POST & TELESTYRELSEN

DATUM
7 februari 2007

DIARIENR
06-14081/59

Tillsyn av den nationella toppdomänen för Sverige på Internet

Promemoria efter genomförd tillsyn

Innehåll

Bilagor

Sammanfattning

Post- och telestyrelsen, PTS, är sektorsmyndighet för området elektronisk kommunikation. Sedan den 1 juli 2006 har PTS uppgiften att utöva tillsyn enligt lagen (2006:24) om nationella toppdomäner för Sverige på Internet, toppdomänslagen.

I toppdomänslagen finns bland annat bestämmelser som reglerar vad som gäller för teknisk drift av nationella toppdomäner för Sverige på Internet. Lagen omfattar den som administrerar nationella toppdomäner som avser Sverige. För närvarande finns en aktör, Stiftelsen för Internetinfrastruktur, .SE.

PTS har under hösten 2006 genomfört ett tillsynsarbete genom informationsinsamling där det har ställts frågor till administratören för den nationella toppdomänen .se. Syftet har varit att bedöma om .SE i nuläget bedriver sin verksamhet på ett säkert och effektivt sätt i allmänhetens intresse och att domännamn, IP-adresser och övriga registeruppgifter är korrekta och tillförlitliga. Enkäten har främst utformats för att kontrollera efterlevnaden av toppdomänslagens 5 och 6 §§. Tillsynsenkäten har kompletterats med ett besök hos .SE.

Vid analys av enkätsvaren och lagens bestämmelser har det framkommit att .SE i huvudsak bedriver verksamheten på ett säkert och effektivt sätt i allmänhetens intresse. Det fysiska och logiska skyddet säkerställer en fungerande trafik och ger ett effektivt skydd av uppgifterna i toppdomänen. Registerföring sker på ett säkert och integritetsskyddat sätt. .SE ställer krav på namnserveroperatörer och sina domännamnsåterförsäljare, så kallade ombud. .SE har också visat upp en beredskap för krissituationer och en tillfredställande nivå på sitt informationssäkerhetsarbete. .SE kommer under 2007 att genomföra en krisövning, vilket PTS anser är en förutsättning för en tillförlitlig krishanteringsplan.

PTS har funnit anledning att påpeka att .SE:s rutiner för åtkomst till att utföra ändringar i den databas som innehåller domännamn bör ses över. Kompetensförsörjning, att verksamheten inte är personberoende och kontroll av personal med nyckelfunktioner är ytterligare viktigt att se över. Näringsdepartementet och .SE arbetar för närvarande med ett avtal som reglerar hur en domänadministratör utses eller hur dennes verksamhet ska upphöra. Anledningen är att toppdomänslagen lämnar frågan oreglerad. PTS vill, trots att domänadministratören arbetar med att bygga upp en redundant domänadministration, understryka vikten att ett avtal kommer till stånd. Ett sådant avtal skall garantera att en fortsatt stabil infrastruktur för Internet i Sverige kan upprätthållas om .SE slutar administrera toppdomänen .se.

Iakttagelserna vid tillsynen har inte gett PTS anledning att för närvarande förslå ytterligare åtgärder från domänadministratörens sida på de områden som nu varit föremål för tillsyn.

1 Inledning

PTS är sektorsmyndighet för området elektronisk kommunikation vilket bland annat inkluderar Internet och dess domännamnssystem, DNS. PTS skall sedan den 1 juli 2006 utöva tillsyn av den nationella toppdomänen enligt toppdomänslagen.

Syftet med lagen är att ge staten en möjlighet till insyn och tillsyn över domänadministrationen för att förhindra eventuella brister i domännamnstjänsten (DNS-tjänsten) och se till att den som har ansvaret för .se-zonen kan tillhandahålla tillfredsställande tillgänglighet, kvalitet och säkerhet. Toppdomänslagen innehåller bland annat krav på teknisk drift och förande av register samt övergripande regler när det gäller domänadministratörens regler för tilldelning av domännamn och tvistlösningsförfarande.

Då Internet idag är en samhällskritisk infrastruktur ligger det i nationens och allmänhetens intresse att den svenska domännamnsdriften sköts på ett effektivt och säkert sätt. Utan en fungerande drift av den svenska toppdomänen skulle Internet, som tillhör .se-domänen, inte fungera.

PTS bedriver tillsyn antingen som en planlagd aktivitet, ofta av tematisk karaktär, eller en händelsestyrd tillsyn av mer akut karaktär.

PTS har under hösten 2006 genomfört ett tematiskt tillsynsarbete gentemot .SE genom informationsinsamling där det ställts frågor om teknisk drift, förande av register och informationssäkerhetsarbete m.m. Denna promemoria beskriver svaren och PTS bedömning.

1.1 Syfte

Syftet med tillsynsarbetet är att kontrollera att lagens krav efterlevs, d.v.s. att .SE bedriver en säker teknisk drift av den nationella toppdomänen där domännamn och IP-adresser i .se-zonen är korrekta och tillförlitliga. Syftet är vidare att i denna promemoria ge en nulägesbild av domänadministrationen i Sverige.

1.2 Metod

Tillsynen har genomförts genom att en enkät har skickats till .SE, se bilaga 3. Enkäten har tagits fram utifrån de krav som ställs i 5 och 6 §§ toppdomänslagen. Härutöver har PTS som ett led i tillsynen och som komplement till nämnda enkät besökt .SE. Vid besöket redogjorde .SE bland annat mer ingående för fysiskt och logiskt skydd, krav på sekundära namnserveroperatörer och förevisade en kontinuitetsplan.

1.3 Tillsynens omfattning och avgränsning

PTS har begränsat tillsynen till att avse de krav som ställs i toppdomänslagen på att namnserverdriften för .se-zonen tekniskt sköts på ett säkert och effektivt sätt och att registerföring sker på ett säkert och integritetsskyddat sätt, 5 och 6 §§ toppdomänslagen.

Tillsynen omfattar följande områden:

- namnservrarnas tekniska lösning, reservkapacitet och skydd (3.1),
- zonfilens tillkomst, distribution och korrekthet (autenticitet) (3.2 och 3.4),
- .SE:s driftsorganisation och övervakningssystem (3.3),
- registerföring (3.5),
- uppdateringar av mjuk- och hårdvara (3.6),
- kontinuitetsplan (3.7),
- informationssäkerhet (3.8); och
- beredskap för möjliga framtida hot och attacker (3.9).

Bestämmelserna om tilldelning av domännamn och tvistlösning, 7 §, och om överföring av uppgifter till tillsynsmyndigheten, 8 §, har inte behandlats vid tillsynen.

1.4 Promemorians disposition

Promemorian inleds med en beskrivning av de bestämmelser i toppdomänslagen som rör teknisk drift, förande av register och informationssäkerhet (kap. 2). Därefter följer en närmare genomgång av enkäten i de delar som är centrala för att avgöra om domänadministrationen sköts på ett säkert och effektivt sätt. I samband med enkätgenomgången analyseras om toppdomänslagens krav kan anses vara uppfyllda (kap. 3). Promemorian avslutas med samlade slutsatser och en kommentar om fortsatt arbete (kap. 4).

I bilagor till promemorian återfinns ordförklaringar (bilaga 1), en kort bakgrundsbeskrivning till domännamnssystemet (bilaga 2) och den enkät som ligger till grund för tillsynen (bilaga 3).

2 Bestämmelser på området

I toppdomänslagen finns bestämmelser som reglerar vad som gäller för teknisk drift av nationella toppdomäner för Sverige på Internet och förande av register. Det finns också övergripande bestämmelser om tilldelning och registrering av domännamn.

Syftet med bestämmelserna är att ge staten en möjlighet att säkerställa en effektiv och säker administration av toppdomänen för Sverige genom insyn och tillsyn.

Av bestämmelsen i **1 § toppdomänslagen** framgår att lagens tillämpningsområde är begränsat till nationella toppdomäner som avser Sverige. När det gäller domänadministratörens återförsäljare (ombud) som utför registreringen åt privatpersoner och affärsidkare som önskar få ett domännamn registrerat under toppdomänen .se förutsätts deras förhållande till domänadministratören regleras genom privaträttsliga överenskommelser (prop. 2004/05:175 s. 240 f.). I förarbetena har det vidare inte ansetts finnas skäl att föreslå särskilda regler om ombud.

I **5 § toppdomänslagen** ställs krav på att verksamheten, domänadministrationen, i alla delar skall utföras på ett säkert och effektivt sätt i allmänhetens intresse. I säkerhetskravet ligger bland annat kapacitet att motstå driftsstörningar till följd av fysiska och logiska hot liksom personell kompetens hos driftsorganisationen. Verksamheten skall förutom att vara driftssäker också tillgodose ett gott integritetsskydd.

I prop. 2004/05:175 s. 246 f behandlas kraven på domänadministratören. Det som behöver säkerställas är att DNS-funktionen, dvs. den funktion som tillhandahåller information från DNS på begäran av användaren (t.ex. vilken IP-adress som motsvarar ett visst domännamn), har tillfredställande tillgänglighet och säkerhet. Informationen i toppdomänens namnserver det vill säga den så kallade zonfilen för den nationella toppdomänen, som är den datafil som motsvarar den del av namnrymden i DNS, som .SE ansvarar för skall vara korrekt, hållas uppdaterad och vara tillgänglig på ett tillfredställande sätt med för ändamålet anpassad anslutning till Internet. Detta gäller även namnservrar som tillhandahåller registreringsuppgifter i den så kallade WHOIS-databasen.

Härutöver bör den administrativt ansvarige se till att alla DNS-data är tillräckligt skyddade mot skada, manipulation eller förlust enligt bästa rimliga teknik. Det bör också finnas beredskap för att stå emot plötslig trafikökning, olika störningar och attacker.

Bestämmelsen pekar på att personalens kompetens är en nyckelfråga och det krävs klara rutiner för verksamheten och en organisation som klarar av de krav som administration av toppdomänen kräver.

