Nåbarhet på nätet

Hälsoläget i .SE 2008

Stiftelsen för Internetinfrastruktur

1 Introduktion 3

1.1 Detta dokument 3
1.2 Förkortningar och ordförklaringar 3

2 Sammanfattning 5

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 och observationer 10

6.1 Testobjekt 10
6.2 Observationer – tester av DNS 11
6.3 Användning av DNSSEC 16
6.4 Viktiga parametrar för e-post 18
6.5 Viktiga parametrar för webb 23

7 Råd och rekommendationer 26

1 Introduktion

1.1 Detta dokument

Dokumentet är en rapport från en undersökning som .SE genomfört 2008 för att se hur det är beskaffat med kvaliteten och nåbarheten i domännamnssystemet (DNS) i .se-zonen och en del andra viktiga funktioner för domäner i .SE. Årets undersökning är till stora delar, men inte fullständigt, en uppföljning av motsvarande undersökning som genomfördes 2007.

Dokumentet riktar sig främst till IT-strateger och IT-chefer, men givetvis också till alla andra med ansvar för drift och förvaltning av en verksamhets 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 .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, *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 som 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 förälderzon 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 Internet användare.

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

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

SPF Sender Policy Framework (SPF). 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.

TLS/SSL SSL är en standard för kryptering av bland annat webbtrafik under transport. http över 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

Efter förra årets något nedslående resultat kring hur det var ställt med hälsoläget i .SE har vi valt att upprepa undersökningen även 2008 för att se om det går att spåra effekten av några av de råd och rekommendationer som vi delade med oss av, och om det kan tänkas det föranlett några åtgärder bland de undersökta verksamheterna.

Förra årets undersökning bekräftade att det generellt brister i kunskap om vad som krävs för att hålla en hög kvalitet på t.ex. domännamnssystemet (DNS), även om man givetvis kan diskutera vad som är ”hög kvalitet”. Vi har valt att definiera nivån efter vad som rekommenderas som praxis internationellt, *Best Common Practice*. Det finns också anledning att tro att dessa bristande kunskaper också gäller kompetens när det gäller drift och operativt ansvar.

.SE har i år företagit en ny undersökning och liksom förra året har vi i första hand undersökt DNS-kvalitet. Men, liksom förra året, har vi också passat på att titta på några andra viktiga parametrar för exempelvis e-post och webb. Undersökningen är genomförd under september-oktober 2008.

Testerna har omfattat totalt 671 domäner och 912 unika namnservrar eller 1870 namnservrar om man räknar dem per domän. En namnserver hos en operatör kan som bekant härbärgera flera domäner.

Vi har försökt hålla oss till ungefär samma population som den som undersöktes förra året, men förändringar har skett, vilket ger en inte alldeles jämförbar bild mellan 2007 och 2008.

I fjol undersöktes t.ex. 828 domäner och i år 671. Den främsta orsaken till det lägre antalet domäner är att vi i år valt att inte ta med de börsnoterade bolagen. Motivet till detta är att bl.a. att observationerna från undersökningen av börsbolagen 2007 var mer positiva än för den offentliga förvaltningen och vi ser därför inget skäl att ha dem med i årets undersökningsunderlag. Andra förändringar är att vissa myndigheter lagts ner, medan andra har kommit till.

Nytt för året är vidare att vi använt en bättre och mer utvecklad programvara för DNSCheck, vilket förmodligen också bidrar till att vi inte kan få alldeles jämförbara observationer för de båda åren. Med utgångspunkt från den programvaran har .SE i årets undersökning gjort automatiserade körningar mot en förutbestämd mängd .SE-domäner och dessutom gjort vissa kompletterande undersökningar när det gäller tjänster som elektronisk post och webb.

Vi har också lagt till undersökningar om vilka vanligaste programvaror som används, och om det finns några dominerande aktörer på marknaden.

Av 671 testade domäner klassades 621 som samhällsviktiga. Av dessa hade 28 procent allvarliga fel som bör åtgärdas snarast och 57 procent brister av en karaktär som genererar varning.

Våra observationer tyder på att det har skett en del förbättringar inom flera områden, men att det fortfarande finns en hel del arbete kvar att göra.

3 Om undersökningen

.SE har ansvar för drift och administration av alla namnservrar för se-domänen och har lång och gedigen erfarenhet av sådant arbete. På basis av egna och andras misstag och erfarenheter har det successivt vuxit fram en Best Common Practice för domännamnssystemet som kan tillämpas även i andra miljöer än på toppdomännivån.

.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 de först ser över och strukturerar sin egen DNS-infrastruktur som helhet.

Av det skälet är vi intresserade av att ta reda på hur väl förberedda domäner i .SE är. Vi är också intresserade av att se på hur verksamheter hanterar sin kommunikation i övrigt, främst när det gäller e-post och webbtrafik.

Under 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 programvaror används, vad är de största synderna, vilka är de värsta syndarna?

- Hur hanterar verksamheten sin e-post? Står servrarna i eller utanför Sverige, vem är tjänsteleverantör, accepteras TLS/SSL (transportskydd), används SPF (en teknik att minska mängden skräppost)? I år har vi även valt att titta på hur utbredd användningen av DKIM är (även det en teknik för att minska mängden skräppost).

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

Testerna har genomförts på domäner och namnservrar för ett stort antal viktiga verksamheter i samhället; affärsverk och statliga bolag, banker och finansföretag, Internetoperatörer, kommuner, landsting, medieföretag och statliga myndigheter inklusive länsstyrelser, totalt 671 domäner.

