Nåbarhet på nätet - Hälsoläget i .se 2014

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

Innehåll

1 Introduktion

För åttonde gången i ordningen har .SE genomfört sin årliga undersökning av nåbarhet på nätet och hälsoläget i .se. Undersökningen 2014 är liksom tidigare år till stora delar, men ändå inte fullständigt, en uppföljning av de tidigare undersökningarna som genomförts sedan 2007.

Syftet med undersökningen är att kartlägga och analysera kvaliteten och nåbarheten i framför allt domännamnssystemet (DNS) i .se-zonen och några andra viktiga funktioner för domäner registrerade i .se. Genom att undersökningen har genomförts flera år i följd kan vi också visa på utveckling och trender inom flera av de undersökta områdena.

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

Undersökningen görs både på ett urval av domäner som representerar viktiga funktioner i samhället och på ett slumpmässigt urval motsvarande en procent av samtliga domäner i .se.

Att undersöka kvaliteten på internets infrastruktur i Sverige är i linje med stiftelsens urkund som säger att vi ska bidra till en positiv utveckling av internet. Främst gör vi detta genom att peka på områden för förbättringar men även genom att förse marknaden med verktyg där man själv kan kontrollera status för domäner i olika avseenden.

Det här året har vi också kartlagt status för filtrering av e-post och om e-postservrar står placerade inom eller utanför Sveriges gränser. I årets rapport redovisar vi dessutom resultatet av en något fördjupad undersökning och analys inom området internationaliserade domännamn, IDN, det vill säga domännamn med andra tecken än a-z, 0-9 och bindestreck (-) och i vilken utsträckning det används i undersökningsgruppen.

2014 blir det sista året som vi genomför Hälsolägetrapporten på det här sättet. Vi kan efter dessa år konstatera att kvaliteten i .se-zonen har förbättrats avsevärt sedan vi började. Hur mycket av dessa förbättringar som kan tillskrivas vårt arbete är svårt att säga, men med tanke på hur mycket uppmärksamhet som undersökningen fått i media åtminstone till en början så vill vi gärna tro att vi har gjort skillnad.

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

Den årliga hälsolägetundersökningen finansieras av .SE. Resultaten av undersökningen har analyserats och rapporten sammanställts av Anne-Marie Eklund Löwinder, säkerhetschef på .SE. Diagram och tabeller har gjorts av Anders Örtengren, Mistat AB för de delar som avser domännamnssystemet. Underlag till de delar som avser säker filtrering av e-post har gjorts av Patrik Wallström, .SE.

För mer information om innehållet i rapporten hänvisas till Anne-Marie Eklund Löwinder, och henne når man på anne-marie.eklund-lowinder@iis.se.

[Sidan har medvetet lämnats blank.]

2 Sammanfattning

Undersökningens främsta fokus ligger på DNS-kvalitet, men vi har kompletterat den delen med en fördjupad undersökning om filtrering av e-post och utbredningen av internationaliserade domännamn, IDN.

Utvecklingen av IPv6 och DNSSEC är viktiga parametrar, inte minst som en uppföljning av tillväxten på dessa områden eftersom dessa har fått särskild uppmärksamhet i ansvariga myndigheters arbete.

I årets undersökning kan vi konstatera att andelen fel i DNS är oförändrat jämfört med 2013 års undersökning och ligger kvar på 15 procent för hela undersökningsgruppen (exklusive jämförelsegruppen).

2.1 Om undersökningsgruppen

I årets undersökning ingår totalt 913 unika domäner. Då har vi tagit bort domäner som förekommer i fler än en kategori.

Domänerna är fördelade på 1 616 unika namnservrar - IPv4 (1 256) och IPv6 (360). Med ”unik” menar vi servrar med unika IP-adresser. En namnserver hos en operatör kan härbärgera många domäner. Vilka kategorier vi använt och hur många domäner som finns i varje kategori redovisas i avsnitt 5.

Dessutom har vi liksom tidigare gjort en jämförelse med en kontrollgrupp som motsvarar en procent av hela .se-zonen, vilket rör sig om 12 791 slumpmässigt valda .se-domäner. Resultatet från den delen av undersökningen redovisas i avsnitt 10.

För att vi ska kunna se trender från år till år försöker vi i allmänhet hålla oss till ungefär samma parametrar och undersökningsgrupp som använts tidigare. Verksamheter som har upphört och tillkommit tas bort respektive läggs till. Det har varit mycket små förändringar mellan 2013 och 2014.

2.2 Nya verktyg

Under 2014 har vi haft ett samarbete med det franska registryt Afnic där vi gemensamt har utvecklat ett nytt verktyg, Zonemaster (se bilaga 3), som ska ersätta dagens DNSCheck. Vi har stora förhoppningar om att Zonemaster kommer att ligga till grund för att etablera en branschstandard för tester av domännamnssystemet. Zonemaster lanserades i början av februari 2015.

Under 2015 kommer vi dessutom att lansera ännu en ny tjänst, Domänkollen. Med den kommer domäninnehavare att kunna få en statusrapport över mätbara kvalitetsvärden på en domän/webbplats. Domänkollen erbjuder allmänheten ett redskap för att kunna ställa bättre och mer relevanta krav på sina leverantörer, och även lära sig mer om den teknik som krävs för att förbättra sin tjänst.

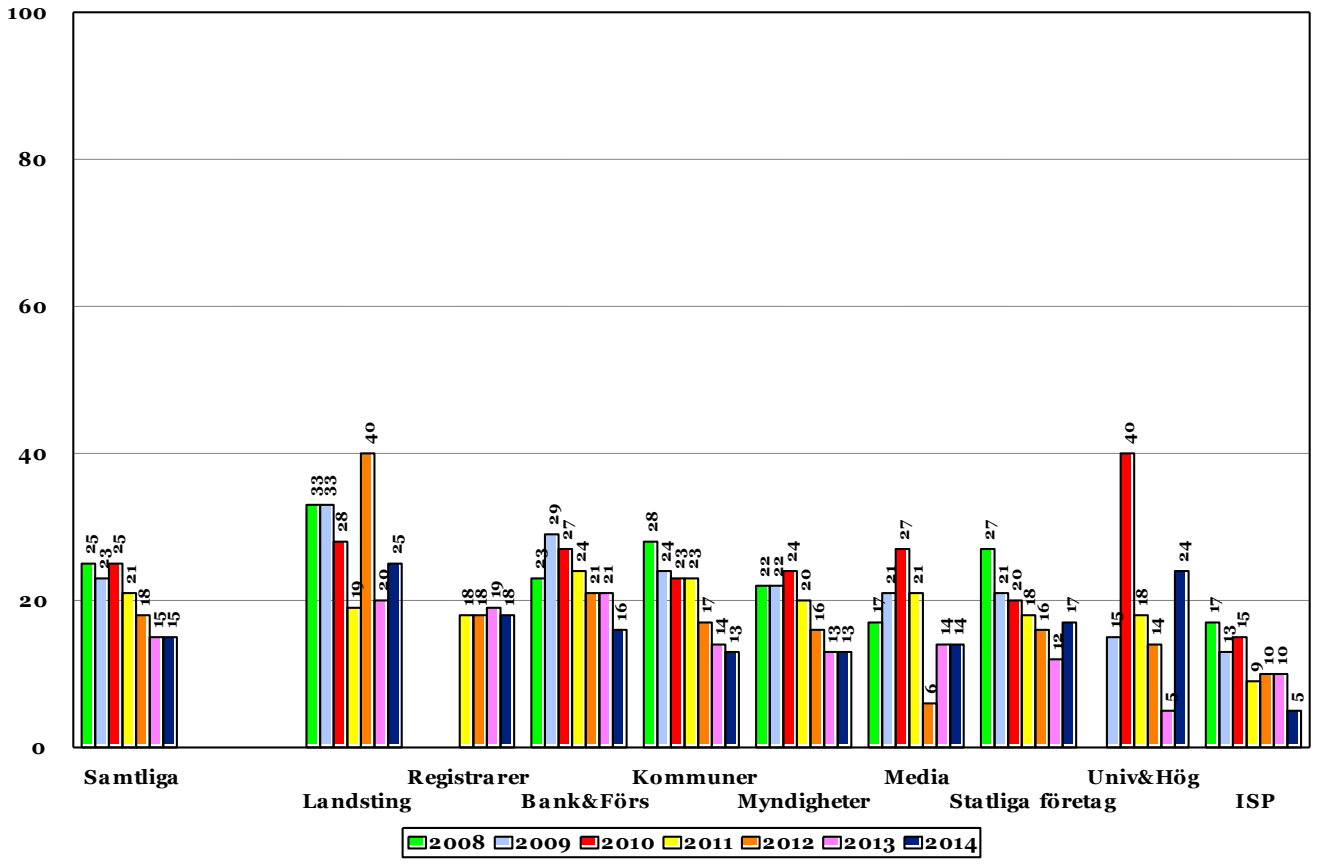
Domänkollen kan i sin enklaste form beskrivas som en webbplats med möjlighet att skapa rapporter som levereras dels direkt över webben, och dels som automatiserad html-mejl i abonnemangsform (se avsnitt 6.3.2).

2.3 Oförändrad andel allvarliga fel

De första tre åren kunde vi konstatera att det fanns stora brister i hanteringen av domännamnssystemet, men resultaten från 2011 och framåt visade på en kontinuerlig förbättring. Från mätningen 2007 med 25 procent fel var vi vid

mätningen 2013 nere i 15 procent fel. Resultatet från 2014 är oförändrat, andelen allvarliga fel ligger fortsatt på 15 procent.

Diagram 1: Utveckling av andel fel i procent 2008-2014



2.4 Branschstandard för domännamnssystemet

Det är vi själva som har definierat vad kvalitet innebär i bland annat domännamnssystemet. Definitionen har utgått från befintliga rekommendationer i standarddokument (*Request for Comments, RFC)* från IETF (*Internet Engineering Task Force*) och vad som är vedertaget som praxis eller branschstandard (*Best Common Practice)* för namnserverdrift tillsammans med våra egna praktiska erfarenheter av domännamnssystemet och av att driva namnservrar både för toppdomänerna .se och .nu samt för de domäner vi själva innehar, som till exempel iis.se.

Genom att undersökningen har genomförts under flera år har vi möjlighet att se utvecklingstrender, om det går att spåra effekten av några av de råd och rekommendationer som vi delar med oss av och slutligen om det har föranlett åtgärder bland de undersökta verksamheterna.

2.5 Slutsatser från undersökningen

Detta avsnitt sammanfattar de slutsatser som vi drar av resultaten från undersökningen 2014.

2.5.1 Behov av kompetenshöjning om DNS

Baserat på undersökningen 2014 är de vanligaste felen i DNS-systemen ungefär samma som tidigare år. Det finns fler namnservrar annonserade i .se-zonen än som faktiskt svarar på frågor för domänen (drygt 5 procent), namnservrar svarar inte på frågor via protokollet TCP (5,5 procent) eller att endast en namnserver svarar på frågor om domänen (2 procent) vilket av robusthetsskäl borde vara minst två.

Dessa fel uppstår bara om den som administrerar och hanterar namnservrarna inte har tillräcklig kunskap om hur domännamnssystemet fungerar och hur det påverkas av exempelvis vissa brandväggsregler.

2.5.2 Det krävs resurser för en bättre DNS-infrastruktur

Medan verksamheter ofta lägger miljontals kronor på webbinfrastruktur med serverhallar, servrar, lastbalanserare, databaser och design så verkar väldigt få lägga några större resurser på en stabil och robust DNS-infrastruktur. I dag är DNS en växande måltavla för bland annat överbelastningsattacker – angreppen sker där motståndet är som svagast. Därför är det fundamentalt viktigt att förbättra infrastrukturen för DNS som en del av åtgärderna mot sådana attacker.

2.5.3 Allt färre namnservrar med rekursion påslaget

Mellan 2007 och 2014 har andelen namnservrar med rekursion påslaget minskat mycket kraftigt, från 40 procent till 4 procent. Skillnaderna mellan kategorierna har minskat. Kategorierna Bank och försäkring, Internetoperatörer och Universitet och högskolor har fortfarande noll procent. Öppna rekursiva namnservrar kan missbrukas av andra och utnyttjas vid överbelastningsattacker (se avsnitt 6.1.5).

2.5.4 Allt fler använder IPv6

När det gäller införande av IPv6 för kommunikation med namnservrar ser vi en fortsatt ökning hos alla kategorier i hela undersökningsgruppen, från 54 procent 2013 till 61 procent 2014. Vanligast är det inom kategorin Universitet och högskolor med 86 procent. Den största ökningen har skett inom kategorin Media där det ökat från 33 procent som använde IPv6 2013 till 58 procent 2014. Även bland myndigheter, landsting och kommuner har ökningen varit avsevärd (se diagram 7).

2.5.5 DNSSEC

Ökningen av DNSSEC-signerade domäner i undersökningsgruppen fortsätter. En del av ökningen kan förklaras med att MSB mellan 2012 och 2013 beviljat medel ur 2:4-anslaget för krisberedskap, vilket har kunnat sökas av utpekade myndigheter. I det här fallet har ansökningarna gjorts av länsstyrelserna för att sedan komma kommunerna inom respektive region tillgodo i form av åtgärder med inriktning mot att säkerställa adressuppslagningar på internet. Totalt har MSB fördelat 10 390 000 kronor att förbruka mellan 2012 och 2014.

Vid årets undersökning är andelen signerade domäner i undersökningsgruppen 29 procent. Som jämförelse var vid årsskiftet 2014/2015 totalt 353 259 (333 423 förra årsskiftet) av 1 331 220 domäner (1 342 674 förra årsskiftet) eller omkring 28 procent av hela .se-zonen signerade med DNSSEC.

Vi kan se en ljusning i kategorin Bank och finans med en ökning från 2 procent 2013 till 5 procent 2014 som är signerade med DNSSEC.

För att ge stöd och vägledning i att införa DNSSEC i en verksamhet har .SE publicerat praktiska rekommendationer. Vägledningen är framtagen för att kunna tjäna som ett hjälpmedel för exempelvis kommuner som håller på att införa DNSSEC och den kan också utgöra ett stöd i det löpande arbetet. Den finns att ladda ner från .SE:s webbplats:
https://www.iis.se/docs/Rekommendationer_for_inforande_av_DNSSEC_kommuner.pdf

2.5.6 E-postservrar placerade i Sverige

I 2014 års mätning har vi än en gång tagit en titt på verksamheternas placering av e-postservrar, och om dessa står placerade i eller utanför Sverige (e-postservrar nåbara med IPv4-adresser) Årets resultat pekar på att det är något färre som har e-postservrar placerade i utlandet än tidigare. Att ha e-postservrar i utlandet ökar sannolikt risken för avlyssning om kommunikationen inte är skyddad med kryptering, vilket den de facto långt ifrån alltid är (se avsnitt 6.2).

3 Kontroller av internets infrastruktur

Resten av rapporten beskriver mer i detalj vad som har mätts, resultaten från mätningarna och hur det påverkar tillgänglighet och säkerhet i infrastrukturen.

I 2014 års undersökning har vi tagit reda på fakta om följande kontrollpunkter:

- Hur hanterar verksamheten sina domännamn och det tekniska domännamnssystemet (DNS)?
- Hur är det uppsatt (jämfört med vad som är att betrakta som branschstandard (Best Common Practice)?
- Vilka är de allvarligaste bristerna?
- Inom vilka kategorier är dessa brister vanligast?
- Hur hanterar verksamheten sin e-post? Står e-postservrarna i eller utanför Sverige?
- Har man infört IPv6 i verksamhetens IT-miljö?
- Har man infört DNSSEC i verksamhetens IT-miljö?
- Utnyttjar man möjligheten att använda internationaliserade domännamn, det vill säga med andra tecken än a-z, 0-9 och bindestreck?

Testerna har genomförts på domäner och servrar för ett stort antal viktiga verksamheter i samhället; statliga bolag, banker, försäkrings- och finansföretag, internetoperatörer, kommuner, landsting, medieföretag, statliga myndigheter, universitet och högskolor samt återförsäljare av .se-domäner (registrarer). Totalt har 913 domäner testats.

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

Dessa tester ger en indikation om hur väl verksamheternas system fungerar i olika avseenden, var de allvarligaste felen finns och hur vanliga de är. Baserat på detta har vi genomfört analys av vad det kan få för konsekvenser för verksamhetens IT-funktion. Den del av rapporten som rör tester av domännamnssystemet sätts i relation till alla tidigare undersökningar, i princip från 2007 till i dag.

I slutet av rapporten återkommer vi till hur vi anser att det borde se ut i den svenska internetinfrastrukturen. Slutligen upprepar vi råd och rekommendationer inom olika områden som ansvariga myndigheter bör ta tag i. Dessa åtgärder är det lämpligt att gå vidare med och utreda mer i detalj.

Vi låter dessa stå kvar i princip oförändrade från förra årets undersökning eftersom resultaten från undersökningen talar sitt tydliga språk, det finns fortfarande brister som, även om trenden pekar åt rätt håll, både bör och enkelt kan åtgärdas.

Vi konstaterar att bank- och finanssektorn även i år ligger långt efter andra kategorier med införandet av DNSSEC, utan att vi kan se någon rimlig förklaring. För en så viktig del av samhället borde det vara en självklar åtgärd för att skydda sina kunder.

4 DNS-tjänst med kvalitet

Domännamnssystemet (DNS) är en av hörnstenarna på internet och har till uppgift att förenkla adresseringen av resurser på nätet.

.SE har ansvaret för .se, Sveriges nationella toppdomän på internet och verksamheten regleras av lagen (2006:24) om nationella toppdomäner för Sverige på internet[1]. .SE har sedan 2013 också ansvaret för toppdomänen .nu. .nu-domäner ingår dock inte i undersökningen.

Varje internetansluten enhet har en egen IP-adress som med hjälp av domännamnssystemet kan kopplas till en adress i en form som är lättare att hantera för oss människor. Via den öppna katalogtjänst som är DNS kan människor använda domännamn, som till exempel iis.se, för att slå upp IP-adresser när de surfar, skickar e-post eller använder internet på något annat sätt. Tack vare domännamnssystemet behöver man inte heller byta webb- eller e-postadress bara för att en server byter IP-adress. En användare med en egen domän kan enkelt flytta sina tjänster från en internetoperatör till en annan, utan att för den skull behöva byta exempelvis e-postadress och göra ”flyttanmälan” till alla sina kontakter.

För arbetet med undersökningen har vi definierat vad som krävs för att skapa en DNS-tjänst med kvalitet. Denna definition har vi använt för årets liksom för tidigare års undersökningar. Hög kvalitet för oss innebär att:

- Det finns en robust infrastruktur för DNS med god nåbarhet.
- Alla inblandade namnservrar svarar korrekt på frågor.
- Domäner och servrar är korrekt uppsatta.
- Data i domännamnssystemet om enskilda domäner är korrekt och äkta.
- Verksamhetens kommunikationsinfrastruktur som helhet uppfyller de krav som ställs i relevanta internet- och andra standarder.

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

I undersökningen utgår vi från våra egna erfarenheter och en brett överenskommen branschstandard eller Best Common Practice (BCP) med vad som är att betrakta som en bra infrastruktur för DNS. Post- och telestyrelsen publicerade 2011 en vägledning[2] som stöd vid anskaffning av extern elektronisk kommunikation, exempelvis internetanslutning och telefoni. I vägledningen ingår bland annat krav som bör ställas på DNS.

Några av de värsta felen har varit relativt vanligt förekommande genom åren. På senare år har vi dock noterat en positiv trend med successiv förbättring. Trenden håller i sig och 2014 är inget undantag.

[1] https://lagen.nu/2006:24
[2] Vägledning för anskaffning av robust elektronisk kommunikation. http://www.pts.se/upload/Rapporter/Internet/2011/V%C3%A4gledning%20f%C3%B6r%20%20anskaffning%20av%20robust%20elektronisk%20kommunikation_110823.pdf

Vi vill trots detta betona behovet av att olika verksamheter vässar sin kompetens på området för att kunna ställa relevanta krav på både konsulter, registrarer och leverantörer som driver namnservertjänster, e-posttjänster och webbtjänster.

För den offentliga förvaltningens vidkommande skulle det underlätta om stöd för sådan kravställning formulerades från centralt håll. Myndigheten för samhällsskydd och beredskap publicerade 2014 en vägledning[3] avsedd att ge ett övergripande stöd till olika typer av organisationer för att genomföra upphandlingar av it-relaterade tjänster så att även informationssäkerhetsaspekterna beaktas. MSB:s vägledning är dock inte på den detaljnivån att den utgör ett direkt stöd när det gäller funktionella krav som bör ställas på säkerhet i exempelvis olika infrastrukturtjänster. Ett sådant verktyg har emellertid företaget CyberCom tagit fram i form av handfasta tips på hur företag och myndigheter kan ställa bättre säkerhetskrav i sina upphandlingar, något de lanserat under namnet Upphandlingskollen[4].

I bilaga 5 redovisar vi för den mer tekniskt bevandrade läsaren vad branschstandarden för att skapa en infrastruktur för DNS i Sverige med hög kvalitet innebär i termer av krav eller rekommendationer.

[3] https://www.msb.se/RibData/Filer/pdf/26589.pdf
[4] http://www.cybercom.com/upphandlingskollen/

5 Tester 2014

Även 2014 års resultat är baserade på månadsvisa körningar. Som tidigare har testerna omfattat både domänernas konfiguration och status för de namnservrar som svarar på frågor om domänen samt några av de enligt vår bedömning viktigaste parametrarna för e-post.

