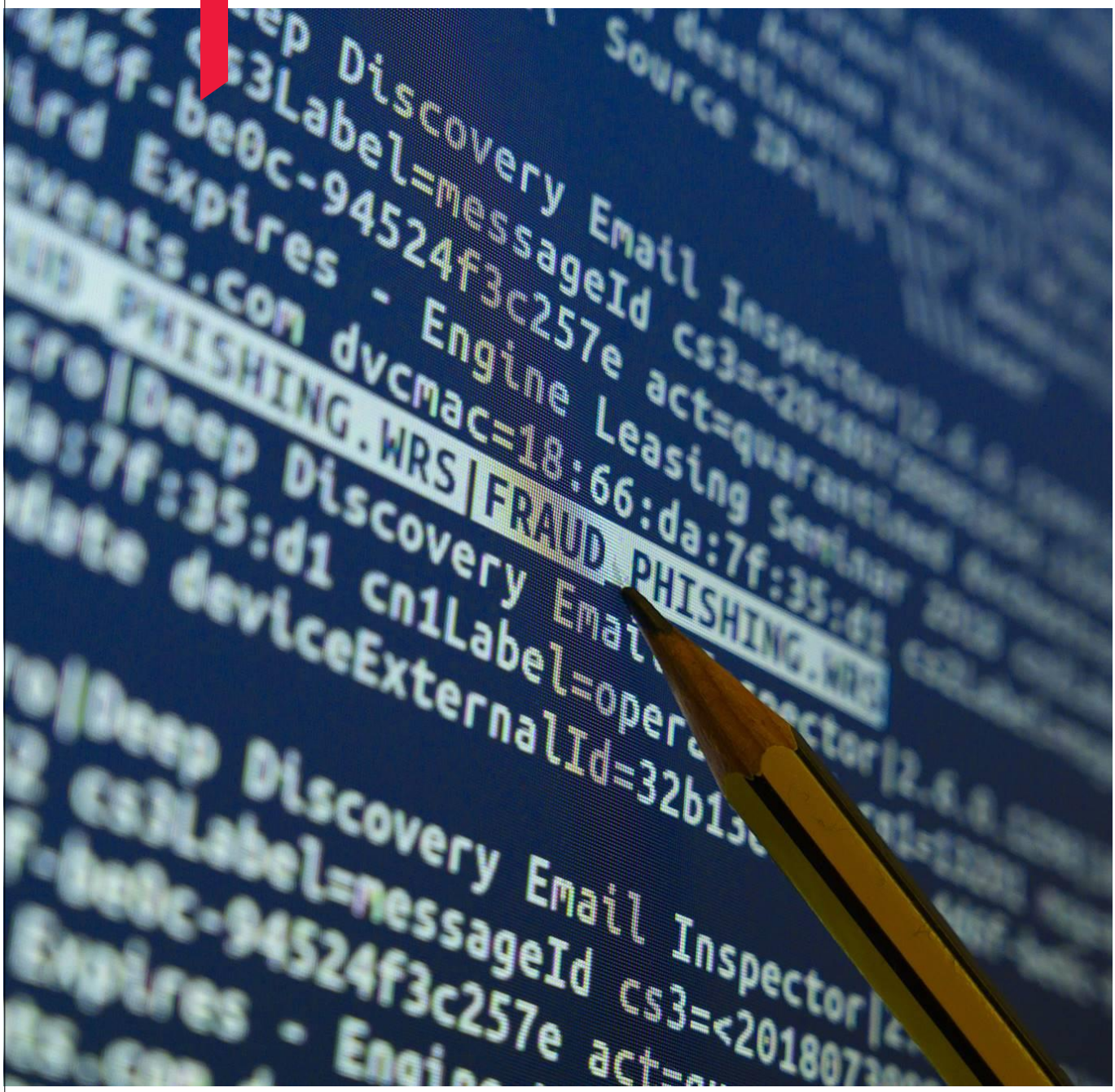


PROSJEKTPLAN

FORVALTINGSREVISJON AV IKT-SIKKERHET I IKT FJELLREGIONEN IKS FOR KONTROLLUTVALGENE I EIERKOMMUNENE

14. MARS 2023

INNHOLD

1 FORMÅL

1.1 FORMÅL

Kontrollutvalget i Tynset kommune har bestilt en forvaltningsrevisjon av IT-sikkerhet av Fjellregionen IT-selskap (FARTT).

