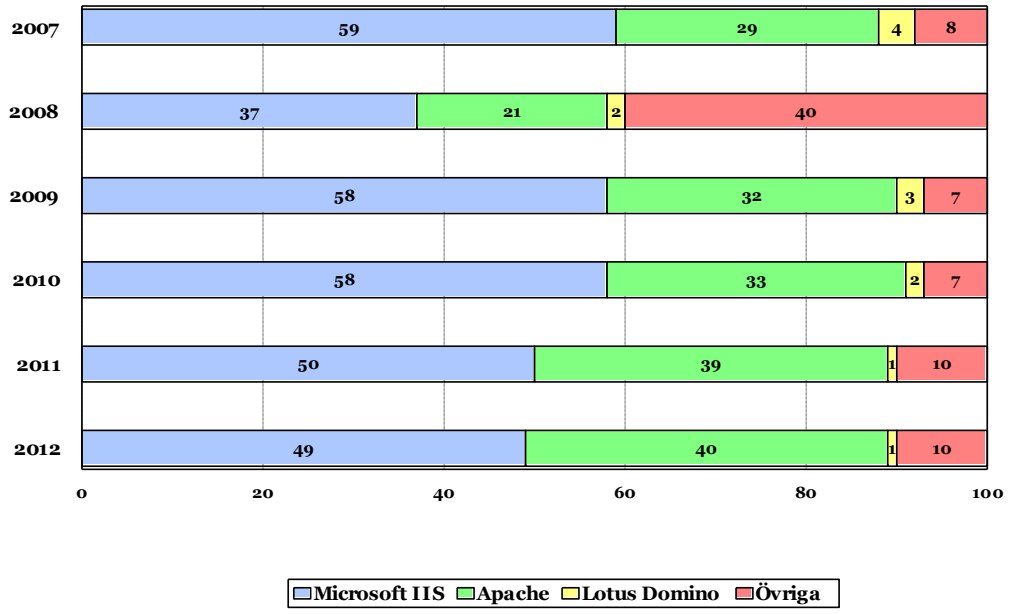
Om man i sin verksamhet har alla namnservrar anslutna till en och samma Internetoperatör och därtill ansluter även webbservern till samma operatör, då får man stora problem den dagen operatören får problem med tillgängligheten.

Då drabbas inte bara namnservrarna utan också webbservrarna, systemen blir helt enkelt onåbara. I en verksamhet bör man därför ha minst ytterligare en namnserver placerad hos en annan operatör, och man kan också överväga att placera en reservwebbplats någonstans för att uppnå största möjliga redundans.

8.2 Programvaror för webbservrar

Vi fortsätter att hålla ett öga på vilka programvaror för webbservrar som används i de undersökta verksamheterna. De klart dominerande är fortfarande Microsoft Internet Information Server (Microsoft IIS) och Apache. Här ser vi mycket små förändringar från föregående år.

Tabell 15: Programvaror som används för webbservrar



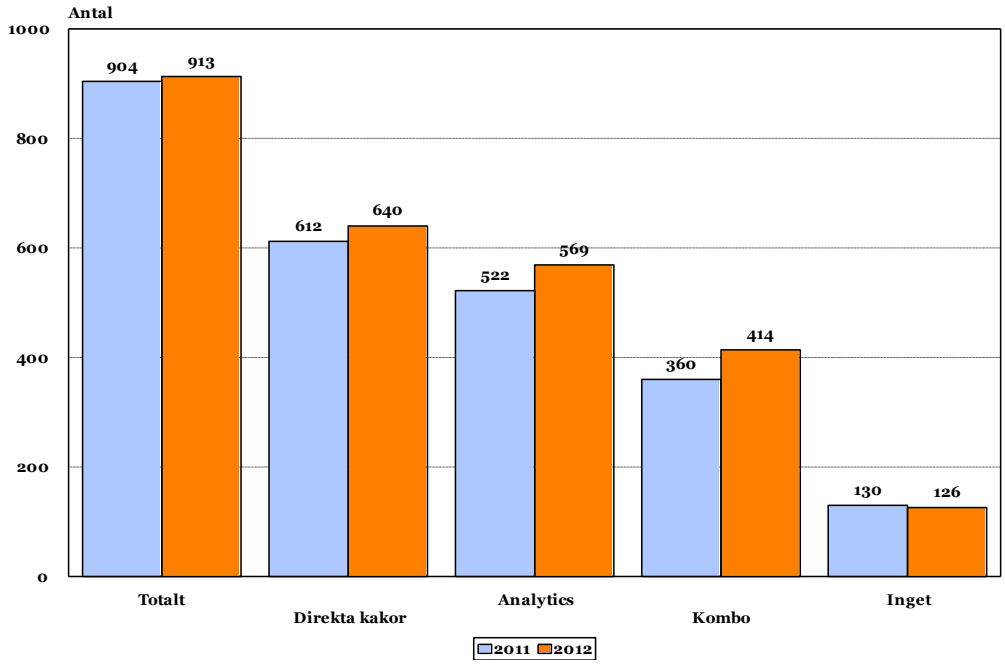
8.3 Andra intressanta iakttagelser kring webb

För andra året i följd kontrollerar vi en del andra parametrar som är av speciellt intresse för webbapplikationer. I årets undersökning har vi medvetet hoppat över fördjupningen kring SSL-certifikat och deras användning. Avsikten är att vi under nästa år ska genomföra en fördjupad studie av just det området.

8.3.1 Kakor

Den 1 juli 2011 förändrades lagen om elektronisk kommunikation (2003:389). En följd av denna ändring är att alla som besöker en webbplats aktivt kan behöva samtycka till att webbplatsen använder så kallade kakor (cookies).

Tabell 16: Användning av kakor



Tabellen redovisar antal domäner som sätter kakor av olika kategorier. Kategorin Direkta kakor är sådana där webbplatsen själv sätter kakor. Kategorin Analytics är de webbplatser som använder Google Analytics och därmed sätter tredjepartskakor. Kombo betyder att webbplatsen använder både Google Analytics och direkta kakor. Kategorin Inget betyder att man varken använder Google Analytics eller direkta kakor, men där det ändå kan finnas tredjepartsresurser som sätter kakor.

Användningen av kakor ser alltså trots den nya regleringen ut att öka. Av undersökningsgruppens 913 domäner satte 640 eller 70 procent direkta kakor på sina webbplatser, vilket är en ökning med tre procent från förra året.

