Hälsoläget i .se 2011

– nåbarhet på nätet

Innehåll

1 Introduktion

Ännu ett år har förflutit och det är dags för den femte rapporten från .SE:s undersökning av nåbarhet på nätet och hälsoläget i .se med resultaten från 2011.

Årets undersökning är precis som tidigare år till stora delar men inte fullständigt en uppföljning av de tidigare undersökningar som genomförts under åren 2007-2010.

Rent statistiskt avviker resultaten i år en del från föregående år på grund av att vi har tagit bort en kategori, OMX-30 och lagt till .SE:s registrarer, det vill säga .SE:s återförsäljare och deras domäner som en ny kategori. Det har dock inte medfört några stora skillnader i grunden.

Syftet med undersökningen är att kartlägga och analysera kvaliteten och nåbarheten i domännamnssystemet (DNS) i .se-zonen och en del andra viktiga funktioner för domäner registrerade i .se, både ett urval av domäner som representerar viktiga funktioner i samhället och ett slumpmässigt urval av 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 .SE:s satsningsområde Hälsoläget. Syftet med satsningsområdet är att övervaka kvaliteten på Internets infrastruktur i Sverige. .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. Syftet är också att vid behov uppmärksamma brister och missförhållanden. Under 2011 har vi gjort en del tekniska förbättringar bland annat för att höja prestandan i de verktyg som används.

Hälsoläget finansieras av .SE. Resultaten av årets undersökning har analyserats och rapporten har sammanställts av Anne-Marie Eklund Löwinder, kvalitets- och säkerhetschef på .SE. Det operationella ansvaret för de verktyg som används har Patrik Wallström, projektledare på .SE. Granskningen av den statistiska analysen har genomförts av Anders Örtengren, Mistat AB.

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

2 Sammanfattning

Liksom tidigare år ligger undersökningens fokus på DNS-kvalitet. Vi granskar dock även andra viktiga parametrar för exempelvis e-post och webb.

Utvecklingen av IPv6 och DNSSEC är givetvis viktiga parametrar, inte minst tack vare den uppmärksamhet som både IPv6 och DNSSEC fått i regeringens nyligen lanserade strategi för det IT-politiska området ”It i människans tjänst - en digital agenda för Sverige”.[1]

Undersökningen är genomförd under oktober 2011.

2.1 Om undersökningsgruppen

I 2011 års undersökning testas totalt 912 domäner fördelade 1 369 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 och hur många domäner som finns i varje kategori redovisas i avsnitt 5.

Dessutom har en jämförelse gjorts med en kontrollgrupp som utgör en procent av hela .se-zonen, det vill säga 10 991 slumpmässigt utvalda .se-domäner som redovisas i avsnitt 9.

För att vi ska kunna följa utvecklingen år från år försöker vi i allmänhet hålla oss till ungefär samma undersökningsgrupp som den som använts tidigare. I år har vi emellertid beslutat att införa vissa förändringar som ger oss en bild från årets undersökning vilken inte helt överensstämmer med bilden från 2010.

I fjol undersöktes till exempel 670 domäner mot årets 912. Den främsta orsaken till det ökade antalet domäner är att vi lagt till kategorin ”Registrarer”. Skälet till det är vi finner det intressant att se hur väl de aktörer som många gånger levererar tjänster till domäninnehavare i .se motsvarar vad som är att betrakta som praxis i sin egen miljö.

Förutom det har vi sedvanliga förändringar bland övriga kategorier där verksamheter har lagts ner, slagits ihop eller kommit till.

Tidigare kunde en domän förekomma i flera kategorier, främst för att vi hade med kategorin OMX-30. Den kategorin innehöll i år i princip bara dubbletter, det vill säga domänerna förekommer också i någon annan kategori. Vår bedömning är att den kategorin inte tillför något utöver det man får ut av resultaten från övriga kategorier och har därför tagit bort den.

2.2 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.

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

Resultaten för 2011 är emellertid positiva i flera avseenden.

Den totala andelen allvarliga fel och varningar har minskat. En del kan möjligen förklaras av förändringar i undersökningsgruppen, men även om vi tittar på procenten slumpmässigt utvalda domäner ur .se-zonen som vi använder som jämförelse så har situationen blivit väsentligt bättre sedan förra året när det gäller andelen allvarliga fel, medan mängden varningar ökat något i den kategorin.

De två domäner som vid förra årets undersökning hade så pass allvarliga fel att de inte ens gick att testa, de ”lever” i någon mening vidare. Enligt våra tester med DNSCheck finns de inte ens med i domännamnssystemet, men likväl går det att surfa till deras webbplatser. Sannolikt går det inte att nå dem med e-post. Domänerna används troligen bara för webbtrafik och inte för e-post vilket förmodligen är orsaken till att innehavarna inte märker att de har problem med nåbarheten till domänerna. Ett lustigt fenomen är det i alla fall, som bevisar det vi brukar säga om DNS, det är extremt förlåtande, det går att göra väldigt mycket fel och det fungerar ändå.

2.3 Skillnader i undersökningen sedan förra året

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

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 det här fallet är det vi själva som har definierat vad vi anser vara hög kvalitet men vi har i definitionen utgått från vad som rekommenderas som praxis, eller branschstandard, internationellt, *Best Common Practice*. Det finns också anledning att tro att kunskapsbristen visar sig i brister både när det gäller drift och operativt ansvar.

Det finns några skillnader i underlaget till årets undersökning förutom vissa ändringar bland kategorierna i undersökningsgruppen. Den slumpmässigt valda gruppen domäner som vi använder för att jämföra med .se-zonen som helhet har valts ut annorlunda än förra gången.

I den förra versionen av verktyget kunde vi ta ut en lista på ett exakt antal slumpmässigt utvalda domäner. Nu följer verktyget en typ av algoritm som innebär att det inte går att bestämma det exakta antalet för testgruppen utan i stället väljer ut en andel, i det här fallet en procent, vilket i den aktuella körningen blir drygt 10 000 domäner, närmare bestämt 10 991.

2.4 Dominerande aktörer ökar riskerna

Spridningen bland operatörer till vilka man ansluter namnservrar har minskat ännu mer under 2011. De stora Internetoperatörerna blir allt större och de mindre för en allt mer tynande tillvaro. Risken med detta är att om en enskild

operatör dominerar inom en viss kategori kan konsekvensen bli att en hel sektor drabbas om den enskilda operatören får problem. Därför är det viktigt att ha namnservrar hos flera olika operatörer.

2.5 Bristande kompetens hos konsulter och tjänsteleverantörer

Tidigare års undersökningsresultat har lett till slutsatsen att det finns bristande kunskaper om vad som krävs för att hålla en hög kvalitet på domännamnssystemet (DNS). Det finns anledning att tro att dessa bristande kunskaper inte bara omfattar design och införande utan sannolikt också omfattar drift och operativt ansvar. Det faktum att några av de grövsta felen fortfarande är relativt vanligt förekommande ger oss också svart på vitt på att situationen inte har förbättrats radikalt från tidigare undersökningar. Det finns starka skäl för verksamheter att vässa sin egen beställarkompetens och ställa relevanta krav på både konsulter, registrarer och de leverantörer som driver namnservertjänster, e-posttjänster och webbtjänster.

2.6 Färre namnservrar med rekursion påslaget

Mellan 2007 och 2011 har andelen namnservrar med rekursion påslaget minskat mycket kraftigt, från 40 till 11 procent. Sedan förra undersökningen har vi haft en minskning med ytterligare fyra procent. Vi ser mycket positivt på den trenden.

2.7 Bristande certifikatshantering

Hanteringen av certifikat i undersökningsgruppens webbmiljö håller fortfarande mycket dålig kvalitet i alla avseenden som undersökningen tar upp. Hos de organisationer som ingår i undersökningen bör man kunna förvänta sig långt bättre resultat, framför allt när det gäller så grundläggande saker som att använda giltiga, aktuella certifikat utgivna av trovärdiga utgivare.

I år har vi sett många allvarliga attacker mot certifikatutfärdare, CA. Det väcker en del frågor om kvaliteten i säkerheten hos utfärdarna. Det har också fått leverantörer av webbläsare att skärpa kraven som ställs på en CA att komma med i listorna över rot-CA-certifikat som följer med varje webbläsare.

3 Kontrollpunkter

I undersökningen 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 hanterar verksamheten sin e-post? Står servrarna i eller utanför Sverige, används TLS/SSL (transportskydd)?
- Hur ansluter verksamheterna sina webbplatser till Internet? Var står servrarna, vilken serverprogramvara används, använder de servercertifikat, det vill säga har de stöd för TLS/SSL (transportskydd)? Hur är certifikaten beskaffade?
- 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 912 domäner. Hur de fördelar sig per kategori framgår i avsnitt 5.

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 fyra års undersökningsresultat.

Till detta knyter vi också generella rekommendationer om hur vi anser att det borde se ut i den svenska DNS-infrastrukturen. Slutligen upprepar vi våra 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 fortfarande finns brister som skulle behöva åtgärdas.

Genom att bearbeta strategiska partners som Kommunikationsmyndigheten PTS och Myndigheten för samhällsskydd och beredskap har .SE medverkat till att kommuner kan ansöka om anslag för att driva projekt för införande av DNSSEC. Dessa medel kommer att beviljas och kunna tas i anspråk från och med 2012. Vi ser gärna att myndigheter och individer i beslutande ställning använder våra råd och rekommendationer och vidtar lämpliga åtgärder för förbättringar inom områdena DNS, DNSSEC och IPv6, men även skydd av kommunikation via e-post och webb.

4 DNS-tjänst med kvalitet

Domännamnssystemet (DNS) är en av hörnstenarna på Internet och kom till för snart 30 år sedan för att förenkla adressering av resurser på Internet.

.SE har ansvaret för Sveriges nationella toppdomän på Internet, en uppgift som anses så samhällsviktig att den regleras av en särskild lag. Varje Internetansluten enhet har en egen IP-adress som med hjälp av DNS kan kopplas till en adress i en form som är lättare att hantera för oss människor, det vill säga domännamn.

Vi ser till att de över 1 000 000 domännamn som slutar med .se kan peka ut rätt resurser på Internet genom att vi för ett register över dem samt dirigerar frågor och svar. På så vis går det att nå 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 4 000-5 000 frågor per sekund.

Vi har använt nedanstående definition av en DNS-tjänst med kvalitet för årets liksom för tidigare års undersökningstillfällen: Hög kvalitet 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.

Tidigare års undersökningsresultat har lett till slutsatsen att det finns bristande kunskaper om vad som krävs för att hålla en hög kvalitet på domännamnssystemet. Det finns anledning att tro att dessa bristande kunskaper inte bara omfattar design och införande utan sannolikt också omfattar drift och operativt ansvar. Det faktum att några av de grövsta felen fortfarande är relativt vanligt förekommande ger oss också svart på vitt på att situationen inte har förbättrats radikalt från tidigare undersökningar. Det finns starka skäl för verksamheterna att vässa sin egen beställarkompetens och ställa relevanta krav på både konsulter, registrarer och de leverantörer som driver namnservertjänster, e-posttjänster och webbtjänster.

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.

5 Tester 2011

De genomförda testerna 2011 har givetvis även denna gång 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.

Vid testerna används en 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 frågor bland annat om hantering av elektronisk post och webb. En fördjupad del av undersökningen har genomförts för att tränga djupare in i frågor kring säkrare, mer tillgängliga och robusta e-post- respektive webbtjänster.

Testerna har omfattat totalt 912 domäner på 1 369 unika namnservrar. Testobjekten har grupperats i kategorier på följande sätt (inom parentes redovisas det antal verksamheter som ingick i respektive kategori förra året):

- 60 affärsdrivande verk och statliga bolag (40).
- 79 banker, finansinstitut och försäkringsbolag (67).
- 22 Internetoperatörer (ISP) (20).
- 290 kommuner (290).
- 21 landsting (21).
- 34 medieföretag (24).
- 228 statliga myndigheter, inklusive länsstyrelser (exkl. myndigheter under Riksdagen) (201).
- 39 universitet och högskolor (35).
- 146 registrarer (ny).

Vi har tagit bort OMX30-listan som omfattade 28 .se-domäner och en ny kategori har införts för registrarer, det vill säga återförsäljare av .se-domäner vilka många gånger också är tillhandahållare av namnserver- och andra tjänster till domäninnehavare.

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

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

Varningar: Varningar är också fel som kan påverka driften, här bedöms emellertid inte åtgärder vara lika akuta, men det skulle givetvis höja kvaliteten och nåbarheten om dessa fel eliminerades.

