Datum	Vår referens	Aktbilaga
2013-06-04	Dnr: 12-10471	14

Nätsäkerhetsavdelningen
Andreas Dahlqvist
08-678 55 51
andreas.dahlqvist@pts.se

Stiftelsen för Internetinfrastruktur
Att: Elisabeth Ekstrand
Box 7399
103 91 Stockholm

Tillsyn rörande administrationen av den nationella toppdomänen för Sverige på internet, .se

Saken

Tillsyn rörande administrationen av den nationella toppdomänen för Sverige på internet, .se; nu fråga om avskrivning.

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) avskriver ärendet från vidare handläggning.

Bakgrund

PTS har vid flera tillfällen bedrivit tillsyn över Stiftelsen för Internetinfrastruktur (.SE) och hur .SE efterlever lagen (2006:24) om nationella toppdomäner för Sverige på internet (Toppdomänlagen). Under hösten 2006 inledde PTS ett tillsynsärende (PTS dnr. 06-14081) som inriktades på att kontrollera att lagens krav efterlevdes med särskilt fokus på att .SE bedrev en säker teknisk drift av den nationella toppdomänen för Sverige, .se.

Den 28 november 2012 inledde PTS tillsyn rörande administrationen av den nationella toppdomänen för Sverige på internet, .se, genom att inhämta upplysningar från .SE. I tillsynsskrivelsen ställde PTS omkring etthundra frågor om den tekniska driften av den nationella toppdomänen för Sverige på internet, se. Frågorna handlade bland annat om .SE:s

- övergripande säkerhetsarbete,
- namnservrars tekniska lösning, redundans, reservkapacitet och skydd,

- övervakningssystem och larm,
- åtgärder vid bortfall av server, återstart och felsökning,
- driftsorganisation,
- krav på att data i .se-zonen ska vara korrekt och tillförlitlig,
- krav på att DNS-data är tillräckligt skyddat mot skada, manipulation eller förlust enligt bästa rimliga teknik,
- register över tilldelade domännamn,
- kontinuitetsplanering,
- rutiner för risk-, driftsäkerhets- och incidenthantering,
- säkerhetsåtgärder vad gäller strömförsörjning, inbrotts-, brand-, och fuktlarm, samt
- bedömning av säkerhetshot mot den nationella toppdomänen, .se.

Den 15 januari 2013 inkom .SE med svar på de frågor som PTS hade ställt. De svar som .SE lämnade till PTS kan bland annat innehålla uppgifter om säkerhets- och bevakningsåtgärder och redogörs därför inte närmare för i detta beslut.

Den 5 april 2013 besökte PTS .SE för att ställa kompletterande frågor, få en mer detaljerad presentation av .SE:s övergripande riskanalys samt riskanalyser över specifika system, få tillfälle att ställa frågor till nyckelpersoner från särskilda verksamheter inom .SE samt få en praktisk demonstration av övervakningssystemen. PTS ställde även frågor om hur driften av .se-zonen påverkas av att .SE har tagit över driften av .nu samt blivit testpartner åt ICANN för nya toppdomäner.

Metod

Tillsynen har i huvudsak genomförts genom att PTS har ställt ett antal frågor till .SE som .SE har besvarat, se bilaga 1. Frågorna har följts upp med intervjuer av utvalda delar av .SE:s personal samt presentationer och fortsatta diskussioner hos .SE. PTS har på plats hos .SE inspekterat hur .SE:s övervaknings- och larmhanteringssystem ser ut och fungerar i praktiken.

Skäl

Tillämpliga bestämmelser

Enligt 5 § Toppdomänlagen ska en domänadministratör bedriva verksamheten på ett säkert och effektivt sätt i allmänhetens intresse. Domännamnsadministratören ska

1. lagra tilldelade domännamn och andra uppgifter som är nödvändiga för att stödja den del av domännamnssystemet som toppdomänen omfattar i en databas,
2. distribuera uppgifterna till namnservrarna för toppdomänen och se till att informationen i dessa är korrekt och lätt tillgänglig,
3. säkerställa en fungerande trafik mellan namnservrarna och Internet,
4. upprätthålla ett effektivt skydd av uppgifterna i toppdomänen,
5. ha personal med tillräcklig kompetens och erfarenhet för verksamheten, samt
6. ha sådana rutiner för verksamheten som uppfyller erkända standarder.

