Forvaltningsrevisjon av IKT-sikkerhet

OPPFØLGING OG TILTAK

Innledning

- Oppdraget
- Arbeidsgruppe
- Arbeidsmetode
- Anbefalingene og tiltak
- Oppsummering
- Nåsituasjon og utfordringsbildet fremover

Oppdraget

- Felles forvaltningsrevisjon IKT sikkerhet i IKT Fjellregionen IKS

- Alle kommuner deltatt, med unntak av Folldal

Arbeidsgruppe

- Bredt sammensatt gruppe, eiere, styret og selskapet representert

(vedtatt K-dir forum)

  - Sverre Jenssen, daglig leder FARTT
  - Kai Røen, sikkerhetsleder FARTT
  - Harald Sørli, styreleder FARTT
  - Amund Aarvelta, assisterende kommunedirektør Tynset kommune
  - Malin Wassdahl, kommunedirektør Folldal kommune

Arbeidsmetode – hvordan ?

- BDO rapport gav føringer for videre arbeid
- FARTT igangsatte oppfølging av BDO rapport umiddelbart
- Mye å ta tak i innledningsvis, landskapet «klarnet» etterhvert
- Arbeidsgruppa gjennomført nødvendig avklaring og forståelse av oppdraget, med utgangspunkt vedtaket i kontrollutvalg-kommunestyrene
- Månedlige møter i arbeidsgruppa, rapportering til styret og k-dir, hyppigere arbeidsfrekvens på slutten
- Rapport og tiltak basert på anbefalingene i vedtakene, innhenting av informasjon hos FARTT og kommunene

Styringssystem for informasjonssikkerhet

- Krav til informasjonssikkerhet
  - Personvernforordningen krever egnede tekniske og organisatoriske tiltak
  - Virksomheter kan benytte standarder som ISO/IEC 27001

- Compilo
  - FARTT og eierkommunene bruker Compilo som styringssystem
  - Felles anskaffelse av GDPR-pakke fra Compilo høsten 2023
  - Utvikling av GDPR prosessbeskrivelse og prosesskart
  - Årshjul i sikkerhetsarbeidet er viktig

Overordnet plan for iKT og IKT-sikkerhet

Sikkerhetsmål for behandling pers.opplysninger (kap 5 i rapport)

- Formål, omfang og ansvarsavklaring
  - Er del av styrende prosedyrer i Compilo
  - Organisasjonen skal vite hvordan behandling av personopplysninger foregår
  - Sikkerhetsmål gjelder alle ansatte
  - Tydelig ansvarsfordeling

Overordnet plan for iKT og IKT-sikkerhet

Sikkerhetsstrategi for informasjonssikkerhet (kap 6 i rapport)

- Strategien skal tydeliggjøre hvordan en ivaretar sikkerhetsmålene
  - Er del av styrende GDPR prosedyre i Compilo
  - Sikkerhetsstrategi gjelder alle ansatte
  - Tydelig ansvarsfordeling

Overordnet plan for iKT og IKT-sikkerhet

Mål for informasjonssikkerhet, verdier (kap 7 i rapport)

- Konfidensialitet
- Integritet
- Tilgjengelighet
- Regulatoriske krav, ivareta det over ihht lovgivning

Overordnet plan for iKT og IKT-sikkerhet

Identifisering av informasjonsverdier (kap 8 i rapport)

- «Ny oppgave» som utfordret arbeidsgruppa, verdibegrepet uklart (i dag snakker man om digitale verdier)
- **Konfidensialitet-integritet og tilgjengelighet**
- Tatt utgangspunkt i flere tjenesteområder
- Litt ulik vurdering av verdiene, høyest score på integritet

Organisering og ansvarsforhold i IKT sikkerhetsarbeidet

(Kap 4 i rapport)

- Behandlingsansvarlig: kommunene og kommunedirektør
  - Ansvar formål med behandling av pers.opplysninger
  - Egen organisering
- Databehandler: IKT Fjellregionen eller andre leverandører
  - Behandler pers.opplysninger på vegne av behandlingsansvarlig
  - Egen organisering
- Databehandleravtaler: FARTT og kommunene=ok
  - Har avtaler med eksterne leverandører, noe «etterslep» og oppdateringer

FARTT ikt

Organisering og ansvarsforhold i IKT sikkerhetsarbeidet

(Kap 4 i rapport)

- Personvernombud
  - 20 % ressurs fra Tolga idag, anbefaler større ressurs fremover
- IKT sikkerhetsutvalg
  - Rådgivende organ med representanter fra kommunene og FARTT
  - Organisering og mandat følger utvalget