6 Observationer 2011

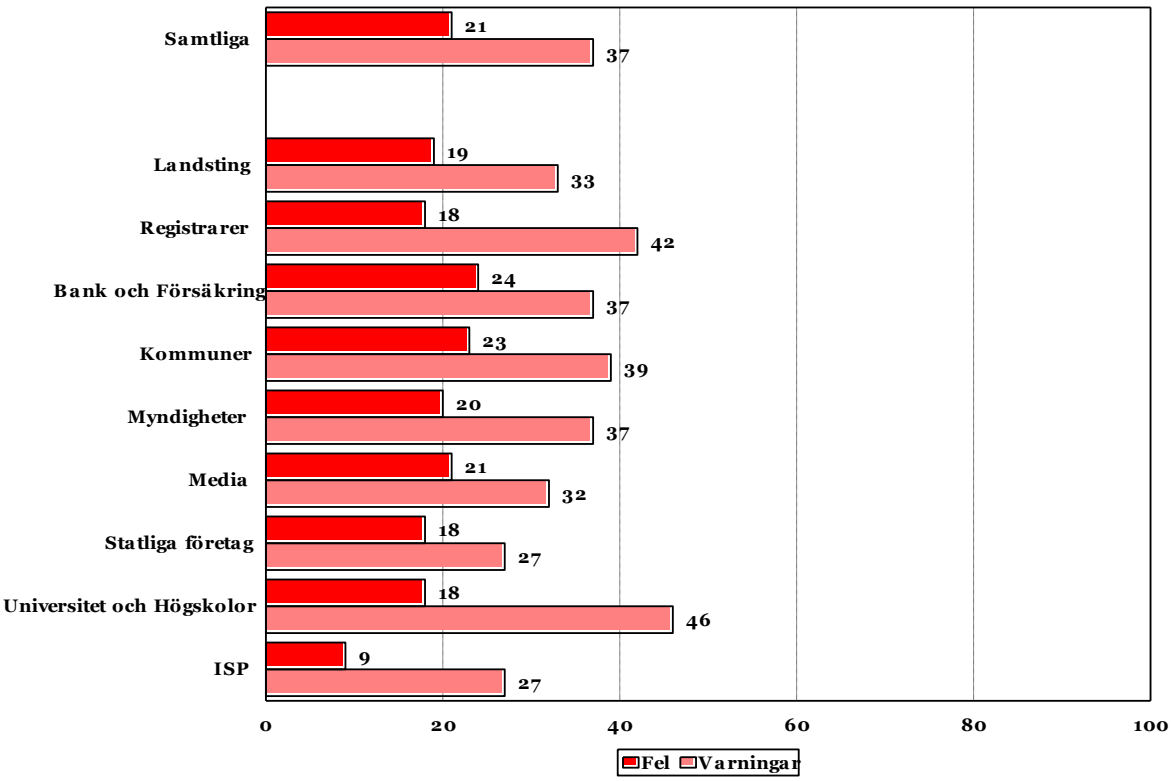
2007 genomförde vi den första mätningen för att få en uppfattning om hur det såg ut i .se-zonen. 2008 års undersökning gav oss en fingervisning om att det hade skett en positiv utveckling på området. När vi 2009 började se trender kunde vi bara konstatera att förändringarna var blygsamma och att det 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 årets undersökning är motsvarande siffror 21 procent domäner med allvarliga fel och 37 procent med brister av en karaktär som genererade varning. Vi kan alltså se en välkommen förbättring av resultaten.

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 912 domänerna i hela undersökningsgruppen (Samtliga), och för varje enskild kategori. Staplarna ska alltså läsas så att av de 912 verksamheter som ingår i undersökningen är 21 procent behäftade med fel av allvarligare karaktär och 37 procent med brister som genererar en varning. Detta är en minskning 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 är:

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

- Verksamheten har inte en 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 DNS-server är inte samma hos barnzonen som föräldrazonen i nivån ovanför. Detta är ett konfigurationsfel och bör korrigeras så snart som möjligt. Sannolikt har administratören för domänen glömt att göra en uppdatering vid förändring.
  - En DNS-server finns listad i föräldrazonen men inte i barnzonen. Det här är troligtvis ett administrationsfel. Föräldrazonen behöver snarast uppdateras så att den listar samma DNS-servrar som finns listade hos barnzonen. Konsekvensen av ett sådant fel är att den redundans som någon har försökt åstadkomma i praktiken inte existerar.

- Namnservern saknar stöd för EDNS. Detta är en utökning av DNS-protokollet för att hantera DNS-svar som överstiger UDP-protokollets begränsning på 512 bytes. EDNS möjliggör större DNS-svar än så, vilket 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 kan felet stå att finna någon annanstans, till

exempel i förbindelsen till namnservern eller att servern inte har en korrekt angiven IP-adress. Testerna på namnservern avslutas om båda dessa tillstånd har konstaterats.

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

- DNS-servern är rekursiv. DNS-servern svarar på rekursiva anrop från tredje part (så som DNSCheck). Det är väldigt lätt att utnyttja öppna rekursiva resolvrar i överbelastningsattacker (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). I DNS är det också möjligt att förfalska avsändaradressen, så den som vill attackera ett system skapar 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.

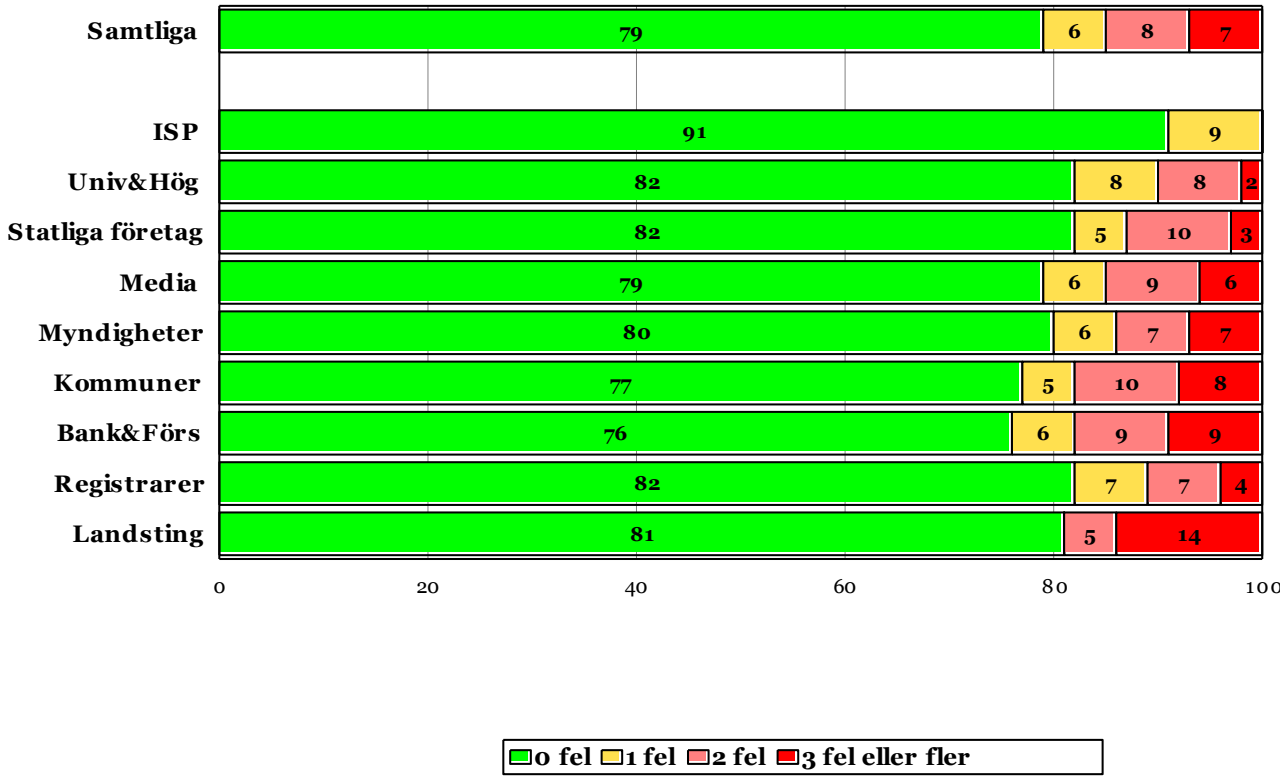
Felkonfigurationer som utförs av en och samma konsult hos många verksamheter eller av någon av de större namnserveroperatörna hos många domäner fortplantar sig till alla domäner som de hanterar och får, om de är många till antalet, givetvis stort genomslag i resultaten från undersökningen. Framför allt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

Värt att nämna är att .SE:s tre största registrarer har 50 procent av marknaden och tar vi de sju största har dessa 75 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 förstås en viss skillnad om en domän bara har ett fel eller om den har flera olika fel som kanske dessutom många gånger 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



Kategorin ISP:er, det vill säga Internetoperatörerna, har den absolut lägsta felprocenten också i år, medan kategorin Bank och försäkring i år har den högsta.

Det dåliga resultatet för kategorin Universitet och högskolor från förra året fick så småningom sin förklaring. Via Sunet kontaktade vi universitet och högskolor och den återkoppling vi fick tillbaka var att de hade ordnat det mesta av problemen (de använde bland annat DNSCheck för att se var problemen låg). Den vanligaste orsaken till fjolårets dåliga resultat var TCP-filtrering i brandväggar, men också att sekundära namnservrar stängts av eller omkonfigurerats utan att överliggande namnserver (master) meddelats.

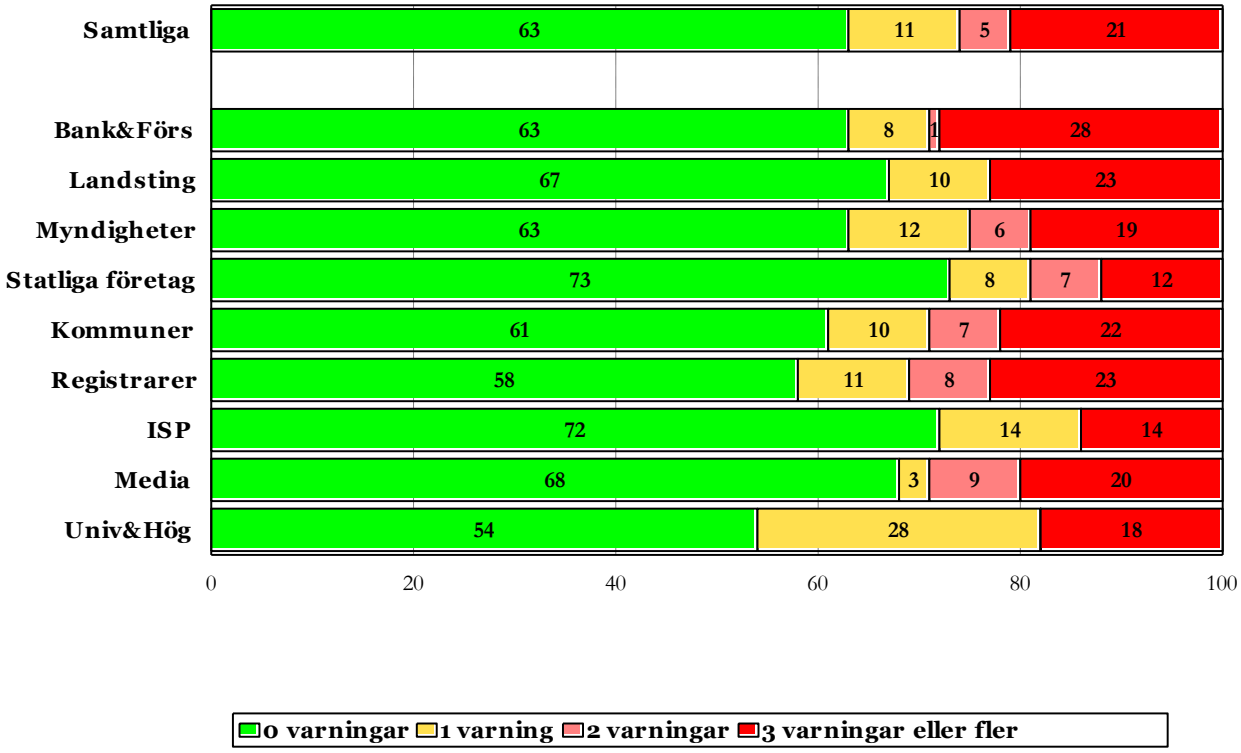
Landstingen förefaller ha många fel när det blir fel.

Vi är övertygade om att alla kan komma under 20 procent fel utan större ansträngningar. För att komma under 15 procent krävs det lite mer än att bara rätta till grundläggande hygienfaktorer.

6.2.2 Mängden varningar per kategori

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

Tabell 3: Procentuell fördelning av mängden varningar per kategori



Kategorin universitet och högskolor har störst andel varningar, följt av registrarer, kommuner och myndigheter. Bank och försäkring samt landsting har däremot väldigt många varningar, det vill säga hög andel med 3 eller fler varningar.