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

I 2014 års undersökning har vi dessutom utöver den vanliga mätningen av det allmänna hälsoläget genomfört en något fördjupad mätning och analys av utbredningen av internationaliserade domännamn, IDN, i synnerhet inom den offentliga förvaltningen där man borde kunna förvänta sig att det finns gemensamma rekommendationer för hanteringen av svenska tecken i domännamn för exempelvis webbplatser.

5.1 Testobjekt

Årets tester har genomförts i slutet av varje månad och har omfattat totalt 913 domäner fördelade på 1 616 unika namnservrar. Vi noterar 2014 en ökning med 38 unika namnservrar för samma domäner jämfört med 2013.

Testobjekten har grupperats i kategorier på följande sätt:

- 57 affärsdrivande verk och statliga bolag
- 81 banker, finansinstitut och försäkringsbolag
- 21 internetoperatörer (ISP)
- 290 kommuner
- 20 landsting
- 36 medieföretag
- 229 statliga myndigheter
- 37 universitet och högskolor
- 151 registrarer

Kategorin registrarer, det vill säga återförsäljare av .se-domäner, är många gånger även leverantör av namnserver- och andra tjänster till domäninnehavare. Hur många ackrediterade registrarer som finns för .se ändrar sig kontinuerligt och är för närvarande något färre än antalet som har ingått i undersökningen.

5.2 Definition av ”fel”

I undersökningen redovisar vi enbart det som vi betraktar som fel enligt följande definition:

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

Verktyget vi använder genererar även sådant som definieras som varningar. Varningar är egentligen också fel som kan påverka driften, men vi bedömer inte att de är lika akuta och därmed är inte heller omedelbara åtgärder lika angelägna. Det skulle dock höja kvaliteten och nåbarheten om dessa fel eliminerades. Varningar särredovisas inte i undersökningen.

6 Observationer 2014

I detta avsnitt redovisar vi våra observationer från undersökningen som har genomförts 2014 och jämförelser med tidigare års undersökningar.

6.1 Tester av DNS

Mellan åren 2007 och 2010 fanns det stora brister i hanteringen av domännamnssystemet som vi pekade på. Vi föreslog också konkreta åtgärder för att komma tillrätta med dessa, åtgärder som kan genomföras av respektive namnserveroperatör vare sig verksamheten har egen drift eller anlitar någon annan.

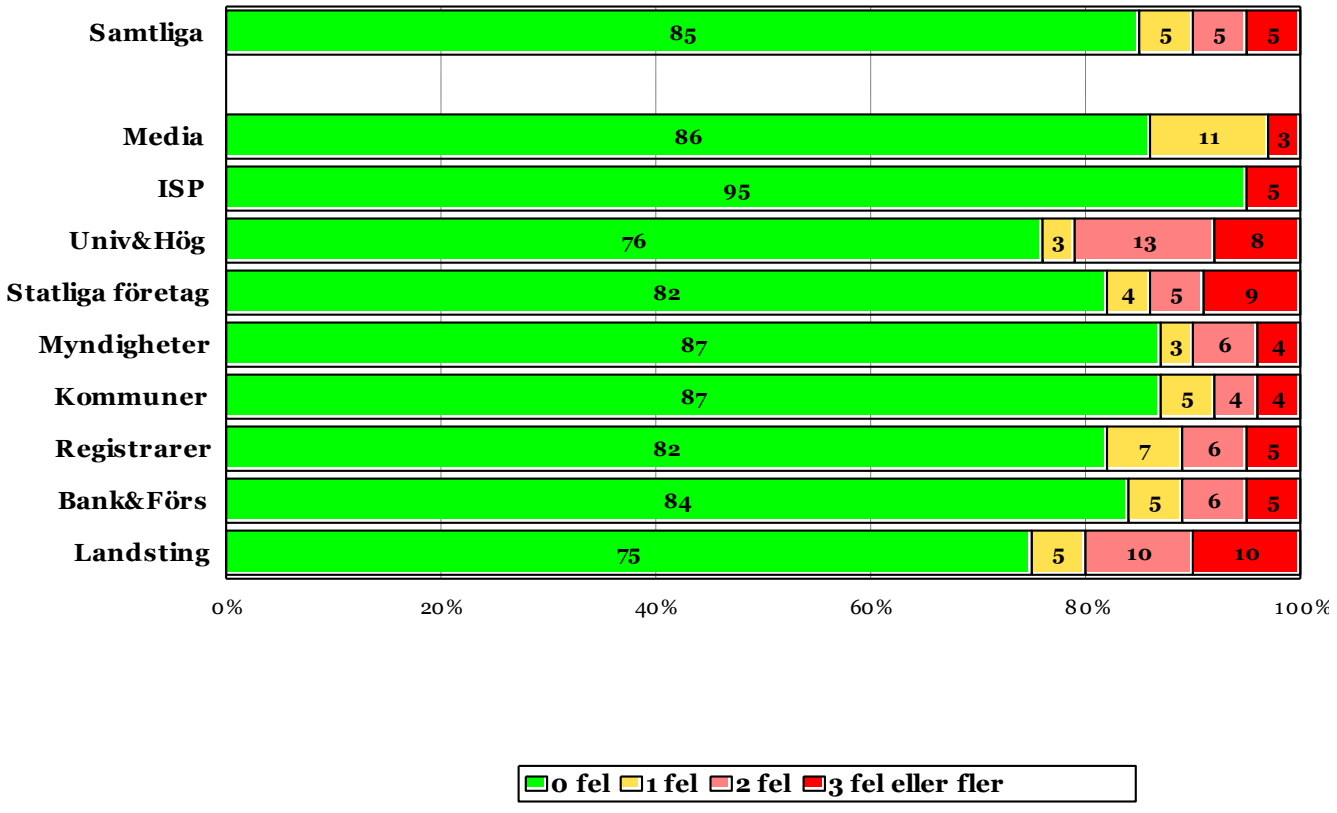
I resultaten från 2011 och framåt har vi sett en kontinuerlig förbättring. Vid 2012 års undersökning hamnade .se-domänen för första gången under 20 procent i andel fel för undersökningsgruppen som helhet, närmare bestämt på 18 procent.

Jämfört med den första mätningen 2007 som gav 25 procent fel var vi vid mätningen 2013 nere i 15 procent fel. Resultatet från 2014 är oförändrat, andelen allvarliga fel ligger fortsatt på 15 procent.

6.1.1 Mängden fel per kategori

Det är förstås en viss skillnad om en domän bara har ett enstaka fel eller om den har flera olika fel, som kanske dessutom samverkar. Av det skälet tittar vi även på spridningen av antal fel per kategori enligt diagram 2.

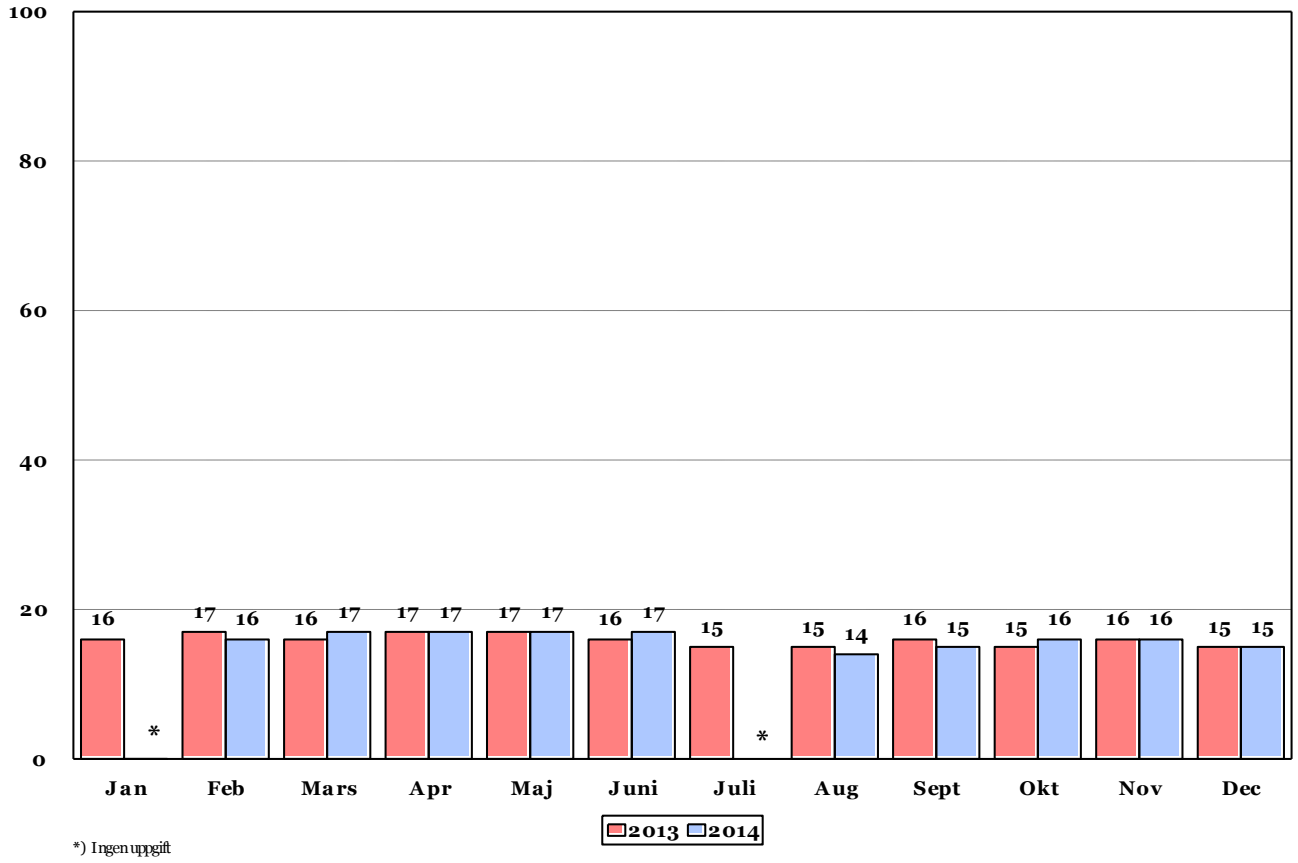
Diagram 2: Procentuell fördelning av mängden fel per kategori



När man tittar på samtliga grupper är fördelningen mellan ett, två och tre eller fler fel jämnt fördelad i undersökningsgruppen. Kategorin ISP har i år den lägsta felprocenten med enbart fem procent, dessa fem procent tillhör dock gruppen ”tre fel eller fler”. Därefter kommer kategorierna Media, Myndigheter och Kommuner.

Tar man hela undersökningsgruppen och resultat per månad så fördelar de sig relativt jämnt över året även 2014 enligt nedanstående diagram.

Diagram 3: Andel fel per månad för hela undersökningsgruppen 2013-2014



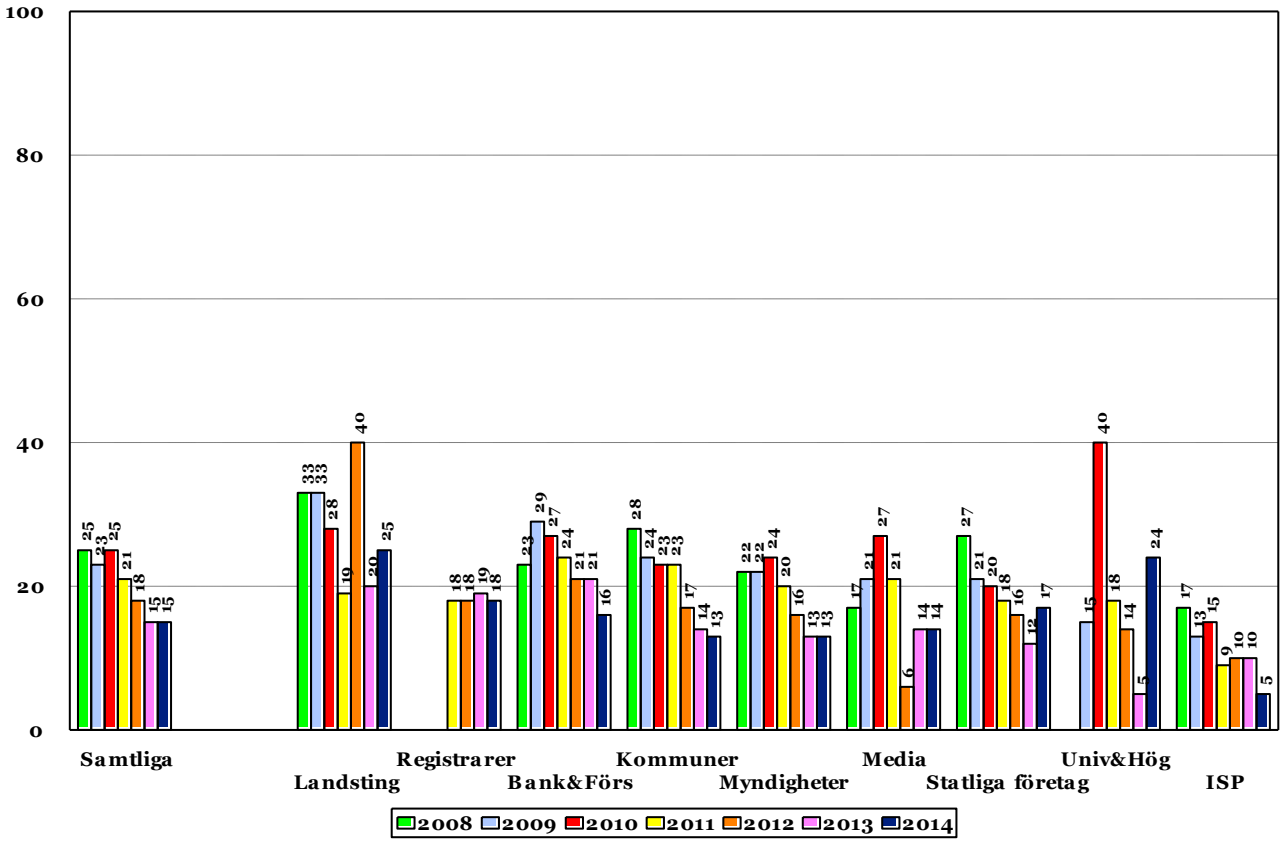
Det är vår klara uppfattning att det går att komma under 20 procent fel utan större ansträngning. I fjolårets mätning uppnåddes det målet med råge då vi noterade 15 procent fel för hela undersökningsgruppen. Felprocenten ligger kvar på samma låga nivå även 2014. För att komma under 15 procent krävs det lite större insatser än att bara rätta till grundläggande hygienfaktorer, men det är absolut ingen omöjlighet. Vi uppmanar därför alla att se över sin DNS-infrastruktur och göra det som krävs för att förbättra den.

6.1.2 Jämförelse av andelen fel över tid

I och med att vi har tillgång till data från tidigare undersökningar har vi också möjlighet att jämföra resultaten mellan årets och tidigare års undersökningar för de kategorier som finns med i undersökningarna för samtliga år.

I diagrammet nedan jämför vi andelen fel per kategori från 2008 till 2014 (med undantag för kategorin Universitet och högskolor som lades till undersökningsgruppen 2009 respektive Registrarer som lades till 2011).

Diagram 4: Andel fel per år och kategori 2008-2014 (procent)



Av diagrammet kan vi se att situationen 2014 är oförändrad för hela undersökningsgruppen jämfört med 2013. Däremot har det rört sig mer om man tittar på varje kategori för sig. Andelen fel har ökat inom kategorierna Landsting, Statliga företag och Universitet och högskolor. Den ligger oförändrad inom kategorierna Myndigheter och Media medan den har minskat inom kategorierna Registrarer, Bank och försäkring, Kommuner och ISP:er. 2014 är det hos Universitet och högskolor som vi ser den största förändringen, från 5 till 24 procent.

Felkonfigurationer som utförs av en och samma konsult hos många verksamheter eller hos någon av de större namnserveroperatörna fortplantar sig givetvis till alla domäner som de hanterar. Detta kan, om domänerna är många till antalet, få mycket stort genomslag på resultaten från undersökningen, framför allt om felen uppträder inom en och samma kategori.

Värt att nämna är att .SE:s tre största registrarer liksom förra året har 50 procent av marknaden och tar vi de sju största har dessa en marknadsandel på cirka 70 procent. Det råder inte något 1:1-förhållande mellan registrar och namnserveroperatör, men många registrarer agerar även namnserveroperatör för de domäner de hanterar.

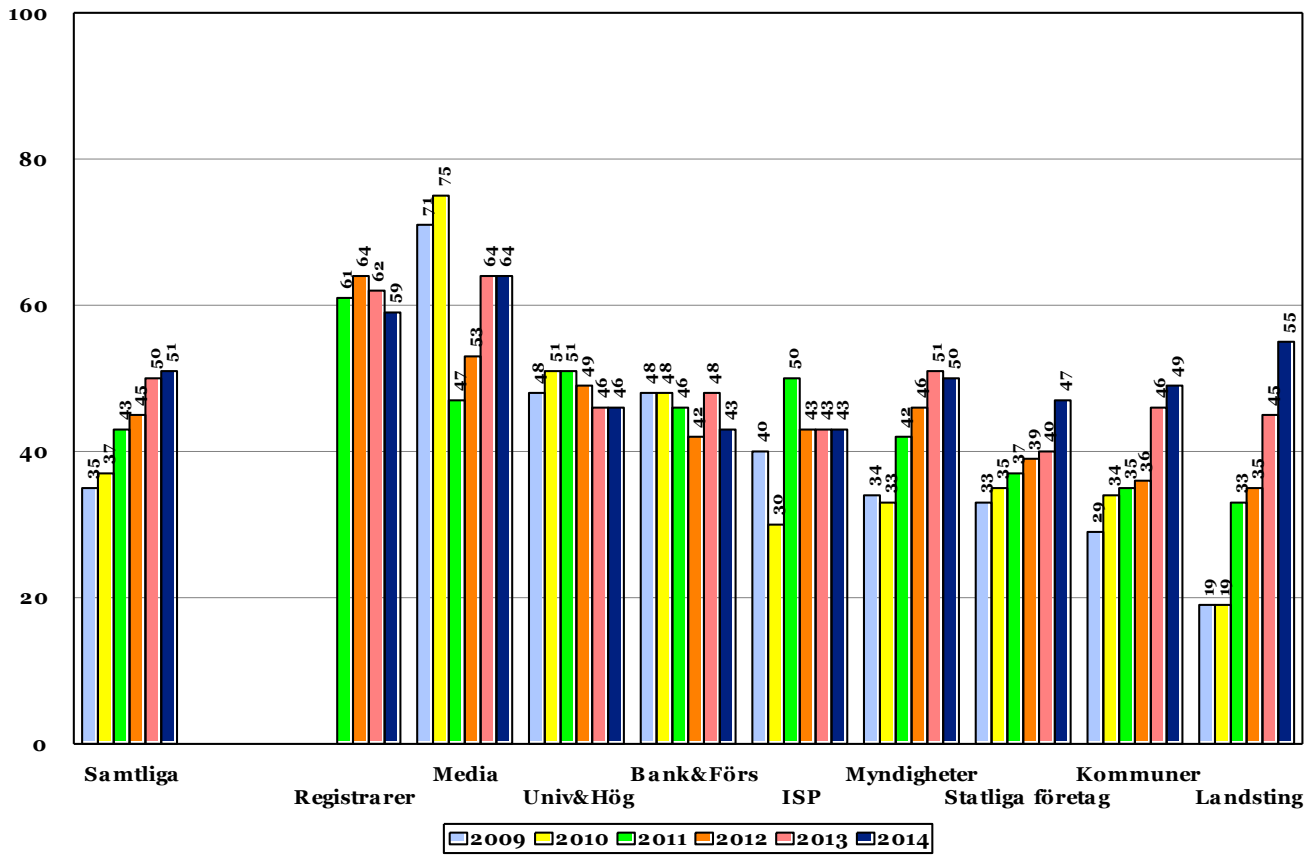
Medan många verksamheter anlitar tredjepartsleverantörer för drift av DNS finns det även de som driver sin egen DNS-infrastruktur.

6.1.3 Anslutning av namnservrar till internet

Spridningen av drift av namnservrar bland olika operatörer verkar fortsätta att utvecklas på samma sätt som tidigare där de stora blir allt större. Risker förknippade med den utvecklingen är till exempel om en enskild operatör i alltför stor omfattning dominerar inom en kategori. Vid en sådan dominans kan i värsta fall konsekvenserna bli att en hel sektor drabbas om den dominerande operatören har problem.

Det ökar redundansen om namnservrarna är anslutna till flera operatörer. I diagrammet nedan ser vi hur stor andel av undersökningsgruppen som har namnservrar anslutna till fler än ett AS (autonomt system), eller hos fler än en operatör.