Av 6 § Toppdomänlagen framgår bl.a. att en domänadministratör ska föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.

Registret ska innehålla

1. domännamnet,
2. namnet på domännamnsinnehavaren och dennes postadress, telefonnummer och adress för elektronisk post,
3. namnet på den som tekniskt administrerar domännamnet och dennes postadress, telefonnummer och adress för elektronisk post,
4. uppgifter om de namnservrar som är knutna till domännamnet, samt
5. övrig teknisk information som behövs för att administrera domännamnet.

Uppgifterna i registret ska kunna hämtas utan avgift via internet.

Personuppgifter får dock göras tillgängliga på detta sätt endast om den registrerade har samtyckt till det.

PTS bedömning

Följande avsnitt utgår från 5 och 6 §§ Toppdomänlagen och följer strukturen i paragraferna. Varje avsnitt innehåller en övergripande beskrivning av vad .SE har framfört och avslutas med PTS bedömning i respektive del. I sista avsnittet finns PTS samlade bedömning.

.SE bedriver verksamheten på ett säkert och effektivt sätt (5 § 1 st. Toppdomänlagen)

.SE har beskrivit sin organisation för produktion, drift och underhåll av databas och zonfil samt sin säkerhetsorganisation. .SE har utpekade ansvariga för sitt drift- och informationssäkerhetsarbetet. .SE har även beskrivit sitt arbete med att tillämpa standardiserade metoder och teknologier för produktion, drift och underhåll av databas och zonfil. .SE ser till att tillämpa den senaste versionen av programvaror.

.SE har beskrivit sin domännamnsarkitektur samt kapacitet för att motstå driftstörningar till följd av logiska hot och har hög tillgänglighet för sina namnservrar. Det finns en primär namnserver i reserv som omedelbart kan tas i drift i händelse av att den ordinarie primära namnservern skulle drabbas av driftstörning eller av annat fel. Redundanta distributionspunkter förser de sekundära namnservrarna med den senaste uppdaterade zonfilen. Namnservrarna tillhandahålls av ett flertal leverantörer och är placerade på flera olika ställen i Sverige och i olika delar av världen. Både anycast- och unicast-teknik tillämpas för distribution av zonfilen för att skapa en redundant domännamnsarkitektur för .se-zonen. De sekundära namnserveroperatörerna tillämpar olika hårdvaruplattformar och namnserverprogramvara.

.SE har flera olika övervakningssystem för att säkerställa informationssäkerhet och driftsäkerhet för bland annat databas och zonfil. .SE testar att alla steg i kedjan från produktion till distribution samt zonfilens korrekthet fungerar inför varje uppdatering av zonfilen. Det finns personal som övervakar DNS-systemet för .se-zonen genom stand-by jour som på viss tid ska kunna reagera på larm från övervakningssystemet.

.SE har en förteckning över alla större planerade förändringsarbeten avseende mjukvaru- eller hårdvaruppdateringar som ska genomföras under ett visst år. SE har även beskrivit sin kapacitet för att motstå störningar till följd av fysiska hot och redovisat hur deras skalskydd ser ut, samt redogjort för åtgärder för att skydda mot brand-, fukt eller temperaturskada samt åtgärder vid förlust av strömförsörjning. .SE har ett sekundärt driftställe som kan tas i bruk om det primära driftstället skulle skadas eller på annat sätt förlora sin tillgänglighet. Reservkraften testas och verifieras och brandövningar sker regelbundet.

Mot bakgrund av ovanstående bedömer PTS att verksamheten idag bedrivs på ett säkert sätt.

Av det underlag som .SE har redovisat framkommer att .SE:s namnservrar har en hög tillgänglighet och att namnserverssystemet idag är robust och har hög logisk och geografisk redundans. Det får därmed anses att verksamheten idag också bedrivs på ett effektivt sätt.