En stor andel (62 procent) av de webbplatser som undersökts i år använder Google Analytics och sätter därmed tredjepartskakor för insamling av besöksstatistik, vilket är en ökning från förra årets 57 procent. Det är viktigt att veta att Google Analytics sätter kakor oavsett vilken kakpolicy som finns i verksamheten, utan att fråga först.

45 procent använder dessutom en kombination av både Google Analytics och direkta kakor.

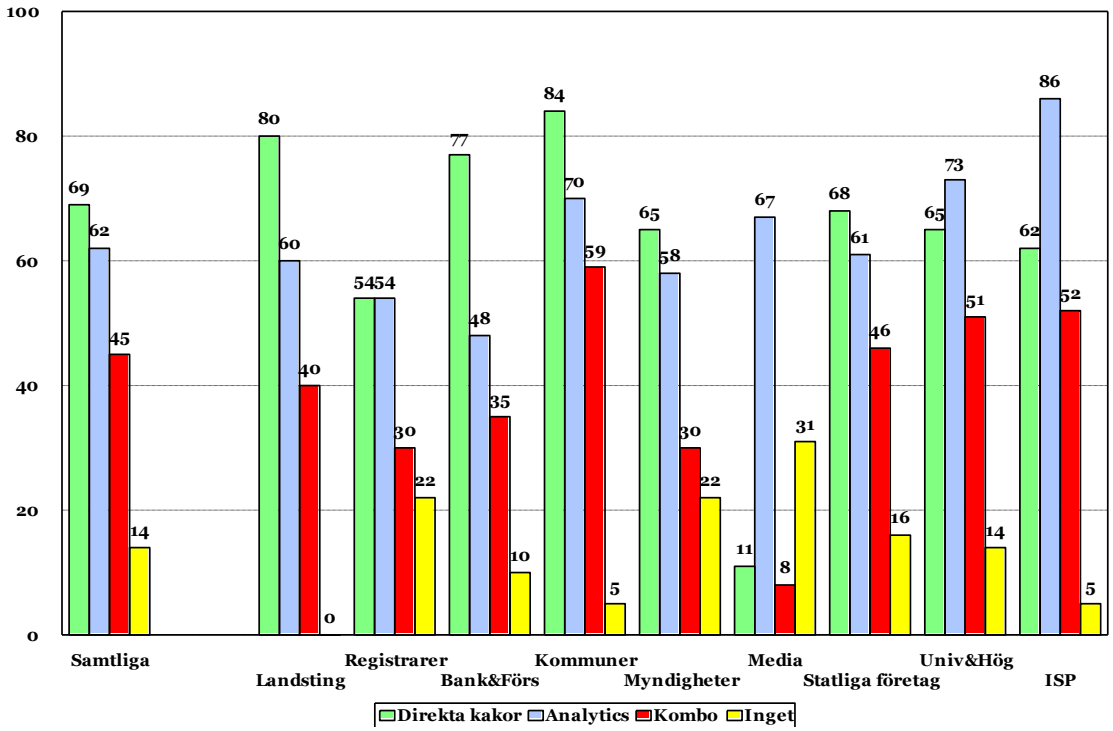
Av tabellen på nästa sida framgår att det skett en mycket kraftig ökning av användningen av kakor inom kategorierna Kommuner och Myndigheter.

Tabell 17: Skillnad i användning av någon typ av kakor 2011 respektive 2012.

Kategori	2011	2012	Ökning/minskning
Bank & Försäkring	140	137	-3
ISP	40	43	+3
Kommuner	578	632	+54
Landsting	32	36	+4
Media	36	42	+6
Myndigheter	388	429	+41
Registrarer	242	241	-1
Statliga företag	108	109	+1
Universitet & Högskola	79	75	-4

Tabellen nedan redovisar hur kakor fördelar sig per typ och mellan de olika kategorierna.

Tabell 18: Kakor per typ och kategori 2012



Den vanligaste formen av kakor är så kallade direkta kakor, men Google Analytics används frekvent inom samtliga kategorier i undersökningsgruppen. Bland kategorierna Landsting och Kommuner sätter mer än 80 procent direkta kakor, men man är också flitig användare av Google Analytics. ISP:erna är de som använder Google Analytics mest, med hela 86 procent.

8.3.2 Uppdrag om uppföljning av kaklagen

I oktober 2011 gav regeringen ett uppdrag till PTS som i korthet går ut på att ta reda på om kaklagen har försämrat tillväxten på eller tilliten till Internet. Uppdraget ska redovisas i en rapport som ska redovisas i slutet av 2012. Om det kommer att innebära några ändringar i den svenska lagstiftningen, som är resultatet av ett EU-direktiv, är för tidigt att säga.

Som ett led i uppdraget har PTS genomfört enkät- och intervjuundersökningar bland ett urval svenska verksamheter, både inom den privata och offentliga sektorn. Preliminära resultat visar att de som deltagit i undersökningen i vart fall känner till att regleringen existerar.

Många av de tillfrågade anser att lagens krav på samtycke riskerar att försvåra deras arbete med att göra webbplatsen användarvänlig och därmed försämra användarupplevelsen. Det finns också en oro för att användaren inte ska förstå vad det är de samtycker till. Flera av de tillfrågade anser att lagen är verklighetsfrånvänd och pekar på att webbsajter idag är beroende av kakor för att de ska fungera. Samtidigt förstår man tanken bakom lagstiftningen och betraktar syftet som gott. I praktiken är det dock svårt att följa lagen eftersom det de facto sätts en kaka så fort man går in på en webbplats, för att kunna be om samtycke.

8.3.3 Google Analytics för 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 till exempel SIS-Index.

Att dela med sig av sina besöksdata till Google Analytics innebär också att man låter Google dra egna slutsatser av besöksströmmarna till exempelvis svenska myndigheters webbplatser. Det kan inte heller 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.

I augusti 2012 hävdade den norska motsvarigheten till Datainspektionen, Dataskyddsmyndigheten, att de myndigheter som använder Google Analytics bryter mot den norska integritetslagstiftningen[12]. Enligt Dataskyddsmyndigheten består integritetsbrottet i att man förlorar kontrollen över hur Google använder informationen om sina användare. Google Analytics samlar in ip-adresser och information om besökarnas beteende på en sajt. Dataskyddsmyndigheten var orolig för att data kan spåras och analyseras ned på individnivå. Den svenska Datainspektionen har emellertid inte resonerat på samma sätt eller dragit samma slutsats, i alla fall inte än.