Diagram 5: Andel med namnservrar som annonseras i fler än ett AS år 2009-2014



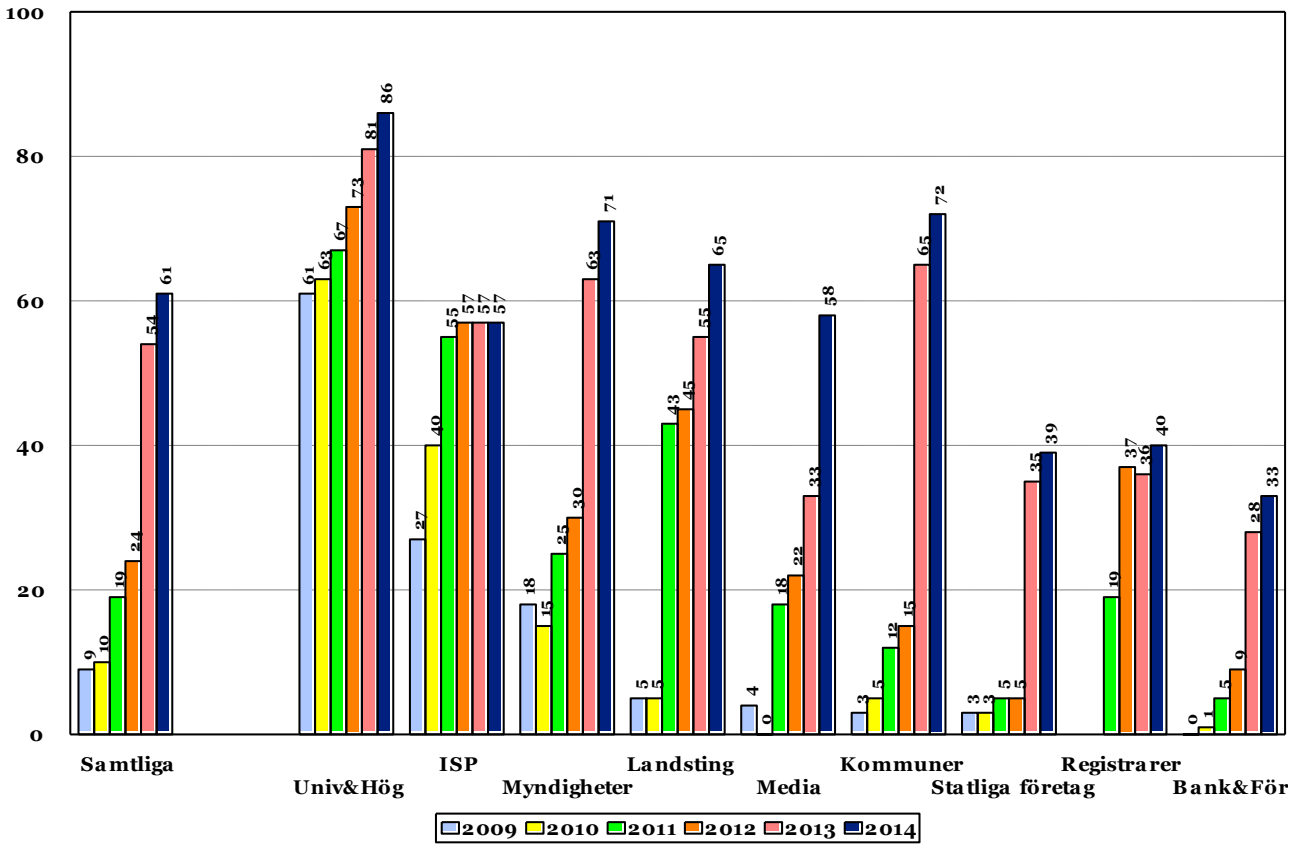
Av diagrammet framgår att trenden med en fortsatt ökning från år till år håller i sig och 2014 är det över 50 procent av verksamheterna i undersökningsgruppen som har sina namnservrar placerade hos fler än en operatör. Även den här gången är det kategorin Landsting som står för den största ökningen, följt av Statliga företag.

6.1.4 Namnservrar med IPv6

Införandet av IPv6 som nästa generations kommunikationsprotokoll är det enda sättet att garantera en stabil framtida internetinfrastruktur. Det har funnits en klart uttalad strategisk vilja från regeringens sida att alla myndigheter bör vara nåbara med IPv6 senast 2013, vilket har slagits fast i några olika politiska ställningstaganden. Det är emellertid alldeles klart att det målet inte är uppfyllt ännu, trots att vi skriver 2015. Av de statliga myndigheterna har 71 procent infört IPv6 på sina namnservrar.

Även om målet inte är uppfyllt så har vi på senare år sett en tydlig utveckling med en ökad aktivitet på IPv6-området och den trenden fortsätter att peka uppåt även i resultaten från undersökningen 2014. Vi har nu hela 61 procent av namnservrarna i undersökningsgruppen som är nåbara med IPv6, ett mycket glädjande resultat.

Diagram 6: Andel som använder namnservrar som går att nå med IPv6 2009-2014

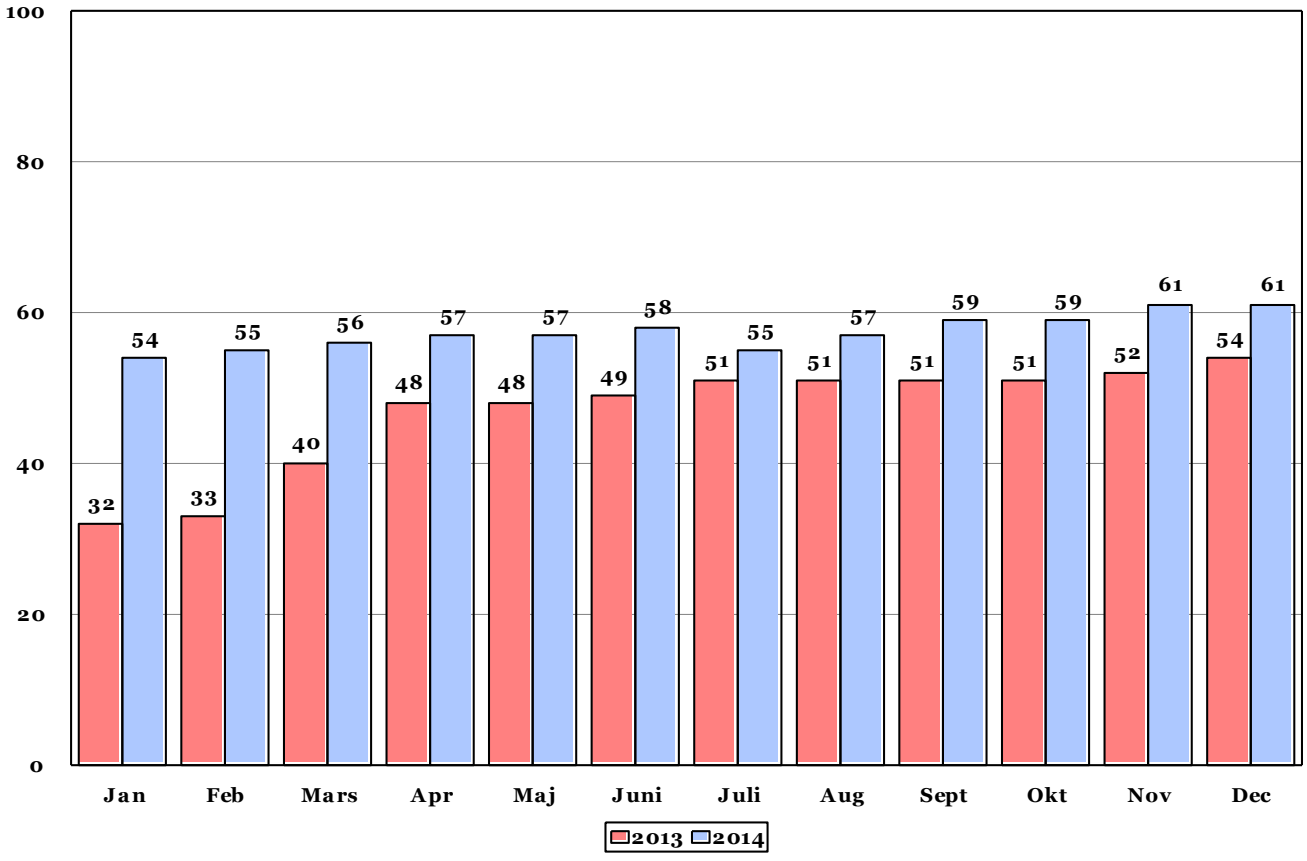


Det är tydligt att också landsting, media, kommuner, företag och organisationer följer efter, även om ökningen är mindre dramatisk 2014 än den var 2013 framför allt hos ISP:er, statliga företag, registrarer samt hos bank och försäkring.

Utvecklingen inom offentlig förvaltning är dramatisk men där har satsningen varit både systematisk och underbyggd av politiska signaler samt konkret stöd från Post- och Telestyrelsen. PTS generaldirektör levererade under en period personligen tårta till de myndigheter som infört IPv6.

IPv6 införs parallellt med IPv4 och det gamla protokollet kommer inte att fasas ut förrän efter en övergångstid på flera år.

Diagram 7: Andel av undersökningsgruppen med IPv6, per månad 2013 respektive 2014



Resultatet från de månadsvisa mätningarna talar sitt tydliga språk. I diagrammet ser vi en fortsatt ökning från mätningarna per månad för 2013 och en lika stadig ökning från mätningarna 2014. För närvarande är vi uppe i 61 procent för hela undersökningsgruppen.

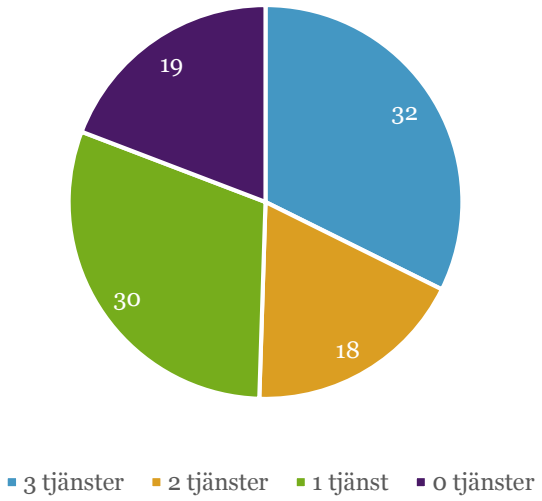
De flesta verksamheter i samhället är beroende av tillgänglig och robust elektronisk kommunikation via internet, inte minst myndigheter. Utrustning som ansluts till internet kräver en unik IP-adress och måste använda gemensamma protokoll för att kunna kommunicera med varandra. Genom att

införa IPv6 i de publika tjänster som riktar sig till medborgarna kan en myndighet vara säker på att vara nåbar för alla även i framtiden. Den förra regeringen uttalade i sin digitala agenda att alla myndigheter bör ha infört IPv6 senast år 2013.

PTS har etablerat en e-tjänst som visar takten på myndigheternas införande av IPv6. De myndigheter som följs upp bygger på underlag från Statistiska Centralbyrån, vilket skiljer sig något från vår kategori då vi hämtar underlaget för våra mätningar från Ekonomistyrningsverkets lista över statliga myndigheter.

PTS e-tjänst genomför dagligen en IPv6-kontroll av webbsidor, DNS och e-post och om servrarna går att nå med IPv6. Det görs ingen kontroll av om länkade tjänster på berörda webbsidor går att nå med IPv6.

Diagram 8: Statliga myndigheter med tjänster nåbara via IPv6 (procent)



På PTS e-tjänst visas även ett diagram över myndigheters nåbarhet via IPv6 över tiden[5], inte bara avseende DNS utan även för externa webbplatser och e-post. PTS mätning av myndigheters tillgänglighet över IPv6 påbörjades i november 2012.

PTS kommentar till dessa resultat är att det finns en hel del återstående arbete för såväl myndigheter som kommuner med att införa IPv6 för sina grundläggande publika tjänster såsom webb, DNS och e-post. Endast en tredjedel av alla myndigheter har i februari 2015 uppnått regeringens mål om att vara nåbara över IPv6. Dessa har stöd för IPv6 för sin webbplats, e-post och DNS.

Knappt en femtedel av myndigheterna är vid samma tidpunkt nåbara över IPv6 i två av tre tjänster. För dessa borde det inte vara alltför betungande att bli nåbara över IPv6 i den återstående tjänsten under 2015. Vidare är en tredjedel

[5] http://e-tjanster.pts.se/internet/ipv6

nåbara över IPv6 i en tjänst medan knappt en femtedel ännu inte har påbörjat sitt arbete med att införa IPv6.

PTS noterar liksom .SE att IPv6-införandet hos myndigheter och kommuner tog fart under 2013. IPv6-införandet utvecklades kontinuerligt under 2013 fram till mars 2014. I mars 2014 hade enligt PTS mätningar 64 procent av myndigheterna stöd för IPv6 i DNS, 56 procent hade IPv6-stöd i sin e-posttjänst och 33 procent hade IPv6 stöd för sin webbplats.

Knappt ett år senare, i februari 2015, har 68 procent av myndigheterna stöd för IPv6 i DNS, 59 procent har stöd för IPv6 för sin e-posttjänst och 38 procent har stöd för IPv6 för sin webbplats. Det vill säga en ökning om fyra procentenheter för DNS, tre procentenheter för e-post och fem procentenheter för webben.

Av Sveriges kommuner är det 12 procent som enligt PTS mätningar har stöd för IPv6 i både DNS, e-post och webb i februari 2015. Det är en ökning med tre procentenheter jämfört med ett år tillbaka.

PTS har för närvarande inget nytt uppdrag om IPv6 från regeringen men kommer ändå vid lämpliga tillfällen under 2015 att kommunicera kring frågan om IPv6. PTS har tagit fram flera olika informationsmaterial som är tänkta att fungera som stöd för organisationer som står i färd med att införa IPv6. Materialet finns på www.pts.se/ipv6

6.1.5 Namnservrar med rekursion påslaget

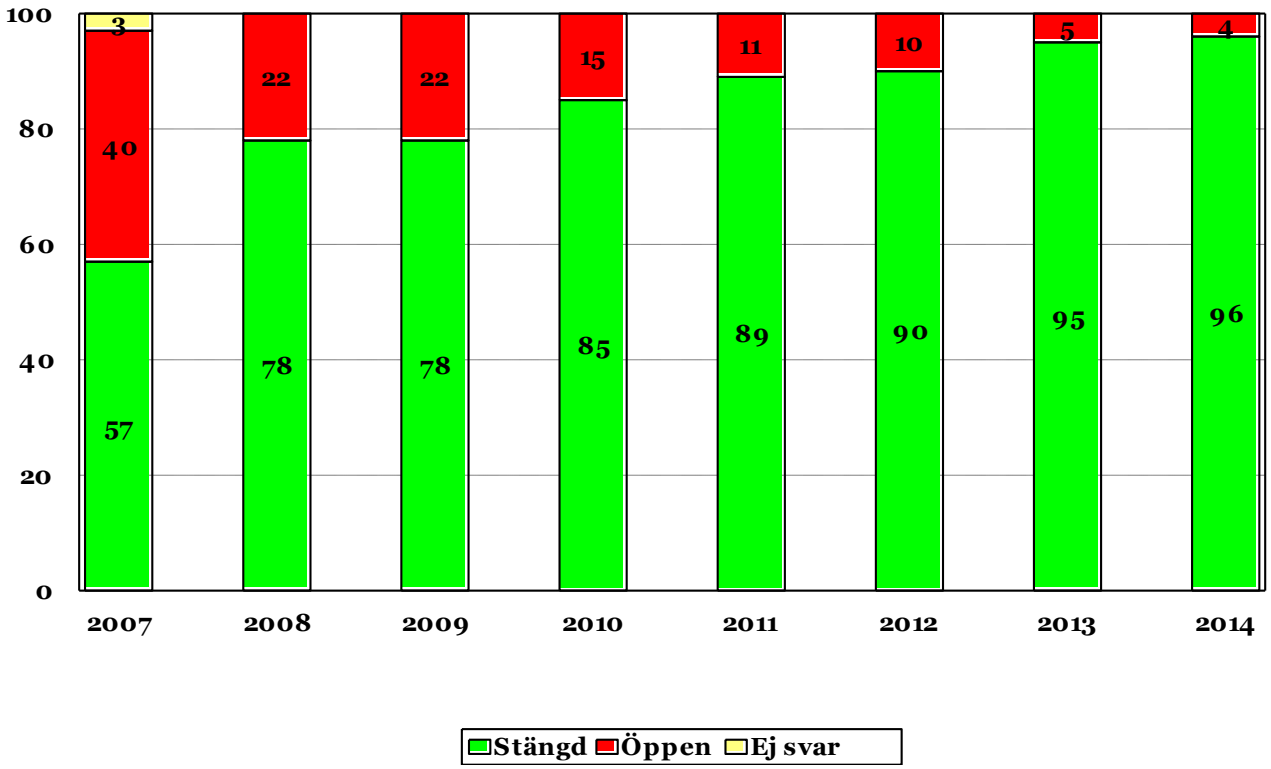
En namnserver som har rekursion påslaget gör mer än vad som kanske är hälsosamt för den. Den svarar inte bara på frågor om de DNS-poster den själv ansvarar för utan går dessutom vidare och frågar andra namnservrar för att ta reda på svaret. Frågandet kan bli både arbetskrävande (ta datorkapacitet) och 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 till exempel utföra tillgänglighetsattacker via den öppna namnservern genom att låta den ställa frågor som kommer att resultera i ovanligt stora svar. I kombination med en falsk avsändaradress som leder svaret till någon helt annan mottagare, exempelvis någon som valts ut till måltavla, utgör det grunden för att utföra en tillgänglighetsattack.

Som vi upprepat vid alla våra tidigare undersökningar har öppna rekursiva namnservrar mycket få legitima användningsområden och kan komma att utnyttjas bland annat i samband med överbelastningsattacker. Mot distribuerade överbelastningsattacker finns inget riktigt effektivt skydd, men det går att minska risken för att man själv blir en del av attacken och utnyttjas som ett vapen mot andra på internet. En stark rekommendation är att eliminera möjligheten att utnyttja öppna rekursiva resolvrar med hjälp av de tillgängliga tekniker som beskrivs i de referenser som anges i bilaga 7.

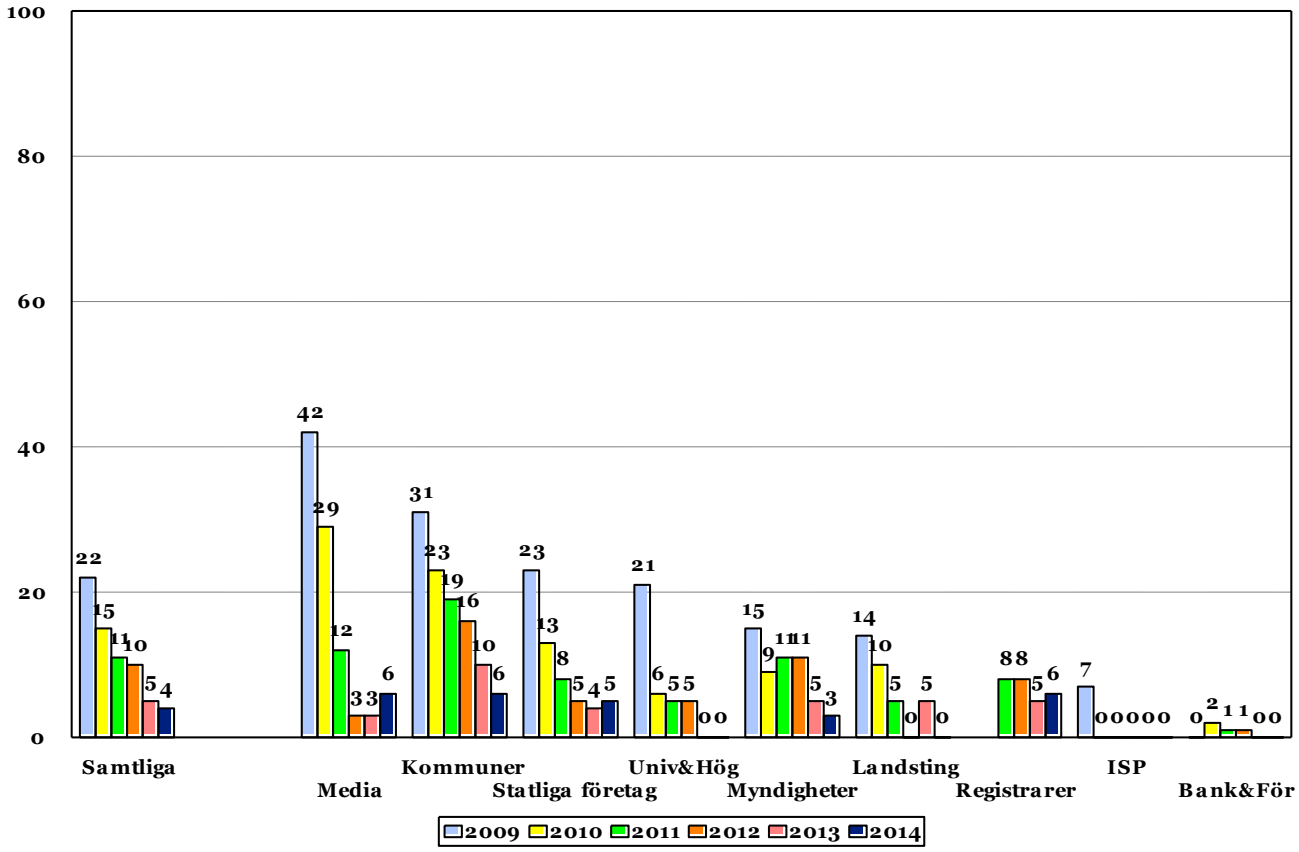
Andelen namnservrar som är öppna för rekursion har kontinuerligt minskat från år till år, 2014 är vi nere i 4 procent jämfört med minst 40 procent när vi inledde hälsolägetundersökningarna 2007.

Diagram 9: Andel namnservrar öppna för rekursion 2007-2014



Vi ser alltså en förbättring även i år men framför allt totalt över tiden. Det finns flera förklaringar till den positiva utvecklingen. En är att namnservrar numera levereras med funktionen rekursion avslagen från början. En annan är att de som ansvarar för DNS-infrastrukturen för en verksamhet faktiskt har blivit bättre på att införa separation mellan auktoritativa namnservrar (de som ska svara på frågor) och resolvrar (de som bara ska förmedla frågor och svar).

