Nåbarhet på nätet
Hälsoläget i .se 2009

1 Introduktion 2
1.1 Detta dokument 2
1.2 Förkortningar och ordförklaringar 2
2 Sammanfattning 4
3 Om undersökningen 6
4 Om testverktyget DNSCheck 8
5 DNS-tjänst med kvalitet 9
5.1 Vad innebär kvalitet i DNS-tjänsten? 9
6 Tester 2009 10
6.1 Testobjekt 10
7 Observationer 2009 11
7.1 tester av DNS – fel och varningar 11
7.2 De vanligaste felen 12
7.3 Jämförelse över tiden - fel och varningar 14
7.4 Anslutning av namnserver till Internet 16
7.5 Namnservrar med IPv6 18
7.6 Namnservrar med rekursion påslaget 20
7.7 Användning av DNSSEC 22
8 Viktiga parametrar för e-post 24
8.1 Stöd för transportskydd (TLS) 24
8.2 Placering av e-postservrar 26
8.3 Åtgärder mot skräppost 28
9 Viktiga parametrar för webb 31
9.1 Anslutning av webbservrar 31
9.2 Programvaror för webbservrar 31
9.3 Stöd för transportskydd 32
10 Jämförelse med .se-zonen som helhet 36
11 Råd och rekommendationer 39

1 Introduktion

1.1 Detta dokument

Dokumentet är en rapport från en undersökning som .SE i år har genomfört för tredje gången i syfte att undersöka kvaliteten och nåbarheten i domännamnssystemet (DNS) i .se-zonen och en del andra viktiga funktioner för domäner registrerade i .se. Årets undersökning är till stora delar, men inte fullständigt, en uppföljning av två tidigare motsvarande undersökningar som genomfördes 2007 respektive 2008. För första gången har vi dessutom material som gör det möjligt att jämföra resultat över en längre period.

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

Mer information om innehållet i rapporten kan erhållas från Anne-Marie Eklund Löwinder, kvalitets- och säkerhetschef, .SE. Henne når man på anne-marie.eklund-lowinder@iis.se.

1.2 Förkortningar och ordförklaringar

Barnzon	Den underliggande *zonen*, till exempel är .example.se barnzon till föräldrazonen .se.
BCP	Best Common Practice, branschstandard.
DKIM	Domain Keys Identified Mail. DKIM gör det möjligt för e-postservrar att skicka och ta emot elektroniskt signerad e-post.
DNS	Domain Name System. En internationell hierarkiskt uppbyggd distribuerad databas som används för att hitta information om tilldelade *domännamn* på Internet. Domännamnssystemet är det system som översätter domännamn (t.ex. iis.se) till IP-adress vilken används för kommunikation över IP-nät som t.ex. Internet.
DNS-data	Information som lagras hos ett *Registry* där det anges vilka *namnservrar* som ska svara på förfrågningar om en viss *domän*.
DNSSEC	Secure DNS. DNSSEC en internationellt standardiserad utökning av DNS som tillför säkrare namnuppslagningar, minskad risk för manipulation av information och förfalskade domännamn. Den grundläggande mekanismen i DNSSEC är kryptografisk teknik som använder digitala signaturer.
DNS-server	Se *Namnserver*.
Domän	Beteckning på en nivå i domännamnssystemet.
Domännamn	Ett unikt namn, sammansatt av namndelar, där en i 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.
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.

2 Sammanfattning

Det stora intresse som visades för resultaten från förra årets undersökning har övertygat oss på .SE (Stiftelsen för Internetinfrastruktur) om att vi ska fortsätta genomföra undersökningen, i år för tredje gången. Undersökningen ingår i ett långsiktigt projekt som går under namnet Hälsoläget, vilket fortfarande är under uppbyggnad.

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

Redan vid 2007 års undersökning bekräftades 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 man givetvis kan diskutera vad som är definitionen på ”hög kvalitet”. I det här fallet är det vi själva som har definierat vad vi anser vara hög kvalitet men vi har definierat nivån efter vad som rekommenderas som praxis internationellt, *Best Common Practice*. Det finns också anledning att tro att kunskapsbristen visar sig i brister när det gäller både drift och operativt ansvar.

Liksom förra året har vi i första hand undersökt DNS-kvalitet i årets undersökning. Men, liksom tidigare år, har vi utöver DNS valt att granska några andra viktiga parametrar för exempelvis e-post och webb. Vi har också tittat extra på användningen av IPv6. Undersökningen är genomförd under oktober 2009.

Testerna har omfattat totalt 663 domäner fördelade på 867 unika namnservrar. Med ”unik” menas här servrar med unika IP-adresser. En namnserver hos en operatör kan härbärgera flera domäner.

Vi har försökt hålla oss till ungefär samma undersökningsgrupp som den som undersöktes förra året, men förändringar har skett, vilket ger en inte helt jämförbar bild över åren. I fjol undersöktes till exempel 671 domäner mot årets 663. Den främsta orsaken till det förändrade antalet domäner är förändringar bland statliga myndigheter där myndigheter har lagts ner, slagits ihop eller kommit till. En annan förändring är att vi den här gången har tagit med de 30 största av de börsnoterade bolagen från OMX samt tagit in universitet och högskolor på nytt. I år kan dessutom en domän förekomma i flera kategorier, men de förekommer bara en gång i den sammanlagda gruppen. Det betyder att summan av alla domäner i de olika kategorierna blir 671, det finns alltså 8 dubbletter. Framför allt förekommer domäner både i kategorin OMX30 och i någon annan kategori.

Nytt för 2009 är att vi har vidareutvecklat användargränssnittet för testverktyget så att det är lättare att granska och jämföra resultaten från de olika kategorierna. I årets undersökning har vi inte bara gjort automatiserade tester mot en förutbestämd mängd .se-domäner, utan också genomfört samma tester mot en kontrollgrupp med 10 000 slumpmässigt utvalda domäner ur hela .se-zonen. Därutöver har vi liksom tidigare år genomfört vissa kompletterande undersökningar framför allt när det gäller säkerhet och webb.

I avsnitt 3 beskrivs varför vi genomför undersökningen och övergripande om vilka kontrollpunkter som undersöks. I avsnitt 4 berättar vi mer om testverktyget DNSCheck och avsnitt 5 definierar vad som avses med ”DNS-tjänst med kvalitet”. Avsnitten 6-10 redovisar resultaten och avsnitt i 11 sammanställs några råd och rekommendationer.

Av de 663 domäner som ingått i undersökningsgruppen hade 23 procent allvarliga fel som bör åtgärdas snarast och 34 procent brister av en karaktär som genererar varning.

Våra observationer tyder därmed på att det sker förbättringar inom vissa områden. Den totala andelen allvarliga fel och varningar har trots allt minskat något under de tre år som undersökningen har genomförts.

3 Om undersökningen

.SE, som sedan 1997 har ansvaret för teknisk drift och administration av alla namnservrar för .se-domänen, 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 som har mer än 25 år på nacken. DNS har genom åren visat prov på enastående skalbarhet och robust design. Ingenting har i princip behövt ändras i de grundläggande protokollen trots den enorma tillväxt som skett på Internet. DNS har emellertid kommit att bli allt viktigare för en fungerande kommunikation mellan Internetanvändare världen över, och det ställer krav på att DNS-systemet håller hög kvalitet i alla delar.

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

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

De så kallade IP-adresserna, det vill säga den unika nummerserie som identifierar varje ansluten enhet på Internet, består av 32 bitar. Därför finns det med IPv4 bara drygt fyra miljarder unika IP-adresser. I takt med att världen blir alltmer uppkopplad närmar vi oss en adressbrist på Internet. Detta problem beräknas enligt olika prognoser bli akut någon gång under åren 2010-2011.

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

Det finns de som säger att det är färre månader kvar till adresserna är slut och en övergång till IPv6 blir nödvändig, än år det har tagit att utveckla protokollet. Detta är ett av skälen till att vi i undersökningen har tittat närmare på den aktuella utbredningen av IPv6.

.SE är också intresserade av att se på hur verksamheter hanterar sin kommunikation i övrigt, främst när det gäller transportsäkerhet för elektronisk post och webbtrafik. Stiftelsen ska enligt sin urkund *”ha 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 viktigt område för oss.

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

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

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

- Hur ansluter verksamheten sin webb till Internet? Var står servrarna, vilken serverprogramvara används, använder de webbcertifikat, det vill säga har de stöd för TLS/SSL (transportskydd). Hur är servercertifikaten beskaffade?

Testerna har genomförts på domäner och namnservrar för ett stort antal viktiga verksamheter i samhället; affärsverk och statliga bolag, börsnoterade företag, banker och finansföretag, Internetoperatörer, kommuner, landsting, medieföretag och statliga myndigheter inklusive länsstyrelser samt universitet och högskolor, totalt 663 domäner.

Datainsamlingen har skett helt automatiserat och har omfattat tester av de allra vanligaste fel och brister som vi förknippar med DNS-drift, e-post och webbhantering.

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

Till detta knyter vi också rekommendationer om hur vi skulle vilja att det såg ut i DNS-infrastrukturen mer generellt. Slutligen lämnar vi några råd och rekommendationer om frågeställningar för ansvariga myndigheter, lämpliga att gå vidare med och utreda mer i detalj. Vi låter dessa stå kvar i princip oförändrade från förra årets undersökning eftersom vi inte har kunnat verifiera att någonting radikalt har skett i det sammanhanget. Vi skulle dock gärna se att myndigheter och individer i beslutande ställning tar emot förslagen och vidtar lämpliga åtgärder.

Undersökningen ingår i ett av .SE:s satsningsområden, Hälsoläget. Syftet med satsningsområdet är att övervaka kvaliteten på Internets infrastruktur i Sverige. .SE har som ambition att bidra till att infrastrukturen har god funktionalitet och hög tillgänglighet. Syftet är också att vid behov uppmärksamma brister och missförhållanden. Målsättningen för 2009 har varit att på allvar etablera satsningsområdet, och vi genomför ständiga förbättringar både vad avser metodstöd och undersökningsområden.

Projektet Hälsoläget finansieras av .SE och drivs av projektledaren Patrik Wallström. Resultaten av årets undersökning har analyserats och rapporten har sammanställts av Anne-Marie Eklund Löwinder, kvalitets- och säkerhetschef på .SE. Programmeringen och de praktiska körningarna har på .SE:s uppdrag gjorts av konsulten Calle Dybedahl från Init. Undersökningarna som rör servercertifikat för webbservrar har genomförts av Robert Malmgren, Romab. Granskningen av den statistiska analysen har genomförts av Anders Örtengren, Mistat AB.

4 Om testverktyget DNSCheck

Som motor för genomförandet av undersökningen har vi använt programvaran för .SE:s tjänst DNSCheck. DNSCheck är ett program designat för att hjälpa människor att kontrollera, mäta och förhoppningsvis också bättre förstå hur domännamnssystemet fungerar. När en domän (även kallad zon) skickas till DNSCheck undersöker programmet domänens hälsotillstånd genom att gå igenom DNS från roten (.) via TLD:n (toppdomänen, till exempel .se) vidare till de namnservrar som innehåller information om den specificerade 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.

Till årets undersökning har vi byggt om ramverket för att kunna komplettera med flera tester och det finns även möjlighet att spara historik från tidigare testkörningar på ett sätt som gör data lätt tillgängligt för jämförelser. Nya tester görs för exempelvis förekomsten av IPv6 samt av SPF och DKIM för hantering av skräppost. En separat testmotor har konstruerats för tester av olika parametrar för webbservrar.