1.2 BAKGRUNN

Ifølge revisors risiko- og vesentlighetsvurdering gjort for kontrollutvalget for 2020 fremgår det følgende om IKT-sikkerhetsområdet:

> *IKT er et viktig virkemiddel for å effektivisere offentlig sektor. Det kan være grunn til å se på hvilke ressurser som blir benyttet til utviklingsarbeid, og hvor høyt strategisk bruk av IKT blir prioritert.*
>
> *I 2018 fikk Norge ny personopplysningslov. Loven består av nasjonale regler og EUs personvernforordning (GDPR - General Data Protection Regulation). Forordningen er et sett regler som gjelder for alle EU/EØS-land. Endringer i lovverket, og at temaer knyttet til informasjonssikkerhet og personvern er viktige områder, innebærer at IKT-sikkerhet kan være et aktuelt tema for en forvaltningsrevisjon.*
>
> *Andre aktuelle områder kan være IKT-sikkerhet i forhold til IKT-drift generelt. For Tynset kommune driftes IT-systemene av IKT Fjellregionen IKS. Organisering av IT-funksjoner i et interkommunalt selskap innebærer større avstand og mindre innflytelse på drift og utvikling fra kommunen enn om kommunen hadde driftet systemene selv. Dette kan innebære både fordeler og ulemper for Tynset kommune.*
>
> *Ettersom en vesentlig del av et forvaltningsrevisjonsprosjekt vil måtte rettes mot IKT Fjellregionen IKS bør det vurderes et samarbeidsprosjekt med de andre eierkommunene. Det vil også være hensiktsmessig å gjennomføre en eierskapskontroll samtidig, ettersom temaet for forvaltningsrevisjon har nær tilknytning til kommunens forvaltning av eierskapet i selskapet.*
>
> *Risikoen vurderes å være middels mens vesentligheten er vurdert til høy.*

På bakgrunn av risiko- og vesentlighetsvurderingen er IKT-sikkerhet trukket frem som et prioritert område for forvaltningsrevisjon.

1.3 AVGRENSNINGER

Revisjonen vil bygge på intervjuer, gjennomgang av dokumentasjon, test av utvalgte kontroller og penetrasjonstest gjennomført av BDO. Revisjonen vil i hovedsak omfatte felles infrastruktur som driftes hos IKT Fjellregionen IKS på vegne av kommunene i FARTT-samarbeidet. Revisjonen vil i utgangspunktet ikke omfatte infrastruktur som driftes av andre eksterne partner. Revisjonen vil ikke kunne gjennomgå alle applikasjonene som benyttes i kommunen, men vil ta utgangspunkt i de applikasjonene kontrollutvalget og administrasjonen anser som særskilt viktige. Dette avklares nærmere i planleggingsfasen av forvaltningsrevisjonen.

2 PROBLEMSTILLINGER OG REVISJONSKRITERIER

Nedenfor foreslås problemstillinger som skal dekke kontrollutvalgets bestilling. Problemstillingene er formulert mer konkret og kortfattet, og drøfting av revisjonskriterier nedenfor utdyper hva forvaltningsrevisjonen kan omfatte.

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

Tabell 1: Forslag til problemstillinger for forvaltningsrevisjonen. Kilde: Kontrollutvalget i Tynset, bearbeidet av BDO.

Nedenfor blir problemstillingene utdypet og kriterier satt.

2.1 KILDEGRUNNLAGET FOR REVISJONSKRITERIENE

I denne prosjektplanen trekkes det særlig på følgende kilder som grunnlag for revisjonskriteriene:

- Lov om kommuner og fylkeskommuner (kommuneloven)
- Forskrift om kommunal beredskapsplikt
- NSMs grunnprinsipper for IKT-sikkerhet 2.0
- ISO/IEC 27001:2017 Ledelsessystemer for informasjonssikkerhet (heretter omtalt som ISO/IEC 27001)
- Digitaliseringsdirektoratet (2020), Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner, Kunnskapsgrunnlag – En dokumentstudie.