För en globalt fungerande och effektiv Internetanvändning krävs dessutom att de system och den utrustning som används är kompatibla med varandra. Domänadministratören ska därför, enligt bestämmelsen, vara skyldig att följa

erkända standarder på området, exempelvis den standardisering som sker inom Internet Engineering Task Force, IETF.

Bestämmelser om register finns i **6 § toppdomänslagen**. Bestämmelsen innebär att domänadministratören ska föra ett register över domännamn under toppdomänen med bland annat kontaktinformation om domännamnsinnehavaren och löpande upprätta säkerhetskopior av registeruppgifter. Möjligheten att kunna söka i ett korrekt och tillförlitligt register är betydelsefull av flera anledningar. Ur teknisk synvinkel fyller tjänsten en viktig funktion, exempelvis för att komma i kontakt med ansvariga för datorer som sprider virus. Ett offentligt register har också betydelse ur ett konsument- och näringslivsperspektiv när det används för att kontrollera vem som innehar ett domännamn vid elektronisk handel eller när ett immaterialrättsligt intrång begåtts. Uppgifterna i registret ska kunna hämtas av allmänheten utan avgift via Internet.

3 Enkätgenomgång och analys av de inkomna svaren

Enkäten omfattar de områden som är relevanta för att kunna bedöma säkerhet och effektivitet i den tekniska driften och administrationen av domännamnssystemet i .se-zonen. De relevanta områdena är namnservrarnas tekniska lösning, redundans, reservkapacitet och skydd. Vidare, hur korrekthet (äkthet) av data i databaser och zonfilen upprätthålls. Härutöver är .SE:s driftsorganisation, ansvarsfördelning mellan .SE och sekundära namnserveroperatörer, övervakningssystem, registerföring, kontinuitetsplanering samt informationssäkerhet relevanta områden att studera.

Nedan redogörs för domänadministratörens svar på enkätens frågor, se nedan *.SE:s beskrivning*. Därpå följer PTS analys och bedömning, se nedan *PTS bedömning*.

3.1 DNS-tjänstens tillgänglighet och säkerhet

.SE:s beskrivning

Domännamnssystemet för .se-zonen utgörs idag (2006) av en masterserver, två distributionspunkter och ett större antal sekundära namnservrar. De sekundära namnservrarna är inte enbart placerade i Sverige utan finns även i ett tjugotal länder världen över. Namnservrarna i Sverige är även de många till antalet, utspridda på ett flertal ställen i landet och fysiskt skyddade. Kraven på skydd är utformade i enlighet med Ledningssystem Informationssäkerhet, LIS. Skyddet innefattar skalskydd, tillträdeskontroll, skydd och utrustning, miljö, reservkraftförsörjning och kabelskydd. För en del av de sekundära namnservrarna i .se-zonen används adresseringsmetoden ”anycast” för att minska konsekvenserna av en oväntat och tillfälligt hög trafikbelastning på en namnserver.

De förbindelser som finns från namnservrarna till Internet är också skyddade, åtminstone fram till distributionspunkterna där respektive namnserveroperatörs ansvar vidtar. Förbindelser från masterservern till distributionspunkterna är kanaliserade samt dubblerade. Kabelskydd, för att skydda kabel mot skadlig påverkan, finns inom respektive fastighetsnät.

Om en sekundär namnservers ena förbindelse till Internet skulle gå förlorad, exempelvis på grund av att ett anslutande nät är otillgängligt, finns ytterligare en förbindelse till en annan operatörs nät för att säkerställa tillgängligheten till domännamnstjänsten.

Vidare är .SE inte den enda organisation som sköter den tekniska driften av namnservrarna för .se-zonen. .SE ger också uppdrag åt andra aktörer att sköta den tekniska driften av zonfilskopior i syfte att upprätthålla säkerhet i domännamnsdriften. .SE har avtalat så kallade SLA: er, Service Level Agreements, med respektive sekundär namnserveroperatör för att säkerställa kvaliteten på

driften där .SE inte kan råda över den. I avtalen ställs krav på namnserveroperatörens tillgänglighet till och samtrafik med andra Internetoperatörer.

.SE utför prestandakontroller av de sekundära namnservrarna och avtalen ses över och uppdateras årligen. .SE kommer att upphandla nya SLA:er i slutet av fjärde kvartalet 2007. .SE framhåller att de arbetar för att ställa utökade kvalitetskrav på sina underleverantörer.

Programvaran som används för det svenska domännamnssystemet är de två mest kända implementeringarna för att konkretisera DNS, nämligen BIND[1] och NSD[2]. Programvaran uppdateras ständigt.

PTS bedömning

Idag finns ett stort antal namnservrar utspridda världen över för .se-zonen. .SE har sedan ett flertal år haft en god redundans av namnservrar i Sverige, men har under 2006 utökat antalet markant i utlandet. Det väl tilltagna antalet namnservrar innebär fortsatt tillgänglighet till domännamnstjänsten för det fall en eller flera namnservrar skulle sluta att fungera. Vidare bidrar namnservrarnas placering i säkra miljöer (i enlighet med erkända LIS-standarder) till en god fysisk säkerhet. De dubblerade förbindelser som finns mellan masterservern och distributionspunkterna säkerställer att DNS-tjänsten med en rimlig grad av säkerhet har en kontinuerlig tillgänglighet.

Förbindelsernas transmissionsmedium, överföringshastighet och namnservrarnas kapacitet (deras förmåga att besvara frågor) möjliggör en effektiv domännamnstjänst. Då namnservrarna även befinner sig på olika logiska nätverk blir tillgänglighetsattacker i syfte att slå ut domännamnssystemet svårare att utföra.

Genom diversitet i namnservrarnas geografiska placering, diversitet i namnserverprogramvara och olika uppdragstagare kan en ökad säkerhet upprätthållas. Att mjukvaran som konkretiserar domännamnstjänsten skiljer sig hos namnserveroperatörerna medför också att systemet inte blir lika sårbart. Det är även av vikt att programvaran som används hålls uppdaterad.

Den genomsnittliga trafiklasten på respektive namnserver är mycket låg i förhållande till den kapacitet som finns avtalad med olika uppdragstagare för respektive namnserver. Även vid hög belastning, för respektive namnserver, är kapaciteten så väl tilltagen att namnservern enkelt hanterar att svara på DNS-förfrågningarna. Varje namnserver har en så tilltagen reservkapacitet att den kan hantera en betydande ökning av antalet DNS-förfrågningar. Dessutom används adresseringstekniken ”anycast” på flera av namnservrarna i .se-zonen för att fördela lasten mellan dem. För ytterligare beskrivningar om .SE:s beredskap, se avsnitt 3.9.

[1] Berkeley Internet Name Daemon från Internet System Consortsium, använder BIND > 9
[2] Name Server Daemon från LNet Labs, använder NSD > 3

Det kan nämnas att i ett test, som utfördes 2003 i syfte att undersöka det svenska domännamnssystemets kapacitet och oberoende av övriga Internets domännamnssystem, visade det sig att en enda namnserver i Sverige hade kapacitet att hantera alla DNS-förfrågningar ställda ifrån Sverige.[3]

PTS välkomnar inriktningen på Näringsdepartementets och .SE:s arbete med det avtal som reglerar hur en ny domänadministratör skall utses och hur nuvarande domänadministratörs verksamhet skall upphöra. Avtalet syftar till att i en extrem situation möjliggöra fortsatt drift av .se genom att en ny administratör utses. Detta på grund av att samhället har ett betydande intresse av att en stabil infrastruktur för Internet kan upprätthållas i Sverige.

PTS noterar att .SE har avtalat SLA:er med de sekundära namnserveroperatörerna och konstaterar att .SE är ytterst ansvarig för en säker och effektiv domännamnsdrift. .SE:s ansvar sträcker sig följaktligen från de system (elektroniska domännamnstjänster) som finns på Internet för att utföra förändringar i .se-zonen via de två distributionspunkter där masterservern lämnar den senaste uppdateringen av zonfilen och till de sekundära namnservrarna (som hämtar den uppdaterade zonfilen). I nästa steg råder .SE över domännamnsdriften genom de avtal de ingått med de sekundära namnserveroperatörerna. .SE leder också verksamheten i en eventuell krissituation för att säkerställa en fortsatt fungerande trafik mellan namnservrarna och Internet.

Slutligen kan konstateras att .SE genom sin uppbyggnad av en redundant namnservermiljö, genom att tillgodose behovet av reservkapacitet och genom SLA-avtal med namnserveroperatörer ser till att DNS-tjänsten är kontinuerligt tillgänglig i enlighet med 5 § p. 3 toppdomänslagen. En fungerande trafik mellan namnservrarna och Internet säkerställs i dagsläget genom dessa åtgärder i förhållande till nu aktuella trafikvolymer.

PTS vill framhålla att det dessutom åligger .SE att upprätthålla ett effektivt skydd för uppgifterna i toppdomänen, vilket regleras genom 5 § p. 4 toppdomänslagen. Uppgifterna kan förutom genom det logiska skyddet (se nedan 3.2 och 3.4), skyddas mot skada, manipulation eller förlust genom att master- och slavservrarna fysiskt hanteras och vidmaktshålls på ett stabilt sätt.

3.2 Korrekthet av data i zonfilen

.SE:s beskrivning

Dagligen utförs omkring hundratalet ändringar av IP-adresser till huvuddomän-namnservrar, så kallade ompekningar i .se-zonen och cirka 600 nya domännamn registreras i genomsnitt under en vardag, färre under lördagar och söndagar. Förändringar i zonfilen kan ske genom att en domännamnsinnehavare utför ändringar eller genom att ett så kallat .SE-godkänt ombud utför sådana.

[3] Är Internet i Sverige robust, PTS-ER-2003:1

För att säkerställa att information inte förvanskas under överföringen av domännamnsdata mellan .SE:s domännamnstjänster på Internet och .SE:s kunddatabas eller att någon obehörig skickar in falsk domännamnsinformation används PGP, *Pretty Good Privacy* för elektronisk signering av e-post. PGP är ett program som används för att signera och kryptera e-post, texter och filer och kan integreras med ett e-post-system.

