Post- og teletilsynet
Norwegian Post and Telecommunications Authority

UNINETT Norid AS
.
7465 TRONDHEIM

Vår ref.: 1200253-5 -
Vår dato: 18.12.2012

Deres ref.: NOA07/12-HAO
Deres dato: 30.5.2012

Saksbehandler:
Elise K. Lindeberg

www.npt.no

Tilsynsrapport - tilsyn med UNINETT Norid AS 2012

Post- og teletilsynet (PT) har i 2012 gjennomført tilsyn hos UNINETT Norid AS (Norid) for å kartlegge og vurdere forhold knyttet til sikkerheten og stabiliteten ved administrasjon av landkodetoppdomenet .no.

Nedenfor følger rapport fra gjennomført tilsyn, med gjennomgang av spørsmålene som er stillet av PT og gjennomgang av informasjon og dokumentasjon som er sendt inn av Norid. PT har foretatt en sammenfatning og vurdering under tilsynets hovedpunkter.

Bakgrunn for tilsyn

Samferdselsdepartementet (SD) har det overordnede ansvaret for samfunnssikkerhet og beredskap i samferdselssektoren, herunder elektronisk kommunikasjon. I 2007 gjennomførte SD en analyse av sårbarhet og risiko innen samferdsel og i et tverrsektorielt perspektiv.

På bakgrunn av ovennevnte analyse utarbeidet SD i 2009 «strategi for samfunnssikkerhet og beredskap i samferdselssektoren». Her fremheves det overordnede målet for arbeidet med samfunnssikkerhet og beredskap, som er å forebygge uønskede hendelser og minske følgene av disse dersom de skulle oppstå - for å kunne sikre samfunnets behov for transport og kommunikasjon. Det påpekes at etater og tilknyttede virksomheter under SD har et selvstendig ansvar for samfunnssikkerhet og beredskap i egen sektor, herunder beskyttelse av kritisk infrastruktur.

PT har et særskilt myndighetsansvar for sikkerhet og beredskap innen elektronisk kommunikasjon, og har ansvar for tilsyn med sentrale internettressurser som domenenavnsystemet (DNS) og internettadresser. PT har tilsynsansvar for registerenheten som har ansvar for drift av våre nasjonale toppdomener, Norid, jf. Lov om elektronisk kommunikasjon (ekomloven) §§ 7-1 og § 10-1, 2 ledd og Forskrift om domenenavn under norske landkodetoppdomener (domeneforskriften) § 9.

Statistikk basert på markedsundersøkelser foretatt av Norid i det norske markedet viser at flertallet av norske organisasjoner og virksomheter på Internett foretrekker å benytte .no adresser som sitt hovedkontaktpunkt. Vår «nasjonale del» av Internett, ved toppdomenet .no, er således en viktig kanal for offentlig og privat kommunikasjon og for innovasjon og næringsutvikling. Sikkerhet og videreutvikling av våre nasjonale domenenavnsressurser er et nasjonalt ansvar.

Ved forvaltning av en sentral samfunnsressurs som .no, vil det måtte foretas en løpende vurdering og avveining av hensyn som sikkerhet, stabilitet, brukervennlighet og effektivitet. Det vises også til domeneforskriften § 3, der det er opplistet hvilke hensyn som skal ivaretas ved Norids utforming av tildelingsreglene for .no. Her er kostnadseffektivitet, høy teknisk kvalitet, ikke-diskriminerende, åpenhet, forutberegnelighet og brukernes og nasjonale interesser opplistet som prioritet.

PT har gjennomført tilsyn med Norid for å kartlegge og foreta en vurdering av sikkerhet, stabilitet og generell administrasjon/drift av no. En sikker og samtidig effektiv administrasjon av våre nasjonale domeneressurser er viktig for tillitten ute hos brukerne og for å bidra til fortsatt vekst i det norske internettmarkedet.

Gjennomføring av tilsyn

PT gjennomførte et forberedende tilsynsmøte med Norid i november 2011 i Norids lokaler i Trondheim. Sentrale tema og fokusområder ble drøftet, og PT gjennomgikk plan for videre gjennomføring av tilsyn.

I februar 2012 oversendte PT en rekke spørsmål til Norid der vi bad om informasjon og dokumentasjon om registreringssystemet for domener, navnetjenerfunksjonen og organisasjonsstruktur/administrative rutiner innad i Norid. PT bad også om informasjon og dokumentasjon vedrørende Norids økonomisk soliditet og tidligere gjennomført ROS- analyse.

