Forvaltningsrevisjonsrapport

RÅDE

16.01.2023

Forvaltningsrevisjon
Informasjonssikkerhet

Innhold

1 SAMMENDRAG

Rapporten besvarer følgende problemstillinger:

Denne forvaltningsrapporten har vi vurdert hvorvidt Råde kommune følger Digitaliseringsdirektoratets (Digdir) krav og anbefalinger gjeldende digital informasjonssikkerhet, og om kommunens ansatte kjenner til kommunens egne retningslinjer og rutiner for informasjonssikkerhet.

Revisjonskriteriene i rapporten er utledet med bakgrunn i Digdirs krav og anbefalinger innen digitalisering, nærmere bestemt de krav og anbefalinger som gjelder informasjonssikkerhet.

Revisjonens fremgangsmåte

En av målsetningene med forvaltningsrevisjonen har vært å kontrollere om kommunens arbeid med digital informasjonssikkerhet er i tråd med de krav og anbefalinger til informasjonssikkerhet som Digdir stiller på tidspunkt for revisjon. Dette gjelder blant annet krav til etablert internkontroll, bruk av protokoller for kommunikasjon på internett og på nettsteder, og bruk av kravspesifikasjon for PKI. Videre gjelder det blant annet anbefalinger knyttet til NSMs grunnprinsipper for IKT-sikkerhet, støtte for protokoller for filoverføringer, og sikkerhetsanbefalinger for å redusere risiko for brudd på integritet ved oppslag i domenenavnsystemet, samt sikring av epost og kommunikasjonskanaler.

Den andre målsetningen har vært å kontrollere om kommunens ansatte har kjennskap til de retningslinjer og rutiner for informasjonssikkerhet som kommunen har etablert, og om de ansatte mener å ha fått tilstrekkelig opplæring og kunnskap innen digital informasjonssikkerhet.

For å svare ut problemstillingene har revisjonen gjennomgått sentrale dokumenter knyttet til internkontroll og informasjonssikkerhet, gjennomført intervjuer med fagansvarlig beredskap og fagansvarlig digital informasjonssikkerhet, samt sendt ut en spørreundersøkelse til ansatte i kommunen som anses å benytte digitale verktøy i sitt daglige arbeide. Spørreundersøkelsen er gjennomført ved hjelp av Questback, et nettbasert verktøy for spørreundersøkelser.

Revisjonens funn og konklusjoner

Kommunen har flere dokumenter og prosedyrer som omhandler internkontroll og informasjonssikkerhet, og revisjonens inntrykk er at kommunen jobber aktivt med informasjonssikkerhet. Etter revisjonens vurdering følger Råde kommune i stor grad Digitaliseringsdirektoratet sine krav og anbefalinger gjeldende digitalisering i sitt informasjonssikkerhetsarbeid. Vi har funnet enkelte forbedringsområder. Undersøkelsen viser i noen tilfeller at det er manglende samsvar mellom hva som er beskrevet i kommunens dokumenter, og hva som er kommunens praksis. I tillegg er det en svakhet at sentralt datarom ikke er sikret med elektronisk dørlås for sporbarhet og sikring mot tilgang fra uvedkommende. Vi ser også at standarder for bruk av VPN i liten grad er fulgt opp, ved at kun seks av syv løsninger er i henhold til veiledning for bruk av VPN.

Når det gjelder ansattes kjennskap til retningslinjer og rutiner har revisjonen funnet at kommunen har etablert flere tiltak som er egnet til å sikre ansattes kjennskap til retningslinjer og rutiner for informasjonssikkerhet. Fakta viser at Råde kommune på flere måter har arbeidet for å skape en kultur med fokus på informasjonssikkerhet og etter revisjonens vurdering har de i stor grad lyktes med det, selv om det viser seg at det er noe manglende kjennskap til konkrete dokumenter/rutiner/retningslinjer.