För att underlätta jämförelser har vi också konstruerat ett internt webbgränssnitt för att kunna följa, sammanställa och analysera resultaten för alla domäner som ingår, respektive för enskilda kategorier och domäner på ett sätt som inte har varit lika enkelt med den metod som använts tidigare.

5 DNS-tjänst med kvalitet

Domännamnssystemet är en av hörnstenarna på Internet och är till för att förenkla adressering av resurser på Internet. Varje ansluten enhet har en egen IP-adress som med hjälp av DNS kan kopplas till en adress i en form som är lättare att hantera för oss människor. DNS gör det alltså möjligt för en användare att skriva in t.ex. en webbadress i textformat istället för att använda IP-adressen (vilket i och för sig också skulle fungera förutsatt att man kommer ihåg den). Vår definition av kvalitet i DNS-tjänsten som redovisas nedan i avsnitt 5.1 ligger fast även för detta undersökningstillfälle.

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

I projektet har vi utgått från en definition av vad som är att betrakta som en bra DNS-infrastruktur, en erfarenhetsmässigt uppbyggd branschstandard eller Best Common Practice (BCP).

Förra årets resultat ledde till slutsatsen att det finns bristande kunskaper om vad som krävs för att hålla en hög kvalitet på till exempel domännamnssystemet (DNS), även om man givetvis kan diskutera vad som är definitionen av ”hög kvalitet”. Det finns anledning att tro att dessa bristande kunskaper sannolikt också omfattar drift och operativt ansvar. Det faktum att några av de grövsta felen fortfarande är relativt vanligt förekommande ger oss också en indikation på att situationen inte har förbättrats nämnvärt från tidigare undersökningar. Den totala andelen allvarliga fel och varningar har emellertid minskat något under de tre år som undersökningen har genomförts.

5.1 Vad innebär kvalitet i DNS-tjänsten?

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

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

I bilaga 1 redovisas de viktigaste åtgärderna som behöver genomföras för att sammantaget skapa en DNS-infrastruktur med hög kvalitet.

6 Tester 2009

De genomförda testerna 2009 har omfattat såväl domänernas konfiguration och de namnservrar som svarar på frågor om domänen. De har också omfattat några av de enligt vår bedömning viktigaste parametrarna för e-post och webb. Vid testerna har en programvara använts som automatiskt kontrollerar de olika kontrollpunkter som angivits i branschstandarden för samtliga domäner som ingått i undersökningen, både för gruppen som helhet och per kategori. Programvaran har utöver detta kompletterats med frågor bland annat kring hantering av elektronisk post och webb. En separat undersökning har dessutom genomförts för att tränga djupare in i frågor kring säkrare webbtjänster.

6.1 Testobjekt

Testerna har omfattat totalt 663 domäner och 867 unika namnservrar. Testobjekten har grupperats i kategorier på följande sätt:

- Affärsdrivande verk och statliga bolag (40)
- Banker och försäkring (21)
- Internetoperatörer (ISP) (15)
- Kommuner (290)
- Landsting (21)
- Medieföretag (24)
- Statliga myndigheter, inklusive länsstyrelser (exkl. myndigheter under Riksdagen) (231)
- OMX-listan (30)
- Universitet och högskolor (33)

Åtta domäner är dubbletter som förekommer i mer än en kategori. Av de testade domänerna hade 23 procent allvarliga fel som bör åtgärdas snarast och 34 procent brister av en karaktär som genererar varning.

VÄRT ATT VETA

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

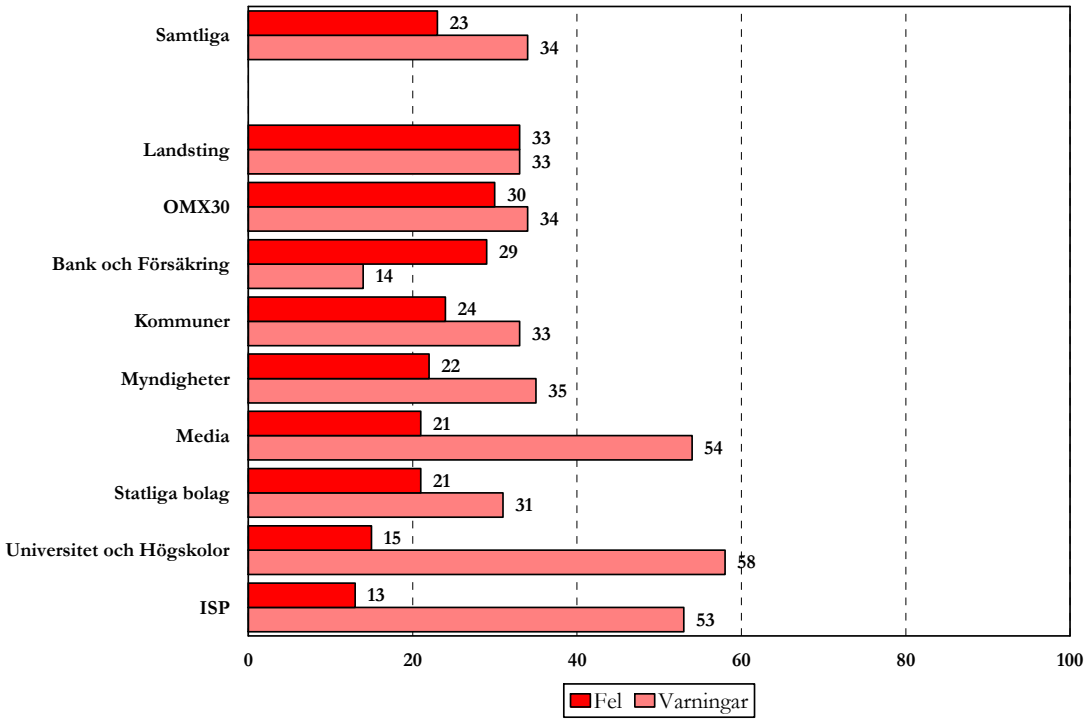
Varningar: Varningar är också fel som kan påverka driften, men åtgärder bedöms inte vara lika akuta, även om de givetvis skulle höja kvaliteten.

7 Observationer 2009

7.1 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 ovan visar procentandelarna fel respektive varningar för hela undersökningsgruppen (Samtliga), och för varje enskild kategori. Staplarna läses alltså så att av de 663 verksamheter som ingår i undersökningen är 23 procent behäftade med fel av allvarligare karaktär och 34 procent med fel som genererar en varning. Av de 21 undersökta landstingen är det en tredjedel (33 procent) som har allvarligare fel och en tredjedel (33 procent) som har fel som genererar varningar, osv.

Av tabellen ser det ut som om situationen för undersökningsgruppen som helhet förbättrats sedan förra året. En jämförelse mellan de olika kategorierna visar att situationen är klart mycket bättre bland universitet och högskolor samt ISP:er än bland de övriga kategorierna vilket är faktorer som kan bidra till den mer positiva totalbilden. Det är förvisso också inom dessa kategorier man bör kunna vänta sig att kunskapen och kompetensen ska vara den bästa inom det här området.

Vi kan av tabellen också utläsa att landstingen fortfarande är den grupp som har den procentuellt största mängden fel. Inom den gruppen är närmare 33 procent av alla namnservrar behäftade med någon typ av fel som kan betraktas som allvarligt, alltså samma resultat som 2008. Av den nytillkomna gruppen OMX30 har 30 procent av de undersökta

verksamheterna allvarligare fel följt av bank och försäkring med 29 procent. Vi kan alltså befara att tillgängligheten till information och tjänster i verksamheter inom dessa kategorier är sämre än vad den skulle behöva vara.

7.2 De vanligaste felen

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

- Namnservern svarade inte på anrop via TCP. Detta beror troligtvis på att DNS-servern inte är korrekt uppsatt eller på en felaktigt konfigurerad brandvägg. Det är en ganska utbredd missuppfattning att DNS inte behöver kunna kommunicera enligt TCP-protokollet (om den inte tillhandahåller zonöverföringar). Sanningen är emellertid att TCP oftast är ett krav, 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 tillräcklig kunskap om DNS.

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

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

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

- 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 förmodligen 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.

- 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 den skulle sluta fungera blir tjänsterna som pekas ut från namnservern också otillgängliga.

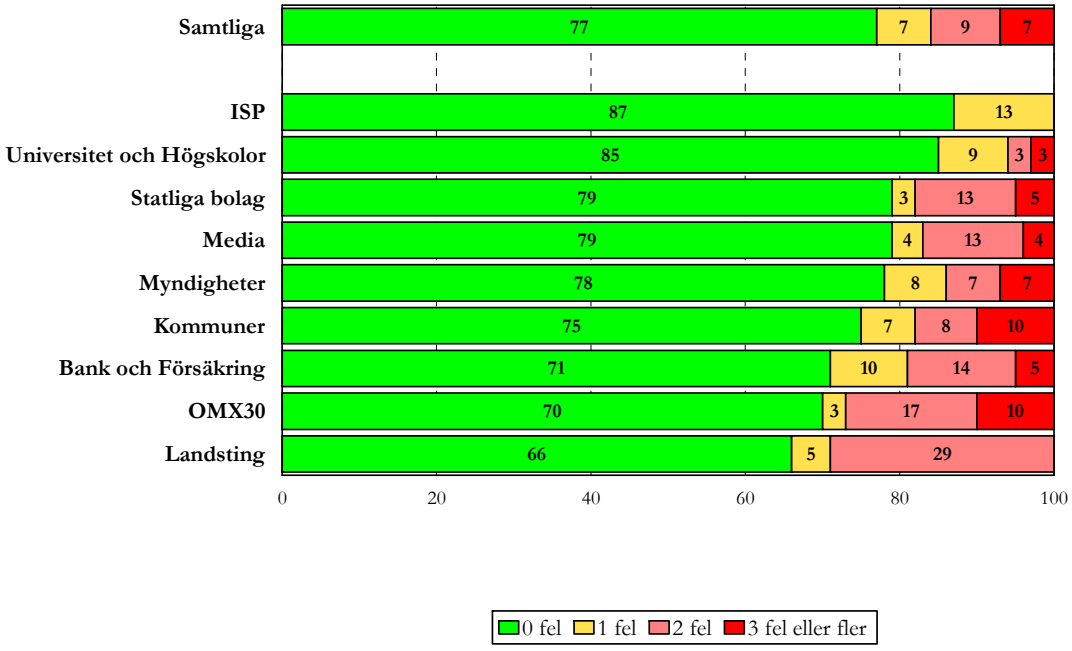
- DNS-servern är rekursiv. DNS-servern svarar på rekursiva anrop från tredje part (så som DNSCheck). Genom rekursiva anrop till en DNS-server som är öppen för rekursion kan en angripare få DNS-servern att slå upp och lägga på minnet information som finns i zoner som kontrolleras av angriparen (se avsnitt 6.7). Således kan DNS-servern tvingas anropa angriparens falska DNS-servrar vilket resulterar i att den angripna DNS-servern cachar och presenterar falsk data.

