FORVALTNINGSREVISJON

IKT-SIKKERHET I FARTT

Siv Irene Aasen & Jonas Strisland

04.12.2023

Agenda

1. INNLEDNING TIL FORVALTNINGSREVISJONEN
2. SAMLET VURDERING OG KONKLUSJON
3. GJENNOMGANG AV PROBLEMSTILLINGER OG VURDERINGER
4. SPØRSMÅL

Forvaltningsrevisjonen kort oppsummert

Bakgrunn

I risiko- og vesentlighetsvurderingen for 2020 er IKT-sikkerhetsområdet trukket frem som et prioritert område for forvaltningsrevisjon.

Kontrollutvalgene i Tynset, Tolga, Alvdal og Rendal kommune har bestilt en forvaltningsrevisjon innenfor IKT-sikkerhet og personvern.

Formål

Den viktigste målsettingen med revisjonen har vært å gi eierkommunene en ekstern vurdering av IKT-sikkerheten hos IKT Fjellregionen IKS (FARTT), og å bidra til å identifisere forbedringsområder som må utbedres for at FARTT skal ha et tilfredsstillende IKT-sikkerhetsnivå.

Avgrensninger

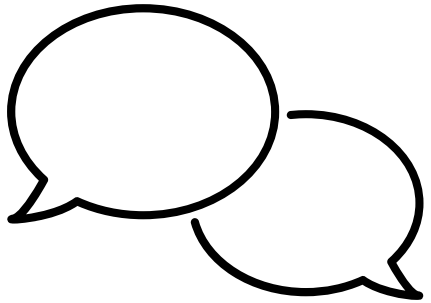
Forvaltningsrevisjonen har vurdert personvern i relasjon til god informasjonssikkerhet.

Revisjonen har ikke omfattet infrastruktur driftet av andre eksterne parter eller av eierkommunene selv.

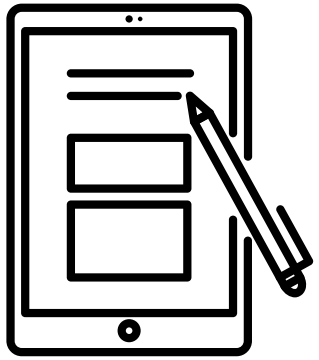
Revisjonskriterier

- NSMs grunnprinsipper for IKT-sikkerhet 2.0
- ISO/IEC 27001:2017 Ledelsessystemer for informasjonssikkerhet

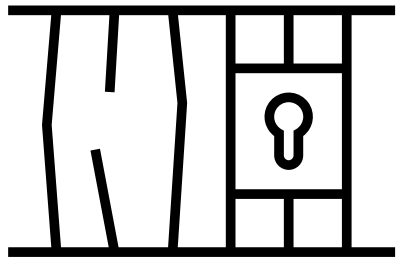
Metodisk har vi brukt intervjuer, dokumentgjennomgang og penetrasjonstest



Intervjuer



Dokumentgjennomgang



Penetrasjonstest

SAMLET VURDERING OG KONKLUSJON

Samlet vurdering og konklusjon

Hovedfunn

- Manglende definering av roller og ansvar knyttet til informasjonssikkerhet i FARTT
- Det er avdekket flere betydelige svakheter i IKT-arkitekturen og konfigureringen til FARTT
- FARTT gjør ingen sikkerhetsrevisjoner av underleverandører
- FARTT har ikke etablert rutiner for å gjennomføre tekniske øvelser. Dette gjør selskapet sårbart i håndteringen av nye og ukjente hendelser.

Hovedanbefalinger

- Tydeliggjøre, beskrive og plassere det overordnede ansvaret for informasjonssikkerhet i FARTT.
- Innføre standard herdeprofiler basert på beste praksis for PCer, servere og mobiltelefoner og innføre sikkerhetskonfigureringer i Microsoft 365 og Azure AD i henhold til beste praksis.
- Etablere rutiner for sikkerhetsrevisjoner basert på kritikalitet og risiko.
- Tilknytte seg en leverandør med spesifikk kompetanse innen cybersikkerhet som kan bistå med vurdering og håndtering av varsler og/eller ved cyberhendelser.

Gjennomgang av problemstillinger og vurderinger

Problemstilling 1: STYRER SELSKAPET INFORMASJONSSIKKERHETEN PÅ EN TILFREDSSTILLENDE MÅTE?

Revisjonskriterier:

- Selskapet har etablert et styringssystem for informasjonssikkerhet.
- Selskapet har definert roller og ansvar knyttet til arbeid med informasjonssikkerhet.
- Selskapet har utarbeidet styrende dokumenter for informasjonssikkerhet.

Funn:

De undersøkte forholdene avviker i noen grad fra revisjonskriteriene.

Anbefalte tiltak:

- Oppdatere Informasjonssikkerhetspolicy og IKT-sikkerhetshåndbok tilpasset organisasjon, trusselbilde og sikkerhetsbehov for 2023.
- Supplere sikkerhetsutvalget med mer kompetanse på informasjonssikkerhet, f.eks. knytte til seg en ekstern rådgivende part.
- Tydeliggjøre, beskrive og plassere det overordnede ansvaret for informasjonssikkerhet i FARTT.

Problemstilling 2: BLIR SIKKERHETSRISIKOER IDENTIFISERT OG HÅNDTERT?

Revisjonskriterier:

- Selskapet har kartlagt alle enheter og programvare som er i bruk.
- Selskapet har kontroll på alle identiteter og tilganger.
- Selskapet har utarbeidet, og reviderer jevnlig, risiko- og sårbarhetsanalyse av IKT-systemene.