2.2 OPERASJONALISERING AV PROBLEMSTILLINGENE

I avsnittene nedenfor konkretiseres revisjonens problemstillinger med forslag til områder som skal undersøkes nærmere, og hvilke kriterier problemstillingene skal vurderes mot.

2.2.1 Problemstilling 1:

Styrer selskapet informasjonssikkerheten på en tilfredsstillende måte?

Denne problemstillingen omfatter hvordan selskapet styres i henhold til informasjonssikkerheten. En viktig kilde vil være det skriftlige grunnlaget til selskapet, herunder om det eksisterer et styringssystem for informasjonssikkerhet. Generelt vil revisjonen omfatte de vurderingene FARTT har gjort i henhold til omfanget av styringssystemet sett opp mot sikringsmål og -tiltak i ISO/IEC 27001.

Under denne problemstillingen er det naturlig å kartlegge hvilke styrende dokumenter for informasjonssikkerhet selskapet har utarbeidet samt hvordan roller og ansvar er definert, jf. ISO/IEC 27001 kontrollkategori A.5 og A.6.

Denne problemstillingen vil hovedsakelig bli kartlagt gjennom dokumentstudier og intervjuer.

Kriterier

Det foreslås å legge følgende kriterier til grunn for forvaltningsrevisjonen:

- *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.*

2.2.2 Problemstilling 2:

Blir sikkerhetsrisikoer identifisert og håndtert?

NSMs grunnprinsipper for IKT-sikkerhet 2.0 og ISO/IEC 27001 har flere tiltak knyttet til identifisering og håndtering av sikkerhetsrisikoer. NSMs grunnprinsipp 9 og 10 omhandler kartlegging av enheter og programvare som benyttes, herunder utarbeide en oversikt over eksisterende.

Kartlegging av enheter og programvare er viktig for å få oversikt over hva som befinner seg i selskapet. Kartleggingen av enheter bør avdekke både virksomhetsstyrte enheter, legitime enheter med begrensede rettigheter (for eksempel IoT-enheter) og ukjente enheter (kan være f.eks. ansattes private utstyr eller 'ondsinnede' enheter). Tilsvarende bør kartlegging av programvare dekke all programvare som benyttes i selskapet, både installert av IT-avdelingen og uautorisert programvare. Det er viktig at selskapet selv skaffer oversikt over enheter, programvare og deres sårbarheter før angripere gjør det.

Det vil til enhver tid være sikkerhetsrisikoer som må håndteres, og for å sikre at tiltak iverksettes der de er mest hensiktsmessig er det nødvendig at det gjennomføres en risiko- og sårbarhetsanalyse av IKT-systemene. ISO/IEC 27001 stiller krav om at kontroller velges på bakgrunn av en risikovurdering.

Problemstillingen vil hovedsakelig bli kartlagt gjennom dokumentstudier, intervjuer og test av utvalgt materiale.

Kriterium

Det foreslås å legge følgende kriterier til grunn for forvaltningsrevisjonen:

- *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.*

2.2.3 Problemstilling 3:

Blir informasjon og informasjonssystemer beskyttet iht. beste praksis?

NSMs grunnprinsipp for IKT-sikkerhet punkt 2.2 har som målsetting at selskapet har etablert en helhetlig sikkerhetsarkitektur som ivaretar ønsket sikkerhetsnivå gjennom gode sikkerhetsfunksjoner og sikkerhetsstrukturer med mulighet for etterprøvbarhet.

Angripere forsøker alltid å finne de inngangene som enklest kan gi tilgang til og kontroll over et informasjonssystem. For å sikre en helhetlig sikkerhet, er det viktig å etablere en sikker IKT-infrastruktur. Vi vil blant annet se på brukerhåndtering, drifts og sikkerhetskonfigurasjon, og inndelingen av IKT-systemene.