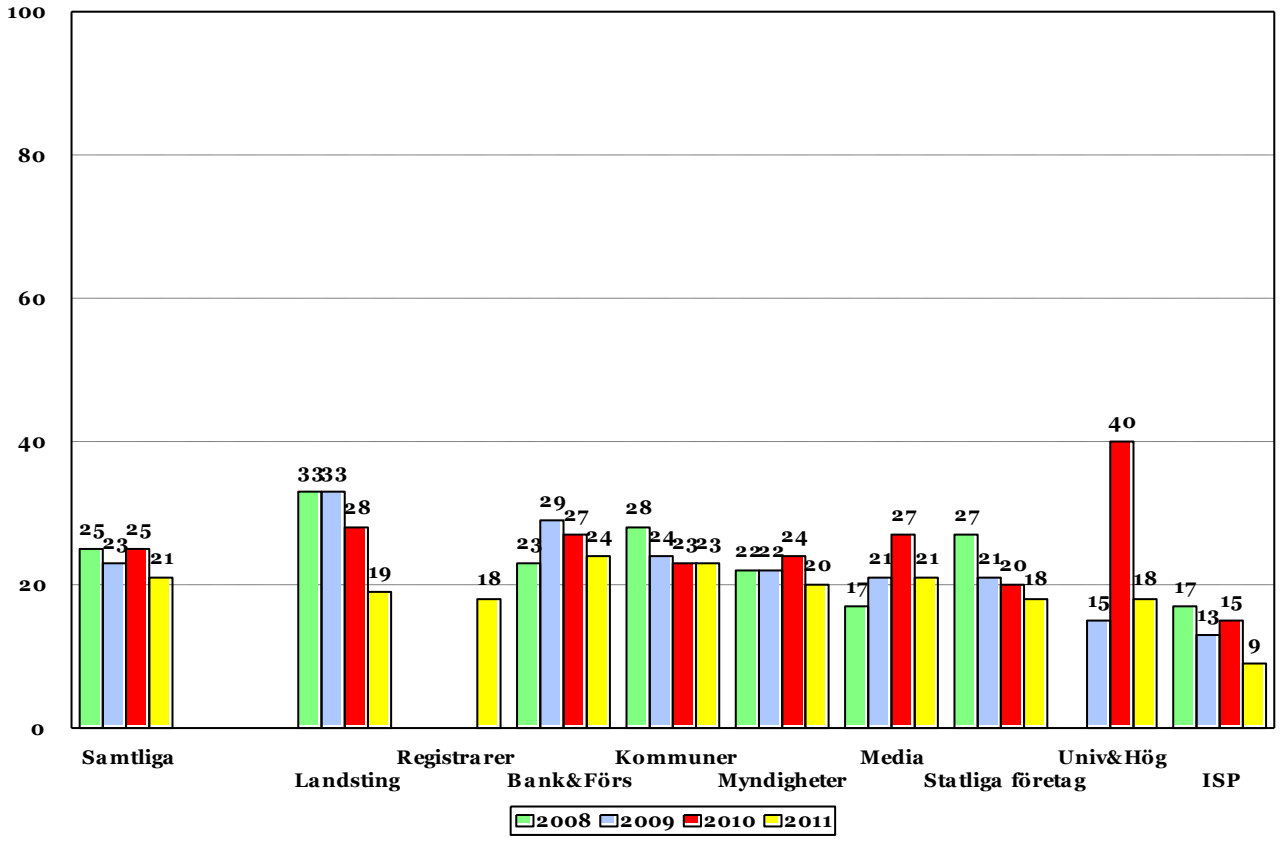
Vår bedömning är att detta i de allra flesta fall beror på administrativa brister, som till exempel att e-postadresser som anges i DNS inte fungerar. Det är generellt också mycket vanligare med varningar än med fel. Både fel och varningar påverkar emellertid nåbarheten negativt.

6.3 Jämförelse över tiden - fel och varningar

I och med att vi har sparat data från tidigare undersökningar har vi 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 för året.

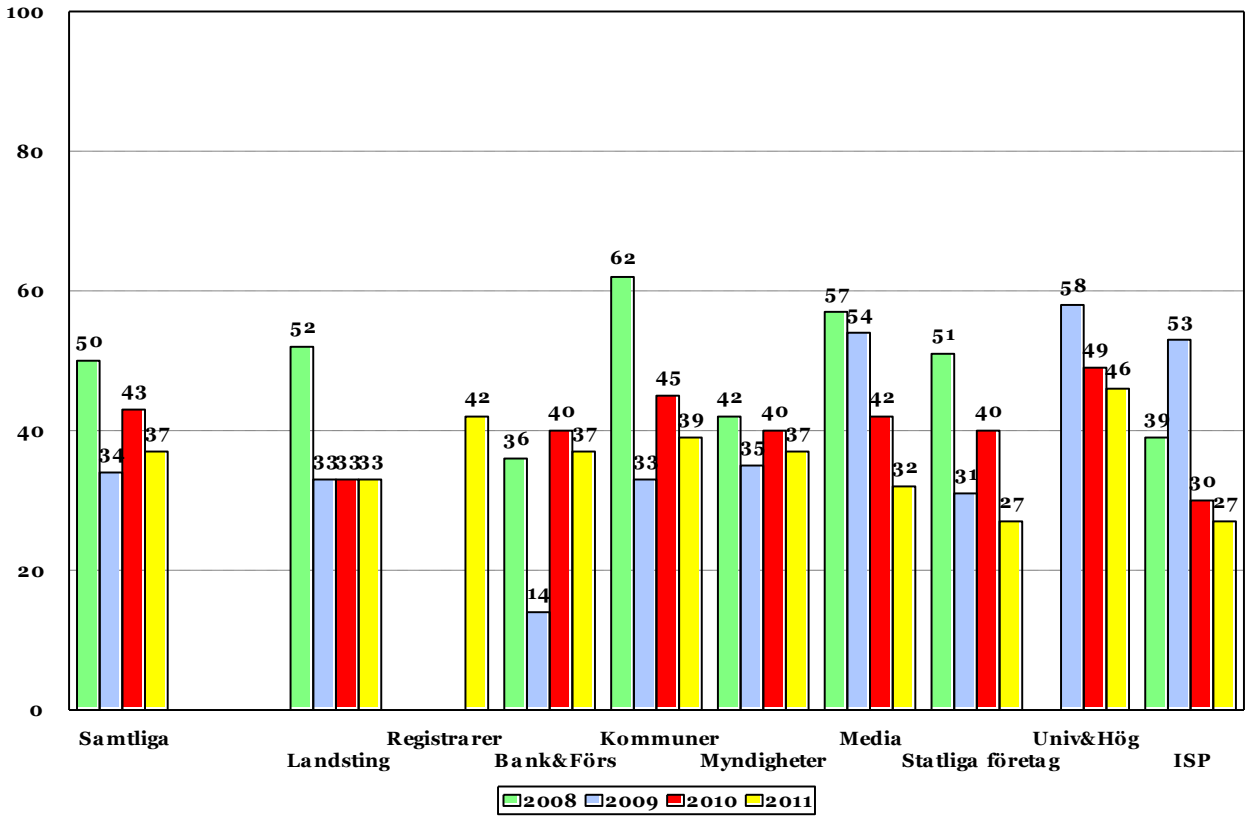
I nästa tabell jämför vi andelen fel över tiden från 2008 till 2011 (med undantag för Universitet och högskolor respektive Registrarer som tillkom 2009 respektive i år).

Tabell 4: Andel fel över tiden



Av tabellen kan vi se att situationen har förbättrats inom alla kategorier jämfört med föregående år.

Tabell 5: Andel varningar över tiden

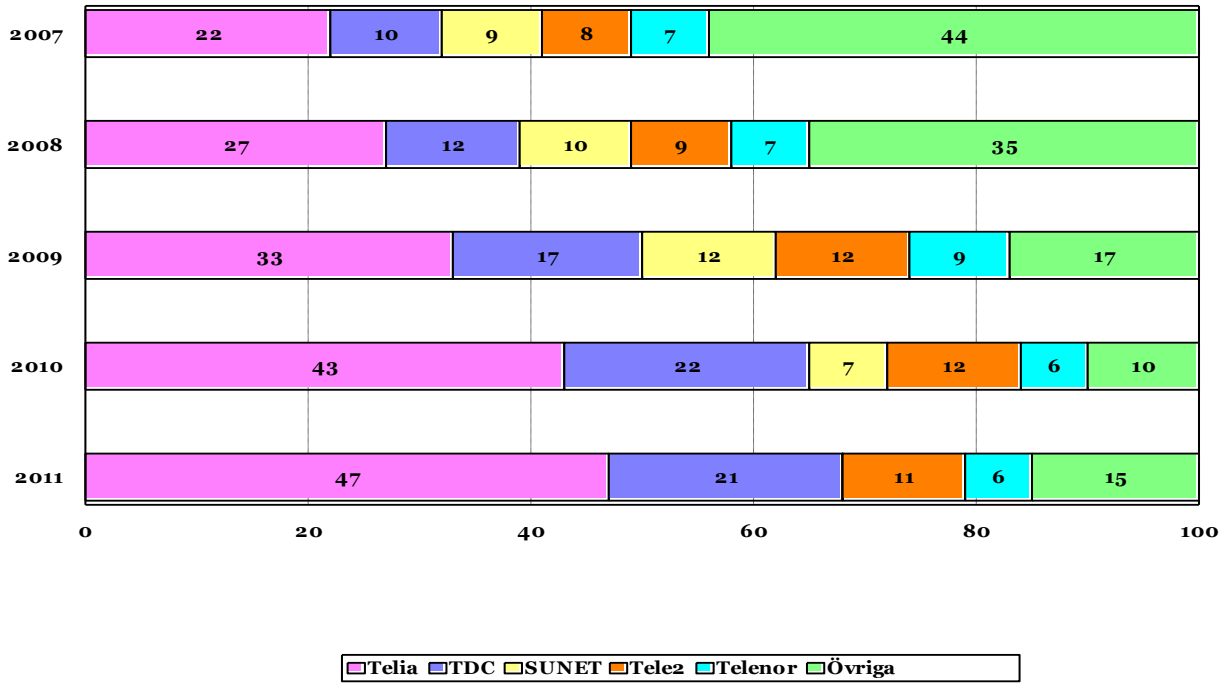


När det gäller varningar är situationen oförändrad för landstingen jämfört med föregående år, medan mängden varningar har minskat i alla andra kategorier som fanns med i förra årets undersökning. Bland registrarerna är det 42 procent där testerna genererar någon form av varning.

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 minskar från år till år om man tittar på den totala mängden domäner.

Andelen ”Övriga” har visserligen ökat något i år, men den har ändå gått från 44 procent 2007 till 15 procent i år. Sunet har helt försvunnit från kartan och förklarar sannolikt ökningen av gruppen Övriga.

Vi ser en ökning överlag hos de största operatörerna där i synnerhet Telia ser ut att allt mer dominera marknaden och i år har ökat sin andel till 47 procent jämfört med 43 procent förra året. TDC och Tele 2 har minskat medan Telenor ligger på oförändrade 6 procent. Förändringarna jämfört med förra året är alltså relativt omfattande.

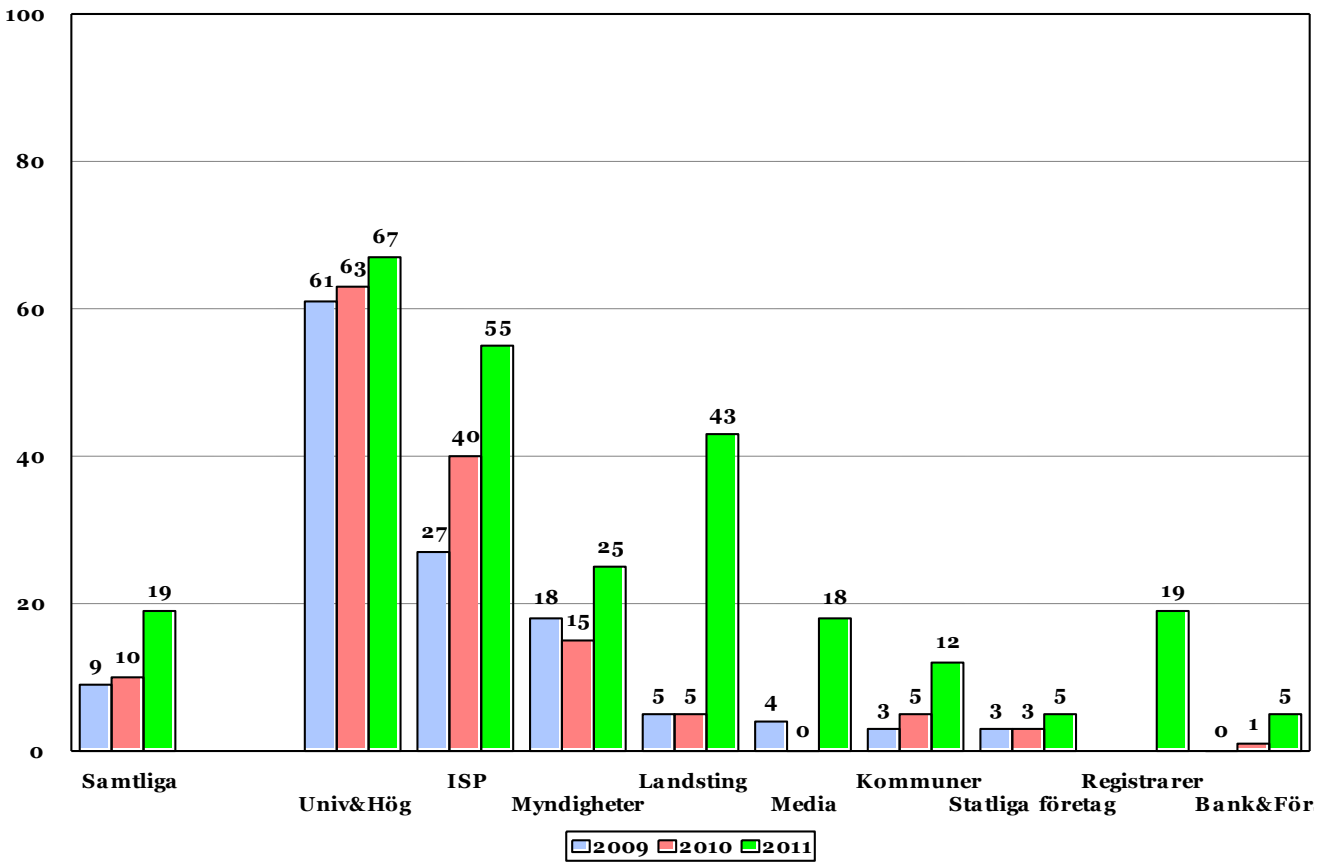
Spridningen av drift av namnservrar av olika operatörer fortsätter alltså att minska. De stora blir allt större och de mindre krymper alltmer. En risk med den utvecklingen är om en enskild operatör skulle dominera inom en viss kategori. Konsekvensen av en sådan dominans blir i värsta fall att en hel sektor drabbas om den dominerande operatören får problem. I fallet Telia vet vi att om Telia får problem så får det stora konsekvenser på många områden.