Revisjonens anbefalinger

Basert på revisjonens funn anbefaler vi at kommunen bør:

a) sørge for at det er samsvar mellom prosedyrer og praksis, og oppdatere dokumentene der det er nødvendig, herunder:
    a. Virksomhetsstyring og internkontroll i Råde kommune
    b. Funksjoner innen internkontroll, beredskap, digital personsikkerhet og HMS
    c. Prosedyre for oppretting eller fjerning av brukere
    d. IKT beredskapsplan
b) vurdere å utarbeide opplæringsplan innen digital sikkerhet
c) anskaffe elektronisk dørlås til sitt sentrale datarom
d) sørge for at alle VPN-løsninger er oppdatert i henhold til Digdirs anbefalinger
e) følge opp at de ansatte gjennomfører nanolæring
f) sørge for at virksomhetene i større grad gjennomfører dialogmøter med IKT-avdelingen
g) sørge for at de ansatte i større grad har kjennskap til IKT reglementet
h) sørge for at relevante ledere har større grad av kjennskap til dokumentet virksomhetsstyring og internkontroll i Råde kommune, herunder også deres ansvar for internkontroll (også innen informasjonssikkerhet)
i) sørge for at ansatte lagrer opplysninger i tråd med kommunens reglement
j) sørge for at det i større grad meldes fra om avvik på informasjonssikkerhetsområdet, og at avvikssystemet benyttes til dette

2 PROSJEKTMANDAT

Revisjonen skal i henhold til kommunelovens § 24-2 (1) utføre forvaltningsrevisjon. Etter loven innebærer forvaltningsrevisjon å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger. Østre Viken kommunerevisjon IKS gjennomfører forvaltningsrevisjon i tråd med god kommunal revisjonsskikk, som vil si å følge *Standard for forvaltningsrevisjon* (RSK 001) (NKRF[1], 2020). Dette innebærer blant annet at rapporten skal skille klart mellom innsamlede data (fakta) og revisjonens vurderinger. Det skal være en tydelig sammenheng mellom problemstillinger, faktaopplysninger[2], vurderinger, konklusjoner og eventuelle anbefalinger. Etter kommuneloven skal revisor rapportere resultatene av sin revisjon til kontrollutvalget.

Forvaltningsrevisjonen er gjennomført på bakgrunn av plan for forvaltningsrevisjon januar 2022 – juli 2024, som ble vedtatt i kommunestyret i Råde kommune i sak 078/21 (9.12.2021).

Plan for gjennomføring av forvaltningsrevisjonen ble vedtatt i kontrollutvalget 20.6.2022.
Planen ble vedtatt i tråd med revisjonens forslag.

Forvaltningsrevisjonen er gjennomført etter vedtatt prosjektplan i tidsrommet august – desember 2022. Vi har gjennomført et oppstartsmøte med kommuneadministrasjonen slik at også administrasjonens innspill er vurdert i planleggingsprosessen.

Vi har kvalitetssikret innsamlet data/fakta underveis, både gjennom verifisering av intervjuer og intern kvalitetssikring. I tillegg er faktaopplysningene i sin helhet verifisert av kommunen, slik at eventuelle feil eller misforståelser er rettet opp. Revisjonen avholdt avsluttende møte med administrasjonen 5.1.2023 hvor revisjonens vurderinger, konklusjoner og anbefalinger ble gjennomgått. I etterkant av møtet er rapporten sendt på høring til kommunedirektøren. Kommunedirektørens uttalelse fremgår av vedlegg 1 (kap. 7.1).

Forvaltningsrevisjonen er gjennomført av forvaltningsrevisor Anita Marie Torp og Lene Brudal. Revisorenes habilitet og uavhengighet er vurdert opp mot kommunen og den undersøkte virksomheten, og revisjonen finner de habile til å utføre forvaltningsrevisjonen.

Revisor vil takke kontaktperson og andre som har deltatt for et godt samarbeid i forbindelse med gjennomføringen av forvaltningsrevisjonen.

Østre Viken kommunerevisjon IKS
Rolvsøy, 16. januar 2023

Lene Brudal (sign.)
oppdragsansvarlig revisor

Anita Marie Torp (sign.)
utførende forvaltningsrevisor

[1] NKRF er en faglig interesseorganisasjon og et kompetanseorgan for kontroll og revisjon av kommunal/offentlig virksomhet.

[2] Fakta er en gjengivelse av informasjonen vi har fått tilgang til gjennom datainnsamlingen.