[12] http://computersweden.idg.se/2.2683/1.461378/olagligt-anvanda-google-analytics

8.4 Stöd för transportskydd (TLS/SSL)

TLS/SSL är den teknik som skyddar trafik mot avlyssning vid användning av webben, och som gör att en användare kan lita på att han eller hon pratar med rätt organisation när de exempelvis vill utföra bankärenden på Internet. En utförligare beskrivning finns i avsnitt 7.1.

Med hjälp av certifikat och tillhörande krypteringsnycklar kan en webbläsare upprätta en säker, krypterad förbindelse för kommunikation med webbservern. Precis som för e-post används TLS/SSL för upprättandet av en säker förbindelse mellan två parter, i det här fallet en webbläsare och en webbplats (https), se bilaga 9.

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

Några anledningar till varför ett certifikat ibland inte är att lita på är om:

- Certifikatet används innan det har blivit giltigt.
- Certifikatet används efter det att giltighetstiden har gått ut.
- Domänen som certifikatet är utfärdat för inte motsvarar domänen för sajten.
- Certifikatet har revokerats (spärrats).
- Certifikatet är självsignerat.
- Utfärdaren inte är en välkänd CA.
- Certifikatutfärdaren inte bedöms vara pålitlig.
- Certifikatskedjan inte är komplett.

Att mäta förekomsten och kvaliteten på certifikat är inte helt enkelt, och vi söker oss fram på lite olika vägar för att hitta en bra mätmetod. Det innebär att vi i år inte har gjort någon körning där vi tittat specifikt på certifikat och deras kvalitet. Däremot planerar vi att göra en sådan granskning nästa år.

I våra tidigare undersökningar har resultaten visat att hanteringen av certifikat i undersökningsgruppens webbmiljö håller mycket dålig kvalitet i alla avseenden som undersökningen visar. Denna typ av kryptoanvändning har ändå funnits länge och är tämligen vanlig. Hos de organisationer som ingår i undersökningen bör man kunna förvänta sig bättre resultat, framför allt att de ska ha giltiga, aktuella certifikat utgivna av trovärdiga utgivare. Vad vi vill få sagt med det är att en bristfällig användning av webbcertifikat undergräver trovärdigheten för 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 jag vill fortsätta ändå”, såsom självsignerade certifikat eller certifikat vars giltighetstid har gått ut gör att det inarbetas dålig säkerhetskultur hos Internetanvändare vilket motverkar själva

grundidén med servercertifikat – nämligen att med rimlig säkerhet 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 och liknande 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 bland annat bevakning av när certifikat går ut och ska förnyas.

Därför ska man tänka på att:

- Behandla verksamhetens certifikat som tillgångar och föra en förteckning över vilka certifikat som används och till vad.
- Använda EV-certifikat[13] där det är befogat.
- Undvika wildcard-certifikat[14] 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 https://www.ssllabs.com kan den som använder certifikat för att skydda webbtjänster lära sig mer om hur det fungerar och dessutom själv testa om webbplatsen har bra säkerhet med avseende på SSL.

8.4.1 Attacker mot SSL

Under fjolåret skedde flera mycket allvarliga attacker mot flera stora certifikatutfärdare, och det kan finnas anledning att fundera över hur mycket det går att lita på SSL-systemet, och vad som kan göras åt de problem som finns.

Här pratar vi om vanlig traditionell säkerhet. Hanteringen hos de CA som har drabbats av de attacker som skett under åren har i allra högsta grad varierat, och vissa av de drabbade certifikatsutfärdarna har agerat både långsamt och bristfälligt när det gäller information till sina kunder och omvärlden. De har helt enkelt visat prov på bristande krishantering.

Vi vill i sammanhanget också påminna om att certifikatsvarningar inte ska ignoreras utan tas under allvarligt övervägande. Det är viktigt att hålla utkik efter https-förbindelsen och försöka förvissa sig om att det är en äkta sådan. Vi rekommenderar även att man lär sig mer om hur man tar sig en extra titt på certifikatet för att värdera äktheten.

Webbläsarleverantörer som Google, Mozilla, Microsoft med flera har efter de senaste händelserna skärpt kraven för utfärdare att komma med i listan över betrodda rotcertifikat som följer med varje webbläsare.

[13] Certifikat med utökad validering (EV = Extended Validation).
[14] Ett wildcard-certifikat aktiverar SSL-kryptering på flera underdomäner med hjälp av ett enda certifikat.

8.4.2 Åtgärder för att motverka attacker mot SSL

Det är många som funderar på lösningar, och ett av de mest intressanta initiativen är för närvarande det som gjorts inom IETF-arbetsgruppen DNS-based Authentication of Named Entities (DANE), vars resultat nyligen blivit färdig standard och publicerats som Transport Layer Security (TLS) Protocol: TLSA, RFC 6698[15].

Med TLSA lagras certifikat i DNS, så att det går att verifiera dem. Tilliten går till DNS med användning av DNSSEC. Tillvägagångssättet kompletterar certifikatutfärdarens signaturer genom att verifiering av certifikatet också sker genom DNS. Det bidrar till att styrka kvaliteten på certifikatet och därmed öka tilliten. Det gör också att man skulle kunna hoppa över de traditionella certifikatutfärdarna och bara lita på DNS i de fall man endast önskar verifiera domännamnet och inte vilken juridisk person som står bakom en tjänst.

En annan förhållandevis vanlig typ av attacker mot webbplatser som använder SSL är olika typer av nedgraderingsattacker. Det innebär att man helt enkelt får användaren att använda ett enklare krypto, eller inget krypto alls för att kommunicera med webbplatsen. Då behöver man inte ens ett för webbplatsen giltigt certifikat för att effektivt kunna genomföra en så kallad man in the middle-attack. Inom IETF jobbar man med utvecklingen av HTTP Strict Transport Security (HSTS), som innebär att webbläsaren tvingas att köra SSL mot webbplatsen, oavsett vad som sägs i övrigt. HSTS fungerar så att den kommer ihåg om en sajt som har besökts tidigare har använt SSL och tvingar upp kommunikationen på samma nivå vid ett återbesök.

Webbläsaren Chrome innehåller många utökningar, bland annat *certificate pinning*[16] som var det som avslöjade en av CA-attackerna, den mot DigiNotar. Andra utökningar i Chrome är *HTTPS-preloading*[17] som innebär att sajter är inkompilerade för att alltid använda SSL.