Själva datainsamligen har varit helt automatiserad och har omfattat tester av förekomsten 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 värsta synderna begås och vad det kan få för konsekvenser. I år har vi i alla fall delvis också haft möjlighet att jämföra med tidigare resultat, vilket gör det möjligt att dra några slutsatser om utvecklingen på området.

Till det knyter vi 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 som lämpliga att gå vidare med och utreda mer i detalj. Dessa har inte ändrat sig från förra årets undersökning, men vi skulle gärna se att myndigheter i beslutande ställning tar emot förslagen och vidtar åtgärder.

.SE har finansierat och drivit undersökningen. Rapporten har sammanställts av Anne-Marie Eklund Löwinder, kvalitets- och säkerhetschef på .SE. Programmeringen för och det praktiska genomförandet av testerna har utförts på .SE:s uppdrag av Jakob Schlyter, Kirei AB. Granskning 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 DNS, eller domännamnssystemet, fungerar. När en domän (även kallad zon) skickas till DNSCheck så 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 test, så som att kontrollera DNSSEC-signaturer, att de olika värdarna går att komma åt och att IP-adresserna är giltiga.

Verktyget finns tillgängligt för användning på http://dnsscheck.iis.se.

5 DNS-tjänst med kvalitet

Vår definition av kvalitet i DNS-tjänsten har inte förändrats sedan förra undersökningstillfället. Det är viktigt att den egna DNS-infrastrukturen ansluter till 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 en annan 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 t.ex. domännamnssystemet (DNS), även om man givetvis kan diskutera vad som är ”hög kvalitet”. Det finns anledning att tro att dessa bristande kunskaper sannolikt också omfattar drift och operativt ansvar. Det faktum att några av de värsta försyndelserna fortfarande är relativt vanligt förekommande ger oss emellertid en indikation om att situationen inte har förbättrats nämnvärt från förra året.

5.1 Vad innebär kvalitet i DNS-tjänsten?

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

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

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

6 Tester och observationer

De genomförda testerna har omfattat såväl domänernas konfiguration och de namnservrar som svarar på frågor om domänen. De har också omfattat några av dem som vi bedömer allra viktigaste parametrarna för e-post och webb. Vid testerna har en programvara använts som automatiskt kontrollerar de olika kontrollpunkter som angivits i vår branschstandard för samtliga domäner som ingått i undersökningen, som helhet och per kategori. Programvaran har utöver detta kompletterats med frågor bland annat kring hantering av elektronisk post och webb.

6.1 Testobjekt

Testerna har omfattat totalt 671 domäner och 912 unika namnservrar. 1870 namnservrar har ingått i undersökningen om man räknar dem per domän. Testobjekten har grupperats i kategorier på följande sätt:

- Affärsdrivande verk och statliga bolag (42)
- Banker och finansbolag (20)
- Internetoperatörer (ISP) (16)
- Kommuner (289)
- Landsting (21)
- Medieföretag (23)
- Statliga myndigheter, inklusive länsstyrelser (exkl. myndigheter under Riksdagen) (260)

De statliga myndigheterna och bolagen har dessutom placerats i olika klasser beroende på hur kritisk deras verksamhet bedöms vara, med en mycket grov uppskattning. T.ex. har vi klassat museer och universitet och högskolor som mindre viktiga ur ett samhällsperspektiv än t.ex. Skatteverket och Försäkringskassan.

Av 671 testade domäner ingår 621 i den viktigaste klassen, och av dessa hade 28 procent allvarliga fel som bör åtgärdas snarast och 57 procent brister av en karaktär som genererar varning.

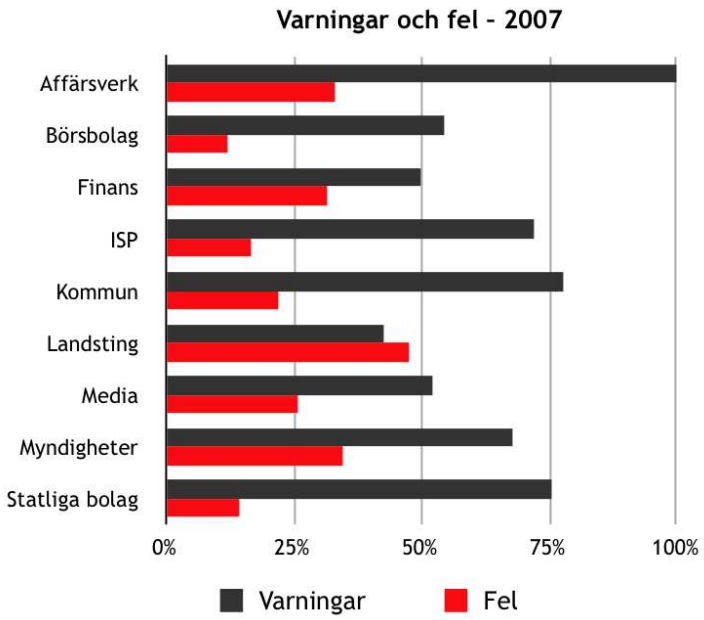
VÄRT ATT VETA

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.

