Trafikministeriet

Koncernfælles it-sikkerhedspolitik

Version 30. april 2004

Trafikministeriet
Frederiksholms Kanal 27
1220 København K
Telefon 33 92 33 55
E-mail trm@trm.dk

Titel: Koncernfælles it-sikkerhedspolitk

Udarb. af: TRM It-råd

Kontakt: Jakob Franck, Trafikministeriet

Arbejdsgrp: Marianne Aabye, Banedanmark
Søren Klostergaard, Banedanmark
Finn Thestrup, DMI
Torben Sløk, Vejdirektoratet

Godkendt: Koncernledelsen

København den../.. 2004

.....

Thomas Egebo, Departementschef

Omfang

It-sikkerhedspolitikken for Trafikministeriet omfatter hele ministerområdet. Dog er undtaget institutioner, der er omdannet til aktieselskaber eller aktieselskabslignende virksomheder. De institutioner, der for tiden ikke er omfattet af politikken, er Banedanmark, Post Danmark, DSB, DSB S-tog a/s, Københavns Havn, Scandlines AG, Sund & Bælt Holding A/S, Øresundskonsortiet, Øresundsbro-Konsortiet og Ørestadsselskabet.

Ansvar

Trafikministeriets koncernledelse har ansvaret for beslutning vedr. it-sikkerhedspolitikken, og den enkelte institutions og departementets ledelse har ansvaret for, at it-sikkerhedspolitikken følges indenfor hvert enkelt område.

Institutioner, der har outsourcet it-driftsopgaven til f.eks. en outsourcingleverandør eller driftsfællesskab har ansvaret for at fastsætte de it-sikkerhedsmæssige krav i en aftale med driftsfællesskabet/outsourcing leverandøren.

Koncernledelsen er ansvarlig for at der føres kontrol og tilsyn med it-anvendelsen i institutionerne, departementet og i de institutioner, der har et driftsfællesskab eller har outsourcet opgaven.

Derudover kan Rigsrevisionen og øvrige myndigheder føre tilsyn.

Mål for it-sikkerhed

It-sikkerhedsarbejdet i Trafikministeriet sker på baggrund af kravene til den basale it-sikkerhed, som er fastsat i Dansk Standard 484, del 1.

Kravene til:

- Tilgængelighed,
- integritet og
- fortrolighed

skal fastsættes således at kravene til it-sikkerheden er tilstrækkelige og medvirker til at lovgivning, bekendtgørelser og god forvaltningsskik overholdes.

Såfremt de enkelte institutioner har behov for yderligere it-sikkerhedskrav, sker fastlæggelse med udgangspunkt i en overordnet økonomi- og risikovurdering.

It-sikkerhedsarbejdet

It-sikkerhedsarbejdet er baseret på at de enkelte institutioner og departementet har:

- Udarbejdet en overordnet risikovurdering
- Fastsat en skriftlig it-sikkerhedspolitik
- Beskrevet implementeringen i en handlingsplan
- Fastsat regler og retningslinier, og kommunikeret dem
- Sørget for at grundlaget er i orden: uddannelse, god sikkerhedsbevidsthed og at ledelsen går i front
- Planer hvis noget går galt → nød - og beredskabsplaner.

Det forudsættes at topledelsen i de enkelte institutioner godkender it-sikkerhedspolitikken, medvirker til implementering, udviser engagement og skaber et godt fundament for god it-sikkerhedsbevidsthed blandt ledelse og medarbejdere.

Bilag

Denne vejledning er hentet fra hjemmesiden OIS (offentlig Information Online)

Standard for it-sikkerhedsprocesser i staten

For at styrke den generelle it-sikkerhed i staten har regeringens økonomiudvalg den 12. januar 2004 tiltrådt, at det gøres obligatorisk for statens institutioner at følge en fælles standard for it-sikkerhedsprocesser efter en 3-årig indføringsperiode samt, i regi af Videnskabsministeriet og med udgangspunkt i denne standard, at etablere et hjælpeprogram, der skal bistå de statslige myndigheder med implementeringen af standarden i indføringsperioden. Det er den enkelte institutions eget ansvar at sikre, at standarden implementeres og efterleves.

1 Baggrunden for indførelse af standarden for it-sikkerhedsprocesser

Ovennævnte beslutning bygger på et sæt anbefalinger, som er udarbejdet af en tværministeriel arbejdsgruppe. Initiativet og anbefalingerne er beskrevet i en rapport, der har været i høring i Statens it-råd, Det koordinerende Informationsudvalg samt Rådet for it-sikkerhed. Rapporten har desuden været i bred høring hos staten og private interessenter.