Den information som skickas i e-post-meddelanden mellan ombud och .SE signeras, vilket gör det möjligt att verifiera att avsändaren är den person den utger sig för att vara**.** För att identifiera ombuden har dessa tilldelats ombudsspecifika ombudsid:n. Domännamnsinnehavarna använder sig av .SE:s webbaserade tjänster och autenticeras med stöd av dold e-postadress i kombination med engångslösenord. Alla förändringar av data mot .se-zonen och kunddatabasen görs antingen via fax, via .SE:s webbapplikationer eller via signerad e-post skickad från ett ombud eller en domännamnsinnehavare till .SE.

.SE godkänner efter prövning nya ombud och har under hösten 2006 infört nya ombudsavtal. Detta i syfte att skärpa kraven på ombuden. För att vara ett .SE-godkänt ombud måste ett antal kriterier vara uppfyllda. Dessa är att ombudet skall ha erlagt en registreringsavgift på 5000 kr, en deposition, varierande mellan 10 000 kr och 30 000 kr, och undertecknat ett ombudsavtal.

I alla led, det vill säga i produktions- och distributionsledet av zonfilen, sker överföringen av domännamnsdata med hjälp av datorprogram. På inget ställe finns en manuell hantering av domännamnsdata mellan olika system.

Zonfilen skapas från de data som finns i produktionssystemets databas (även kallad kunddatabas). I zonfilsdistributionen tillämpar .SE IETF:s protokollstandard DNSSEC (DNS Security Extensions), vilket medför ett mer tillförlitligt domännamnssystem. (DNSSEC-krypteringsnycklarna i den signerade zonfilen valideras och den signerade zonfilen jämförs med en osignerad zonfil för att säkerställa att ingen manipulation har skett.)

Varannan timme överförs en uppdaterad zonfil från masterservern till de sekundära namnservrarna, dygnet runt, hela året. För zonfilsöverföringen, det vill säga från masterservern till de två distributionspunkterna och vidare från distributionspunkterna till namnservrarna, används protokollet T-SIG, *Transaction Signature*, som är ett protokoll som autentiserar masterservern och namnservrarna samt autentiserar de sekundära namnservrarna, det vill säga verifierar att de verkligen är dem de utger sig för att vara. Överföringen av zonfilen från masterservern till de sekundära namnservrarna tar cirka fem minuter.

Förändringar i kunddatabasen sker när .SE får en begäran om förändring från en domännamnsinnehavare eller från ett .SE-godkänt ombud. I zonfilsproduktionen kontrolleras att den nya (uppdaterade) zonfilen har skapats på ett korrekt sätt och att den inte har förändrats mer än rimligt jämfört med föregående zonfil innan den distribueras.

PTS bedömning

På grund av de många förändringar som sker i .se-zonen varje dag är det viktigt att zonfilen hålls uppdaterad. Det täta intervallet med uppdateringar av zonfilen bidrar till aktualitet i se-zonen, särskilt i beaktande av det stora antalet nyregistreringar, ompekningar och borttagande som sker i .se-zonen varje dag. Det är viktigt att informationen som läggs i zonfilen är korrekt. Därför är det viktigt att verifiera att det endast är de som har behörighet till .SE:s system/domännamnstjänster som utför förändringarna, så att inte någon obehörig lägger in falsk information i .se-zonen.

Det är enligt PTS mening betydelsefullt att använda begränsande åtkomsträttigheter till domännamnssystemet för att kunna kontrollera de förändringar som görs i zonfilen, särskilt i de fall personer har skrivrättigheter till .se-zonen. Detta är viktigt för att upprätthålla en tillförlitlig zonfil. Det åligger .SE i enlighet med 5 § p. 2 toppdomänslagen att se till att informationen där är korrekt och tillgänglig.

Att .SE har infört standarden DNSSEC i .se-zonen ser PTS positivt på. DNSSEC medför att frågor besvaras på ett säkrare sätt i .se-zonen och bidrar till ett säkrare Internet. Detta på så sätt att man, när DNSSEC är fullt implementerat, som slutanvändare kan med större säkerhet förvänta sig att den webbplats som man önskar besöka är den rätta.

3.3 Driftsorganisation, ansvarsfördelning och övervakningssystem

.SE:s beskrivning

Dygnet runt, året om finns det personal som övervakar att .se-zonen finns tillgänglig på Internet. Övervakningen av sekundära namnservrar sker genom en stand-by jour och .SE:s driftspersonal mottar larm om namnserverdrift på sina mobiltelefoner dygnet runt. .SE har också möjlighet till fjärradministration av såväl sina egna namnservrar som av de sekundära namnservrarna.

Beträffande den dagliga driften av de egna namnservrarna är den delegerad till .SE:s driftspersonal som består av två personer. Inom .SE finns det sju till åtta personer som har kompetens att sköta driften av .SE:s namnservrar. Det finns inte personal som dygnet runt, omedelbart, kan vidta korrigerande åtgärder för de namnservrar som .SE administrerar.

Chefen för *IT- och systemutveckling* är den ytterst ansvariga för driften av .SE:s egna (primära) namnservrar. Avdelningen ansvarar för såväl de system som skapar som överför zonfilen till distributionspunkterna. Efter distributionspunkterna övergår driftsansvaret till .SE:s avdelning *Domänproduktion/DNS-drift*. Denna avdelning ansvarar för att zonfilen finns tillgänglig på Internet och kontrollerar att de externa leverantörerna sköter sitt åtagande i enlighet med avtal. På denna avdelning arbetar fyra personer.

Nödvändiga kontaktuppgifter till ytterst ansvariga finns dokumenterade. Kontaktuppgifter finns även till varje enskild individ som har kompetens att sköta namnserverdriften hos respektive uppdragstagare. Minst två personer med denna kompetens måste finnas hos respektive namnserveroperatör. Genom att se till att ha minst två personer som kan utföra samma arbetsuppgifter och genom att bilda arbetsteam som turas om med de vitala arbetsuppgifterna, gör att .SE:s drift och administration inte blir personberoende. Vidare, genom att .SE styrs med tydliga verksamhetsövergripande processer som beskriver dokumenterade rutiner och beslutsmoment blir det lätt att träda in på en uppgift. Månadsvis uppdateras och distribueras en lista över kontaktpersoner till berörda. Kommunikationen mellan .SE och namnserveroperatörer sker i första hand med e-post genom funktionsadress. Med funktionsadress avses en e-postadress som når flera personer inom en organisation, exempelvis drift@iis.se.

För den dagliga namnserverdriften kan driftspersonal kontakta varandra genom ”instant messaging” eller ett chattprogram där alla namnserveroperatörer kan ta del av kommunikationen eller endast ”tilltalade”.

Någon kompetenskontroll vid nyrekrytering har inte skett då nyrekrytering har varit mycket blygsam. Vidareutveckling av gemensamma rutiner och processer håller dock på att framarbetas för att säkerställa den kompetens som krävs för att utföra arbetsuppgiften och för att trivas i organisationen. Att se över kompetensförsörjningen är ett pågående arbete. Varje medarbetare kommer under 2007 att få ett individuellt kompetensutvecklingsprogram med syfte att tillgodose både framtidens kompetensbehov och medarbetarnas utvecklingsbehov.

Sedan 2003 finns ett centralt övervakningssystem över namnservrarna (såväl primär- som sekundärservrar) som ingår i .se-zonen. Genom detta får .SE en automatiserad lägesrapport över namnservrarnas tillgänglighet, belastning och svarstider.

Övervakningssystemet genererar automatiskt larm i fyra olika situationer;

- vid otillgänglig ”unicast”-server och ”anycasttjänst”,
- vid onormalt hög och/eller låg last per server (gäller för samtliga servrar),
- vid felaktig eller gammal zon; och
- vid felaktig eller gammal DNSSEC-signatur.

Övervakningssystemet genererar larm och felrapporteringar vid såväl störningar som avbrott. Om störningen eller avbrottet berör en namnserveroperatör skickas larm automatiskt till denna.

PTS bedömning

Ett övervakningssystem som åskådliggör respektive namnservers belastning, svarstider och tillgänglighet är nödvändigt för att kunna bedriva en säker drift. Att larm autogenereras till aktuell namnserveroperatör när ett avbrott, dålig

tillgänglighet eller ett fel har uppstått, dygnet runt, är också nödvändigt. Att fjärradministration kan ske av såväl egna som sekundära namnservrar är också bra.

Kontaktuppgifter till nödvändig driftspersonal ska finnas lättillgängliga och vara uppdaterade.

I enlighet med 5 § p. 3 ska .SE ha beredskap att motstå olika former av störningar. En förutsättning är då att ett övervakningssystem ger signaler om situationer som innebär en risk.

Personalens kompetens är en nyckelfråga. Såsom organisationen har beskrivits av .SE är den uppbyggd på ett sätt som idag ger goda personella och tekniska förutsättningar för DNS-driften. .SE bör dock planera för kompetensförsörjning, då den tekniska driften framstår som delvis personberoende och därmed sårbar. Detta då det enligt 5 § p. 5 toppdomänslagen åligger .SE se till att personalen har tillräcklig kompetens och erfarenhet för verksamheten. .SE bör dessutom överväga kontroller för personal med nyckelfunktioner för den tekniska driften då det framgår av lagens förarbeten (prop. 2004/05:175 s. 246) att det är av vikt att det förekommer kontroll av de personer som skall utföra domänadministrationen.

3.4 Åtkomsträttigheter till .se-zonen och domännamnssytemet

.SE:s beskrivning

De förändringar ombud eller innehavare av domännamn kan begära i .se-zonen är:

- nyregistrering av domännamn,
- överlåtelse av domännamn,
- e-postadressändring,
- ompekning och borttagande av namnservrar; och
- övriga kontaktuppgiftsändringar.