Virksomheter tjenesteutsetter flere og flere tjenester, men har likevel det samme ansvaret for å ivareta sikkerheten. NSM Grunnprinsipp punkt 2.1.10 stiller krav om å undersøke sikkerheten hos tjenesteleverandør ved tjenesteutsetting. BDO ønsker å gjennomgå risikovurderinger og leverandøroppfølging gjort i forbindelse med tjenesteutsettelse.

En virksomhet kan aldri garantere at et dataangrep ikke vil inntreffe. Det er derfor essensielt at det er etablert en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap om en hendelse likevel skulle inntreffe. Dette vil undersøkes ved å gjennomgå prosesser og rutiner som er etablert for sikkerhetskopiering og lagring av data.

Denne problemstillingen vil primært kartlegges gjennom dokumentstudier, intervjuer og test av utvalgt materiale.

Kriterier

Det foreslås å sette følgende kriterier for denne problemstillingen:

- *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 sikkerhetskopiering av all virksomhetsdata for kommunene.*

2.2.4 Problemstilling 4:

Hvordan oppdages avvik og mulige trusler mot virksomheten?

Norske virksomheter står overfor en eskalering i antall dataangrep mot IKT-systemer. Innsamling og analyse av relevante data kan resultere i at sikkerhetshendelser oppdages tidlig, og med det avgrense angrepet eller minimere skadeomfanget. NSM grunnprinsipp punkt 3.2 stiller krav om å etablere sikkerhetsovervåkning av IKT-systemer.

NSMs grunnprinsipp 3.4 fremmer behovet for å gjennomføre inntrengningstester (penetrasjonstest) for å teste elementer i egne forsvarsmekanismer. BDO skal som en del av forvaltningsrevisjonen gjennomføre en penetrasjonstest. Videre er det ønskelig å gjennomgå

resultatene av eventuelle tidligere gjennomførte penetrasjonstester for å se i hvilken grad endringer gjøres når avvik oppdages.

Sikkerhetsovervåkning og inntrengningstester er to av flere måter å oppdage sårbarheter og trusler i IKT-systemet. NSMs grunnprinsipp 3.1. omhandler å oppdage og fjerne sårbarheter og trusler. BDO vil se hvilke rutiner som er etablert for å oppdage og kartlegge sårbarheter, samt hvordan oppdagede sårbarheter håndteres (reduseres eller fjernes).

Denne problemstillingen vil primært kartlegges gjennom dokumentstudier, intervju og penetrasjonstesting.

Kriterier

Vi foreslår følgende 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.*

2.2.5 Problemstilling 5:

Blir hendelser håndtert på en tilfredsstillende måte?

Den økende trusselen for angrep mot IKT-system setter krav til at virksomheter må være forberedt på hvordan de håndterer hendelsene når de inntreffer. Målet med NSMs grunnprinsipp 4.1 er at selskapet har implementert effektive prosesser for hendelseshåndtering. BDO vil evaluere etablerte prosesser for hendelseshåndtering og krisehåndtering.

For å være mest mulig forberedt på en uønsket hendelse er det essensielt å gjennomføre øvelser. BDO ønsker derfor å vurdere dokumentasjon av de siste øvelsene som slekspaet har gjennomført, evalueringer av disse og læringspunkter. BDO ønsker også å gjennomgå dokumentasjon fra de siste hendelsene som har inntruffet og oppfølgingen av disse.

Denne problemstillingen vil primært kartlegges gjennom dokumentstudier, intervjuer og test av utvalgt materiale.

Kriterier

Vi foreslår følgende 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.*

3 GJENNOMFØRING AV REVISJONEN

Forvaltningsrevisjonen vil gjennomføres i henhold til RSK 001 - Standard for forvaltningsrevisjon. Det innebærer blant annet at kommunedirektøren vil få en orientering om oppdraget før oppstart og gis mulighet til å uttale seg om rapportutkast før endelig rapport gis.

Revisor har taushetsplikt i alle forhold som vedrører forvaltningsrevisjonsprosjektet. For alle formål er vurderingene som gjøres avhengig av at informasjonsgrunnlaget de bygger på, er riktig og fullstendig. Vi legger til grunn at alle nødvendige opplysninger gjøres tilgjengelig i

gjennomføringen av oppdraget. Videre er vi avhengige av at sentrale ressurser gjøres tilgjengelige for intervju og samtale i den grad dette er nødvendig.