Formålet med rapporten var at præsentere og anbefale en strategi for, hvordan staten kan tilrettelægge det fælles arbejde med it-sikkerhed, så både nutidens og fremtidens krav om tryg og sikker anvendelse af it opfyldes.

God it-sikkerhed er en forudsætning for, at regeringens visioner om digital forvaltning kan realiseres med succes. Og i takt med den øgede integration og interaktion mellem statslige forvaltninger stiger behovet for en systematisk tilgang til håndteringen af it-sikkerheden.

For at imødekomme dette anbefaler rapporten, at statens institutioner gør brug af et fælles koncept, en standard for it-sikkerhedsprocesser, som foreslås at være både en referencemodel og inspirationskilde til tilrettelæggelsen af it-sikkerheden i den enkelte institution. Anbefalingen er endvidere at indføre standarden over en treårig periode. Perioden skal sikre en smidig implementering, som uden de store anstrengelser kan indarbejdes i institutionernes løbende tilrettelæggelse af it-sikkerhedsarbejdet og it-driften.

Høringen har vist, at der er bred opbakning til initiativet. Der var i høringssvarene gennemgående fokus på, hvordan initiativet kunne gennemføres med succes, og ikke om det skulle gennemføres. Det fremhæves i en del af høringssvarene, at netop hjælpeprogrammet er en forudsætning for, at initiativet kan gennemføres.

KL har deltaget i arbejdsgruppen, og der er undervejs i udarbejdelsen af anbefalingerne afholdt orienteringsmøder med Rigsrevisionen og Datatilsynet. Videnskabsministeriet har endvidere drøftet initiativet og anbefalingerne med Amtsrådsforeningen, som er enige i rapportens anbefalinger.

2 Standarden

Standard for it-sikkerhedsprocesser i staten forventes baseret på Dansk Standards standard for it-sikkerhedsprocesser, DS 484: "Norm for edb-sikkerhed" del 1.

DS 484 er i to dele. Første del rummer de krav, som skal overholdes for, at en organisation med rimelighed kan hævde at have en forsvarlig it-sikkerhedshåndtering. Anden del er

skærpede krav, der finder anvendelse, når det er nødvendigt at stille særlige krav til it-sikkerheden.

Standarden kræver, at alle institutioner anvender en metodik, som i det væsentlige er indeholdt i nedenstående krav:

- *Udarbejd en overordnet skriftlig risikovurdering.*
  Risikovurderingen kan opfattes som et filter, som ordner information om sårbarheder efter, hvor kritisk sårbarheden er, og som giver ledelsen et grundlag for prioritering af indsatsen.
- *Udform en skriftlig it-sikkerhedspolitik.*
  It-sikkerhedspolitikken fastlægger ledelsens overordnede sikkerhedsmålsætning og generelle retningslinier, de organisatoriske rammer for it-sikkerhedsarbejdet og det organisatoriske ansvar. Politikken fastlægges i høj grad på baggrund af viden om sårbarhederne i den pågældende institution.
- *Læg en it-sikkerhedsstrategi.*
  Strategien beskriver i hovedtræk hvordan it-sikkerhedspolitikken/målsætningen skal gennemføres, hvornår og med hvilken prioritet de enkelte aktiviteter gennemføres. Strategien skal skriftliggøres.
- *Etablér et sikkerhedsstyringssystem.*
  Sikkerhedsstyringssystemet er det centrale i sikkerhedsimplementeringen og indebærer blandt andet, at ansvarsplacering, tildeling af privilegier, anskaffelser og samarbejde med andre organisationer sker efter it-sikkerhedspolitikkens overordnede retningslinier. Systemet skal være dokumenteret skriftligt.
- *Udarbejd en skriftlig beredskabsplan.*
  Beredskabsplanlægningens formål er, at nedbringe konsekvenserne ved brud, ulykker eller fejl på it-systemerne. Beredskabsplanlægningen koordineres med sikringsforanstaltningerne, så der opnås en balance, der er i overensstemmelse med den risiko, som ledelsen har valgt at acceptere.

Desuden indeholder DS 484 også en række krav inden for områderne personalesikkerhed, fysisk sikkerhed, systemrelaterede krav og håndtering af lovbestemte og kontraktlige krav, der ligeledes er afspejlet i standarden. I alt indeholder standarden ca. 260 krav.

