

Vår referens: 21–8995, Aktilaga: 7

Beslut – avskrivning av tillsyn över den tekniska driften av toppdomänen .se

Part

Stiftelsen för internetinfrastruktur (Internetstiftelsen), 802405–0190

Saken

Tillsyn avseende teknisk drift 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

I Lag (2006:24) om nationella toppdomäner för Sverige på internet (toppdomänlagen) finns övergripande bestämmelser om den tekniska driften av nationella toppdomäner för Sverige på internet. Det finns även bestämmelser som reglerar förande av register, tilldelning och registrering av domännamn och tillhandahållandet av ett effektivt tvistlösningsförfarande.

PTS är tillsynsmyndighet över toppdomänlagen. PTS roll som tillsynsmyndighet är att granska och kontrollera att toppdomänlagen följs. Tillsyn kan inledas både händelsestyrt och planlagt. Detta innebär att tillsyn kan föräledas av en specifik händelse, men kan även inledas utan att något specifikt har skett. Planlagd tillsyn är en del av PTS kontinuerliga arbete för att säkerställa att kraven i toppdomänlagen följs.

Det är viktigt att den tekniska driften av den nationella toppdomänen för Sverige på internet sköts på ett säkert och effektivt sätt i allmänhetens intresse och att verksamheten i övrigt följer toppdomänlagen.

PTS beslutade den 1 juli 2021 att inleda planlagd tillsyn för att inhämta information om Internetstiftelsens administration av toppdomänen för Sverige på internet med avseende på den tekniska driften. Syftet med tillsynen har varit att få en övergripande bild av

Internetstiftelsens efterlevande av 5 § toppdomänlagen. PTS har därför begärt in svar på ett antal frågor om hur Internetstiftelsen, med utgångspunkt i 5 § toppdomänlagen, hanterar och realiserar den tekniska driften av toppdomänen .se.

Internetstiftelsens yttrande

Internetstiftelsen har i sitt svar till PTS på ett övergripande sätt beskrivit processen för lagring av domännamn och på vilket sätt lagringen sker samt hur processen för att distribuera uppgifterna till namnservrarna för toppdomänen ser ut.

Vidare har Internetstiftelsen beskrivit hur de säkerställer att informationen i namnservrarna är korrekt och lätt tillgänglig, hur de säkerställer en fungerande trafik mellan namnservrarna och internet, samt hur de realiserar och upprätthåller ett effektivt skydd av uppgifterna i toppdomänen, både avseende driftsäkerhet och integritetsskydd.

Slutligen har Internetstiftelsen också beskrivit hur de säkerställer att personalen har tillräcklig kompetens och erfarenhet för verksamheten, vilka verksamhetsrutiner de arbetar efter samt hur de följer upp nya och/eller förändrade standarder.

Internetstiftelsen har anfört bland annat följande;

Alla tilldelade domännamn lagras i systemets relationsdatabas med tillhörande information såsom innehavare, registrarer och DNS-delegeringar. Informationen i databasen uppdateras i takt med att förändringar sker av respektive domännamns registrar, exempelvis vid nyregistrering, omdelegering och avregistrering. För spårbarhet sparas även, utöver aktuella data, historik över samtliga förändringar som skett avseende domännamn. Innan en förändring accepteras sker ett antal kontroller.

Identiteten hos systemanvändaren (registraren) som begär förändringen säkerställs genom ett autentiseringsförfarande med flera faktorer, det kontrolleras att systemanvändaren har rätt att utföra förändringen för det aktuella domännamnet och all indata valideras mot gällande policys. Efter att dessa kontroller genomförts med lyckat resultat registreras förändringen i databasen och kvitteras tillbaka till användaren.

Informationen för samtliga .se-domännamn som pekats ut med DNS-data samlas i zonfiler som förs över till de auktoritativa namnservrarna för .se-zonen. .se-zonen uppdateras varje timme 24/365. För att DNS-tjänsten för .se ska vara robust används fler än en auktoritativ namnserver för att informera om en och samma zon. Internetstiftelsens primära namnserver är den som hämtar zonfilen direkt från de interna systemen. Därifrån hämtar sekundära namnserverar zonfilen för distribution på internet. Grunden för Internetstiftelsens strategi för

sekundära namnservrar är att ha en god stabilitet och robusthet i domännamnsystemet (DNS). Det innebär bland annat att risker för manipulering av data hanteras genom signering av zonfilen med DNSSEC och starka algoritmer samt att risker för otillgänglighet på grund av överbelastning hanteras genom diversifiering (flera leverantörer, Unicast- och Anycast-protokoll, olika operativsystem och olika DNS-programvaror).

