Hälsoläget i .se 2013

– fördjupning i kryptering av trafik på nätet

1 Introduktion

För sjunde gången i ordningen har .SE genomfört en undersökning av nåbarhet på nätet och hälsoläget i .se. 2013 års undersökning är liksom tidigare år till stora delar men inte fullständigt en uppföljning av de tidigare undersökningar som genomförts under åren 2007-2012.

Syftet med den årliga 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 rad kan vi också visa på utveckling och trender inom de undersökta områdena. Undersökningen görs på både ett urval av domäner som representerar viktiga funktioner i samhället och ett slumpmässigt urval motsvarande en procent av samtliga domäner i .se.

En nyhet i årets undersökning är att vi har resultat från återkommande månadsvisa tester för hela 2013. I stället för att ta en enda ögonblicksbild av hur det ser ut vid en viss tidpunkt har vi alltså genomfört en datainsamling varje månad. Avsikten är främst att visa om bilden ändras avsevärt under ett år orsakat till exempel av förändringar i de undersökta verksamheternas IT-miljö.

I undersökningen kartlägger och analyserar vi kvaliteten och nåbarheten i domännamnssystemet (DNS) i .se-zonen för både ett urval av domäner som representerar viktiga funktioner i samhället och ett slumpmässigt urval motsvarande en procent av samtliga domäner i .se.

I den här rapporten redovisar vi även resultatet av en fördjupad undersökning och analys inom området säker kommunikation, det vill säga användning av och kvalitet på certifikat för att skydda kommunikation mellan klient och server för e-post respektive webbtjänster. Den delen av undersökningen har genomförts under hösten 2013 och bygger på ett verktyg som .SE har låtit utveckla särskilt för ändamålet.

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

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

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

Den årliga hälsolägetundersökningen finansieras av .SE, liksom aktiviteterna inom hela fokusområdet Internets ekosystem. Resultaten av undersökningen har analyserats och sammanställts av Anne-Marie Eklund Löwinder, säkerhetschef på .SE. Granskningen av den statistiska analysen samt diagram och tabeller har gjorts av Anders Örtengren, Mistat AB för de delar som avser domännamnssystemet och av Jakob Schlyter, Kirei AB, för de delar som avser säker kommunikation och certifikatsanvändning.

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

2 Sammanfattning

Liksom tidigare år ligger undersökningens fokus på DNS-kvalitet, men vi har kompletterat den med en fördjupad undersökning av användningen av certifikat som används för transportskydd på internet.

För ett halvår sedan briserade visselblåsaren Edward Snowdens avslöjanden inte bara om massiv signalspaning och avlyssning av internetanvändare, men vad värre är, även avslöjanden om åtgärder som syftar till att försvaga de tekniska åtgärder som användare valt för att skydda sin information under kommunikation. För var och en som driver tjänster som VPN, e-post eller andra kommunikationstjänster i USA, finns risken att de kan drabbas av en så kallad "pen register order" som kan användas för att tvinga en leverantör att lämna ut exempelvis de SSL-nycklar som används för att skydda meddelandeinnehåll från insyn av obehöriga.

Utvecklingen av IPv6 och DNSSEC är också viktiga parametrar, inte minst som en uppföljning av utvecklingen av både IPv6 och DNSSEC eftersom dessa faktorer uppmärksammats särskilt i regeringens strategi för det IT-politiska området "It i människans tjänst - en digital agenda för Sverige".1

I årets undersökning kan vi konstatera att andelen fel fortsätter att minska och nu ligger på 15 procent för undersökningsgruppen som helhet.

2.1 Om undersökningsgruppen

I årets undersökning ingår totalt 922 domäner. 922 domäner är alltså det antal domäner vi avsåg att samla information om, medan 913 är det antal som vi har lyckats samla in information om. Orsaken till att det skiljer sig är främst att vissa namn förekommer i mer än en kategori och därför skulle räknas mer än en gång om vi bara skulle slå ihop antalen i de olika kategorierna.

Domänerna är fördelade på 1 538 unika namnservrar - IPv4 (1 239) och IPv6 (299). Med "unik" menas här servrar med unika IP-adresser. En namnserver hos en operatör kan härbärgera flera domäner. Vilka kategorier vi använt och hur många domäner som finns i varje kategori redovisas i avsnitt 5 nedan.

Dessutom har en jämförelse gjorts med en kontrollgrupp som motsvarar en procent av hela .se-zonen, det vill säga 12 598 slumpmässigt utvalda .se-domäner som redovisas i avsnitt 9.

För att vi ska kunna följa utvecklingen år från år försöker vi i allmänhet hålla oss till ungefär samma parametrar och undersökningsgrupp som använts tidigare. I 2013 års undersökning kontrollerades samma domäner som 2012.

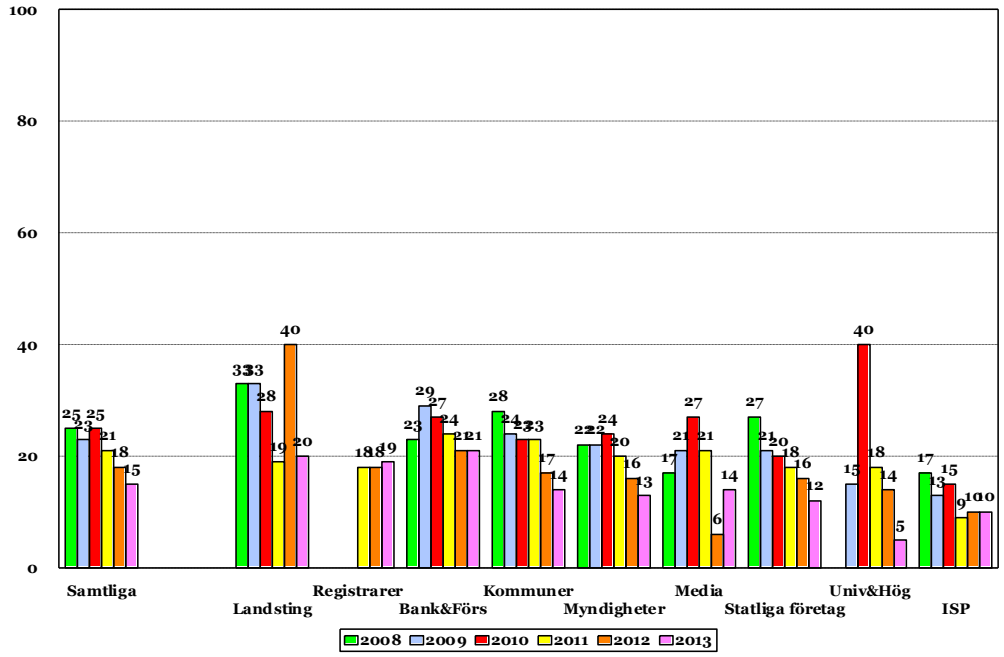
2.2 Fortsatt minskning av mängden allvarliga fel

Mellan åren 2007 till 2009 var förändringarna blygsamma och det fanns stora brister som vi pekade på samtidigt som vi föreslog konkreta åtgärder för att komma tillrätta med dessa. I resultaten från undersökningen 2010 kunde vi tyvärr inte se någon större förändring till det bättre. Resultaten för 2011 och 2012 var positiva i flera avseenden. Glädjande nog fortsätter den trenden även 2013.

[1] http://www.regeringen.se/content/1/c6/17/72/56/5a2560ce.pdf

Den totala andelen allvarliga fel och varningar har minskat ytterligare, och från att 2012 hamnat på en felprocent under 20 procent för majoriteten av de undersökta domänerna är vi för första gången nere på 15 procent för 2013.

Diagram 1: Utveckling av andel fel i procent 2008-2013.



2.3 Skillnader i undersökningen sedan förra året

Vårt syfte med att regelbundet publicera resultaten från undersökningen av domännamnssystemet och andra viktiga funktioner på internet är att skapa uppmärksamhet kring de problem och brister som en hel del domäner i .se-zonen lider av och att höja kvaliteten generellt. Att genomföra undersökningen flera år i följd ger oss möjlighet att se utvecklingstrender, och 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.

Det är vi själva som har definierat kvalitet i bland annat domännamnssystemet. Definitionen har dock utgått från vad som är vedertaget som praxis eller branschstandard, *Best Common Practice,* tillsammans med våra egna praktiska erfarenheter av domännamnssystemet och av att driva namnservrar.

I rapporten för 2013 redovisar vi även resultatet av en fördjupad undersökning och analys inom området säker kommunikation, det vill säga användning av och kvalitet på certifikat för att skydda kommunikation under transport mellan klient och server för e-post respektive webbtjänster. Den delen av undersökningen har genomförts under hösten 2013 och bygger på ett verktyg som .SE har låtit utveckla särskilt för ändamålet och redovisas i avsnitt 10.

2.4 Slutsatser från undersökningen

Detta avsnitt sammanfattar de slutsatser som vi dragit av resultaten från undersökningen 2013.

2.4.1 Vässa beställarkompetensen

Det förefaller som att de verksamheter som ingår i undersökningen behöver vässa sin beställarkompetens när det gäller domännamnssystemet och ställa relevanta krav på både konsulter, registrarer och andra leverantörer, inte minst de som driver namnservertjänster, e-posttjänster och webbtjänster.

De vanligaste felen i DNS 2013 är att det finns fler namnservrar annonserade i .se-zonen än som faktiskt svarar på frågor för domänen i fråga, att man inte svarar på frågor via TCP och att man har för få namnservrar, det vill säga bara en enda, som svarar på frågor om domänen.

2.4.2 Få lägger resurser på en bättre DNS-infrastruktur

Medan man lägger miljoner på sin webbinfrastruktur med serverhallar, servrar, lastbalanserare, databaser och design så är det extremt få som lägger några verkliga resurser på en bättre DNS-infrastruktur. I dag är DNS en växande måltavla bland annat för överbelastningsattacker – man angriper där motståndet är som svagast. Därför är det fundamentalt viktigt att förbättra DNS som en del av åtgärderna mot överbelastningsattacker.

2.4.3 Allt färre namnservrar med rekursion påslaget

Mellan 2007 och 2013 har andelen namnservrar med rekursion påslaget minskat mycket kraftigt, från 40 procent till 5 procent. Sedan förra undersökningen har vi haft en fortsatt minskning med ytterligare några viktiga procent, från 10 till 5. Kategorin Kommuner är den som står för den största kvarvarande andelen rekursiva namnservrar, 10 procent av kommunernas namnservrar har det fortfarande påslaget. Tre kategorier, nämligen ISP, Bank & Försäkring samt Universitet & Högskolor är samtliga nere på 0 procent! Övriga ligger på eller under 5 procent. Öppna rekursiva namnservrar kan missbrukas av andra och användas i överbelastningsattacker (se avsnitt 6.6).

2.4.4 Allt fler använder IPv6

När det gäller införande av IPv6 ser vi en ökning över hela linjen, bland samtliga kategorier, från 24 till 54 procent. Den största ökningen har skett inom kategorin Kommuner där det ökat från 15 procent som använde IPv6 2012 till hela 65 procent 2013. Universitet och högskolor är den kategori där det är allra vanligast, 81 procent använder IPv6. .SE driver ett mycket aktivt arbete för att påskynda spridningen av IPv6.

2.4.5 Allt fler signerar domäner med DNSSEC – men var är bankerna?

Som ett resultat av återkommande kampanjer från .SE riktade till registrarerna har vi sett en kraftig ökning av DNSSEC-signerade domäner.

.SE stödjer och uppmuntrar införandet av DNSSEC även på andra sätt och har i ett samarbete med MSB, PTS, och SKL arbetat med att ta fram en paketlösning som kommunerna kan använda sig av.

MSB har de senaste åren haft möjlighet att bevilja medel ur det så kallade 2:4-anslaget, Krisberedskap, som kan sökas av utpekade myndigheter. Med början 2012 prioriterade MSB området robusthetshöjande åtgärder med inriktning mot att säkerställa adressuppslagningar på internet, det som sker via domännamnssystemet, DNS.

Enligt uppgift från MSB har totalt 230 (av totalt 290) kommuner via länsstyrelserna beviljats medel för åtgärder som syftar till att införa DNSSEC, alla är dock inte klara med genomförandet. Myndigheten har bland annat tryckt på att det är mycket angeläget att domäner för offentliga webbplatser signeras med DNSSEC, något som vi på .SE förstås tycker är utmärkt. Totalt har MSB fördelat 10 390 000 kronor att förbruka mellan 2012 och 2014.

Vid årets undersökning är andelen signerade domäner i undersökningsgruppen 22 procent. Som jämförelse var vid årsskiftet 2013/2014 totalt 333 423 av 1 342 674 domäner eller 25 procent av hela .se-zonen signerade med DNSSEC.

Bank- och finanssektorn lyser i princip helt med sin frånvaro när det gäller DNSSEC. Detta trots att .SE sedan 2007 fört diskussioner med banksektorn och även erbjudit vår expertis, kostnadsfritt.

I princip alla internetbaserade tjänster är beroende av att domännamnssystemet (DNS) fungerar. Konsekvensen av att göra fel kan bli omfattande. Detta gäller i än högre grad vid införandet av DNSSEC som är ett sätt att skydda informationen som kommuniceras mellan servrarna i DNS från manipulation. DNSSEC ställer högre krav på teknisk kompetens för drift än traditionell DNS.

.SE har därför publicerat en vägledning 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 för andra typer av verksamheter inom både offentlig förvaltning och näringsliv. Den finns att ladda ner från .SE:s webbplats på adressen https://www.iis.se/docs/dnssec-rek-2013.pdf

2.4.6 E-postservrar placerade i Sverige

Även i 2013 års mätning har vi tittat på verksamheternas placering av e-postservrar, och om dessa står placerade i eller utanför Sverige. Vi kan bara titta på domäner som har e-postservrar med IPv4-adresser, och av dessa ser det ut som att 25 procent har alla sina e-postservrar placerade i utlandet. Det är enligt vår uppfattning ett problem eftersom det sannolikt ökar risken för avlyssning om kommunikationen inte är skyddad med kryptering, och det är den de facto långt ifrån alltid. (se avsnitt 7.2).

3 Kontroller av internets infrastruktur

I 2013 års undersökning har vi tagit reda på fakta rörande följande kontrollpunkter:

- Hur hanterar verksamheten sina domännamn och det tekniska domännamnssystemet (DNS)?
- Hur är det uppsatt (i relation till vad som är att betrakta som branschstandard eller Best Common Practice)?
- Vilka är de allvarligaste bristerna och inom vilka branscher eller kategorier är dessa vanligast?
- Hur vanligt är det med namnservrar som är öppna för rekursion?
- Hur hanterar verksamheten sin e-post? Står servrarna i eller utanför Sverige?
- Används TLS/SSL (transportskydd) för e-post och webb?
- Har man infört IPv6 i verksamhetens IT-miljö?
- Har man infört DNSSEC i verksamhetens IT-miljö?

Testerna har genomförts på domäner och servrar för ett stort antal viktiga verksamheter i samhället; affärsverk och statliga bolag, banker, försäkrings- och finansföretag, Internetoperatörer, kommuner, landsting, medieföretag och statliga myndigheter inklusive länsstyrelser, universitet och högskolor samt .SE:s registrarer totalt 913 domäner. Hur de fördelar sig per kategori framgår i avsnitt 5.

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.

Med dessa tester undersöker vi hur väl verksamheternas system fungerar i olika avseenden, var de allvarligaste felen finns, hur vanliga de är och slutligen har vi genomfört analyser av vad det kan få för konsekvenser för verksamhetens IT-funktion. Den del av rapporten som rör DNS-tester sätts i relation till alla tidigare undersökningar, i princip från 2007 till nu.

Till resultaten knyter vi generella rekommendationer om hur vi anser att det borde se ut i den svenska internetinfrastrukturen. Slutligen – och med en dåres envishet – upprepar vi råd och rekommendationer inom olika områden att ta tag i för ansvariga myndigheter, åtgärder som det är lämpligt att gå vidare med och utreda mer i detalj.

Vi låter dessa stå kvar i princip oförändrade från förra årets undersökning eftersom resultaten från undersökningen talar sitt tydliga språk, nämligen att det finns brister som både behöver och enkelt kan åtgärdas. Samtidigt noterar vi med en viss tillfredsställelse att det går framåt på flera fronter, så snart kan vi stryka några av våra rekommendationer då kravet redan uppfyllts.

Genom samarbete med strategiska partners som MSB, PTS och SKL har .SE medverkat till att kommuner under flera års tid har kunnat ansöka om anslag för att driva projekt för införande av DNSSEC.

Vi konstaterar att bank- och finanssektorn ligger långt efter med införandet av DNSSEC, utan att vi kan se någon rimlig förklaring. För en så viktig del av samhället borde det vara självklart.

Vi ser gärna att myndigheter och deras medarbetare i beslutande ställning använder våra råd och rekommendationer och vidtar åtgärder för förbättringar inom samtliga berörda områden; DNS, DNSSEC och IPv6, men även skydd av kommunikation via e-post och webb.

4 DNS-tjänst med kvalitet

De flesta som använder internet reflekterar inte över vad som egentligen händer när de har skrivit in en adress i sin webbläsare och tryckt på returtangenten.

Internets infrastruktur kopplar samman en enorm mängd datorer som alla i princip utan hinder kan kommunicera med varandra. För att kommunikationen ska fungera måste datorerna använda samma uppsättning regler för att skicka och ta emot information, så kallade protokoll. På internet används många olika protokoll, men det mest grundläggande av dem alla är internetprotokollet IP. Det är med hjälp av detta protokoll datorerna kan hitta fram till varandra via så kallade IP-adresser.