I mai 2012 sendte Norid inn svar på PTs spørsmål med vedlagt dokumentasjon og kontrakter inngått med underleverandører og andre kontraktører, jf. vedlegg 2, brev fra Norid av 30. mai 2012. PT har på bakgrunn av innsendt materiale foretatt en vurdering av sikkerhet, stabilitet og driftsstruktur ved forvaltning og drift av .no.

Deler av innsendt dokumentasjon fra Norid omhandler informasjon om sikringstiltak og forretningshemmeligheter, og er unntatt offentlighet, jf offentleglova § 13, jfr. forvaltningsloven § 13, 1 ledd nr. 2.

Vurdering av tilsynets hovedpunkter

1. <u>Registreringssystemet</u>

Det er viktig at brukerne til .no kan registrere, fornye og flytte domenenavn på en sikker og brukervennlig måte slik at det er tilrettelagt for en effektiv utnyttelse og fortsatt vekst under vår nasjonale domenenavnsressurs. PT har bedt Norid om en overordnet beskrivelse av registreringssystemet for .no. Hensikten har altså vært å få en oversikt over og kunne vurdere funksjonalitet og systemarkitektur.

Norid innførte i oktober 2010 et nytt registreringssystem med prosjektnavn «Draupne». Draupne er egenutviklet, men basert på registreringssystemet som benyttes av registerenheten for det nasjonale toppdomenet i Østerrike. Systemet understøtter registrering, endring, overføring og sletting av domenenavn, - med tilhørende abonnentinformasjon, lagring av dette i intern database og publisering av utvalgte data i ulike eksterne databaser (Whois, DAS, DNS).

Begrunnelsen for innføring av et nytt registreringssystem for .no har først og fremst vært den sterke veksten i antall domenenavn under .no, og behovet for et system som er robust og designet for å kunne håndtere dette. Det nye registreringssystemet har, slik det fremstår i Norids

redegjørelse, bedre funksjonalitet enn det man har benyttet tidligere, i form av automatisering, kortere behandlingstid og større grad av selvbetjening for registrarene. Systemet er også laget med passordbeskyttelse mot flytting av domenenavn, noe som skal hindre uautorisert og utilsiktet flytting av domenenavn mellom registrarer.

Norid har oversendt redegjørelse for registreringssystemets oppbygning og hvilke funksjon de ulike komponentene har. I hovedtrekk består løsningen av registrartjenester med et web basert grensesnitt som brukerprotokollen EPP, publikumstjenester som Whois og søkefunksjon for ledige domenenavn, - samt registreringsdatabasen.

I tilsynsbrevet etterspurte PT også mer detaljerte opplysninger i forbindelse med bruk av Draupne, nærmere bestemt en redegjørelse for:

- hvilken plattform som benyttes
- fysisk plassering av registreringssystemet
- hvem som har driftsansvar og vedlikeholdsansvar for registreringssystemet, herunder opplysninger om evt. underleverandører
- rutiner for sikkerhetskopiering av registrerings data og testing av gjenopprettelse, jf. domeneforskriften § 6
- rutiner for behandling og beskyttelse av personopplysninger som legges inn i databasen ved domeneregistrering
- hvordan Norid begrenser og foretar kontroll av hvem som tillates som bruker av registreringssystemet
- hvilke tilgang en godkjent bruker av registreringssystemet har vedrørende registrering og endring av opplysninger
- hvordan systemdokumentasjon og mulighet for erfaringsoverføring om registreringssystemet ivaretas innad i organisasjonen. Det vises her til domeneforskriften § 10 vedrørende krav til prosedyrer for avvikling og overføring av registrerings data til ny registerenhet eller PT

Norid har levert grundig beskrivelse av alle ovennevnte forhold med dokumentasjon i relevante vedlegg, herunder oversikt over nettverksoppsett og rutinebeskrivelser for sikkerhetskopiering.

PT vil spesielt kommentere på behandling og beskyttelse av personopplysninger som legges inn i databasen ved domeneregistreringer. Dette omfattes av reglene i personopplysningsloven (popplyl), jf. § 3, 1 1 ledd bokstav a. Norid er såkalt behandlingsansvarlig, jf. popplyl § 2, nr. 4 - og må oppfylle kravene i personopplysningsloven.