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

7.2.1 MÄNGDEN FEL PER KATEGORI

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

Tabell 2: Procentuell fördelning av mängden fel per kategori

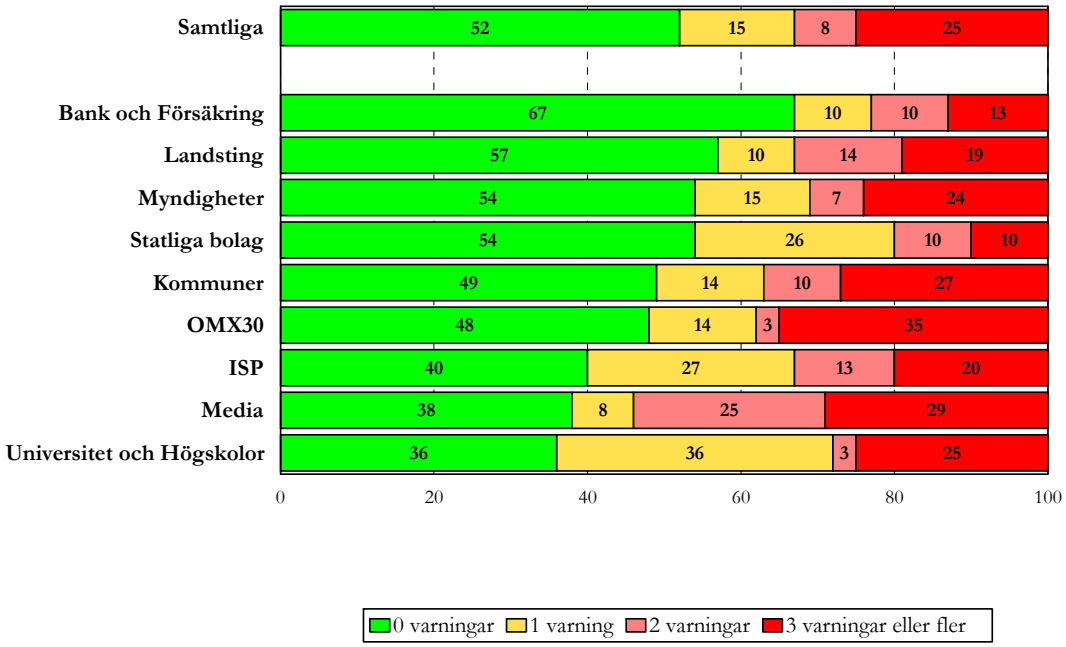


Som vi kanske hade väntat är det Internetoperatörerna samt universitet och högskolor som har den lägsta felprocenten. Där kan vi också förvänta oss att den största kunskapen och kompetensen kring DNS finns, och erfarenhet av hur det drivs och administreras. Liksom tidigare år uppvisar kategorin landsting fortfarande en relativt stor andel fel, 33 procent. Av årets nya kategori OMX30 har också de många fel, 30 procent, och där har 10 procent dessutom tre eller fler fel.

7.2.2 MÄNGDEN VARNINGAR PER KATEGORI

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

Tabell 3: Procentuell fördelning av mängden varningar per kategori



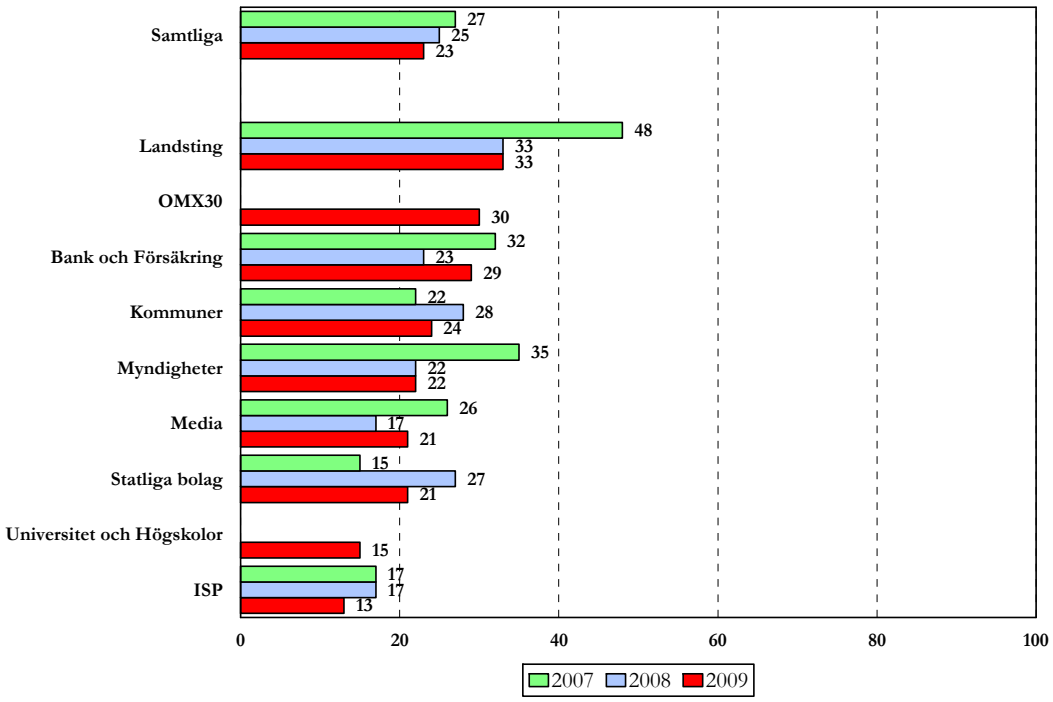
Kategorin universitet och högskolor har flest varningar. Vår bedömning är att det framför allt beror på administrativa brister, som till exempel att e-postadresser som anges i DNS inte fungerar. Det är generellt också mycket vanligare med varningar än med fel. Båda påverkar nåbarheten negativt.

7.3 Jämförelse över tiden - fel och varningar

I och med att vi har sparat rådata från tidigare undersökningar har vi i år också haft en möjlighet att jämföra resultaten mellan årets och de båda tidigare undersökningarna för de kategorier som finns med i undersökningarna för alla tre åren. För de kategorier som är definierade första gången i år kan vi givetvis bara visa 2009 års resultat, det vill säga bara en röd stapel.

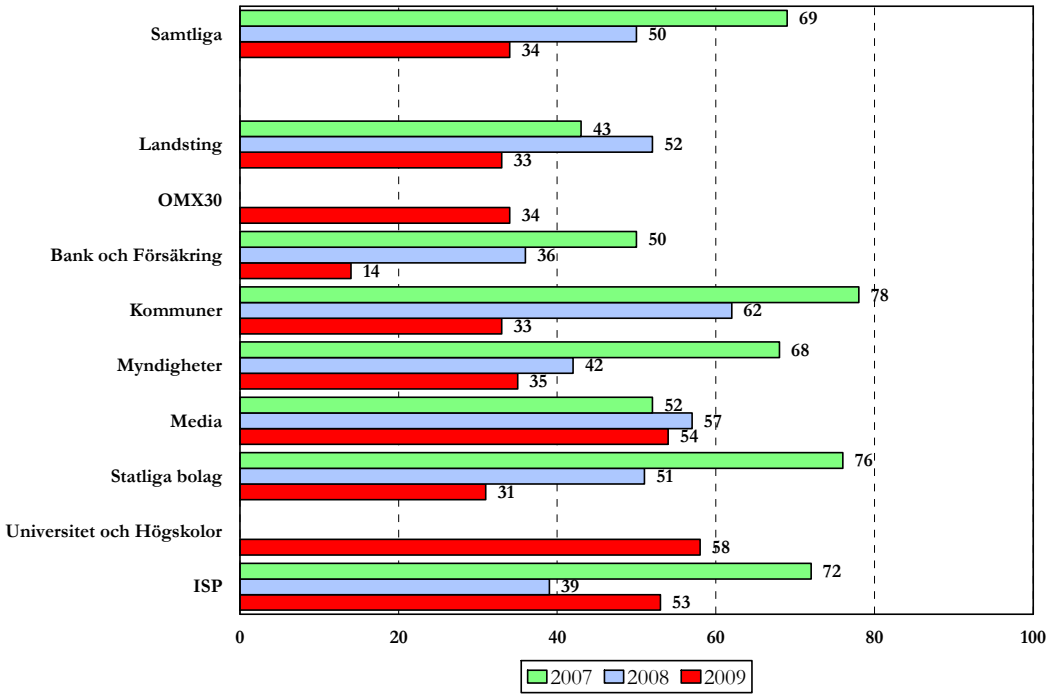
I den första tabellen jämför vi andelen fel över tiden, från 2007 till 2009.

Tabell 4: Andel fel över tiden



Av tabellen kan vi se att situationen generellt har förbättrats jämfört med den första undersökningen. Den är emellertid i princip oförändrad sedan förra året för kategorierna landsting och statliga myndigheter. Situationen har försämrats något hos media, bank och försäkring medan den har förbättrats hos Internetoperatörerna, kommunerna och de statliga bolagen.

Tabell 5: Andel varningar över tiden

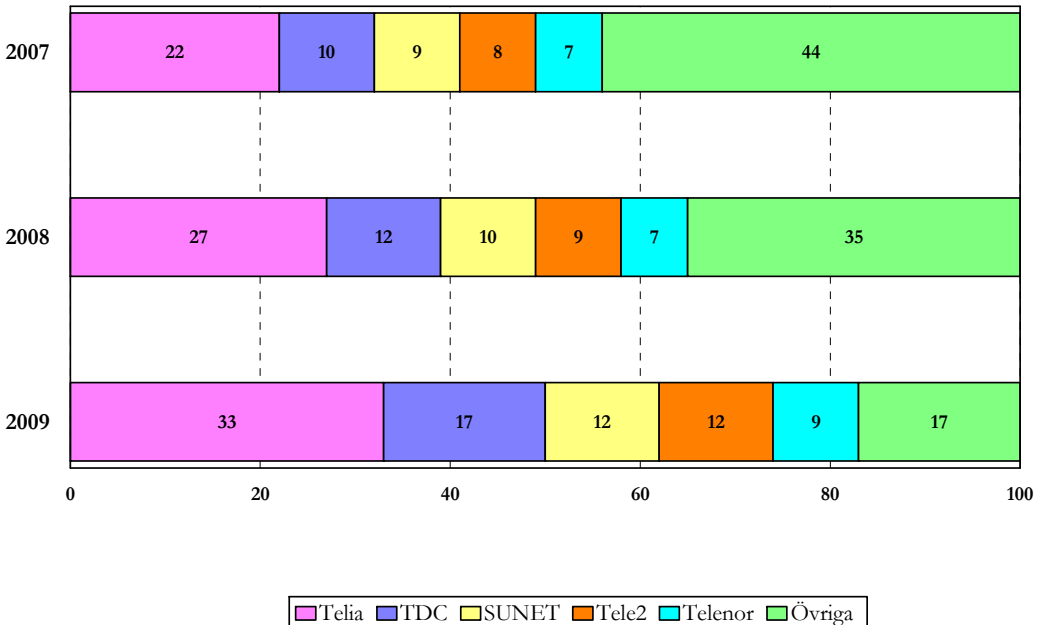


När det gäller varningar har dessa minskat kraftigt mellan 2007 och 2009 om vi ser till helheten. De enda undantagen är kategorierna Media som i princip har varit oförändrat från år till år och Internetoperatörerna där fler än hälften har varningar i år jämfört med 39 procent 2008.

7.4 Anslutning av namnserver till Internet

Vi har också i år liksom tidigare tittat närmare på vilka operatörer som namnservrarna ansluts till för de olika verksamheterna. Tabellen nedan visar alltså inte vilken operatör som driver namnserver för domänerna, utan enbart via vilken operatör namnservern är ansluten till Internet.