Domännamnssystemet (DNS) är en av hörnstenarna på internet och har till uppgift att förenkla adressering av resurser på internet. Hur det fungerar finns beskrivet i bland annat en av .SE:s guider: DNS – Internets vägvisare[2].

.SE har ansvaret för Sveriges nationella toppdomän på internet, en uppgift som anses så viktig att den regleras av en särskild lag, lag (2006:24) om nationella toppdomäner för Sverige på internet[3]. Varje internetansluten enhet har en egen IP-adress som med hjälp av DNS kan kopplas till en adress i en form som är lättare att hantera för oss människor.

Via den öppna katalogtjänst som DNS utgör 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 DNS behöver man dessutom inte heller byta webb- eller e-postadress bara för att en server byter IP-adress.

.SE ser till att de drygt 1,3 miljoner domännamn som slutar med .se kan peka ut rätt resurser på internet genom att vi för ett register över dem och dirigerar alla frågor och svar som ställs i domännamnssystemet. På så vis går det som regel blixtsnabbt att hitta fram exempelvis till rätt webb- eller e-postserver.

Sedan september 2013 administrerar vi dessutom alla domännamn som slutar på .nu, som är en annan toppdomän på internet. .nu-domäner ingår för närvarande inte i undersökningen.

Vi har definierat vad som krävs för att skapa en DNS-tjänst med kvalitet. Den definitionen har vi använt för årets liksom för tidigare års undersökningstillfällen, där hög kvalitet för oss innebär:

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

[2] https://www.iis.se/docs/dns-internets-vagvisare.pdf
[3] https://lagen.nu/2006:24

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

I undersökningen utgår vi från 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.

Några av de grövsta felen har varit relativt vanligt förekommande genom åren. På senare år har vi noterat en positiv trend med successiv förbättring, vilket är glädjande, och 2013 är inget undantag.

Vi vill ändå betona behovet av att olika verksamheter vässar sin beställarkompetens och ställer relevanta krav på både konsulter, registrarer och leverantörer som driver namnservertjänster, e-posttjänster och webbtjänster. För den offentliga förvaltningens vidkommande skulle det förmodligen underlätta om stöd för sådan kravställning formulerades från centralt håll.

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

5 Tester 2013

2013 års tester har för första gången genomförts som månadsvisa körningar, som vi sedan för vissa delar av undersökningen redovisar för hela året. 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.

I 2013 års undersökning har vi utöver den vanliga mätningen av det allmänna hälsoläget fokuserat på en fördjupad mätning och analys av certifikatshantering för både e-post och webb. För att kunna genomföra den delen av undersökningen har vi utvecklat ett verktyg som bygger på SSLyze[4]. SSLyze är ett verktyg, en SSL-skanner, programmerat i Python, som analyserar SSL-konfigurationen på en server genom att ansluta till den och se vad den lämnar för svar på relevanta parametrar.

Vid 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 vissa frågor bland annat om hantering av elektronisk post.

Årets tester har genomförts i slutet av varje månad och har omfattat totalt 913 domäner fördelade på 1 538 unika namnservrar. Vi noterar en ökning med 93 unika namnservrar för samma domäner jämfört med 2012. Testobjekten har grupperats i kategorier på följande sätt (2012 och 2013 års undersökningsunderlag är identiska):

- 57 affärsdrivande verk och statliga bolag.
- 81 banker, finansinstitut och försäkringsbolag.
- 21 Internetoperatörer (ISP).
- 290 kommuner.
- 20 landsting.
- 36 medieföretag.
- 229 statliga myndigheter, inklusive länsstyrelser (exkl. myndigheter under Riksdagen).
- 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.

Tidigare år har vi rapporterat två olika typer av problem, och kategoriserat dem som fel respektive varningar enligt följande definition:

[4] https://github.com/iSECPartners/sslyze

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

Varningar: Varningar är också fel som kan påverka driften, men de bedöms inte vara lika akuta och åtgärder inte lika angelägna. Det skulle dock höja kvaliteten och nåbarheten om dessa fel eliminerades.

I resultaten från undersökningen 2013 har vi valt att inte på detaljnivå redovisa andelen varningar förutom i det första översiktliga diagrammet. Det beror framför allt på ändringar i mätinfrastrukturen som gjort att e-postrelaterade frågor mot e-postservrar blivit svartlistade när vi bytt IP-adress. Resultaten ser därför ut som att andelen varningar har skjutit i höjden. Vi kan inte med säkerhet verifiera andelen varningar utan ett grannlaga arbete med att gå igenom rådata, och avstår därför från att särredovisa varningar i årets rapport. Andelen fel påverkas emellertid inte av dessa mätproblem.

6 Våra observationer 2013

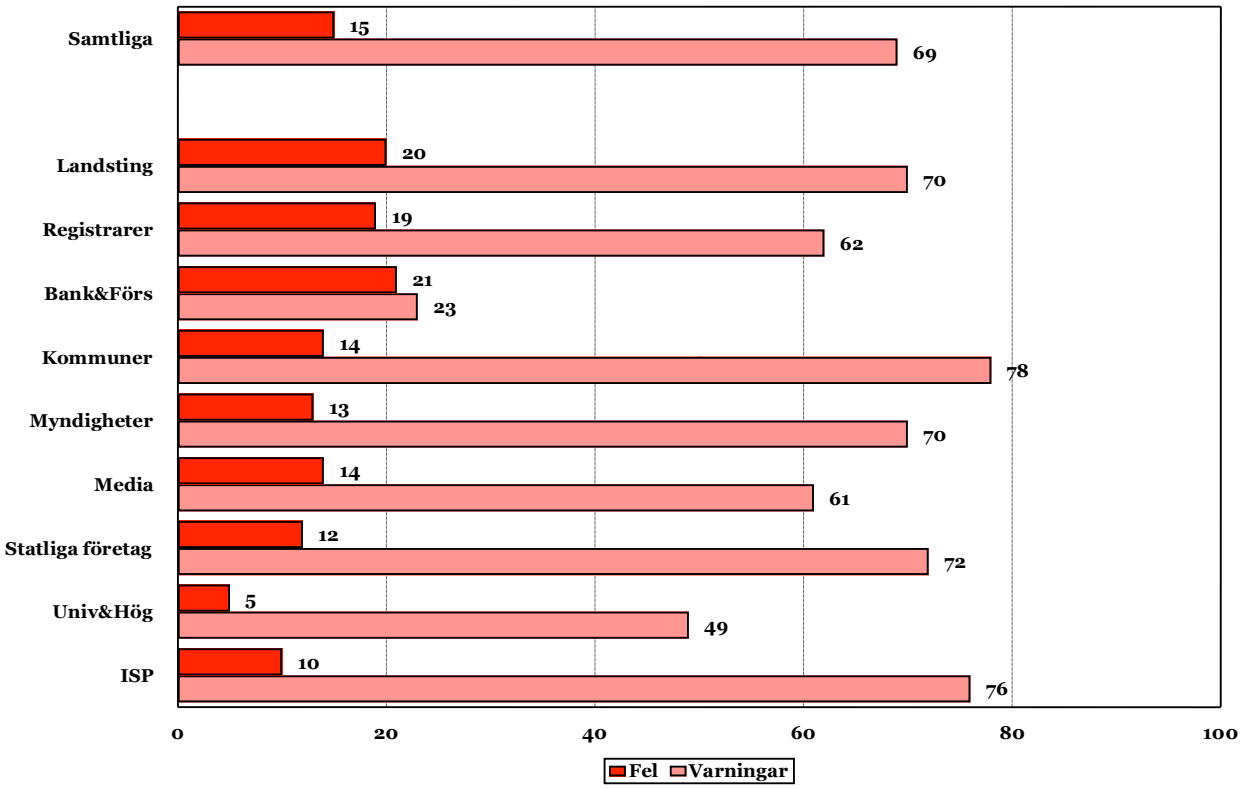
De första tre åren (2007-2009) då undersökningen genomfördes var förändringarna blygsamma och det fanns stora brister som vi pekade på samtidigt som vi föreslog konkreta åtgärder för att komma tillrätta med dessa. 2010 kunde vi tyvärr inte se någon större förändring till det bättre. Däremot var resultaten för 2011 och 2012 positiva i flera avseenden. Glädjande nog fortsätter den trenden även 2013.

I 2012 års undersökning hamnade vi för första gången under 20 procent i andel fel för undersökningsgruppen som helhet, närmare bestämt på 18 procent. 2013 har den siffran minskat ytterligare och vi är nu nere på 15 procent, vilket är ett mycket gott resultat.

6.1 Tester av DNS

Hur fel och varningar fördelar sig mellan de olika kategorier som ingår i undersökningen framgår av nedanstående diagram. Här ser ni också hur resultatet för varningar påverkats negativt av de mätproblem vi haft i det avseendet.

Diagram 2: Procentuell andel fel och varningar 2013.



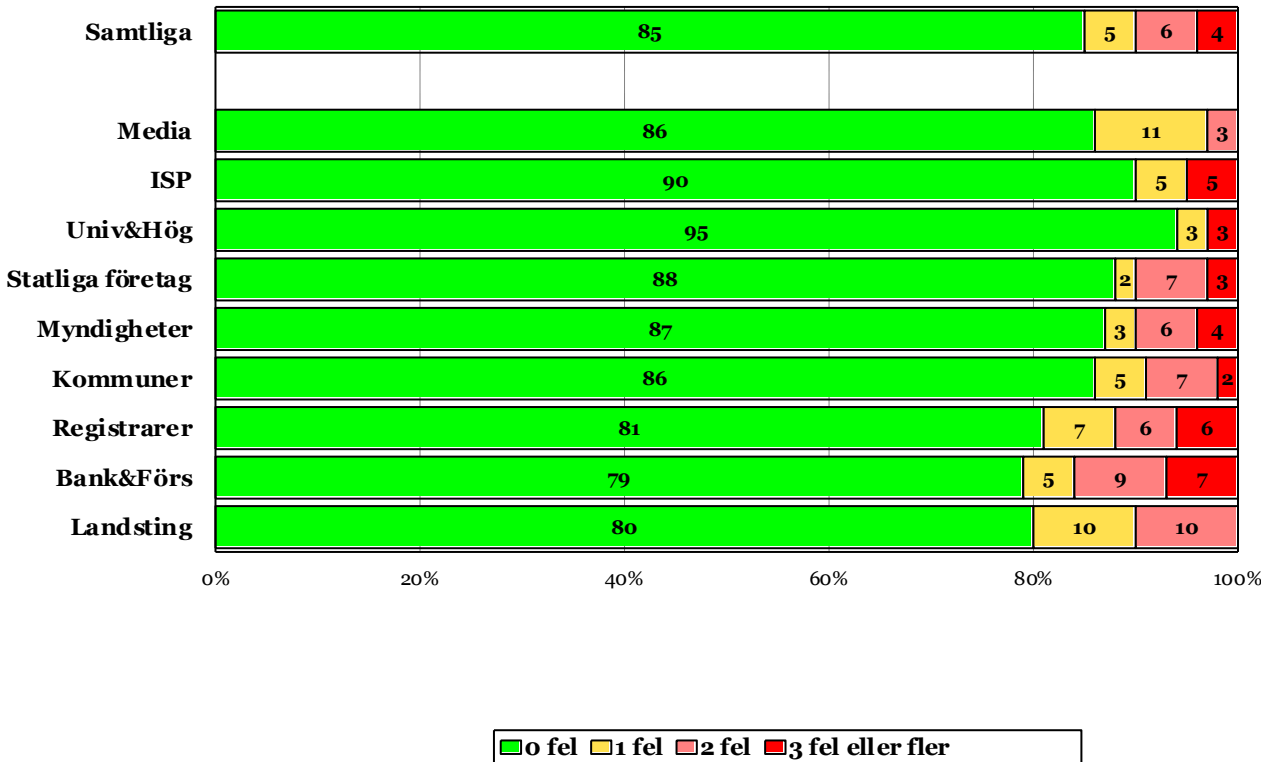
Diagrammet visar procentandelarna fel respektive varningar för de 913 domänerna som ingår i undersökningsgruppen (Samtliga) och fördelat på varje kategori. Staplarna ska alltså läsas så att av de verksamheter som ingår i undersökningen är endast 15 procent behäftade med fel av allvarligare karaktär. Detta är en solklar förbättring från föregående års undersökning.

Samtidigt ser det ut som att hela 69 procent av domänerna har brister som genererar en varning. Den siffran orsakas alltså av ett mätproblem och vi fokuserar därför enbart på sådant som genererar fel.

6.2 Mängden fel per kategori

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

Diagram 3: Procentuell fördelning av mängden fel per kategori

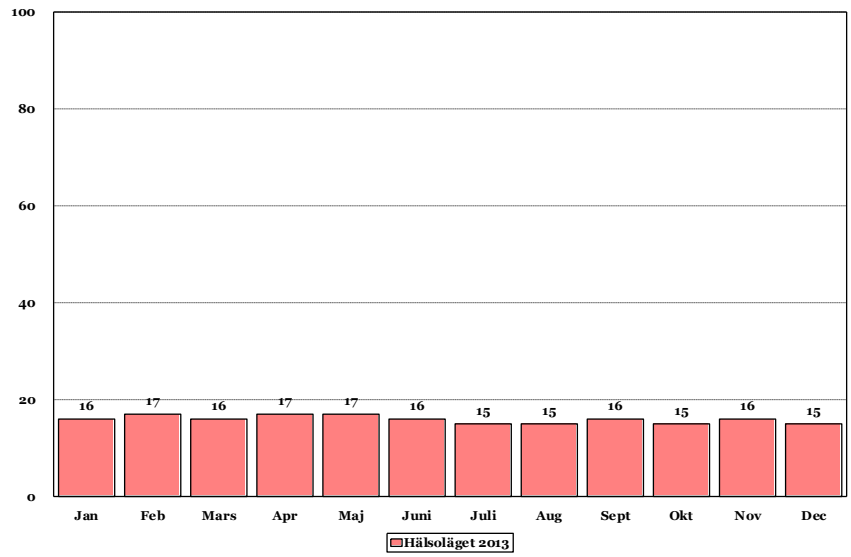


När man ser totalt på samtliga grupper är fördelningen mellan 1, 2 och 3 eller fler fel hyfsat jämn i undersökningsgruppen. Kategorin Universitet och högskolor har i år den lägsta felprocenten, tätt följt av ISP:er. Kategorierna Bank och Försäkring och Registrarer har flest fel, med två, tre eller flera. Trots att ISP:erna generellt har en låg felprocent är det en relativt stor andel som har tre eller flera fel.

För första gången är vår undersökning inte bara en ögonblicksbild av hur det ser ut just då mätningarna görs, utan vi har regelbundet mätt varje månad. Det innebär att även om det kan finnas anledning till att saker och ting förändras väldigt snabbt så verkar det i alla fall inte ha skett under förra året.

Tar man hela undersökningsgruppen och resultat per månad så fördelar de sig relativt jämnt över året.

Diagram 4: Andel fel per månad 2013 för hela undersökningsgruppen.



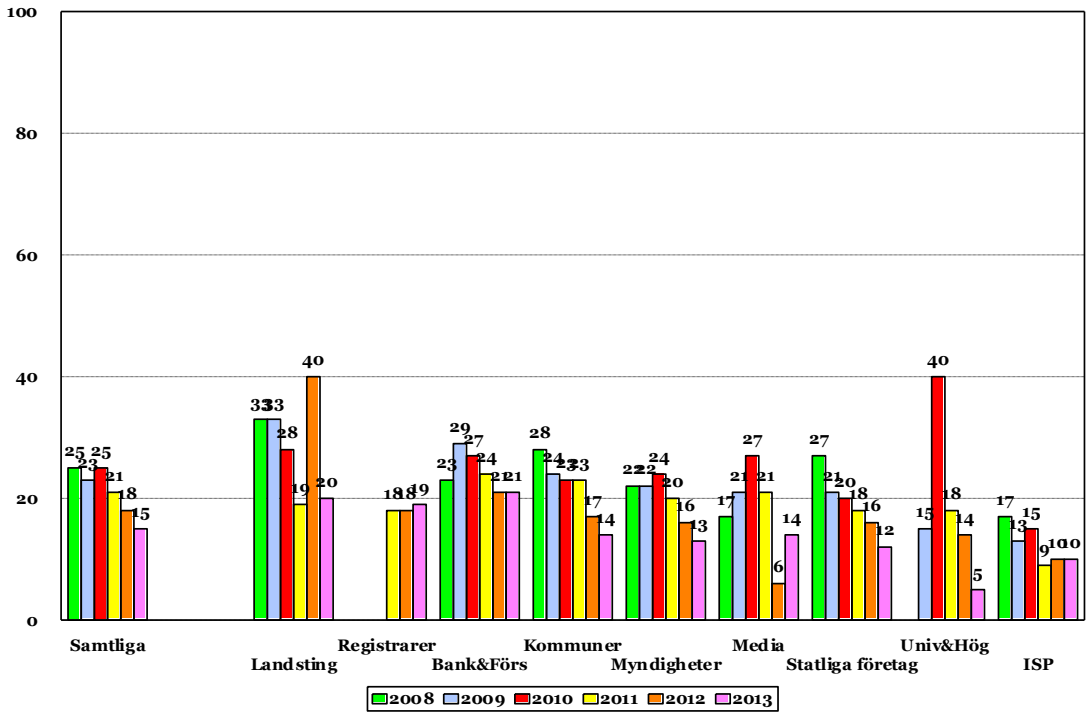
Vi har ju tidigare hävdat att alla kan komma under 20 procent fel utan större ansträngning. I årets mätning ser det ut som om det målet har uppnåtts för alla kategorier och över hela året. För att komma under 15 procent krävs det ytterligare insatser utöver att bara rätta till grundläggande hygienfaktorer, men det är absolut ingen omöjlighet. Det ska bli intressant att se om detta kommer att inträffa under 2014.