Norid viser god oversikt over egne plikter i henhold til popplyl, herunder plikt til kun å foreta behandling der det foreligger hjemmel og da igjen kun der det er legitime formål som er saklig begrunnet i Norids virksomhet, jf. popplyl § 11. Videre oppsummerer Norid de øvrige kravene i popplyl. når det gjelder retting, innsyn, sikkerhet og konfidensialitet. Det er utfyllende beskrivelser av hvordan disse pliktene er ivaretatt i det nye registreringssystemet. PT vurderer at behandling og beskyttelse av personopplysninger er godt ivaretatt, også i det nye registreringssystemet.

PT har gjennomgått avtalene Norid har inngått for drift- og vedlikeholdstjenester og for overvåkning av Norids systemer. Det er også levert eksemplar av ny registraravtale. PT har ingen spesifikke kommentarer til oversendt kontrakts materiale utover at hensynet til personvernet er ivaretatt også i Norids kontraktsforhold med leverandører av tjenester som omhandler ivaretakelse av systemet/systemdriften.

<u>Delkonklusjon/sammenfatning:</u>

Det er de færreste registerenhetene for landkodetoppdomener (ccTLDer) som kjøper ferdige løsninger med registreringssystemer. De fleste ccTLDer må foreta tilpasninger til lokale forhold, lokal forretningsskikk, lokale registrarkorps, lokal klageordning, osv. Mange ccTLDer har således

egenutviklede systemer. Også Norid har valgt å utvikle Draupne som et eget/Norid eid program der man har hatt full kontroll over funksjonalitet og tilpasninger til registerenhetens behov. Utvikling av slikt eget registreringssystem koster mye ressurser for en relativt liten registerenhet som Norid.

Norid har oversendt grundig dokumentasjon av tekniske og administrative rutiner for registreringssystemet. Ut fra Norids redegjørelse og vedlagt dokumentasjon vurderer PT at utviklingen av Draupne har resultert i et godt system for en effektiv og brukervennlig håndtering av stadig større etterspørsel etter .no domener, samt ivaretakelse av viktige hensyn som robusthet, sikkerhet og personvern. PT har også deltatt på Registrarforum i regi av Norid, der tilbakemeldingen fra registrarene er at Draupne fungerer meget tilfredsstillende og er en klar forbedring fra tidligere.

PT har ikke fått forelagt eller gjennomgått dokumentasjonen av selve programvaren til Draupne. Ved egenutvikling av programvare vil slik dokumentasjon være viktig for Norids mulighet til å vedlikeholde programvaren dersom nøkkelpersonell slutter. PT vil følge opp og ha ytterligere kommunikasjon med Norid når det gjelder dette siste punktet.

2. Navnetjenerene

Navnetjenerene er en viktig del av domenenavnsystemet på Internett. Domenenavnsystemet er hierarkisk oppbygget og består av rotnavnetjenere, navnetjenere til alle toppdomenene og diverse andre navnetjenere til subdomener under hvert toppdomene. At navnetjenesten for et toppdomene er tilgjengelig, er avgjørende for funksjonalitet for tjenester på Internett.

For å oppnå tilgjengelighet for navnetjenere i ulike autonome system på Internett, benyttes Anycast. Dette er en metode som gjør at navnetjenere kan dupliseres og anvende samme IP-adresse for mange fysiske navnetjenere. Duplisering gjør igjen at man oppnår en stor grad av redundans og internettjenester vil således ikke bli påvirket av om en eller flere fysiske navnetjenere er nede eller utilgjengelig på grunn av vedlikehold eller på annen måte satt ut av spill.

PT bad Norid om en overordnet beskrivelse av Norids bruk av Anycast - dette for å kunne vurdere om det er sørget for tilstrekkelig grad av redundans slik at navnetjenere for .no til enhver tid vil være tilgjengelige for de norske internettbrukerne.