Alla ovannämnda förändringar mot .se-zonen utförs antingen genom PGP-signerad e-post som skickas från ett ombud eller av en domännamnsinnehavare via .SE:s webbgränssnitt och engångslösenord till .SE. Varje ombud har tilldelats ett unikt ombudsid för att logga in till .SE:s olika domännamnstjänster som finns åtkomliga via ett för ombuden anpassat extranät (ombudssidor) på Internet. På så sätt kan ombudet verifieras. De ombudsid:n som ombuden har tilldelats är ombudsspecifika och inte personspecifika. Alla ändringar/borttagningar av information sköts normalt av innehavaren av ett domännamn, men ombuden kan dock via speciella formulär som PGP-signeras hjälpa innehavarna med förändring av DNS-data, så kallad ompekning. Hos .SE valideras (verifieras) e-posten genom

att verifiera att ombudets signatur stämmer överens med den publika nyckel som .SE har lagrat hos sig. Från särskilda ombudssidor kan ombuden även utföra ett begränsat antal utökade WHOIS-slagningar för att få utökad information om domännamnsinnehavarna.

För att minska ombudens eventuella missbruk eller utnyttjande av möjligheten att genomföra olika transaktioner i .se-zonen som medför uppdateringar i .SE:s databas, finns begränsningar i systemet som syftar till att upptäcka avvikelser. Dessa innefattar bland annat begränsningar i antal nyregistreringar, ompekningar och WHOIS-slagningar. Dessutom finns ett maxantal för de engångslösenord som tilldelas.

All inkommande e-post, med nyregistreringar mot .se-zonen, accepteras och utförs automatiskt/digitalt mot kunddatabasen så länge som den elektroniska signaturen kan valideras.

PTS bedömning

Att all information som skickas in till .SE:s domännamnssystem är krypterad och dessutom signerad säkerställer att informationen inte manipuleras under transportens gång. Vidare är det viktigt att det är personer med behörighet som utför förändringar i .se-zonen (nyregistreringar och ompekningar m.m.). Det är av vikt att åtkomsträttigheter för att utföra förändringar är begränsade.

Att krypterad och signerade e-post innehållande domännamnsförändringar accepteras (om signaturen accepteras) och genomförs, innebär att det finns stora möjligheter att utföra många olika typer av förändringar gentemot kunddatabasen och indirekt mot zonfilen. För att begränsa eventuell felaktig användning, eller utnyttjande av de elektroniska domännamnstjänsterna har .SE infört ett maximalt antal gånger som en domännamnsinnehavare eller ett ombud kan utföra förändringar gentemot .SE:s system (databas). Endast ett begränsat antal engångslösenord kan tilldelas.

Dessa åtgärder är viktiga komponenter i att tillse att zonfilen i enlighet med 5 § p. 2 toppdomänslagen är korrekt och för att upprätthålla ett effektivt skydd av uppgifterna i toppdomänen i enlighet med 5 § p. 4. Det åligger .SE att säkerställa att alla DNS-data är tillräckligt skyddade mot skada, manipulation eller förlust med hjälp av bästa rimliga teknik.

Det kan finnas anledning för .SE att se över behörighetsadministationen avseende ombuden. .SE bör överväga att göra ombudsid:n personunika för att skicka signerad e-post personunika och inte ombudsunika. Om en person hos .SE:s ombud skulle utnyttja sin ställning/ möjlighet att utföra förändringar i zonfilen och införa falsk eller ta bort riktig domännamnsdata är det ytterst viktigt att kunna spåra detta på personnivå och inte enbart till ett visst ombud.

3.5 Rutiner för registerföring och informationshantering enligt Personuppgiftslagen

.SE:s beskrivning

.SE:s rutiner för registerföring över tilldelade domännamn sker vid nyregistreringstillfället och sedan löpande på kundens begäran i .SE:s kundregister. Ändring av registerinformation sker vid: överlåtelse, avregistrering, förändring av DNS-data (ompekning eller borttagande), ändring av kontaktuppgifter samt ändring av e-postadress till innehavaren. Personuppgifter, inklusive personnummer lagras i .SE:s kundregister.

Alla registeruppgifter sparas direkt i en databas lagrad i två från varandra, både logiskt och fysiskt, separerade system. Ytterligare säkerhetskopiering av registeruppgifterna sker en gång per dygn till ett externt elektroniskt valv.

En domännamnsinnehavares personuppgifter behandlas av .SE och av .SE:s godkända ombud. Att personuppgifter hanteras enligt Personuppgiftslagen, PuL, säkerställs genom de regleringar som finns i gällande ombudsavtal. Vid registrering hos ett ombud godkänner domännamnsinnehavaren .SE:s ”Allmänna villkor”. I punkten 14 regleras behandling av personuppgifter. Samtycke till behandling av personuppgifter och t.ex. samtycke till publicering på Internet, inhämtas genom innehavarens godkännande av gällande ”Allmänna villkor”. Om inget godkännande av ”Allmänna villkor” har lämnats vid registreringstillfället nekas registreringen. .SE:s chefsjurist är anmäld till Datainspektionen som personuppgiftsombud.

Domännamnsinnehavaren har rätt till information om de uppgifter som behandlas om honom/henne av .SE.

PTS bedömning

.SE beskriver registerföring och säkerhetskopiering i enlighet med den grundläggande skyldigheten i 6 § toppdomänslagen. .SE:s informationshantering sker i enlighet med PuL då personuppgifter får göras tillgängliga via Internet endast om den registrerade har samtyckt till det (6 § 2 st. toppdomänslagen).

3.6 Rutiner för uppdatering, nykonfigurationer av mjukvara respektive hårdvara

.SE:s beskrivning

Fyra gånger per år har domänadministratören schemalagda driftsmöten med de sekundära namnserveroperatörerna. Där diskuteras bland annat förändringar för driftsmiljön såsom genomförande av uppdateringar och nykonfigurationer. Allt underhåll av namnservrar i .se-zonen måste aviseras i förhand och ingen namnserveroperatörer tillåts genomföra uppdateringar samtidigt. Det finns en

rutin för att utannonsera uppdatering bland de sekundära namnservrarna och driftspersonal har veckovis kontakt via e-post.

Uppdateringar, omkonfigurationer och nyinstallationer på masterservern sker ungefär en gång per halvår. En sådan ändring på masterservern, som medför att den behöver tas ur bruk, brukar inte överstiga en halvtimme.

Uppdateringar, omkonfigurationer och nyinstallationer av hårdvara samt mjukvara på de sekundära namnservrarna sker vid behov. Det brukar innebära en gång per server och år. Avbrottet på sekundära namnservrar brukar normalt pågå i mindre än 10 minuter.

Vid bortfall av en namnserver finns dokumenterade rutiner för återstart samt felsökning.

För närvarande finns inga väldokumenterade instruktioner hos .SE för hur uppgradering av hårdvara respektive mjukvara skall gå till på namnservrarna. .SE har ett pågående projekt som går ut på att införa ITIL[4], ”Change management” och ”Release management”. ITIL är ett ramverk med ”best practices” som innehåller ett stort antal mjukvarubibliotek vilka syftar till att underlätta utförandet av kvalitativa IT-tjänster. Detta system kommer att innebära att förändringar kan hanteras och kontrolleras på ett systematiskt och standardiserat sätt. Införandet av ITIL, Change och Release management kommer enligt .SE att ske under de närmsta månaderna.

.SE är medlem i ”ISC BIND Forum” vilket man blir efter att ha betalat en relativt hög årsavgift. Medlemmar i ISC BIND Forum får tillgång till information om de senaste sårbarheterna i olika BIND-versioner, tips på omkonfigurationer och säkerhetsuppdateringar. Under inga omständigheter får medlemmar föra informationen vidare till icke-medlemmar, därför försöker .SE påverka sina sekundära namnserveroperatörer att ingå medlemskap. Forumet är en mycket betydelsefull informationskälla för .SE för att upprätthålla säkerhet i domännamnssystemet.

.SE har god kontakt med ICANN (Internet Corporation for Assigned Names and Numbers) och har deltagit regelbundet på ICANN:s möten. Under hösten 2006 har .SE haft direkta möten med representanter från ICANN vid ett antal tillfällen. Därutöver har .SE kontakt med ICANN i samband med uppdatering av kontaktuppgifter och .SE:s uppgifter som ingår i rotzonen.

PTS bedömning

Att tydliga rutiner finns för hur uppdateringar av mjuk- och hårdvara sker för namnservrarna i toppdomänen är enligt PTS mening av vikt för att behålla en stabil drift när förändringar utförs. Rutiner är viktiga för att systematiskt kunna spåra eventuella fel i uppdaterings-/förändringsprocessen. Införandet av ett versionshanterings- och återställelsesystem som ITIL, Change management och

[4] Information Technology Infrastructure Library

Release management bedöms vara viktigt. Att allt underhåll av namnservrar i .se-zonen aviseras i förhand och ingen namnserveroperatör genomför uppdateringar samtidigt är en betydelsefull rutin och en del i att säkerställa att trafiken mellan namnservrarna och Internet fungerar i enlighet med 5 § p. 3 toppdomänslagen.

Mjukvarudiversiteten hos namnservrarna i .se-zonen är viktig för att namnserverdriften inte ska vara kritisk allteftersom nya sårbarheter upptäcks i namnservermjukvara. Nya sårbarheter upptäcks varje månad. Det viktiga är alltså att alla namnservrar inte använder en och samma mjukvara och version samtidigt. På det sättet kan .SE också sägas säkerställa en fungerande trafik mellan namnservrarna och Internet i enlighet med 5 § p. 3 toppdomänslagen.

Det är positivt att .SE har god kontakt med ICANN och att de har deltagit regelbundet på ICANN:s möten.

3.7 Kontinuitetsplan och rutiner för incidentrapportering

.SE:s beskrivning

.SE har dokumenterade och testade rutiner för såväl hantering som rapportering av incidenter. Rutinerna omfattar bland annat instruktioner för hur avbrott av olika längd skall hanteras och för eskalering då en incident riskerar att utvecklas till en kris.

Alla säkerhetsrelaterade händelser och incidenter ska enligt .SE:s fastställda rutin dokumenteras och rapporteras till respektive avdelnings- och säkerhetschef. Incidenter dokumenteras på en särskild blankett utarbetad för ändamålet. Rapporteringen används för att bygga upp en erfarenhetsbank som utgör underlag för förbättringsåtgärder.