6.3 Jämförelse av andelen fel över tiden

I och med att vi har tillgång till data från tidigare undersökningar har vi också möjlighet att jämföra resultaten mellan årets och tidigare undersökningar för de kategorier som finns med i undersökningarna och för samtliga år. Några kategorier lades till 2009 och därför kan vi för dessa kategorier bara redovisa resultat från det året och framåt. Kategorin Registrarer tillkom först 2011.

I diagrammet nedan jämför vi andelen fel över tiden från 2008 till 2013 (med undantag för Universitet och högskolor respektive Registrarer som tillkom 2009 respektive 2011).

Diagram 5: Andel fel per år och kategori 2008-2013 (procent).



Av diagrammet kan vi se att situationen har förbättrats väsentligt inom i princip alla kategorier jämfört med tidigare år. Kategorin Media har dock ökat, från 6 till 14 procent, medan kategorin Universitet och högskolor har minskat i motsvarande grad, från 14 till 5 procent.

Kategorin Landsting utgör det stora undantaget. Andelen landsting med fel var 19 procent 2011 för att 2012 ha ökat till hela 40 procent fel. Vi gjorde dem uppmärksamma på problemet och nu är de tillbaka på mer acceptabla 20 procent.

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

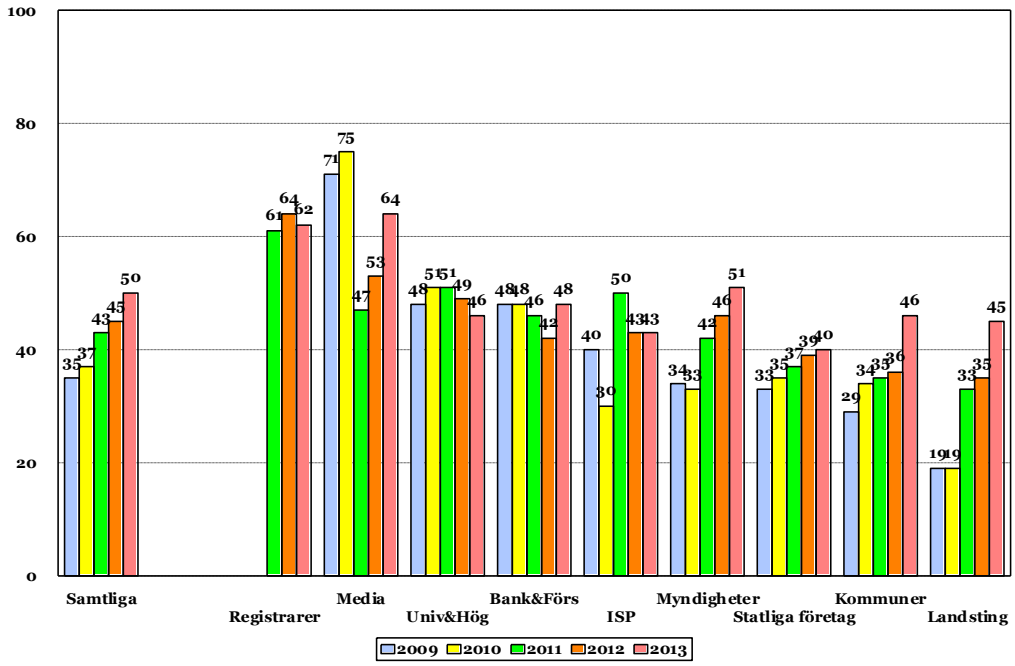
Värt att nämna är att .SE:s tre största registrarer har cirka 50 procent av marknaden men tar vi de sju största har dessa ökat sin marknadsandel till cirka 70 procent. Det råder inte något 1:1-förhållande mellan registrar och namnserveroperatör, men många registrarer agerar även namnserveroperatör för de domäner de hanterar. Vissa verksamheter driver sin egen DNS-infrastruktur eller anlitar andra tredjepartsleverantörer för drift av DNS.

6.4 Anslutning av namnserver 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. En risk med den utvecklingen är om en enskild operatör skulle dominera inom en viss kategori. Konsekvensen av en sådan dominans blir i värsta fall att en hel sektor drabbas om den dominerande operatören får problem.

Det ökar redundansen om namnservrarna är anslutna till olika operatörer. I diagrammet nedan ser vi hur stor andel av undersökningsgruppen som har namnservrar anslutna till fler än 1 AS (autonomt system), det vill säga hos fler än en operatör.

Diagram 6: Andel med namnservrar som annonseras i fler än 1 AS år 2009-2013.



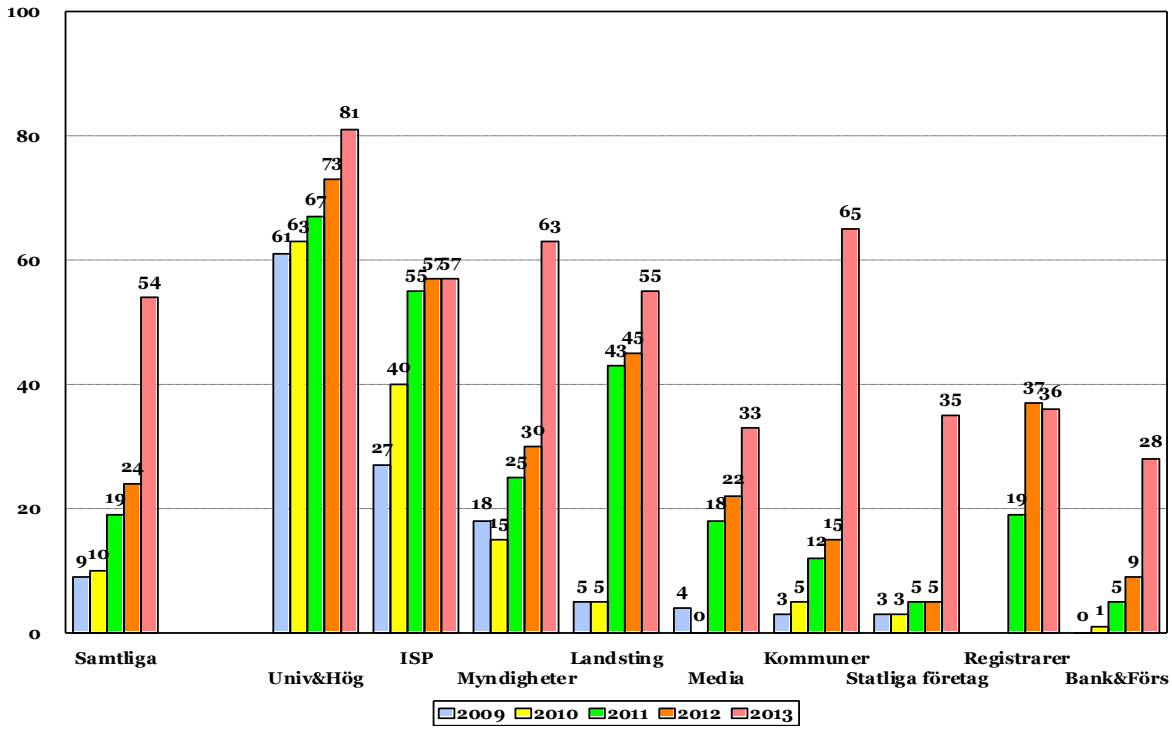
Av diagrammet ovan framgår en tydlig trend, det har skett en ökning från år till år och 2013 är det alltså 50 procent som har namnservrar placerade hos fler än en operatör. Procentuellt sett förefaller den största ökningen ha skett hos landstingen.

6.5 Namnservrar med IPv6

Det står väl numera klart för de flesta att införandet av IPv6 som gemensamt kommunikationsprotokoll är det enda sättet att garantera en stabil framtida internetinfrastruktur. Det finns en klart uttalad strategisk vilja från regeringens sida att alla myndigheter bör vara nåbara med IPv6 senast 2013, vilket slogs fast i En digital agenda för Sverige.

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 2013.

Diagram 7: Andel som använder namnservrar som går att nå med IPv6 2009-2013.



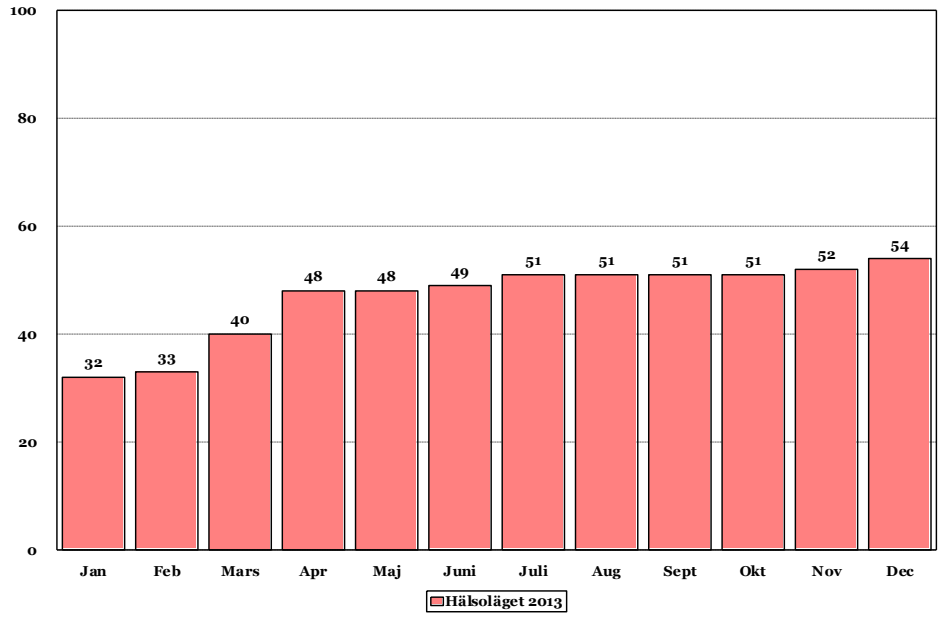
2013 har andelen av de undersökta domäner som har någon namnserver som går att nå via IPv6 nästan fördubblats, från 24 procent 2012 till 54 procent i den nu aktuella undersökningen. Det pågår ett intensivt arbete med att införa det nya protokollet för fullt hos internetleverantörerna, och även företag och organisationer har börjat följa efter.

Särskilt tydlig är utvecklingen inom offentlig förvaltning, där satsningen varit systematisk och underbyggd av både politiska signaler och konkret stöd från Post- och Telestyrelsen.

IPv6 införs parallellt med IPv4 och det gamla protokollet kommer inte att fasas ut förrän efter en övergångstid på flera år. .SE verkar på olika sätt för att underlätta och stödja införandet av IPv6 i Sverige.[5]

[5] https://www.iis.se/lar-dig-mer/ipv6/om

Diagram 8: Andel av undersökningsgruppen med IPv6 redovisat per månad 2013.

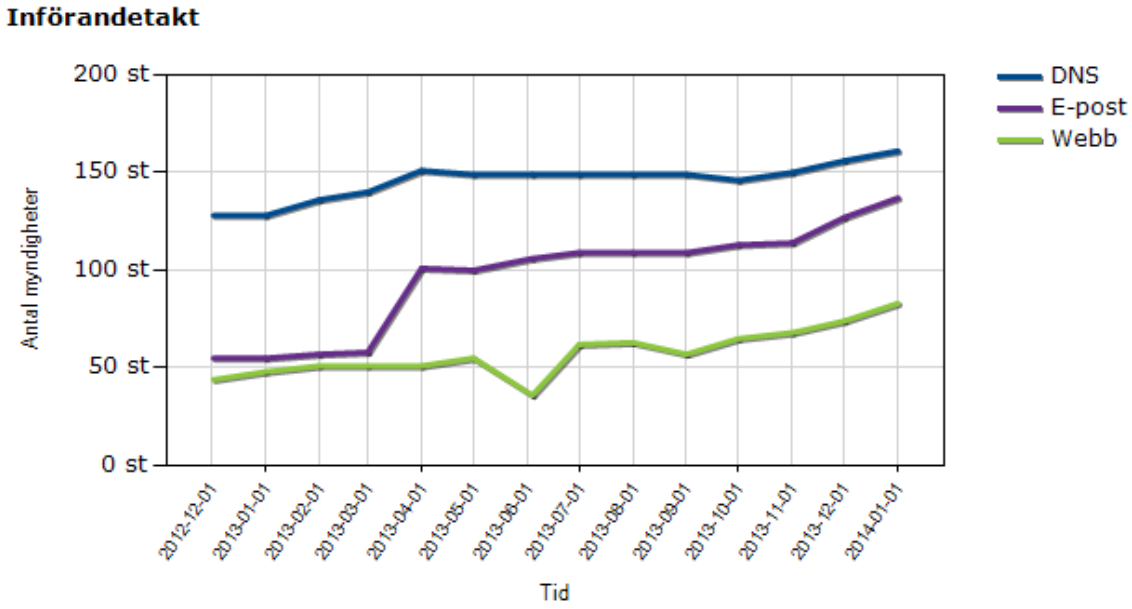


I diagrammet ser vi en tydlig förändring av resultaten från mätningarna per månad för 2013, och en stadig ökning.

Post- och telestyrelsen (PTS) ska enligt ett regeringsuppdrag följa upp myndigheternas införande av IPv6 specifikt. I samband med det har PTS lanserat webbsidan ”Myndigheter med IPv6”[6]. Där går det att kontinuerligt följa IPv6-införandet i det offentliga Sverige.

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

Diagram 9: Införandetakt av IPv6 2013 för DNS, e-post och webb.



Diagrammet visar myndigheters nåbarhet via IPv6 över tiden, inte bara avseende DNS, utan även för extern webbplats och e-post. PTS mätning av myndigheters tillgänglighet över IPv6 påbörjades i november 2012.

Det är viktigt att förstå att en övergång av det här slaget kräver förberedelser och arbete på omkring 12-18 månader. .SE:s råd är att planera i förväg och låta tekniker börja testa, de kommer långt med en brandvägg och en dator. .SE tillhandahåller en omfattande e-utbildning för IPv6: https://www.iis.se/lar-dig-mer/ipv6/e-utbildning/.

6.6 Namnservrar med rekursion påslaget

En namnserver som har rekursion påslaget 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 både vara arbetskrävande (ta datorkapacitet) och resultera i en relativt stor mängd data, vilket gör att man normalt sett faktiskt vill begränsa vem som får använda funktionen rekursion.

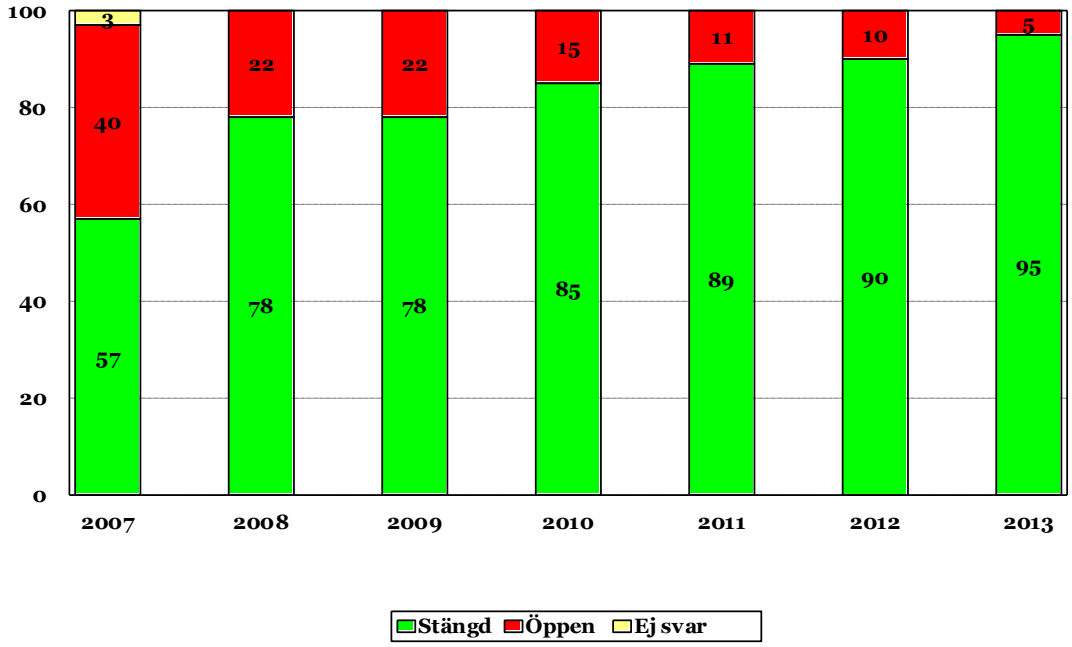
En **öppen** rekursiv namnserver svarar på alla frågor den får där rekursion har begärts. Detta gör det möjligt för utomstående att till exempel utföra tillgänglighetsattacker via den öppna namnservern genom att låta den ställa frågor som kommer att resultera i ovanligt stora svar. Detta i kombination med en falsk avsändaradress som leder till att svaret skickas någon annanstans, exempelvis en tredje part som valts ut till måltavla, utgör med stor sannolikhet en tillgänglighetsattack.