PT etterspurte også om mer detaljerte opplysninger knyttet til sikkerhet og tilgjengelighet til Norids navnetjeneste, nærmere bestemt en redegjørelse for:

- hvordan Norid sikrer tilgjengelighet til navnetjenerne, herunder geografisk tilgjengelighet og nettopologisk tilgjengelighet
- hvordan Norid vurderer risiko for programvarefeil/Software-feil og hvilke sikringstiltak som er satt inn for å unngå at eventuelle programvarefeil medfører nedfall av tjenester
- hvordan Norid sikrer at navnetjenerne har tilstrekkelig kapasitet til å håndtere oppslag under .no
- hvilke avtaler Norid har med underleverandører for fysisk tilgjengelighet til navnetjenerne
- hvordan sonefilen sikres i transporten fra registreringssystemet til navnetjenerne, - altså hvordan Norid sikrer at sluttbrukerne får riktig svar ved oppslag i DNS
- hvilke synspunkter Norid har vedrørende bruk av Domain Name System Security Extensions (DNS SEC)
- valg av sikkerhetsnivå for Norids navnetjeneste, eventuelle spesielle sikringstiltak

Norid har levert beskrivelse av alle ovennevnte forhold med dokumentasjon i relevante vedlegg. Herunder beskrivelse av sikringstiltak for tilgjengelighet, risikovurderinger, kapasitetsvurdering og kontrakter med leverandører av DNS anycast tjenester. PT har bedt om ytterligere systemdokumentasjon for unicast-navnetjenerne.

Norid opplyser at det skjer en fortløpende vurdering av behovet for endringer i navnetjenerinfrastrukturen. Det legges her vekt på å ha diversitet i valg av driftsoperatører, nettleverandører, maskinvareplattform, operativsystemer og navnetjenerprogramvare. Norid viser også til at det for samtlige navnetjenere foreligger avtale og kontaktpunkter som sikrer at Norid raskt kan få stanset den aktuelle tjenesten.

Norid opplyser at det til nå ikke har vært alvorlige ting å utsette på noen av leverandørene av ovennevnte navnetjenerfunksjoner. Norid opplyser om enkelte konkrete hendelser der det har vært problemer eller utfall. Ved disse tilfellene har det skjedd en rask håndtering av problemene og det har blitt levert gode hendelsesrapporter i ettertid. Brukerne av .no har ikke merket noe, ettersom de øvrige navnetjenerene var tilgjengelig som normalt. Dette viser at systemet rundt .no er robust med tilstrekkelig grad av redundans.

Ved gjennomført Risiko- og sårbarhetsanalyse (ROS- analyse) hos Norid i november 2011, ble det foretatt en vurdering av risikoen for hendelser der navnetjenesten til .no blir utilgjengelig eller sender ut feilinformasjon. Risikoen ble her vurdert som svært lav totalt sett - også når man legger inn marginer for mulige manuelle feil.

PT har fått oversendt og gjennomgått avtaler Norid har inngått med leverandører av navntjenerfunksjonen. Det som er mest interessant er informasjon om hvordan Norid sikrer fysisk tilgang til egen servere, og informasjon om Norids kontraktspartnere / tjenesteleverandører og deres rutiner for å hindre uvedkommende tilgang. PT har gjennomgått relevante avtaler på dette, og konkludert med at ovennevnte hensyn til tilgjengelighet, sikkerhet og personkontroll er tilstrekkelig ivaretatt.

Norid opplyser at de planlegger å innføre DNS Security Extentions (DNSSEC) i løpet av 2013. DNSSEC sørger for integritet for data (DNS records) som ligger på Norids navnetjenere og internettbrukere vil således være beskyttet mot forfalskning av DNS-responser. Norid har videre beskrevet fordeler og ulemper med innføring, hvilke driftsmessig endringer som vil måtte gjennomføres ved innføring av DNSSEC, samt at navnetjenerne vil kunne håndtere den økte belastningen DNSSEC vil medføre.

Delkonklusjon/sammenfatning:

Norid har valgt ikke å bygge ut egendrevet anycast-infrastruktur og heller kjøpe denne tjenesten fra underleverandører. Det opplyses fra Norid om at det finnes totalt ca 60 instanser for navnetjeneste for Norid rundt på ulike steder på Internett. PT er enig i vurderinger som Norid har foretatt med hensyn på kjøp av anycast-tjenester. Kostnader ved drift av egen anycast-infrastruktur vil ikke nødvendigvis gjøre seg utslag i bedre tilgjengelighet for navnetjenesten til .no.

Det er dokumentert at navnetjenerne har tilstrekkelig kapasitet til å håndtere oppslag ved normal og stor belastning. Norid har dokumentert bruk av ulik maskinvare, operativsystem og navnetjenerprogramvare for de ulike instansene av navnetjenere. PT mener således det er foretatt tilstrekkelige tiltak i forhold til å kunne tåle feil i maskinvare og programvare og holde navnetjenesten tilgjengelig. PTs vurdering er at tilgjengeligheten for navnetjenesten for .no er tilstrekkelig ivaretatt.