Tabell 6: Operatörsvis fördelning – anslutning av namnservrar till Internet.

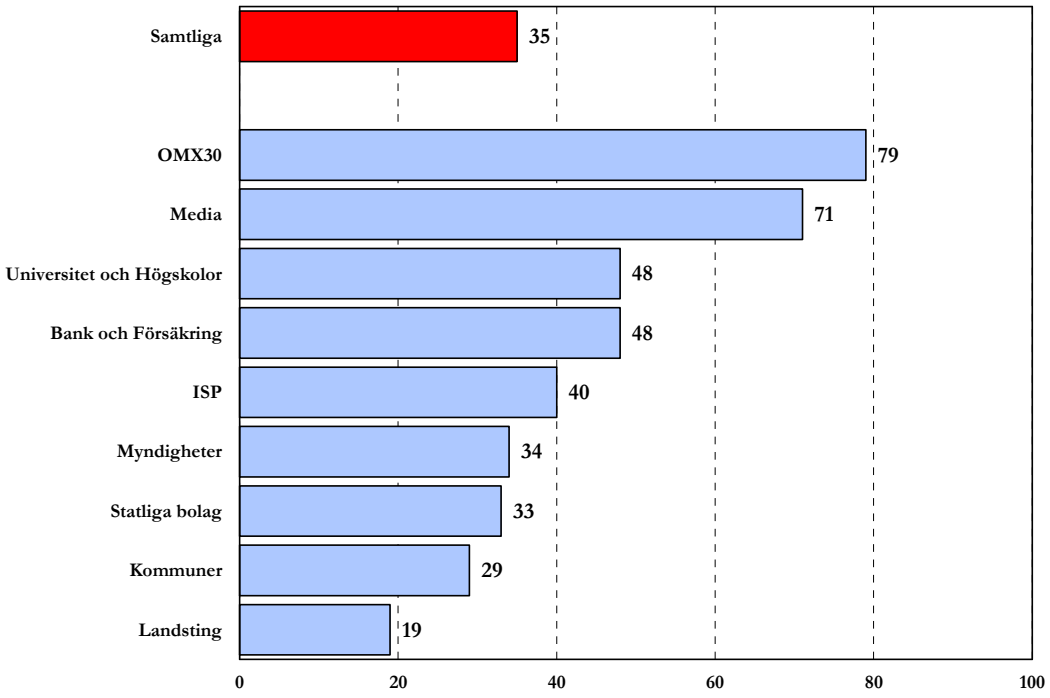


Vi konstaterar att det fortfarande finns en viss spridning bland operatörer när det gäller anslutning av namnservrar om man tittar på den totala mängden domäner. Andelen ”Övriga” har dock minskat kraftigt, från 44 procent 2007 till 17 procent i år. Vi ser en ökning överlag hos de största operatörerna där i synnerhet Telia ser ut att allt mer dominera marknaden och i år har ökat sin andel till 33 procent jämfört med 27 procent förra året.

Förändringarna jämfört med förra året är synbara. Närmare 70 procent av de undersökta domänerna har emellertid alla sina namnservrar stående hos en och samma operatör. Det råder delade meningar om detta är ett problem eller inte, men faktum kvarstår att när operatören får problem med tillgängligheten så riskerar man också att domänen med de underliggande tjänsterna får problem.

Vi har därför också valt att titta närmare på i vilken utsträckning de verksamheter som har flera namnservrar, också har dessa placerade hos en och samma operatör.

Tabell 7: Domäner med namnservrar i fler än ett AS (Autonomt System)



Av tabellen kan vi alltså dra slutsatsen att förhållandevis många verksamheter har sina namnservrar hos en och samma operatör.

Vid en första anblick ser det alltså ut som att vi har en god spridning av driften bland operatörerna, samtidigt förefaller det som om en enskild operatör kan dominera inom en viss kategori. Konsekvensen av det blir i värsta fall att en hel sektor kan drabbas om den dominerande operatören får problem. Därför kan det vara angeläget med en mer detaljerad kartläggning av just den frågeställningen.

7.5 Namnservrar med IPv6

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

De så kallade IP-adresserna, det vill säga den unika nummerserie som identifierar varje uppkopplad enhet på Internet, består av 32 bitar. Därför kan det med IPv4 bara finnas drygt fyra miljarder unika IP-adresser. I takt med att världen blir alltmer uppkopplad uppstår det helt enkelt adressbrist på Internet. Detta problem beräknas bli akut under åren 2010-2011.

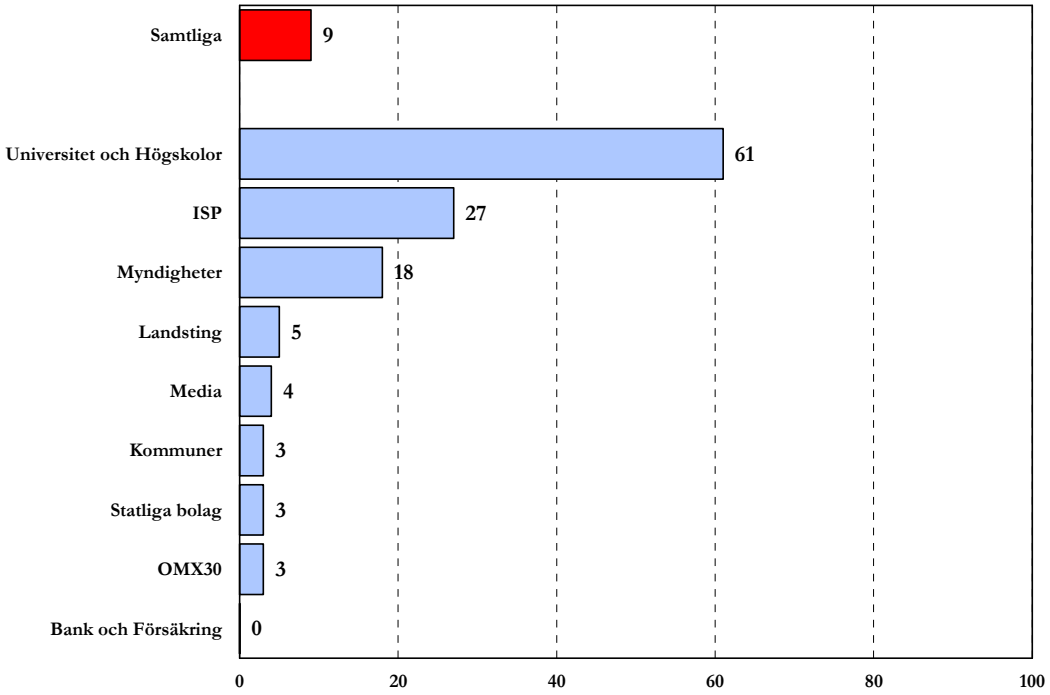
Lösningen för att komma till rätta med adressbristen är att införa en ny version av protokollet, IPv6, med 128 bitar långa adresser. Det råder ingen som helst tvekan om att dessa IP-adresser kommer att räcka och bli över under lång tid framöver när övergången till IPv6 väl har genomförts. Med IPv6 blir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

Från att det med IPv4 inte ens finns en IP-adress per person i världen, skulle varje nu levande individ kunna få 5 x 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.

I år har vi kunnat se en viss ökning av aktiviteten på IPv6-området, även om den fortfarande är mycket begränsad. Nedanstående tabell visar inom vilka kategorier IPv6 har börjat tas i bruk på namnservrar. Även om det som helhet är en mycket liten ökning sedan förra året, ser vi att universitet och högskolor, Internetoperatörer och statliga myndigheter är de kategorier där övergången till IPv6 har kommit längst.

Tabell 8: Använder IPv6 på namnservrar



Totalt 9 procent av de undersökta domänerna har någon namnserver som går att nå via IPv6.

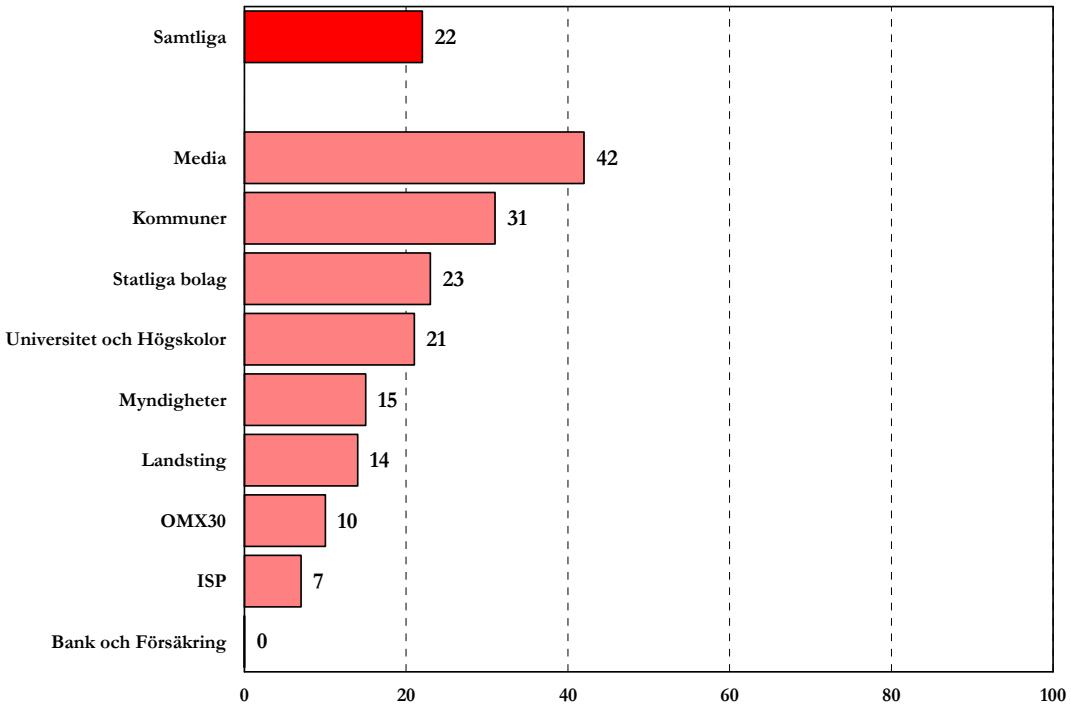
Adressbristen blir snart akut, och det finns de som säger att det är färre månader kvar till adresserna är slut än år det tagit att utveckla protokollet. Det är alltså hög tid att påbörja skiftet till IPv6. Det är det enda sättet att garantera en stabil framtida Internetinfrastruktur. .SE tar en aktiv roll för att underlätta samarbete och samordning kring övergången. Av den anledningen har vi startat en webbplats för att kontinuerligt rapportera om IPv6-aktiviteten i Sverige. Den finns på http://ipv6.iis.se/.

7.6 Namnservrar med rekursion påslaget

Öppna rekursiva namnservrar har mycket få legitima användningsområden. Öppna rekursiva namnservrar kan tvärtom komma att utnyttjas som medel i samband med överbelastningsattacker. En stark rekommendation är därför att eliminera möjligheten att missbruka öppna rekursiva resolvrar med hjälp av de tekniker som beskrivs i de referenser som anges i bilaga 2.