Som vi upprepat vid varje tidigare undersökning har öppna rekursiva namnservrar mycket få legitima användningsområden och kan alltså komma att utnyttjas bland annat i samband med överbelastningsattacker. Mot distribuerade överbelastningsattacker finns inget riktigt effektivt skydd, men det går att motverka att man blir en del av attacken och 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.

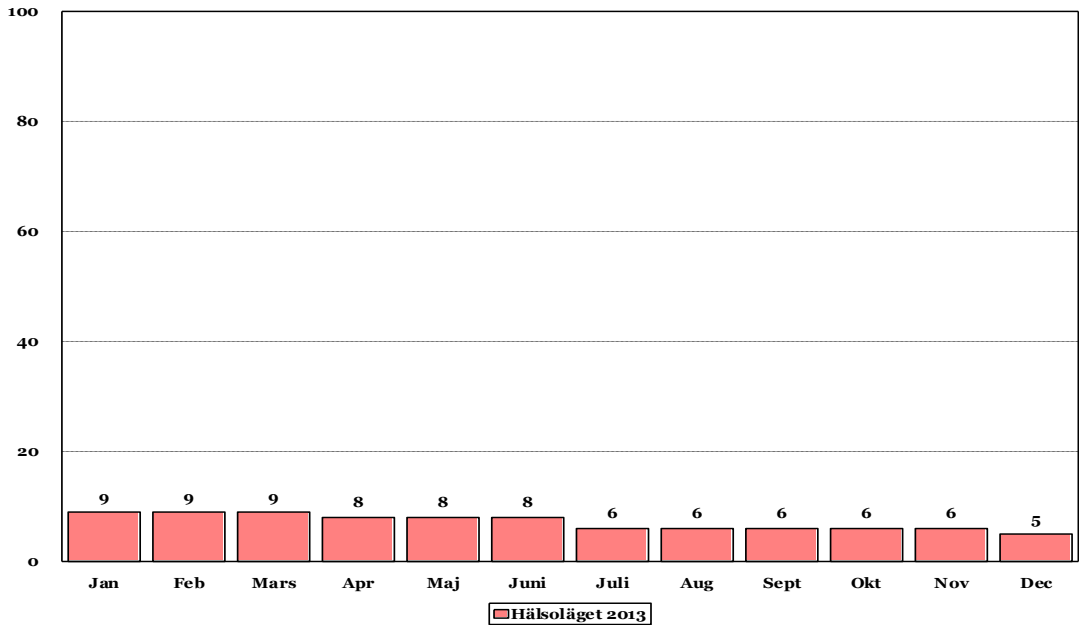
Andelen namnservrar som är öppna för rekursion minskar stadigt från år till år, och vi är 2013 nere i 5 procent jämfört med 10 procent 2012. Andelen har alltså halverats från 2012 till 2013, vilket är ett fantastiskt gott resultat.

Diagram 10: Andel namnservrar öppna för rekursion 2007-2013.



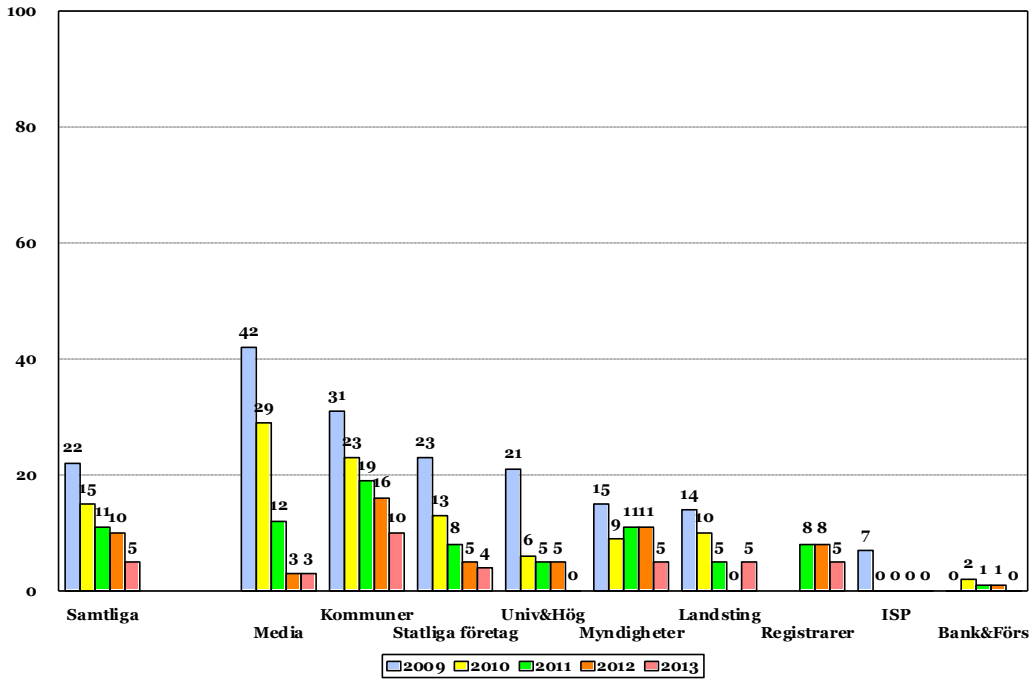
Vi ser alltså en tydlig förbättring även i år, och i synnerhet totalt över tiden. En av förklaringarna till dessa förbättringar är att namnservrar idag levereras med grundinställningen att funktionen rekursion är avslagen. Vi tror också att de som ansvarar för DNS-infrastrukturen för en verksamhet har blivit bättre på att införa separation mellan auktoritativa namnservrar (de som faktiskt ska svara på frågor) och resolvrar (de som bara förmedlar frågor och svar).

Diagram 11: Andel med öppna rekursiva namnservrar per månad 2013.



Diagrammet ovan redovisar resultaten per månad och visar att det skett en tydlig förbättring över året från 9 procent i januari till 5 procent i december, med en stadigt fallande andel om man ser till året som helhet.

Diagram 12: Namnservrar öppna för rekursion per kategori.



Offentlig förvaltning, det vill säga kategorierna Landsting, Myndigheter och Kommuner står sammantaget för den största andelen rekursiva namnservrar, men det har ändå skett en förbättring bland både myndigheter och kommuner.

Kategorin Landsting hade förra året andelen 0 procent, så där har det skett en försämring eftersom man nu landar på 5 procent. Kategorin ISP behåller sitt resultat med 0 procent även i 2013 års undersökning.

6.7 Användning av DNSSEC

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

DNSSEC 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 verifiera signaturen kan man förvissa sig om att DNS-informationen inte har förändrats på vägen från namnserver till mottagande system.

.SE:s lansering 2005 av DNSSEC för säkrare DNS bidrog till att ett ökat fokus hamnade på DNS och DNS-drift. Den som har för avsikt att göra sin DNS-infrastruktur säkrare genom att använda DNSSEC inser tämligen snabbt att införandet inte låter sig göras med mindre än att det först görs en översyn av den egna DNS-infrastrukturen som helhet.

Även DNSSEC fick stor uppmärksamhet i regeringens IT-politiska strategi ”IT i människans tjänst – En digital agenda för Sverige”[7], tillsammans med aktiviteter från PTS och i MSB:s handlingsplan ”Samhällets informationssäkerhet – Nationell handlingsplan 2012”[8]. .SE driver på utvecklingen också inom detta område genom att ha regelbundna kampanjer för registrarer med .se-domäner.

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 som på olika sätt stödjer och uppmuntrar införandet av DNSSEC har i ett samarbete med MSB, PTS, och SKL arbetat med att ta fram en paketlösning som kommunerna kan använda sig av.

I princip alla internetbaserade tjänster är beroende av att DNS fungerar. Konsekvensen av att göra fel kan bli omfattande. Detta gäller i än högre grad vid införandet av DNSSEC för att skydda informationen som kommuniceras mellan servrarna i DNS från manipulation. DNSSEC ställer högre krav på teknisk kompetens för drift än traditionell DNS.

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

.SE har publicerat en vägledning[9] 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 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.

Det - och 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 så kallade 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.

6.8 Hur utbredd är användningen av DNSSEC?

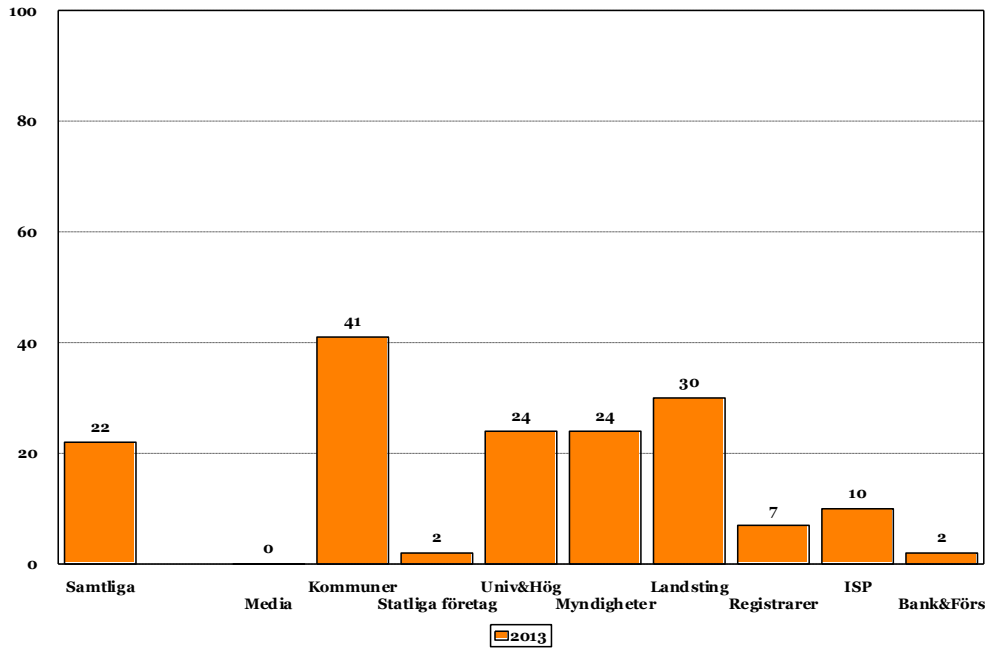
Vid 2012 års undersökning hade antalet signerade domäner bland undersökningsgruppens 913 domäner ökat till 100 domäner, motsvarande 11 procent.

Vid 2013 års undersökning har antalet signerade domäner i undersökningsgruppen ökat till 204 domäner, motsvarande en andel om 22 procent, och en dryg fördubbling av antalet signerade domäner i undersökningsgruppen.

Kontrollgruppen som utgör 1 procent av .se-zonen hade vid årsskiftet totalt 3 193 signerade domäner, eller 25 procent, alltså något fler än vad som finns i undersökningsgruppen.

[9] https://www.iis.se/docs/dnssec-rek-2013.pdf

Diagram 13: Procentandel med DNSSEC totalt och per kategori 2013.



Inte oväntat toppar kommunerna med 41 procent signerade domäner, därefter följer kategorierna Landsting med 30 procent samt Universitet och Högskolor och Myndigheter med vardera 24 procent. Här kan vi konstatera att den offentliga sektorn leder stort när det gäller DNSSEC-signerade domäner.

Media saknar totalt signerade domäner. Både kategorin Statliga företag och Bank och Försäkring ligger på blygsamma 2 procent. Framför allt det senare är förvånande då .SE sedan åtminstone 2007 fört aktiva samtal med svenska storbanker via Svenska Bankföreningen och erbjudit olika former av stöd för ett sådant införande. Varför man inom bank- och finanssektorn inte bedömer DNSSEC som en viktig åtgärd för att skydda sin infrastruktur är oklart.

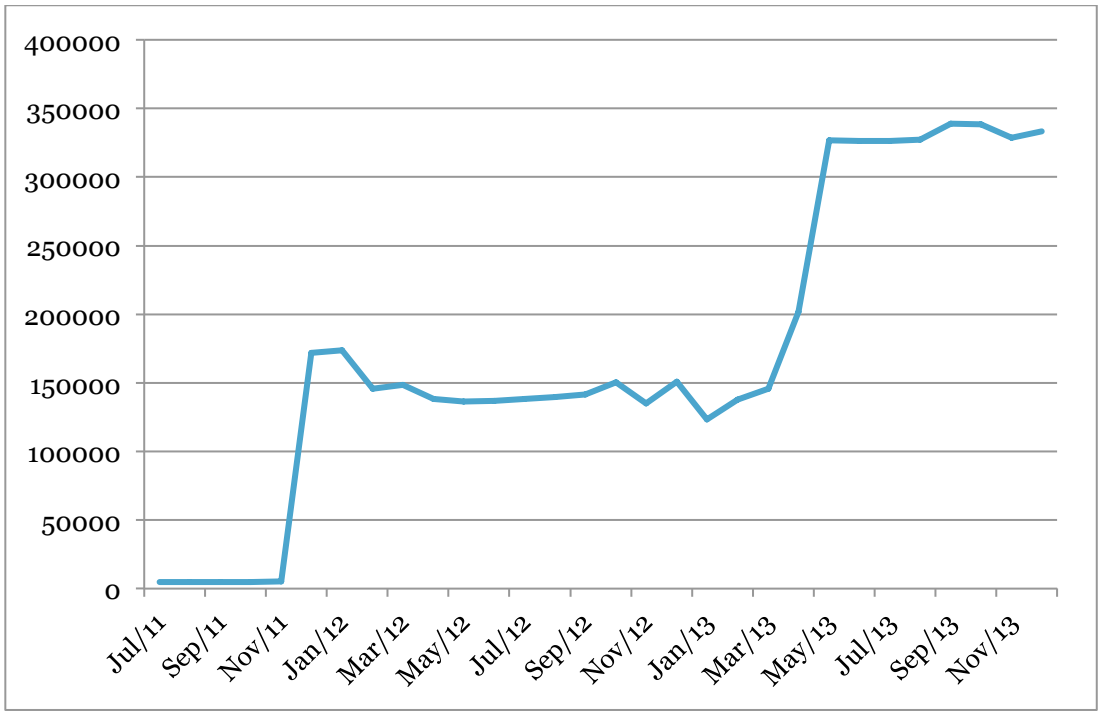
Som resultat av en omfattande kampanj från .SE som inleddes i december 2011 har vi sett en mycket omfattande ökning av DNSSEC-signerade domäner i .se-zonen som helhet. I februari 2012 gjorde vi en djupdykning i DNSSEC-mätningar vilket redovisades i en rapport[10] som publicerades i mars 2012, och som var särskilt inriktad på DNSSEC-kvalitet.

2012 noterade vi emellertid en minskning eller åtminstone stagnering av antalet signerade domäner då en del DNS-operatörer tvingades att slå av DNSSEC på grund av att de stötte på problem i den tekniska miljön.

I diagrammet på nedan redovisas tillväxten för DNSSEC-signerade domäner för hela .se-zonen, alltså inte bara undersöknings- och kontrollgrupperna.

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

Diagram 14: Tillväxt – domäner signerade med DNSSEC i hela .se-zonen 2011-2013.



Den starka tillväxt som noteras under 2013 kan hänföras till ett beslut från några av .SE:s registrarer att signera alla sina kunders domäner. I tabellen nedan redovisas andelen signerade domäner av det totala antalet domäner som respektive registrar hanterar.

Registrar (bokstavsordning)	Andel signerade domäner (%)
Binero	68
City Network	71
Domeneshop	77
GTLD Systems	82
Internetbolaget	75
Larsen Data	87
One.com	86
Vildmarksdata	80

I oktober 2011 hade 24 kommuner signerat sina domäner. I oktober 2012 var antalet 36, en ökning med 12 kommuner. I december 2013 är antalet kommuner med DNSSEC-signerade domäner så många som 120. Vi befarade tidigare att det med den tillväxttakt vi noterade 2012 skulle ta mycket lång tid innan samtliga kommuners domäner var signerade, men med påtryckningar och inte minst stöd genom både de politiska målen och resurser från ansvariga myndigheter har tillväxttakten ökat väsentligt. Det går om man vill!

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 betyder att alla resurser som knyts till den domänen i form av till exempel e-post och webb också 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 litet utrymme för att reagera och reparera vid driftstörningar.

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 inte.

Varje domän har ett antal poster knutna till sig i DNS, det är 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.

6.9 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 nya toppdomäner börjat läggas till i rotzonen, efter beslut från ICANN. Innehavare av dessa nya toppdomäner har som obligatoriskt krav att toppdomänen måste vara signerad med DNSSEC.

Enligt aktuell statistik[11] är av totalt 391 toppdomäner som annonseras i rotzonen (2014-01-11) för närvarande 198 signerade med DNSSEC och av dessa har 191 också publicerat information om sina nycklar i rotzonen. Dessa siffror förändras i takt med att nya toppdomäner godkänns och läggs till i rotzonen.

[11] Aktuell statistik redovisas kontinuerligt på http://stats.research.icann.org/dns/tld_report/.

7 Viktiga parametrar för elektronisk post

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

Under 2012 publicerade vi en fördjupad rapport[12] 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 även gjorde en djupdykning i en del tekniska parametrar genom mätningar med användning av vårt verktyg MailCheck[13].