PT støtter beslutningen om innføring av DNSSEC under .no. PT konstaterer at innføring av DNSSEC vil medføre samarbeid med norske internettilbydere for å kunne nyttiggjøre seg av funksjonaliteten og gjennomføre validering av DNS-oppslag i internettilbydernes resolvende navnetjenere.

3. Organisasjon

Rammebetingelsene for drift av .no er knyttet til nasjonale forhold og nasjonal regulering, men er også i stor grad avhengig av i den internasjonale utviklingen innen domenenavnsadministrasjon og marked/ brukermønster. Det vises her blant annet til liberaliseringen av domenemarkedet som nå skjer ved etablering av nye generiske toppdomenen i rotsonen.

En organisasjon med tilstrekkelig og godt kvalifisert personell er en forutsetning for å sikre en fleksibel drift og stadig forbedring av tjenesten under .no, for sikring av tjenesten under kriser og for sikring av brukerne av .no ved endringer av rammebetingelsene og konkurransesituasjonen.

PT bad Norid om en overordnet beskrivelse av organisasjonsstrukturen i Norid, herunder antallet ansatte, stillingsfunksjoner, arbeidsoppgaver i organisasjonen og kompetansekrav.

PT bad også om mer detaljerte opplysninger knyttet til det som anses som kritiske arbeidsoppgaver i Norid og til rutiner for sikkerhetsarbeid, nærmere bestemt en redegjørelse for:

- hvilke stillinger/arbeidsoppgaver som Norid anser som kritiske når det gjelder å sikre tilstrekkelig sikkerhet og beredskap for drift av .no, samt en vurdering av hvorvidt disse funksjonene er tilstrekkelig bemannet
- hvilke styringsdokumenter Norid har for IT-sikkerhet i organisasjonen
- hvorvidt Norid har beredskapsplaner og rutiner for øving av planer

PT bad også å få oversendt kopi av relevante styringsdokumenter, - herunder instrukser og policy.

Norid har levert beskrivelse av alle ovennevnte forhold med dokumentasjon i relevante vedlegg.

Norid har tilknytning til eksternt kundesenter, og kjøper inn lønn- og personaltjenester fra UNINETT. For øvrig opplyser Norid at de har nødvendig kompetanse ansatt i egen organisasjon - Det satses altså på å bygge kjernekompetanse innad i organisasjonen.

Norid har totalt 15 fast ansatte og er organisert i tre avdelinger, - administrativ avdeling, teknisk avdeling og avdeling for støttefunksjoner. Norid har gitt en utførlig beskrivelse av hovedoppgavene og stillingene under de ulike avdelingene i organisasjonen. Det er også gitt en oversikt over lederansvaret i Norid og hvilke oppgaver som ligger inn under de ulike ledelsesnivåene, som er delt inn i funksjonene daglig leder, avdelingsledere, fagansvarlig og prosjektledere. Norid har en bevist prioritering av hvilke funksjoner som anses å være kritiske for driften av .no. Norid henviser til at de har en egen policy som slår fast at alle kritiske funksjoner er dekket opp av minst to ansatte for å redusere avhengigheten av enkeltpersoner.

PT har fått oversendt dokumentasjon på Norids policy for informasjonssikkerhet, som ble vedtatt av Norids styre i 2012. Denne policyen legger overordnede føringer for hvordan informasjonssikkerheten i Norid skal ivaretas og definerer roller og setter krav til underlagsdokumenter som skal finnes. Policyen peker spesielt på at Norid skal ha fokus på og ivareta kontinuitetsplaner, backup-prosedyrer, forsvar mot skadelig kode, ondsinnede aktiviteter, tilgangskontroll til systemet og informasjon, avvikshåndtering og rapportering. Planverk for gjennomføring av ovennevnte fokusområder er igjen formalisert gjennom skriftlige prosedyrer og retningslinjer.

I henhold til Norids policy for informasjonssikkerhet, skal det finnes kontinuitetsplaner som dekker kritiske og viktige informasjonssystemer og infrastruktur. UNINETT konsernet har en felles beredskapsplan som er en del av, og som skal dekke tilfeller ved død eller andre krisetilfeller blant de ansatte i konsernet. Norid har i tillegg utarbeidet en egen beredskapsplan for driften av .no. Begge planene er oversendt PT til gjennomsyn.