3.1 METODER FOR GJENNOMFØRING

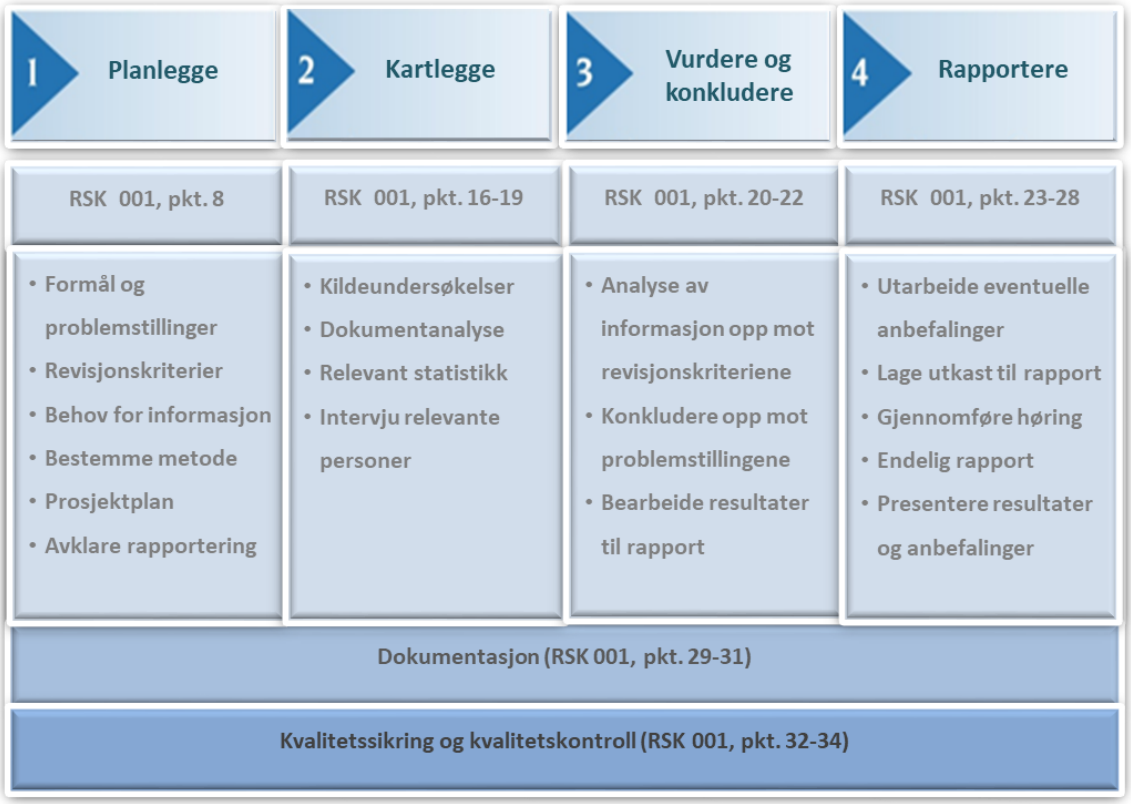
Metoder for gjennomføring av prosjektet vil primært være dokumentgjennomgang, intervjuer og test av utvalgt materiale. Det vil videre gjennomføres en penetrasjonstest. Det redegjøres nærmere for disse metodene under.

3.2 PRAKTISK GJENNOMFØRING

Arbeidet vil bli gjennomført i følgende faser:

- planlegge
- kartlegge
- vurdere og konkludere
- rapportere

Innholdet i fasene kan illustreres slik:



Figur 1 Metodisk gjennomføring (Kilde: BDO)

3.2.1 Planlegge

Planleggingsfasen starter med at foreliggende prosjektplan godkjennes i kontrollutvalget.

Revisjonsteamet har på forhånd satt seg inn i relevant regelverk. Dette danner bakgrunnen for operasjonalisering av problemstillingene skissert over. I tillegg er det identifisert relevante revisjonskriterier for problemstillingene.