Tilgangsstyring og rutiner

- Innføring av IAM (Kap 11 i rapport)

- Skybasert løsning
  - Sikrer trygg og sikker opprettelse av brukeridenter, endring og fjerning av brukere
  - Visma HRM modersystem som delegerer rettigheter, lisenser og tilganger
  - Automatiserte prosesser og mindre manuell oppfølging, gode rutiner

- Integrasjon med eksisterende systemer
  - Knyttet opp mot fagsystemer, teknisk infrastruktur og økosystem

- Lovhjemlet løsning
  - NSM Grunnprinsipper 2.6: Kontroll på identiteter og tilganger
  - Normen 5.2: Tilgangsstyring og 5.2.1: Autorisering
  - GDPR Personvernforordningen artikkel 17 ("Rett til sletting") og artikkel 32 ("Sikkerhet ved behandlingen").
  - Tilgang til helseopplysninger er i tillegg regulert i flere lover og forskrifter.

Verdivurdering og identifisering av informasjonsverdier i kommunene

(Kap 10 i rapport)

- Oppdrag gitt til ledergruppene i hver kommune, i samråd med kommuneledelsen
- Arbeidsgruppas rolle
  - Fokus på overordnet nivå i kommunene
- Prioriterte områder
  - Områder/sektorer med store verdier
  - Samsvarer med beredskapsplanen til FARTT
- Samlet verdivurdering, Målt mot ulike kriterier
  - Konfidensialtitet
  - Tilgjengelighet
  - Integritet

FARTT ikt

Risikostyring og risikovurdering i FARTT

(Kap 15 og 16 i rapport)

- Metode for risikovurdering
  - Basert på KINS-modellen, 5 kombinasjoner av konsekvens og sannsynlighet
- Momenter for gjennomføring
  - Risikobeskrivelse
  - Sårbarheter og svakheter
  - Eksisterende risikoreduserende tiltak
  - Vurdering av sannsynlighet og konsekvens
  - Aksepterbar risiko og tiltak
- Tiltak
  - Oppfølging av ROS, tiltak på kort og lengre sikt
  - Flere risikoer er redusert til akseptabelt nivå

Oppfølging og tiltak

(Kap 17 i rapport)

- Sikring mot ulike angrep
  - FARTT har gode systemer på plass for å beskytte mot cyberangrep
  - Regelmessig oppdatering og revisjon nødvendig
- Sårbarheter i IT-systemer
  - Ingen systemer kan være 100 % sikre
  - Får på plass ekstern beskyttelse mot DDoS-angrep
- Beskyttelse mot ransomware og phishing
  - Utfordrende å forhindre helt
  - Viktig med god opplæring og bevissthet blant ansatte
- Beskyttelse av identiteter og enheter
- Fysisk sikring av kommunale bygg

IKT hendelser og dokumentasjon

Kap 13 i rapport

- Alle hendelser av betydning for sikkerhet, personvern, oppetid og funksjonalitet skal som minimum loggføres, videreført som avvik
- Loggføring og dokumentasjon bidrar til god dokumentasjon-historikk som igjen er «lærende»
- Avhjelper hendelsehåndtering på ulike nivåer
- Hendelser med varighet og som berører viktige systemer for daglig tjenesteproduksjon, er også avvik
- Oppfattes å fortsatt være høy terskel for å melde avvik

Hendelsehåndtering og gjenoppretting

Kap 18 i rapport

- FARTT beredskapsplan er førende ift hvordan ulike hendelser oppfattes og håndteres
- Hendelseshåndtering bygger på en plan med prosedyrer og rutiner som følges før, under og etter en hendelse
- Ulike scenarier legger føringer for håndtering, noen likhetstrekk
- Gjenoppretting følger prioriterte områder
- Datamengde og overføringshastighet er kritiske faktorer ved gjenoppretting

FARTT ikt

Cyber-sikkerhet, store behov for kompetanse

Kap 19 i rapport

- Norge står overfor betydelige sikkerhetsutfordringer, NSM - Nasjonal sikkerhet mot 2030
- NIFU anslår at Norge i 2030 vil mangle 4000 personer med denne kompetansen, behov for rask løsning
- Utfordrende for kommuner eller IKT-samarbeid å skaffe seg denne kompetansen, ingen «Quick fix» på dette
- FARTT deltar på rammeavtalen sikkerhetsovervåkingstjenester for å anskaffe SOC og IRT
- Spille videre på gode kompetansemiljøer, utvikle egen organisasjon