Delkonklusjon/sammenfatning:

Forvaltningen av .no kan karakteriseres som et fagfelt med høy grad av spesialkompetanse både innenfor den rene tekniske driften og innenfor ressursforvaltning og arbeidet for videreutvikling av .no som en nasjonal ressurs. Norid dokumenterer at organisasjonen er bevist på hvilke stillingsfunksjoner som er kritiske i forhold til opprettholdelse av .no. og at man her søker å unngå avhengighet av enkeltpersoner. Det vises for øvrig til kommentarer til ROS-analysen vedrørende sårbarhet knyttet til kritisk kompetanse.

Norid har foretatt en inndeling av hvilke bruksområde gjeldende planverkene (driftsinstruks og beredskapsplan), skal benyttes på. PT vurderer at det fremlagte planverket er solid og gjennomtenkt. Når det gjelder beredskapsplanen til Norid er det foretatt en opplisting av hvilke hendelser som skal defineres som krisesituasjoner. Videre håndtering av konkrete hendelser, herunder varsling av relevante organer og igangsetting av konkrete tiltak avhenger av om man befinner seg innenfor noen av de definerte kriseområdene.

PT er oppsatt som varlingsinstansene i krisesituasjoner i Norid. PT mener at det bør foretas en klar angivelse av hvilke av de pr. i dag indentifiserte krisetilfellene som skal medføre en varsling til PT. Ved å sette opp en klarere identifisering av varslingsplikt forenkler man bruken av planverket og unngår man å måtte foreta en skjønnsmessig vurdering av varslingsrutinene i den aktuelle krisesituasjonen.

For å bidra til Norids kompetanse på krisehåndtering, vil PT løpende vurdere hvordan Norid kan involveres i relevante øvelser i ekomsektoren.

4. Økonomisk soliditet

Norid er rent brukerfinansiert og mottar ingen tilskudd, hverken over statsbudsjettet eller fra organisasjoner som f.eks Forskningsrådet. Norid skal være en nøytral aktør og blir drevet ikke-kommersielt. Domeneforskriften § 3 slår fast at tildelingsreglene under .no skal være slik at de sikrer kostnadseffektivitet.

Norid har ansvar for forvaltningen av et toppdomene i et domenemarked i rask utvikling. PT har tidligere hatt en dialog med Norid vedrørende viktigheten av å ha et tilstrekkelig økonomisk fundament for å kunne følge opp utviklingen som skjer både nasjonalt og internasjonalt

Det økonomiske resultatet for Norid kan variere fra år til år. PT bad Norid om en overordnet vurdering av den økonomiske situasjonen for 2011/2012, og hvorvidt man mener at organisasjonen har en økonomisk soliditet som er med å sikre internettbrukerne og nasjonale interesser.

Norid har levert beskrivelse av alle ovennevnte forhold med dokumentasjon i relevante vedlegg.

PT ser det som viktig at Norid har en økonomi som tillater å utføre tiltak utover ren minimumssikring. Økonomisk soliditet er en forutsetning for kontinuerlig forbedring av tjenester, opprettholdelse av tjenester under kriser, sikring av brukerne/domeneabonnenter ved endringer av ytre rammebetingelser og mulighet til å følge opp forvaltningen av .no gjennom blant annet gjennomføring av rettslige prosesser i saker knyttet til spørsmål om erstatningsansvar e.l.

Delkonklusjon/sammenfatning:

Norid opplyser og dokumenterer at det er satt av økonomiske reserver i tråd med lovbestemte sikringstiltak og retningslinjer for informasjonssikkerhet. Videre opplyses det at nivået er satt med utgangspunkt i hva som trengs for en sikker, tillitsvekkende og ryddig drift av .no. Det er også tatt hensyn til behovet for å kunne investere i nye systemer og teknologi på domenefeltet. PT vurderer at den økonomiske situasjonen til Norid er solid.

5. Risiko- og sårbarhetsanalyse (ROS-analyse)

For å kunne forebygge uønskede hendelser er det avgjørende for enhver virksomhet å kartlegge hva slags hendelser som kan oppstå og hvilke sårbarheter som finnes. Gjennomføring av en ROS-analyse er derfor en viktig aktivitet i det forebyggende sikkerhetsarbeidet i en organisasjon som Norid.