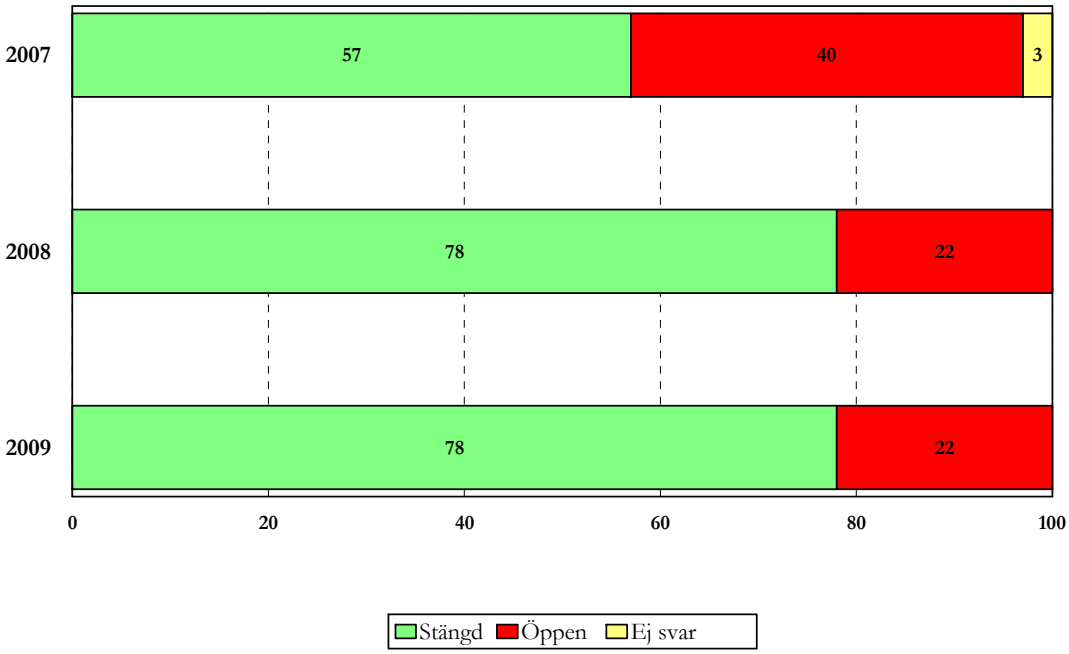
Det är emellertid fortfarande relativt vanligt med namnservrar som är öppna för rekursion, trots de risker det innebär. Allra vanligast är det inom kategorierna Kommuner och Media, vilket framgår av tabellen nedan.

Tabell 9: Namnservrar öppna för rekursion per kategori



Mellan 2007 och 2008 minskade andelen namnservrar med rekursion påslaget markant från 40 till 22 procent. Tyvärr verkar utvecklingen på den här punkten ha stagnerat, och vi har i år lika många namnservrar med rekursion påslaget som vi hade förra året.

Tabell 10: Namnservrar öppna för rekursion 2007-2009



Det har med andra ord inte hänt någonting på det är området mellan 2008 och 2009, trots att vi kunde ha förväntat oss någonting annat inte minst i spåren av den så kallade Kaminskybuggen som gick som en chockvåg över världen (se avsnitt 7.7).

VÄRT ATT VETA

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 en relativt stora mängder data, vilket gör att man normalt sett vill begränsa vem som får använda funktionen rekursion.

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

7.7 Användning av DNSSEC

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

2008 fick forskaren Dan Kaminsky på allvar upp säker DNS på Internetvärldens agenda och .SE fick därmed stort internationellt genomslag för sitt arbete med säkrare DNS-uppslagningar. Redan hösten 2005 signerade emellertid .SE som första landstoppdomän i världen sin zon med DNSSEC och var även först med att 2007 erbjuda en kommersiell DNSSEC-tjänst till sina domäninnehavare, registranterna.

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.

Under 2008 tog intresset för tekniken fart ordentligt. .SE hamnade i hela Internetvärldens blickfång genom att ligga i framkant på området och gärna dela med sig av sina erfarenheter. Detta visade sig bland annat genom det stora intresse vi rönte för ett internationellt DNSSSEC-seminarium som anordnades i oktober 2008 som lockade 150 deltagare, bland annat från 20 toppdomäner runt om i världen.

7.7.1 Vad DNSSEC skyddar mot

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

DNSSEC är till exempel det enda långsiktiga skyddet som kan användas mot den så kallade Kaminskybuggen. .SE har under året informerat om sårbarheter i DNS via en särskild webbplats, http://www.kaminskybuggen.se. Där är det bland annat möjligt att testa om

den resolver man använder är sårbar för Kaminskybuggen, och om DNSSEC används för en domän.

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

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

7.7.2 VAD DNSSEC INTE SKYDDAR MOT

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

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

7.7.3 .SE:S ROLL I DNSSEC

I väntan på att roten, dvs. föräldrazonen till .se, ska bli signerad är .SE:s roll, förutom att signera .SE:s zonfil, att kunna 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.

7.7.4 HUR UTBREDD ÄR ANVÄNDNINGEN AV DNSSEC?

Bland våra undersökta domäner 2009 är knappt tre procent signerade med DNSSEC. Kommuner, landsting och statliga myndigheter är de som går i bräschen för den utvecklingen.

Som jämförelse kan vi nämna att i hela .se-zonen finns det för närvarande totalt knappt 2 000 domäner som har infört DNSSEC, och antalet växer kontinuerligt, men inte i den takt vi skulle önska oss.

Globalt finns det 12 toppdomäner som är signerade, och det finns konkreta planer för signering av roten med en tidplan som pekar på mitten av nästa år.

Mer information om DNSSEC finns i Bilaga 3.

7.7.5 OPENDNSSEC

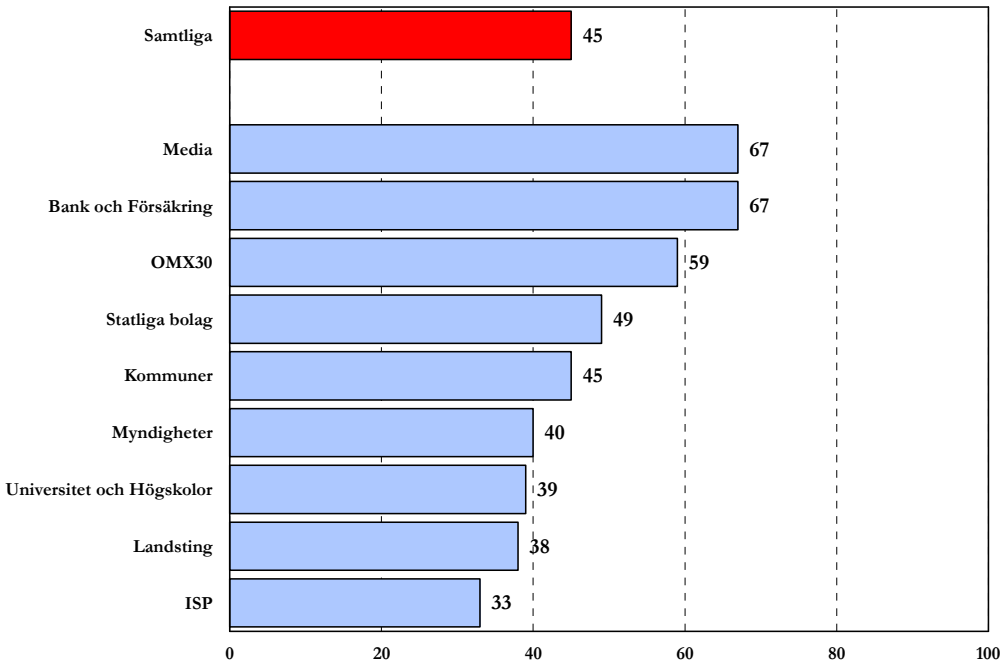
Efter att .SE noterade att bristen på bra och tillgängliga verktyg på marknaden för signering av zonfiler med DNSSEC var ett hinder för många att inleda införandet av DNSSEC påbörjades ett utvecklingsprojekt tillsammans med några av de främsta utvecklarna på området. Resultatet är OpenDNSSEC som är en nyckelfärdig programvara, eller ett verktyg för att underlätta införandet och användningen av DNSSEC. OpenDNSSEC säkrar DNS-informationen momentet innan den ska publiceras på en auktoritativ namnserver. OpenDNSSEC tar en osignerad zonfil, lägger till signaturer och andra poster för DNSSEC och skickar filen vidare till de auktoritativa namnservrarna för den aktuella zonen. Läs mer om OpenDNSSEC i Bilaga 3.

8 Viktiga parametrar för e-post

8.1 Stöd för transportskydd (TLS)

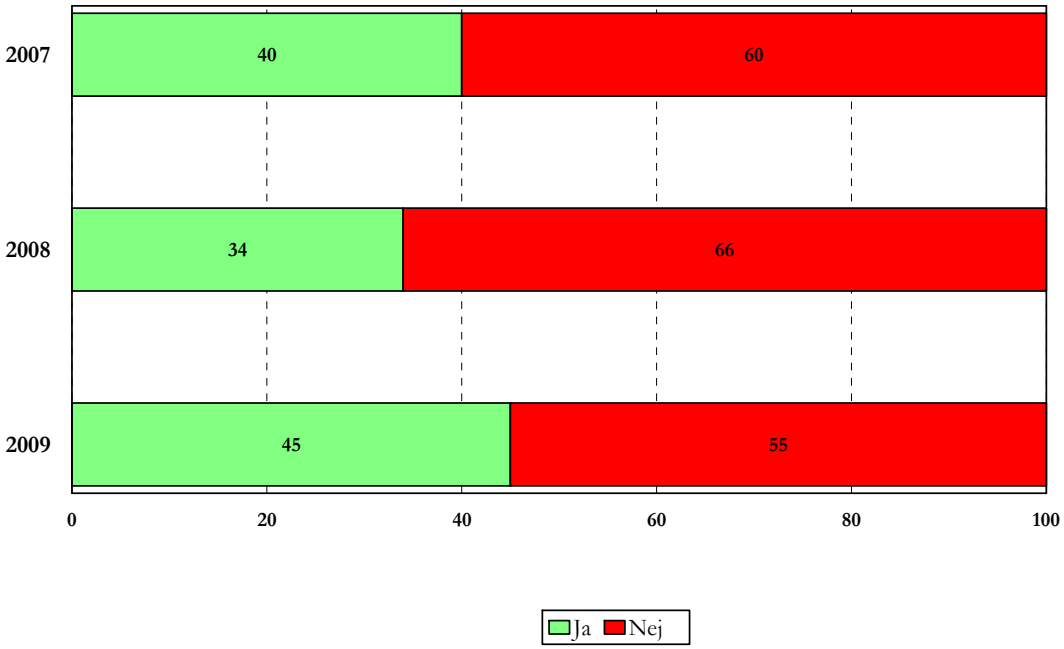
För att säkert utbyta information mellan e-postservrar bör ett transportskydd läggas på kommunikationen. Av de undersökta verksamheterna 2009 har knappt hälften, eller 45 procent, stöd för TLS/SSL i sina e-postservrar. Det betyder att många fortfarande inte vidtar tillräckliga åtgärder för att skydda e-posttrafiken från insyn även om situationen blivit bättre. Alla programvaror har i praktiken inbyggt stöd för det idag.

Tabell 11: E-postservrar med stöd för TLS



Tabellen nedan visar utvecklingen de tre undersökta åren. Vi kan se att andelen e-postservrar med stöd för TLS har ökat under perioden.

Tabell 12: E-postservrar med stöd för TLS 2007-2009



VÄRT ATT VETA

Transport Layer Security (TLS) är en öppen standard för säkert utbyte av information. TLS erbjuder konfidentialitet (kryptering) och riktighet (dataintegritet), samt beroende på användning även äkthetsskydd (källskydd). Äldre versioner av metoden benämns Secure Socket Layer (SSL).