Funn:

De undersøkte forholdene avviker i stor grad fra revisjonskriteriene.

Anbefalte tiltak:

- Fullføre innrulleringen av forvaltningssystemet og etablere prosesser for kontinuerlig vedlikehold.
- Begrense bruken av global admin-rettigheter til absolutt minimumsnivå, og heller bruke mer granulære rettigheter for andre administratorbehov.
- Etablere rutiner for sikkerhetskonfigurering i Microsoft 365 i henhold til beste praksis, inkludert forvaltning av gjestebrukere.
- Heve kvaliteten i risiko- og sårbarhetsvurderinger som gjennomføres, herunder dokumentasjon av vurderinger og metodisk oppfølging av identifiserte risikoer og tiltak.

Problemstilling 3: BLIR INFORMASJON OG INFORMASJONSSYSTEMER BESKYTTET IHT. BESTE PRAKSIS?

Revisjonskriterier:

- Selskapet har etablert et regime for sikker IKT-arkitektur og konfigurasjon.
- Selskapet har oversikt og kontroll over hele livsløpet til de tjenestene som forvaltes på vegne av kommunen og som er tjenesteutsatt.
- Selskapet har en plan for regelmessig sikkerhets-kopiering av all virksomhetsdata for kommunene

Funn:

De undersøkte forholdene avviker i stor grad fra revisjonskriteriene.

Anbefalte tiltak:

- Innføre tiltak for å redusere konsekvensene ved hendelser mot datasenteret, eksempelvis en redundant løsning i sky eller en sekundær lokasjon. Vi anbefaler samtidig for å undersøke mulighetene for alternative ISP-løsninger
- Innføre rutiner for test av gjenoppretting fra backup og disaster recovery øvelser for gjenoppretting på alternativ lokasjon. Dette bør i første omgang omfatte de mest kritiske systemene i kommunene.
- Gjennomføre og dokumentere en risikovurdering knyttet til bruken av en felles Azure AD tenant for alle kommunene i FARTT. Innføre tiltak som sikrer seperasjon mellom de ulike kommunene.

Problemstilling 3 forts.: BLIR INFORMASJON OG INFORMASJONSSYSTEMER BESKYTTET IHT. BESTE PRAKSIS?

Revisjonskriterier:

- Selskapet har etablert et regime for sikker IKT-arkitektur og konfigurasjon.
- Selskapet har oversikt og kontroll over hele livsløpet til de tjenestene som forvaltes på vegne av kommunen og som er tjenesteutsatt.
- Selskapet har en plan for regelmessig sikkerhets-kopiering av all virksomhetsdata for kommunene

Funn:

De undersøkte forholdene avviker i stor grad fra revisjonskriteriene.

Anbefalte tiltak:

- Gjennomgå sikkerhetskonfigureringene i Microsoft 365 og Azure AD og oppdatere disse i henhold til beste praksis.
- Innføre standard herdeprofiler basert på beste praksis for PCer, servere og mobiltelefoner.
- Etablere rutiner for sikkerhetsrevisjoner basert på kritikalitet og risiko.
- Påse at det er løpende føres oversikt over alle underleverandører, og at avtaler og databehandleravtaler med underleverandørene reflekterer kommunenes sikkerhetskrav og de tjenestene som leveres.

Problemstilling 4: HVORDAN OPPDAGES AVVIK OG MULIGE TRUSLER MOT VIRKSOMHETEN?

Revisjonskriterier:

- Selskapet har etablert sikkerhetsovervåkning av utvalgte deler av IKT-systemet.
- Selskapet har rutiner for å oppdage og fjerne kjente sårbarheter og trusler.
- Selskapet har gjennomført inntrengningstester på utvalgte IKT-systemer.

Funn:

De undersøkte forholdene avviker i noen grad fra revisjonskriteriene.

Anbefalte tiltak:

- Implementere en vaktordning som sikrer at varsler fra sikkerhetsovervåkningen håndteres også utenfor normal arbeidstid.
- Tilknytte seg en leverandør med spesifikk kompetanse innen cybersikkerhet som kan bistå med vurdering og håndtering av varsler og/eller cyberhendelser.
- Etablere rutiner for inntrengingstester basert på kritikalitet og risiko. Denne bør sees i sammenheng med anbefalte tiltak vedrørende sikkerhetsrevisjoner i kapittel 5.4.1.

Problemstilling 5: BLIR HENDELSER HÅNDTERT PÅ EN TILFREDSSTILLENDE MÅTE

Revisjonskriterier:

- Selskapet har et planverk for hendelseshåndtering og som revideres jevnlig.
- Selskapet har gjennomført regelmessige øvelser på informasjonssikkerhetshendelser.
- Selskapet har evaluert og implementert tiltak etter tidligere hendelser eller øvelser.

Funn:

De undersøkte forholdene avviker i noen grad fra revisjonskriteriene.

Anbefalte tiltak:

- Gjennomføre andre former for øvelser i tillegg til diskusjonsøvelser, herunder tekniske øvelser som omfatter gjenoppretting av utvalgte systemer, infrastruktur og gjenoppretting fra backup. Øvelsene bør involvere andre relevante parter som tjenesteeiere, kriseledelse og et utvalg sluttbrukere.
- Utarbeide handlingsplaner for de utpekte områdene i beredskapsplanen.

Spørsmål?

BDO

tett på