Diagram 10: Namnservrar öppna för rekursion per kategori



Kategorierna Media, Statliga företag och Registrarer visar en liten ökning. Landstingen är tillbaka på noll procent efter 2013 års ökning. Kategorin ISP behåller sitt goda resultat i 2014 års undersökning, så även Universitet och högskolor samt Bank och försäkring.

6.1.6 Säker DNS

Säker DNS, eller DNSSEC, skapar en förtroendekedja i domännamnssystemet från rotzonen, via toppdomäner till huvuddomäner. Det skyddar internetanvändare från förfalskad eller manipulerad DNS-information exempelvis genom så kallad DNS *cache poisoning*. Svar på DNS-frågor som säkrats med DNSSEC förses med en digital signatur och genom att kontrollera signaturen i mottagaränden (validering) kan man förvissa sig om att DNS-informationen inte har förändrats på vägen från namnserver till mottagande system.

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. Det är viktigt att ha ordning och reda.

I princip alla internetbaserade tjänster är beroende av att DNS fungerar bra. Konsekvensen av att göra fel kan bli omfattande. Detta gäller generellt men i än

högre grad vid införandet av DNSSEC. DNSSEC ställer högre krav på teknisk kompetens för drift än vad traditionell DNS gör.

6.1.6.1 Aktiviteter för att öka användningen av DNSSEC

MSB har de senaste åren haft möjlighet att bevilja medel ur det så kallade 2:4-anslaget, Krisberedskap, som kan sökas av utpekade statliga myndigheter. Med start 2012 prioriterade MSB området robusthetshöjande åtgärder med inriktning mot att säkerställa adressuppslagningar på internet, det som sker via domännamnssystemet, DNS. 2013 har totalt 230 (av totalt 290) kommuner via länsstyrelserna beviljats medel för åtgärder som bidrar till ett införande av DNSSEC. Totalt har MSB fördelat 10 390 000 kronor mellan 2012 och 2014.

.SE har publicerat en vägledning[6] med rekommendationer för DNSSEC. Vägledningen är framtagen för att kunna tjäna som ett hjälpmedel och verktyg för kommuner som är på väg att införa DNSSEC. Ambitionen är att den också ska utgöra ett stöd i det löpande arbetet med DNSSEC. Den fungerar givetvis också i andra typer av verksamheter inom både offentlig förvaltning och näringsliv.

Enligt MSB:s handlingsplan från 2012 ska DNSSEC vara infört hos merparten av de offentliga verksamheterna vid utgången av 2014. Åtgärder som myndigheten kommer att vidta är att följa upp de tidigare insatser som gjorts och också fortsätta arbetet med att införa DNSSEC för återstående domäner i samverkan med .SE, PTS och SKL. Någon sådan uppföljning är ännu inte påbörjad.

Det tillsammans med det faktum att .SE ansvarar för den svenska toppdomänen är de viktigaste skälen till varför vi fokuserar flera av våra tester på just kvalitet i DNS. Att internets rotzon signerades sommaren 2010 satte ytterligare fart på spridningen av DNSSEC. Eftersom rotzonen är toppen av DNS-hierarkin blev det därmed enklare för de underliggande toppdomänerna att införa DNSSEC. Dessutom ställer ICANN krav på att alla nya toppdomäner[7] som beviljas ska vara signerade med DNSSEC.

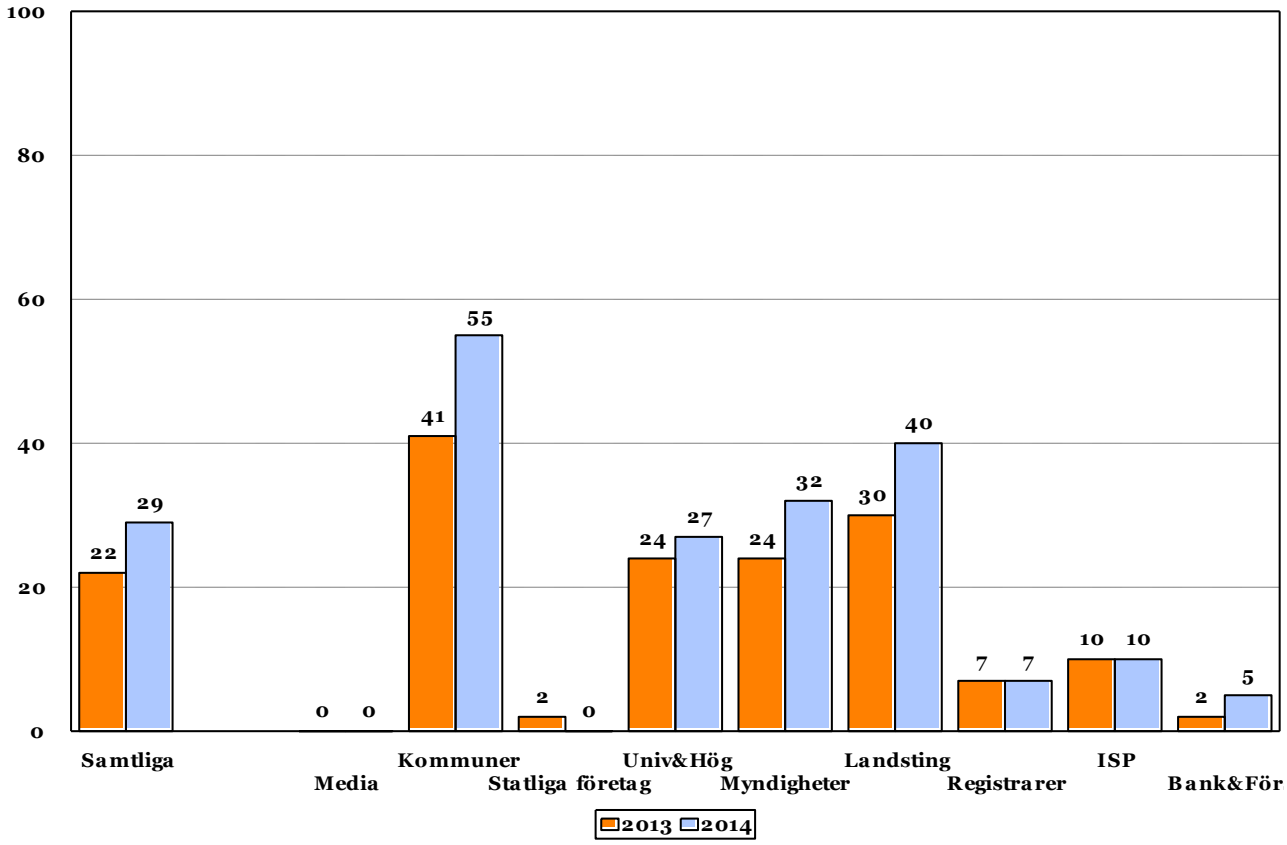
6.1.6.2 Hur utbredd är användningen av DNSSEC?

Vid 2013 års undersökning hade antalet signerade domäner bland undersökningsgruppens 913 domäner ökat till 204 domäner, motsvarande 22 procent, en dryg fördubbling av antalet signerade domäner 2012. 2014 har andelen ökat ytterligare till 29 procent (265 domäner).

Kontrollgruppen som utgör 1 procent av .se-zonen hade vid årsskiftet totalt 3 559 signerade domäner, eller nästan 28 procent, alltså något färre än vad som finns i undersökningsgruppen.

[6] https://www.iis.se/docs/Rekommendationer_for_inforande_av_DNSSEC_kommuner.pdf
[7] http://newgtlds.icann.org/en/

Diagram 11: Procentandel med DNSSEC totalt och per kategori 2013-2014



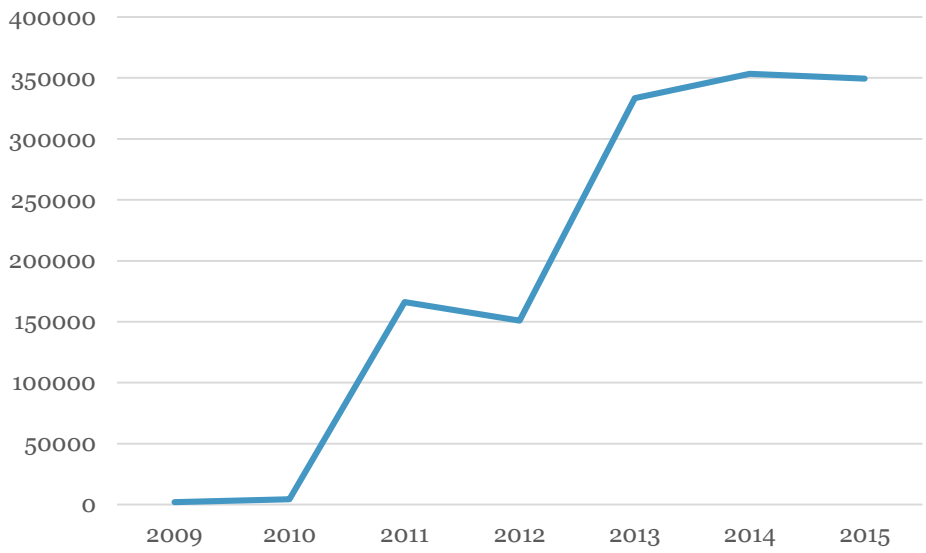
Inte oväntat toppar kommunerna med 55 procent signerade domäner (116 av 290), därefter följer kategorierna Landsting med 40 procent, Myndigheter med 32 procent samt Universitet och Högskolor med 27 procent. Här kan vi återigen konstatera att den offentliga sektorn leder stort när det gäller DNSSEC-signerade domäner men att kategorin Myndigheter har sprungit om kategorin Universitet och högskolor.

Kategorin Media saknar fortfarande signerade domäner. Kategorin Statliga företag ligger kvar på blygsamma 2 procent medan Bank och Försäkring åtminstone har ökat något och nu har 5 procent signerade domäner i undersökningsgruppen.

.SE driver på utvecklingen inom området genom att ha regelbundna kampanjer för registrarer med .se-domäner.

I diagram 12 redovisas tillväxten för DNSSEC-signerade domäner för hela .se-zonen, alltså inte bara undersöknings- och kontrollgrupperna.

Diagram 12: Tillväxt – domäner signerade med DNSSEC i hela .se-zonen 2009-2014



Den starka tillväxt som noteras fram till 2014 har stagnerat. Kampanjer till trots så är det fortfarande några av .SE:s största registrarer som av olika anledningar inte har genomfört signering av alla sina kunders domäner.

6.1.6.3 Säker DNS kräver kompetens

På samma sätt som för IPv6 är det viktigt att ha eller anlita rätt kompetens vid införandet av DNSSEC. Det är lätt att göra fatala misstag om man inte förstår hur det fungerar. Om man inte är säker på vad och hur man ska göra kan det vara en god idé att vänta tills kompetent hjälp tillkallats.

Exempel på sådant som kan orsaka problem är att signaturerna i DNSSEC har en viss bestämd livslängd och därför måste förnyas regelbundet. Om de inte förnyas i tid så slutar domänen att fungera vilket även betyder att alla resurser som är knutna till domänen, till exempel e-post och webb, slutar fungera.

Vi ser också exempel på verksamheter som har en livslängd på signaturerna på kortare tid än en vecka och andra liknande parametrar vilket ger mycket lite utrymme för att reagera och reparera vid driftstörningar.

Att köpa nyckelfärdiga system är inte heller någon garanti för att det blir rätt. Erfarna konsulter har noterat att många (dyra) system som grundinställning (defaultvärde) både har för kort livslängd på signaturer och signerar om för sällan.

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

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

Varje domän har ett antal poster knutna till sig i DNS. Det är bland annat pekare till namnservrar (NS), till e-postservrar (MX) och liknande. En mycket viktig post som förknippas med DNSSEC kallas DS-post. DS-posten innehåller DNSSEC-specifik information för en DNSSEC-signerad domän. Med DNSSEC-signerad domän menar vi här en domän som har en DS-post publicerad i .se-zonen, vilket innebär att zonen måste fungera med DNSSEC påslaget. En DS-post måste matcha en i zonen publicerad DNSSEC-nyckel (DNSKEY), som i sin tur genererar signaturer över alla de poster som är publicerade i zonen.

6.1.7 DNSSEC i andra toppdomäner

Spridningen av DNSSEC har tagit fart bland toppdomäner över hela världen, i synnerhet efter signeringen av rotzonen år 2010.

Dessutom har de nya toppdomäner som läggs till i rotzonen som obligatoriskt krav att de måste vara signerade med DNSSEC.

Enligt aktuell statistik[8] är för närvarande 622 av totalt 795 toppdomäner som annonseras i rotzonen (2015-01-16) signerade med DNSSEC och av dessa har 615 publicerat information om sina nycklar i rotzonen. Dessa siffror förändras i takt med att nya toppdomäner godkänns och läggs till i rotzonen.

Motsvarande siffror för 2013 var 391 annonserade toppdomäner i rotzonen av vilka 198 var signerade. 191 av dessa hade publicerat information om sina nycklar i rotzonen. Detta ger en indikation på med vilket tempo rotzonen växer för närvarande.

6.2 Tester av elektronisk post

Elektronisk post (e-post) har funnits under mycket lång tid och var en av de första både riktigt använda och användbara applikationerna. Elektronisk post är fortfarande en av de allra vanligaste applikationerna. För att det ska fungera optimalt är det viktigt att sätta upp systemen korrekt från början och att använda tillgängliga funktioner som ökar säkerheten i användningen av e-post.

Under 2012 publicerade .SE en fördjupad rapport[9] om e-post där vi inte bara genomförde en enkätundersökning bland e-postansvariga utan också berättade mer om historik och statistik, förklarade hur e-post bör fungera och gjorde en djupdykning i en del tekniska parametrar genom mätningar med användning av vårt verktyg MailCheck[10].

[8] http://stats.research.icann.org/dns/tld_report/
[9] https://www.iis.se/docs/Elektronisk_post_med_kvalitet_och_finess.pdf
[10] https://mailcheck.iis.se

6.2.1 Stöd för transportskydd

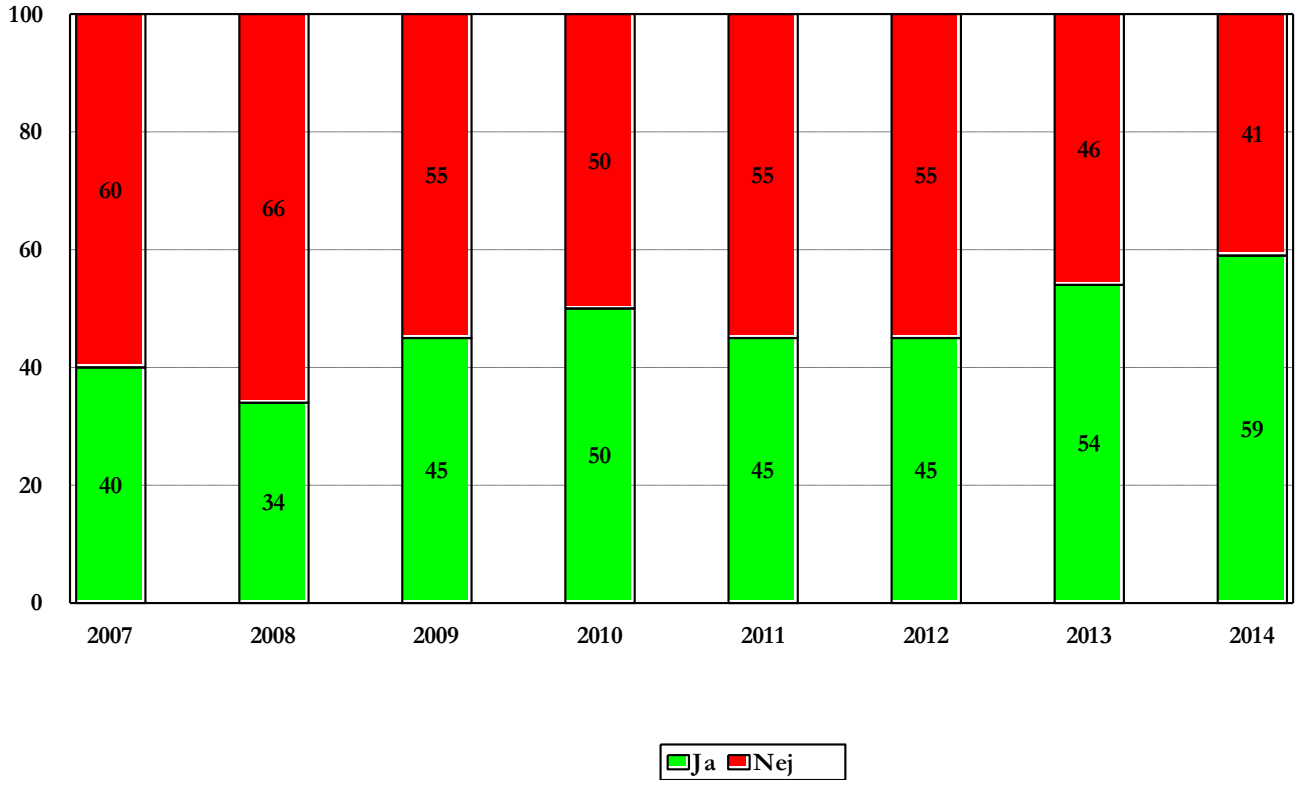
Transport Layer Security (TLS), ungefär transportlagersäkerhet på svenska, är en öppen standard för säkert utbyte av krypterad information mellan datorsystem.

TLS används för att kryptera kommunikationen mellan två enheter, varav den ena ofta är en webbserver och den andra en webbläsare, men e-postservrar och e-postprogram använder samma teknik vid överföring av elektronisk post (Simple Mail Transfer Protocol, SMTP). Tanken med att skydda den information som utväxlas mellan dessa enheter är att ingen annan på nätverket, till exempel det publika internet, ska kunna avlyssna eller förvanska informationen. Om du handlar eller förväntas lämna känslig information hos en webbtjänst via internet så faller det sig naturligt att TLS används för att kryptera exempelvis kreditkortsinformation eller personinformation.

TLS är en vidareutveckling av version 3 av SSL-protokollet och står under IETF:s kontroll. TLS erbjuder förutom sekretess (konfidentialitet) även riktighet (dataintegritet) och beroende på hur det används även äkthetsskydd (källskydd).

Av de undersökta verksamheterna 2011 respektive 2012 hade endast 45 procent stöd för TLS/SSL i sina e-postservrar. Vid undersökningen 2013 hade andelen ökat till 54 procent som har stöd för TLS. 2014 visar undersökningen att det är så mycket som 59 procent, alltså ytterligare fem procent av undersökningsgruppen som vidtar åtgärder för att skydda e-posttrafiken från insyn än tidigare. Diagrammet nedan visar utvecklingen för TLS åren 2007-2014.

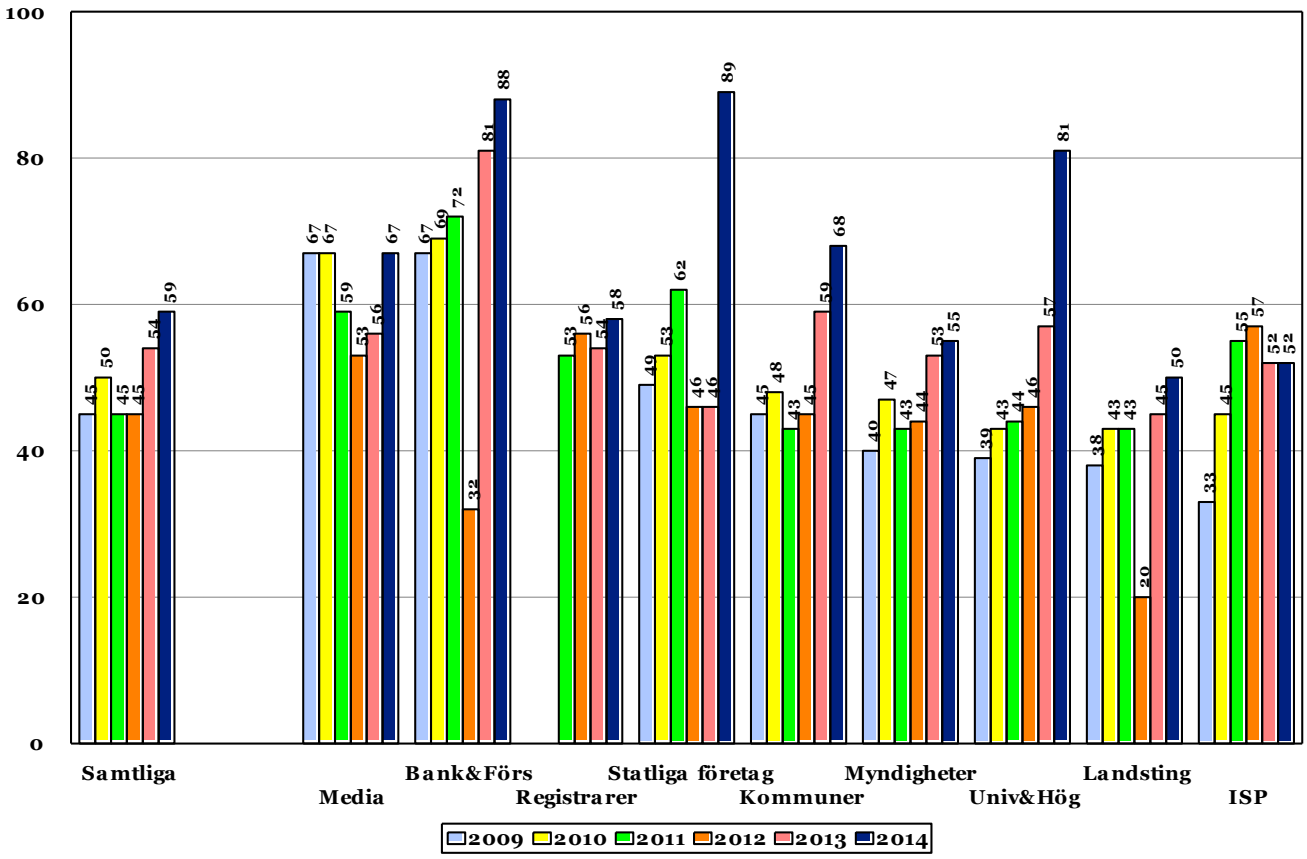
Diagram 13: Andel e-postservrar med stöd för TLS 2007-2014



Grönt visar andelen e-postservrar som har stöd för TLS, rött visar andelen som saknar sådant stöd.