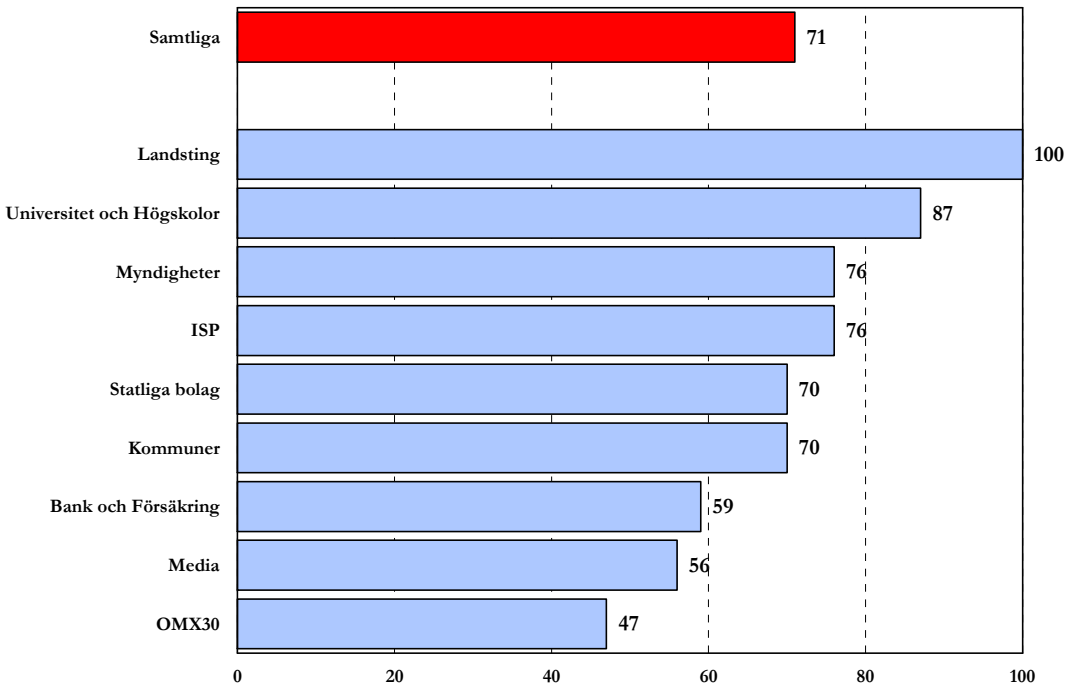
TLS/SSL kan bland annat användas för överföring av elektronisk post (SMTP) och vid upprättandet av en säker förbindelse mellan en webbläsare och en webbplats (HTTPS).

8.2 Placering av e-postservrar

För 2009 och de undersökta verksamheterna har 29 procent sina e-postservrar placerade utanför Sveriges gränser vilket är fler än förra året men färre än 2007.

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

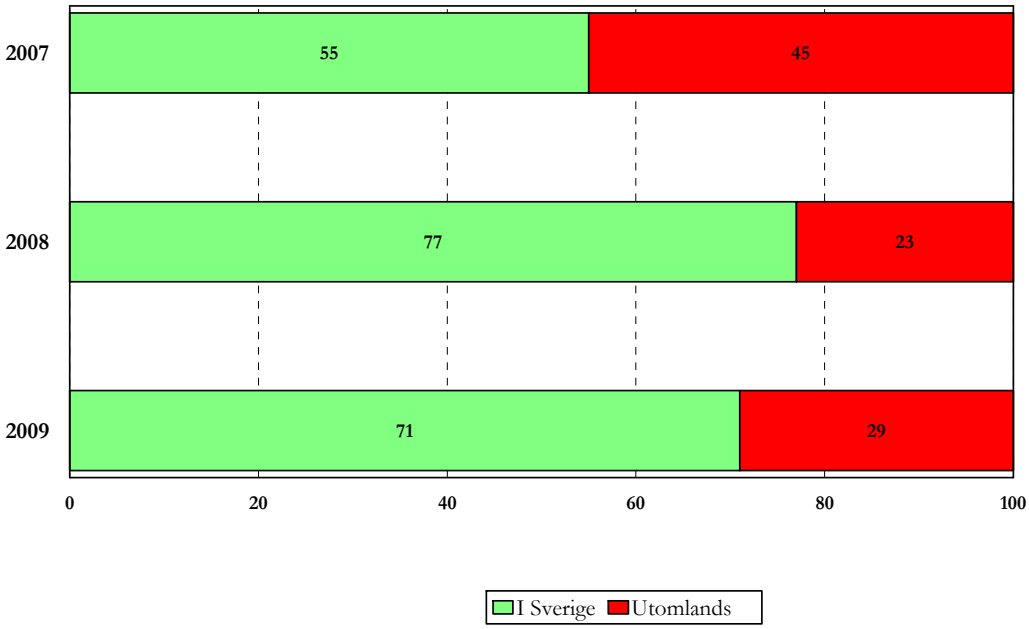
Tabell 13: Andel som har e-postservrar i Sverige



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

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

Tabell 14: Andel som har e-postservrar placerade i Sverige 2007-2009



Av tabellen framgår att andelen e-postservrar placerade utanför landets gränser har ökat sedan förra året. De vanligaste placeringarna utanför Sverige är främst i länder inom EU, men det förekommer även att man har servrarna placerade i USA och Kanada.

Sammanfattningsvis kan vi konstatera att det fortfarande är vanligt förekommande att verksamheter skickar sin e-post utomlands för tvätt.

Samtidigt vet vi att det fortfarande är mycket få 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, däremot kan vi inte säga om de använder funktionen för utgående e-post (avsnitt 8.1).

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 kan få konsekvenser när vi i Sverige ska börja tillämpa det regelverk som formulerats i den mycket omdebatterade FRA-lagen som riksdagen fattade beslut om nyligen. Att ha e-postservrarna i utlandet innebär de facto att informationen passerar landets gränser och sedan kommer tillbaka, vilket gör det mer eller mindre omöjligt att avgöra om det är svensk trafik eller inte.

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

VÄRT ATT VETA

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 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.

8.3 Åtgärder mot skräppost

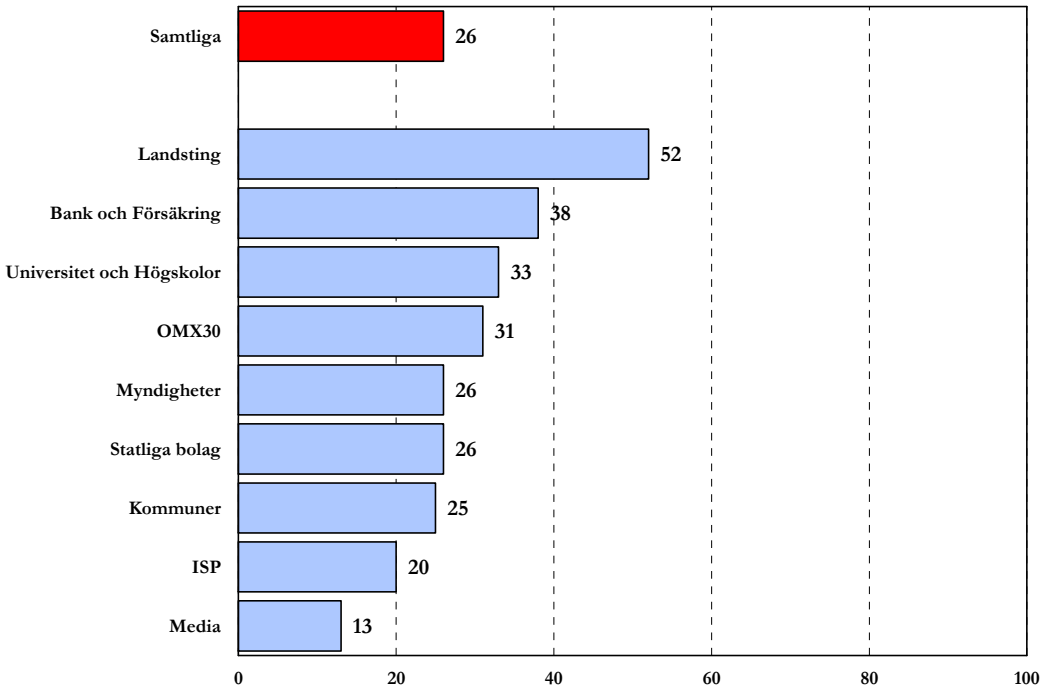
Standardprotokollet för att skicka e-post, SMTP, gör det möjligt att skicka meddelanden med valfri domän som avsändaradress. Det finns några olika lösningar som syftar till att begränsa framkomligheten för skräppost genom att försöka verifiera att det är legitima avsändare bakom ett meddelande.

Sender Policy Framework – SPF

SPF ger domäninnehavaren en 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.

Tabell 15: Använder SPF



26 procent av de undersökta verksamheterna använder SPF. Där ligger landstingen i topp, med över 50 procent.

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

Domain Keys Identified Mail - DKIM

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

På grund av hur standarden för DKIM är utformad går det inte med exakthet att bestämma om en domän använder DKIM eller inte. Men med den mätmetod som vi har använt i undersökningen går det ändå att få ett svar nära verkligheten. 2007 var DKIM-standarden relativt ny och vi kunde då inte se att det fanns någon användning av den värd att notera över huvud taget.

I 2008 års undersökning hittade vi endast två domäner med DKIM påslaget och resultatet för 2009 är i princip lika magert.

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

VÄRT ATT VETA

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

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

DKIM är en relativt ny standard som man kan läsa mer om på http://www.dkim.org.

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.

9 Viktiga parametrar för webb

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

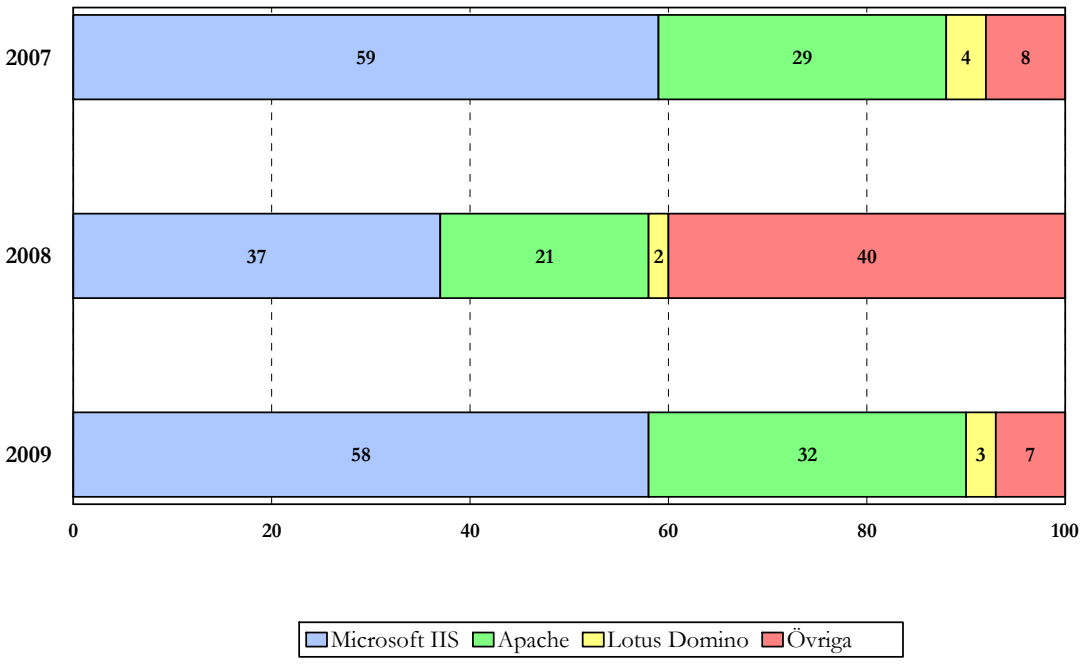
9.1 Anslutning av webbservrar

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

9.2 Programvaror för webbservrar

Även i denna omgång av undersökningen har vi tittat på vilka programvaror för webbservrar som används i de undersökta verksamheterna. De klart dominerande är fortfarande Microsoft Internet Information Server (Microsoft IIS) och Apache. Övriga programvaror har mer eller mindre försvunnit från kartan. Svängningarna mellan 2008 och 2009 är svåra att förklara på något enkelt sätt, utan att dyka djupare ner i materialet. Vi bedömer det i nuläget som mindre intressant. Det som kan vara av intresse att notera är att dominansen av Microsofts programvara bland de undersökta verksamheterna inte har någon motsvarighet varken i .se-zonen som helhet (avsnitt 10) eller internationellt.