P 1. tilldelade domännamn och andra uppgifter som är nödvändiga för att stödja den del av domännamnssystemet som toppdomänen omfattar lagras i en databas

.SE har beskrivit hur nödvändiga uppgifter överförs och lagras i databasen. .SE säkerställer att nödvändiga uppgifter finns för .se-zonen bl.a. genom sitt gränssnitt och applikation med standarden Extensible Provisioning Protocol (EPP). Det är ett protokoll är anpassat för kommunikation mellan registrarer (.SE:s ombud för bl.a. registrering av domännamn) och en domänadministratör (registry) för att t.ex. kunna registrera och förnya domännamnsinformation.

P 2. .SE distribuerar uppgifterna till namnservrarna för toppdomänen och ser till att informationen i dessa är korrekt och lätt tillgänglig

.SE har beskrivit vilken teknisk lösning som används för distribution och vilka säkerhetsåtgärder som vidtas vid .se-zonfilsöverföring. En ny zonfil genereras och distribueras ett flertal gånger varje dag till en särskild namnserver. Flera tester av .se-zonfilen genomförs för att verifiera dess korrekthet. Den särskilda namnservern signerar .se-zonfilen med DNSSEC och skickar en notifiering till distributionspunkter. När distributionspunkterna får notifieringen hämtas den nya zonfilen. Distributionspunkterna notifierar de sekundära namnservrarna som hämtar den nya zonfilen. Överföringen av zonfilen sker krypterat.

.SE har flera olika övervakningssystem. Till exempel finns övervakningssystem som kontrollerar tillgängligheten till den primära namnservern, distributionspunkterna och de sekundära namnservrarna samt att informationen är korrekt. Det finns även övervakningssystem som övervakar loggar i produktionssystemet för .se-zonfil, och som rapporterar avvikelser.

De åtgärder som .SE vidtar i detta avseende får idag anses tillräckliga för att se till att informationen i namnservrarna är korrekta och lätt tillgängliga.

P 3. .SE säkerställer en fungerande trafik mellan namnservrarna och internet

.SE har uppgett att från den primära namnservern finns redundanta separata fibervägar till distributionspunkterna. Anslutningarna mellan distributionspunkterna och de sekundära namnservrarna har en kapacitet på 100 Megabit per sekund. .SE säkerställer tillgängligheten till de sekundära namnservrarna genom avtal om tillgänglighet med de sekundära namnserveroperatörerna. .SE ställer även krav på antal DNS-transaktioner per sekund och på svarstider för de sekundära namnservrarna.

.SE har övervakningssystem över bland annat de sekundära namnservrarna och har löpande kontakt med de sekundära namnserveroperatörerna och ser över sina avtal med dem vid behov. .SE har enligt avtalen rätt att genomföra revision hos de sekundära namnserveroperatörerna.

Även om det inte är möjligt att skydda sig från varje avbrott i anslutningsmöjligheten, får detta idag anses vara rimliga åtgärder för att säkerställa en fungerande trafik mellan namnservrarna och internet.

P 4. .SE upprätthåller ett effektivt skydd av uppgifterna i toppdomänen

.SE har beskrivit på vilket sätt DNS-data är skyddat mot skada, manipulation och förlust. Åtkomstkontroller till databasen med relevanta uppgifter för .se-zonfil genomförs t.ex. för registrarer på flera nivåer. Överföringen av uppgifterna från registrarer till databasen sker krypterat. Skydd mot manipulation av DNS-data sker med användning av DNSSEC. Dessutom används krypterade förbindelser för att överföra zonfilen t.ex. mellan primär server och distributionspunkterna, samt mellan distributionspunkterna och de sekundära namnservrarna. Det finns en fastställd grundskyddsnivå för .SE registry. För hanteringen av DNS-data finns kompletterande säkerhetsåtgärder som beskrivs i en systemsäkerhetsplan. Samtliga sekundära namnservrar kör också DNSSEC.

Även om det vore bra och lämpligt att verifiera att säkerhetskopiorna av zonfilen i de olika lagringsmedia med säkerhetskopiorna är identiska, anser PTS att grundskyddet och de kompletterande säkerhetsåtgärderna för DNS-data sammantaget får anses utgöra ett effektivt skydd av uppgifterna i toppdomänen.

P 5. .SE har personal med tillräcklig kompetens och erfarenhet för verksamheten

.SE har uppgett att kompetens är ett prioriterat område och att de fokuserar på att rekrytera kompetenta medarbetare och utveckling av befintliga medarbetare. Varje medarbetare på .SE erbjuds den utveckling som behövs för att bidra till verksamhetens utveckling och kunna möta interna och externa krav.