Det finns även plugin till Mozilla Firefox och andra webbläsare för bättre certifikatshantering, som till exempel *HTTPSEverywhere*[18] som utvecklats gemensamt av Electronic Frontier Foundation (EFF) och Tor-projektet.

[15] http://tools.ietf.org/html/rfc6698
[16] http://www.imperialviolet.org/2011/05/04/pinning.html
[17] http://dev.chromium.org/sts
[18] https://www.eff.org/https-everywhere

9 Jämförelse med .se-zonen

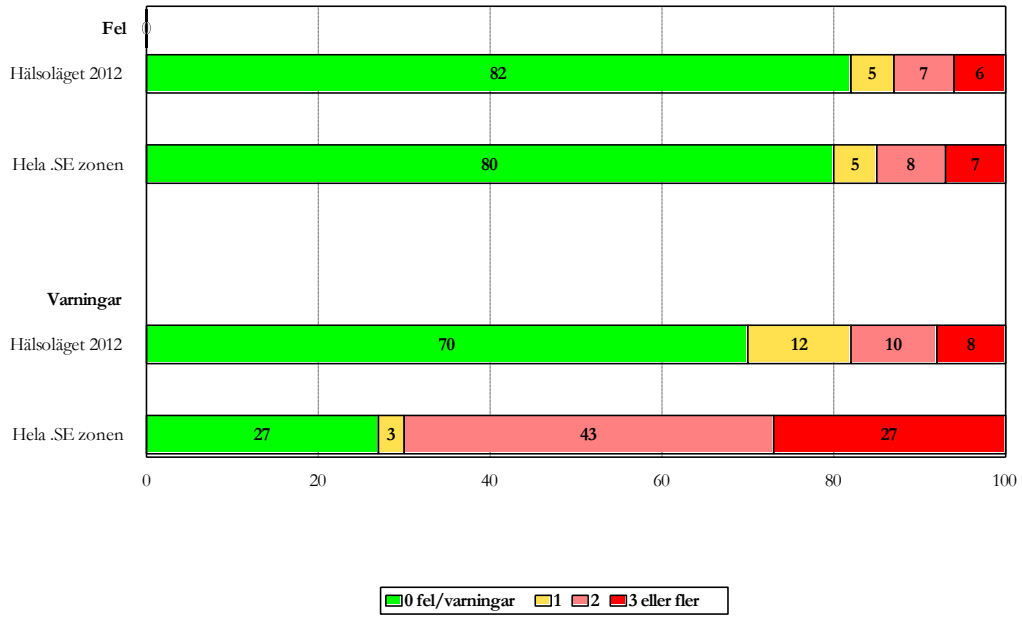
För att se om vår undersökningsgrupp är i bättre eller sämre skick än .se-zonen som helhet har vi även i årets undersökning gjort ett utsnitt av en procent slumpmässigt valda domäner ur .se-zonen för att ha som jämförelse.

I tabellerna nedan representerar ”Samtliga” den aktuella undersökningsgruppen med sina 913 domäner medan ”Hela .se-zonen” representerar det slumpmässiga urvalet på en procent eller 11 806 domäner ur en version av zonfilen från den 2 oktober 2012.

9.1 Fördelning av fel och varningar

Vi tittar som tidigare först och främst på fördelningen av fel och varningar, och hur undersökningsgruppen Samtliga - som ändå innehåller en hel del kritiska funktioner och verksamheter - förhåller sig till jämförelsegruppen Hela .se-zonen.

Tabell 19: Andel fel och varningar



I år är det till skillnad från 2011 färre fel i vår undersökningsgrupp än i jämförelsegruppen för .se-zonen som helhet, alltså en något annorlunda situation än tidigare år. Andelen varningar är som synes långt färre i vår undersökningsgrupp än i jämförelsegruppen. I hela .SE-zonen är det endast 27 procent som inte får någon form av varning.

En del av orsaken till detta står att finna i felkonfigurerade namnservrar för DNS men en del också i det faktum att allt fler använder olika typer av filtreringsfunktioner för att detektera skräppost.

En metod för filtrering är att använda DNS-baserade svartlistor för att ta reda på om den avsändande IP-adressen sedan tidigare finns listad som avsändare av skräppost eller är känd som en infekterad dator. Så vad vi ser här är effekten av att vi går ut och försöker skicka e-post till nästan 12 000 domäner. Just den delen av resultaten är alltså inte helt tillförlitliga och går inte att dra några säkra slutsatser från, mer än just den att det blir allt vanligare med filtrering av det här slaget.

Vi kommer senare i år att publicera en rapport som enbart behandlar e-post och hur man behöver sätta upp det för att det ska fungera bra för alla, både avsändare, leverantör och mottagare. I den undersökningen har vi använt oss av en metod där vi inte lika enkelt blir svartlistade.

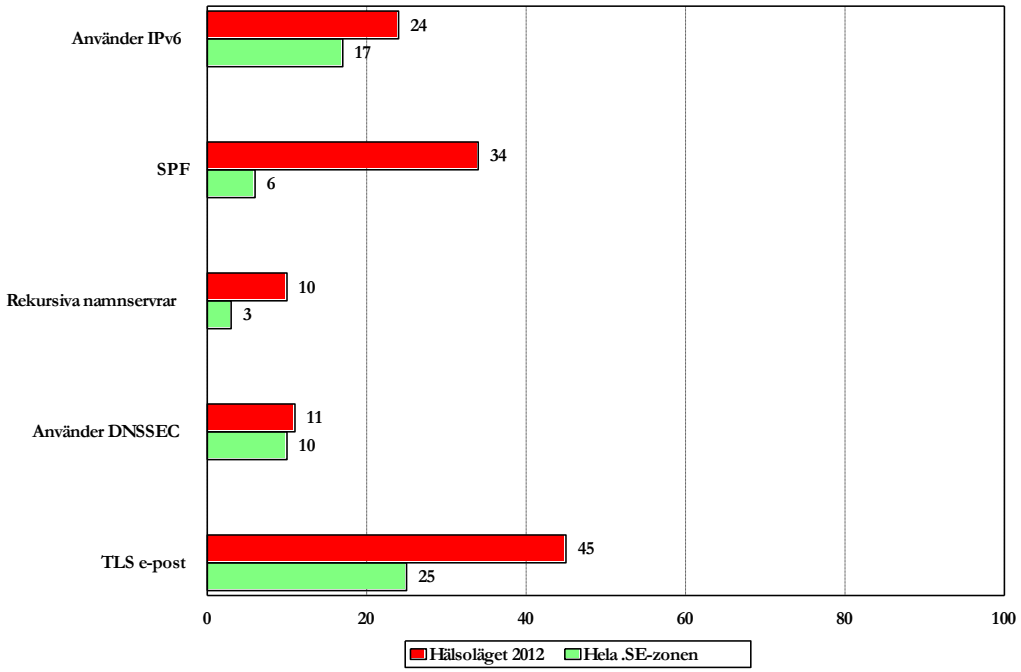
9.2 Skillnader mellan undersökningsgruppen och jämförelsegruppen