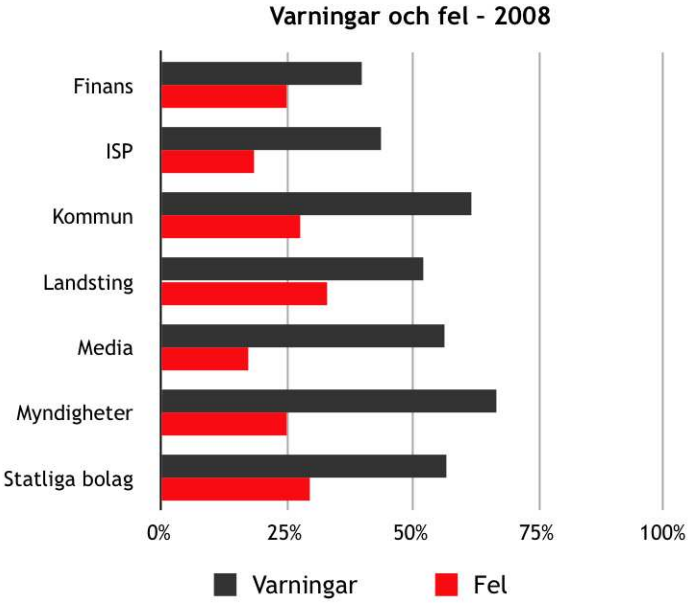
Varningar: Varningar är också fel som kan påverka driften, men åtgärder bedöms inte vara lika akuta, även om de givetvis skulle höja kvaliteten.

6.2 Observationer – tester av DNS

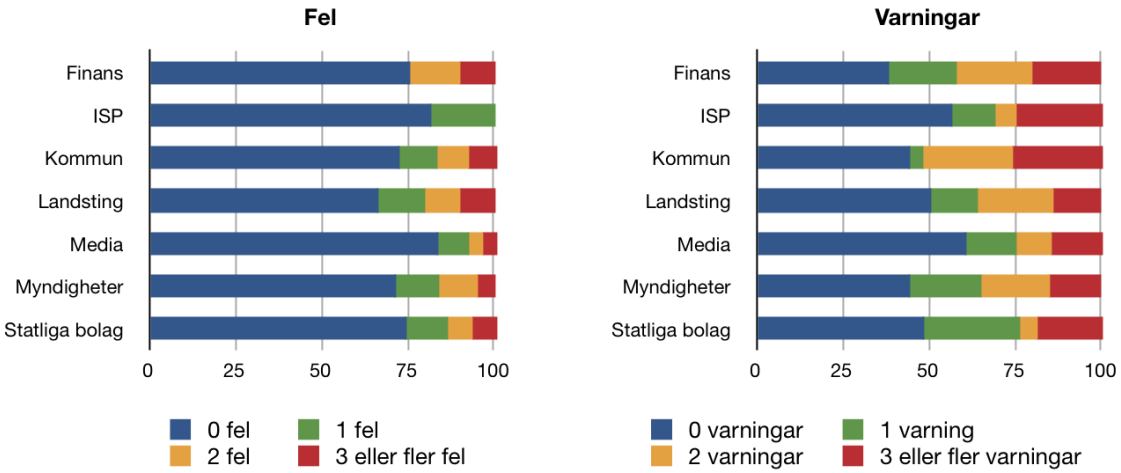
Först visar vi hur fel och varningar fördelade sig vid förra årets undersökning, även om populationen inte är densamma. Men det ger ändå en möjlighet att jämföra skillnaderna mellan de båda undersökningarna för de kategorier som finns med båda åren.



I årets undersökning redovisas fel och varningar enbart för klass 1, dvs. alla verksamheter som vi betraktar som samhällsviktiga. Hur fel och varningar fördelar sig mellan de olika undersökta kategorierna framgår av nedanstående tabell:



Det är lätt att konstatera att situationen har förbättrats en hel del sedan förra årets undersökning. Vad som dessutom är intressant att se är hur mängden fel och varningar fördelar sig per kategori.



Vi kan av tabellen ovan 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. Av den anledningen har vi även grund för en stark misstanke om att tillgängligheten till information och tjänster är sämre än vad den skulle behöva vara.

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 en felaktigt konfigurerad brandvägg. Det är en ganska vanlig missuppfattning att DNS inte behöver kunna kommunicera enligt TCP-protokollet om den inte tillhandahåller zonöverföringar - kanske är inte namnserverns administratör medveten om att TCP oftast är ett krav. Detta är en indikation på att den som har konfigurerat namnservern inte har tillräcklig kunskap om DNS.

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

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

  - En DNS-server finns listad i förälderzonen men inte i barnzonen. Det här är troligtvis ett administrationsfel. Förälderzonen 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, t.ex. i förbindelsen till namnservern eller att servern inte har någon korrekt angiven IP-adress.

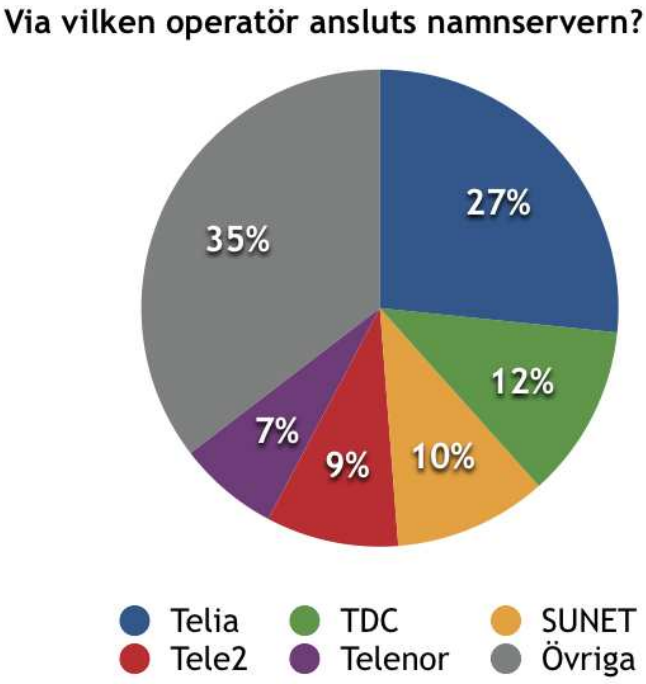
- Endast en DNS-server hittades för domänen. Det bör alltid finnas minst två DNS-servrar för en domän för att kunna hantera tillfälliga problem med förbindelserna. Om den enda servern eller förbindelsen till den skulle sluta fungera så blir tjänsterna som pekas ut från namnservern också otillgängliga.