7.1 Stöd för transportskydd (TLS)

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

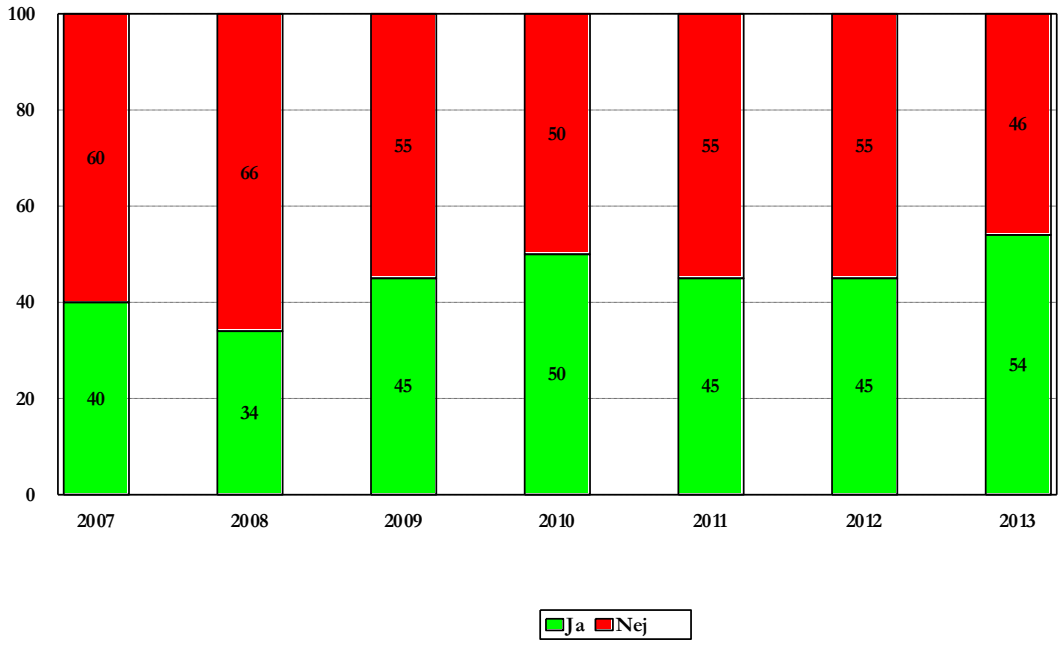
TLS används för att kryptera kommunikationen mellan två enheter, varav den ena ofta är en webbserver och den andra en webbläsare, men e-postservrar och e-postprogram använder samma teknik vid överföring av elektronisk post (SMTP). Tanken med att skydda den information som utväxlas mellan dessa enheter 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 man använder TLS 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 konfidentialitet (kryptering) även riktighet (dataintegritet), och beroende på hur det används dessutom 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 och det betyder att det är fler som vidtar åtgärder för att skydda e-posttrafiken från insyn än tidigare. Diagrammet nedan visar utvecklingen av andelen e-postservrar med stöd för TLS åren 2007-2013.

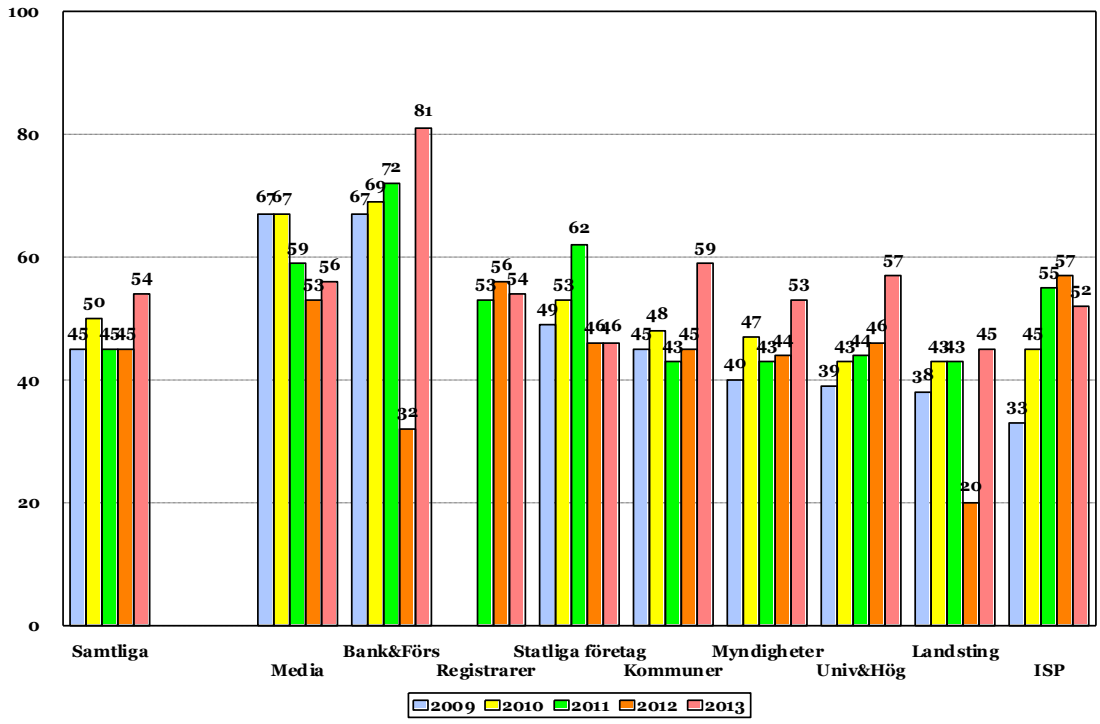
[12] https://www.iis.se/docs/Elektronisk_post_med_kvalitet_och_finess.pdf
[13] https://mailcheck.iis.se

Diagram 15: Andel e-postservrar med stöd för TLS 2007-2013.



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

Diagram 16: E-postservrar med stöd för TLS per kategori 2009-2013.



Att användningen av transportskydd av e-post inte har fått större genomslag än 56 procent sedan denna del av undersökningen påbörjades 2009 i kategorin Media är särskilt intressant i ljuset av det så viktiga meddelarskyddet, alltså vikten av att skydda uppgiftslämnare som förser journalister med information. Tvärtom har andelen minskat sedan den första mätningen 2009.

Vi borde kunna förvänta oss en ökad användning av kryptering i efterdyningarna av Snowdens avslöjanden om massiv avlyssning från signalspaningsmyndigheter i olika länder (som amerikanska NSA) av internetanvändares kommunikation.

Användningen har ökat mest inom kategorin Bank & Försäkring som är uppe i hela 81 procent. Ökat har det också gjort inom hela den offentliga förvaltningen inklusive Universitet och högskolor.

7.2 Placering av e-postservrar

Vi kan utan tvekan dra slutsatsen att det 2013 är en ännu större andel e-postservrar som använder IPv6-adresser än tidigare år. En svårighet med denna del av undersökningen som mäter var e-postservrar står placerade rent geografiskt är att det inte med någon visshet går att bestämma var IPv6-adresserade e-postservrar står placerade, åtminstone inte med de verktyg vi har till vårt förfogande.

Tack vare att IPv4-adresser fortfarande används parallellt i mycket stor utsträckning fortsätter vi dock att mäta den uppskattade placeringen av åtminstone de servrar som använder IPv4-adresser.

Diagram 17: Geografisk placering av domäners e-postservrar.

Vårt antagande om den huvudsakliga anledningen till placeringen av e-postservrar utanför landet är att det med största sannolikhet beror på att verksamheter anlitar någon tredjepartsleverantör för att hantera filtrering av virus och skräppost (spam) för deras räkning, men det är svårt att härleda resultaten utan att fördjupa oss i den delen av materialet, något som vi valt att inte göra i denna rapport.

Vad vi kan säga är att de undersökta domänernas MX-pekare fördelar sig på 3 276 olika servrar (unika IP-adresser). De utländska operatörer som har många kunder skalar upp antalet rejält, både med många namn och IP-adresser. Vi har kontrollerat per namn om de har namnservrar utomlands.

Den vanligaste placeringen verkar vara i USA. Andra relativt vanligt förekommande länder är exempelvis Irland, Tyskland, Nederländerna, Frankrike, Storbritannien, Finland och Norge.

En konsekvens av att till exempel myndigheters och kommuners e-postservrar är placerade utanför Sverige är emellertid att en hel del av bland annat den offentliga förvaltningens e-postkommunikation passerar ett främmande land på sin väg till mottagaren. I medias fall gäller detsamma för e-postkommunikation mellan exempelvis uppgiftslämnare och journalister. Med tanke på att kommunikationen ofta också är 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 lite drygt hälften, eller 54 procent, av de undersökta verksamheterna som har möjlighet att använda kryptering för transportskydd av elektronisk post.

Om kryptering inte används för transportskydd innebär det att inte bara den svenska utan även 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 gissa.

Under 2013 har exempelvis FRA:s medverkan i NSA:s övervakning visat vad många befarade när den så kallade FRA-lagen klubbades igenom juni 2008, FRA tittar på vad som skickas i kablarna och de delar med sig av materialet till den amerikanska signalspaningsmyndigheten NSA.

TV-programmet Uppdrag Granskning[14] avslöjade i början av december 2013 nya uppgifter i Snowden-dokumenten om Sverige. Där konstateras att USA sedan 2004 får unik tillgång till svenska signalunderrättelsemyndigheten FRA:s avlyssning och sedan 2011 en kraftigt ökad tillgång till FRA:s kabelavlyssning. 2004, fyra år innan FRA-lagen ens fanns på plats, knöts än tätare band direkt mellan FRA, amerikanska NSA och brittiska GCHQ i bilaterala samarbetsavtal.

.SE har i samarbete med Journalistförbundet producerat en guide med titeln ”Digitalt källskydd – en introduktion”[15] 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”[16] – som förklarar hur exempelvis kryptering används i praktiken.

[14] http://www.svt.se/ug/fra-spionerar-pa-bestalning-av-nsa-avtal-sedan-1954
[15] https://www.iis.se/lar-dig-mer/guider/digitalt-kallskydd-en-introduktion/
[16] https://www.iis.se/docs/lar-dig-kryptering.pdf

8 Viktiga parametrar för webbtjänster

I undersökningen från 2013 har vi inte särskilt analyserat hur anslutning av webbservrar sker till internet, om man använder sig av en och samma internetoperatör för alla servrar eller vilka programvaror för webbservrar som är vanligast. Det finns dock ingenting som tyder på att dominansen från Microsoft Internet Information Server (Microsoft IIS) och Apache har ändrats nämnvärt.

Många verksamheter förmedlar information och tjänster via webbgränssnitt och många verksamheter är helt beroende av att deras webbtjänster 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.

Många organisationer som omsätter åtskilliga miljoner och kanske till och med miljarder i verksamheten varje år, med miljontals användare av tjänsterna varje år och där tjänsterna representerar deras kärnverksamhet borde ha råd med redundans, som till exempel att sätta upp en spegelsajt hos en annan leverantör, att ha anslutning till fler än en internetoperatör och att ha system för reservkraft. Det borde dessutom vara prioriterade åtgärder. Tyvärr saknas detta i många fall.

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 och där man kan vänta sig starka reaktioner från sina användare om det inte fungerar tillräckligt bra.

Å andra sidan kanske det är så att webbplatsen inte är en verksamhetskritisk funktion, och att det därmed inte gör något om den skulle vara nere några timmar om året.

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

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

9 Jämförelse med .se-zonen

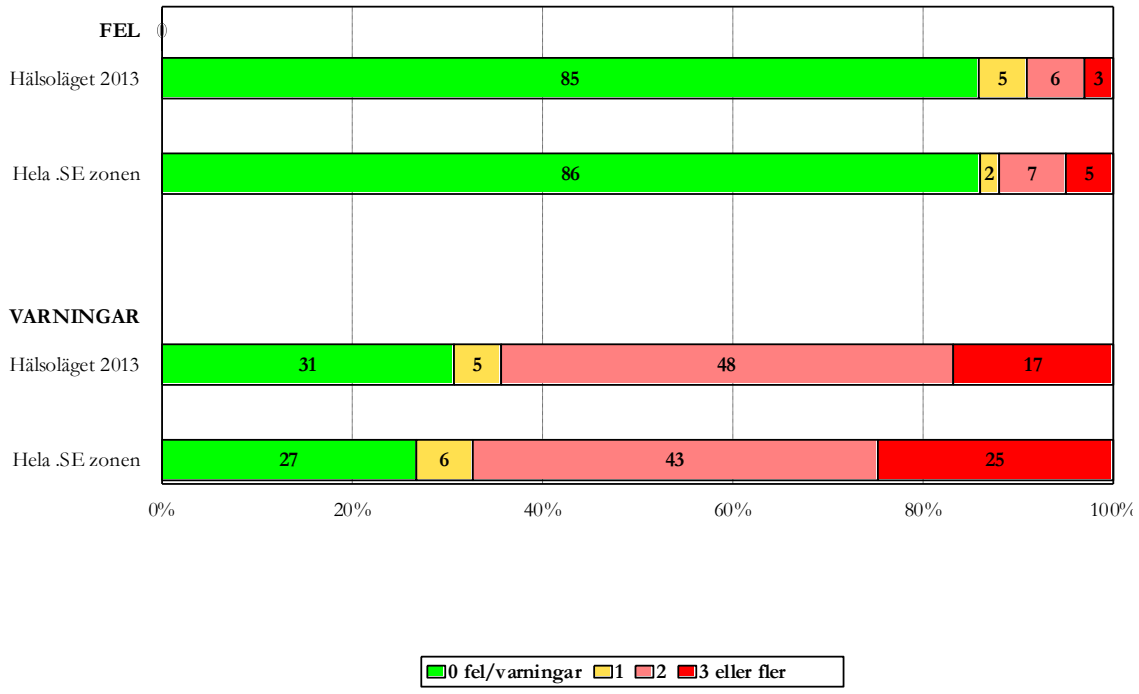
För att se om vår undersökningsgrupp är i bättre eller sämre skick än .se-zonen som helhet har vi även i årets undersökning gjort ett utsnitt av en procent slumpmässigt valda domäner ur hela .se-zonen för att ha som jämförelse.

I diagrammen nedan representerar ”Hälsoläget 2013” den aktuella undersökningsgruppen med sina 913 domäner medan ”Hela .se-zonen” representerar det slumpmässiga urvalet motsvarande en procent av hela .se-zonen eller 12 598 domäner.

9.1 Fördelning av fel

Vi tittar som tidigare först och främst på fördelningen av fel och varningar, och hur undersökningsgruppen Hälsoläget 2013 som ändå innehåller en hel del kritiska funktioner och verksamheter förhåller sig till jämförelsegruppen Hela .se-zonen.

Diagram 18: Andel fel i Hälsoläget 2013 respektive Hela .se-zonen 2013.



I 2013 års undersökning är det i princip lika många felfria domäner i undersökningsgruppen som kontrollgruppen för .se-zonen som helhet.

Däremot ser det ut som att hela 69 procent av domänerna är behäftade med brister som genererar en varning. Den siffran är emellertid orsakad av samma mätproblem som redovisats tidigare i rapporten.

Som en del av vårt arbete med att utveckla internet släppte .SE i januari 2013 rapporten Elektronisk post med kvalitet och finess[17]. I rapporten behandlar vi e-post och hur man behöver sätta upp det för att det ska fungera bra för alla, både avsändare, leverantör och mottagare.

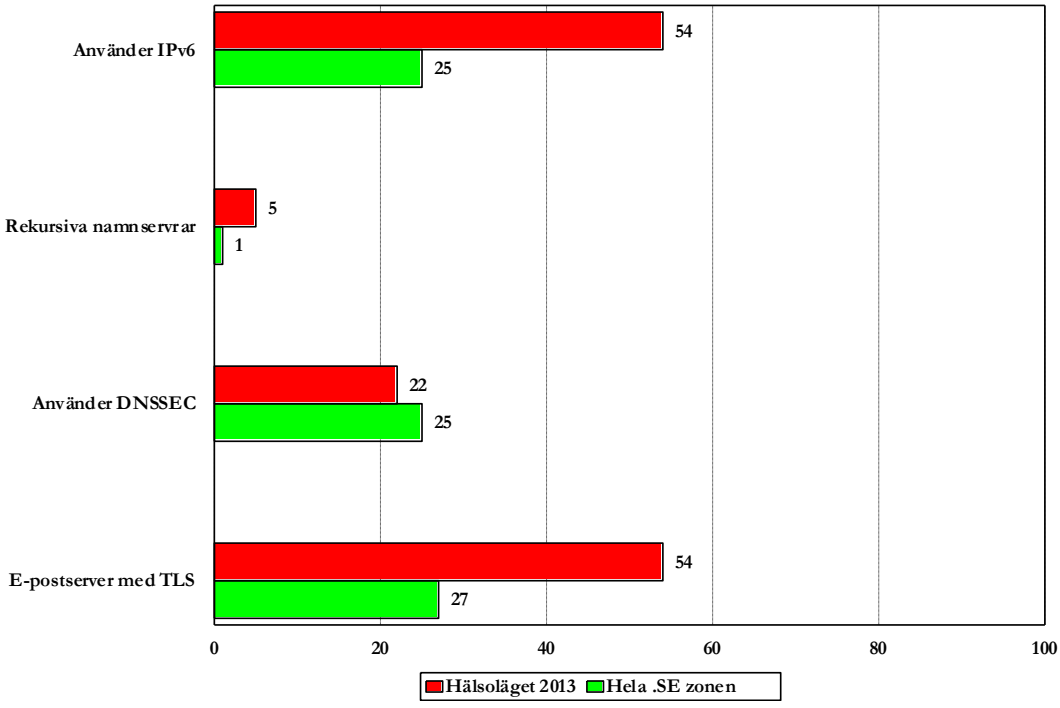
9.2 Skillnader mellan undersökningsgruppen och jämförelsegruppen

De största skillnaderna mellan undersökningsgruppens 913 domäner och jämförelsegruppens 12 598 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 även där mot 27 för .se-zonen som helhet.