Det ökar redundansen om namnservrarna är anslutna till olika operatörer.

6.5 Namnservrar med IPv6

Trenden med en ökad aktivitet på IPv6-området håller i sig och har i år tagit ett rejält kliv uppåt. Universitet och högskolor toppar utvecklingen. Det största glädjeämnet är landstingen som har gått från 5 till 43 procent. Också myndigheter, kommuner och media visar en positiv utveckling. Det är endast inom kategorierna Statliga företag respektive Bank och försäkring som det verkar gå långsammare.

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



Totalt 19 procent av de undersökta domänerna har någon namnserver som går att nå via IPv6, jämfört med 10 procent 2010.

Adressbristen är redan ett faktum och det är mer än hög tid att införa IPv6. Det är viktigt att förstå att en sådan övergång kräver förberedelser och arbete på omkring 12-18 månader.

Att vänta med införandet av IPv6 är som att vänta med att gå till tandläkaren. Till sist kommer man till en punkt då det inte går att vänta längre, det blir dyrt

och det gör ont. Allt som måste göras akut innebär högre kostnader och sämre kvalitet. Det i sin tur leder till kunder och användare som är missnöjda.

Att införa IPv6 är det enda sättet att garantera en stabil framtida Internetinfrastruktur. .SE tar en aktiv roll för att underlätta samarbete och samordning kring övergången. Av den anledningen har vi en avdelning på vår webbplats som är ägnad åt att sprida information och att kontinuerligt rapportera om IPv6 i Sverige. Den finns på https://www.iis.se/internet-for-alla/ipv6.

Regeringen har också gett Post- och telestyrelsen (PTS) i uppdrag att beskriva hur IPv6 kan införas på myndighetsnivå med avseende på tillgänglighet, säkerhet och ekonomi. Syftet med beskrivningen är att den ska kunna fungera som stöd till myndigheter, kommuner och andra organisationer i offentlig sektor i deras införande av IPv6. PTS ska ta tillvara de erfarenheter som myndigheten fick när den under våren 2010 implementerade IPv6 i delar av sin IT-miljö. Inom uppdraget ska PTS även göra en konsekvensanalys av införandet av IPv6 som enda protokoll men även i samexistens med IPv4. Uppdraget avrapporterades nyligen och rapporten finns att läsa på http://www.pts.se/upload/Rapporter/Internet/2011/2011-18_Att_infora_internetprotokollet_IPv6.pdf.

6.6 Operatörer för drift av namnservrar

I normalfallet är det en registrar som också svarar för driften av namnservrar för en domän. De sju största registrarerna hanterar som tidigare nämnts sammantaget 75 procent av domänerna i se-zonen. Allvarliga felkonfigurationer hos de registrarer som också driver namnservrar för sina kunder skulle sannolikt bli mycket märkbara.

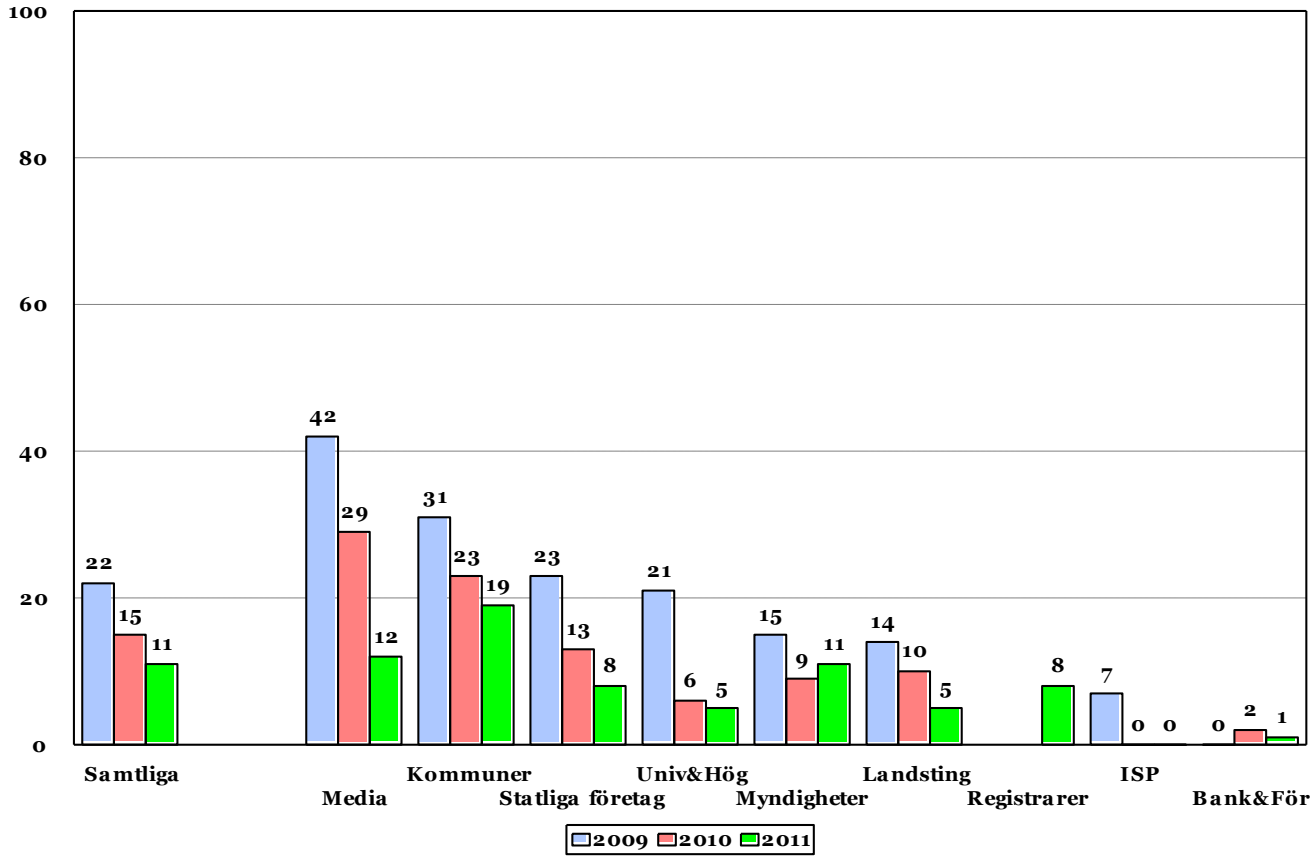
6.7 Namnservrar med rekursion påslaget

Som vi har upprepat varje år har öppna rekursiva namnservrar mycket få legitima användningsområden och kan komma att missbrukas 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 mer i år och är nu nere i 11 procent jämfört med 15 procent 2010. Det är mycket positivt, med tanke på vilka risker det innebär.

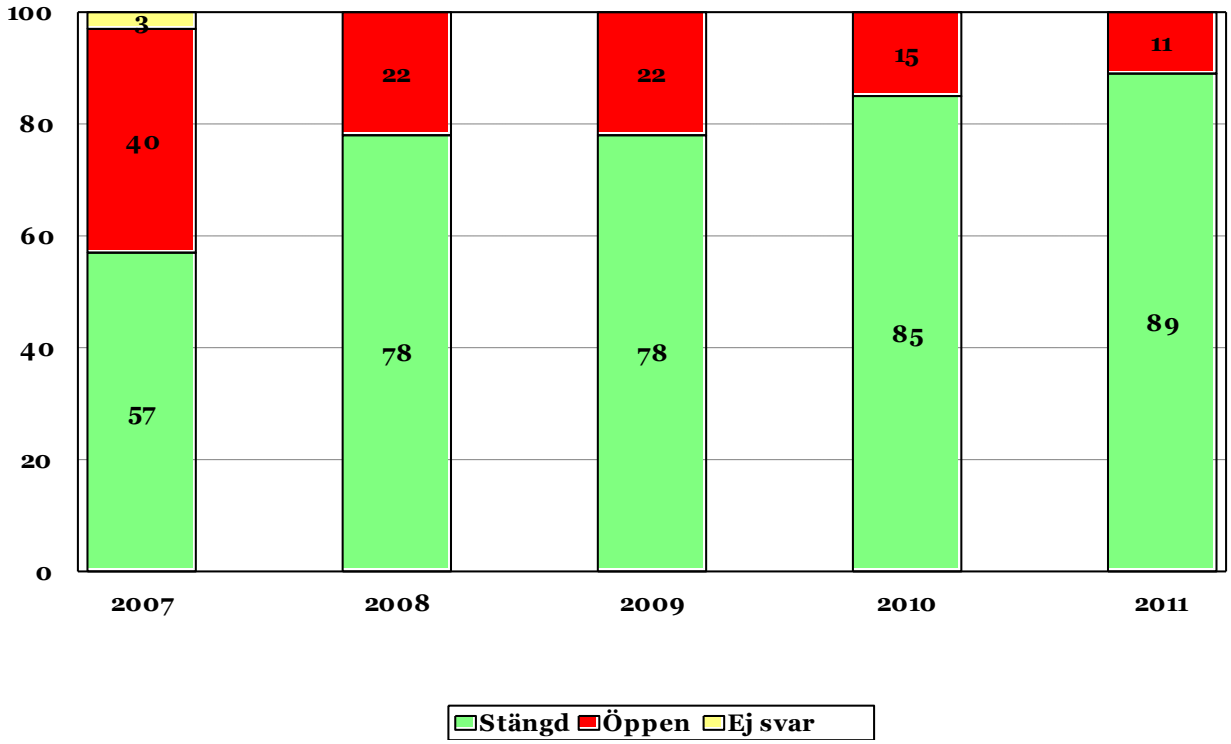
Vanligast förekommande är det hos kommunerna (19 procent) vilket framgår av tabellen nedan.

Tabell 8: Namnservrar öppna för rekursion per kategori



En av förklaringarna till de förbättrade resultaten som vi ser i tabellen är 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).

Tabell 9: Namnservrar öppna för rekursion 2007-2011



Mellan 2007 och 2011 har andelen namnservrar med rekursion påslaget minskat mycket kraftigt, från 40 till 11 procent. Sedan förra undersökningen har vi haft en minskning med ytterligare fyra procent. Vi ser mycket positivt på den trenden.

6.8 Användning av DNSSEC

DNSSEC skyddar Internetanvändare från förfalskad eller manipulerad DNS-information såsom exempelvis det som kallas 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.