- 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 6.2.3). 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.

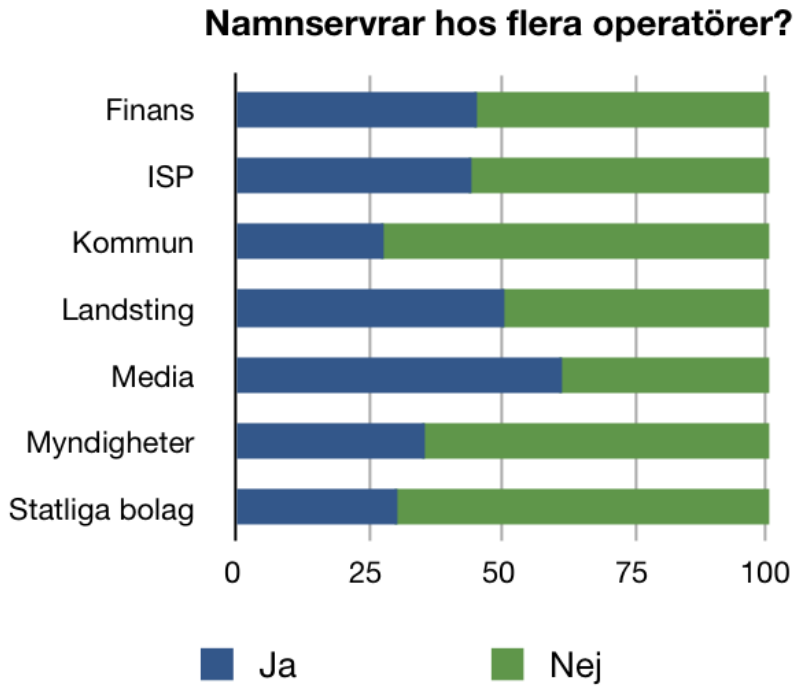
6.2.1 Anslutning av namnserver till Internet

Vi kan konstatera att det fortfarande finns en viss spridning bland operatörer när det gäller anslutning av namnservrar om man tittar på den totala mängden domäner. Ingen operatör verkar dominera marknaden. Telia är störst med totalt 27 procent. Skissen nedan visar alltså inte vem som driver namnserver för domänen, utan enbart via vilken operatör namnservern är ansluten till Internet.



Förändringarna jämfört med förra året är marginella. Närmare 70 procent av alla domäner har emellertid alla sina namnservrar stående hos en och samma operatör. Det råder delade meningar om detta är ett problem eller inte, men faktum är att när operatören får problem 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 har dessa placerade hos en och samma operatör.



Av bilden ovan går det alltså att dra slutsatsen att förhållandevis många verksamheter har sina namnservrar hos en och samma operatör. Går vi djupare in i resultatet per kategori kan vi göra följande observation när det gäller val av operatör för namnservrar:

- Av kommunerna har 38 procent åtminstone en namnserver hos Telia.
- Av landstingen har 57 procent åtminstone en namnserver hos TDC.

Därav kan vi sluta oss till att även om det som helhet ser ut som att vi har god spridning bland operatörerna så förefaller det som om en enskild operatör ändå 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.

Som kuriosa kan vi även nämna att 8 procent av de undersökta domänerna har någon namnserver som går att nå via IPv6, vilket är glädjande och tyder på att spridningen av IPv6 börjar komma igång. 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 2010-11.

Lösningen för att komma till rätta med adressbristen är att införa en ny version av protokollet, IPv6, med 128 bitar långa adresser. Med IPv6 kommer adresserna att räcka för överskådlig framtid. En riklig tillgång till IP-adresser öppnar också upp för applikationer som annars blir svåra att förverkliga i praktiken.

6.2.2 DNS-PROGRAMVAROR

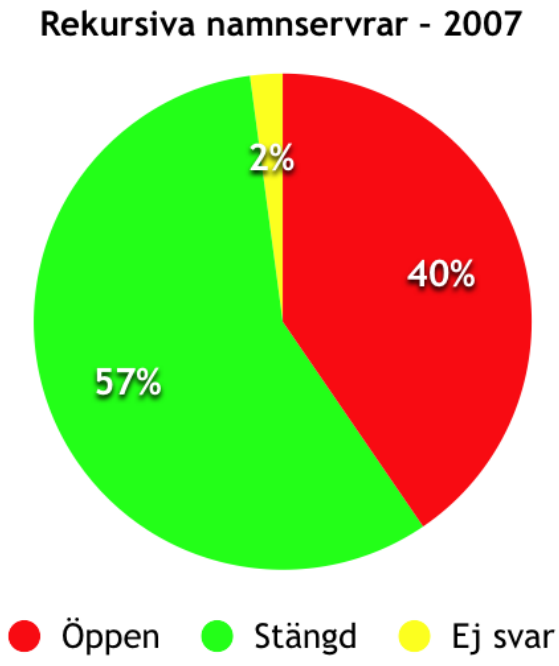
Vi har i år inte försökt ta reda på vilken programvara namnservrarna kör. Det finns inga nya programvaror som har lanserats sedan förra året, bara nya versioner av befintliga programvaror.