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

Andelen som använder DNSSEC är betydligt större 2013 än den var 2012, 22 respektive 25 procent mot tidigare 11 procent i undersökningsgruppen och 10 procent i jämförelsegruppen för .se-zonen som helhet.

Diagram 19: Jämförelse mellan undersökningsgruppen och .se-zonen 2013.



[17] https://www.iis.se/docs/Elektronisk_post_med_kvalitet_och_finess.pdf

I diagrammet ser vi skillnaderna mellan undersökningsgruppen (röd stapel) och jämförelsegruppen för .se-zonen som helhet (grön stapel) för de olika delar som vi har studerat. Generellt finns det 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 till exempel öppna rekursiva namnservrar. När det gäller utbredningen av DNSSEC är det relativt lika i båda grupperna.

10 Stöd för skydd vid kommunikation

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.

10.1 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), även känt som Secure Socket Layer (SSL), 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.

10.2 Kan man lita på certifikat?

Det räcker inte med att ha ett certifikat utfärdat för domänen eller webbservern. Certifikatet måste också kunna betraktas som pålitligt genom att det uppfyller några grundläggande krav som ska ställas på den typen av säkerhetsmekanismer, 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.

10.3 Vem behöver använda certifikat?

Alla som via en webbplats begär från eller lämnar ut till användare någon form av känslig information såsom 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 för säkerhetskritiska webbservrar.

10.4 Resultat från tidigare undersökningar 2007-2012

Vid undersökningen 2007 genomförde vi den första granskningen av förekomsten av och kvaliteten på skydd vid kommunikation. Vid det tillfället hade endast en fjärdedel av de undersökta webbservrarna stöd för TLS/SSL. Motsvarande siffra 2008 var tre fjärdedelar. Vi kan tyvärr inte jämföra undersökningarna över åren då vi 2009 ändrade metoden för hur vi kontaktar webbservrarna.

Vid undersökningen 2010 testade vi vad som levereras som svar på en HTTP och HTTPS GET-fråga till domännamnen i undersökningsgruppen med "www." placerat framför. 2010 returnerade 227 av 670 domäner eller 34 procent något vettigt på frågor som rör certifikat. Av dessa 227 domäner kunde vi enbart ladda ner helt korrekta certifikat utfärdade av någon känd CA från 190, eller 84

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

procent, vilket var en ökning med 6 procent från året innan. Av den totala mängden undersökta domäner var det 2010 alltså endast 28 procent som hade certifikat som användarna i någon mån kunde lita på.

2011 mätte vi enbart på e-postservrar och om de använde TLS. Av de undersökta verksamheterna 2011 hade endast 45 procent stöd för TLS/SSL i sina e-postservrar. Huruvida dessa var utrustade med certifikat som var utfärdade av någon godkänd CA kontrollerade vi inte.

Vi konstaterade dock att webbteknik, förutom i traditionella webbtjänster, allt oftare används för M2M-kommunikation (maskin-till-maskin). Där är det också viktigt med säkrad kommunikation i form av transportskydd, skydd mot återuppspelningsattacker, autentisering av server respektive autentisering av klientdelen.

Fortfarande 2012 hade endast 45 procent stöd för TLS/SSL i sina e-postservrar. Det var alltså oförändrat från året innan, och det betyder att det i vart fall inte var fler som hade vidtagit tillräckliga åtgärder för att skydda e-posttrafiken från insyn. I 2012 års undersökning hoppade vi medvetet över undersökningen av certifikat för användning i webb, och lade i stället energin på att utveckla ett nytt verktyg för att kunna göra fler och mer detaljerade mätningar 2013.

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.

10.5 Resultat från undersökningen av certifikat

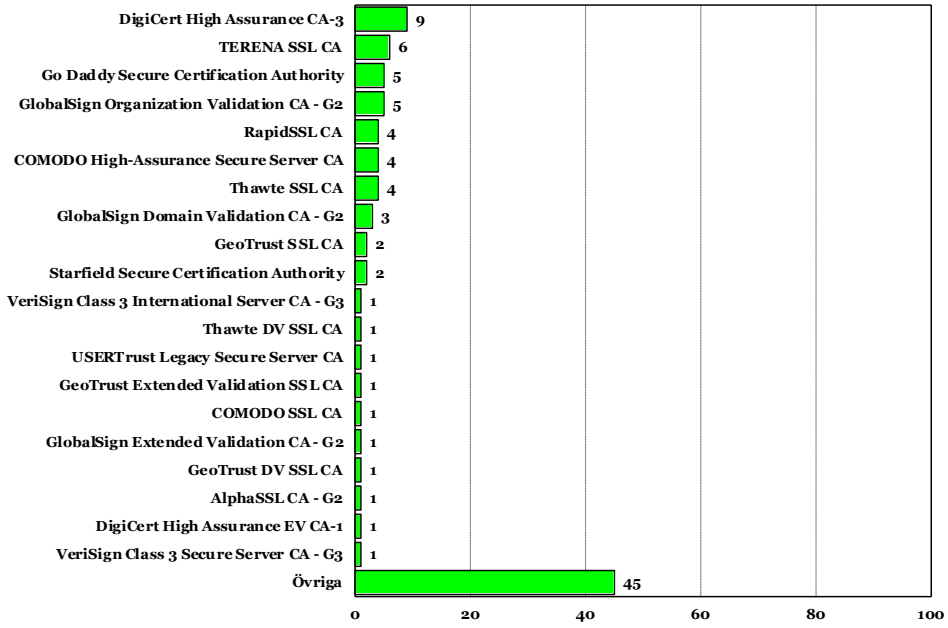
För att mäta förekomsten och kvaliteten på certifikat har vi till 2013 års undersökning utvecklat ett nytt verktyg för att kunna göra fler och mer detaljerade mätningar från användningen av och kvaliteten på certifikat för både e-post och webbtjänster. Med hjälp av programmet har vi gjort körningar mot undersökningsgruppen där vi tittat specifikt på de certifikat som används och deras kvalitet.

Totalt har 1 648 ändpunkter (424 för e-post och 1 224 för webb) analyserats. Dessa presenterar totalt 629 unika certifikat (171 för e-post och 458 för webb).

10.5.1 De vanligaste certifikatutfärdarna

Vi har under tidigare år rekommenderat att verksamheter ska skydda e-post respektive webbservrar med certifikat som är utfärdade av allmänt accepterade certifikatutfärdare och även ha kontroll över deras giltighet. Enligt vår uppfattning bör det dessutom finnas minst en svensk sådan aktör. I undersökningen 2013 har vi kartlagt vilka som utfärdat certifikat till de domäner där det förekommer över huvud taget.

Diagram 20: Vanligt förekommande certifikatutfärdare.



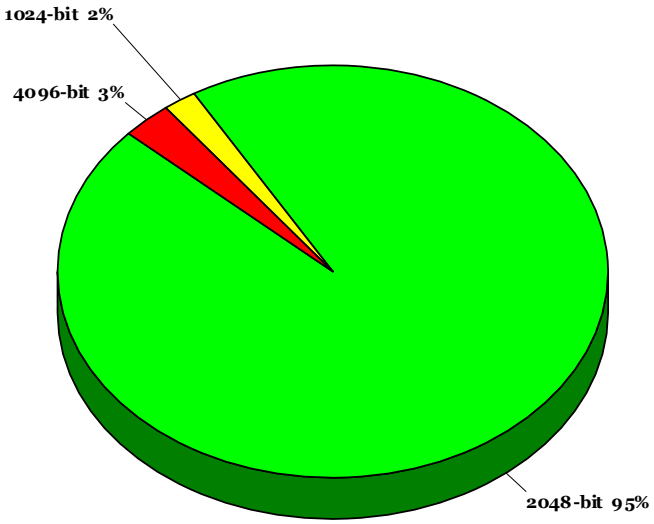
10.5.2 Certifikattyp och nyckellängder

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).

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.

Diagram 21: Nyckellängder.



Av de undersökta certifikaten är 95 procent RSA-certifikat med 2048-bitars nyckellängd, övriga är antingen gamla RSA 1024-bitars certifikat (2 procent) eller certifikat med RSA 4096-bitar (3 procent).

10.5.3 Jokercertifikat och interna värdnamn

Användningen av jokercertifikat (wild card) är anmärkningsvärt hög, 83 procent för e-post och 58 procent för webb. Ett jokercertifikat 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.

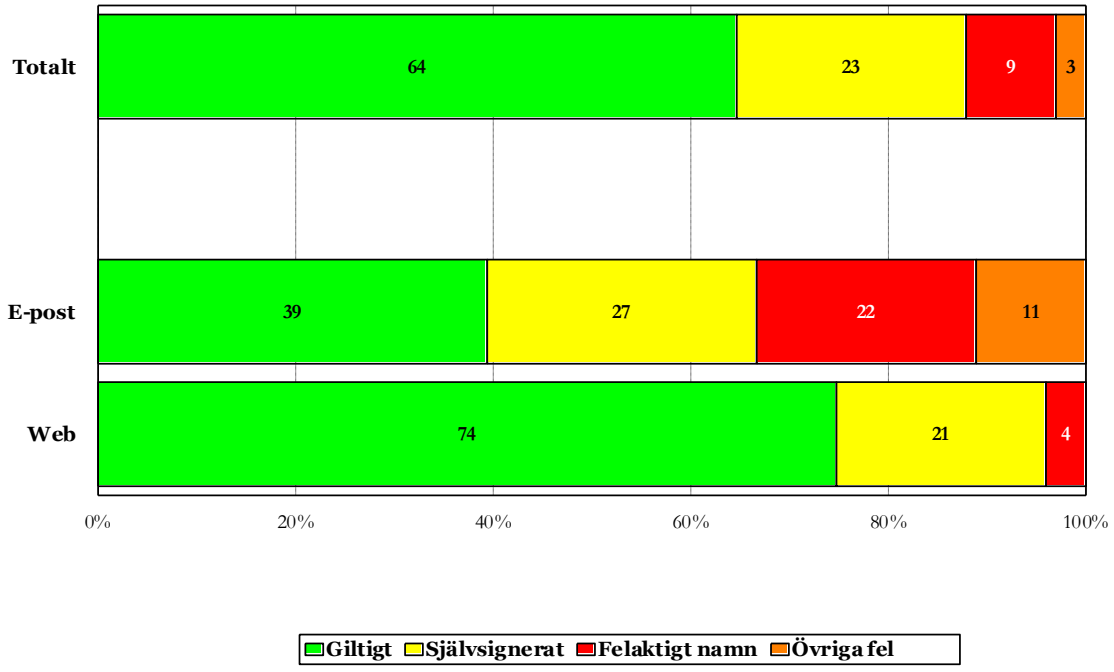
16 procent av certifikaten var utgivna till interna värdnamn (som till exempel "intranet.local"). Detta är särskilt anmärkningsvärt då de därmed inte unikt identifierar en tjänst och lätt kan missbrukas av någon med ont uppsåt för att förfalska information.

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

10.5.4 Giltiga certifikat

Av de certifikat som var utfärdade för domänerna i undersökningsgruppen gick endast 64 procent att verifiera mot en publik certifikatutfärdare. 23 procent av certifikaten var självsignerade, resterande 13 procent hade antingen gått ut (det vill säga passerat sista användningsdag) eller hade andra typer av fel.

Diagram 22: Giltiga och verifierbara certifikat.

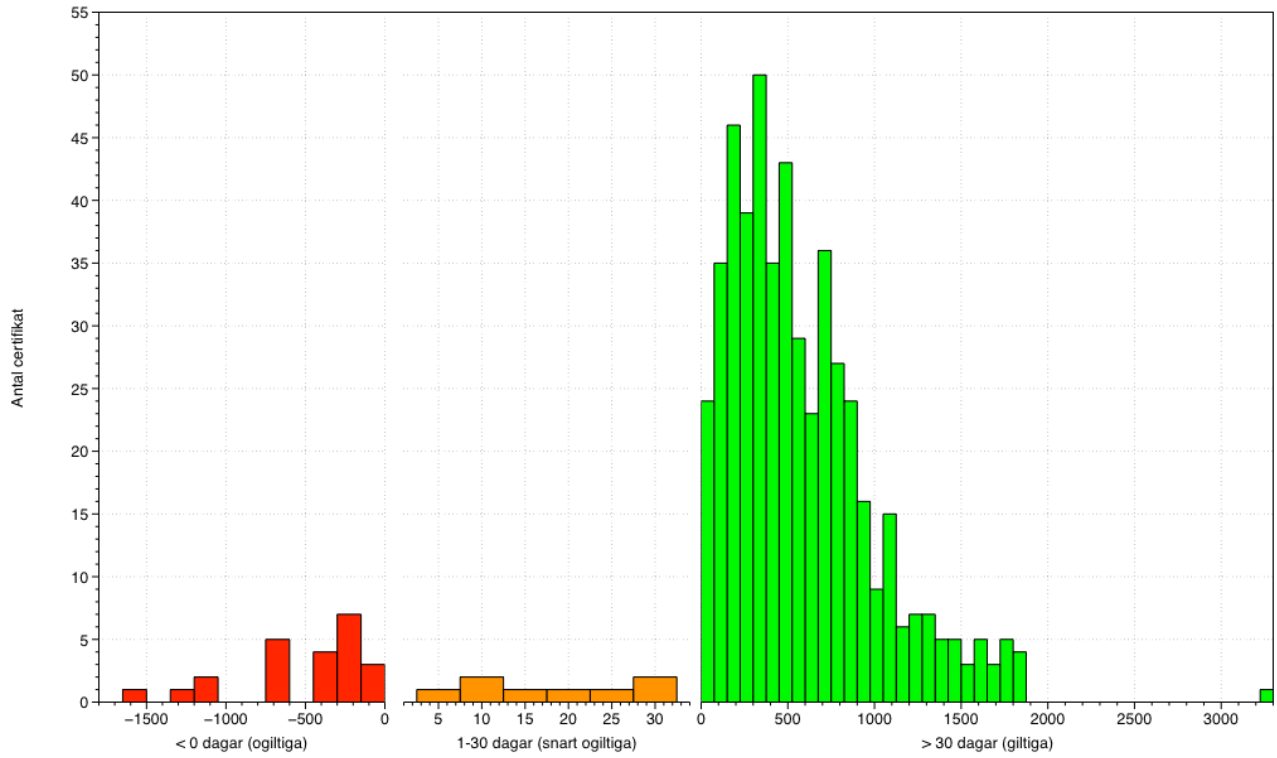


Det finns flera anledningar till att ett certifikat inte går att verifiera, trots att det är utgivet av en allmänt accepterad certifikatutfärdare. Den absolut vanligaste anledningen är att certifikatet inte används för rätt tjänst (till exempel att certifikatet för www.example.se används för tjänsten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

10.5.5 Certifikatens giltighetstid

Av diagram 23 framgår hur lång tid som återstår av certifikatens giltighetstid samt hur många som redan har gått ut.

Diagram 23: Giltighetstid för undersökta certifikat.



Som synes befinner sig de flesta på den säkra sidan, men det finns en relativt stor andel med certifikat som har passerat sista användningsdag, eller är på god väg att göra det genom att de förfaller inom den närmaste 30-dagarsperioden. En intressant mätning vore att följa upp hur många av de som var på väg att gå ut vid undersökningstillfället de facto inte förnyades i tid.

10.5.6 Spärrkontroll

Drygt 99 procent av 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.

10.5.7 Användning av https-anrop

Så stor andel som 24 procent av webbplatserna skickar en användare som anropar tjänsten över HTTPS (krypterat) tillbaka till HTTP (klartext). Detta kan tyckas vara lite underligt, särskilt som man borde göra tvärtom, det vill säga skicka användare som anropar tjänsten i klartext till den skyddade webbplatsen när sådan finns.

32 procent av webbplatserna ger ett felmeddelande. Detta beror oftast på att webbplatsen inte är publicerad över HTTPS men att webbservern ändå lyssnar på anrop (som således hanteras felaktigt).