I nästa diagram gör vi en jämförelse mellan de olika kategorierna och utvecklingen 2009-2014.

Diagram 14: E-postservrar med stöd för TLS per kategori 2009-2014



Här kan vi konstatera att det har hänt saker inom de flesta kategorier, framför allt att kategorierna Statliga företag och Universitet och högskolor haft en stark ökning. Media samt Bank och försäkring har också ökat om än inte lika kraftigt. Media är tillbaka på samma nivå som man hade 2009-2010. Kategorin Media är enligt vår uppfattning särskilt intressant i ljuset av det så viktiga meddelarskyddet, alltså vikten av att skydda uppgiftslämnare som förser journalister med information.

Även om FRA själva påstår[11] att de har infört tekniska filter som ska skydda journalister på medieredaktioner i Sverige från att bli avlyssnade av FRA så tror vi att det är bättre att själv ta kontrollen över det skydd man behöver.

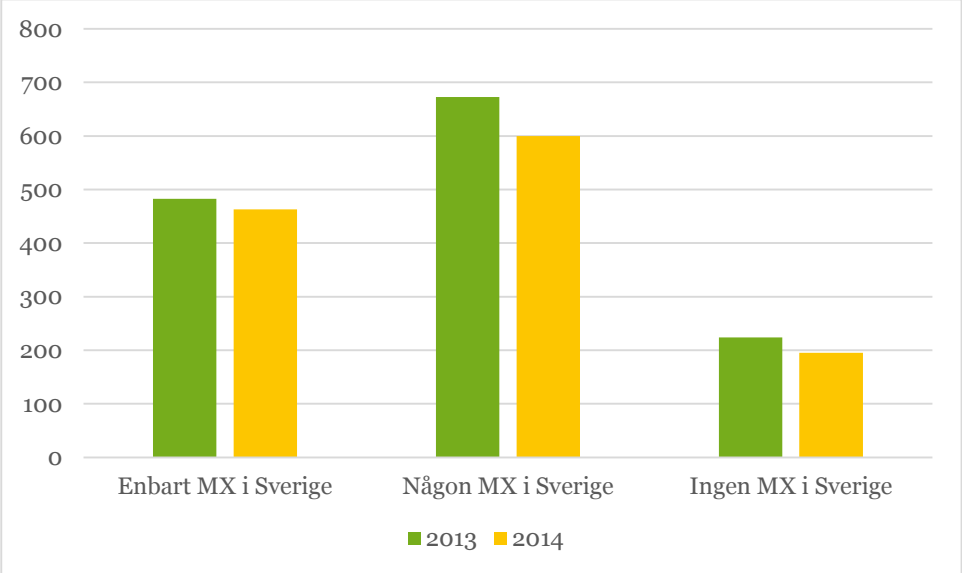
6.2.2 Placering av e-postservrar

Tack vare att IPv4-adresser fortfarande används parallellt med IPv6 i mycket stor utsträckning kan vi fortsätta mäta den uppskattade placeringen av e-postservrar, åtminstone för de servrar som använder IPv4-adresser.

[11] http://www.nyteknik.se/nyheter/it_telekom/allmant/article3878439.ece

Av det totala antalet domäner i undersökningsgruppen så omfattar e-postdelen av undersökningen 795 domäner (exklusive dubbletter). Av dessa saknar 61 domäner MX-post i DNS, 463 har enbart MX i Sverige, 600 har åtminstone någon MX i Sverige och 195 har MX som pekar på servrar enbart utanför Sverige. Det är alltså en minskning över hela linjen jämfört med 2013.

Diagram 15: Jämförelse - geografisk placering av domäners e-postservrar (MX) 2013-2014



Placeringen av e-postservrar utanför landet beror med största sannolikhet på att verksamheterna anlitar en tredjepartsleverantör för att hantera filtrering av virus och skräppost (spam) för deras räkning.

Utländska leverantörer av filtreringstjänster med många kunder skalar upp antalet servrar rejält. I vår undersökning har vi kontrollerat per domännamn om de har MX-pekare mot e-postservrar utomlands.

Vanligaste placeringarna 2014 är Storbritannien, och därefter i fallande skala USA, Tyskland, Danmark, Frankrike, Norge och Spanien.

En konsekvens av att till exempel myndigheters och kommuners e-postservrar är placerade utanför Sverige är att den offentliga förvaltningens e-post passerar ett främmande land på sin väg till mellan avsändare och mottagare. I medias fall gäller detsamma för e-post mellan exempelvis uppgiftslämnare och journalister. Med tanke på att kommunikationen ofta också transporteras oskyddad innebär det en onödig risk för exponering av känslig information.

Samtidigt som vi noterar att många verksamheter med förmodat känslig information skickar sin e-post till någon tredjepartsleverantör i utlandet ser vi att det fortfarande bara är 59 procent av de undersökta verksamheterna som har tekniska förutsättningar att använda kryptering för transportskydd av elektronisk post. Huruvida de faktiskt gör det och om det sker i båda riktningarna kan vi inte se.

Om kryptering inte används för transportskydd innebär det inte bara att den svenska utan också utländska underrättelsetjänster utan större svårighet kan avlyssna trafiken. Med facit i hand kan vi också konstatera att det görs – systematiskt och i en omfattning som få hade kunnat ana.

.SE har i samarbete med Journalistförbundet producerat en guide med titeln ”Digitalt källskydd – en introduktion”[12] som redovisar fallstudier, lösningar och konkreta tips på hur journalister och andra som hanterar känslig information kan värna om anonymiteten. Det finns också bra tips på hur den som har känslig information att dela kan skydda sig själv. Vi har även tagit fram extramaterial till guiden – ”Digitalt källskydd XL”[13] – som förklarar hur exempelvis kryptering används i praktiken.

6.3 Tester av webbtjänster

I stort sett alla verksamheter förmedlar information och tjänster via webbgränssnitt och många verksamheter är dessutom helt beroende av att deras webbtjänster alltid fungerar och är tillgängliga för kunder, samarbetspartners eller medborgare i samhället. Med den ökade användningen borde det också ställas högre krav på tillgänglighet och nåbarhet.

6.3.1 Krav på tillgänglighet för webbtjänster

Det är viktigt att överväga vilka konkreta åtgärder som behöver vidtas för att öka redundansen även för webbtjänster om man har någon typ av kritisk funktion som tillhandahålls via webb där man kan vänta sig starka reaktioner från sina användare, vare sig det är medborgare eller kunder, om det inte fungerar tillräckligt bra.

Organisationer som omsätter åtskilliga miljoner, kanske till och med miljarder, i sin verksamhet och har miljontals användare av tjänsterna varje år där tjänsterna representerar organisationens kärnverksamhet borde ha råd med redundans. Till exempel genom att sätta upp en spegelsajt hos ytterligare en leverantör, ha anslutning till fler än en internetoperatör och system för reservkraft. Det borde dessutom vara prioriterade åtgärder. Tyvärr saknas detta i många fall.

Å andra sidan kanske det är så att webbplatsen **inte** är en verksamhetskritisk funktion, och att det därmed inte heller spelar så stor roll om den skulle vara nere några timmar om året.

Oavsett vilket är det viktigt att de åtgärder som vidtas är resultatet av ett balanserat beslut om vilken tillgänglighet och nåbarhet som krävs.

Krav på tillgänglighet är en viktig del som aktualiseras alltmer, inte minst i ljuset av de överbelastningsattacker (DDOS-attacker) som blivit allt vanligare.

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

De senaste årens allvarliga sårbarheter i till exempel krypteringsprogramvaran OpenSSL borde även de föranleda en del åtgärder för att skydda verksamheten.

[12] https://www.iis.se/lar-dig-mer/guider/digitalt-kallskydd-en-introduktion/
[13] https://www.iis.se/docs/lar-dig-kryptering.pdf

Åtgärder för att motverka att man drabbas av den typen av sårbarheter är förhållandevis enkla:

- Systemadministratörer bör snarast se över möjligheterna att sluta stödja SSL v3 på sina webbplatser, särskilt på de webbplatser som **endast** stödjer SSL v3.
- De flesta webbläsare kan ställas in så att de inte använder SSL utan i stället TLS vilket är namnet på nyare versioner av SSL. Observera dock att detta kan omöjliggöra åtkomst till vissa webbplatser.
- Användare av Internet Explorer 6 bör snarast se över möjligheten att uppgradera till en senare version eller helt byta webbläsare då denna inte stödjer nyare versioner av SSL än 3.0.
- Webbläsarna Google Chrome och Mozilla Firefox arbetar med uppdateringar av sina produkter. Användare av dessa ska få en varning ifall en webbplats vill använda en äldre krypteringsteknik trots att modernare alternativ stöds.

I bilaga 10 redogör vi mer utförligt för vad som krävs. Vi redogör också för de senaste årens avslöjanden om avlyssning, sårbarheter i krypteringsprogramvara med mera.

6.3.2 Domänkollen

När webben var ny krävdes det mycket teknisk kunskap för att kunna bygga och underhålla en webbplats. Trots detta var det många internettekniker som tidigt tog avstånd från webben som teknisk plattform, vilket ledde till att det var fritt fram för informatörer, formgivare, reklammakare och andra icke-tekniker att bli ”webmaster”. Med denna bakgrund är det kanske inte så konstigt att många av dagens webbansvariga inte har rätt och relevant teknisk kompetens för att kunna bedöma den tekniska kvaliteten på sin egen webbplats när det gäller utförande, serverteknik, drift, säkerhet, DNS-hosting, och så vidare.

Det är rimligt att anta att många av de som äger en webbplats inte har den tekniska kompetens som krävs för att kunna bedöma kvaliteten på den webbplats de antingen köpt av en konsult eller byggt själva. Det finns enligt vår uppfattning därför ett stort uppdämt behov av en förenklad tjänst som kan ge snabba och enkla mätresultat presenterade på ett sätt som är begripligt även för den som inte är insatt i webbteknik. För den tänkta slutanvändaren är det i dag ganska svårt att göra bedömningen av den tekniska och säkerhetsmässiga kvaliteten på såväl webbplats som domännamn.

Därför har .SE startat ett projekt för att utveckla och erbjuda en tjänst som ska gå under namnet Domänkollen. Domänkollen kan skapa sinnesfrid för en stor grupp av människor som i dag inte har någon att vända sig till för att genomföra en teknisk kontroll. Alternativt kan Domänkollen automatiskt säga till när något är fel och ge tillräcklig teknisk information för att användaren ska kunna gå vidare med åtgärder för att förbättra den tekniska och säkerhetsmässiga kvaliteten på sin webbplats, genom att åtgärda själv eller ställa krav på sin leverantör.

Genom att erbjuda ett mycket enkelt verktyg för att redovisa mätbara kvalitetsvärden på en domän/webbplats ger vi allmänheten ett redskap för att kunna ställa bättre och mer relevanta krav på sina leverantörer samt lära sig mer om den teknik som krävs för att förbättra sin tjänst.

Domänkollen kan i sin enklaste form beskrivas som en webbplats med möjlighet att skapa rapporter som levereras dels direkt över webben, och dels som automatiserad HTML-mejl i abonnemangsform.

6.4 Tester av internationaliserade domännamn

Frågan hur olika nationella tecken ska kunna användas i domännamn har diskuterats under många år. Det har diskuterats både med avseende på teknik och på politik. Internationaliserade domännamn, IDN, har varit föremål för en diskussion med kulturella hänsyn som grund. Internet har en viktig roll att spela för bevarandet av kulturella intressen, särskilt med tanke på den demokratiska och opinionsbildande roll som nätet har. Minoritetsspråken måste kunna användas fullt ut även på internet. .SE, med ansvar för internets svenska toppdomän och Naturhistoriska riksmuseet som driver toppdomänen .museum, arbetar sedan flera år för att minoritetsspråken ska kunna användas i domännamn.

Målet med IDN är att kunna använda tecken på alla språk i de applikationer som använder domännamn som en del av sin adressering, till exempel elektronisk post och webb.

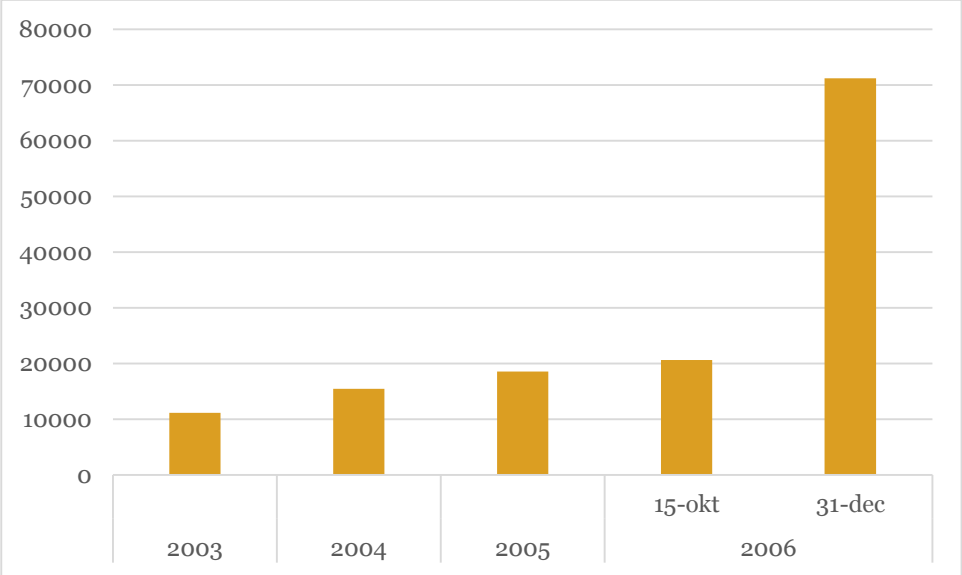
6.4.1 Utvecklingen i .SE

Redan 2003 blev det möjligt att registrera internationaliserade .se-domäner som innehöll tecknen å, ä och ö samt é och ü. För närvarande finns över 70 000 domännamn som innehåller bland annat dessa tecken, så kallade IDN-domäner (Internationalised Domain Names). Precis som med vanliga domännamn sker registrering av internationaliserade domäner genom .SE:s registrarer.

Det går sedan länge att använda IDN-domännamn i webbläsare medan det ännu inte finns någon färdig lösning för att hantera dessa tecken i e-post till vänster om snabel-a.

Från och med juli 2007 blev det även möjligt att registrera .se-domäner på de officiella svenska minoritetsspråken, finska, meänkieli (tornedalsfinska), samiska, romani och jiddish. Samtidigt blev också skrivtecknen för de övriga nordiska språken möjliga att använda i .se-domäner. Det innebar att närmare 200 nya tecken lades till de tidigare 42.

Diagram 16: Tillväxt IDN-domännamn per år 2003-2006



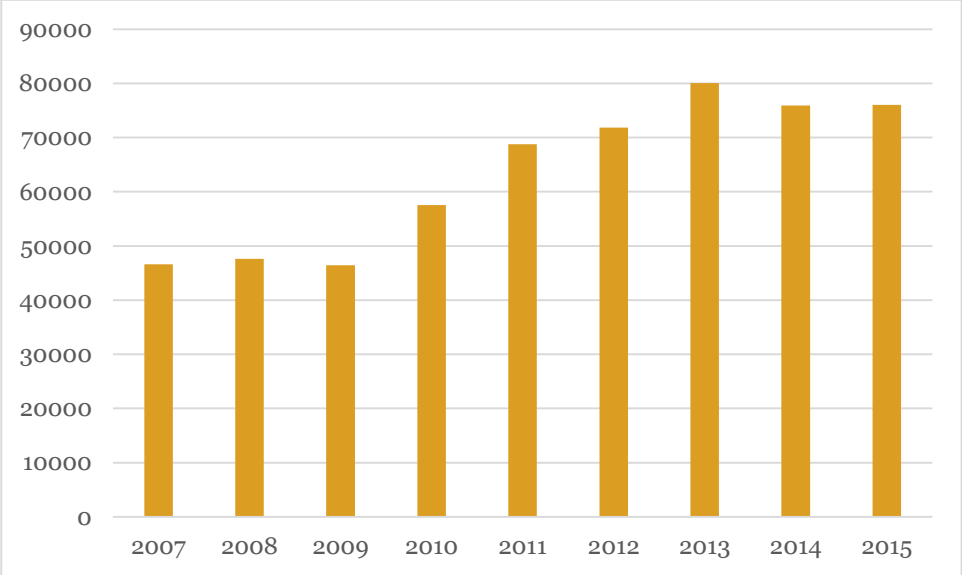
Som framgår av diagrammet ovan var tillväxten av IDN-domännamn sedan introduktionen i oktober 2003 relativt blygsam. .SE arbetade systematiskt för ett bredare genomslag via bland annat IDN-kampanjer riktade mot både registrarer och i viss mån innehavare. .SE genomförde under perioden oktober-december 2006 en kampanj för att öka medvetenheten om möjligheten att registrera internationaliserade domännamn. Under kampanjperioden subventionerades registrarerna för IDN-registreringar. Effekterna av kampanjen syns tydligt.

Under kampanjperioden registrerades hela 50 516 nya IDN-domännamn, vilket gav en ordentlig skjuts åt statistiken.

Nästa steg i genomförandet av IDN erbjöd möjlighet att registrera domännamn på de i Sverige enligt lag fastställda officiella minoritetsspråken; finska, meänkieli (tornedalsfinska), samiska, romani och jiddisch.

Den utökade repertoaren för IDN genomfördes 2007 och innehöll närmare 200 tecken. Först och främst rörde det sig om cirka 150 latinska tecken. Dessa ger stöd för samtliga språk som använder sig av det latinska alfabetet, inklusive de nordiska språken och de svenska minoritetsspråken, med undantag för jiddisch som kräver ytterligare omkring 30 tecken.

Diagram 17: Tillväxt IDN-domännamn per år 2007-2015 (januari)



Tekniskt skapades möjligheten genom att domännamn med internationaliserade tecken kodas om med så kallad ACE-kodning (ASCII Compatible Encoding). Domännamnssystemet (DNS) hanterar fortfarande bara tecknen a-z, 0-9 och bindestreck men de nya IDN-domännamnen kodas alltså om så att de passar in i det nuvarande systemet. Principen är att alla IDN-domännamn ges ett prefix (xn--) för att signalera att det **inte** är ett klassiskt domännamn men att det representerar en omkodning. Därefter kan domännamnet avkodas i till exempel webbläsare eller e-postprogram igen och visas med de aktuella tecknen angivna i sin ursprungliga form.

6.4.2 Vad undersökningen visar om IDN och offentlig förvaltning

.SE anser det angeläget att internetanvändare ska ha möjlighet att uttrycka sig på nätet på det språk och med de tecken de själva använder.

Det är också rimligt att domäninnehavare som i verksamhetens namn har något svenskt diakritiskt tecken representerat också använder sig av möjligheten att presentera sig på internet med det korrekta namnet. Det ökar till exempel möjligheten för deras användare att komma till rätt webbplats.

För att se hur det förhåller sig med den saken inom vår undersökningsgrupp har vi gjort en specialgranskning av just det området. Framför allt har vi synat den offentliga förvaltningen där vi förväntat oss att det finns gemensamma regler för användning av IDN-domännamn och webbplatser.

Resultatet är att några ”gör rätt”. De har sin webbinformation tillgänglig inte bara via en omdirigering från domännamnet med ringar och prickar till en variant utan diakritiska tecken utan presenterar även sitt innehåll under domännamnet med svenska tecken, exempelvis Säkerhetspolisen och Strålskyddsmyndigheten. Dessa tillhör dock en minoritet. Det är långt fler myndigheter som inte presenterar något innehåll med IDN-domännamnet och trots att de är innehavare av domänen så använder de den inte.

Ett exempel är myndigheten för Tillväxtanalys. De har registrerat och är innehavare av IDN-domänen men systemet skickar tillbaka ett felmeddelande om man skriver in domännamnet med ”ä”, alltså www.tillväxtanalys.se i webbläsarens adressfönster.

Andra exempel är sophiahemmethögskola.se som är parkerad hos en registrar trots att högskolan står som innehavare av domänen eller modernaförsäkringar.se som ger tillbaka en felkod.

Fenomenet är även vanligt hos kommunerna. Undersökningen (som till stora delar har gjorts manuellt) ger varierande resultat. Allt från att returnera en blank sida till felmeddelanden som betyder att den begärda sidan inte finns.