Med indførelsen af standarden for it-sikkerhedsprocesser i staten er der tale om at strukturere it-sikkerhedshåndteringen på alle ministerområder efter et fælles koncept – en aktivitet, som allerede er eller burde være implementeret på de enkelte ministerområder.

3 Uddybende bemærkninger om håndtering af it-sikkerhed

Nedenfor er gennemgået en række centrale temaer og problemstillinger, som giver et billede på de udfordringer, der ligger i at efterleve standarden.

3.1 Risikostyret it-sikkerhed

Udgangspunktet for it-sikkerhedsarbejdet bør være risikostyring. Det er den for ledelsen acceptable risiko, der knytter sig til organisationens anvendelse af informationer og informationssystemer, som skal være styrende for tilrettelæggelsen af it-sikkerhedsarbejdet. Der bør anvendes en systematisk metode til vurdering af risici, som involverer alle væsentlige interessenter, herunder den øverste ledelse og data/systemejere.

En risikovurdering skal gennemføres regelmæssigt, og bør give information om:

- Hvilke aktiver, herunder data, der er kritiske for organisationens aktiviteter.
- Hvilke risici, der kan true organisationens aktiver.

- Hvilke risici, der kan påvirke omverdenens tillid til organisationens data.
- Hvad det vil koste at fastholde risikoen på det for ledelsen acceptable niveau.
- Hvilke udækkede rest risici, som fortsat er til stede.

Enhver organisation bør have en it-sikkerhedspolitik, der løbende justeres og som er godkendt af den øverste ledelse. I it-sikkerhedspolitikken skal fastlægges ledelsens målsætning samt krav til følgende problemstillinger, som beskrives uddybende i det følgende:

- Ansvarsfordelinger i relation til it-sikkerhed.
- Krav til kontrolniveau.
- Styring af sikkerhed.
- Kultur og bevidsthed.
- Projekt- og udviklingsarbejde.
- Beredskab.

3.2 Ansvarsfordelinger og organisering i relation til it-sikkerhed

It-sikkerhed er et ledelsesansvar, hvilket indebærer, at ministerområdet skal have it-sikkerhed som et punkt i den overordnede ledelse af ministeriets styrelser, virksomheder, institutioner mm.

Internt i den enkelte organisation bør ledelsen udpege en it-sikkerhedsansvarlig, som har til opgave at koordinere en løbende proces med risiko- og omkostningsvurdering, som skal sikre, at ledelsen har det fornødne grundlag for at vurdere behovet for nye sikkerhedstiltag. I større organisationer bør der tages stilling til, om der skal etableres en sikkerhedsorganisation som støtte for den sikkerhedsansvarlige. Vedrørende ansvar bør der være tænkt over, hvordan suboptimerings-problemstillinger og interessekonflikter undgås, hvem der har ansvar for hvad og hvordan sikkerhedsorganisationen samarbejder med resten af organisationen.

3.3 Krav til kontrolniveau

I en sikkerhedspolitik skal ledelsens accepterede sikkerhedsniveau udformes som målsætninger for kontrolniveauet på alle it-sikkerhedens hovedområder som krav til:

- beskyttelse af aktiver.
- uafhængighed af enkeltpersoner.
- datakvalitet.
- driftskvalitet.

3.4 Styring af sikkerhed

Sikkerhed er en "ferskvare" forstået på den måde, at den forgår meget hurtigt, hvis ikke man er på vagt overfor forandringer og hændelser. Der skal tænkes over, hvordan man sørger for, at it-sikkerhedspolitikken hele tiden overholdes.
Ligeledes skal det overvejes, om sikkerheden fortsat har et relevant niveau i forhold til organisationens afhængighed af it og dertil knyttede risiko.

3.5 Kultur og bevidsthed

Det anbefales, at der arbejdes imod en sikkerhedskultur, som tager udgangspunkt i og giver optimal understøttelse af organisationens sikkerhedspolitikker. Brud på it-sikkerhed skyldes ofte menneskelige fejl, eller manglende kompetencer og forståelse hos medarbejdere. Men det kan også være et resultat af en manglende eller uklar udmelding fra ledelsens side om dens holdninger til it-sikkerhed. Derfor er et vigtigt element bevidsthed om og forståelse for sikkerhed. Det kan f.eks. opnås igennem awarenesskampagner, uddannelse og revision eller kontrol.