De stora skillnaderna när vi tittar närmare på de specifika områden vi har granskat för de parametrar som vi förknippar med DNS-kvalitet enligt definitionen i bilaga 4 gäller fler felaktiga utpekningar, eller delegeringar, i jämförelsegruppen för se-zonen som helhet än i undersökningsgruppen och fler som är beroende av endast en namnserver. Samtidigt är det fler i undersökningsgruppen som har öppna rekursiva namnservrar (10 procent mot 3 i jämförelsegruppen).

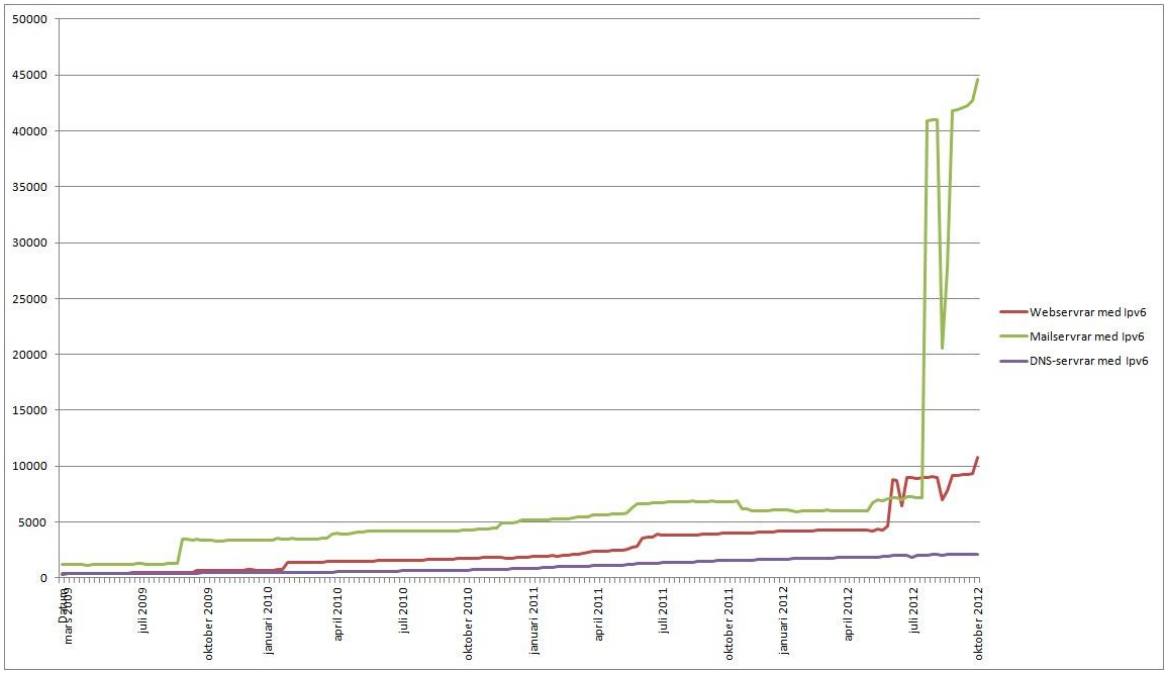
I år är det ännu fler som har infört IPv6 i båda grupperna (24 procent i undersökningsgruppen och 17 procent i jämförelsegruppen), det är långt fler som använder DNSSEC (11 procent i undersökningsgruppen och 10 procent i jämförelsegruppen för .se-zonen som helhet) och fler som skyddar sin e-post med TLS (45 procent i undersökningsgruppen och 25 procent i jämförelsegruppen för .se-zonen som helhet). SPF används också mycket oftare i undersökningsgruppen (34 procent) än i jämförelsegruppen (6 procent).

I nedanstående tabell ser vi skillnaderna mellan undersökningsgruppen och jämförelsegruppen för .se-zonen som helhet för de olika delar som vi har studerat. Generellt finns det alltså mer av allt som kan uppfattas som positivt i undersökningsgruppen än i jämförelsegruppen, men också av det som är mindre bra, som till exempel öppna rekursiva namnservrar.

Tabell 20: Jämförelse mellan undersökningsgruppen och .se-zonen



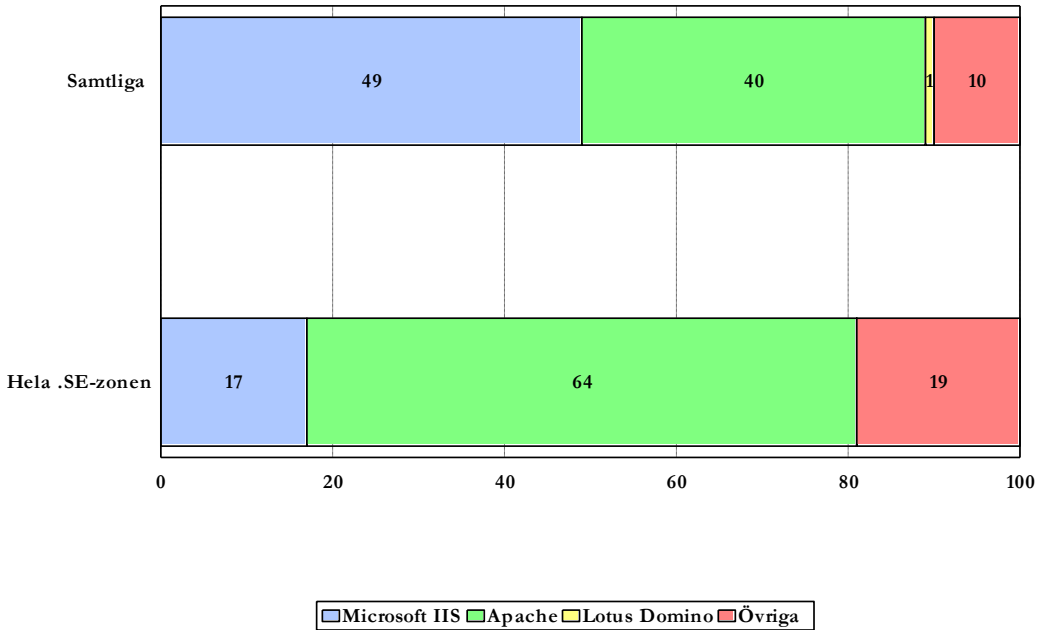
Hur stor den faktiska tillväxten på IPv6 är i hela .se-zonen framgår av nedanstående bild:



9.3 Skillnader i användning av programvaror för webbservrar

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 kvarstår fortfarande. Microsoft IIS fortsätter att tappa något till förmån för Apache och övriga programvaror, men skillnaderna är mycket små. Lotus Domino har minskat ytterligare och försvunnit från kartan.

Tabell 21: Programvaror för webbservrar

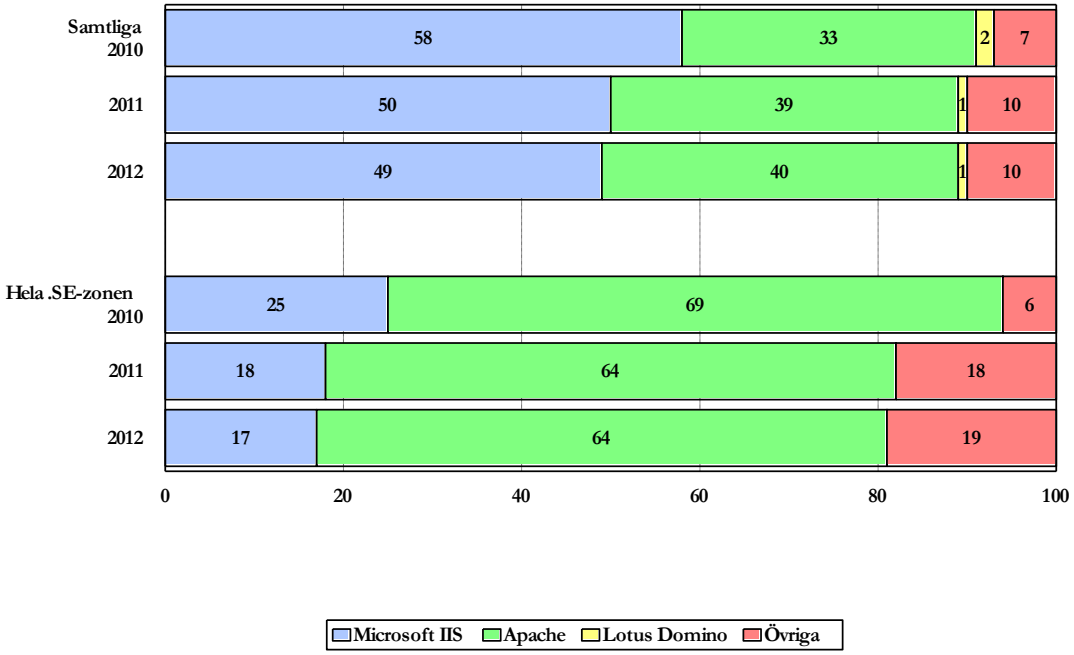


I tabell 22 gör vi samma jämförelse men för åren 2010-2012. Där kan vi konstatera att Microsoft IIS har tappat mark både inom undersökningsgruppen och jämförelsegruppen. Den har emellertid fortfarande ett mycket starkt fäste i undersökningsgruppen.

Kategorin Övriga har ökat än mer för jämförelsegruppen och är i år tre gånger så stor som vid förra undersökningen. Det tyder på att det finns andra programvaror som också vinner i popularitet.

En förklaring till Microsoft IIS starka dominans i undersökningsgruppen står förmodligen att finna i systemet med offentlig upphandling och ramavtal vilken bidrar till en homogenisering av den offentliga förvaltningens IT-miljöer som kanske inte alltid är optimal.

Tabell 22: Programvaror för webbservrar – förändring över tiden



10 Råd och rekommendationer

Efter att ha genomfört ännu en omgång mätningar med ett relativt positivt resultat jämfört med 2011 ser vi trots allt fortfarande ett starkt behov av större samordning mellan olika intressenter för bättre säkerhet och nåbarhet på den svenska delen av Internet och inte minst ser vi möjligheter till stora effektivitetsvinster och kostnadsbesparingar. Där hyser vi en förhoppning om att regeringens digitala agenda kan ha en positiv effekt på utvecklingen.

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. Leverantörer som erbjuder sådana tjänster med god kvalitet är en bristvara. 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.

- Inför gemensamt upphandlade funktioner 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 ställa relevanta och enhetliga krav på transportskydd och kryptering.

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

- Ställa 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 ett systematiskt införande av 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. Helst bör det finnas en svensk sådan aktör.

- Införa DNSSEC på alla domäner i den offentliga förvaltningen.

Utöver ovanstående åtgärder finns det ytterligare åtgärder som behöver vidtas bland annat på operatörsnivå för att stärka infrastrukturen för Internet. Dessa åtgärder landar huvudsakligen på Post- och Telestyrelsen, PTS, som är den myndighet som är tillsynsansvarig för bland annat lagen om elektronisk kommunikation, och här handlar det om att formulera krav som bör ställas på operatörer.

I det sammanhanget ser vi särskilt positivt på det förslag som ligger i regeringens digitala agenda för Sverige, att det för att få en säkrare kommunikation för myndigheter behövs underlag till en Internetspecifikation som kan användas vid myndigheters upphandling av Internetanslutning.

Regeringen har föreslagit att det senast 2013 ska finnas en gemensam internetspecifikation med olika robust- och säkerhetskrav (typfall) framtagen för myndigheter. Vidare har regeringen föreslagit att alla myndigheter senast 2013 bör använda sig av DNSSEC och vara nåbara med IPv6.

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.
DANE	Arbetsgrupp inom IETF. DNS-based Authentication of Named Entities.
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 (till exempel iis.se) till IP-adress vilken används för kommunikation över IP-nät som till exempel 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 domännamnssystemet lägre placerad domän står före en högre placerad domän. Ett registrerat *domännamn* är ett *domännamn* som har tilldelats en viss *innehavare*.
DS-post	En posttyp i DNS som innehåller DNSSEC-specifik information för en DNSSEC-signerad domän.
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. Förekommer som IPv4-adresser och IPv6-adresser.
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.