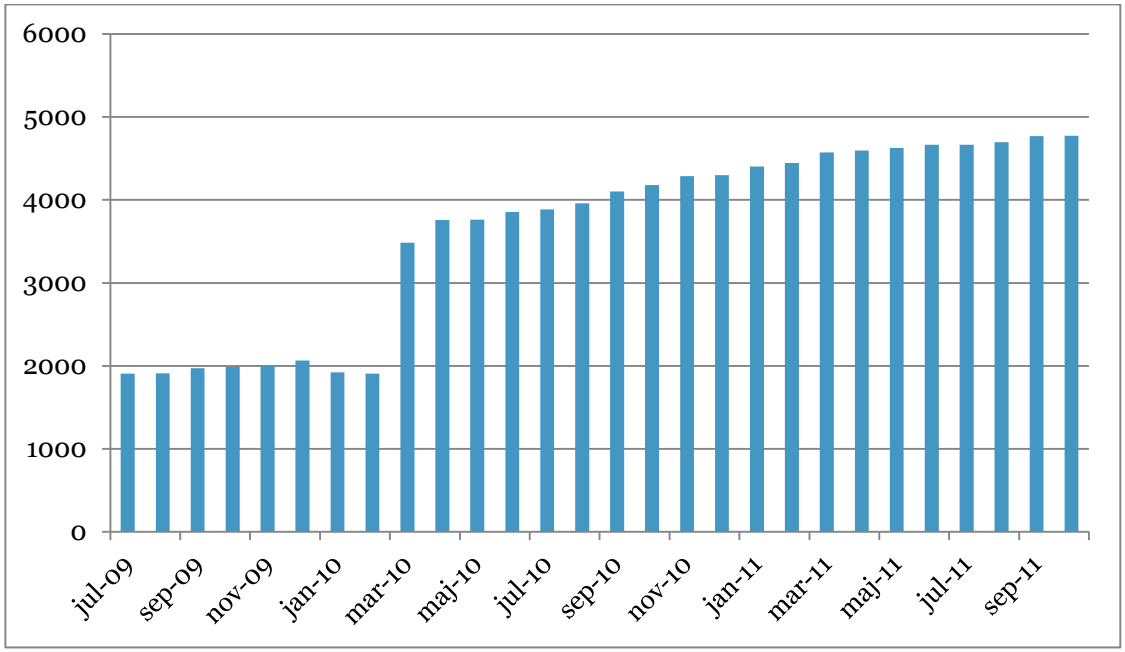
Vi särredovisar som vanligt hur många domäner i .se-zonen som är signerade med DNSSEC.

6.8.1 Hur utbredd är användningen av DNSSEC?

Bland domänerna i undersökningsgruppen 2011 är 6,69 procent eller 61 domäner signerade med DNSSEC. Det är framför allt kommuner, myndigheter, landsting och ISP:er som har börjat införa den säkrare tekniken. Som jämförelse kan vi nämna att i hela .se-zonen är för närvarande bara 0,45 procent

av det totala antalet domäner signerade. Vi ser en tillväxt, men långt ifrån i den takt vi skulle önska oss. I tabellen nedan redovisas tillväxten för DNSSEC-signerade domäner för hela .se-zonen, alltså inte bara jämförelsegruppen.

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



Källa: .SE:s webbplats.

Den 6 oktober 2011 publicerade Näringsdepartementet ”IT i människans tjänst – En digital agenda för Sverige”, 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. För 2012 har MSB prioriterat området robusthetshöjande åtgärder med inriktning mot att säkerställa adressuppslagningar på Internet, det som sker via domännamnssystemet. MSB skriver bland annat att ”det är mycket angeläget att domäner för offentliga webbplatser signeras med DNSSEC”. Kommunerna har under hösten 2011 kunnat ansöka om pengar. Vi har stora förhoppningar om att det kommer att ge resultat under nästa år.

För ett år sedan hade 15 kommuner signerat sina domäner och i oktober 2011 är det 24. Det går långsamt framåt med andra ord.

Det är viktigt att anlita rätt kompetens vid införandet av DNSSEC. Det finns fatala misstag som kan göras, ett exempel är att signaturerna har en viss livslängd och om dessa inte förnyas då slutar domänen att fungera. Vi ser exempel på verksamheter som har livslängd på signaturerna på under en vecka och andra parametrar som ger mycket litet utrymme för att reagera och reparera. Det betyder att man måste kunna hantera olika typer av avbrott i systemen tämligen snabbt, och exempelvis under semestertid eller långhelger kan detta bli ett problem om man inte har drift som är verksam dygnet runt, alla dagar i veckan, året om.

Det finns verktyg som hjälper till med administration av nycklar för DNSSEC och signering av zonfiler för en domän.

Det är inte heller sant som vissa kommuner har fått höra av mindre pålästa konsulter att det kräver minst en halvtidstjänst för att hantera DNSSEC, med moderna verktyg påverkar det driften i relativt liten omfattning. Det finns också konsulter som verkar tro att det går att använda Windows 2008 R2 för DNSSEC, vilket inte heller är med sanningen överensstämmande.

Så, ja, det är viktigt att använda rätt konsulter och i dagsläget är det inte så många som varit inblandade i ett praktiskt införande som ger bra erfarenheter, men med tanke på det ringa antalet signerade domäner så är det å andra sidan inte heller så många som har försökt utan att ha tillräckliga kunskaper och därmed kunnat rasera något.

6.9 DNSSEC i andra toppdomäner

Spridningen av DNSSEC har tagit fart bland andra toppdomäner i världen, i synnerhet efter signeringen av rotzonen som skedde förra året. Av de totalt 310 toppdomäner som annonseras i rotzonen är 83 signerade med DNSSEC och 76 av dessa har publicerat information om sina nycklar i rotzonen.

Aktuell statistik finns på http://stats.research.icann.org/dns/tld_report/
Mer information om DNSSEC finns i bilaga 5.

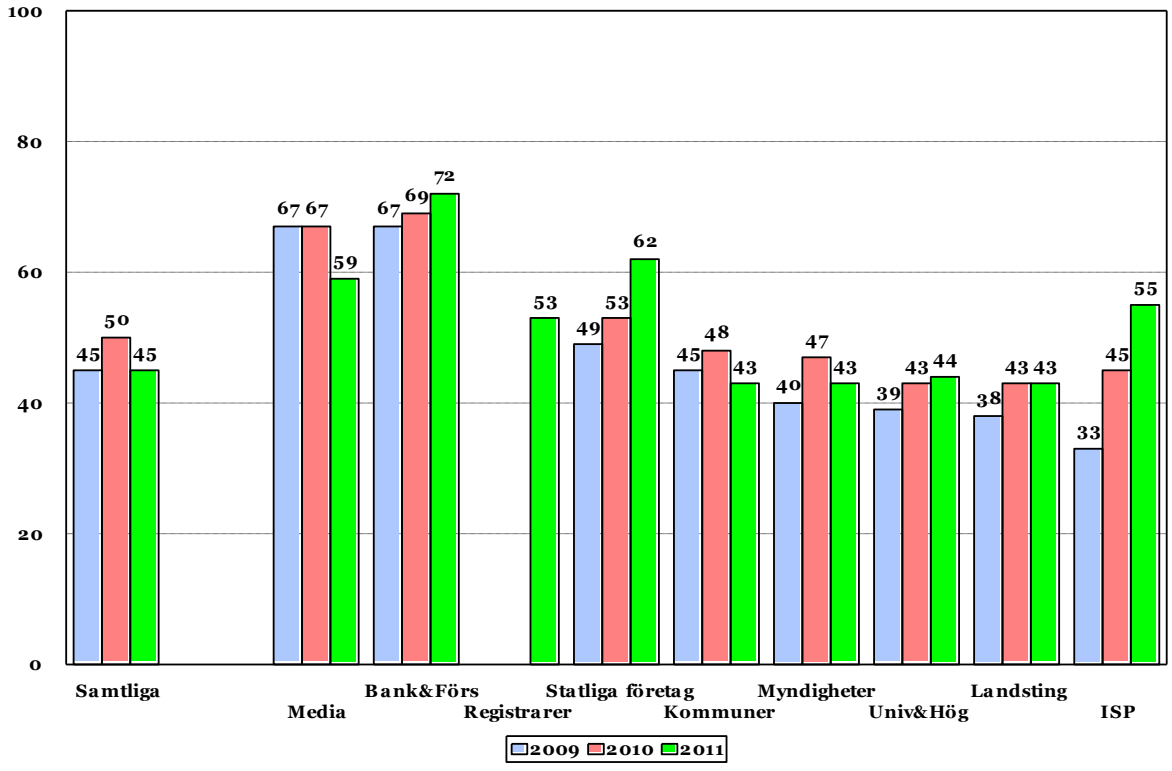
7 Viktiga parametrar för e-post

7.1 Stöd för transportskydd (TLS)

För att säkert utbyta information mellan e-postservrar bör 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).

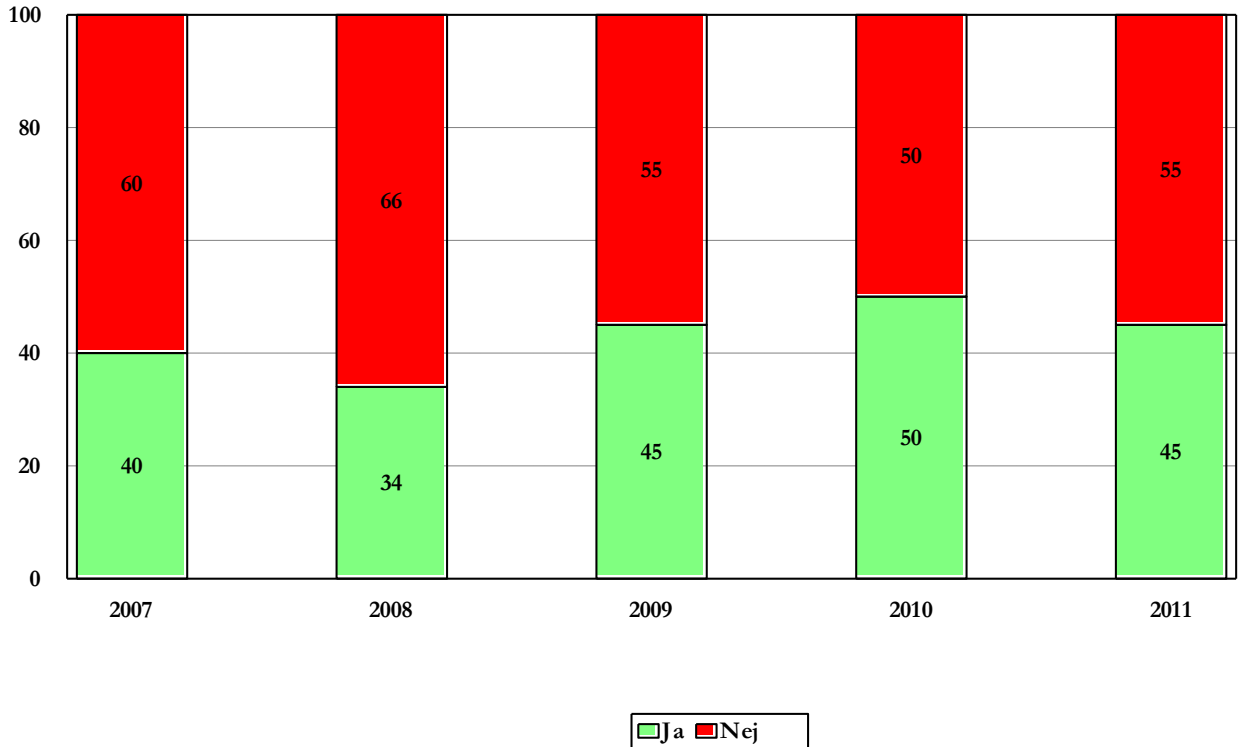
Av de undersökta verksamheterna 2011 har endast 45 procent stöd för TLS/SSL i sina e-postservrar. Det är minskning totalt sett från förra året (50), och det betyder att det i vart fall inte är fler som vidtar tillräckliga åtgärder för att skydda e-posttrafiken från insyn även om de ändrade undersökningsgrupperna påverkar bilden en smula. Det har visserligen ökat i vissa kategorier, men det har också minskat i andra. Alla programvaror har emellertid inbyggt stöd för det idag, och det är inte svårt att införa. För mer information, se bilaga 9.

Tabell 11: E-postservrar med stöd för TLS



Användningen av StartTLS har ökat i kategorierna Bank och försäkring, Statliga företag, Universitet och högskolor samt ISP:er. Användningen är oförändrad i kategorin Landsting men har minskat i kategorierna Media, Kommuner och Myndigheter. I den nya kategorin Registrarer är det endast 53 procent som använder StartTLS. Att det har minskat i kategorierna Media, Kommuner och Myndigheter är 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 fem senaste åren.