Vid en incident sker en intern bedömning av situationen, av respektive system- eller verksamhetsansvarig, dels för att få kontroll över situationen, dels för att avgöra behovet av att sammankalla den särskilda krisledningsgruppen. I samband med rapportering finns en möjlighet att redovisa behov av åtgärder för att undvika att incidenten upprepas och i det fall det bedöms nödvändigt genomförs förslaget omgående.

.SE har också utarbetat en krishanteringsplan. Dessutom har .SE en policy som styr agerandet i en kris- eller katastrofsituation.

.SE har även etablerat en krisledningsgrupp vari ansvarsfördelningen är reglerad vid avbrottssituationer. Den person som tar emot ett larm om eventuell kris ska sammankalla krisledningen. Det är .SE:s VD eller två personer ur ledningsgruppen som fattar beslut om när .SE har hamnat i en kris, som aktiverar krisplanen och som också beslutar om återgång till normalläge.

.SE har även definierat en prioritetsordning som gäller om en exceptionell händelse inträffar. Prioritetsordningen är följande: 1) liv och hälsa, 2)

kommunikation, produktion och drift av anläggningar, system och tjänster för .se, 3) dataintegritet, 4) ekonomi, transaktioner och bokföring.

Vid en allvarlig kris eller omfattande störning finns en samordnad plan för återställande till normal drift. .SE:s mål under 2007 är att driften skall, i en extrem krissituation i domännamnssystemet (där primära namnservrar är utslagna i .se-zonen), kunna återupptas (på en rimlig nivå) på ett alternativt driftställe och i skyddad miljö inom loppet av fyra timmar. Tillgång till ett säkert alternativt driftsställe är redan säkerställt. .SE har där i dagsläget ett så kallat ”cold” standby system och kommer att arbeta med fullbordan av detta reservdriftsställe under 2007. Under det första halvåret 2007 kommer .SE ha ersatt ”cold” standby systemet med ett ”warm” standby system. .SE anser inte idag att den hotbild föreligger som krävs för ett mer avancerat reservsystem än så. De utesluter dock inte att de utvecklar ett ”hot” standby system i framtiden, men det ligger inte i planerna för det närmaste året.

I en krissituation är .SE:s alternativa kommunikationsformer till Internet primärt mobiltelefoni. Den sekundära kommunikationskanalen är fast telefoni och en extern telefonbrygga. Dokumenterade handlingsplaner finns för ett flertal krissituationer, exempelvis om organisationen skulle bli korrupt eller vid brand.

De primära och sekundära namnservrarna är utrustade med extra reservkraft för det fall ett strömavbrott skulle inträffa. Reservkraften startar inom 15-30 sekunder och räcker i minst 15 timmar vid normal last. .SE:s primära och sekundära driftställen är utrustade med fukt-, brand-, temperatur- och inbrottslarm.

.SE utför regelbundet, och vid stora förändringar, säkerhetsgranskningar avseende sin organisation, produktion och namnserverdrift och utgående från en definierad hotbild och med en utgångspunkt från hotbilden definierad grundskyddsnivå.

I ett scenario där .SE:s organisation med system skulle slås ut, skulle .SE:s alternativa reservdriftställe kunna skötas med hjälp av .SE:s styrelse. Där finns kompetenser inom såväl teknisk drift som administration och ledning. Styrelseordförande går exempelvis in som VD (att jämföra med vad som just skett inom .org). I styrelseordförandes krispaket ingår vad som krävs för att få tillträde till det alternativa driftstället.

Under tredje och fjärde kvartalet 2007 avser .SE att utföra en övning av delar av krishanteringsplanen. Dessutom kommer en enskild övning för krisledningen att genomföras. .SE arbetar även med att ta fram ett så kallat ”krispaket” att tillhandahålla sina underleverantörer för att de snabbt, vid en kris skall kunna ha en fungerande slavserverfunktion för .se. Detta krispaket innebär att en uppdaterad och fungerande akutlösning distribueras till de större Internetoperatörerna.

PTS bedömning

Att en krishanteringsplan är utformad för domänadministratören är angeläget. PTS ser positivt på att .SE har en krishanteringsplan och anser det nödvändigt att den övas.

PTS ser också positivt på de handlingsplaner som .SE har tagit fram för specifika krisscenarios.

.SE:s utbyggnad av ett alternativt primärt ställe för .SE:s administration i säker miljö är viktigt. Om .SE:s ordinära ställe för administration skulle slås ut, där såväl personal som system drabbas, är det nödvändigt att såväl aktuell backup-information på kunddatabasen som på zonfilen snabbt kan hämtas och bli tillgänglig för det alternativa stället. Ett ”cold” standby system finns idag och det utvecklas ett ”warm” standby system. PTS anser det viktigt att den primära driften med ett kort tidsintervall kan ställas om till det alternativa primära stället, vilket en lösning med ett ”warm” standby system tillförsäkrar. PTS ser också fördelen med ett ”hot” standby system eftersom det medför att det direkt, i en krissituation, finns ett primärt ställe för administration.

Att ett primärt ställe för domännamnsadministration i säker miljö är viktigt beror på att det finns en grundläggande skyldighet i 5 § toppdomänslagen att säkerställa att DNS-tjänsten är kontinuerligt tillgänglig. Anslutningsmöjlighet via Internetprotokollet till namnservrarna bör, enligt förarbetena (prop. 2004/05:175 s. 246) tillhandahållas dygnet runt.

Det är enligt PTS mening angeläget att ett avtal mellan Näringsdepartementet och .SE kommer till stånd, eftersom toppdomänslagen lämnar oreglerat hur en domänadministratör utses eller hur dennes verksamhet skall upphöra. Ett sådant avtal skall också garantera att en fortsatt stabil infrastruktur för Internet kan upprätthållas i Sverige om .SE slutar administrera toppdomänen .se. Det bör finnas en plan för hur bytet skall gå till och hur det ska hanteras.

3.8 Informationssäkerhet

.SE:s beskrivning

.SE har nyligen utarbetat en informationssäkerhetspolicy vilken omfattar all verksamhet som utförs av .SE, såväl domänadministration som stöd till Forskning och utveckling (FOU). .SE:s målsättning är att organisationens ledningssystem för informationssäkerhet skall klara kraven enligt standarden ”Ledningssystem för informationssäkerhet” (SS-ISO/IEC 27001:2006). Policyn antogs av .SE:s styrelse och gäller från och med 2006-03-06. Ytterst ansvarig för inriktningen av informationssäkerhetsarbetet är styrelsen för .SE. Ansvaret för det praktiska genomförandet är delegerat till .SE:s VD. Informationssäkerhetspolicyn omfattar säkerhet i administrativa rutiner, fysisk säkerhet och IT-säkerhet samt personalens ansvar och delaktighet.

I .SE:s säkerhetspolicy står det att ”.SE skall säkerställa att information som överförs, lagras eller behandlas manuellt, i kommunikationsnät, datasystem, och datorer ska skyddas mot: oavsiktlig, obehörig eller otillåten åtkomst eller kopiering, oavsiktlig, obehörig eller otillåten förändring eller förstöring. Informationssäkerhetsarbetet inom .SE ska också säkerställa att

kommunikationsnät, datasystem och datorer skyddas mot intrång eller otillåten användning, stöld eller skadegörelse samt funktionsstörning."

Beträffande åtkomst till system och lokaler är in- och utpassering till och från namnservrar, produktion samt primära och sekundära driftställen säkerställda genom att kort och kod krävs.

.SE har vidare utarbetat ett antal dokument som definierar grundnivån för att upprätthålla säkerheten i den interna produktionsmiljön samt i namnserverdriften vilka presenterades vid själva tillsynsbesöket.

PTS bedömning

Att en informationssäkerhetspolicy är definierad är ett första steg på vägen mot en ökad informationssäkerhet. Är den sedan väl förankrad i organisationen tyder det på en ytterligare en säkerhetsmedvetenhet. PTS anser att de många logiska och fysiska säkerhetssystem och rutiner som .SE och varje namnserveroperatör tillämpar bidrar till en god informationssäkerhet.

Ett exempel som bidrar till en ökad informationssäkerhet är att tillträdeskontroll sker vid in- och utpassering till .SE:s lokaler och driftmiljöer. Ytterligare ett är att brand- och fuktlarm finns installerade i såväl .SE:s lokaler som i driftslokaler hos sekundära namnserveroperatörer.

I linje härmed ligger också att .SE i enlighet med 5 § p. 6 toppdomänslagen enligt PTS mening har sådana rutiner för verksamheten som uppfyller erkända standarder.

3.9 Beredskap för möjliga framtida hot och attacker

.SE:s beskrivning

.SE anser att de allvarligaste hoten mot den svenska toppdomännamnsdriften är "den mänskliga faktorn", manipulation, DDoS-attacker samt "social engineering".

.SE gör årligen en utvärdering utifrån en sammanställning av .SE:s incidentrapporter. Utvärderingen visar på vilka särskilda åtgärder som kan behöva genomföras mer långsiktigt. I .SE:s incident- och krishanteringsplan finns också beskrivet tillgänglighetsattacker med olika scenarion.

Månadsvis utför .SE en risk- och sårbarhetsanalys av sin organisation och namnserverdrift.

Hittills har .se-zonen inte utsatts för en överbelastningsattack på grund av ont uppsåt, till exempel genom en DDoS-attack. Däremot har överbelastningsattacker utan ont uppsåt skett vid ett flertal tillfällen på grund av felkonfigurerade kundresolvrar. Felkonfigurationerna har lett till en kraftig ökad last på mycket kort tid, men namnserverdriften för .se-zonen har inte påverkats märkbart av dessa

incidenter. Respektive sekundär namnserveroperatör ansvarar för sin säkerhetslösning, sitt skydd och sina rutiner vid en tillgänglighetsattack.

För att hantera en ökande mängd trafik på de sekundära namnservrarna i .se-zonen kan nya namnservrar placeras på nya nättopologiska platser för att sprida ut lasten på flera servrar och därmed öka den sammantagna kapaciteten i anslutningarna på Internet.