Av 290 kommuner är det 121 som har minst ett svenskt tecken i namnet. Av dessa är det 37 kommuner som inte använder sina idn-domäner, trots att de i de allra flesta fall är innehavare av domänen i fråga.

I hela zonen är det 73 458 domäner av totalt 1 269 185 (15 januari 2015) som börjar med strängen “xn—“, vilket markerar att det är ett IDN-domännamn.

I tabellen på nästa sida redovisar vi status för användning av IDN-domännamn hos svenska kommuner.

Tabell 1: Status för IDN hos kommunerna

Kommun	Returnerar	Innehavare
Övertorneå	Blanksida utan information	kommunen
Överkalix	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Östra Göinge	Blanksida utan information	kommunen
Östhammar	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Örkelljunga	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Örebro	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Älmhult	Service Temporarily Unavailable	privatperson
Åsele.se	Parkeringssida	Name Navigation
Årjäng	Parkeringssida	Safenames
Västervik	Blanksida utan information	kommunen
Täby	Blanksida utan information	kommunen
Trollhättan	HTTP Error 404. The requested resource is not found	kommunen
Tjörn	Blanksida utan information	kommunen
Timrå	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Strömsund	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Strömstad	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Skellefteå	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Ovanåker	Parkeringssida	privatperson
Olofström	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Nynäshamn	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Mönsterås	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Malung-Sälen	www.malung-sälen.se: Webbsidan inte tillgänglig, DNS-sökning misslyckades. www.malungsälen.se omdirigeras till http://www.malung-salen.se/	kommunen
Lidingö	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Laxå	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Köping	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Kävlinge	omdirigeras till http://www.kartaover.se/karta.php?%C3%B6ver=k%C3%A4vlinge	privatperson
Kungälv	Blanksida utan information	kommunen
Kungsör	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Järfälla	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Höganäs	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Härryda	404 - The requested resource is not available	kommunen
Gävle	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Gullspång	404 - The requested resource is not available	kommunen
Grästorp	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Eksjö	Parkeringssida	privatperson
Ekerö	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen
Burlöv	Webbsidan inte tillgänglig DNS-sökning misslyckades	kommunen

6.4.3 Internationaliserade domännamn i andra landskodtoppdomäner

En landskodtoppdomän (ccTLD) är en toppdomän som används och reserverats för ett land eller territorium som till exempel .se för Sverige, .uk för Storbritannien eller .de för Tyskland. Varje landskodstoppdomän har en förvaltare som sätter reglerna för fördelning av domäner.

ccTLD:er skiljer sig från generiska toppdomäner (gTLD:er) som är toppdomäner som inte är knutna till ett land eller territorium och som är öppna för registranter från hela världen.

Ett internationaliserat domännamn (IDN) är ett domännamn som innehåller tecken som används i den lokala representationen av språk och alltså inte är begränsade till de 26 bokstäver som finns i det grundläggande latinska alfabetet (a-z). En IDN-domän kan innehålla latinska bokstäver med diakritiska tecken, vilket krävs enligt många europeiska språk, eller kan bestå av tecken från icke-latinska skript som arabiska eller kinesiska. En IDN ccTLD är ett internationaliserat domännamn på toppdomännivå, exempelvis är IDN-toppdomänen för den Ryska Federationen .РФ som är den kyrilliska versionen av .rf.

EURid och Unesco har forskat på internationaliserade domännamn (IDN) sedan 2010 och publicerar årliga rapporter. Den för 2014 har titeln ”World report on Internationalised Domain Names 2014”[14]. Rapporterna omfattar uppgifter om IDN, som status, fallstudier och en jämförande analys av de faktorer som kan påverka IDN:s utbredning (positivt eller negativt).

Organisationen CENTR genomför också regelbundna undersökningar. 2014 var det 75 procent av de tillfrågade registryerna som erbjöd IDN och flera andra arbetade med förberedelser. Av de registryer som infört IDN erbjuder 75 procent skript som krävs för att stödja det nationella språkbruket, medan resterade 24 procent erbjuder en utökad teckenuppsättning.

Överlag kan vi konstatera att takten på införandet av IDN i toppdomäner är förhållandevis blygsam. Satt i relation till registryernas förväntningar har IDN minskat mellan 2013 och 2014, liksom registrarernas stöd för och domäninnehavarnas kännedom om IDN.

[14] http://www.eurid.eu/files/publ/IDNWorldReport2014_Interactive.pdf

[Sidan har medvetet lämnats blank.]

7 Observationer – jämförelse med hela .se-zonen

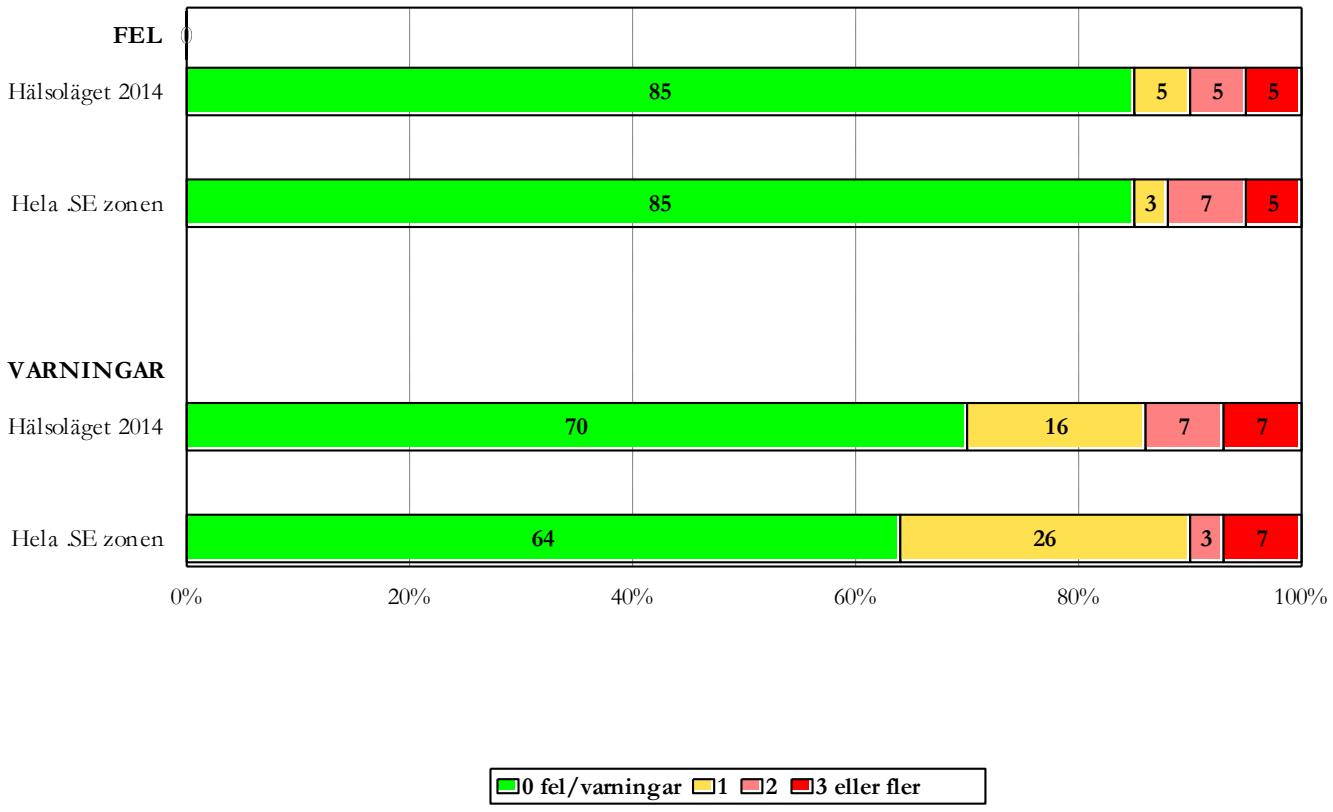
För att kontrollera om vår undersökningsgrupp är i bättre eller sämre skick när det gäller hanteringen av domännamnssystemet med mera än .se-domäner i allmänhet har vi som vanligt gjort ett slumpmässigt urval motsvarande en procent domäner ur hela .se-zonen för att ha som jämförelse.

I diagrammen nedan representerar ”Hälsoläget 2014” den aktuella undersökningsgruppen med sina 913 domäner medan ”Hela .se-zonen” representerar det slumpmässiga urvalet motsvarande en procent av hela .se-zonen eller 12 791 domäner.

7.1 Fördelning av fel

Vi tittar som tidigare först och främst på fördelningen av fel och varningar, och hur undersökningsgruppen Hälsoläget 2014 som ändå innehåller en hel del kritiska funktioner och verksamheter förhåller sig till jämförelsegruppen Hela .se-zonen.

Diagram 18: Andel fel i Hälsolägetrespektive Hela .se-zonen 2014



Enligt resultaten från 2014 års undersökning är det fortfarande lika många felfria domäner i undersökningsgruppen som i kontrollgruppen för .se-zonen som helhet.

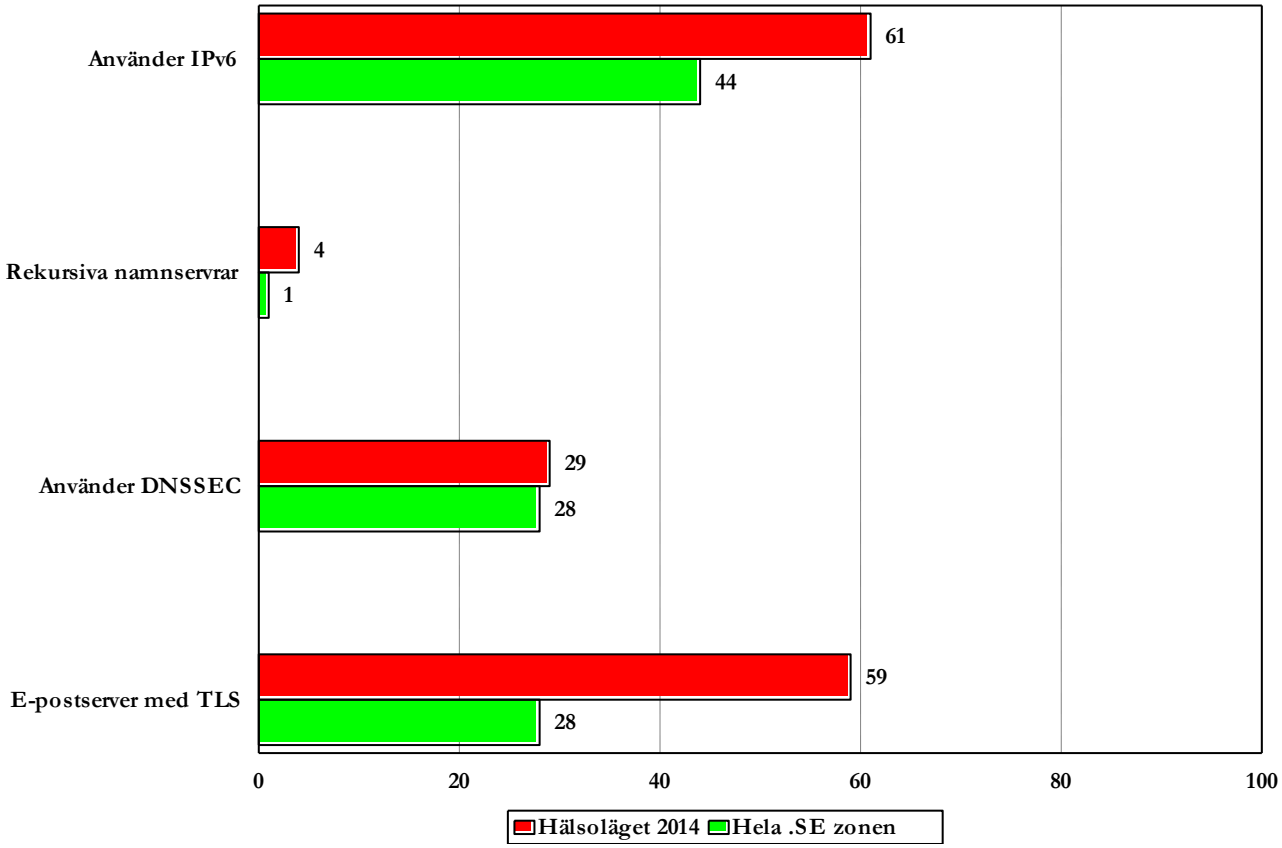
7.2 Skillnader mellan undersökningsgruppen och jämförelsegruppen

De största skillnaderna mellan undersökningsgruppens 913 och jämförelsegruppens 12 791 domäner är framför allt att det är långt fler i undersökningsgruppen som använder IPv6, 54 procent mot 25 för hela .se-zonen. Det är också långt fler som använder TLS för e-post i undersökningsgruppen, 54 procent mot 27 procent för .se-zonen som helhet.

Trenden med fler i undersökningsgruppen som har öppna rekursiva namnservrar än i hela .se-zonen består. År 2012 var det 10 procent i undersökningsgruppen mot 3 procent i jämförelsegruppen, 2013 är motsvarande andelar 5 respektive 1 procent.

Andelen som använder DNSSEC fortsätter att öka 2014 jämfört med 2013, 29 procent i undersökningsgruppen respektive 28 procent i hela .se-zonen. Alltså är det 2014 fler i undersökningsgruppen som har domäner signerade med DNSSEC än i jämförelsegruppen. Tidigare år har det varit tvärtom. 2013 var andelarna 22 procent i undersökningsgruppen respektive 25 procent i jämförelsegruppen för .se-zonen som helhet.

Diagram 19: Jämförelse mellan Hälsoläget och hela .se-zonen 2014



I diagrammet ser vi skillnaderna mellan Hälsoläget 2014 (röd stapel) och hela .se-zonen 2014 (grön stapel) för de olika delar som vi har studerat. Generellt finns det något mer av allt som kan uppfattas som positivt i undersökningsgruppen än i jämförelsegruppen, men det finns också mer av det som är mindre bra, som öppna rekursiva namnservrar. När det gäller utbredningen av DNSSEC är det fortfarande lika vanligt (eller ovanligt) i båda grupperna.

[Sidan har medvetet lämnats blank.]

8 Råd och rekommendationer

Efter att vi 2014 för åttonde gången har genomfört vår sista omgång mätningar, åtminstone med den här utformningen, med ett relativt positivt resultat jämfört med 2013 framstår det ändå som att det fortfarande finns ett behov av större samordning mellan olika intressenter för bättre säkerhet och nåbarhet på den svenska delen av internet. Inte minst möjligheter till effektivitetsvinster och kostnadsbesparingar.

I första hand måste åtminstone verksamheterna inom den offentliga förvaltningen kunna enas om relevanta upphandlingskrav, till exempel kring filtrering av e-post och generell användning av kryptering, men också om gemensamma rekommendationer för hantering av domännamn och domännamnssystemet samt gärna om en handlingsplan för genomförandet av några viktiga aktiviteter:

- Kritiska resurser i Sverige bör ha namnservrar som är anslutna till flera operatörer samtidigt, till exempel med användning av tekniken Anycast. Det finns behov av att någon på central nivå bestämmer vad som är att betrakta som en kritisk resurs.
- Sätt upp en gemensam sekundär DNS-drift för kritiska tjänster exempelvis via de svenska internetknutpunkterna dit dessa kan anslutas som en extra åtgärd för att skapa redundans. En sådan funktion kan regleras genom avtal.
- Inför gemensamt upphandlade funktioner för virustvätt och rensning av skräppost med krav på servrar placerade i landet. Det skulle bli effektivare, förmodligen spara resurser och göra det enklare att göra revision. Samtidigt skulle det förhindra att myndighetsinformation lämnar landet.
- Utfärda riktlinjer om vad som är acceptabelt när det gäller skräpposthantering och virustvätt i offentlig förvaltning. Det borde till exempel inte vara accepterat att svenska myndigheter och kommuner skickar all e-post utomlands utan att samtidigt ställa relevanta och enhetliga krav på transportskydd och kryptering.
- Utfärda rekommendation om att svenska myndigheters e-postservrar, för kritiska verksamheter med känslig information, fysiskt bör ligga i Sverige för att skydda spårbarheten av information mellan myndigheter och för att skydda mot de konsekvenser som följer av FRA-lagen och signalspaning från främmande makt.
- Ställa krav på offentlig förvaltning om att använda TLS för käll- och transportskydd av både e-post och webb.
- Göra samtliga publika tjänster tillgängliga över IPv6 inom hela den offentliga förvaltningen snarast.
- Skydda webbservrar med certifikat som är utfärdade av allmänt accepterade certifikatutfärdare och ha kontroll över deras giltighet.
- Införa DNSSEC på alla domäner i den offentliga förvaltningen.

Utöver dessa finns det ytterligare åtgärder som behöver vidtas bland annat på operatörsnivå för att stärka infrastrukturen för internet. Dessa åtgärder landar huvudsakligen på Post- och Telestyrelsen, PTS, som är den myndighet som är tillsynsansvarig myndighet enligt bland annat lagen om elektronisk kommunikation, och här handlar det om att formulera krav som bör ställas på operatörer. År 2014 inträffade 47 allvarliga störningar i svenska nät för internet och telefoni. Motsvarande siffra 2013 var 49. Många av avbrotten har varit långvariga och vid flera tillfällen blev det bland annat omöjligt att komma fram till 112. Siffrorna är hämtade ur en genomgång av rapporter till PTS och sammanställda av Dagens Nyheter[15].

PTS kommer att formulera hårdare krav på operatörerna för att de ska vara bättre rustade mot avbrott. Det omfattar bland annat krav på redundans, att klara av långvariga strömavbrott genom att ha reservkraft upp till 24 timmar och högre krav på övervakning dygnet runt. De har snarare karaktären av skall-krav än råd och rekommendationer vilket ytterst kan leda till vite för den operatör som inte uppfyller kraven. Enligt PTS plan ska de nya föreskrifterna fastställas under våren och träda i kraft från den 1 september 2015.

Den förra regeringen föreslog att det senast 2013 ska finnas en gemensam internetspecifikation med olika robust- och säkerhetskrav (typfall) framtagen för myndigheter och att PTS skulle få i uppdrag att genomföra – något sådant uppdrag lämnades dock aldrig till PTS. Trots att den förra regeringen rekommenderade att alla myndigheter senast 2013 bör använda sig av DNSSEC och vara nåbara med IPv6 så kan vi inte se att något av dessa mål uppfyllts ännu, även om 2014 ser ljusare ut för DNSSEC och framför allt för IPv6 jämfört med tidigare år.

[15] http://www.dn.se/ekonomi/hardare-regler-efter-haverierna-i-telenatet/

Bilaga 1 - Förkortningar och ordförklaringar

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

BCP Best Common Practice, branschstandard.

DANE DNS-based Authentication of Named Entities. Arbetsgrupp inom IETF.

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 ett domännamn (till exempel iis.se) till en IP-adress vilken används för kommunikation över IP-nät, till exempel internet.

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

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

DNS-server Se *Namnserver*.

Domän Beteckning på en nivå i domännamnssystemet.

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

DS-post En posttyp i DNS som innehåller DNSSEC-specifik information för en DNSSEC-signerad domän.

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

IP-adress Numerisk adress som tilldelas varje dator som ska vara nåbar via internet. Förekommer som IPv4-adresser och IPv6-adresser.

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

Namnserveroperatör Den som tillhandahåller en DNS-tjänst för internetanvändare.

Registrar	Ackrediterad återförsäljare av .SE-domäner.
Resolver	Den programvara som översätter namn till *IP-adresser* eller tvärtom.
Secure DNS	Se *DNSSEC*.
SOA	Start of Authority, en pekare till var information om en zon börjar.
TLS/SSL	TLS är en standard för kryptering av bland annat webbtrafik under transport. Kommunikation med http med TLS kallas https. SSL ersätts numera av IETF:s öppna standard TLS.
TLSA	The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.
Zon	Avgränsning av det administrativa ansvaret för domännamnsträdet. En *zon* utgörs av en sammanhängande del av domännamnsträdet som administreras av en organisation och lagras på dess *namnservrar*.
Zonfil	Datafil där man lagrar den information som behövs om en *zon* för att adressering med *DNS* ska kunna användas.

Bilaga 2 - Om DNS och om undersökningen

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

Även om undersökningen rönt stort intresse genom åren kan vi konstatera att trenden är en förbättring över tiden på de allra flesta områden. Vi har beslutat att detta är det sista året som vi gör Hälsolägetundersökningen i sin nuvarande form. Undersökningen ingår i ett långsiktigt fokusområde som går under namnet Internets ekosystem och omfattar fler områden och mätningar. Inom ramen för området har vi tillsammans med det franska registryt Afnic utvecklat en modernare version för att genomföra tester av DNS under namnet Zonemaster (se bilaga 3).

.SE, som sedan 1997 har ansvaret för teknisk drift och administration av alla namnservrar för .se-domänen och sedan september 2013 även för driften av .nu-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 med sina mer än 30 år på nacken och har genom åren visat prov på enastående skalbarhet och robust design. Ingenting har i princip behövt ändras i de grundläggande protokollen trots den enorma tillväxt som skett på internet. DNS har emellertid kommit att bli allt viktigare för en fungerande kommunikation mellan internetanvändare världen över, och det ställer krav på att DNS håller hög kvalitet i alla delar.

DNSSEC

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

Därför har man utvecklat säkerhetstillägg till DNS som fått beteckningen DNSSEC (DNS Security Extensions). DNSSEC bygger på kryptografiska nycklar som används för signering av innehållet i zonfilerna. Genom att validera signaturer på svaren i DNS går det att säkerställa att dessa verkligen kommer från rätt källa och inte har ändrats under överföringen.