Kompetens i nyckelfunktioner speglas så att det finns flera personer som har liknande eller samma kompetens.

.SE har en strategi och processer för kompetensöverföring, kontinuerlig vidareutbildning, erfarenhets- och kompetensutbyte med bland annat andra toppdomänadministratörer, domännamnssystemtillverkare och DNS-operatörer.

.SE bedriver omvärldsbevakning om nya standarder och teknologier, har externa nationella och internationella nätverk med kunniga inom DNS-drift och namnserverprogramvaror.

.SE får därmed anses ha de personella förutsättningar som krävs för att klara administrationen av den nationella toppdomänen.

P 6. .SE har sådana rutiner för verksamheten som uppfyller erkända standarder

.SE tillämpar standardiserade processer och rutiner för produktion, drift och underhåll av .se-zonen och databasen. Processerna och rutinerna är förankrade i organisationen samt är dokumenterade. .SE har dokumenterad informationssäkerhetsmanual, informationssäkerhetspolicy, policy och plan för krishantering, rutiner för internrevision, särskilda systemsäkerhetsplaner, säkerhetshandbok, säkerhetsinstruktioner för drift samt för personal för administration och förvaltning och checklista för resor. Dokumentationen ses över regelbundet och övningar kris- och kontinuitetsplanen sker en gång per år. .SE har också certifierats enligt standarden SS-ISO/IEC 27001:2006, Ledningssystem för informationssäkerhet, för sin domänverksamhet. .SE tillämpar även vedertagna internetstandarder som tas fram av Internet Engineering Task Force (IETF).

Av den beskrivning av säkerheten för verksamheten som .SE har lämnat framkommer att säkerhetsarbetet idag bedrivs i enlighet med bästa möjliga praxis i enlighet med erkända standarder.

Registret över tilldelade domännamn innehållande personuppgifter publiceras på internet endast om den registrerade samtyckt till det

.SE har uppgett att endast för- och efternamn visas i den publika söktjänsten på internet. Om en innehavare återkallar sitt samtycke till att få sitt namn publicerat på internet så hanteras detta av jurist hos .SE. Från och med den 3 juni 2013 publiceras inte personuppgifter om domännamnsinnehavare på internet. Den som vill veta vem som står bakom ett visst domännamn måste numera vända sig till .SE på annat sätt för att erhålla den informationen.

Någon skyldighet för .SE att inhämta samtycke för publicering av personuppgifter på internet finns inte. PTS bedömer att .SE hanterar registret över tilldelade domännamn i enlighet med reglerna i Toppdomänlagen.

Samlad bedömning

Av vad som framkommit vid nu aktuellt tillsynsärende bedriver .SE idag verksamheten på ett säkert och effektivt sätt i allmänhetens intresse och att registret över tilldelade domännamn hanteras i enlighet med reglerna i Toppdomänlagen. Ärendet avskrivs därför från vidare handläggning.

Hur man överklagar

Beslutet kan inte överklagas.

Beslutet har fattats av avdelningschefen Annica Bergman. I ärendets slutliga handläggning har även enhetschefen Helena Åkerlund, enhetschefen Patrik Bystedt, enhetschefen Ove Landberg, Erika Hersaeus (föredragande) och juristen Andreas Dahlqvist (föredragande) deltagit.

Frågor till Stiftelsen för Internet Infrastruktur

Med primär namnserver avses namnserver som IIS ansvarar för och driver.
Med sekundär namnserver avses namnserver som drivs av namnserveroperatör.
Med distributionspunkt avses IIS avlämningspunkt mot namnserveroperatör.

1. Övergripande frågor om IIS säkerhetsarbete

1.1)

a. Finns en säkerhetsorganisation med ansvar för driftsäkerhet- och informationssäkerhet vid administrationen av den nationella toppdomänen för Sverige på Internet, .se,?
□ Ja □ Nej

b. Om ja, beskriv hur säkerhetsorganisationen ser ut.

c. Om ja, beskriv hur det löpande och förebyggande säkerhetsarbetet bedrivs samt förvaltas.