FARTT ikt

Cybersikkerhet, tjenester, kunnskap og kompetanse

- FARTT benytter tjenester gjennom KommuneCERT
  - Overvåking av trafikk bidrar til økt fokus på unormale hendelser
  - Rapporterer sårbarheter og trusler

- FARTT benytter verktøy for sårbarhetsskanning
  - Kjøpt i 2024 for ukentlig skanning, kan også skanne skytjenester

- Hurtigtest utføres av HelseCERT

- Begrensede ressurser i FARTT kommunene

- Strategisk arbeid med sikkerhetskultur

Generelle sikkerhetstiltak

Kap 20 i rapport

- Beredskap
- Infrastruktur, fiber og mobilnett, redundans
  - Godt utbygd infrastruktur i Nord-Østerdals regionen
  - Fiberforbindelser mellom datasenter og kommuner
- NSM grunnprinsipper
  - Følges opp
- Sikkerhetsnøkler
  - Innføres i 2024

Anskaffelse sikkerhetstjenester

- Felles anskaffelse med DIGI Innlandet
  - Prosjektstart våren 2024, avtaleinngåelse i oktober 2024

- Tjenester som kan kjøpes
  - Sikkerhetsovervåking med SOC-tjenester (Security Operations Center)
  - Sikring av alle enheter
  - Incident Response Team (IRT) ved hendelser
  - Lagring av sikkerhetslogger i skyen

Kompetanse-ressurs innafor informasjonssikkerhet

- Fokus på riktig kompetanse og ressurser
  - Arbeid med IKT sikkerhet og personvern
- Videreutdanning for sikkerhetsleder
  - Grunnleggende studie i personvernregelverk
  - Digital sikkerhetskultur og personvern
- Nytilsatt ressurs i august
  - Støtte til informasjonssikkerhet og personvern
- Områder uten spesifikk kompetanse
  - Cybersikkerhet, hendelseshåndtering, overvåking-SOC tjenester og IRT
- Være i dialog med kommuneledelse, bidra til å øke generell kompetanse i kommunene

FARTT ikt

KINS/KS informasjonskampanje-program

Mål: Endre vaner hos kommuneansatte

- Samarbeid der KS og flere kommuner involvert
  - Oppdragstaker utarbeidet informasjonskampanjen
- Kampanjen består av ti temaer
  - Eget tema-klart budskap hver måned som rulles ut over 10 måneder
- IKT Sikkerhetsutvalg ansvarlig for intern informasjon
- Ledere tar opp temaer i møter
- Kampanjen kjøres årlig i FARTT samarbeidet

Oppsummering

- IKT sikkerhet er et kontinuerlig arbeid
  - FARTT og kommunene må jobbe sammen videre
  - Innbyggernes tillit og lovverk viktig, Informasjon må behandles i henhold til lovverket
  - Konfidensialitet, integritet og tilgjengelighet må ivaretas

- Kommunenes fokus på informasjonssikkerhet
  - Har et «større potensiale» i å utvikle sikkerhetsarbeidet
  - Veldig mye handler om kompetanse

- Samarbeid og kunnskapsdeling
  - Bygge god sikkerhetskultur sammen, jobbe strategisk

Nåsituasjon sikkerhetsarbeidet

- FARTT styrket personressurs med arbeidsoppgaver innafor IKT sikkerhet

- FARTT operativ sikkerhet med stort fokus på ulike tiltak
  - NSM grunnprinsipper, snart kommer NIS2 (EU direktibv for å styrke info.sikkerhet)
  - Overvåking og rapporter fra KommuneCERT, andre leverandører også
  - Innsidetesting og testing i driftsmiljø

- Økonomi og tiltak
  - 2024: 1,5 mill til sikkerhetsnøkler
  - 2025: 1,1 mill sikkerhetstiltak i årlig drift
  - 2025: 0,8 mill - 12,7 % av *investeringer i FARTT* styrke selskapets evne til sikkerhetsovervåking
    - Rammeavtale Tjenester sikkerhetsovervåking
    - SOC (overvåking infrastruktur)
    - IRT (Incident Response Team) hendelseshåndtering

Trusselsituasjonen

- Forsøk på stjeling av identiteter
  - E-post phishing (tilfeldig og målrettet)
  - Stjeling av session token
- Sosial manipulasjon (digitalt og fysisk)
  - Lure mennesker til å del sensitiv informasjon
  - Passord eller identifiserbar informasjon
- Manglende oppdateringer på enheter og APPer
- Dårlig passordhygiene
- Ukritisk bruk av IKT utstyr