.SE:s lansering av DNSSEC för säkrare DNS år 2005 har också bidragit till att ett ökat fokus hamnat på DNS och DNS-drift. Den som har för avsikt att göra

sin DNS-infrastruktur säkrare genom att använda DNSSEC inser tämligen snabbt att införandet inte låter sig göras med mindre än att det först görs en översyn av den egna DNS-infrastrukturen som helhet.

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

Att internets rotzon signerades sommaren 2010 satte fart på spridningen av DNSSEC. Eftersom rotzonen är toppen av DNS-hierarkin är det därmed enklare för de underliggande toppdomänerna att införa DNSSEC. I samband med att ICANN 2013 inledde processen med att godkänna ett stort antal nya toppdomäner som alla har som obligatoriskt krav att de ska vara signerade med DNSSEC gör att spridning ökar än mer.

IPv6

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

IPv4-adresser består av 32 bitar. Därmed kan det i IPv4 bara finnas drygt fyra miljarder unika adresser. När världen blev alltmer uppkopplad resulterade det i en adressbrist på internet och de sista IPv4-adresserna delades ut under 2010.

Lösningen för att komma till rätta med adressbristen var att införa en annan version av protokollet, IPv6, som har 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 kan varje nu levande individ få 5×10^{28} adresser **var**. Varje individ skulle alltså kunna förfoga över 50 000 000 000 000 000 000 000 000 000 egna IP-adresser. En så riklig tillgång till IP-adresser öppnar upp för applikationer som annars blir svåra att förverkliga i praktiken till exempel inom områden som Internet of Things (ungefär Sakernas internet) och intelligenta hem. Det finns en räknare på https://samsclass.info/ipv6/exhaustion.htm som räknar på när IPv6-adresserna beräknas ta slut. Det är humor.

Tjänster för e-post och webb

På .SE är vi intresserade av att titta närmare på hur verksamheter hanterar sin kommunikation i övrigt, främst när det gäller säkerhet, tillgänglighet och robusthet för de vanligaste tjänsterna elektronisk post och webbtrafik. Vi arbetar kontinuerligt med vidareutveckling av mätverktyg för att kunna se fler detaljer, inte minst kring parametrar som rör webbapplikationer, men också mer detaljer kring användning av e-post.

Bilaga 3 - Om .SE:s testverktyg

Hälsoläget

Hälsoläget är en plattform där vi har en verktygslåda som vi har använt för att genomföra den årliga undersökningen.

DNSCheck

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

Övriga verktyg

Andra verktyg som används i undersökningen är Page Analyzer och Whatweb. Page Analyzer mäter prestanda och prestandapåverkande parametrar som antalet externa resurser, och resursernas storlekar. Whatweb analyserar webbtekniken.

Dataanalys

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

Zonemaster är framtiden

Verktyget DNSCheck för test av DNS-delegeringar har en lång historia. Det började som ett verktyg för .SE (NIC-SE) för att testa delegeringar, och utvecklades av Patrik Fältström redan 2003. Originalet lever vidare på dnscheck.se. Det skrevs senare om av Jakob Schlyter, Kirei, och har löpande förbättrats och förändrats sedan dess. Det är i den här formen vi i dag känner till DNSCheck.

Med tiden har vi dock sett DNSChecks begränsningar i formellt testande av DNS, och har övervägt olika alternativ till att skriva om verktyget. När vår franska motsvarighet Afnic som bland annat driver toppdomänen .fr, befann sig i samma situation med sitt verktyg Zonecheck såg vi en fördel med att inleda ett samarbete kring att skriva ett nytt verktyg.

Med .SE:s uppdrag för ICANN där vi testar de nya gTLD:erna så fick vi med oss ett stort antal testspecifikationer för DNS. .SE ser chansen att göra ett ännu bättre jobb med det här nya verktyget, och för första gången har vi riktigt bra specifikationer för hur man testar en DNS-delegering. Det är med dessa specifikationer det gemensamma arbetet med Afnic inleddes. Vi utgick från att vi skulle implementera all funktionalitet som fanns i både Zonecheck och

DNSCheck, och började med att dokumentera alla dessa krav på både tester och funktioner. När kraven fanns på plats kunde vi börja skriva noggranna specifikationer för hur den nya programvaran skulle bete sig, och exakt hur och vad den skulle testa.

Master Test Plan

Det vi har i dag är alltså ett helt nytt verktyg, Zonemaster, med tydliga krav och specifikationer för hur vi testar DNS-delegeringar. Testspecifikationerna finns dokumenterade i något som är en standard för testspecifikationer, IEEE 829-2008, men vi har valt att bara behålla de delar som är relevanta för det här området. Huvuddokumentet är således en Master Test Plan som sedan gräver ner sig till de olika områden vi testar, adresser, nåbarhet, syntax, DNSSEC och så vidare, för att sedan bli så noggrant som ett enskilt Test Case.

Målet med att dokumentera testerna på det här sättet är flera. Det viktigaste är att användaren vet exakt vad det är vi testar och varför. Men det finns flera skäl, vi vill att Zonemaster ska bli ett referensverktyg för tester av DNS på det här sättet. Kommande steg blir att öppna upp arbetet med testspecifikationerna och förhoppningen är att vi till slut kan få det genom IETF och publicera ett BCP-dokument (Best Current Practice) som RFC.

Stabil version släppt

Alla tester som specificerats är implementerade i Zonemaster Engine. Det finns utförliga installationsinstruktioner för den som själv vill ladda ner och testa koden. Zonemaster är stabil och släppt som en version vi kallar 2014.1. Vi har dock många saker planerade och fler tester att specificera och implementera. Ett nytt område som är lite svårare att testa – har vi lärt oss genom vårt samarbete med ICANN – är mätningar av Anycast-nät. Den typen av mätningar kräver att man testar från olika platser på nätet för att få en rättvis vy av hur DNS ser ut. Det finns ännu ingen som beskrivit hur man bäst testar en delegering av den här typen. Vår förhoppning är att Zonemaster blir först.

Bilaga 4 – De vanligaste felen i DNS - detaljbeskrivningar

De vanligaste felen i DNS bland undersökta domäner och namnservrar som genererar antingen fel eller varning enligt vår definition har under alla år då vi genomfört undersökningen varit i princip desamma, även om de minskat i antal:

- Namnservern svarar inte på anrop via TCP. Detta beror troligtvis på att DNS-servern inte är korrekt uppsatt eller på felaktigt konfigurerade brandväggar. Det är en ganska utbredd missuppfattning att DNS inte behöver kunna kommunicera enligt TCP-protokollet (om den inte tillhandahåller zonöverföringar). TCP är emellertid ett krav enligt standard (RFC 5966, *DNS transport over TCP implementation requirements*[16]) och trenden är att behovet av TCP ökar då nya protokoll som IPv6 och DNSSEC leder till att det används i större omfattning än tidigare. Felet är en indikation på att den som har konfigurerat namnservern eller brandväggen inte har tillräckligt aktuella kunskaper om DNS.

- Verksamheten har ingen konsekvent namnserveruppsättning. De namnservrar (NS) som listats med NS-poster i en barnzon skiljer sig från den information som finns i DNS för föräldrazonen, och därmed kan namnservrarna inte svara auktoritativt och korrekt för domänen. Om informationen inte är konsekvent påverkar det tillgängligheten för domänen negativt och tyder på brister i den interna DNS-hanteringen. Följande är exempel på sådan inkonsekvens:
  - IP-adressen för en namnserver är inte samma hos barnzonen som hos föräldrazonen i nivån ovanför. Detta är ett konfigurationsfel och bör korrigeras så snart som möjligt. Sannolikt har administratören för domänen glömt att göra en uppdatering vid förändring.
  - En namnserver finns listad i föräldrazonen men inte i barnzonen. Det här är troligtvis ett administrationsfel. Föräldrazonen behöver snarast uppdateras så att den listar samma namnservrar som finns listade hos barnzonen. Konsekvensen av ett sådant fel är att den redundans som någon har försökt åstadkomma i praktiken inte finns.

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

- DNS-servern svarade inte på anrop via UDP. Detta beror troligtvis på att DNS-servern inte är korrekt uppsatt eller på en felaktigt konfigurerad brandvägg. En namnserver som varken svarar på TCP eller UDP är inte nåbar över huvud taget och då ligger felet sannolikt någon annanstans, till exempel i förbindelsen till namnservern eller att servern inte har en korrekt angiven IP-adress. Våra tester på namnservern avslutas direkt om båda dessa tillstånd har konstaterats.

[16] http://tools.ietf.org/search/rfc5966

- Endast en namnserver hittades för domänen. Det bör alltid finnas minst två namnservrar för en domän för att kunna hantera tillfälliga problem med förbindelserna. Om denna enda server eller förbindelsen till servern slutar fungera blir tjänsterna som pekas ut från namnservern också onåbara. Vi räknar namnservrar separat för IPv4 och IPv6. Att ha för få servrar anser vi vara allvarligare för IPv4 (ger fel) medan vi i nuläget betraktar det som mindre allvarligt för IPv6 (ger en varning) eftersom det är under införande. Det är givetvis bättre att ha en ensam namnserver som kommunicerar via IPv6 än att inte ha någon alls.

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

- SOA-serienumret (Start of Authority) är inte detsamma på alla DNS-servrar. Detta beror vanligtvis på en felkonfiguration, men kan ibland bero på långsam spridning av zonen till sekundära DNS-servrar. Det innebär att den som frågar efter resurser under en domän kan få olika svar beroende på vilken namnserver som får frågan eftersom de då innehåller olika versioner av information om domäner.

Bilaga 5 - Branschstandard för DNS-tjänst med kvalitet

För den mer tekniskt bevandrade läsaren redovisar vi i denna bilaga mer detaljerat 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.

1. Minst två namnservrar

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

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

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

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

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

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

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

3. Auktoritet

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

Förklaring: Vid kontroll mot servrarna för underdomänen ska man kunna få konsekventa och repeterbara auktoritativa svar för SOA- och NS-poster för

underdomänen. Detta gäller samtliga servrar som finns listade i den underliggande zonens DNS för domänen i fråga.

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

4. Serienummer för zonfil

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

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

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

5. Kontaktadress

Rekommendation: Zonkontaktadressen i SOA-posten ska vara nåbar.

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

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

6. Nåbarhet

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

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

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

Bilaga 6 – Mer information om DNSSEC

DNSSEC står för DNS Security Extensions och är en utökning av DNS i syfte att göra säkrare uppslagningar av internetadresser för exempelvis webb och e-post. Den ökade betydelsen av DNS har gjort DNSSEC allt mer aktuellt med åren.

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

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

Cacheförgiftning innebär att en situation skapas, antingen genom en attack eller oavsiktligt, som förser en namnserver med DNS-data som inte kommer från en auktoritativ källa. Ett av de mest välkända exemplen på detta är den under 2008 mycket uppmärksammade Kaminskybuggen.

Farmning innebär att någon får själva innehållet i DNS att peka på felaktiga servrar. Rent konkret innebär det att en webbadress för exempelvis en bank kan pekas om till en helt annan server, men för besökaren ser det fortfarande i adressfältet ut som att det är rätt server han besöker.

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

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

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

Vad DNSSEC skyddar mot

DNSSEC används för att säkra DNS från missbruk och man-in-the-middle-attacker som cacheförgiftning.

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

För gemene man innebär DNSSEC en minskad risk för att bli utsatt för bedrägerier vid till exempel bankaffärer eller shopping på nätet eftersom det blir

lättare för användaren att fastställa att man verkligen kommunicerar med rätt bank eller butik och inte någon bedragare.

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

Vad DNSSEC inte skyddar mot

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

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

Lär dig mer om DNSSEC

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

Här finns några pekare till ytterligare information:

Introduktion till och krav på DNSSEC: http://www.ietf.org/rfc/rfc4033.txt

Beskrivning av resursposter (resource records for the DNS Security Extensions) i DNSSEC: http://www.ietf.org/rfc/rfc4034.txt

Protokollmodifieringar för DNSSEC: http://www.ietf.org/rfc/rfc4034.txt

Ett ramverk för hur man disponerar en säkerhetsdeklaration för DNSSEC: https://tools.ietf.org/html/rfc6841

Rekommendationer för det praktiska införandet av DNS och DNSSEC: http://tools.ietf.org/search/rfc6781/

Vägledning med rekommendationer för införande av DNSSEC: https://www.iis.se/domaner/teknik/dnssec/vagledning-for-inforande-av-dnssec/

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

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

Nyheter om DNSSEC sprids regelbundet av **DNSSEC Deployment Initiative:** http://www.dnssec-deployment.org/. Där kan man även se en animerad kartbild som visar spridningen av DNSSEC i ccTLD:er från 2005 fram till i dag och en framtidsbild baserad på publicerade och uttalade planer om den framtida utvecklingen från olika toppdomäner.

DNSSEC-deployment har även en e-postlista som vem som helst kan prenumerera på, ställa frågor och hålla sig uppdaterad om utvecklingen på området.

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

OpenDNSSEC

OpenDNSSEC är en nyckelfärdig programvara, eller ett verktyg för att underlätta införandet och användningen av DNSSEC. OpenDNSSEC signerar DNS-informationen momentet innan den ska publiceras på en auktoritativ namnserver. OpenDNSSEC tar en osignerad zonfil, lägger till signaturer och andra poster för DNSSEC och skickar filen vidare till de auktoritativa namnservrarna för den aktuella zonen.

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

.SE startade och deltog aktivt i utvecklingen av ett nyckelfärdigt system för signering av zonfiler med DNSSEC för att underlätta spridningen av DNSSEC. 2014 lämnade .SE över den fortsatta utvecklingen till NLNetLabs.

Läs mer på: http://www.opendnssec.org/

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

Bilaga 7 - Öppna rekursiva namnservrar

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

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

Grundproblemet är egentligen inte öppna rekursiva namnservrar utan att operatörerna inte filtrerar trafik på avsändaradresser (ingress filtering). Om de gjorde det skulle öppna rekursiva resolvrar kanske inte betraktas som ett problem. Då sådan filtrering är relativt svår och kostsam att införa för operatörerna, vilket gör att de drar sig för att genomföra detta, behöver vi under tiden försöka begränsa de skador som DDOS-attacker orsakar tills dess att operatörerna har åtgärdat grundproblemet. Att stänga en rekursiv resolver är en relativt enkel uppgift som det är mödan 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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

DNS Amplification attacks, en bra beskrivning av hur attacken går till och vad den innebär: https://www.us-cert.gov/ncas/alerts/TA13-088A

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

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

BIND 9 Administrator Reference Manual. Innehåller exempel på konfigurering, praktiska tips och en detaljerad beskrivning av funktioner i BIND:
https://kb.isc.org/article/AA-00845/0/BIND-9.9-Administrator-Reference-Manual-ARM.html

Bilaga 8 - Åtgärder mot skräppost

DKIM

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

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

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

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

För att upptäcka otillåten borttagning av signaturen används Author Domain Signing Practices (ADSP). Med ADSP kan avsändaren meddela mottagaren huruvida den aktuella domänen signerar sina meddelanden eller inte. Denna information sprids också via avsändarens DNS. ADSP dokumenteras i RFC 5617[17]. I korthet definierar RFC:n en posttyp som kan annonsera huruvida en domän signerar sin utgående e-post och hur andra servrar kan komma åt och tolka den informationen.

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

Läs mer om DKIM: http://www.dkim.org.

SPF

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

SPF ger domäninnehavaren möjlighet att i DNS publicera regler som anger från vilka datoradresser e-post från domänen ska komma. När en mottagande e-postserver får ett meddelande kontrollerar den mot SPF-informationen i DNS hur dessa regler ser ut. Om meddelandet kommer från en sändande server som

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

inte är publicerad i reglerna tolkas det av den mottagande servern som en indikation på att allt inte står rätt till.

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

Läs mer om SPF: http://tools.ietf.org/html/rfc6652.

Bilaga 9 - Åtgärder för transportskydd i de vanligaste tjänsterna

Elektronisk post

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

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

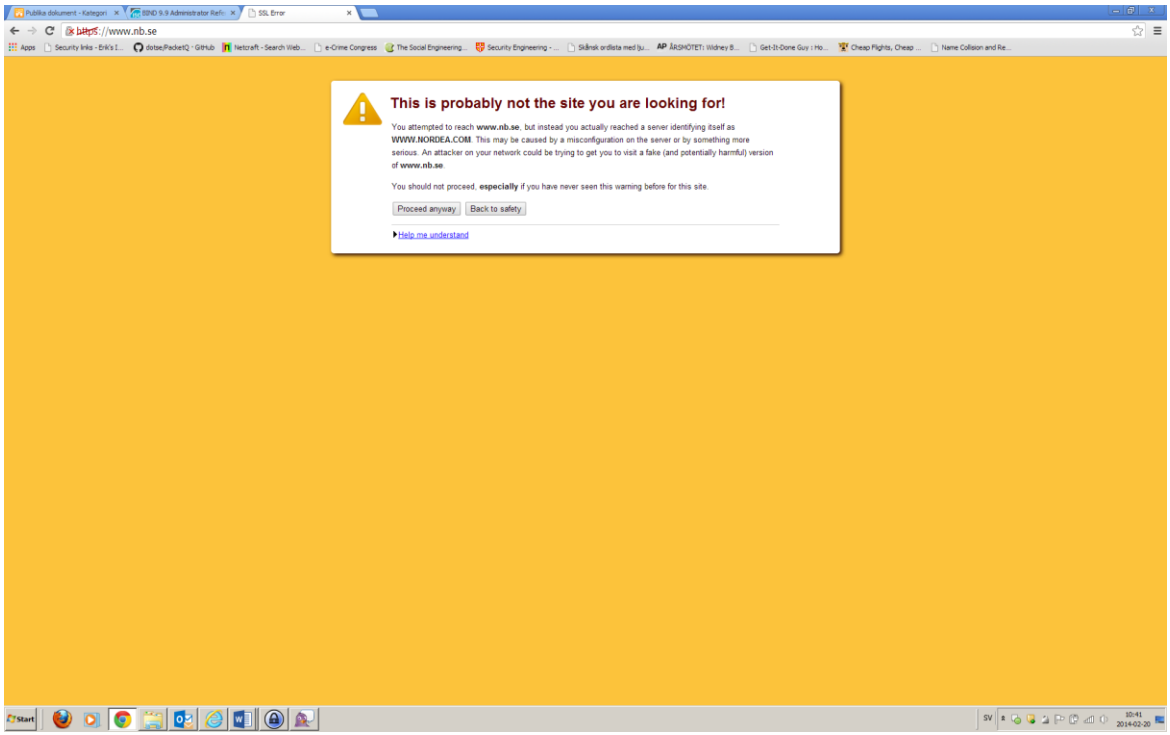
Webbtrafik

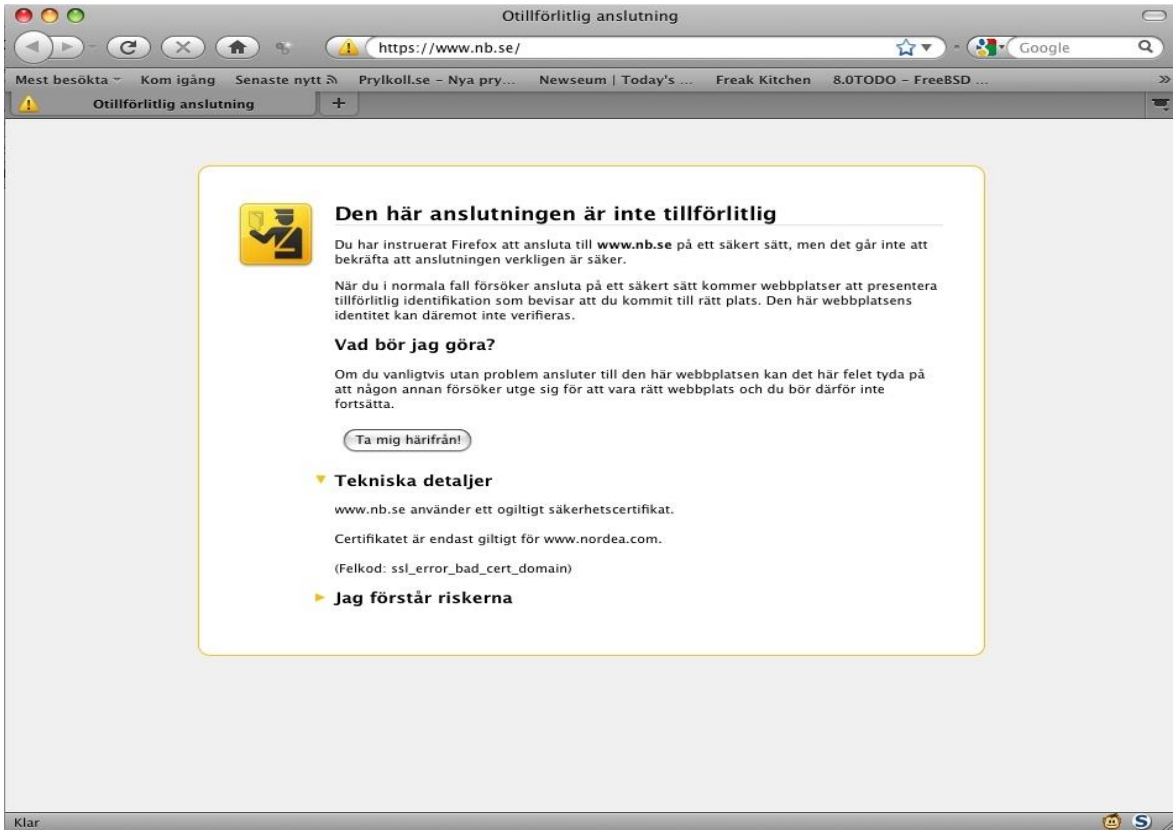
För en användare som exempelvis vill komma i kontakt med en svensk myndighet eller bank är det viktigt att veta att den server man har kontakt med är rätt server, att anslutningen av någon anledning inte har skett till fel tjänst eller server på grund av felkonfiguration eller medvetet bedrägeriförsök.