1.2) Vilka standardiserade processer och metoder tillämpar IIS vid produktion och drift av .se-zonen?

1.3) Hur arbetar IIS kontinuerligt med att se över sitt informationssäkerhets- och driftsäkerhetsarbete?

1.4) Hur övas rutiner rörande IIS säkerhetsarbete?

1.5) Hur förvaltas IIS rutiner rörande säkerhetsarbete?

2. Namnservrarnas tekniska lösning, redundans, reservkapacitet och skydd

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

2.2) Var och hur används anycast i namnserverdriften?

2.3) Vilket eller vilka operativsystem och versioner av dessa används för namnservrarna och om olika operativsystem och versioner förekommer hur är de fördelade?

Post- och telestyrelsen

Postadress: Box 5398 102 49 Stockholm
Besöksadress: Valhallavägen 117 www.pts.se
Telefon: 08-678 55 00 Telefax: 08-678 55 05 pts@pts.se

2.4)
a. Tillämpar IIS standardiserade rutiner för när och hur uppgradering av DNS-applikationer ska ske?
□ Ja □ Nej
b. Om ja, beskriv rutinerna för uppgradering av DNS-applikationerna.

2.5) Beskriv nätanslutningarna som ingår i driftsmiljön.

2.6) Beskriv hela kedjan i distributionsnätet för zonfilen.

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

2.8) På vilket sätt säkerställs nätanslutningar mellan
a. primär namnserver och distributionspunkterna,
b. distributionspunkterna och sekundära namnservrar, och
c. sekundära namnservrar och avlämningspunkterna med avseende på transmissionsmedium och redundans?

2.9) Hur stor är reservkapaciteten i de sekundära namnservrarnas internetanslutningar
a. under normalt DNS-trafikflöde?
b. under toppar i DNS-trafikflödet?

2.10) Vilka krav ställer IIS på antalet DNS-transaktioner/sekund samt svarstid för sina namnservrar?

2.11) Redovisa driftstatistik för respektive namnserver fr.o.m. den 1 augusti 2012 t.o.m. 30 november 2012. Gärna i diagramform.

2.12) Hur många namnservrar kan sluta fungera utan att svarstiden mot slutkunder påverkas?

2.13) Beskriv IIS plan för utbyggnad av kapacitet i de sekundära namnservrarnas anslutning till internet.

2.14) Om plan finns för framtida kapacitetsutbyggnad, beskriv eller bifoga densamma.

2.15) Tillämpar IIS standardiserade processer och metoder för uppgradering av mjukvara och hårdvara?
□ Ja □ Nej
Om ja, vilka standardiserade processer och metoder tillämpas?

2.16) Finns dokumenterade instruktioner hur uppgradering av hårdvara respektive mjukvara ska gå till?

□ Ja □ Nej
Om ja, bifoga.

2.17) Hur ofta utförs uppdateringar av hårdvara, mjukvara, omkonfigureringar, nyinstallationer etc. på primär namnserver så att den måste tas ur drift och hur länge varar ett sådant avbrott i genomsnitt?

2.18) Hur ofta utförs uppdateringar av hårdvara, mjukvara, omkonfigureringar, nyinstallationer etc. på sekundära namnservrar så att de måste tas ur drift och hur länge varar sådana avbrott i genomsnitt?

2.19) Används IPv6
a. i den tekniska administrationen av .se-zonfil?
□ Ja □ Nej
b. för överföring av .se-zonfil till primär namnserver?
□ Ja □ Nej
c. för överföring av .se-zonfil till sekundära namnservrar?
□ Ja □ Nej
d. för andra funktioner eller tjänster?
□ Ja □ Nej
e. Om ja, för vilka?

2.20) Bedömer IIS att det finns någon risk med att använda IPv6 i den tekniska administrationen och överföringen av .se-zonfil?
□ Ja □ Nej

2.21) Om ja, vilka risker har IIS identifierat och vilka åtgärder har IIS vidtagit för att förhindra/minimiera effekterna om dessa inträffar?

3. Övervakningssystem och larm

3.1) Vilka övervakningssystem finns för driften av .se-zonfil, domännamnssystemet, kunddatabasen, whois-registret och extensible provisioning protocol (EPP)-systemet?