Tabell 16: Programvaror som används för webbservrar



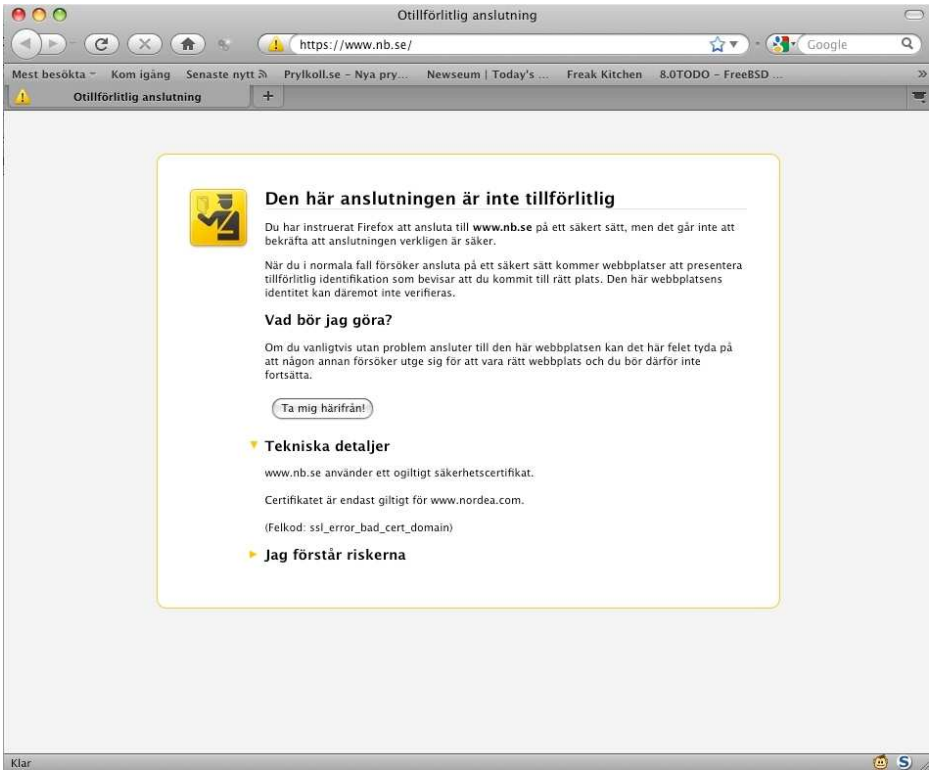
9.3 Stöd för transportskydd

Med hjälp av certifikat och tillhörande krypteringsnycklar kan en webbläsare upprätta en säker, krypterad kommunikation med webbservern.

För en användare som exempelvis vill komma i kontakt med en svensk myndighet eller med sin bank är det viktigt att veta att den server man har kontakt med är rätt server, att anslutningen av någon anledning inte har skett till fel tjänst eller server på grund av felkonfiguration eller något 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. (Se avsnitt 8.1, Värt att veta, för en beskrivning av TLS/SSL).

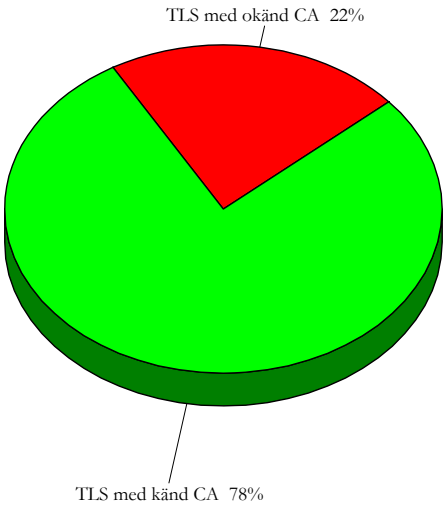
Webbläsaren kontrollerar adressen som uppgivits i webbläsaren med den serveradress som ingår i webbcertifikatet. Om dessa inte stämmer överens, får användaren en varning om att allt kanske inte står rätt till, som exemplet nedan.



Vid 2007 års undersökning hade enbart en fjärdedel av de undersökta webbservrarna stöd för TLS/SSL medan motsvarande siffra för 2008 var tre fjärdedelar. Vi kan inte jämföra undersökningarna över åren då vi i år har ändrat metoden för hur vi kontaktar webbservrarna. I år har vi bara testat vad vi får för svar på en HTTP och HTTPS GET till domännamnen i undersökningsgruppen med "www." placerat framför.

Bland de totalt 663 domäner som ingått i undersökningsmaterialet 2009 finns 165 webbservrar som returnerar något vettigt på frågor som rör certifikat, det vill säga 25 procent. Av dessa 25 procent har 78 procent certifikat som är utgivna av en utfärdare, en Certification Authority, som kan anses vara erkänd och allmänt accepterad, där vår

definition av godkänd innebär att de förekommer i listan över rotcertifikat som finns installerade i webbläsaren Firefox från Mozilla. De flesta certifikaten är utfärdade av certifikatutfärdarna Verisign, Thawte, Equifax och Comodo.



En konsekvens av att använda certifikat som man antingen har utfärdat själv, eller som är utfärdade av en CA som inte anses erkänd eller allmänt accepterad är att besökarna på dessa webbplatser inte har någon möjlighet att verifiera om de har kommit rätt vilket gör skyddet tämligen värdelöst.

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

Av de undersökta webbplatserna kan vi konstatera att fler än 20 har certifikat som är **ogiltiga** på grund av att de inte har förnyats inom giltighetstiden. Ett av dessa certifikat gick ut för fem år sedan, i juli 2004, men används alltså fortfarande eftersom det de facto returnerar svar via https.

Mätningen mot webbservrarna gjordes vid flera tillfällen. Det var intressant att under mättiden hösten 2009 kunna se hur en svensk myndighets certifikat passera sista giltighetstid utan åtgärd från myndighetens sida.

Ett mycket litet antal använder så kallade EV-certifikat (Extended validation), en variant av certifikat som medför utökat visuellt stöd i webbläsarna för att visa att certifikatet är godkänt och att utfärdarna har granskats mer noggrant än vanliga servercertifikat.

Påfallande många använder MD5 som hashalgoritm, en algoritm som olika forskare har utfört lyckade kollisionsattacker på, vilket innebär att de har lyckats generera ett falskt SSL-certifikat som kan användas för att skapa certifikat för en godtycklig webbplats. Följden är att en webbläsare inte kan upptäcka förfalskningen utan godkänner dessa falska certifikat och visar ett stängt hänglås som markerar en säker anslutning, utan varningar.

VÄRT ATT VETA

MD5 är en hashfunktion som tar en godtyckligt lång bitsträng och skapar ett "fingeravtryck" av bestämd längd. En viktig egenskap för en hashfunktion är att en liten förändring i bitsträngen ska ge ett helt annat resultat. Hashvärdet (resultatet) ska inte avslöja något om innehållet i bitsträngen. Med andra ord ska hashfunktionen vara en envägsfunktion, vilken är lätt att beräkna åt ena hållet men svår, för att inte säga omöjlig, att knäcka andra vägen. En kollision inträffar när två olika bitsträngar ger samma hashvärde. En digital signatur består av ett hashvärde, som i RSA är krypterat med den privata nyckeln. Signaturen valideras genom att jämföra hashvärdet som räknats fram på nytt med hashvärdet som dekrypterats med den publika nyckeln. Om kollisioner kan genereras är det alltså möjligt att förfalska en signatur. Svagheterna i MD5 har varit kända sedan slutet av 1990-talet. Genomförda attacker undanröjer alla tvivel om att MD5 måste ersättas.

Ett fyrtiotal domäner använder sig av så kallat wild card-certifikat eller certifikat som inte är relaterade till domännamnet. Ett wild card SSL-certifikat aktiverar SSL-kryptering på flera subdomäner med hjälp av ett och samma certifikat, förutsatt att domänerna kontrolleras av samma organisation och har samma huvuddomän. Det är långt ifrån riskfritt att dela certifikat mellan domäner bland annat för att:

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

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

Fem av de granskade certifikaten är användbara som CA, Certification Authority, så att det går att skapa nya certifikat från dessa certifikat.

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

Det förvånade oss att hanteringen av certifikat i undersökningsgruppens webbmiljö håller så 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 hade vi förväntat oss bättre resultat, framför allt med avseende på att använda 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, vilka tillsammans utgör någonting mellan 25-33 procent gör att det inarbetas dålig säkerhetskultur hos Internetanvändare vilket motverkar själva grundidén med servercertifikat – nämligen att helt säkert veta att man står i förbindelse med rätt server.

Alla som via sin webbplats begär någon form av information från användare, såsom inloggning, personuppgifter, användaruppgifter, betalinformation, kreditkortsnummer, telefonnummer m.m. bör använda sig av TLS/SSL med certifikat utfärdade av allmänt

accepterade certifikatutfärdare som finns installerade i de vanligaste webbläsarna. Det behöver finnas någon som internt ansvarar för bl.a. bevakning av när certifikat går ut och ska förnyas. Därutöver kan man tänka på att:

- Använd så långa RSA-nycklar som möjligt.
- Nyttja EV-certifikat där det är möjligt.
- Använd inte wild card-certifikat för webbtjänster, speciellt inte för utkontrakterad drift på webbhotell eller molntjänster där det inte finns någon egen kontroll över nyckelmaterial och certifikat.
- Använd hårdvarustöd för att spara privat nyckel för känsliga webbservrar.