Viktige aktiviteter som inngår i planleggingsfasen, inkluderer:

- oppstartsmøte med nøkkelpersoner i kommunen, andre kommuner i FARTT-samarbeidet, IKT Fjellregionen IKS og BDO
- oppnevne kontaktperson(er) i kommunene
- avklare hvilke personer, funksjoner og områder som skal involveres i prosjektet
- avgrense hvilke sektorvise IKT-systemer og applikasjoner som skal omfattes av revisjonen
- detaljplanlegging av når ulike aktiviteter skal gjennomføres

3.2.2 Kartlegge

Formålet med kartleggingsfasen er å fremskaffe nødvendig informasjon og dokumentasjon som grunnlag for revisjonen. Det må sikres at denne informasjonen er tilstrekkelig både i omfang, detaljeringsnivå og kvalitet. Kartleggingen vil bestå av dokumentanalyser, intervjuer samt innhenting av relevante materiale.

Dokumentanalyser

Formålet med analyse av dokumenter er å kartlegge hva som er de førende dokumentene og det viktigste planverket for IKT-sikkerhet i kommunene i FARTT-samarbeidet og IKT Fjellregionen IKS. Dette inkluderer informasjonssikkerhetspolicyer og andre styrende dokumenter, risikovurderinger og beredskapsplanverk og øvrige relevante rutiner og retningslinjer.

Intervjuer

Vi foreslår at det gjennomføres intervjuer med følgende:

- medlemmer av Sikkerhetsutvalget i FARTT
- utvalgte nøkkelpersoner i kommunene
- driftsleder i IKT Fjellregionen IKS og ev. andre nøkkelpersoner
- utvalgte IKT rådgivere i kommunene

Intervjuene kan være en kombinasjon av individuelle samtaler og gruppesamtaler avhengig av hva som er mest hensiktsmessig.

Intervjuene vil være semistrukturerte dybdeintervjuer basert på intervjumaler. Referatene fra intervjuene vil bli verifisert.

Penetrasjonstest fra internett

Tjenester eksponert på internett utsettes daglig for angrepsforsøk. Et vellykket dataangrep kan føre til tap av virksomhetssensitive data og skape nedetid. Det er også en risiko for at sårbarheter i skytjenester kan utnyttes til å installere spionprogramvare eller annen skadevare på ansattes PC-er.

En penetrasjonstest fra internett vil gi kunden kunnskap om aktuelle angrepsvektorer og eventuelle sårbarheter i tjenestene. Tjenestene er webbasert, slik at testingen vil konsentreres om tilgang til disse gjennom brukeridentiteter (skykontoer) og webbaserte sårbarheter (OWASP Top 10). Testresultatene kan brukes som grunnlag for å prioritere forebyggende tiltak for å styrke sikkerheten for selskapets digitale verdier.

BDO tilbyr en penetrasjonstest som inkluderer passordgjetting og forsøk på målrettet datainnbrudd. Våre funn dokumenteres i en rapport. Rapporten inneholder

- sammendrag – forklaring av sårbarheter og konsekvenser på et overordnet nivå
- testresultater – tekniske detaljer til IT-personell inkludert anbefalte tiltak

Penetrasjonstest

Penetrasjonstesting er en effektiv måte å få testet motstandsdyktighet mot datainnbrudd. Hensikten er å identifisere angrepsvektorer mot virksomhetskritiske systemer, sensitiv informasjon og økonomiske verdier. Ofte kan slike tester peke på risiko som selskapet ikke var kjent med.

Gjennom en penetrasjonstest fra internett (utsidetest) simuleres en målrettet trusselaktørs aktiviteter for å utnytte sårbarheter og forsøksvis oppnå uautorisert tilgang til webtjenester og PC-er/servere. Testen inkluderer

- manuell rekognosering og søk i åpne kilder
- passordgjetting
- utnyttelse av sikkerhetshull
- realistisk test av eksisterende sikkerhetsmekanismer
- IT-personell kan få oppleve deteksjon og håndtering av målrettet datainnbrudd

Manuell rekognosering og søk i åpne kilder

BDO gjennomfører manuell rekognosering og søk i åpne kilder med formål om å identifisere relevante angrepsvektorer som kan utnytte eventuelle svakheter i selskapets IT-systemer som er eksponert mot internett. Det søkes blant annet etter e-postadresser og brukernavn, og tjenester som kan utnyttes til å gjette passord.