3.2) Vilken typ av information kan IIS få ut av övervakningssystemen?

3.3) Beskriv vilka förbättringar eller förändringar som har skett av övervakningssystem och larm sedan januari 2007.

3.4) Hur arbetar IIS med övervakningssystemen?

3.5) När och hur utvärderar IIS övervakningssystemen?

3.6) Beskriv vilka typer av larm IIS kan få från övervakningssystemen.

4. Bortfall av server, återstart och felsökning

4.1) Beskriv IIS rutiner för återstart och felsökning vid bortfall av namnserver.

5. Driftsorganisation

5.1)Finns personal som har

a. kontinuerlig, 24/7/365, övervakning av DNS-systemet för .se-zonen?
   □ Ja □ Nej

b. □ Aktiv jour och/eller □ Stand-by jour för övervakning av DNS-systemet för .se-zonen?

5.2)

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.

5.3) Beskriv utförligt IIS driftsorganisation för den nationella toppdomänen för Sverige på Internet.

5.4) Beskriv hur IIS ser över krav i SLA:er med sekundära namnserveroperatörer samt hur samarbete med dessa sker.

5.5)

a. Beskriv utförligt IIS plan för kompetensförsörjning för den tekniska driften av den nationella toppdomänen för Sverige på Internet.

b. Hur säkerställer IIS att personal är ständigt uppdaterad på de senaste inom sitt område, är tillräckligt kompetent och kan hantera de tekniska systemen?

5.6) Hur arbetar IIS med att undvika personberoenden?

5.7) Beskriv på vilket sätt och hur ofta kontroller av personal med nyckelfunktioner för den tekniska driften av den nationella toppdomänen för Sverige på Internet utförs.

5.8) Har IIS någon resepolicy? □ Ja □ Nej
Om ja, bifoga den.

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

6.1) Vilka kriterier måste vara uppfyllda för att en registrar ska godkännas?

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

6.3) Ange registrarernas åtkomsträttigheter (läsning, skrivning, ändring, borttagning) för relevanta databaser och filer.

6.4) Hur skapas ny zonfil? Beskriv även i svaret på frågan hur informationssäkerhet och driftsäkerhet säkerställs i produktionen av zonfilen.

6.5) Vilken teknisk lösning och vilka säkerhetsåtgärder finns vid zonfilsöverföring? Bifoga gärna schematisk bild.

6.6) Hur ofta sker zonfilsöverföring till de sekundära namnservrarna och hur lång tid tar det?

6.7) Beskriv back-up-systemet för zonfilen.

6.8) IIS har upprättat en informationssäkerhetspolicy. Bifoga den.

6.9) Hur tillämpar IIS i praktiken sin informationssäkerhetspolicy?

6.10) Hur förankras informationssäkerhetspolicyn i organisationen?

6.11) Hur håller IIS informationssäkerhetspolicyn uppdaterad?

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

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

7.2) Hur många av de sekundära namnservrarna kör DNSSEC?

7.3) Beskriv IIS rutiner inklusive ev. roller för att signera zonfilen.

7.4) Beskriv IIS rutiner för att genomföra en roll back/återställelse om en felaktig uppdatering har inträffat zonfilen.

7.5)

a. Bedömer IIS att det finns några risker med att använda DNSSEC?
   Ja □ Nej □
b. Om ja, på vilket sätt arbetar IIS med riskhantering och -minimering vid användning av DNSSEC?

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

7.7) Fungerar informationsutbytet med IANA på ett tillfredställande och effektivt sätt?
Ev. kommentar.

7.8) Kan IPv6 för närvarande användas vid kommunikation med IANA?
Ja □ Nej □

8. Register

8.1) Beskriv rutinerna kring registerföring av tilldelade domännamn.

8.2) Hur säkerställs kvalitet i registret?

8.3) Hur säkerställs en tillfredställande tillgänglighet till registret?

8.4) Hur ofta upprättas säkerhetskopior av registeruppgifterna?

8.5) Hur ofta testas och verifieras återställande av registret från säkerhetskopior?

8.6) I vilken utsträckning publiceras personuppgifter från registret över tilldelade domännamn på internet?

8.7) Hur hanterar IIS återkallelse av samtycke till publicering av personuppgifter från registret på internet?