Vi rekommenderar förstås ännu starkare i år att de verksamheter som fortfarande använder ISC BIND 8 snarast uppgraderar till senaste versionen av BIND 9, då BIND 8 är behäftad med allvarliga säkerhets- och andra brister. Leverantören Internet Systems Consortium (ISC) informerade dessutom i augusti 2007 att BIND 8 har nått "end of life" och inte längre underhålls. Det innebär att fel i programvaran, t.ex. säkerhetsbrister, inte längre kommer att åtgärdas.

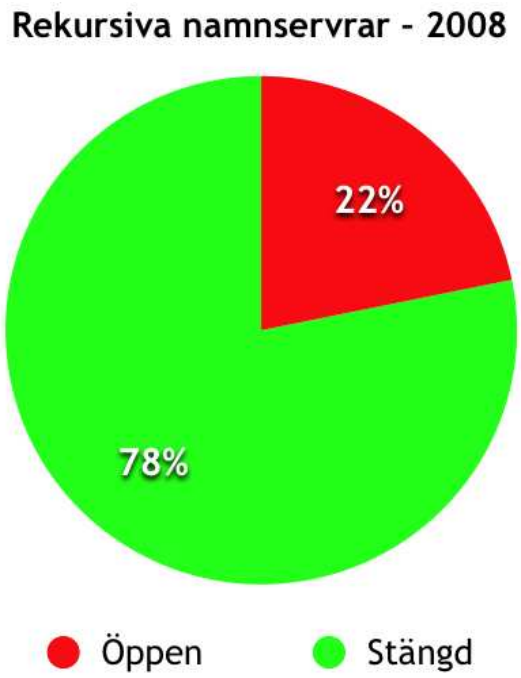
BIND 9, som ersätter BIND 8, är betydligt säkrare samt har bättre funktionalitet och prestanda i jämförelse med tidigare versioner. Använder man den version av BIND som distribueras med operativsystemet så finns det med största sannolikhet en uppgradering att tillgå via den egna leverantören.

6.2.3 NAMNSERVRAR MED REKURSION PÅSLAGET

En mycket stor andel (40 procent) av de undersökta namnservrarna hade rekursion påslaget 2007.



I år är andelen betydligt lägre, 22 procent, vilket är ett stort steg i rätt riktning.



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

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 (dvs. ta datorkapacitet) och resultera i en relativt stor mängd 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 t.ex. utföra tillgänglighetsattacker via den öppna namnservern genom att låta den ställa frågor som kommer att resultera i ovanligt stora svar. Detta i kombination med en falsk avsändaradress som leder till att svaret skickas någon annanstans kan utgöra en tillgänglighetsattack.

6.3 Användning av DNSSEC

DNSSEC, vilket står för DNS Security Extensions, är en utökning av DNS i syfte att göra säkrare uppslagningar på Internetadresser för exempelvis webb och e-post. Den ökade betydelsen av DNS har gjort att DNSSEC blivit allt mer aktuellt.

Till skillnad från det vanliga domännamnssystemet (DNS) 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 tjänsten är att domännamnsinnehavaren ska kunna säkra sina domäner med DNSSEC. .SE erbjuder sedan 2006 möjligheten att använda DNSSEC.

6.3.1 DNSSEC – VAD DET SKYDDAR MOT

Syftet med DNSSEC är att säkerställa innehållet i DNS. DNSSEC innebär att användaren kan 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 .t.ex. det enda långsiktiga skyddet som kan användas mot den s.k. Kaminskybuggen. .SE planerar att informera mer om sårbarheter i DNS via en särskild webbplats som lanseras inom kort. Där kommer det bland annat att vara möjligt att testa om den resolver som används är sårbar för Kaminskybuggen, och om DNSSEC används för en domän.

För gemene man innebär DNSSEC att risken för att bli lurad minskar 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. Det är endast konstruerat för att förhindra attacker där angriparen manipulerar svar på DNS-frågor för att uppnå sitt mål.

6.3.2 DNSSEC - VAD DET INTE SKYDDAR MOT

Fortfarande finns det mängder av andra säkerhetsluckor 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 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 t.ex. attacker på IP- eller nätnivå.

6.3.3 .SE:S ROLL I DNSSEC

I väntan på att root ska bli signerad så är .SE:s roll förutom att signera .SE:s zonfil också 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 jämförligt med hanteringen av NS-poster i DNS.

6.3.4 HUR UTBREDD ÄR ANVÄNDNINGEN AV DNSSEC?

Bland våra undersökta domäner 2008 är det ännu bara åtta som har infört DNSSEC. Av dessa är sex kommuner och två statliga myndigheter.