Sedan ICANN:s tillkomst har .SE regelbundet deltagit vid deras möten. Under 2006 hade .SE flera direkta möten med representanter för ICANN. Därutöver har .SE kontakt med ICANN i samband med uppdatering av kontaktuppgifter och .SE:s uppgifter som ingår i rotzonen.

PTS bedömning

.SE ska i enlighet med 5 § p. 3 toppdomänslagen säkerställa en fungerande trafik mellan namnservrarna och Internet. Den utrustning som används för verksamheten skall ha en för ändamålet lämplig nättopologisk, geografisk och organisatorisk spridning. Detta, för att det ska finnas en beredskap att stå emot olika former av störningar, exempelvis DDoS-attacker.

Distribuerade DoS-attacker, DDoS, har förekommit under de senaste åren. Dessa kan bestå av ett stort antal datorer som verkar tillsammans för att slå ut ett specifikt system. Det har inträffat att hundratusentals datorer har ingått i en DDoS-attack, där en enda dator har styrt alla andra. Det är viktigt att även nätverkskomponenter i .se-zonen, såsom routrar, klarar att hantera de nya höga överföringsvolymerna, som en eventuell DDoS-attack kan föra med sig. DDoS-attacker kan vara riktade och sker kanske bara en gång.

Det är självfallet betydelsefullt att ständigt uppdatera sin kunskap om nya attackers form och skepnad för att kunna vidta lämpliga och effektiva åtgärder och därmed mildra deras effekter.

PTS vill framhålla att medlemskap i ISC BIND Forum förvisso är bra och PTS ser gärna att .SE i stor utsträckning också har kontakt med olika forum för informationsutbyte. Detta gäller såväl information om rotserverfunktionen (genom säkerhetslistor el.dyl.) som kontakt med ICANN. Härutöver är en aktiv omvärldsbevakning av vikt.

4 Slutsats

4.1 Områden PTS har undersökt vid tillsynen

- Att DNS-tjänsten är kontinuerligt tillgänglig,
- Att databasen med domännamn, IP-adresser, andra data drivs på ett säkert och effektivt sätt och att informationen distribueras till toppdomänens namnservrar,
- Att anslutningsmöjlighet via IP-protokollet till namnservrarna tillhandahålls dygnet runt,
- Att de auktoritativa eller officiella master– och slavnamnservrarna för toppdomänen hanteras och vidmakthållas på ett stabilt och säkert sätt,
- Att det finns beredskap och kapacitet att motstå olika former av störningar och attacker, t.ex. distribuerade tillgänglighetsattacker.,
- Att zonfilen för den nationella toppdomänen är korrekt och att registreringsuppgifter är uppdaterade och fortlöpande hålls tillgängliga för att trygga driftsstabiliteten,
- Att den administrativt ansvarige säkerställer att alla DNS-data är tillräckligt skyddade mot skada, manipulation eller förlust enligt bästa rimliga teknik,
- Att personalen är tillräckligt kompetent,
- Att det finns klara rutiner för verksamheten samt en organisation som har såväl tekniska som personella förutsättningar att klara de krav som administrationen av den nationella toppdomänen .se kräver; och
- Att domänadministratören följer erkända standarder på området, tex. den standardisering som sker inom IETF.

4.2 Samlade slutsatser av tillsynen

PTS bedömer att .SE bedriver en tillfredställande teknisk drift av .se-zonen.

De många namnservrar som utgör .se-zonen är såväl logiskt som geografiskt utspridda och placerade i säkra miljöer. .SE:s avtal med de sekundära namnserveroperatörerna innehåller krav på namnserveroperatörens tillgänglighet och samtrafik med andra Internetoperatörers nät. De många namnservrarna, deras

logiska och fysiska placering, .SE:s avtal med olika namnserveroperatörer och att varje namnserver har redundanta nätförbindelser till alternativa operatörer bidrar till en kontinuerlig drift av DNS-tjänsten. Den utrustning som används för verksamheten har alltså en lämplig nättopologisk, geografisk och organisatorisk spridning. I avtal säkerställer .SE sina underleverantörers säkerhetsnivå och kvalitet (SLA). Dessa avtal ser .SE över årligen. Krav på tillgänglighet är det sätt på vilket .SE kan se till att anslutningsmöjlighet via IP-protokollet till namnservrarna tillhandahållas dygnet runt. Även .SE:s övervakningssystem möjliggör kontroll av namnservrarnas tillgänglighet. Det leder till att databasen med domännamn, IP-adresser och andra data effektivt kan distribueras till toppdomänens namnservrar.

Dessutom bidrar namnservrarnas tilltagna kapacitet att besvara frågor till att en säker domännamnstjänst för .se-zonen kan bevaras även vid höga trafikbelastningar, såsom vid DDoS-attacker. Att adresseringsmetoden ”anycast” används för några namnservrar bidrar ytterligare till en stabil domännamnsdrift i händelse av en överbelastningsattack. Vidare kan sägas att såväl vid genomsnittslast per namnserver som vid trafiklastpeakar, vad gäller att besvara frågor, har de sekundära namnservrarna en tillfredställande överkapacitet. Det visar att när det gäller förmågan att besvara frågor hanteras och vidmakthålls de auktoritativa master– och slavnamnservrarna för toppdomänen på ett stabilt och säkert sätt.

Vidare anser PTS att det är bra att det finns en krishanteringsplan utarbetad för hur administrationen kan återupptas på ett alternativt driftställe inom fyra timmar efter en incident. .SE ska ha en beredskap och kapacitet att motstå olika former av störningar och attacker, t.ex. distribuerade tillgänglighetsattacker. Att månadsvis bedöma hoten mot och sårbarheten i organisationen anses fullgott.

Att en väl fungerande kommunikation finns mellan .SE och de sekundära namnserveroperatörerna och att utarbetade rutiner finns för hur uppgraderingar av mjukvara och hårdvara ska ske hos namnserveroperatörerna är viktigt i sammanhanget. Rutinen för att utannonsera uppdatering bland alla sekundära namnservrar anses bra och att en veckovis kontakt sker via e-post-korrespondens. Att ett väl fungerande versionshanterings- och back up system samt att väldokumenterade rutiner finns för hur uppdateringar av namnservrarnas mjukvara ska utföras anser PTS som nödvändigt för att kunna behålla en robust domännamnstjänst.

Vidare, vad gäller tillförlitligheten till och korrektheten av data i .se-zonen säkerställer protokollen PGP, SSH, T-SIG och DNSSEC överföring av information mellan olika instanser i distributionskedjan genom autentisering av personer och/eller namnservrar. I zonfilsproduktionen verifieras att zonfilen inte har förändrats mer än rimligt sedan den uppdaterades senast, det vill säga två timmar tidigare. Ett maxantal förändringar tillåts utföras per ombud/domännamnsinnehavare genom att bara ett begränsat antal engångslösenord tillhandahålls. .SE har dessutom under hösten 2006 ingått nya ombudsavtal, detta i syfte att skärpa kraven på ombuden.

.SE:s engagemang i införandet av DNSSEC för den svenska toppdomänen visar på en säkerhetsmedvetenhet och ansvarsfullhet i uppbyggnaden av ett säkrare Internet i Sverige.

.SE visar vidare på en öppenhet med sin domännamnsverksamhet genom sin webbplats där de presenterar information till såväl konsumenter som ombud. Där kan konsumenten finna information om det svenska Internets driftstatus (namnservrarnas status samt tillgängligheten till dem), statistik över antalet nya domännamnsregistreringar utförda per dag och år samt statistik över manuella och automatiska ompekningar samt adressändringar. .SE visar vidare att de har kunskap om och är väl förberedda för utvecklingen och tillväxten av det ”svenska Internet” genom att de har utökat antalet namnservrar markant under år 2006. Sedan 2003, då reglerna för registrering av domännamn under .se blev enklare, har antalet domännamn vuxit till idag närmare 600 000. Genom såväl den logiska som fysiska infrastrukturen av namnservrarna i toppdomänen, samt .SE:s förberedelse inför olika incidenter, såsom belastningsattacker, kan namnserverdriften i dagsläget sägas vara säker.

Det kan finnas anledning för .SE att se över behörighetsadministationen avseende ombuden. .SE bör överväga att göra ombudsid:n för att skicka signerad e-post personunika och inte ombudsunika. Om en person hos .SE:s ombud skulle utnyttja sin ställning till att utföra förändringar i zonfilen och införa falsk eller ta bort riktig domännamnsdata är det ytterst viktigt att kunna spåra detta till en viss person och inte enbart till ett visst ombud. Att införa personunika id:n skulle medföra ytterligare arbete för domänadministratören som behöver ”utöka” antalet användaridentiteter och administrera flera användarkonton. .SE har att säkerställa dels att zonfilen är korrekt, dels att alla DNS-data är tillräckligt skyddade mot skada, manipulation eller förlust enligt bästa rimliga teknik. Ett sätt, utöver att se till att filen inte manipuleras, är också deponering eller ”spegling” av data som handhas av .SE.

När det gäller kontinuitet vill PTS framhålla vikten av att ett avtal mellan Näringsdepartementet och .SE kommer till stånd. Ett avtal, vilket skulle garantera att en fortsatt stabil infrastruktur för Internet kan upprätthållas i Sverige om .SE slutar administrera toppdomänen .se.

Domänadministratörens personal är en kritisk faktor på flera sätt. .SE har att se över att det finns tillräckligt med personal och att kontroll av personal som utför domänadministrationen sker. Driftspersonal bör kontinuerligt utbildas i, och förberedas för nya trender och hot. Dessutom bör .SE se till att verksamheten inte är personberoende och att kompetensförsörjning av organisationen sker.

I och med deltagande i bland annat ICS BIND Forum, användning av NSD, IETF-standarder och LIS (och uppdateringar i enlighet därmed) följer .SE erkända standarder på området. .SE kan härutöver överväga att inleda ett mer aktivt informationsutbyte i Sverige och internationellt.