Tabell 12: E-postservrar med stöd för TLS 2007-2011

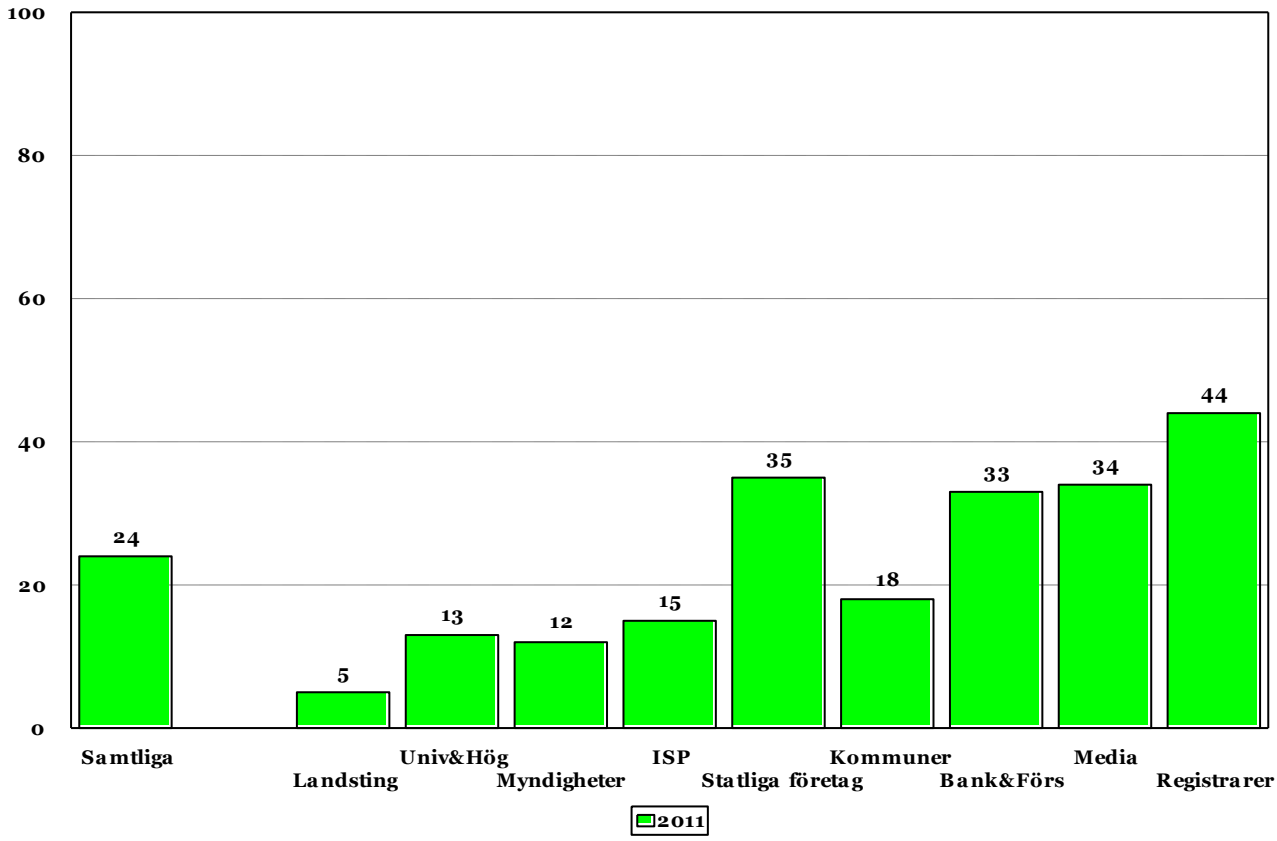


7.2 Placering av e-postservrar

Eftersom vi 2011 har en ökad andel e-postservrar som använder IPv6-adresser, och vi inte med någon visshet kan bestämma var dessa står enligt den metod som använts tidigare år har vi den här gången valt att särredovisa resultat för endast de servrar som använder IPv4-adresser.

Nedanstående tabell visar procentandelen e-postservrar placerade utanför Sverige fördelat per kategori.

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



I 2011 års undersökning har totalt 19,5 procent av domänerna namnservrar, e-postservrar eller webbservrar som är IPv6-adresserade.

För kategorin Registrarer är en del av förklaringen till att så många har servrar utanför landet att hela 46 av 146 ackrediterade registrarer är aktörer med verksamhet i något annat land än Sverige.

Ytterligare en annan sak som skiljer sig från föregående års undersökning är att registrarer kör väldigt många e-postservrar eftersom de många gånger levererar e-post som en tjänst till andra. Det betyder att de procentuella värdena för e-

postservrar i Sverige förändrats radikalt, eftersom antalet servrar som ingår i undersökningen i år är dubbelt så många (1 856) jämfört med 2010 (940).

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 ofta är oskyddad (se avsnitt 7.1) innebär det en onödig risk för exponering av känslig information.

Sammanfattningsvis kan vi konstatera att det fortfarande verkar vara 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. Vi kan dock inte avgöra om funktionen används för utgående e-post.

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

Det innebär också 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. DKIM respektive SPF eller en kombination av båda. De bygger på någon form av autentisering av avsändare på servernivå och domän.

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.

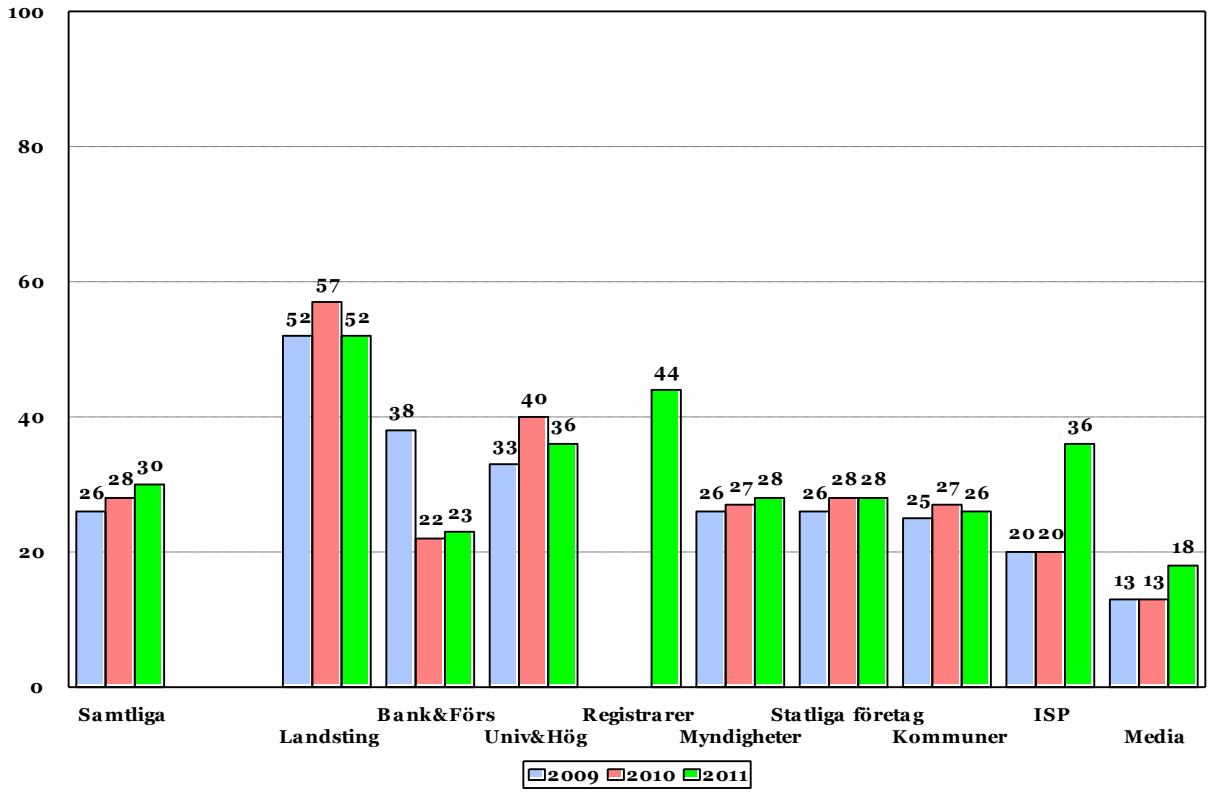
På grund av hur standarden för DKIM är utformad går det dessvärre inte med exakthet att bestämma om en domän använder DKIM eller inte. Vi kan i nuläget inte redovisa resultat om utbredningen av DKIM eftersom det inte säkert går att härleda förekomsten av DKIM för en domän förrän användningen av Author Domain Signing Practices (ADSP) blir mer vanlig (se bilaga 8). DKIM i sig hjälper inte mot skräppost om man inte kombinerar det med en ADSP-policy. I dagsläget är användningen av ADSP i princip obefintlig. Förekomsten av ADSP är något vi förmodligen kommer att redovisa i kommande undersökningar. Det går att mäta eftersom det publiceras i DNS.

7.3.2 SPF

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

I den nu aktuella mätningen tittar vi bara på om domänen har en SPF-post publicerad eller inte. Vi gör ingen bedömning av innehållet i övrigt.

Tabell 14: Använder SPF



Vi ser en blygsam men dock ökad användning av SPF i årets undersökning från 28 procent 2010 till 30 procent 2011. Landstingen har minskat något, från 57 till 52 procent, men de ligger fortfarande i topp. Användningen hos ISP:erna har ökat relativt kraftigt från 20 till 36 procent och bland registrarerna är det 44 procent som använder SPF. Bank och Försäkring, Myndigheter, Statliga företag och Kommuner ligger på i princip oförändrad nivå jämfört med förra året.

8 Viktiga parametrar för webb

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.

Ökad tillgänglighet är en viktig del, ökad säkerhet i termer av skydd av information (konfidentialitet) är en annan och väl så viktig del som vi fokuserar på i resten av detta avsnitt.

Förutom traditionella webbtjänster används webbteknik allt oftare för M2M-kommunikation (maskin-till-maskin), det vill säga Web Services. Där är det också viktigt med säkrad kommunikation i form av transportskydd, skydd mot återuppspelningsattacker, autentisering av server respektive autentisering av klientdelen.

Webbteknik används även ofta i så kallade appar då de kommunicerar med serverfunktioner. Huruvida dessa använder SSL/TLS vet ofta inte ens de som utvecklat apparna. Tester med linjelyssnare har visat att flera populära appar skickar information i klartext.

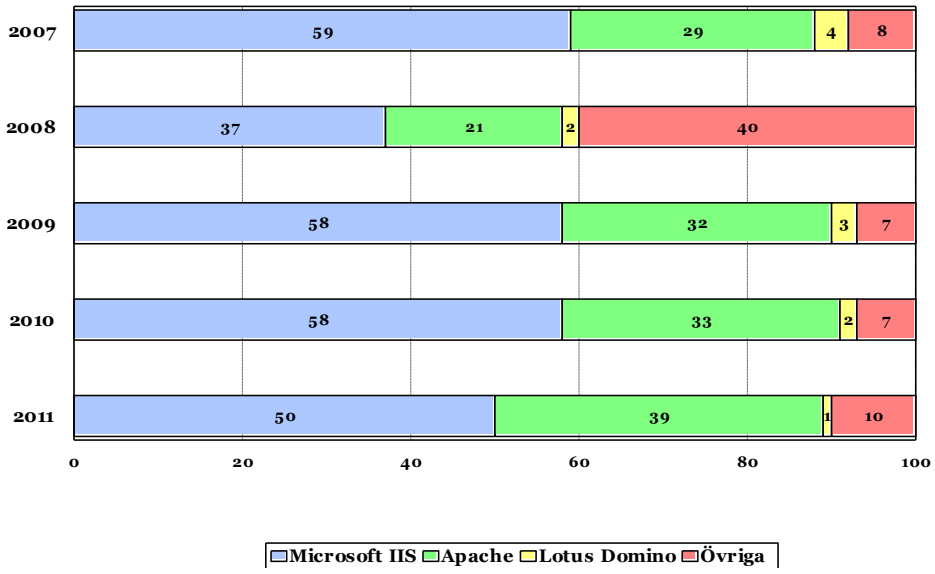
8.1 Anslutning av webbservrar

Om man i verksamheten har alla sina namnservrar anslutna till en och samma Internetoperatör och ansluter även webbservern till samma operatör 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 ha minst en ytterligare namnserver placerad hos en annan operatör, och man kan också överväga att placera en reservsajt någonstans för att uppnå största möjliga redundans.

8.2 Programvaror för webbservrar

Som vanligt har vi i undersökningen tittat på vilka programvaror för webb-servrar som används i de undersökta verksamheterna. De klart dominerande är fortfarande Microsoft Internet Information Server (Microsoft IIS) och Apache.

Tabell 15: Programvaror som används för webbservrar



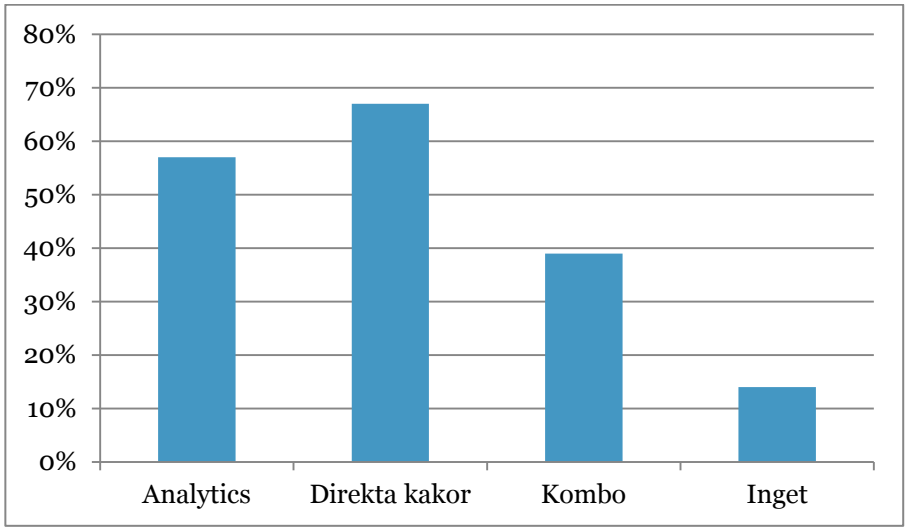
8.3 Andra intressanta iakttagelser kring webb

För andra året i följd kontrollerar vi en del parametrar som är av speciellt intresse för webbapplikationer.