Passordgjetting

Vår erfaring fra sikkerhetstester viser at svake passord i mange tilfeller kan representere sikkerhetshull. BDO utfører derfor utvidet passordgjetting mot påloggingstjenester, noe som kan være særlig relevant for skytjenester, for å gi et reelt bilde av sårbarhet fra internett. Gjettingen utføres i begrenset omfang, slik at det er lav sannsynlighet for at brukerkontoer blir sperret.

Manuell penetrasjonstesting og eskalering av rettigheter

Som del av en penetrasjonstest fra internett vil BDOs etiske hackere forsøke å utnytte eventuelle sikkerhetshull, eskalere brukerrettigheter og identifisere mulighetene for videre spredning i øvrige systemer og interne nettverk. Det overordnede målet med disse øvelsene er å identifisere hvor langt inn i selskapets IT-systemer en ondsinnet trusselaktør kan komme, og hvilken informasjon som potensielt kan uthentes.

Innsidetest

BDO vil utføre sårbarhetsskanning internt i selskapets nettverk. BDO kommer on-site og kobler seg til en nettverksport for å simulere vellykket utsideangrep. Det skannes for klienter og servere, og det undersøkes om det finnes kjente sårbarheter.

Klienttest

BDO mottar en klient-pc fra selskapet og vurderer denne for sårbarheter som kan utnyttes av en trusselaktør som har fått tak i maskinen fysisk, eller som har tatt kontroll over maskinen basert på et vellykket nettfiskeangrep.

3.2.3 Vurdere og konkludere

De etablerte revisjonskriteriene vil være målestokken for våre vurderinger. Ut fra dokumentasjonen og analysene vil det bli konkludert opp mot den enkelte problemstilling.

3.2.4 Rapportere

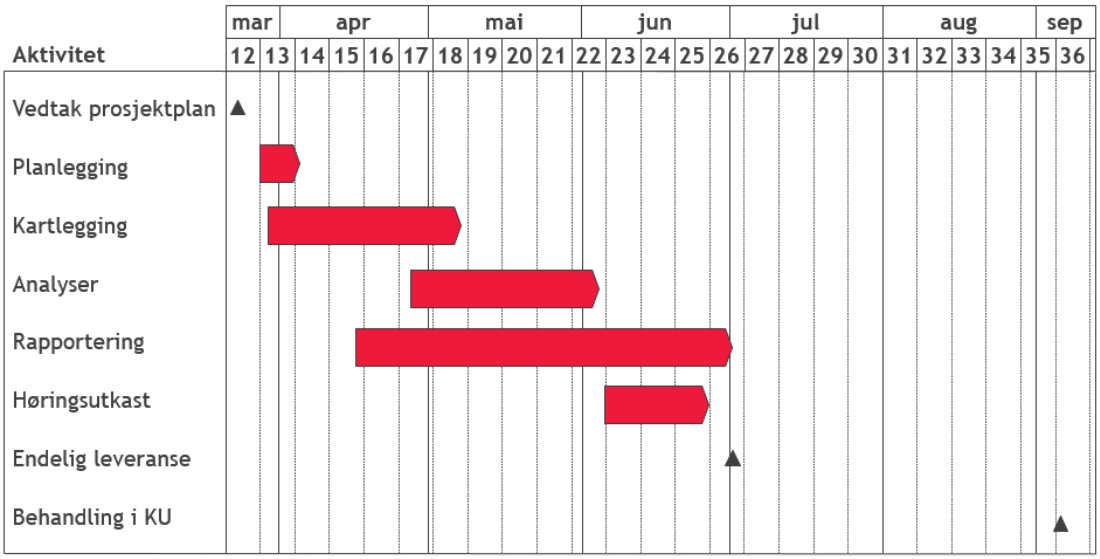
Rapporten vil ta utgangspunkt i de enkelte problemstillingene og redegjøre for faktagrunnlaget, våre vurderinger opp mot revisjonskriteriene og våre konklusjoner. Der det anses hensiktsmessig, vil vi gi anbefalinger.