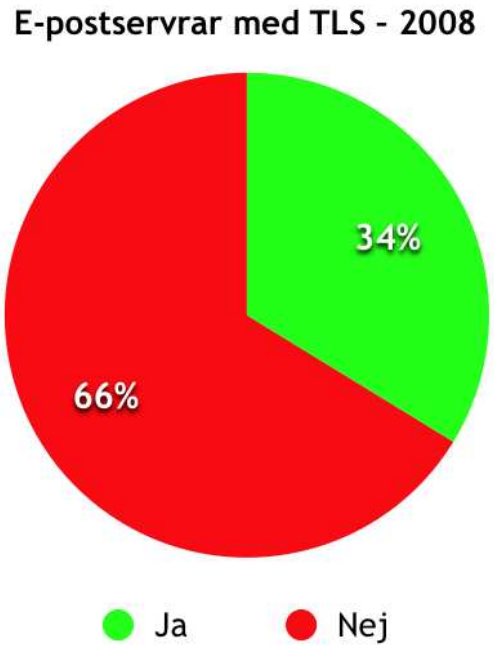
Som jämförelse kan vi nämna att i hela .SE-domänen finns det för närvarande totalt 891 domäner som har infört DNSSEC. Glädjande nog så växer det antalet ganska snabbt.

Mer information om DNSSEC finns i Bilaga 3.

6.4 Viktiga parametrar för e-post

6.4.1 STÖD FÖR TRANSPORTSKYDD

Av de undersökta verksamheterna 2008 så hade 34 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. Alla programvaror har i praktiken inbyggt stöd för det idag.



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 bl.a. användas för överföring av elektronisk post (SMTP) och vid upprättandet av en säker förbindelse mellan en webbläsare och en webbplats (HTTPS).

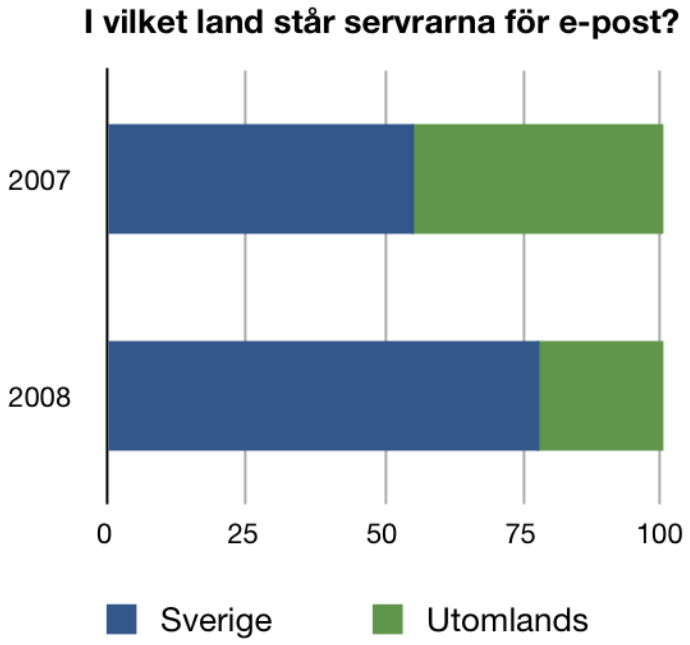
6.4.2 PLACERING AV E-POSTSERVRAR

Ett testresultat som fortsätter att överraska oss är när vi tittar på var verksamheterna har sina e-postservrar placerade. För 2008 och de undersökta verksamheterna är det 23 procent som har sina e-postservrar placerade utanför Sveriges gränser. Det är dock färre i år än vid förra undersökningen.

Anledningen till placeringen är förmodligen fortfarande densamma, dvs. att man anlitar någon leverantör för filtrering av virus och SPAM. Det innebär att en stor del av bl.a. den offentliga förvaltningens e-postkommunikation passerar ett främmande land på sin väg till mottagaren.

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

Kategori	**Antal servrar**	**Placerade inom landet (%)**
Landsting	41	100
Myndigheter	628	85
ISP	26	81
Bank och försäkring	43	74
Statliga bolag	79	71
Kommuner	484	69
Media	50	68
Affärsverk	8	38



De vanligaste placeringarna utomlands är främst länder inom EU, men det förekommer även att man har servrarna placerade i USA och Kanada.

Sammanfattningsvis kan vi konstatera att det fortfarande förekommer 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 34 procent av de undersökta domänerna accepterar transportskydd med kryptering för inkommande e-post, däremot kan vi inte säga om de använder funktionen för utgående e-post (avsnitt 6.4.1).

Det vi vill visa med denna del av undersökningen är att detta kan få implikationer för när vi i Sverige börjar tillämpa det regelverk som formulerats i den mycket omdebatterade FRA-lagen. 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.

Inte nog med det, 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.

När det uppstår kommunikationsproblem mellan Sverige och omvärlden innebär det som ytterligare en komplikation att dessa företag och myndigheter har problem att nå varandra.

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 skall kunna läsa, inte ens de som ansvarar för e-postsystemet (dvs. "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 göra en analogi med traditionell postgång. De två vanligaste metoderna för denna typ av kryptering är PGP och S/MIME.

6.4.3 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** klarar en SPF-validering.

Testerna 2008 visade att 84 procent av domänerna som ingick i underlaget inte använder sig av SPF, trots att detta är både förhållandevis enkelt och fullt möjligt att införa. Det innebär att det är enkelt för vem som helst att ange t.ex. en myndighets domän som avsändaradress för att lura mottagaren, utan att denne har någon möjlighet att upptäcka det. SPF tillför en sådan möjlighet till upptäckt.

Domain Keys Identified Mail - DKIM

DomainKeys Identified Mail (DKIM) är en standard som skyddar utvalda 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, vilket 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 via avsändarens DNS. I skrivande stund är utvecklingen av ADSP i sitt slutskede och är på väg att bli en standard.