8.8) Hur hanterar IIS personuppgifter i registret efter det att samtycke återkallats av en registrerad?

9. Kontinuitetsplanering

9.1) Hur ser IIS kontinuitetsplan ut? Bifoga.

9.2) Under vilka förutsättningar aktiveras den?

9.3)
a. Har kontinuitetsplanen övats?
□ Ja □ Nej
b. Om ja, när övades den senast?

9.4) Hur arbetar IIS med att förankra kontinuitetsplanen i organisationen?

9.5) Hur hålls kontinuitetsplanen uppdaterad?

9.6) Hur ser IIS krishanteringsplan ut? Bifoga.

9.7)
a. Har krishanteringsplanen övats?
□ Ja □ Nej
b. Om ja, hur ofta har den övats och när övades den senast?

9.8)
a. Har krishanteringsplanen någon gång tillämpats i skarpt läge?
□ Ja □ Nej
b. Om ja, beskriv händelsen och hur den hanterades.

9.9) Hur arbetar IIS med att förankra krishanteringsplanen i organisationen?

9.10) Hur hålls krishanteringsplanen uppdaterad?

10. IIS rutiner för risk-, driftsäkerhets- och incidenthantering

10.1) Beskriv IIS rutiner för incidenthantering (rutin för incidentrapportering, rapporteringsskyldighet, uppföljning m.m.).

10.2) Hur många driftsäkerhets- och informationssäkerhetsrelaterade incidenter per år har inträffat mellan den 1 januari 2008 och 1 januari 2012.

10.3) Hur många driftsäkerhetsrelaterade och integritetsrelaterade incidenter har inträffat under 2012?

10.4) Har IIS upprättat årliga utvärderingar utifrån sammanställningar av IIS:s incidentrapporter för åren 2007–2011?
□ Ja □ Nej
Om ja, Bifoga.

10.5) Är ansvarsförhållandena reglerade vid avbrottssituationer?
□ Ja □ Nej
Ev. kommentar:

10.6) Finns instruktioner för hur avbrott av olika längd ska hanteras?
□ Ja □ Nej
Ev. kommentar:

10.7) Finns prioriteringar vid exceptionella händelser?
□ Ja □ Nej

Ev. kommentar:

10.8) I händelse av en omfattande störning, finns samordnad plan för återställning till normal drift?
□ Ja □ Nej
Ev. kommentar:

10.9) 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?

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

11.1)
a. Finns reservkraft till respektive namnserver?
□ Ja □ Nej
b. Vilken typ av reservkraft används?

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

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

11.4) Hur ofta testas och verifieras att reservkraften fyller sin funktion?

11.5)
a. Finns fukt-, brand-, temperatur- och inbrottslarm för IIS primära och sekundära driftställe?
□ Ja □ Nej
b. Finns fukt-, brand-, temperatur- och inbrottslarm hos varje sekundär namnserveroperatör?
□ Ja □ Nej

11.6) Hur ofta sker brandövning vid IIS primära och sekundära driftställe?

11.7) Hur säkerställer IIS driften av den svenska toppdomänen, .se i händelse av att IIS primära driftställe sätts ur funktion?

11.8)
a. Har IIS övat på att starta om/upp/återta driften vid sitt sekundära driftställe?
□ Ja □ Nej
b. Om ja, när genomförde IIS en sådan övning senast? Vilka erfarenheter drog IIS av denna övning?

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

12. Säkerhetshot mot den nationella toppdomänen

12.1) Avseende de tre allvarligaste DDoS-attackerna mot .se-zonen, hur påverkades driften och vilka blev konsekvenserna?

12.2) Avseende de tre allvarligaste DDoS-attackerna, hur hanterade/löste IIS dessa (drift)hot?

12.3) Vilken är den vanligaste orsaken till bortfall av en namnserver?

12.4) Hur arbetar IIS med vidtagande av åtgärder sett till identifierade hot och/eller risker vid genomförande av risk- och sårbarhetsanalys samt vid uppföljning av inträffade incidenter?

12.5) Vilka hot ser IIS mot den tekniska administrationen av den nationella toppdomänen för Sverige på Internet, .se, i framtiden?

13. Övrigt

13.1) Beskriv IIS arbete med omvärldsbevakning.