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).

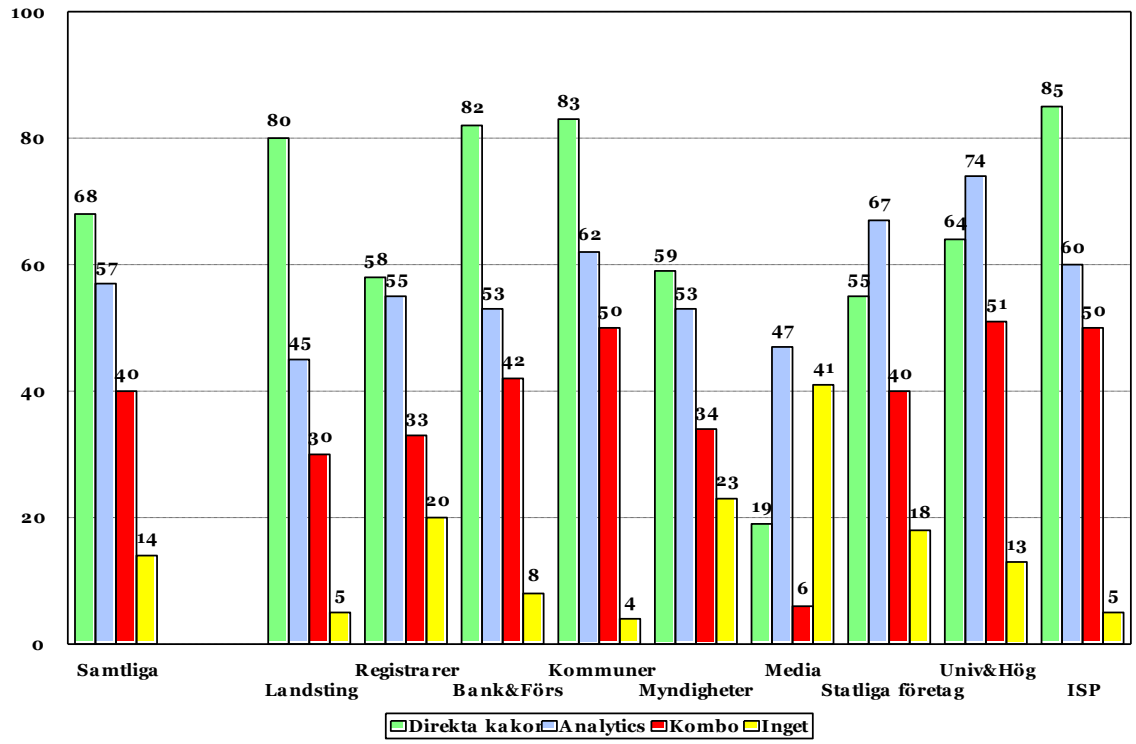
Tabell 16: Kakor



Av undersökningsgruppens 912 domäner kunde dessa tester genomföras på 904. En stor andel (57 procent) av de undersökta webbplatserna använder Google Analytics och sätter därmed tredjepartskakor för insamling av besöksstatistik, vilket är en ökning från förra året. Det är viktigt att veta att Google Analytics sätter kakor oavsett vilken kakpolicy som finns i verksamheten, utan att fråga först.

612 av de 904 undersökta domänernas webbplatser, eller 67 procent, sätter direkta kakor själv. Nästan 40 procent använder en kombination av både Google Analytics och direkta kakor. ”Inget” betyder i det här sammanhanget att varken Google Analytics eller direkta kakor används, men det utesluter inte användning av andra tredjepartsresurser som sätter kakor.

Tabell 17: Kakor per typ och kategori



Regeringen verkar i efterhand ha börjat känna viss oro över effekterna av kaklagen. I oktober i år 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 lämnas 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.

En tänkbar fördjupning från .SE:s perspektiv inom detta område kan vara att undersöka hur många webbplatser som försöker följa lagen och faktiskt begär aktivt samtycke från användarna.

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.

8.3.2 Publiceringssystem

Det överlägset vanligaste publiceringssystemet (CMS) som förekommer i de verksamheter som ingår i undersökningen är fortfarande EPiServer. Vi ser ingen märkbar ökning av användningen av alternativ byggda på öppen källkod. Vi gjorde förra året ett antagande att den andelen troligen skulle komma att öka, både tack vare minskade licenskostnader med de fria alternativen och för att mjukvara byggd på öppen källkod kan förväntas bli vanligare bland svenska myndigheter, men detta har vi alltså inte kunnat se, i alla fall inte än.

Det kan finnas en förklaring i att det är ett omfattande arbete att byta CMS, och att det kanske därför är funktionaliteten snarare än licenskostnaden som styr.

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.
- Om certifikatet används efter det att giltighetstiden har gått ut.
- Om domänen som certifikatet är utfärdat för inte motsvarar domänen för sajten.
- Om certifikatet har revokerats (spärrats).
- Om certifikatet är självsignerat.
- Om utfärdaren inte är en välkänd CA.
- Om certifikatutfärdaren inte bedöms vara pålitlig.
- Om 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 en exakt likadan körning som förra året, därför är det inte i alla avseenden relevant att jämföra siffrorna från 2010 med dem från 2011, men vi redovisar dem i alla fall i korthet nedan.

2010 var det 227 av 670 domäner eller 34 procent som returnerade något relevant på frågor som rör certifikat. Av dessa 227 domäner kunde vi ladda ner helt korrekta certifikat från 190 domäner där certifikaten var utfärdade av någon känd CA, det vill säga 84 procent, vilket var en ökning med 6 procent sedan 2009.

2011 har vi fått ut totalt 175 domäner med certifikat av 912 testade, motsvarande 19 procent, vilket är en minskning. Av dessa underkändes 16 helt och hållet (de får det lägsta betyget – F - på en sexgradig skala A-F). 46 certifikat håller toppkvalitet och får betyget A. Hur graderingen går till framgår av https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide_2009.pdf

De vanligaste felaktigheterna bland testade domäner är att:

- De använder certifikat utställda på fel hostnamn.
- De använder certifikat vars giltighetstid gått ut.
- De använder självsignerade certifikat.
- De använder certifikat signerade av någon okänd root-CA.
- De använder certifikat vars elektroniska signatur inte stämmer.

Det är dessutom vanligt att de domäner som inte har korrekta certifikat har fler än ett problem.

Hanteringen av certifikat i undersökningsgruppens webbmiljö håller alltså fortfarande mycket dålig kvalitet i alla avseenden som undersökningen visar. Denna typ av kryptoanvändning har funnits länge och är tämligen vanlig. Hos de organisationer som ingår i undersökningen borde 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 denna del av undersökningen är att en bristfällig användning av webbcertifikat undergräver trovärdigheten av denna typ av säkerhetslösningar.

Allt som innebär att en användare måste klicka på knappar som i praktiken innebär ”Ja, jag vet att det inte stämmer, men ta mig vidare ändå”, såsom självsignerade certifikat eller certifikat vars giltighetstid har gått ut gör att det inarbetas dålig säkerhetskultur hos 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.

Därutöver ska man tänka på att:

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

På 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.

8.5 Attacker mot SSL

Under året har det förekommit 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 säkerhet. Hanteringen hos de CA som har drabbats av de attacker som skett under året har i allra högsta grad varierat, och vissa av de drabbade certifikatsutfärdarna har agerat både långsamt och bristfälligt.

Vi vill i sammanhanget påminna om att certifikatsvarningar inte ska ignoreras utan tas under allvarligt övervägande, se bilaga 8. 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 tar en extra titt på certifikatet.

Webbläsarleverantörer som 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.

8.6 Åtgärder för att motverka attacker mot SSL

Det är många som funderar på lösningar, och ett av de mer intressanta initiativen vi sett är det som görs inom IETF-arbetsgruppen DNS-based Authentication of Named Entities (DANE), som snart kan förväntas vara färdiga. Med DANE lagras certifikat i DNS, så att det går att verifiera dem med 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*[2] som var det som avslöjade en av årets CA-attacker, den mot DigiNotar. Andra utökningar i Chrome är *HTTPS-preloading*[3] 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*[4] som utvecklats gemensamt av Electronic Frontier Foundation (EFF) och Tor-projektet.

En annan svensk undersökning[5] av certifikatsanvändning har under året genomförts av ROMAB. De har tittat närmare på användning av certifikat för Alexa topp 100 företag, svenska mediesajter, Alexa topp 100 internationella media, svenska fackföreningar och svenska politiska partier. Det är andra undersökningsgrupper än de vi har fokuserat på i vår undersökning, men resultaten är intressanta att ta del av för den som vill titta närmare på kvalitet hos, användning och hantering av certifikat.

.SE har för avsikt att genomföra en utökad undersökning av kvaliteten hos och användningen av certifikat i .se-zonen under 2012.

[2] http://www.imperialviolet.org/2011/05/04/pinning.html
[3] http://dev.chromium.org/sts
[4] https://www.eff.org/https-everywhere
[5] https://www.romab.com/swessl/

9 Jämförelse med .se-zonen

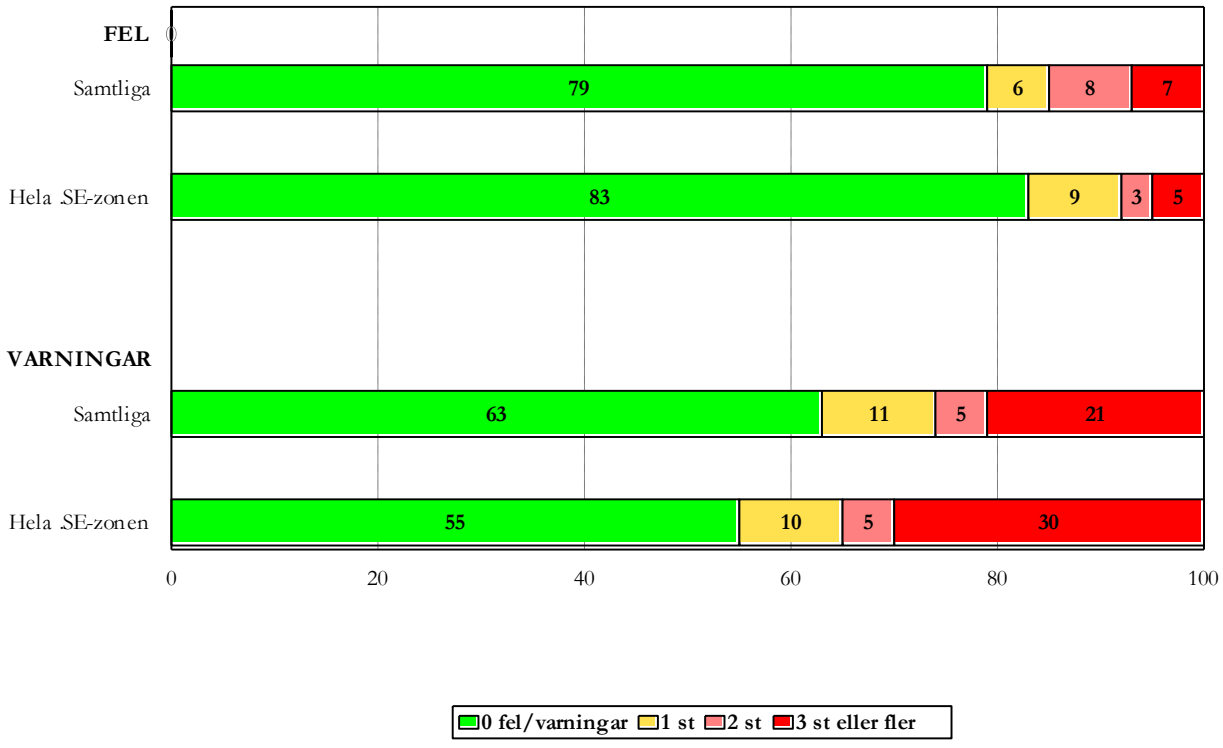
För att se om vår undersökningsgrupp är i bättre eller sämre skick än .se-zonen som helhet har vi även i årets undersökning gjort ett utsnitt av en procent slumpmässigt valda domäner ur .se-zonen för att ha som jämförelse.

I tabellerna nedan representerar ”Samtliga” den aktuella undersökningsgruppen medan ”Hela .se-zonen” representerar det slumpmässiga urvalet på en procent eller 10 991 domäner ur en version av zonfilen från den 31 oktober 2011.

9.1 Fördelning av fel och varningar

Först och främst har vi tittat 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 18: Andel fel och varningar



I år är det fler fel i vår undersökningsgrupp än i jämförelsegruppen för .se-zonen som helhet, alltså samma situation som förra året. Andelen varningar är emellertid färre i vår undersökningsgrupp än i jämförelsegruppen.