På grund av att ADSP ännu inte är en fastställd standard är det få som använder ADSP tillsammans med DKIM. Genom att leta efter de publika DKIM-nycklarna kan man dock 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 så går det inte med exakthet att bestämma om en domän använder DKIM eller inte. Men med den mätmetod som använts 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 årets undersökning har vi tittat på om användningen av DKIM har ökat sedan förra undersökningen. Dessvärre verkar utvecklingen på den kanten gå mycket långsamt. Endast två domäner med DKIM påslaget hittades i undersökningen 2008.[1]

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 detta kallas Domain Keys Identified Mail (DKIM). DKIM bygger till skillnad från SPF på kryptografi, genom att avsändarens postkontor signerar (stämplar) all utgående post. Mottagarna kan i sin tur verifiera stämpeln.

DKIM är en relativt ny standard, och används så vitt vi kan se ännu inte i någon större omfattning. Läs mer om DKIM på http://www.dkim.org.

Både SPF och 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.

[1] Rickard Bondesson från Linköpings Universitet har genomfört ett examensarbete hos .SE. Examensarbetets syfte har varit att undersöka och utvärdera DKIM Milter, som av .SE har utökats med DNSSEC-stöd. DKIM Milter är en implementation av DKIM-standarden och fungerar tillsammans med bland annat Sendmail och Postfix, två olika e-postservrar. I undersökningen ingår funktionstester, hotanalyser, interoperabilitetstester samt statistikinsamling. Rapporten från examensarbetet kommer att finnas på www.ep.liu.se i slutet av november 2008.

6.5 Viktiga parametrar för webb

Det finns åtgärder som kan vidtas för att se till att ha redundans även för webbtjänsten. Det kan vara bra att överväga dessa om det är en kritisk funktion som tillhandahålls via webb.

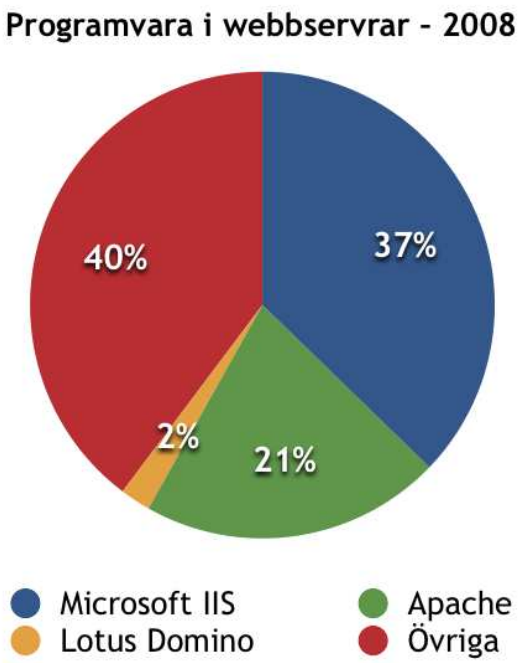
6.5.1 Anslutning av webbservrar

Har man alla namnservrar anslutna till en och samma operatör spelar det ingen roll om man lägger webbservern där också. Får operatören problem så blir webbservern onåbar. Har man sina namnservrar placerade hos två olika operatörer så kan man också överväga att placera webbservern hos en tredje operatör för att få största möjliga redundans.

99 procent av de 1685 webbservrarna som ingår i underlaget för de undersökta domänerna står placerade i Sverige.

6.5.2 Programvaror för webbservrar

Vi har också i år 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. I Sverige är fördelningen Apache 21 procent och Microsoft IIS 37 procent. Internationellt har emellertid Apache 50 procent av marknaden medan Microsoft står för 34. (Källa: Netcraft, september 2008).



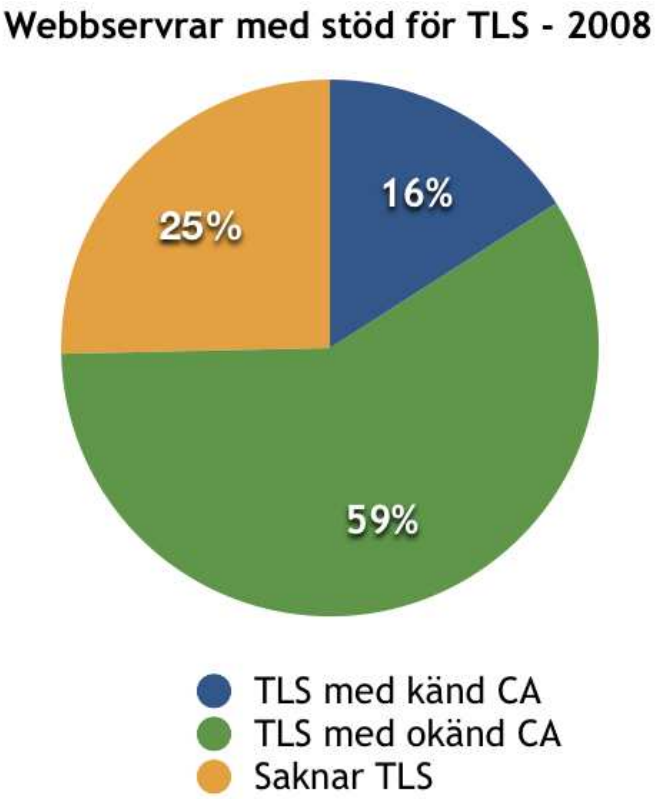
6.5.3 Stöd för transportskydd

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 p.g.a. felkonfiguration eller medvetet bedrägeri.