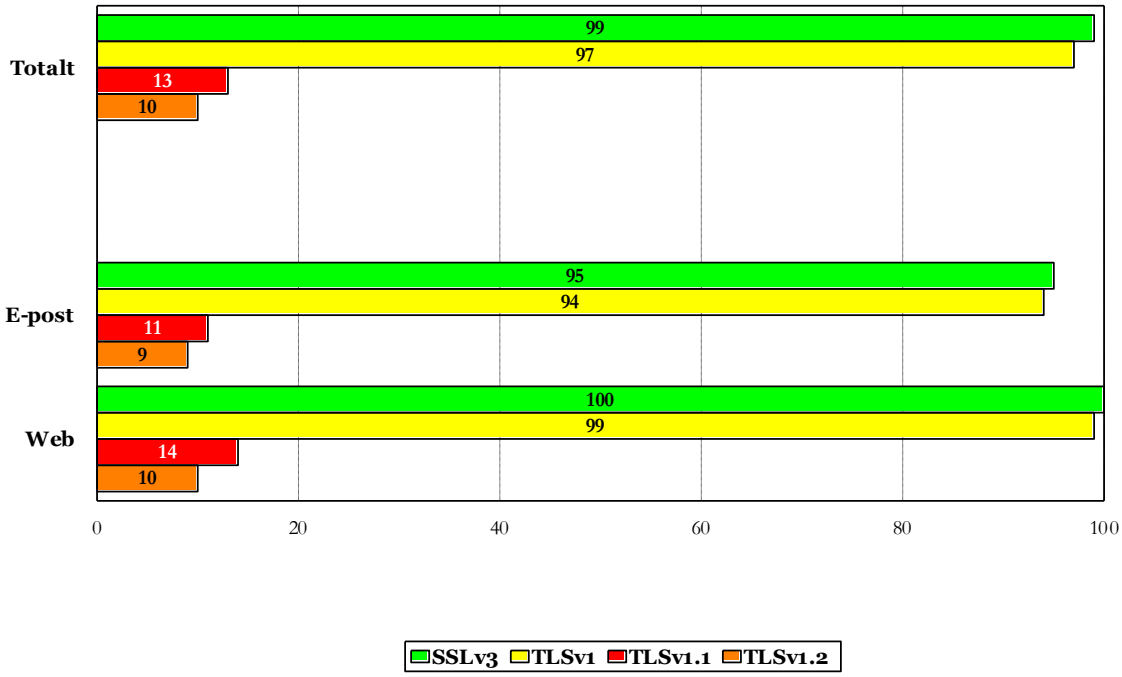
43 procent av webbplatserna svarar med innehåll över HTTPS.

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

10.5.8 Protokollversioner

Protokoll för skydd på transportnivå förekommer i flera olika versioner, men bör realiseras genom användning TLSv1 eller ekvivalent metod. Följande diagram redovisar fördelningen av använda protokollversioner hos de domäner i undersökningen som har certifikat för transportskydd.

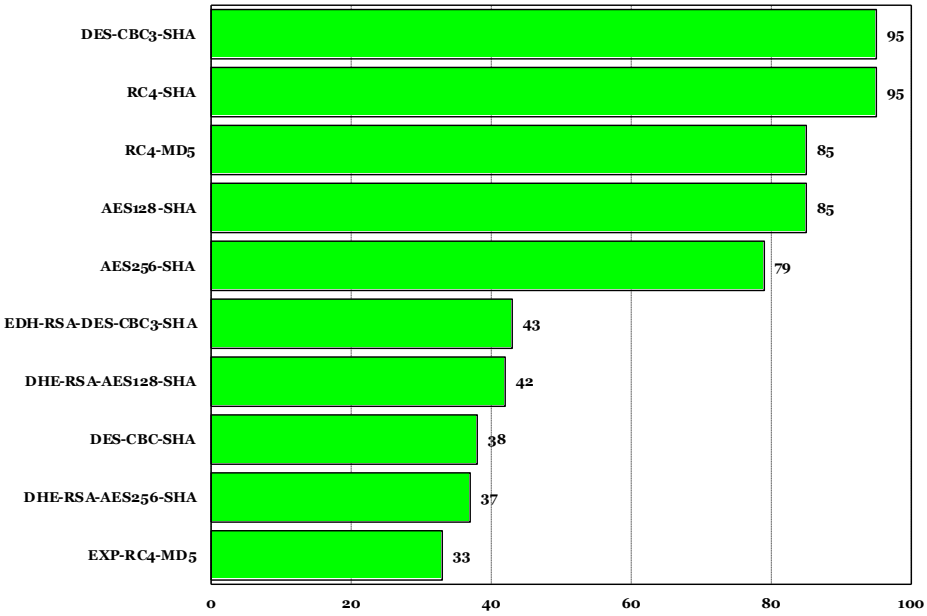
Diagram 24: Protokollversioner.



10.5.9 Vanliga krypteringsalgoritmer

Transportnivåskydd kan åstadkommas med någon ur en stor uppsättning algoritmer för identifiering, kryptering och återuppspelningsskydd. De vanligast förekommande algoritmerna i den aktuella undersökningsgruppen framgår av följande diagram.

Diagram 25: Krypteringsalgoritmer.



RC4 har länge ansetts lida av en del problem. Många av dessa problem är numera hanterade på klientsidan (till exempel i webbläsare) och RC4 har trots problemen fortsatt att vara populär, kanske framför allt på grund av sin goda prestanda. Vissa påstår att RC4 står för så stor andel som drygt 50 procent av all TLS-trafik[21].

10.6 Sammanfattning av resultat

Av de 1 648 servrar som kan kommunicera krypterat med TLS hade 64 procent korrekta certifikat. Bland övriga 36 procent hittar vi följande felaktigheter:

- 9 procent har certifikat utställda på fel tjänst.
- 23 procent har självsignerade certifikat.
- 4 procent har certifikat som är ogiltiga på grund av att de inte har förnyats inom giltighetstiden.

Det är dessutom stor sannolikhet att de domäner som inte har korrekta certifikat har mer än ett problem.

Vi kunde bland de servrar som hade godkända certifikat endast hitta 7 procent med EV-certifikat (Extended validation).

[21] https://community.qualys.com/blogs/securitylabs/2013/03/19/rc4-in-tls-is-broken-now-what

Ett par certifikat är konfigurerade med relativt korta RSA-nycklar, 1024 bitar, medan den vanligaste nyckellängden idag är 2048 och i vissa enstaka fall även 4096 bitar.

En mycket stor andel servrar använder sig av så kallade wild card-certifikat (83 procent för e-post och 58 procent för webb).

Hanteringen av certifikat i undersökningsgruppens IT-miljö håller alltså fortfarande 2013 mycket låg kvalitet i alla avseenden som undersökningen visar.

Denna typ av kryptoanvändning har ändå funnits länge och är tämligen vanlig. Hos de organisationer som ingår i undersökningen måste man kunna förvänta sig bättre resultat, framför allt att de ska ha giltiga, aktuella certifikat utgivna av betrodda utgivare. Vad vi vill få sagt med denna del av undersökningen är att en bristfällig användning av webbcertifikat undergräver trovärdigheten av denna typ av säkerhetslösningar.

Allt som innebär att en användare måste klicka på knappar som i praktiken innebär ”Ja, jag vet att det inte stämmer, men ta mig vidare ändå”, såsom självsignerade certifikat, certifikat utfärdade av en icke-betrodd CA eller certifikat vars giltighetstid har gått ut gör att det inarbetas en dålig säkerhetskultur hos internetanvändare vilket i sin tur motverkar själva grundidén med servercertifikat – nämligen att säkert veta att man med sin klientprogramvara står i förbindelse med rätt server (se bilaga 9).

10.7 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 förstå hur SSL är infört och 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.

10.8 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, och 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.

10.8.1 DNS-baserad autentisering av namngivna enheter

Det är många som funderar på lösningar, och 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[22].

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.

10.8.2 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)[23], 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.

[22] http://tools.ietf.org/html/rfc6698
[23] http://tools.ietf.org/html/rfc6797

10.8.3 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.

Resultatet från vår undersökning visar att 86 procent av e-postservrarna och 69 procent av webbservrarna stödjer PFS.

10.8.4 Andra initiativ

Webbläsaren Chrome innehåller många utökningar, bland annat *certificate pinning*[24] som var det som avslöjade en av CA-attackerna, den mot DigiNotar. Arbete inom det området pågår även inom IETF[25].

Andra utökningar i Chrome är *HTTPS-preloading*[26] 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*[27] som utvecklats gemensamt av Electronic Frontier Foundation (EFF) och Tor-projektet.

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

11 Råd och rekommendationer

Efter att 2013 ha genomfört ännu en omgång mätningar med ett relativt positivt resultat jämfört med 2012 ser vi trots allt fortfarande ett behov av större samordning mellan olika intressenter för bättre säkerhet och nåbarhet på den svenska delen av internet och inte minst ser vi möjligheter till stora effektivitetsvinster och kostnadsbesparingar.

I första hand verksamheterna inom den offentliga förvaltningen måste kunna enas om relevanta upphandlingskrav men även om rekommendationer och en handlingsplan för genomförandet av några viktiga aktiviteter:

- Kritiska resurser i Sverige bör ha namnservrar som är anslutna till flera operatörer samtidigt, till exempel med användning av tekniken Anycast. Leverantörer som erbjuder sådana tjänster med god kvalitet är en bristvara. Det finns behov av att någon på central nivå bestämmer vad som är att betrakta som en kritisk resurs.

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

- Inför gemensamt upphandlade funktioner för virustvätt och rensning av skräppost med krav på servrar placerade i landet. Det skulle bli effektivare, förmodligen spara resurser och göra det enklare att göra revision. Samtidigt skulle det förhindra att myndighetsinformation lämnar landet.

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

- Utfärda rekommendation om att e-postservrar hos svenska myndigheter, för kritiska verksamheter med känslig information fysiskt ska 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 användning av både e-post och webb med TLS för käll- och transportskydd.

- Göra samtliga tjänster tillgängliga över IPv6 och planera omgående för ett systematiskt införande av IPv6 inom hela den offentliga förvaltningen.

- Skydda webbservrar med certifikat som är utfärdade av allmänt accepterade certifikatutfärdare och ha kontroll över deras giltighet. Helst bör det finnas en svensk sådan aktör.

- Införa DNSSEC på alla domäner i den offentliga förvaltningen.

Utöver ovanstående åtgärder finns det ytterligare åtgärder som behöver vidtas bland annat på operatörsnivå för att stärka infrastrukturen för internet. Dessa åtgärder landar huvudsakligen på Post- och Telestyrelsen, PTS, som är den

myndighet som är tillsynsansvarig för bland annat lagen om elektronisk kommunikation, och här handlar det om att formulera krav som bör ställas på operatörer.

Regeringen har föreslagit att det senast 2013 ska finnas en gemensam internetspecifikation med olika robust- och säkerhetskrav (typfall) framtagen för myndigheter. Vidare har regeringen föreslagit att alla myndigheter senast 2013 bör använda sig av DNSSEC och vara nåbara med IPv6. Vad vi kan se har inte något av dessa mål uppfyllts ännu, men det ser ljusare ut för både DNSSEC och IPv6 i år, än det gjort tidigare år.

Bilaga 1 - Förkortningar och ordförklaringar

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

BCP Best Common Practice, branschstandard.

CRL Certificate Revocation List (spärrlista).

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

DKIM Domain Keys Identified Mail. DKIM gör det möjligt för e-postservrar att skicka och ta emot elektroniskt signerad e-post.

DNS Domain Name System. En internationell hierarkiskt uppbyggd distribuerad databas som används för att hitta information om tilldelade *domännamn* på internet. Domännamnssystemet är det system som översätter domännamn (till exempel iis.se) till IP-adress vilken används för kommunikation över IP-nät som till exempel internet.

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

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

DNS-server Se *Namnserver*.

Domän Beteckning på en nivå i domännamnssystemet.

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

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

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

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

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

Namnserveroperatör Den som tillhandahåller en *DNS-funktion* för internetanvändare.

OCSP	Online Certificate Status Protocol.
Registrar	Ackrediterad återförsäljare av .SE-domäner.
Resolver	Den programvara som översätter namn till *IP-adresser* eller tvärtom.
SOA	Start of Authority, en pekare till var information om en zon börjar.
TLS/SSL	SSL är en standard för kryptering av bland annat webbtrafik under transport. Kommunikation med http med SSL kallas https. Ersätts numera av IETF:s öppna standard TLS.
TLSA	The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA
Zon	Avgränsning av det administrativa ansvaret för domännamnsträdet. En *zon* utgörs av en sammanhängande del av domännamnsträdet som administreras av en organisation och lagras på dess *namnservrar*.
Zonfil	Datafil där 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 skall härvid prioritera områden som ökar effektiviteten i infrastrukturen för elektronisk datakommunikation, varvid stiftelsen bland annat skall sprida information om forsknings- och utvecklingsarbete, initiera och genomföra forsknings- och utvecklingsprojekt samt genomföra kvalificerade utredningar”. Säker och robust internetinfrastruktur är ett mycket viktigt och centralt område för oss.

Det stora intresse som har visats för resultaten från tidigare års undersökningar och det faktum att vi kan konstatera att trenden är en förbättring över tid övertygar oss på .SE att det finns ett värde av undersökningen och vi kommer att fortsätta genomföra den, i år gör vi den för sjunde gången. Undersökningen ingår i ett långsiktigt projekt som går under namnet Internets ekosystem och omfattar fler områden och mätningar.

.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 30 år på nacken och som 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 validering av signaturer av svaren på DNS-frågor går det att säkerställa att dessa verkligen kommer från rätt källa och inte har ändrats under överföringen.

.SE:s lansering 2005 av tjänsten DNSSEC för säkrare DNS har också bidragit till att ett ökat fokus hamnat på DNS och DNS-drift. Den som har för avsikt att göra sin DNS-infrastruktur säkrare genom att använda DNSSEC inser tämligen

snabbt att införandet inte låter sig göras med mindre än att det först görs en översyn av den egna DNS-infrastrukturen som helhet.

Därför är vi givetvis intresserade av att ta reda på hur väl förberedda domäner i .se är för DNSSEC. Det - och det faktum att vi 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 godkänner ett stort antal nya toppdomäner med start 2013 som har som obligatoriskt krav att de ska vara signerade med DNSSEC ökar spridningen 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 samlas kring Internet Protocol som förkortas IP. Dagens internet domineras fortfarande av IPv4 (IP version 4), som togs fram redan 1981.

De så kallade IP-adresserna, det vill säga den unika nummerserie som identifierar varje uppkopplad enhet på internet, består i IPv4-versionen av 32 bitar. Därför kan det med IPv4 bara finnas drygt fyra miljarder unika IP-adresser. I takt med att världen blir alltmer uppkopplad uppstår det helt enkelt adressbrist på internet. De sista IPv4-adresserna delades ut under 2010.

Lösningen för att komma till rätta med adressbristen är att införa en ny version av protokollet, IPv6, med 128 bitar långa adresser. Det råder ingen som helst tvekan om att dessa IP-adresser kommer att räcka och bli över under lång tid framöver när övergången till IPv6 väl har genomförts. Från att det med IPv4 inte ens finns en IP-adress per person i världen, skulle varje nu levande individ kunna få 5×10^{28} adresser var med IPv6. Var och en skulle alltså kunna få 50 000 000 000 000 000 000 000 000 000 egna IP-adresser att förfoga över. En riklig tillgång till IP-adresser öppnar också upp för applikationer som annars blir svåra att förverkliga i praktiken till exempel Internet of Things (ungefär Sakernas internet) och intelligenta hem.

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

Tjänster för e-post och webb

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

Verktyget MailCheck syftar till att förbättra kvaliteten på e-postrelaterade tjänster generellt genom att peka ut möjliga konfigurationsproblem, svagheter i

programvaror eller avvikelser från standarder för både systemadministratörer och slutanvändare.

Bilaga 2 - Om .SE:s testverktyg

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

DNSCheck finns tillgängligt för användning via ett webbgränssnitt på http://dnscheck.iis.se. Källkoden till bland annat plattformen Hälsoläget och verktyget DNSCheck finns på http://github.com/dotse/.

Där finns även ett verktyg som enbart tittar på mer detaljer för DNSSEC-signerade domäner. Det verktyget finns att hämta på https://github.com/dotse/dnssec-analysis.

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

Det senaste tillskottet till verktygslådan har utvecklats under arbetsnamnet Pyssla, Python SSL Analyzer. Det är en vidareutveckling av SSLyze, som är ett Python-verktyg för analys av SSL-konfiguration på en server genom att ansluta till den. Det är designat för att vara snabbt och utförligt, och bör kunna bistå den som använder verktyget att hitta felkonfigurationer som negativt påverkar deras SSL-servrar. Källkoden finns tillgänglig på https://github.com/kirei/sslyze.

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.

Bilaga 3 – 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 minskar 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*[28]), och trenden är att behovet av TCP ökar då nya protokoll som IPv6 och DNSSEC leder till att det används i större omfattning än tidigare. Felet är en indikation på att den som har konfigurerat namnserver eller brandvägg inte har tillräckligt aktuella kunskaper om DNS.

- Verksamheten har ingen konsekvent namnserveruppsättning. 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 huvudtaget, och då ligger felet sannolikt någon annanstans, till exempel i förbindelsen till namnservern eller att servern inte har en korrekt angiven IP-adress. Våra tester på namnservern avslutas direkt om båda dessa tillstånd har konstaterats.

[28] 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 4 - Branschstandard för DNS-tjänst med kvalitet

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

Verktyget DNSCheck kan även utföra så kallade odelegerade domäntester. Ett odelegerat domäntest är ett test som genomförs på en domän som kan (men inte måste) vara fullständigt publicerad i DNS. Funktionen är mycket användbar för den som till exempel tänker flytta en domän från en namnserveroperatör till en annan. Låt oss ta som exempel att domänen exempel.se ska flyttas från namnservern 'ns.nic.se' till namnservern 'ns.iis.se'. I detta fall kan man genomföra ett odelegerat domäntest på domänen (exempel.se) med den namnservern domänen ska flyttas till (ns.iis.se) INNAN själva flytten genomförs. När testet visar grönt är det tämligen säkert att den nya hemvisten för domänen åtminstone vet att den ska svara på frågor om domänen. Det kan emellertid fortfarande finnas fel i zoninformationen som detta test inte känner till.