Registrar Ackrediterad återförsäljare av .SE-domäner.

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.

TLSA The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA

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 och robust 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 gör vi den för sjätte gången. Undersökningen ingår i ett långsiktigt projekt som från nästa år kommer att gå under namnet Internets ekosystem och omfatta fler områden och mätningar.

.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 snart 30 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 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). DNSSEC bygger på kryptografiska nycklar som används för signering av innehållet i zonfilerna. Genom validering av signaturer av svaren på DNS-frågor går det att säkerställa att dessa 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 de viktigaste skälen till varför vi fokuserar våra tester på just kvalitet i DNS.

Att Internets så kallade rotzon signerades sommaren 2010 satte mer fart på spridningen av DNSSEC. Eftersom rotzonen är toppen av DNS-hierarkin är det därmed enklare för de underliggande toppdomänerna att införa DNSSEC.

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 uppkopplad enhet på Internet, består i IPv4-versionen 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. De sista IPv4-adresserna delades ut under 2010.

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. 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 50 000 000 000 000 000 000 000 000 000 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 till exempel Sakernas Internet och intelligenta hem.

Av dessa och andra anledningar är det mer eller mindre akut att införa IPv6. Därför tittar vi också närmare på den aktuella utbredningen av IPv6i Sverige.

Regeringen med IT-ministern Anna-Karin Hatt i spetsen försöker föregå med gott exempel genom att i regeringens digitala agenda föreslå att IPv6 bör införas på alla svenska myndigheter före 2013. Men den privata delen av samhället har ännu inte hakat på.

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 mätverktygen 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 ett av de senare tillskotten som har utvecklats. Mailcheck syftar till att förbättra kvaliteten på e-postrelaterade tjänster generellt genom att peka ut möjliga konfigurationsproblem, svagheter i programvaror eller avvikelser från standarder för både systemadministratörer och slutanvändare.

Bilaga 3 - Om testverktyget DNSCheck

Som motor för genomförandet av undersökningen och insamlingen av data har vi använt programvaran för .SE:s tjänst DNSCheck. DNSCheck är ett program designat för att hjälpa Internetanvändare 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 bland annat detta verktyg finns att hämta på http://github.com/dotse/.

Vårt vanliga verktyg DNSCheck är inte riktigt färdigutvecklat för att hantera dessa värden, varför vi utvecklade ett nytt verktyg som enbart tittar på DNSSEC för signerade domäner. Det verktyget finns att hämta på https://github.com/dotse/dnssec-analysis.

Andra verktyg som används är Page Analyzer och Whatweb. Page Analyzer mäter prestanda och prestandapåverkande parametrar som antalet externa resurser, och resursernas storlekar. Whatweb analyserar webbtekniken. Ett specialutvecklat verktyg används också för mätningar av DNSSEC-relaterade parametrar.

En fullständig körning av både undersökningsgruppen och kontrollgruppen tar omkring ett dygn att genomföra. För dataanalysen använder vi sedan ett egenutvecklat gränssnitt som hämtar data från databasen och sammanställer dessa för de grupper som väljs och enligt de parametrar som bestämts. Vi kan också få en vy med resultat från flera olika mätningar samtidigt för att snabbt kunna se skillnader och trender.

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.

Verktyget DNSCheck kan även 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 för den som till exempel tänker flytta en domän från en namnserveroperatör 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 (till exempel ”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 DNSSEC allt mer aktuellt med åren.

Många andra Internetprotokoll är beroende av DNS, men DNS-information i resolvrarna har kommit att bli så sårbar för attacker att den inte längre går att lita på. Den ökade säkerhet som DNSSEC tillför gör att många attacker inte längre får någon effekt.

Några av de mest kända och största hoten mot DNS är cacheförgiftning (cache poisoning) och farmning (pharming).

Cacheförgiftning 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 mest välkända exemplen på detta är den under 2008 mycket uppmärksammade Kaminskybuggen.

Farmning 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.

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 DNSSEC till våra domäninnehavare. Vi har för närvarande ett trettiotal återförsäljare (registrarer) som erbjuder DNSSEC.

Det är inte bara en tillfällighet att en av .SE:s medarbetare har valts till Trusted Community Representative (TCR) för att som Crypto Officer (CO) delta i de nyckelceremonier som genomförs för rotzonen fyra gånger per år, två gånger på den sajt som ligger på den amerikanska västkusten och två gånger på motsvarande sajt på den amerikanska östkusten.

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 hjälp av kryptografiska metoder som använder elektroniska signaturer. DNSSEC innebär att användaren, när han gör en uppslagning i DNS, genom validering av signaturer ska kunna avgöra 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 och inte någon 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 nätfiske (phishing, sidor som liknar eller är identiska med originalet för att lura till sig lösenord och personuppgifter) som farmning (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, det vi säga 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 genom att .SE publicerar sina DNSSEC-nycklar i rotzonen är det numera 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 sina respektive underliggande domäner. Med roten signerad behöver resolveroperatören 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 https://www.iis.se/domaner/dnssec/kaminskybuggen

Där finns det bland annat länkar till en film som demonstrerar hur en attack går till och möjlighet att testa om den resolver som används är sårbar för Kaminskybuggen.

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

En uppdatering sker också av RFC-draft-4641-bis som också tar sikte på det praktiska införandet. Den är under diskussion inom IETF.

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.

Internet Society (ISOC) gör också sitt bästa för att driva på utvecklingen av DNSSEC. På http://www.internetsociety.org/deploy360/dnssec/ samlar den mycket nyttig och användbar information.