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 ovan 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.

Till skillnad från 2007 års undersökning då enbart en fjärdedel av de undersökta webbservrarna hade stöd för TLS/SSL är motsvarande siffra för 2008 cirka tre fjärdedelar.



Av de totalt 1685 webbservrar som ingått i undersökningsmaterialet skyddas alltså 722 av någon typ av certifikat. Av dessa har dessvärre bara lite drygt 100 certifikat som är utgivna av en utfärdare, en Certification Authority, som kan anses vara erkänd och allmänt accepterad.

En konsekvens av detta är att besökarna på de webbplatser som har ett certifikat som är utfärdat antingen av någon okänd aktör eller av domäninnehavaren själv, inte kan verifiera om de har kommit rätt vilket gör skyddet tämligen värdelöst.

En bristfällig användning av webbcertifikat undergräver trovärdigheten av denna typ av säkerhetslösningar.

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

7 Råd och rekommendationer

Efter att ha genomfört en ny omgång tester med ett relativt likartat resultat 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 en tidplan för genomförandet av nedanstående aktiviteter:

- Anslut kritiska resurser i Sverige till flera operatörer samtidigt, t.ex. med användning av tekniken Anycast. Det finns behov av att någon på central nivå bestämmer vad som är att betrakta som en kritisk resurs.

- Upprätta en central sekundär DNS-drift för kritiska tjänster exempelvis via de svenska Internetknutpunkterna. 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 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 inom Sverige för att skydda spårbarheten av information mellan myndigheter.

- Organisera en central nationell CA-funktion för certifikatbaserade tjänster för myndigheter. En sådan central funktion grundad på tillit kan utgöra en gemensam certifikatutfärdare för till exempel statliga myndigheter. Det är en funktion som går att upphandla hos någon etablerad och känd CA vilken kan få i uppdrag att upprätta en sub-CA för t.ex. gruppen svenska myndigheter.

- 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 långsiktigt planera för en systematisk övergång till IPv6 inom hela den offentliga förvaltningen.

Utöver ovanstående åtgärder så finns det ytterligare åtgärder som behöver vidtas bl.a. på operatörsnivå för att stärka infrastrukturen för Internet. Dessa åtgärder landar huvudsakligen på Post- och Telestyrelsen, PTS, såsom tillsynsansvarig myndighet, och handlar om att ställa krav på hos operatörerna. Vi är medvetna om att sådant arbete redan pågår, men vill ändå betona vikten av att sådana åtgärder genomförs.

Bilaga 1 - Branschstandard för DNS-tjänst med kvalitet

För den mer tekniskt bevandrade läsaren har vi 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. 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 spridda så att de är placerade på olika operatörsnät i olika autonoma system (AS).

Förklaring: För varje underliggande domän skall det finnas minst två fungerande namnservrar. De skall 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 någon 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 skall 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 skall samtliga finnas införda i den underliggande zonen.

Förklaring: I den överliggande zonen används NS-poster för att överlåta ansvaret för en viss domän till andra servrar. Denna lista av datorer skall 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 zonfilen för toppdomänen också återfinns i den underliggande domänen. Listan i den överliggande zonfilen uppdateras inte automatiskt, utan endast efter "manuell" anmälan till ansvarig registreringsenhet. Vid förändring som leder till behov av ändring i överliggande zon skall underliggande zons administrativa kontaktperson utan dröjsmål se till att registreringsenheten meddelas om detta.

Konsekvens: Om den överliggande zonen innehåller information om den underliggande zonen som inte existerar i den underliggande zonen 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 skall svara auktoritativt för domänen.

Förklaring: Vid kontroll mot servrarna för underdomänen skall man kunna få konsistenta 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 skall 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 skall 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 enkel kontroll skall 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 p.g.a. 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 (kompletteras?)

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

Securing an Internet Name Server **http://www.cert.org/archive/pdf/dns.pdf** En bra praktisk sammanfattning för systemadministratören.

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

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

ISC BIND **http://www.isc.org/sw/bind** Här finns källkod och binärer för BIND samt länkar till mycket intressant och matnyttig information.

BIND 9.3 Administrator Reference Manual **http://www.isc.org/sw/bind/arm93** Innehåller exempel på konfigurering, praktiska tips och detaljerad beskrivning av funktioner i BIND.

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 året så uppmärksammade Kaminskybuggen.

Det råder inget tvivel om att DNS behöver bli säkrare. – DNSSEC 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/products/sednssec2.

. .SE planerar att informera mer om sårbarheter i DNS via en särskild webbplats som lanseras inom kort. Där kommer det bland annat att vara möjligt 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:

Under denna länk samlas en hel del information om DNSSEC och utvecklingen av både användning och verktyg.
http://dnssec.net

Under denna länk återfinns en praktiskt inriktad guide till hur man gör för att införa DNSSEC.
http://www.nlnetlabs.nl/dnssec_howto/

Utvecklingsprojekt

http://www.opendnssec.se/

Stiftelsen för Internetinfrastruktur (.SE) ansvarar för Internets svenska toppdomän, .SE. Kärnverksamheten är registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret under .se. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige. Genom .SE:s Internetfond avsätter stiftelsen varje år medel till projekt som på olika sätt bidrar till Internets utveckling och användning. Se mer på www.iis.se

.se

Stiftelsen för Internetinfrastruktur