3.6 Projekt- og udviklingsarbejde

Det anbefales at have indarbejdet analyse af de sikkerhedsmæssige behov i for-analysen til projekter og udviklingsarbejde. Der vil være administrative, tekniske og fysiske foranstaltninger, som skal understøttes eller tilpasses nye systemer. Der vil ofte være krav til fortrolighed, integritet og tilgængelighed, som har indflydelse både på arbejdsgange og systemers tekniske udformning, konfiguration og implementering. Der kan endvidere være eksterne krav til f.eks. sporbarhed og lovbestemte krav fra eksempelvis Rigsrevisionen og Datatilsynet, som skal indarbejdes i en kravspecifikation.

3.7 Beredskab

Det er vigtigt at have et beredskab for hvordan man forholder sig, hvis der opstår brud på sikkerheden, hvad enten bruddet påvirker tilgængeligheden eller fortroligheden mm. Det anbefales, at organisationen fastlægger:

- krav til rapporteringer, så alvorlige sikkerhedsbrud bliver erkendt hurtigst muligt.
- fastlæggelse af, hvem der er ansvarlig for igangsættelse af beredskabet.
- prioritering af og retningslinier for reetablering af sikkerheden.

4 Hjælpeprogrammet

Hjælpeprogrammet tager udgangspunkt i arbejdsgruppens anbefalinger og de under høringen indkomne forslag. Hjælpeprogrammet har tre overordnede formål:

- hjælpe de statslige institutioner med at effektivisere it-sikkerhedsarbejdet.
- forberede statslige institutioner på at kunne håndtere de it-sikkerhedsmæssige udfordringer som følger af digital forvaltning.
- sikre, at alle statens institutioner efter tre år efterlever standarden.

Videnskabsministeriet etablerer en portal, der bliver samlingsstedet for hjælpeprogrammets aktiviteter og ressourcer.

Øvrige elementer i hjælpeprogrammet er:

- Kampagner målrettet mod statens institutioner om hjælpeprogrammet.
- Udarbejdelse af vejledninger og værktøjer.
- Seminarrække og workshops.
- Benchmarkingaktiviteter.

5 En statslig arbejdsgruppe for it-sikkerhed

Til at følge implementeringen af den statslige standard nedsætter Statens it-råd en arbejdsgruppe, der får til opgave at:

- sikre øget videndeling bredt i staten. Videndelingen skal blandt andet bidrage til, at der skabes en fælles forståelse for og præcisering af almindelig god praksis.
- bidrage til koordinering mellem myndigheder med ansvar for it-sikkerhed.
- sikre at hjælpeprogrammet tager højde for særlige it-sikkerhedsmæssige problemstillinger.

Det forventes, at arbejdsgruppen afholder ca. 6 årlige møder. Til arbejdsgruppens arbejde og diskussioner vil der blive knyttet såvel offentlige som private "faglige eksperter":

Arbejdsgruppen består af en repræsentant fra alle ministerier. Repræsentanten vil typisk være en person, der har særlig it-sikkerhedsfaglig viden og generel indsigt i og viden om ministerområdets opgaver og organisation.

Derudover deltager særskilt en repræsentant fra:

- Beredskabsstyrelsen
- Datatilsynet
- Den Digitale Taskforce
- Finanstilsynet
- Forsvarets Efterretningstjeneste
- Politiets Efterretningstjeneste
- Rigsrevisionen
- Økonomistyrelsen

Som observatører deltager en repræsentant fra KL og Amtsrådsforeningen. Derudover varetager Videnskabsministeriet formandskabet i arbejdsgruppen ligesom Videnskabsministeriet leverer sekretariatsbistand til arbejdsgruppen.

6 Den videre proces

Det anbefales, at det enkelte ministerium nedsætter en arbejdsgruppe/udvalg, som formulerer en strategi for implementering af standarden.

Videnskabsministeriet er i færd med at forberede etablering og drift af hjælpeprogrammet. I løbet af 2. og 3. kvartal af 2004 forventes programmet at være operationelt og i drift. Detaljer om indholdet og brugen af hjælpeprogrammet kommunikeres ud direkte til alle relevante brugere. Arbejdsgruppen, der nedsættes i regi af Statens it-råd, forventes at være etableret med udgangen af marts måned 2004.

7 Økonomi

Videnskabsministeriet undersøger, om det er muligt at indgå en fælles aftale med dansk standard om brugen af DS484 i staten samt udviklingen af hjælpeprogrammet.

Den enkelte institution forudsættes selv at finansiere implementeringen af standarden såfremt denne ikke i forvejen er implementeret som en naturlig del af den løbende it-drift.