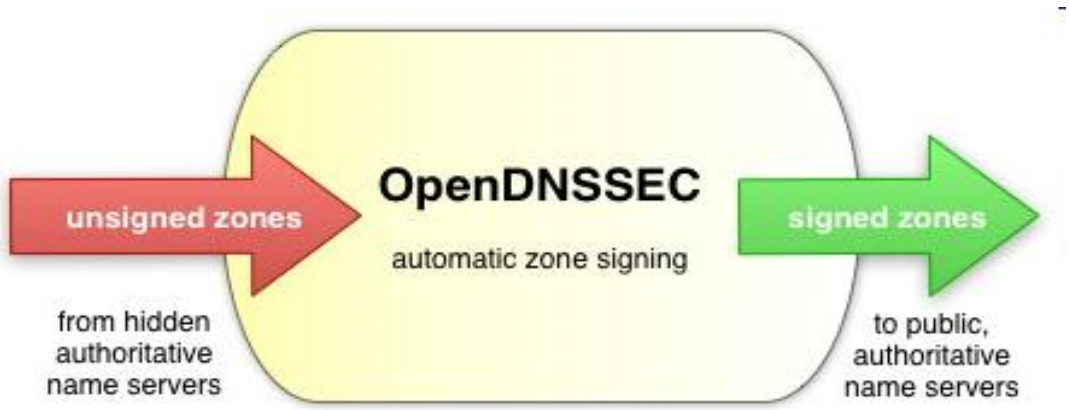
OpenDNSSEC

DNS är relativt komplicerat, och så är 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 signerar 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 ett särskilt bolag som ägs av .SE (Stiftelsen för Internetinfrastruktur).

Programvaran OpenDNSSEC är resultatet av ett samarbete mellan utvecklare från .SE, Nominet, NLNet Labs, SIDN, SURFnet, Kirei AB och Sinodun. 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 försöker 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 (en så kallad 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 skulle öppna rekursiva resolvrar kanske inte betraktas som ett problem. Då sådan filtrering är relativt svår och kostsam att införa för operatörerna vilket gör att de drar sig för att genomföra detta, behöver vi under tiden försöka begränsa de skador som DDOS-attacker orsakar tills dess att operatörerna har åtgärdat grundproblemet. Att stänga en rekursiv resolver är en relativt enkel uppgift som det är värt mödan 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/nistpubs/800-81r1/sp-800-81r1.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://www.isc.org/files/arm97.pdf

Bilaga 7 - Åtgärder mot skräppost

DKIM

En teknik för att motverka att meddelanden via elektronisk post skickas med falskt domännamn i avsändaradressen, det vill säga att någon 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[19]. 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.

Genom att leta efter de publika DKIM-nycklarna kan man få reda på vilka domäner som eventuellt signerar sin e-post med hjälp av DKIM. Den metod som används för att hitta dessa domäner kan dock inte skilja på om domänen använder DKIM eller dess föregångare, DomainKeys. Den huvudsakliga förklaringen till detta är att både DKIM och DomainKeys publicerar sina nycklar på liknande sätt.

Läs mer om DKIM på http://www.dkim.org.

SPF

Sender Policy Framework (SPF) är en metod för att motverka att meddelanden via elektronisk post skickas med falskt domännamn i avsändaradressen, det vill säga att avsändaren använder någon annan adress än sin egen som avsändaradress.

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

[19] http://tools.ietf.org/html/rfc5617

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.

Läs mer om SPF på http://tools.ietf.org/html/rfc4408.

Bilaga 8 - 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.

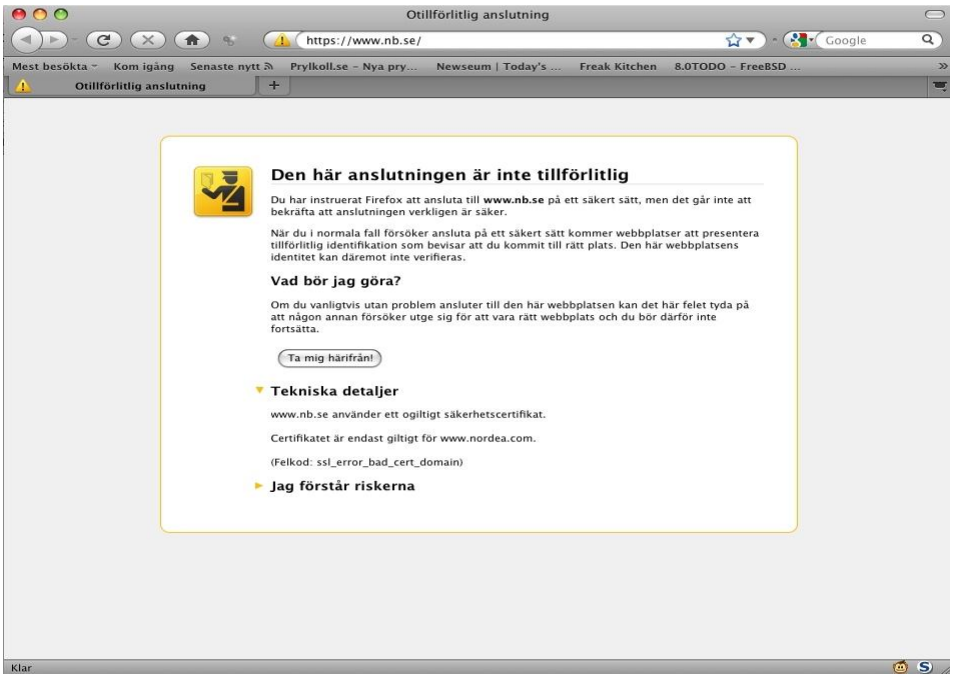
Om man vill skicka e-post som ingen annan ska kunna läsa, inte ens de som ansvarar för e-postsystemet (det vill säga "sitter på postkontoret"), behövs det ytterligare skydd. I dessa fall krypterar man hela brevet genom att man "klistrar igen kuvertet och skickar brevet rekommenderat", för att jämföra 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 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 ansvarar för Internets svenska toppdomän .se. Vi har hand om administrationen och driften av alla de över en miljon domännamn på Internet som slutar på .se. Vårt överskott går till fortsatt utveckling av Internet i Sverige genom en rad olika satsningar som på olika sätt bidrar till utvecklingen och användningen av Internet.

Hälsoläget i .se är en av dessa satsningar. Syftet med satsningsområdet är bland annat:

- att övervaka kvaliteten på Internets infrastruktur i Sverige genom att samla in och analysera fakta,
- att sprida resultaten från undersökningarna, samt
- att genom råd och rekommendationer medverka till att infrastrukturen har god funktionalitet och hög tillgänglighet.

Syftet är också att vid behov uppmärksamma och informera om brister och missförhållanden.

.SE (Stiftelsen för Internetinfrastruktur)
Box 7399, 103 91 Stockholm
Tel 08-452 35 00, Fax 08-452 35 02
Org. nr 802405-0190, www.iis.se

.se
Vi driver Internet framåt