Fra: Ragnhild Aashaug
Til: Ragnhild Aashaug
Emne: Fwd: Innspill til IKT-sikkerhet i FARTT
Dato: 10. februar 2023 09:57:22

Mvh
Ragnhild Aashaug

Sendt fra min iPhone

Videresendt melding:

> **Fra:** Øyvind Sunde <Oyvind.Sunde@bdo.no>
> **Dato:** 21. november 2022 kl. 10:10:40 CET
> **Emne: SV: Innspill til IKT-sikkerhet i FARTT**
>
> Hei,
> Vi har svart ut fra en IKT-sikkerhetsrevisjon av FARTT. Jeg tror vi må kjenne mer til samhandlingen med kommunene og ev. kommunenes egne prosesser og systemer for å kunne si noe om det. Det er ikke umulig å inkludere denne samhandlingen i en problemstilling, men som sagt da må vi vite mer. Dere kan jo drøfte det i kontrollutvalgene, så får vi komme tilbake til konkretisering og ev. konsekvenser for budsjettet senere.
>
> Med vennlig hilsen
>
> **Øyvind Sunde**
> Mobil +47 976 10 122
>
> 
>
> 
>
> ---
>
> **Fra:** Ragnhild Aashaug <ra@kontrollutvalgfjell.no>
> **Sendt:** mandag 21. november 2022 09:56
> **Til:** Øyvind Sunde <Oyvind.Sunde@bdo.no>
> **Kopi:** Dagfinn Buset <Dagfinn.Buset@bdo.no>
> **Emne:** Re: Innspill til IKT-sikkerhet i FARTT
>
> Hei!
> Tusen takk for et gjennomarbeidet forslag! Det er nyttig for oss i det videre arbeidet. Dette ser bra ut i forhold til det som var intensjonen.
> Det som henger litt i løse lufta er kommunedirektørens innspill om samhandlingen mot kommunene, som kan være et kritisk punkt. Forstår jeg deg riktig om at dette ikke er inkludert nå? Og at dersom vi ønsker mer på dette, så kommer det i tillegg?
>
> Mvh
> Ragnhild Aashaug

Sendt fra min iPhone

21. nov. 2022 kl. 09:18 skrev Øyvind Sunde <Oyvind.Sunde@bdo.no>:

Hei igjen,
Vi har tenkt litt rundt din forespørsel om en mulig forvaltningsrevisjon av IKT-sikkerhet og personvern i IKT Fjellregionen IKS (FARTT). Ut fra informasjonen på fartt.no ser det ut til at FARTT ivaretar både felles programmer (Microsoft) og mange fagsystemer for sine fem kommuner. FARTT har også et eget IKT Sikkerhetsutvalg som indikerer at IKT-sikkerhet er ivaretatt. Personvern blir også i stor grad ivaretatt gjennom IKT-sikkerhetsrutiner. Vi oppfatter at henvendelsen om IKT-sikkerhet og personvern omfatter denne siden av personvernet. (Hvordan kommunene ivaretar personvern i sine prosedyrer, er en annen og mye mer omfattende revisjon.)

Jeg har under hånden snakket med kommunedirektøren i Tynset kommune. Han har ikke ment å utfordre organiseringen av IKT-tjenester i FARTT, men han var opptatt av samhandlingen mellom FARTT og kommunene. I en eventuell forvaltningsrevisjon av FARTT må det gjøres en avgrensning mot eller konkretisering av om og i hvilken form denne samhandlingen skal omfattes.

Problemstillinger
I våre IKT-sikkerhetsprosjekter bygger vi på en risikobasert revisjon basert på standardene ISO/IEC 27001 og NSMs grunnprinsipper for IKT-sikkerhet (Nasjonal Sikkerhetsmyndighet). Ifølge disse kontrolleres både må- og bør-krav til IKT-sikkerhet. Vi kan foreslå å legge følgende problemstillinger til grunn:

1. Styrer selskapet informasjonssikkerheten på en tilfredsstillende måte?
2. Blir sikkerhetsrisikoer identifisert og håndtert?
3. Blir informasjon og informasjonssystemer beskyttet i henhold til beste praksis?
4. Hvordan oppdages avvik og mulige trusler mot virksomheten?
5. Blir hendelser håndtert på en tilfredsstillende måter?

Vi kontrollerer både ledelse og styringssystem for informasjonssikkerhet, de forebyggende tiltakene samt kapasitet for hendelseshåndtering. Tilnærmingen omfatter både menneskelige, organisatoriske og teknologiske sikkerhetstiltak.

Sikkerhetstesting
Det er ikke uvanlig å inkludere en sikkerhetstesting som en del av sikkerhetsrevisjonen, vil dette i kombinasjon med revisjonen gi tilstrekkelig verifikasjon av sikkerhetstilstanden i virksomheten. Sikkerhetstestene skal simulere angrepsteknikker som brukes av trusselaktører for å oppnå uautorisert tilgang til informasjonssystemer, eller for å påvirke tilgjengeligheten eller integriteten til systemer og data. Hensikten med testingen er å avdekke sårbarheter som utnyttes til misbruk og datakriminalitet, samt foreslå eventuelle forebyggende tiltak. For de aktuelle systemene vil BDO i samråd med selskapet finne hensiktsmessige testscenarioer. Dette må gjøres basert på systemenes verdier, trusler og mulige sårbarheter som er kartlagt i den innledende risikovurderingen. For å identifisere og simulere de mest sannsynlige trusselscenarioene vil nøyaktig omfang av sikkerhetstestingen utarbeides i samarbeid med selskapet. Resultatene fra sikkerhetstesting vil gi et godt grunnlag for å vurdere reelle angrepsvektorer og faktisk risiko, samt for å anbefale og implementere konkrete tiltak.

Budsjett
Vi har skissert dette ut fra et budsjett på 250-300 timer. Vi må komme tilbake med mer eksakt anslag når/hvis kontrollutvalgene går videre med ideen om en felles forvaltningsrevisjon på dette området. Vi må også vurdere tidsestimatet for om sikkerhetstesting skal inkluderes eller ikke.

Da hører vi nærmere fra deg når du har fått drøftet en mulig forvaltningsrevisjon med IKT-sikkerhet i FARTT med de øvrige deltakerkommunenes kontrollutvalg.

PS: Dagfinn, kopiadressat, er ansvarlig partner for våre tjenester innen sikkerhet og beredskap, og vil være den ansvarlige for gjennomføring av en eventuell forvaltningsrevisjon.

Med vennlig hilsen

Øyvind Sunde
Direktør Rådgivning
Mobil +47 976 10 122
Oyvind.Sunde@bdo.no

BDO AS
Munkedamsveien 45
Postboks 1704 Vika, 0250 OSLO
www.bdo.no