SD sin strategi for samfunnssikkerhet og beredskap i samferdselssektoren definerer det overordnede målet for sikkerhetsarbeidet:

Å forebygge uønskede hendelser og minske følgene av disse hvis de skulle oppstå, for å kunne sikre samfunnets behov for transport og kommunikasjon.

SD presiserer under grunnleggende tiltak og virkemidler, at det er viktig at alle nivå i samferdselssektoren gjennomfører ROS-analyser. Det vises her til *«NS-ISO/IEC 27002:2005 - Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet»* der det slås fast at en ROS-analyse skal identifisere, kvantifisere og prioritere risiko opp mot kriterier for akseptabel risiko definert i egen organisasjon.

Norid gjennomførte en ROS-analyse i november 2011. Resultatene skal brukes aktivt og gi veiledning i forhold til Norids ledelse sin prioritering av tiltak for å kunne forbygge hendelser og minske følgene dersom hendelser skulle oppstå. Det opplyses at forrige ROS-analyse var gjennomført i 2006. PT bad om kopi av rapporten som ble laget for Norid ved gjennomført analyse i 2011, samt en overordnet redegjørelse for selve gjennomføringen og resultatene.

Norid har levert beskrivelse av gjennomført ROS-analyse med dokumentasjon i relevante vedlegg.

Norid ROS-analyse ble gjennomført av eksternt selskap, og gir en risikovurdering av registreringssystemet med støttesystemer samt navnetjenesten. Som en del av denne ble det også gjennomført en teknisk sikkerhetstest av registreringssystemet. Tilbakemeldingene er jevnt over gode selv om det gis anbefalinger på tiltak som bør settes i verk for å redusere risiko og oppnå økt sikkerhet.

Delkonklusjon/sammenfatning:

PT konstaterer at Norid har fulgt opp og gjennomført det meste av det som ble foreslått som konkrete tiltak i ROS-analysen. Ett punkt som kan nevnes spesifikt er sårbarhet knyttet til kritisk kompetanse blant personell, og konkrete tiltak som Norid har igangsatt for og ytterligere redusere denne sårbarheten. Dette er et svært viktig punkt som det fortsatt bør være stort fokus på. Det kan også nevnes de konkrete tiltak som er iverksatt for å bedre overvåkning og logging, samt gjennomføre logganalyse. Med henvisning til økt angrepsaktivitet på Internett, mener PT at dette også bør være et høyt prioritert område. PT viser her blant annet til kvartalsrapport, tredje kvartal 2012, fra Nasjonal Sikkerhetsmyndighet (NSM).

PT vil understreke viktigheten og nytteverdien av gjennomføring av denne typen ROS-analyser, der sårbarheter avdekkes med påfølgende råd om tiltak for å forebygge og forbedre sikkerheten. Organisasjonen settes i stand til å håndtere sikkerhetshendelser samt lære av hendelsene, både for intern opplæring og for oppdatering av realistiske scenarier i beredskapsplanen. Ofte vil en ekstern analyse, slik Norid her har gjennomført, være svært verdifull. I henhold til Norids sikkerhetspolicy skal ROS-analyser gjennomføres jevnlig. Etter PTs vurdering bør ROS-analyse i Norid gjennomføres noe oftere enn det som har vært gjort til nå.

Sammendrag

PT vurderer at dialogen mellom PT og Norid ved gjennomføringen av tilsynet har fungert godt. Norid har levert relevante redegjørelser, beskrivelser og dokumentasjon på alle forhold som PT har ønsket å kartlegge og vurdere. I de tilfellene der det har vært behov for ytterligere presiseringer eller tilleggsinformasjon, har dette også blitt oversendt fra Norid snarlig etter forespørsel.

På noen områder er det pekt på tiltak som kan forbedre prosesser og ivareta sikkerheten ytterligere. PT vil i det videre tilsynsarbeidet følger opp kritisk kompetanse, implementering av DNSSEC, forbedringer i rutiner knyttet til publisering av sonefil samt involvering av Norid i øvelser i ekomsektoren.

Samlet sett er PT meget godt fornøyd etter sikkerhetsgjennomgangen av hele Norid sin virksomhet. PT vil understreke viktigheten av videre prioritering av arbeid med forebyggende sikkerhet i Norid og at dette er en kontinuerlig prosess som hele tiden vil krever tid og resurser.

Med hilsen

Einar Lunde (e.f.)
avdelingsdirektør

Ørnulf Storm
seksjonssjef