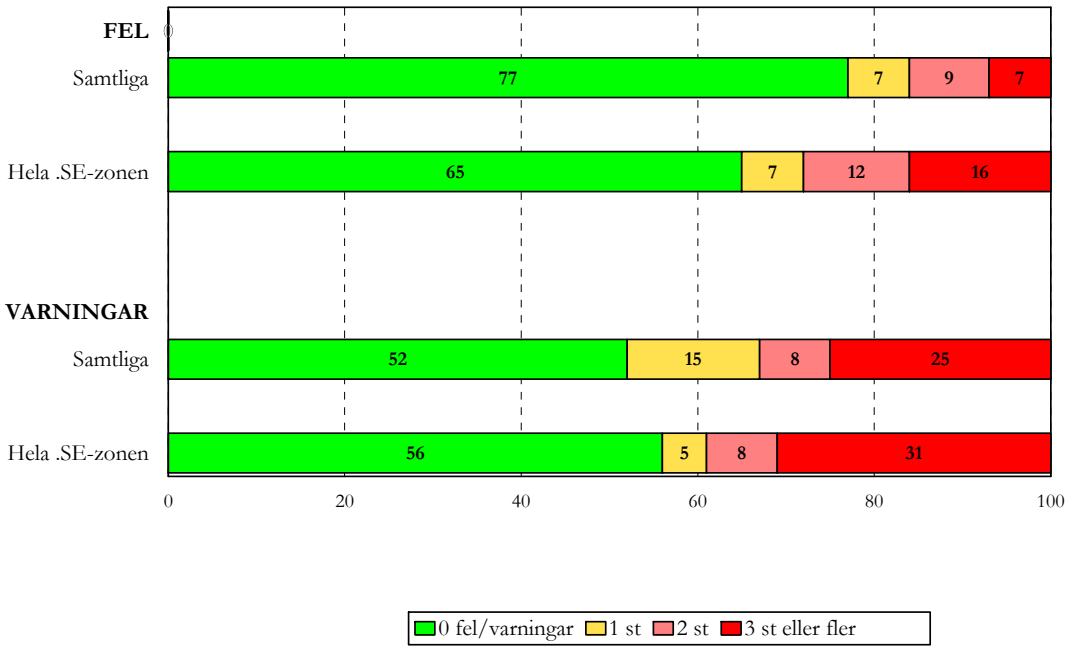
På http://www.networking4all.com/en/support/tools/site+check/ kan den som använder sig av certifikat för att skydda webbtjänster själv testa om sajten har bra säkerhet med avseende på SSL.

10 Jämförelse med .se-zonen som helhet

För att se om vår undersökningsgrupp är bättre eller sämre än .se-zonen som helhet har vi i årets undersökning gjort ett utsnitt av att antal slumpmässigt valda domäner ur .se-zonen för att jämföra med. I tabellerna nedan representerar ”Samtliga” den aktuella undersökningsgruppen medan ”Hela .se-zonen” representerar det slumpmässiga urvalet på 10 000 domäner ur en version av zonfilen från den 1 oktober 2009.

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

Tabell 17: Andel fel och varningar



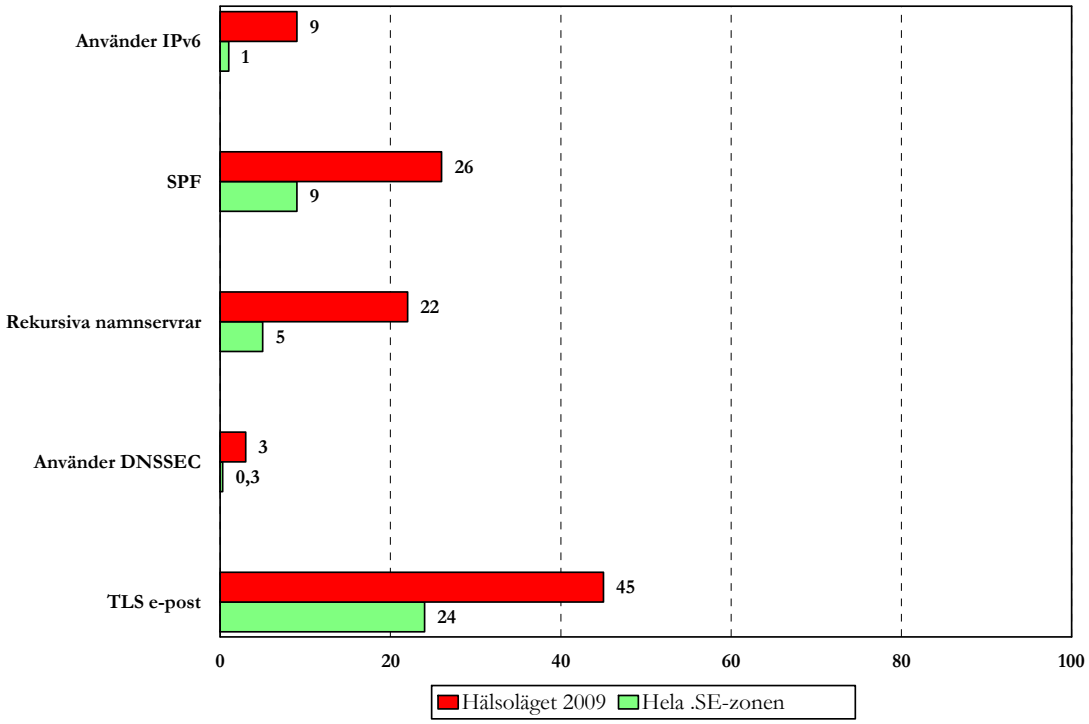
Som det ser ut är det inte några stora skillnader, även om antalet fel verkar vara färre i vår undersökningsgrupp än i .se-zonen som helhet.

De stora skillnaderna ser vi först när vi tittar på de andra specifika områden vi har granskat närmare förutom de parametrar som vi förknippar med DNS-kvalitet enligt definitionen i avsnitt 5. I undersökningsgruppen är det fler som använder SPF, det är fler som har öppna rekursiva namnservrar, fler som använder DNSSEC och fler som skyddar sin e-post med TLS. Vilka slutsatser vi kan dra av det är inte alldeles uppenbart. För det behöver vi göra fler och mer specifika undersökningar.

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

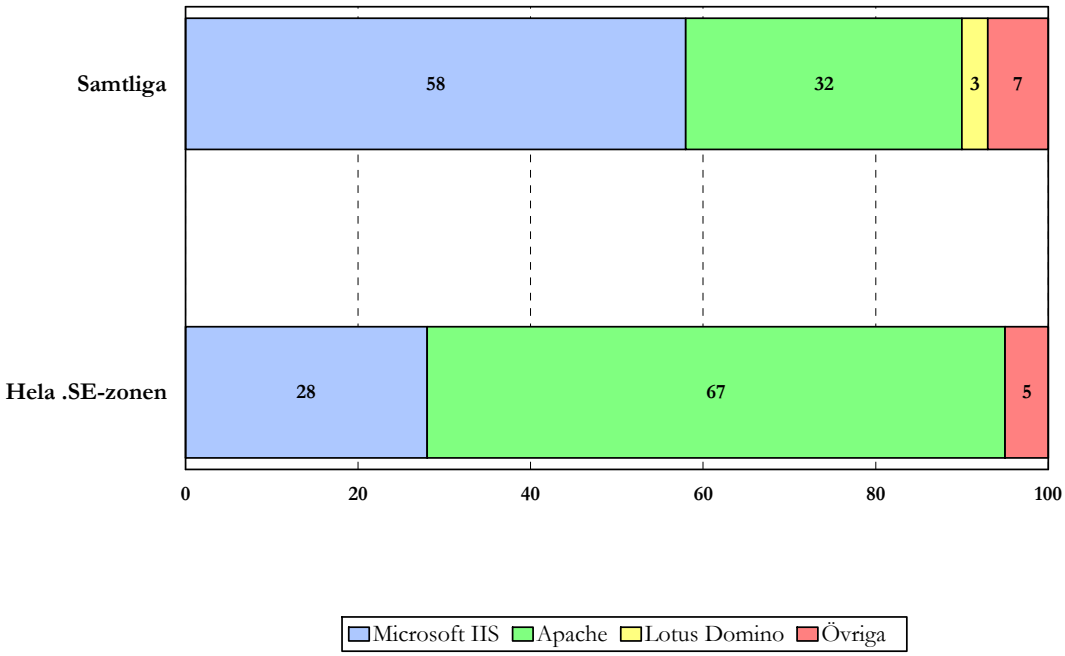
kommuner och statliga myndigheter har ramavtal med leverantörer som baseras på kravspecifikationer där IPv6 ingår som ett krav.

Tabell 18: Använder IPv6



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

Tabell 19: Programvaror för webbservrar



11 Råd och rekommendationer

Efter att ha genomfört en ny omgång tester med ett relativt likartat resultat jämfört med 2008 ser vi fortfarande samma starka behov av mycket större samordning mellan olika intressenter för bättre säkerhet på den svenska delen av Internet och inte minst möjligheter till mycket stora effektivitetsvinster och kostnadsbesparingar.

I första hand verksamheterna inom den offentliga förvaltningen anser vi bör kunna enas om rekommendationer och en handlingsplan för genomförandet av nedanstående 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.

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

- Upprätta en gemensam funktion för virustvätt och rensning av skräppost placerad inom landet. Det skulle bli effektivare och förmodligen spara resurser. Samtidigt skulle det förhindra att myndighetsinformation lämnar landet.

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

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

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

- Göra samtliga tjänster tillgängliga över IPv6 och planera långsiktigt för en systematisk övergång till IPv6 inom hela den offentliga förvaltningen.

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

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

Bilaga 1 - Branschstandard för DNS-tjänst med kvalitet

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

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

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

http://dnscheck.iis.se/

1. Minst två namnservrar

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

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

Konsekvens: När den enda servern eller den enda operatören får ett avbrott blir DNS-tjänsten onåbar för den domän som ligger på servern eller i operatörens nät. Därmed kan man inte heller nå tjänster hos 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 införda även i den zonfil som "tar emot" ansvaret, och som innehåller övriga data om zonen. Listorna måste hållas synkroniserade, så att alla NS-poster som förekommer i föräldrazonen också återfinns i barnzonen. Listan i föräldrazonen uppdateras inte automatiskt, utan endast efter "manuell" anmälan till ansvarig registreringsenhet. Vid förändring som leder till behov av ändring i överliggande zon ska

underliggande zons administrativa kontaktperson utan dröjsmål se till att registreringsenheten meddelas om detta.

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

3. AUKTORITET

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

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

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

4. SERIENUMMER FÖR ZONFIL

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

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

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

5. KONTAKTADRESS

Rekommendation: Zonkontaktadressen i SOA-posten ska vara nåbar.

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

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

6. NÅBARHET

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

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

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

Bilaga 2 - Öppna rekursiva namnservrar

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

Pekare till mer information

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

Secure Domain Name System (DNS) Deployment Guide
http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.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/downloadables/11

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 3 – Mer information om DNSSEC

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

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

Det råder 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.

Sverige var med .se först i världen med att få igång en fungerande implementation av DNSSEC. .SE:s DNSSEC-tjänster och -produkter presenteras under nedanstående logga.

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

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

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

Här finns några pekare till ytterligare information:

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

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

Regelbundna nyheter sprids av **DNSSEC Deployment Initiative**
http://www.dnssec-deployment.org/

Utvecklingsprojekt – OpenDNSSEC

DNS är relativt komplicerat, och så även elektroniska signaturer, kombinationen av dessa båda i DNSSEC är givetvis också den komplicerad. Syftet med OpenDNSSEC är att hantera dessa svårigheter och att lyfta dem från systemoperatörens axlar efter att denne väl har satt upp systemet.

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

OpenDNSSEC utvecklas inom ramen för ett samarbete mellan .SE, Nominet, NLNet Labs, SIDN, SURFnet, Kirei och John Dickinson. Mer information finns på http://opendnssec.se. Programvaran som är öppen går också att ladda ner och testa från den webbplatsen.

http://www.opendnssec.org/