Kommunedirektøren gis anledning til å kommentere forhold som framgår av rapporten, og høringssvaret legges ved rapporten. I høringen blir det bedt om å bekrefte faktabeskrivelsen slik at forvaltningsrevisor bygger sine vurderinger og konklusjoner på riktig grunnlag. Revisor kan også finne det riktig å kommentere kommunedirektørens høringskommentar. Det kan være hensiktsmessig å presentere utkast til rapport i et møte med kommunedirektøren.

Endelig rapport oversendes kontrollutvalgssekretariatet. Rapporten vil presenteres for kontrollutvalget når forvaltningsrevisjonsrapporten skal behandles.

4 FREMDRIFTSPLAN

Prosjektet er planlagt gjennomført slik figuren under viser.



Figur 2: Forslag til fremdriftsplan for oppdraget. (Kilde: BDO)

Figuren viser at oppstart legges til siste uken i mars etter at kontrollutvalget har behandlet foreliggende prosjektplan i møte 21. mars 2023. Deretter følger fasene for kartlegging og analyse. Vi oversender utkast til høring primo juni 2023 med ca. en ukes høringstid. Deretter bearbeides høringsinnspillene og rapporten ferdigstilles. Endelig rapport oversendes til kontrollutvalgssekretariatet før sommerferien slik at den kan behandles i kontrollutvalgets møte 4. september 2023.

Fremdriftsplanen er laget med forbehold om oppstart kort tid etter kontrollutvalgsmøte 21. mars 2023. Ved lengre utsettelse av igangsetting, kan høringsutkast utsettes til uke 32. Rapporten vil da fortsatt kunne behandles i kontrollutvalgets møte 4. september 2023.

Revisor vil gi løpende orientering om fremdrift underveis i prosjektet.

5 ORGANISERING OG RESSURSESTIMAT

BDO planlegger å gjennomføre oppdraget med følgende revisjonsteam:

- Siv Irene Aasen: Oppdragsansvarlig partner
- Øyvind Sunde: Kvalitetssikrer
- Jonas Strisland: Prosjektleder og gjennomføringsressurs
- Niklas Krohn: Gjennomføringsressurs, Fagekspert IT-sikkerhet
- Simen Rune Bragen: Fagekspert penetrasjonstest
- Gjennomføringsressurser etter behov (fastsettes eventuelt senere)

Nedenfor følger et ressursestimat for oppdraget. Avtalt gjennomsnittlig timepris på kroner 1 200 ekskl. mva. ligger til grunn for estimatet.

Fase	Estimert tidsbruk	Sum i kroner ekskl. mva.
Planlegging	20 timer	24 000
Kartlegging	70 timer	84 000
Analyser	50 timer	60 000
Penetrasjonstest	70 timer	84 000
Rapportering	50 timer	60 000
Presentasjon	10 timer	12 000
Samlet	**270 timer**	**324 000**

Tabell 2: Ressursestimat for oppdraget. (Kilde: BDO)

Tabellen viser at vi estimerer samlet ressursbruk på 270 timer for dette oppdraget, tilsvarende 324 000 kroner ekskl. mva. Arbeid med planlegging omfatter hovedsakelig å utvikle foreliggende prosjektplan. Estimatet inkluderer også fysisk oppmøte én gang for å presentere rapporten, eksempelvis for kommunestyret. Øvrige møter, intervjuer og lignende foreslås gjennomført digitalt.

Dersom det ikke er ønskelig med presentasjon for alle kontrollutvalgene, kan rammen reduseres med 5 timer, eller omdisponeres til tid brukt på kartlegging og rapportering.

5.1 REVISORS UAVHENGIGHET

De personene som skal gjennomføre forvaltningsrevisjonen, vil bli vurdert for uavhengighet og objektivitet. Den enkeltes uavhengighet vil også bli vurdert løpende gjennom hele prosjektperioden.

KONTAKT

SIV IRENE AASEN

Partner

m: +47 982 06 148
e: siv.irene.aasen@bdo.no