4.3 Fortsatt arbete

Vad som framkommit vid tillsynen föranleder inte några ytterligare åtgärder från PTS sida. Emellertid kommer PTS löpande under 2007 att följa upp .SE:s säkerhetsarbete, övning av krisplan och följa utvecklingen när det gäller det avtal mellan Näringsdepartementet och .SE som tar form. PTS vill också påpeka att bedömningarna i denna promemoria bygger på dagens trafiklast, uppslagningskapacitet, antal domännamn, hotbild m.m. i förhållande till .SE:s säkerhetsarbete. En betydande ökning av antalet registrerade domännamn i .se-zonen kan vid ett senare tillfälle föranleda en annan bedömning om .SE inte bygger ut system och reservkapacitet i takt med ökningen.

I och med denna promemoria avslutas detta tillsynsärende.

Anders Johanson

Avdelningschef

Bilaga 1 - Ordförklaringar

Nedan förklaras kortfattat innebörden av vanligt förekommande vokabulär för domännamnssystemet i syfte att etablera en gemensam begreppsapparat.

Anycast-adressering är en adresseringsmetod som innebär att flera identiska namnservrar tilldelas samma IP-adress som då kan dela på arbetet med att svara på DNS-förfrågningar när trafikbelastningen är mycket hög på en namnserver.

Cold standby är ett passivt reservdriftsläge som innebär att systemet är avstängt eller i viloläge så länge systemet inte behövs. Fördelen med ett cold standby system är att det är lägre strömförbrukning och mindre slitage, nackdelen är att det tar tid att komma igång och igångsättningen kan leda till störningar.

DNS (Domain Name System) även kallat domännamnssystemet.

Domän är en del av domännamnssystemet och omfattar alla underliggande resurser som finns i det delsystemet. .se-domänen är ett sådant delsystem och omfattar underliggande domäner såsom exempelvis pts.se och mail.pts.se.

Hot standby innebär att ett ”skuggsystem” (reservsystem) finns berett och är ständigt redo att ta över om det ordinarie systemet havererar. Ett sådant system är alltid i drift och kopierar allt som görs i det ordinarie systemet. Reservdriften kan sättas igång på mindre än en bråkdel av en sekund.

Kunddatabas eller produktionsdatabas är den databas som rymmer information om domänens domännamnsinnehavare. Exempel på information som kunddatabasen innehåller är domännamnsinnehavarens kontakt- och personuppgifter, domännamn, namnserver. Kunddatabasen är första instansen i zonfilsproduktionen.

Masterserver eller **master** är synonymer för den namnserver som ligger till grund för en zon. Masterservern rymmer zonfilen som distribueras till de sekundära namnservrarna.

Resolver är en s.k. frågeställare i DNS-systemet. Den finns fysiskt nära slutanvändarna, ofta på slutanvändarens Internetoperatörs nät. Resolvern ställer frågor till de olika nivåerna i DNS-hierarkin och levererar ett svar i form av en IP-adress till Internetanvändaren. Svaret lagras i resolverns s.k. cache (minne) under en viss begränsad tid och kan under denna tid levereras direkt till Internetanvändaren utan att fråga officiella namnservrar, förutsatt att någon annan slutanvändare på samma nät har efterfrågat densamma. På detta sätt minskas trafikbelastningen i DNS-systemet. Resolvern innehåller ingen databas i sig självt men ”cachar” (lagrar) svar från andra slutanvändares efterfrågade webbplatser, dock under en begränsad tid.

Slavservrar, **namnservrar** eller **sekundära namnservrar** är synonymer för de namnservrar som tillgodoser Internets användare med DNS-tjänsten, dvs. översätter domännamn till IP-adresser och omvänt. Namnserveroperatörer är underleverantörer till domänadministratören och tillhandahåller kopior på

zonfilen. Domänadministratören har särskilda avtal med namnserveroperatörer för att säkerställa kvalitet på DNS-tjänsten.

Tillgänglighetsattack eller en **överbelastningsattack** kan till exempel vara en DoS- (Denial of Service-) eller en DDoS-attack (Distribuerad Denial of Service). Det är en attack där det angripna systemet (till exempel en dator eller server) inte kan utföra sin avsedda tjänst då systemets resurser är fullkomligt allokerade på grund av alltför många förfrågningar till servern.

Unicast-adressering är en adresseringsmetod som innebär att det bara finns en avsedd mottagare i nätverket som ska besvara förfrågan/utföra/ den efterfrågade tjänsten.

Warm standby är ett förberett reservdriftssystem som är färdigt att starta med kort väntetid. Det är klart och uppdaterat så att det kan komma igång snabbt, men inte helt utan väntetid.

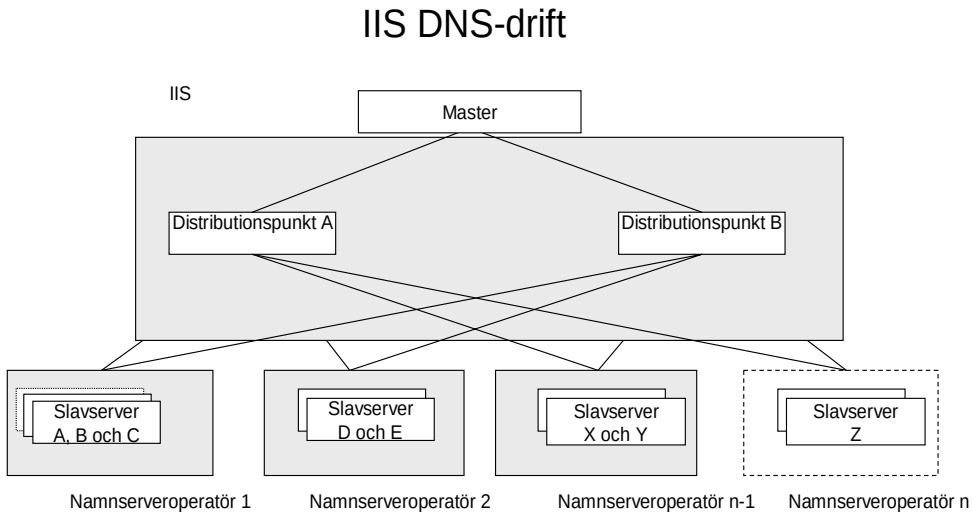
Zon används liksom en domän för att beskriva ett område i domännamnssystemet. En zon beskriver hur det administrativa ansvaret för domännamnssystemet delas upp mellan olika organisationer. Om man relaterar till begreppet domän finns i ovannämnda exempel två zoner; .se och pts.se. Var och en av zonerna förväntas administreras av olika organisationer som lagrar information om sin zon på den namnserver de själva ansvara för.

Zonfil är den DNS-databas som innehåller domännamn och motsvarande IP-adress för en viss zon. I detta fall är zonen .se.

Zonfilsöverföring är en överföring av zonfilen från masterservern till de sekundära namnservrarna.

Bilaga 2 - Domännamnssystemet för .se-zonen

För att förstå genomgång och analys av enkäten underlättar det om man känner till domännamnssystemets arkitektur. Alla webbplatser (domännamn) med toppdomänen .se tillhör .se-zonen. Det sätt på vilket domänadministratören har byggt upp den s.k. domännamnsarkitekturen bidrar i mycket hög grad till säkerheten i domännamnssystemet. Därför redogörs för den domännamnsarkitektur som .SE har byggt upp för .se-zonen.



Figur – *Driftsarkitektur för .se-zonen*

Hur fungerar processen, vad händer i .se-zonen vid tillkomsten av ett nytt domännamn?

I och med tillkomsten av ett nytt domännamn i .se-zonen registreras domännamnsinnehavaren, hans/hennes kontaktuppgifter, domännamn och dess motsvarande IP-adress i en s.k. kunddatabas. Tillkomst och borttagning av domännamn, ändring av namnservrars IP-adresser (ompekning) i .se-zonen sker över Internet och genom PGP-krypterade e-post på .SE:s eller .SE:s ombuds webbplatser. Från kunddatabasen extraheras de uppgifter som är nödvändiga för domännamnstjänsten, det vill säga domännamnet och den tilldelade IP-adressen för domännamnet. Dessa läggs i DNS-databasen eller den s.k. zonfilen. Masterservern innehåller zonfilen, varifrån den distribueras till de två distributionspunkterna och vidare till sekundära namnservrarna. Dessa

namnservrar förser i sin tur Internetanvändarna med översättningen mellan ”de svenska domännamnen” mot IP-adresser och omvänt. I dagsläget (2006) sker en zonfilsöverföring, med en uppdaterad zonfil, från masterservern till distributionspunkterna och vidare, varannan timme, dygnet runt. Skulle något fel i zonfilsöverföringen uppstå mot någon av distributionspunkterna hämtar de sekundära namnservrarna zonfilen från den andra distributionspunkten, samtidigt som övervakningssystemet larmar om problemet.

Domännamnssystemets beroenden

Domännamnssystemet som ligger till grund för Internet och som möjliggör att vi t.ex. kan vara ute och ”surfa” och att skicka e-post, är världens största och mest distribuerade databas. Domännamnssystemet är ett hierarkiskt uppbyggt system, om minst tre nivåer för att hantera (den globala) DNS-lastbalanseringen.

Det är värt att förtydliga och uppmärksamma skillnaden mellan domänadministratörens kontinuerligt fungerande namnserverdrift och respektive huvuddomäns fungerande namnserverdrift, det vill säga driften för respektive (underliggande) zon i exempelvis se-domänen.

När en (enda) webbplats i .se-zonen inte är tillgänglig kan det bero på att administratören för denna underliggande zon, dennes namnserver har slutat att vara tillgänglig eller fungera och därför kan den efterfrågade webbsidan inte visas. Detta har inget att göra med toppdomänadministratörens namnserverdrift att göra, utan är den underliggande zonens och administratörens ansvar.

Vidare, för att det överhuvudtaget ska kunna gå att erhålla DNS-information om toppdomänerna, måste aktuell och korrekt DNS-information om deras namnservrar finnas i rotzonen. (För detta krävs att toppdomänsadministratörerna har dokumenterade rutiner för hur kontakten med rotdomänadministratören ska gå till t.ex. vid ändring av IP-adress för en namnsserver eller tillkomst av ny namnserver för aktuell toppdomän.)