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

http://dnscheck.iis.se/

1. Minst två namnservrar

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

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

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

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

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

Förklaring: I den överliggande zonen används NS-poster för att överlåta ansvaret för (delegera) en viss domän till andra servrar. Denna lista av datorer ska enligt DNS-dokumentationen finnas införd även i den zonfil som "tar emot" ansvaret, och som innehåller övriga data om zonen. Listorna måste hållas synkroniserade, så att alla NS-poster som förekommer i föräldrazonen också återfinns i barnzonen. Listan i föräldrazonen uppdateras inte automatiskt, utan

endast efter "manuell" anmälan till ansvarig registreringsenhet. Vid förändring som leder till behov av ändring i överliggande zon ska underliggande zons administrativa kontaktperson utan dröjsmål se till att registreringsenheten meddelas om detta.

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

3. Auktoritet

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

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

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

4. Serienummer för zonfil

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

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

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

5. Kontaktadress

Rekommendation: Zonkontaktadressen i SOA-posten ska vara nåbar.

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

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

6. Nåbarhet

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

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

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

Bilaga 5 – Mer information om DNSSEC

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

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

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

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

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

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

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

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

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

DNSSEC används för att säkra DNS från missbruk och man-in-the-middle-attacker som cacheförgiftning. .SE har under flera år varit en pådrivande kraft för att införa och sprida DNSSEC.

Vad DNSSEC skyddar mot

DNSSEC säkerställer innehållet i DNS med hjälp av kryptografiska metoder som använder elektroniska signaturer. DNSSEC innebär att användaren, när han gör en uppslagning i DNS, genom validering av signaturer ska kunna avgöra om informationen som kommer tillbaka som svar kommer från rätt källa och om

den har manipulerats på vägen. Det blir alltså svårt att förfalska information i DNS som är signerad med DNSSEC utan att det upptäcks.

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

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

Vad DNSSEC inte skyddar mot

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

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

.SE:s roll i DNSSEC

Många har väntat på att rotzonen, det vi säga föräldrazonen till .se, ska bli signerad och 2010 blev detta verklighet. Fram till dess har det varit .SE som haft ansvaret för att dels signera .SE:s zonfil, dels utgöra ett *trust anchor* i kedjan för den svenska delen av internet. Ett *trust anchor* signerar de underliggande zonernas nycklar och fungerar som startpunkt i verifieringskedjan. Signeringen består av att .SE tar hand om och verifierar de underliggande zonernas DS-poster. Det är jämförbart med hanteringen av NS-poster i DNS.

.SE kommer fortfarande att signera .SE:s zonfil, men genom att .SE publicerar sina DNSSEC-nycklar i rotzonen är det numera rot som utgör *trust anchor* för internet. Detta underlättar för alla resolveroperatörer som annars blir tvungna att hålla reda på alla nycklar för alla signerade toppdomäner som är *trust anchor* för sina respektive underliggande domäner. Med roten signerad behöver resolveroperatören bara hålla reda på rotnyckeln. Moderna standarder erbjuder dessutom enklare hantering av nyckelbyten och nya verktyg har tagits fram för att underlätta (se nedan om Open DNSSEC).

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

Här finns några pekare till ytterligare information:

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

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

En uppdatering har också skett av tidigare RFC 4641 som numera heter RFC 6781[29] som även den tar sikte på det praktiska införandet av DNS och DNSSEC.

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 till idag, och med en framtidsbild baserad på publicerade och uttalade planer om den framtida utvecklingen från olika toppdomäner.

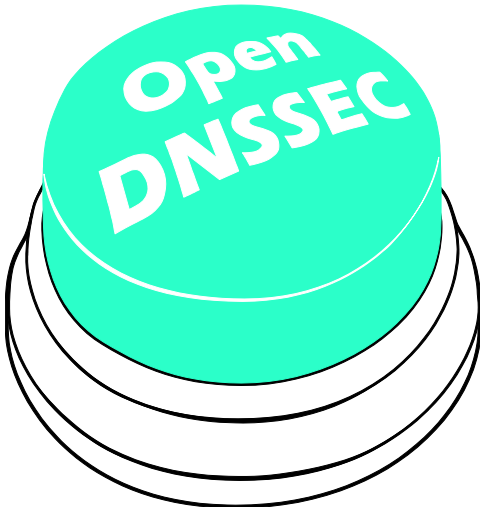
Dnssec-deployment har en e-postlista som vem som helst kan prenumerera på, ställa frågor och hålla sig uppdaterad om utvecklingen på området.

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

OpenDNSSEC

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

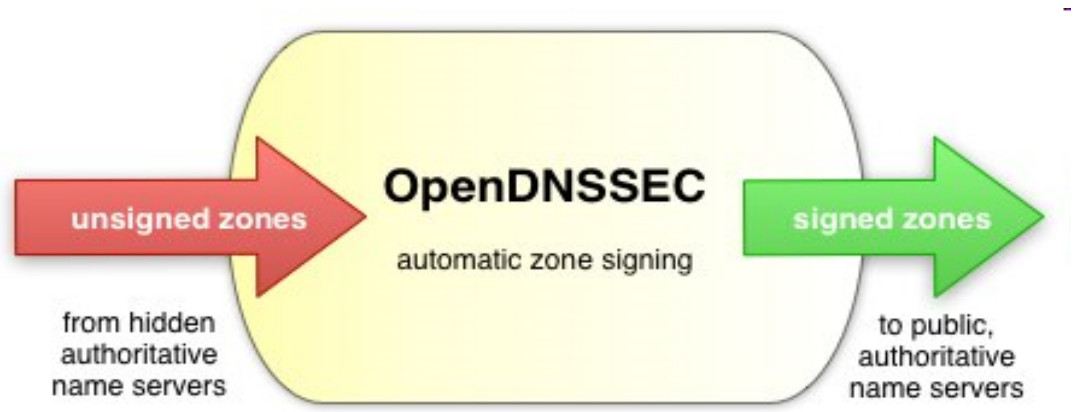
Efter att .SE noterat att bristen på bra och tillgängliga verktyg på marknaden för signering av zonfiler med DNSSEC var ett hinder för många att inleda införandet av DNSSEC påbörjades ett utvecklingsprojekt tillsammans med några av de främsta utvecklarna på området. Resultatet är OpenDNSSEC som är en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



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

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

[29] http://tools.ietf.org/search/rfc6781/



OpenDNSSEC utvecklas inom ett separat bolag som ägs av .SE (Stiftelsen för Internetinfrastruktur).

Programvaran OpenDNSSEC är resultatet av ett samarbete mellan utvecklare från .SE, Nominet, NLNet Labs, SIDN, SURFnet, Kirei AB och Sinodun. Mer information finns på http://www.opendnssec.org/

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

Bilaga 6 - Öppna rekursiva namnservrar

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

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

Grundproblemet är egentligen inte öppna rekursiva namnservrar, utan att operatörerna inte filtrerar trafik på avsändaradresser. Om de gjorde det skulle öppna rekursiva resolvrar kanske inte betraktas som ett problem. Då sådan filtrering är relativt svår och kostsam att införa för operatörerna vilket gör att de drar sig för att genomföra detta, behöver vi under tiden försöka begränsa de skador som DDOS-attacker orsakar tills dess att operatörerna har åtgärdat grundproblemet. Att stänga en rekursiv resolver är en relativt enkel uppgift som det är värt mödan att göra då det hjälper till att lindra de problem som uppstår vid DDOS-attacker.

Pekare till mer information

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

Secure Domain Name System (DNS) Deployment Guide
http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf

DNS Amplification attacks
En bra beskrivning av hur attacken går till och vad den innebär.
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 detaljerad beskrivning av funktioner i BIND.
https://kb.isc.org/article/AA-00845/0/BIND-9.9-Administrator-Reference-Manual-ARM.html

Bilaga 7 - 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[30]. I korthet definierar RFC:n en posttyp som kan annonsera huruvida en domän signerar sin utgående e-post och hur andra servrar kan komma åt och tolka den informationen.

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

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

SPF

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

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

[30] 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 på http://tools.ietf.org/html/rfc6652.

Bilaga 8 - Åtgärder för transportskydd

Elektronisk post

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

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

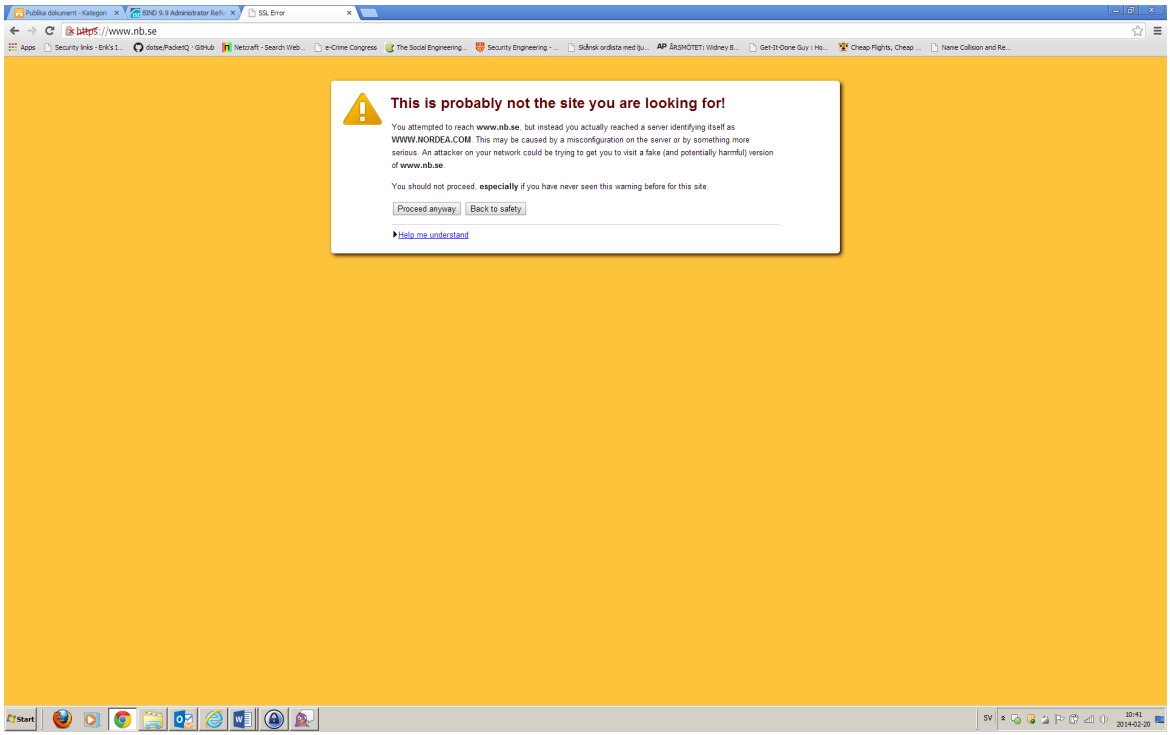
Webbtrafik

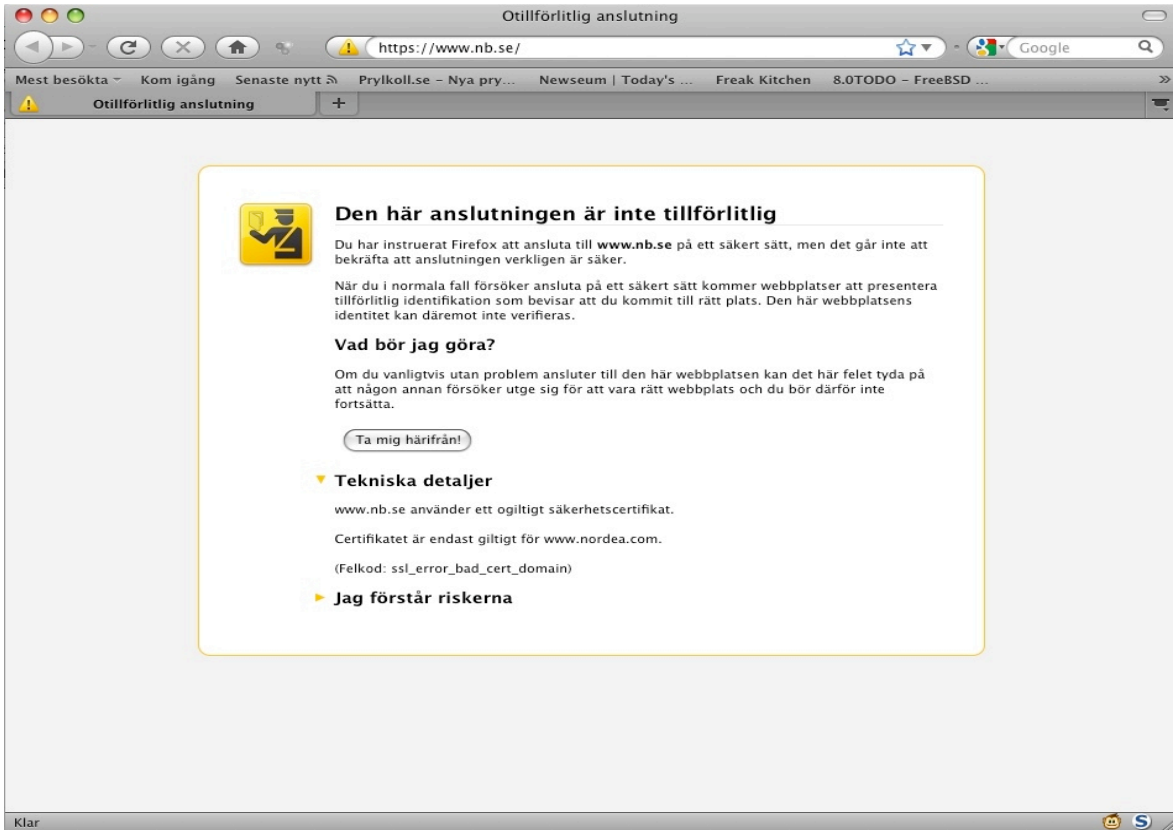
För en användare som exempelvis vill komma i kontakt med en svensk myndighet eller bank är det viktigt att veta att den server man har kontakt med är rätt server, att anslutningen av någon anledning inte har skett till fel tjänst eller server på grund av felkonfiguration eller medvetet bedrägeriförsök.

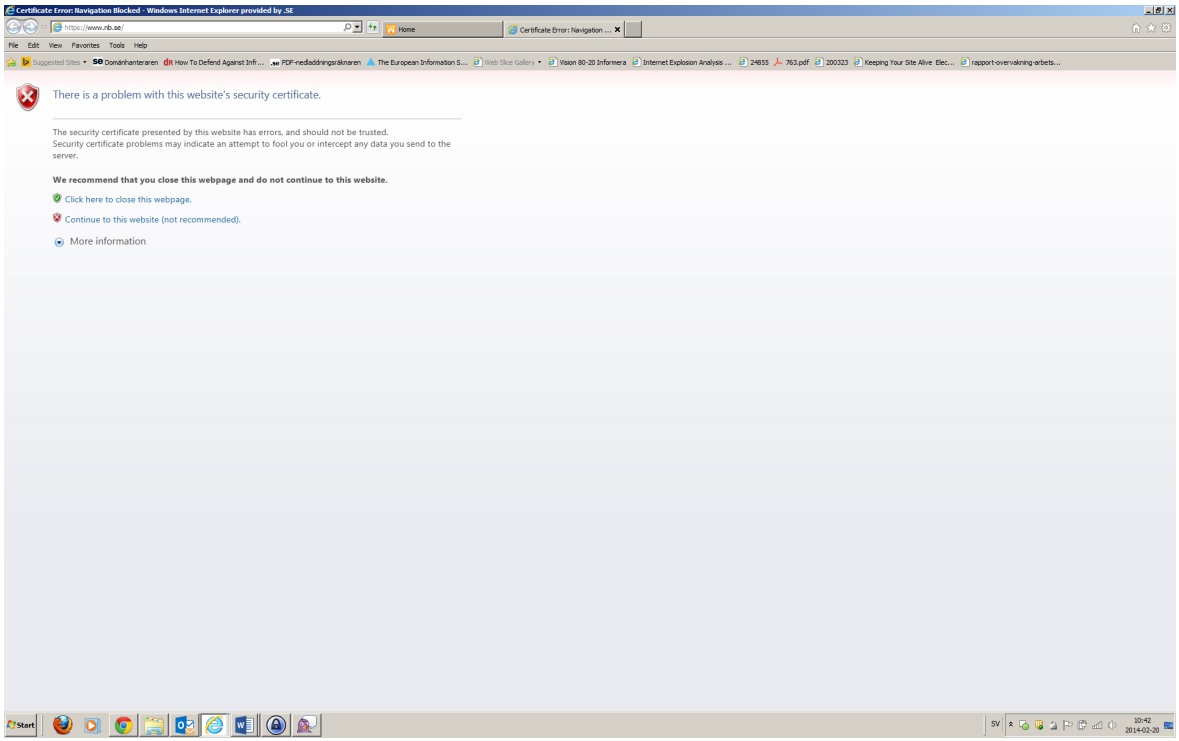
En av de tekniker som används även för detta är Transport Layer Security (TLS). TLS/SSL ger användarna möjlighet att kontrollera att man hamnat hos rätt server eller tjänst.

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, det kan 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

.SE (Stiftelsen för Internetinfrastruktur) är en oberoende allmännyttig organisation som ansvarar för Internets svenska toppdomän .se. Vi har hand om administrationen och driften av alla de över en miljon domännamn på Internet som slutar på .se. Vårt överskott går till fortsatt utveckling av Internet i Sverige genom en rad olika satsningar som på olika sätt bidrar till utvecklingen och användningen av Internet.

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

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

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

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

.se
Vi driver Internet framåt