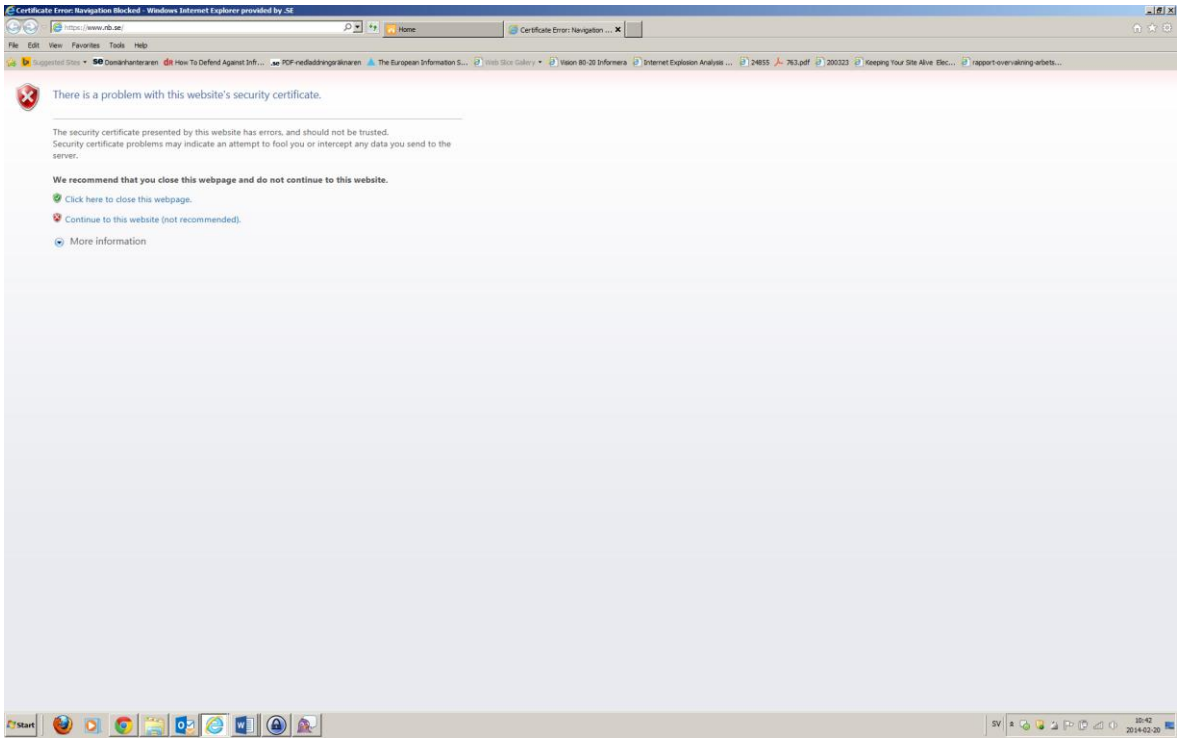
En av de tekniker som används för detta är Transport Layer Security (TLS). TLS/SSL ger användarna möjlighet att kontrollera att man hamnat hos rätt server eller tjänst.

Felmeddelanden och varningar

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 i exemplen nedan. Det ser lite olika ut beroende på vilken webbläsare som används. Självklart ska man inte gå vidare i det här läget utan att undersöka certifikatet närmare eller försöka få mer information om var problemet ligger. Som vår undersökning visar kan det exempelvis bero på att certifikatet har passerat sista giltighetsdatum eller att det är utfärdat för en annan domän.


https://www.nb.se
This is probably not the site you are looking for!
You attempted to reach www.nb.se, but instead you actually reached a server identifying itself as WWW.NORDEA.COM. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of www.nb.se.
You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand


Otillförlitlig anslutning
https://www.nb.se/
Google
Mest besökta
Kom igång
Senaste nytt
Prylkoll.se – Nya pry...
Newseum | Today's ...
Freak Kitchen
8.0TODO – FreeBSD ...
Otillförlitlig anslutning
Den här anslutningen är inte tillförlitlig
Du har instruerat Firefox att ansluta till www.nb.se på ett säkert sätt, men det går inte att bekräfta att anslutningen verkligen är säker.
När du i normala fall försöker ansluta på ett säkert sätt kommer webbplatser att presentera tillförlitlig identifikation som bevisar att du kommit till rätt plats. Den här webbplatsens identitet kan däremot inte verifieras.
Vad bör jag göra?
Om du vanligtvis utan problem ansluter till den här webbplatsen kan det här felet tyda på att någon annan försöker utge sig för att vara rätt webbplats och du bör därför inte fortsätta.
Ta mig härifrån!
Tekniska detaljer
www.nb.se använder ett ogiltigt säkerhetscertifikat.
Certifikatet är endast giltigt för www.nordea.com.
(Felkod: ssl_error_bad_cert_domain)
Jag förstår riskerna
Klar


Certificate Error: Navigation Blocked - Windows Internet Explorer provided by .SE
There is a problem with this website's security certificate.
The security certificate presented by this website has errors, and should not be trusted.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Bilaga 10 - Skydd mot avlyssning, certifikat och certifikatshantering

Överföring av elektronisk post sker vanligen i klartext och brukar därför ofta jämföras med vykort. Även för en användare som via webben vill komma i kontakt med en svensk myndighet eller bank är det viktigt att veta att den webbserver 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.

Standard för skydd mot avlyssning

Med hjälp av certifikat och tillhörande krypteringsnycklar kan ett e-postprogram upprätta en säker, krypterad förbindelse för kommunikation med e-postservern och en webbläsare upprätta en säker, krypterad förbindelse för kommunikation med webbservern.

Det finns standardprotokoll som används för skydd mot avlyssning genom upprättandet av en säker förbindelse mellan två parter. Transport Layer Security (TLS), en äldre standard var känd som Secure Socket Layer (SSL).

TLS är den standard som implementerad i teknik och med hjälp av kryptering skyddar trafik mot avlyssning vid kommunikation via internet, vilket gör att en användare kan lita på att han eller hon pratar med rätt organisation när de exempelvis vill utföra bankärenden.

Kan man lita på certifikat?

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

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

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

Vem behöver använda certifikat?

Alla som via en webbplats begär eller lämnar ut någon form av känslig information till användare, som inloggning, personuppgifter, betalinformation, kreditkortsnummer, med mera, eller producerar någon typ av viktigare information till användare som exempelvis nyheter, börskurser eller motsvarande, bör använda TLS/SSL med certifikat utfärdade av allmänt accepterade certifikatutfärdare som finns installerade i de vanligaste webbläsarna.

Det behöver också finnas någon internt i den verksamhet som certifikatet utfärdats för som ansvarar för bland annat bevakning av när certifikat går ut och måste förnyas. Utöver det behöver man tänka på att:

- Använda så långa RSA-nycklar som möjligt. För närvarande är detta minst 2048 bitar enligt beslut från Certification Authority/Browser (CA/B) Forum som är de som definierar branschstandarder för SSL-certifikat. Skälet till de skärpta kraven är att datorkraften ökar och det finns därmed en risk för att kortare nycklar kan knäckas av hackare med tillgång till omfattande processorkraft.
- Behandla verksamhetens certifikat som kritiska tillgångar och föra en förteckning över vilka certifikat som används, vad de används till och deras giltighetstid.
- Använda EV-certifikat[18] där det är befogat.
- Undvika wildcard-certifikat[19] för webbtjänster, speciellt där driften är utlagd på tredjepart som exempelvis webbhotell eller molntjänster där det inte finns någon egen kontroll över vare sig nyckelmaterial och certifikat.
- Ha certifikat som använder en signaturalgoritm som är starkare än MD5 (SHA1/SHA256).
- I vissa speciella fall använda hårdvarustöd för att skydda privata nycklar.

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

Certifikattyp och nyckellängder

Extended validation-certifikat (EV) är en variant av certifikat som medför utökat visuellt stöd i webbläsarna för att visa vem certifikatet är utfärdat till. EV innebär att utfärdarna har granskats mer noggrant än när det gäller vanliga servercertifikat och framför allt att utfärdarna vidtar särskilda åtgärder för att säkerställa att certifikatet utfärdas till rätt mottagare.

Av de undersökta certifikat som används för webbplatser är endast 8 procent så kallade EV-certifikat (Extended validation).

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

När det gäller nyckellängder behöver dessa ses över regelbundet. Här vill vi poängtera att CAB Forum har publicerat en ny branschstandard för SSL-certifikat som innebär att alla certifikat utfärdade efter den 1 januari 2014 måste ha minst nyckellängden 2048 bitar. De som fortfarande har certifikat med nyckellängden 1024 bitar eller över huvud taget certifikat med kortare nyckellängd än 2048 bitar måste byta till längre (starkare) nycklar nästa gång certifikatet förnyas.

Jokercertifikat och interna värdnamn

Ett jokercertifikat (wild card) 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 kan vara så att vissa jokercertifikat är utfärdade för något webbhotell som i sin tur använder det för att utfärda certifikat för sina kunder. Det är långt ifrån riskfritt att dela certifikat mellan domäner bland annat därför att:

- Om säkerheten hos en server eller subdomän har komprometterats finns det risk för att alla subdomäner också har komprometterats.
- Om jokercertifikatet 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 jokercertifikat.

Vi rekommenderar också starkt att man enbart använder fullständiga globala värdnamn (till exempel "intranet.example.se") och avråder från att använda interna värdnamn.

Det finns flera anledningar till att ett certifikat inte går att verifiera, trots att det är utgivet av en allmänt accepterad certifikatutfärdare. Den absolut vanligaste anledningen är att certifikatet inte används för rätt tjänst (till exempel att certifikatet för www.example.se används för tjänsten intranet.example.se).

Certifikatens giltighetstid

Det är viktigt att förnya certifikat inom den angivna giltighetstiden. Det har vid våra tidigare undersökningar funnits en relativt stor andel med certifikat som har passerat sista användningsdag, eller är på god väg att göra det genom att de förfallit inom den närmaste 30-dagarsperioden.

Spärrkontroll

Alla certifikat utgivna av en publik certifikatutfärdare gick att kontrollera via spärrlistor (CRL), medan 85 procent av dem gick att kontrollera via OCSP (Online Certificate Status Protocol)[20]. Vilken av dessa två metoder som används för spärrkontroll varierar, men båda används och när de inte fungerar korrekt påverkar det svarstiderna i till exempel en webbapplikation på ett negativt sätt.

Protokollversioner

Protokoll för skydd på transportnivå förekommer i flera olika versioner, men bör realiseras genom användning TLSv1 eller ekvivalent metod.

[20] http://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

Testa TLS/SSL

Om det finns något problem med det certifikat som finns på exempelvis en webbplats så genereras det oftast en varning som presenteras av webbläsaren. Certifikatsvarningar ska inte ignoreras utan tas på allvar, och man bör alltid försöka härleda vad som ligger bakom varningen.

Det är viktigt att hålla utkik efter tecken på att det upprättats en skyddad förbindelse och att försöka förvissa sig om att det är en äkta sådan. Vi rekommenderar också att man lär sig mer om hur man tar sig en extra titt på ett certifikat för att värdera äktheten.

Det finns flera publikt tillgängliga verktyg för att testa kvalitet och säkerhet i TLS/SSL.

Verktyget på sajten https://www.howsmyssl.com/ skapades ursprungligen för att hjälpa webbutvecklare att lära sig mer om vad TLS-klienter kunde göra. Från det har det utvecklats till att ge utvecklare och riktigt teknik-savvy användare ett snabbt och enkelt sätt att lära sig mer om de TLS-verktyg de själva använder. Syftet är också att uppmuntra utvecklare att modernisera och förbättra sina TLS-protokollstackar. Många säkerhetsproblem kommer sig av att utvecklare och tekniker inte vet vad de borde oroa sig för. How's My SSL demonstrerar något av vad den oron ska fokuseras på när det gäller TLS-klienter, som till exempel en vanlig webbläsare.

Ett annat verktyg kommer från SSLLabs och nås på https://www.ssllabs.com Där kan den som använder certifikat för att skydda webbtjänster lära sig mer om hur det fungerar och dessutom själv testa om webbplatsen på serversidan har bra säkerhet med avseende på SSL. På senare tid har även ett klienttest lagts till på sajten. SSL Labs är en samling dokument, verktyg och funderingar relaterade till SSL. Informationen syftar till att bättre förklara hur SSL är infört och är ett sätt att genomföra ständiga förbättringar. Initiativet till SSL Labs har tagits av Ivan Ristic, Qualys, och hans förhoppning är att det ska växa till ett forum för SSL där olika idéer till vidareutveckling kan mötas och diskuteras seriöst.

Attacker mot SSL och åtgärder för att motverka dessa

Som vi nämnt i våra tidigare rapporter har det på senare år skett flera, mycket allvarliga attacker mot ett antal stora certifikatutfärdare. Därför finns det anledning att fundera över hur man gör det bästa möjliga för att lösa de problem som finns. Vi pratar om vanlig traditionell säkerhet.

Hanteringen hos de CA som har drabbats av framgångsrika attacker har i allra högsta grad varierat. Vissa av de drabbade certifikatsutfärdarna har agerat både långsamt och otillräckligt när det gäller att förmedla information till sina kunder och omvärlden. De har helt enkelt visat prov på bristande krishantering.

DNS-baserad autentisering av namngivna enheter

Det är många som funderar på lösningar. Ett av de mest intressanta initiativen är för närvarande det som har utvecklats inom IETF-arbetsgruppen DNS-based Authentication of Named Entities (DANE), vars resultat finns som färdig

standard och har publicerats som Transport Layer Security (TLS) Protocol: TLSA, RFC 6698[21].

Med DANE lagras certifikat i DNS så att det går att verifiera dem. Tilliten går till DNS med användning av DNSSEC. Tillvägagångssättet kompletterar certifikatutfärdarens signaturer genom att verifiering av certifikatet kompletteras eller i vissa fall ersätts med DNS. Det bidrar till att höja kvaliteten på certifikatet och därmed öka tilliten.

Metoden gör det också möjligt att hoppa över de traditionella certifikatutfärdarna och bara lita på DNS i de fall man bara vill verifiera domännamnet och inte vilken juridisk person som står bakom en tjänst.

Skydd mot nedgraderingsattacker

En annan förhållandevis vanlig typ av attacker mot webbplatser som använder SSL är olika typer av nedgraderingsattacker. Det innebär att användaren förmås att gå över till att använda ett enklare eller inget krypto alls för att kommunicera med webbplatsen. Då behöver en angripare inte ens ett för webbplatsen giltigt certifikat för att effektivt kunna genomföra en så kallad janusattack (man-in-the-middle attack).

Inom IETF har man tagit fram det som går under namnet HTTP Strict Transport Security (HSTS)[22] som innebär att webbläsaren tvingas att köra SSL mot webbplatsen, oavsett vad som sägs i övrigt. HSTS fungerar så att webbläsaren kommer ihåg om en sajt som har besökts tidigare har använt SSL och tvingar upp kommunikationen på samma nivå vid ett återbesök.

Skydd mot röjning av nycklar i efterhand

För att skydda sig mot att någon kommer över nyckeln och använder den vid en senare tidpunkt finns Perfect forward secrecy (PFS). I praktiken betyder detta att om certifikatets nyckelmaterial skulle röjas så kan all trafik som skickats till eller från den aktuella servern och som inte är skyddad av PFS dekrypteras i efterhand. PFS innebär att de kryptonycklar som används för transportskydd inte går att härleda från det nyckelmaterial som hör till serverns certifikat.

Andra initiativ

Webbläsaren Chrome innehåller många utökningar, bland annat *certificate pinning*[23] som var det som avslöjade en av CA-attackerna, den mot DigiNotar. Arbete inom det området pågår även inom IETF[24].

Andra utökningar i Chrome är *HTTPS-preloading*[25] som innebär att vissa sajter är hårt konfigurerade att endast nås via SSL.

Det finns även plugin till Mozilla Firefox och andra webbläsare för bättre certifikatshantering, som till exempel *HTTPSEverywhere*[26] som utvecklats gemensamt av Electronic Frontier Foundation (EFF) och Tor-projektet.

[21] http://tools.ietf.org/html/rfc6698
[22] http://tools.ietf.org/html/rfc6797
[23] https://www.imperialviolet.org/2011/05/04/pinning.html
[24] http://tools.ietf.org/html/draft-ietf-websec-key-pinning-11
[25] http://dev.chromium.org/sts
[26] https://www.eff.org/https-everywhere

Aktuella sårbarheter i krypteringsprogramvara

Vi lever numer i en period man kan kalla för Post Snowden, eller ett Post Privacy-samhälle. Efter Snowdens avslöjanden om NSA:s massövervakning 2013 har den överväldigande omfattningen sakta sjunkit in. Vi har hört om hur USA kopplat in sig i andra länders nät, manipulerat hårdvara, mjukvara och kryptoalgoritmer, och inte minst telefonistandarder. Då känns behovet av stark kryptering extra angeläget, samtidigt som en av de vanligaste implementationerna av SSL – OpenSSL – har behäftats med ett antal allvarliga sårbarheter.

Heartbleed

Det har väl knappast undgått någon att en programbugg i krypteringsbiblioteket OpenSLL upptäcktes 2014 som påverkade stora delar av servrar på internet. Buggen som fick namnet Heartbleed kunde potentiellt göra det lättare för illvilliga hackare att komma över servrars privata krypteringsnycklar och i förlängningen även vanliga användares lösenord, kreditkortsnummer och andra känsliga uppgifter. Buggen i OpenSSL rättades 7 april 2014, samma dag som den offentliggjordes. Systemägare, webbhotell och andra IT-funktioner behöver dock installera den rättade programvaran för att avvärja hotet. Det mest anmärkningsvärda med Heartbleed är att sårbarheten funnits i två år utan att upptäckas. Det spekuleras givetvis i att NSA känt till och utnyttjat buggen sedan den introducerats, men detta har inte kunnat beläggas.

Säkerhetsföretaget Codenomicon gav buggen dess namn och en logotyp för att öka allmänhetens medvetande om buggens existens.

Poodle

Bara några månader senare släppte Google information om en ny sårbarhet i SSL. Sårbarheten finns i SSL version 3.0 och har fått namnet Poodle. Poodle är exempel på en sårbarhet som är framgångsrik tack vare mekanismer som införts för att underlätta interoperabilitet, men på bekostnad av säkerhet. Sådana misstag förtjänar extra uppmärksamhet eftersom de gör nedgraderingsattacker möjliga. Eftersom version 3 av SSL är föråldrad krävs att angriparen lurar

klientens webbläsare att använda den äldre krypteringsversionen istället för en modern säkrare version.

När mer detaljerad information så småningom tillkännagavs så kom många farhågor på skam då sårbarheten visade sig vara mindre allvarlig än vad många befarat.

Poodle är i grunden ett programvarufel i krypteringstekniken SSL (Secure Socket Layers). SSL används för att skydda datatrafik med kryptering, exempelvis när information som användarnamn och lösenord utväxlas mellan en användare och den webbplats denne besöker. I många webbläsare representeras en krypterad uppkoppling av ett hänglås bredvid webbadressen. Den sårbara versionen av SSL är version 3, detta är en äldre teknik som sedan länge ersatts av nyare versioner men den används fortfarande på ett stort antal webbplatser och i många webbläsare.

För att en angripare ska kunna utnyttja sårbarheten i SSL så krävs det att denne har tillfälle att avlyssna samt påverka datatrafik från offret. Oftast drabbade av denna typ av avlyssning är användare av gratis WiFi-anslutningar på flygplatser eller hotell men en angripare kan i teorin sitta varsomhelst längst med den rutt som datatrafiken tar från offrets webbläsare till webbplatsen. Angriparen utnyttjar sedan Poodle-sårbarheten i syfte att utvinna läsbar information från den uppfångade datatrafiken trots att den är krypterad.

Mängden okrypterad information som angriparen kan utvinna är relativt liten och på grund av att sårbarheten kräver tillgång till offrets datatrafik så var Poodle-sårbarheten inte lika akut som Heartbleed när den upptäcktes. Detta kan dock förändras i takt med att illvilliga aktörer konstruerar nya sätt att använda sårbarheten till sin fördel.

Åtgärder för att skydda sig:

• Systemadministratörer bör snarast se över möjligheterna att sluta stödja SSL v3 på sina webbplatser. Särskilt de webbplatser som endast stödjer SSL v3.
• De flesta webbläsare kan ställas in så att de inte använder SSL utan i stället TLS, vilket är namnet på nyare versioner av SSL. Observera dock att detta kan omöjliggöra åtkomst till vissa webbplatser.
• Användare av Internet Explorer 6 bör snarast se över möjligheten att uppgradera till en senare version eller byta webbläsare då denna inte stödjer nyare versioner av SSL än 3.0.
• Webbläsarna Google Chrome och Mozilla Firefox arbetar bägge med uppdateringar av sina produkter. Användare av dessa får en varning ifall en webbplats vill använda en äldre krypteringsteknik även då modernare alternativ stöds.