Internetstiftelsen driftar sekundär namnservrar (Unicast) i egen regi samt har utöver det tre externa leverantörer av sekundära namnservrar.

Informationen överförs med kryptering till sekundära namnservrar/leverantörer, vilket minimerar risken att information blir manipulerad i överföringen. Signering med DNSSEC förhindrar manipulation av data. Sekundära namnservrar övervakas kontinuerligt via Internetstiftelsens övervakningssystem, och även av organisationen RIPE genom deras tjänst DNSMON.

Testdomäner, vilka ändras vid varje zonuppdatering, används som övervakning av att rätt zondata distribueras ut och är oförändrad samt tillgänglig på de sekundära namnservrarna. Genom redundans, failover och en disaster recovery-miljö finns en god grund för 100 procent tillgänglighet till DNS-tjänsten. För skydd av information används kryptering, och övervakning sker med en rad kontrollmekanismer med tillhörande larm och rutiner för att hantera eventuella händelser.

Internetstiftelsen har dedikerade länkförbindelser mellan sina datacenter vilket betyder att det bara är Internetstiftelsen som använder dessa. Utöver det så skyddas alla förbindelser med kryptering. Samma sak gäller för de servrar där Internetstiftelsen förvarar data. Den privata nyckeln hanteras enligt strikta rutiner och processer som innefattar både spårbarhet och utökad säkerhet. Tvåfaktorsautentisering tillämpas för alla kritiska system.

Internetstiftelsens IT-avdelning arbetar kontinuerligt med att skapa, underhålla och avyttra dokumentation för systemen. Medarbetare har en individuell kompetensutvecklingsplan med utgångspunkt i det egna primäransvarsområdet.

Som toppdomänadministratör verkar Internetstiftelsen på den tekniska sidan i enlighet med Best Common Practice (BCP) när det gäller drift av deras system. BCP omfattar komponenter som redundans och diversifiering för hög tillgänglighet. Internetstiftelsen följer även relevanta standarder från Internet Engineering Task Force (IETF) och deltar i standardiseringsarbetet inom IETF på de områden som har växt fram under senare tid. Internetstiftelsen genomför regelbundet externa säkerhetsgranskningar av nya och förändrade funktioner i sina verksamhetskritiska system. Av flera skäl är det strategiskt viktigt för Internetstiftelsen att delta i olika internationella forum, för att finna rätt samarbetspartner för sina satsningar, för att öka sin egen och andras kompetens samt för att

delge och ta del av andras erfarenheter. Council of European National Top-Level Domain Registries (CENTR), DNS Operations, Analysis, and Research Center (DNS-OARC) och de europeiska nationella toppdomänadministratörerna är Internetstiftelsens främsta arena för internationella samarbeten inom administration av domännamn och DNS. Även kontinuerligt deltagande i internationellt arbete inom Internet Corporation for Assigned Names and Numbers (ICANN), IETF och andra internationella forum är av stor vikt för att bibehålla och öka Internetstiftelsens DNS-kompetens. Internetstiftelsen har medarbetare som deltar aktivt i IETF:s standardiseringsarbete.

Skäl

Tillämpliga bestämmelser

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

1. lagra tilldelade domännamn och andra uppgifter som är nödvändiga för att stödja den del av domännamssystemet 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 10 § toppdomänlagen och 2 § förordning (2006:25) om nationella toppdomäner för Sverige på Internet framgår att PTS ska ha tillsyn över efterlevnaden av lagen och av föreskrifter som har meddelats med stöd av lagen.

Enligt 11 § toppdomänlagen ska en domänadministratör bl.a. på tillsynsmyndighetens begäran lämna den information och bereda den tillgång till utrustning och annat som behövs för tillsynen.

PTS bedömning

Syftet med denna tillsyn har varit att få en övergripande bild över hur Internetstiftelsen sköter den tekniska driften av toppdomänen utifrån de krav och bestämmelser som återfinns i 5 § toppdomänlagen. PTS anser att de svar som Internetstiftelsen inkommit med, visar att Internetstiftelsen sköter den tekniska driften av toppdomänen på ett tillfredställande sätt. Internetstiftelsen har inte heller under de senaste fem åren drabbats av någon incident som påverkat tillgänglighet och/eller riktighet i informationen i namnservrarna. Trafiken mellan

namnservrarna och internet eller skyddet av uppgifterna i toppdomänen har inte heller påverkats av någon incident under samma period.

Mot denna bakgrund ser PTS inte skäl att vidta någon ytterligare åtgärd inom ramen för detta tillsynsärende. Ärendet ska därför avslutas utan vidare åtgärder.

Beslutet har fattats av enhetschefen Robert de Try. I ärendets slutliga handläggning har även Claes Hultholm (föredragande) och Bo Martinsson deltagit.