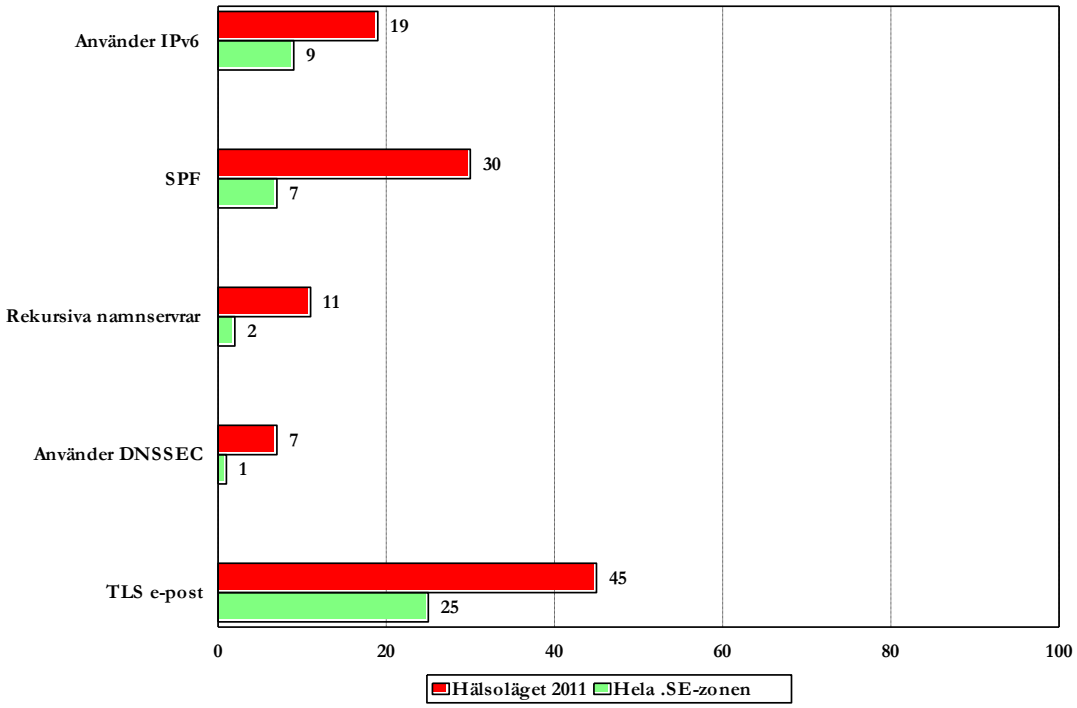
9.2 Skillnader mellan undersökningsgruppen och jämförelsegruppen

De stora skillnaderna ser vi först när vi tittar närmare på de specifika områden vi har granskat, som exempelvis de parametrar som vi förknippar med DNS-kvalitet enligt definitionen i bilaga 4. Det finns 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 (11 procent mot 2,4 i jämförelsegruppen).

I undersökningsgruppen är det fler som har infört IPv6 (19,5 procent mot 9 procent i jämförelsegruppen), det är långt fler som använder DNSSEC (6,6 procent mot 0,5 procent i jämförelsegruppen för .se-zonen som helhet) och fler som skyddar sin e-post med TLS. Under 2012 kommer vi att göra några mer detaljerade undersökningar för olika avgränsade områden.

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 19: Jämförelse mellan undersökningsgruppen och .se-zonen

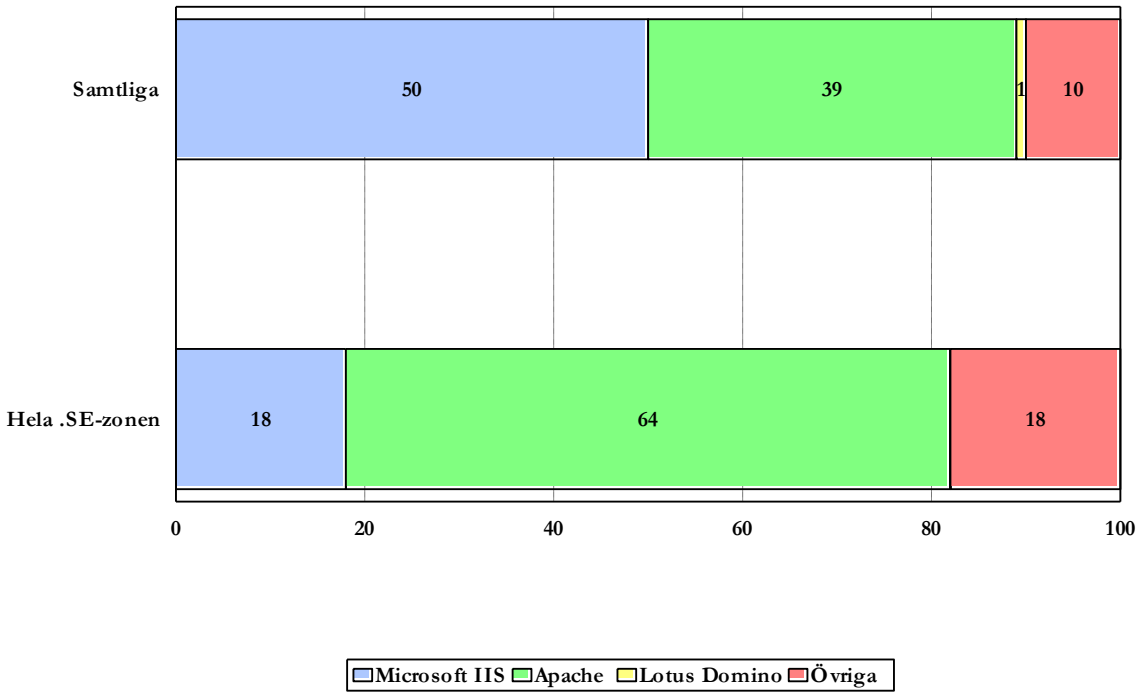


9.3 Skillnader i användning av programvaror för webbservrar

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 sedan förra året. Microsoft IIS har tappat något till förmån för Apache och övriga programvaror.

Lotus Domino har minskat ytterligare från två procent 2010 till en procent 2011 medan kategorin övriga har ökat.

Tabell 20: Programvaror för webbservrar

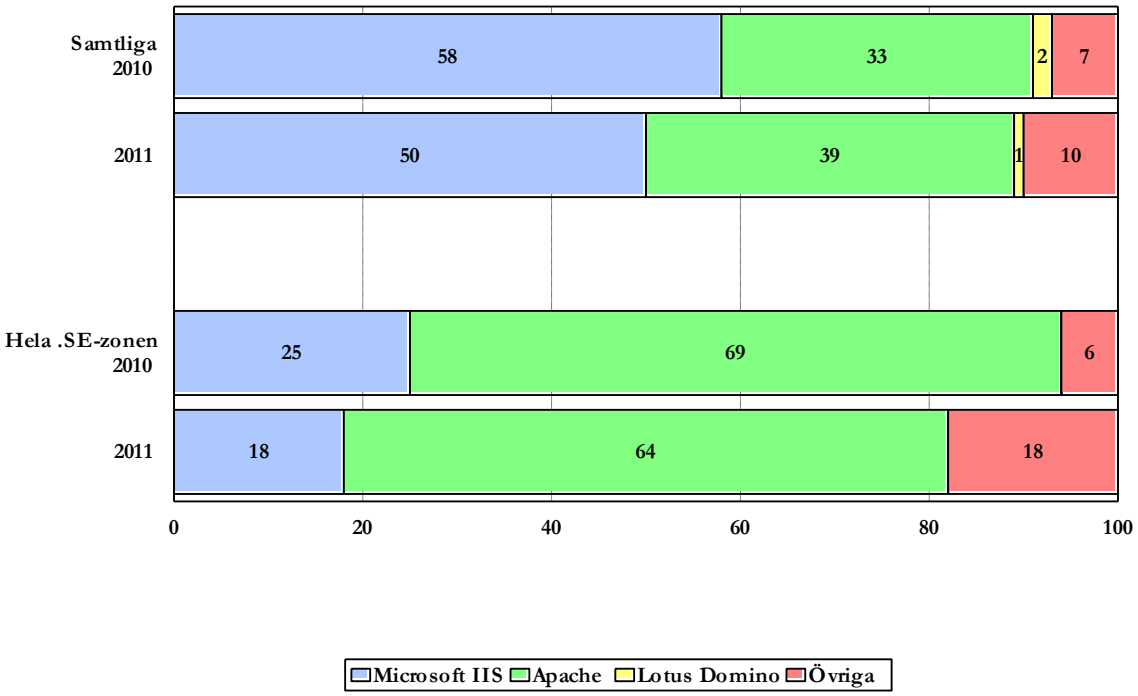


I tabell 21 gör vi samma jämförelse men för både 2010 och 2011. Där kan vi konstatera att Microsoft IIS har tappat mark både inom undersökningsgruppen och jämförelsegruppen. Den har emellertid fortfarande ett mycket starkt fäste i undersökningsgruppen.

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 21: Programvaror för webbservrar – förändring över tiden



10 Råd och rekommendationer

Efter att ha genomfört ännu en omgång tester med ett relativt positivt resultat jämfört med 2010 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. 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 Kommunikationsmyndigheten PTS, såsom

tillsynsansvarig myndighet, och handlar 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 om att det 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.

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*.

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.

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

SOA	Start of Authority, en pekare till var information om en zon börjar.
TLS/SSL	SSL är en standard för kryptering av bland annat webbtrafik under transport. Kommunikation med http med SSL kallas https. Ersätts numera av IETF:s öppna standard TLS.
zon	Avgränsning av det administrativa ansvaret för domännamnsträdet. En *zon* utgörs av en sammanhängande del av domännamnsträdet som administreras av en organisation och lagras på dess *namnservrar*.
zonfil	Datafil där den information finns lagrad som behövs om en *zon* för att adressering med *DNS* ska kunna användas.

Bilaga 2 - Om DNS och om undersökningen

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

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

.SE, har sedan 1997 ansvaret för teknisk drift och administration av alla namnservrar för .se-domänen och har genom åren skaffat sig gedigen erfarenhet av domännamnssystemet (DNS). På basis av våra egna och andras misstag och erfarenheter har det i branschen successivt vuxit fram en internationell Best Common Practice för DNS som kan tillämpas även i andra miljöer än på toppdomännivån. DNS är lite av en doldis med 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.

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.

IPv4-adresserna tog officiellt slut redan i februari i fjol. Därför börjar det bli mer och mer 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 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/.

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.

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. 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

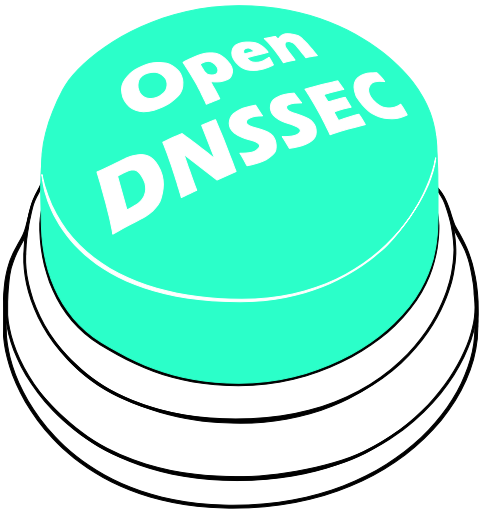
Nyheter om DNSSEC sprids regelbundet av DNSSEC Deployment Initiative
http://www.dnssec-deployment.org/

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

OpenDNSSEC

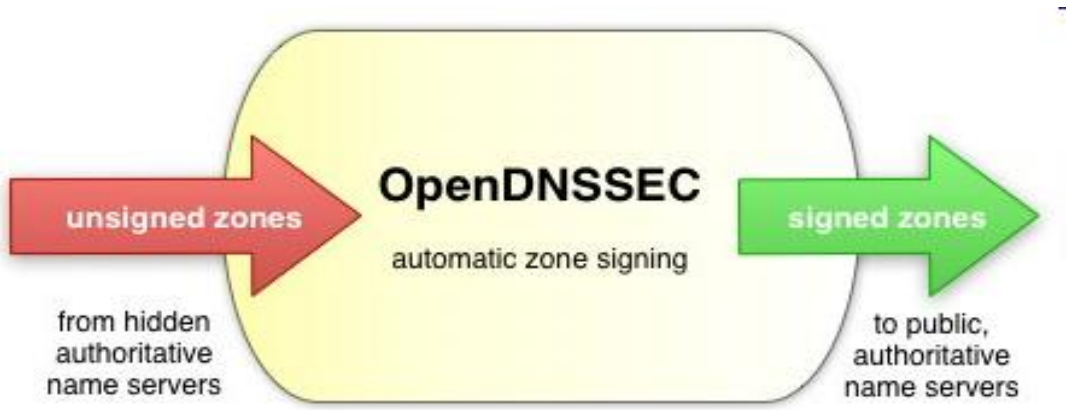
DNS är relativt komplicerat, och så är även elektroniska signaturer, kombinationen av dessa båda i DNSSEC är givetvis också den komplicerad.

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://oldwww.isc.org/index.pl?/sw/bind/arm95/index.php

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. 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, dvs. 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 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.