Den s.k. roten eller rotservern återfinns högst upp i DNS-systemhierarkin och innehåller information om IP-adresserna till toppdomänernas namnservrar. Det finns totalt tretton rotservrar i världen, varav en är placerad i Sverige.

En s.k. toppdomän återfinns på nivån under rotnivån. Toppdomänerna pekar ut officiella namnservrar/auktoritativa servrar för huvuddomäner. En toppdomän kan per definition vara en s.k. landsdomän eller en s.k. generisk domän. En landsdomän, även kallad ccTLD (country code TopLevelDomain), är en domän för en nation. En generisk toppdomän, även kallad gTLD (generic Top Level Domain) är en domän för specifikt ändamål t.ex. .org, .com, .edu, .gov, .biz eller en .arpa-domän vars uppgift är att bygga upp Internets infrastruktur. Det finns ca 260 toppdomäner för tillfället.

En huvuddomän ansvarar för att finna IP-adressen till det slutgiltiga domännamnet Internetanvändaren har eftersökt.

PTS tidigare undersökningar relaterade till domänadministratören

PTS har tidigare, i egenskap av sektorsmyndighet, vid ett flertal undersökt den svenska domänadministrationen. Exempel är utredningarna ”Säkra toppdomäner”, ”Strategi för ett säkrare Internet i Sverige” och ”Ökad tillit till Internet genom förbättrad säkerhet i domännamnssystemet” [5].

[5] PTS-ER-2004:19, 19 maj 2004, PTS-ER-2005:7, 15 maj 2005, respektive PTS-ER-2006:36, 12 oktober 2006

Bilaga 3 - Enkät

Frågor till Stiftelsen för Internet Infrastruktur, 2006-10-02

Namnservrarnas tekniska lösning, redundans, reservkapacitet och skydd

1) Vilka namnservrar ingår i .se-zonen idag, var är de geografiskt placerade och vilka är respektive namnservers uppdragstagare för driften?

2) Var och hur används anycast i namnserverdriften?

3) Vilken DNS-applikation och version körs på respektive namnserver?

4) Beskriv nätanslutningarna som ingår i driftsmiljön.

5) Beskriv hela kedjan i distributionsnätet för zonfilen.

6) Vilket logiskt och fysiskt skydd finns för att säkra DNS-driften?

7) På vilket sätt säkerställs nätanslutningar mellan

   a) masterserver och distributionspunkterna

   b) distributionspunkterna och slavservrarna

   c) slavservrarna och avlämningspunkterna

   med avseende på transmissionsmedium och redundans?

8)

   a) Hur stor är reservkapaciteten i slavservrarnas Internet-anslutningar under normalt DNS-trafikflöde?

   b) Hur stor är reservkapaciteten i slavservrarnas Internet-anslutningar under peak:ar i DNS-trafikflödet?

9) I vilken mån kan kapaciteten byggas ut i slavservrarnas anslutningar till Internet?

10) Redovisa driftstatistik för respektive namnserver under de tre senaste månaderna. Gärna i diagramform.

11) Hur stor är

   a) CPU-belastningen i genomsnitt/månad per namnserver?

   b) minnesbelastningen i genomsnitt/månad per namnserver?

12) Hur många namnservrar kan falla ifrån utan att svarstiden mot slutkunder påverkas?

13) Ifall utarbetad planläggning finns för framtida kapacitetskrav, beskriv eller bifoga densamma

14) Finns väldokumenterade instruktioner hur uppgradering av hårdvara respektive mjukvara ska gå till?

☐ Ja ☐ Nej

15) Hur ofta utförs normalt uppdateringar av hårdvara, mjukvara, omkonfigureringar, nyinstallationer etc. på mastern så att den måste tas ur drift och hur länge varar normalt ett sådant avbrott?

16) Hur ofta utförs normalt uppdateringar av hårdvara, mjukvara, omkonfigureringar, nyinstallationer etc. på slavservrar så att de måste tas ur drift och hur länge varar normalt sådana avbrott?

Övervakningssystemet

17) Vilken typ av information kan ni få ut av övervakningssystemet hösten 2006?

18) Beskriv på vilket sätt övervakningssystemet används (manuell övervakning, automatisk övervakning m.m.)

19)

a) Beskriv vilka typer av larm ni kan få från övervakningssystemet hösten 2006.

b) Finns automatiserat larm vid bortfall av en namnserver?

☐ Ja ☐ Nej

c) Finns automatiserat larm i händelse av otillgängligt nät?

☐ Ja ☐ Nej

Bortfall av server; återstart och felsökning

20) Finns dokumenterade rutiner för återstart samt felsökning vid bortfall av namnserver.

☐ Ja ☐ Nej

Kontinuerlig tillgänglighet till DNS i Sverige – driftsorganisation

21)

a) Finns personal som kontinuerligt, 24/7/365, övervakar DNS-systemet för .se-zonen?

☐ Ja ☐ Nej

b) ☐ Aktiv jour ☐ Stand by jour

22)

a) Finns personal som kontinuerligt, 24/7/365, kan vidta korrigerande åtgärder för DNS-systemet och .se-zonen?

☐ Ja ☐ Nej

b) Om ja, beskriv hur så sker.

23) Finns möjlighet för IIS till fjärradministration av .se-zonens namnservrar som IIS administrerar?

☐ Ja ☐ Nej

24) Finns möjlighet för slavserveroperatörer till fjärradministration av .se-zonens namnservrar?

☐ Ja ☐ Nej

25) Beskriv driftsorganisationen. Exempel på frågor som önskas svar på: finns en ytterst ansvarig person för drift, hur många personer har kompetens för att drifta de namnservrar som IIS hanterar, finns nödvändiga kontaktuppgifter till ytterst ansvariga?

26) Beskriv (era krav på) hur driftsorganisationen hos slavserveroperatörer ser ut (hur många personer har kompetens för att sköta namnserverdriften hos respektive slavserver, finns kontaktperson och ytterst ansvarig med kontaktuppgifter för namnserverdriften?)

Krav ställs på att data i .se-zonfilen samt i databasen är korrekt och tillförlitlig.

27) Vilka kriterier måste vara uppfyllda för att ett ombud skall vara godkänt?

28) Hur säkerställs ombudens åtkomst till och kommunikation med relevanta databaser och filer (autencitet, auktorisation, kryptering etc.)?

29) Ange ombudens åtkomsträttigheter (läsning, skrivning, ändring, borttag) för relevanta databaser och filer.

30) Hur skapas ny zonfil?

31) Vilken teknisk lösning och vilka säkerhetsåtgärder finns vid zonfilsöverföring?

32) Hur ofta sker zonfilsöverföring till slavservrarna och hur lång tid tar det?

33) Beskriv back-up-systemet för zonfilen.

Krav på att DNS-data är tillräckligt skyddat mot skada, manipulation eller förlust enligt bästa rimliga teknik.

34) Beskriv på vilket sätt DNS-datat är skyddat mot fysisk skada, manipulation eller förlust.

35) Hur många av slavservrarna kör DNSsec?

36) Hur många ISP:er i Sverige har infört DNSsec-stöd i namnservrar?

37) I vad mån har IIS informerat ICANN om DNSsec-testerna och de goda testresultaten?

38) Vid vilka tillfällen och hur ofta sker informationsutbyte med ICANN/IANA?

39) Hur fungerar informationsutbytet med ICANN/IANA?

Register

40) Beskriv kort rutinerna kring registerföring av tilldelade domännamn.

41) Hur ofta upprättas säkerhetskopior av registeruppgifterna?

42) Hur säkerställs att personuppgifter hanteras enligt Personuppgiftslagen (t.ex. hur och av vem inhämtas kundernas samtycke till publicering på Internet?)

Kontinuitetsplanering

43) Hur ser er kontinuitetsplan ut? Bifoga.

44) Under vilka förutsättningar aktiveras den?

45)

a) Har kontinuitetsplanen övats?

□ Ja □ Nej

b) Om ja, när övades den senast?

46) Beskriv era rutiner för incidenthantering (rutin för incidentrapportering, rapporteringsskyldighet m.m.)?

47) Finns rutiner för undvikande av nya incidenter?

48) Är ansvarsförhållandena reglerade vid avbrottssituationer?

□ Ja □ Nej

Ev. kommentar:

49) Finns instruktioner för hur avbrott av olika längd ska hanteras?

□ Ja □ Nej

Ev. kommentar:

50) Finns prioriteringar vid exceptionella händelser?

□ Ja □ Nej

Ev. kommentar:

51) I händelse av en omfattande störning, finns samordnad plan för återställelse till normal drift?

□ Ja □ Nej

Ev. kommentar:

52) Vilka alternativa kommunikationsformer till Internet och telefoni finns i sådana händelser?

53) På vilket sätt finns beredskap och kapacitet för att motstå olika former av störningar och attacker? T.ex. vilket skydd finns mot tillgänglighetsattacker för en namnserver?

Säkerhetsåtgärder vad gäller strömförsörjning, inbrott-, brand- och fuktlarm

54) Finns reservkraft till respektive namnserver?

□ Ja □ Nej

55) Hur lång tid tar det innan reservkraft sätter igång?

56) Hur lång tid räcker reservkraften under ”normal” belastning?

57) Finns fukt-, brand-, temperatur- och inbrottslarm hos varje slavserveroperatör?

□ Ja □ Nej

58) Finns dokumenterade rutiner för brand?

□ Ja □ Nej

59) Hur säkerställs in- och utpassage till och från namnservrar?

60) Har någon riktad attack skett mot .se-zonens namnservrar?

□ Ja □ Nej

61) Om ja på fråga 60, påverkades driften och vilka blev konsekvenserna?

62) Om ja på fråga 60, hur hanterade/löste ni dessa (drift)hot?

63) Om bortfall av en namnserver har inträffat, vilken är den vanligaste orsaken?

64) Ställer IIS krav på de SLA som slavserveroperatörerna avtalar med sina respektive ISP:er?

65) Vilka hot ser ni mot namnserverdriften i framtiden?