3 FREMGANGSMÅTE

3.1 Problemstillinger og avgrensninger

Rapporten besvarer følgende problemstillinger:

Problemstilling 1: Følger Råde kommune Digitaliseringsdirektoratet sine krav og anbefalinger gjeldende digitalisering i sitt informasjonssikkerhetsarbeid?
Problemstilling 2: Har de ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

3.2 Om revisjonskriterier

I henhold til forskrift om kontrollutvalg og revisjon § 15 skal revisor fastsette revisjonskriterier for den enkelte forvaltningsrevisjon. Revisjonskriteriene er den objektive målestokk som setter revisor i stand til å gjøre vurderinger på de fleste områder uten å ha formell fagspesifikk kompetanse. Revisjonskriteriene og revisors kunnskap og erfaring innen forvaltningsrevisjonsmetodikk, gjør at revisor kan gjøre objektive og holdbare vurderinger.

Revisjonskriteriene etablerer den norm som de innsamlede dataene skal vurderes opp mot. I tillegg til dette skal revisjonskriteriene også gjøre det tydelig for den reviderte enhet hva de måles opp mot. Revisjonskriteriene klargjør også overfor folkevalgte, media og andre lesere av forvaltningsrevisjonen, hva revisors vurderinger bygger på. Dette vil gjøre det enklere å etterprøve revisors vurderinger. Revisjonskriteriene skal være relevante, konkrete og i samsvar med de kravene som gjelder for revidert enhet.

Revisjonskriterier fastsettes vanligvis med basis i en eller flere følgende kilder: lovverk, politiske vedtak og føringer, kommunens egne retningslinjer, anerkjent teori på området, eller andre sammenlignbare virksomheters løsninger og resultater.

3.3 Revisjonsmetoder

I henhold til god revisjonsskikk skal praksis eller tilstand innen det reviderte området beskrives i et omfang som i tilstrekkelig grad underbygger revisors vurderinger og konklusjoner. I denne forvaltningsrevisjonen har vi benyttet data fra ulike kilder, og brukt ulike metoder for innsamling av data, for å sikre et faktagrunnlag med høyest mulig grad av gyldighet og pålitelighet.

Utfordringer og begrensninger i rapportens faktagrunnlag beskrives nedenfor sammen med beskrivelsen av de ulike metodene som er benyttet. Vi tar også hensyn til metodens begrensninger i vurderingene.

I denne forvaltningsrevisjonen er informasjonen hentet inn gjennom bruk av følgende metoder:

- Dokumentanalyse
- Intervjuer
- Spørreundersøkelse

Dokumentanalyse

Vi har gjennomgått sentrale dokumenter på området. Blant annet er IKT reglementet, IKT beredskapsplan, Virksomhetsstyring og internkontroll i Råde kommune og Håndbok for informasjonssikkerhet og personvern Råde kommune sentrale for revisjonens undersøkelse. Dokumentene er oversendt fra kommunen. Fullstendig oversikt over dokumentene fremgår av kildehenvisningene i kapittel 6.

Intervjuer

Det er totalt gjennomført 2 intervjuer:

- Fagansvarlig beredskap
- Fagansvarlig digital informasjonssikkerhet

Alle intervjuer er verifisert. Det betyr at den som er intervjuet, har fått lese gjennom referatet fra intervjuet for å bekrefte at referatet er i overenstemmelse med det som ble sagt under intervjuet, og rette opp eventuelle misforståelser.

Det er i tillegg gjennomført arbeidsmøte med fagansvarlig beredskap og fagansvarlig internkontroll, samt stilt spørsmål per e-post til fagansvarlig internkontroll.

Spørreundersøkelse

Det er gjennomført en spørreundersøkelse blant kommunens ansatte. Undersøkelsen er gjennomført ved hjelp av det nettbaserte spørreundersøkelsesverktøyet Questback.

Spørreundersøkelsen ble sendt ut til de av kommunens ansatte som antas å bruke kommunens informasjonssystemer i sitt daglige arbeid. Undersøkelsen ble sendt til 261 ulike e-postadresser, og det ble mottatt 101 svar. Det gir en svarprosent på 38,7 %. Dette er lavere enn ønskelig, men revisjonen vurderer likevel at spørreundersøkelsens resultater sammenstilt med funn fra øvrige kontrollhandlinger er tilstrekkelig for å gjøre pålitelige vurderinger. Hovedtyngden av respondentene, 87,1 %, jobber 80 % eller mer, og 91,1 % er fast ansatt i kommunen. Tabellen nedenfor viser hvordan respondentene fordeler seg i kommunen.

Hvor i kommunen jobber du?	Prosent
Kommunedirektørens administrasjon	4,0%
Stab kompetanse og utvikling	14,9%
Stab økonomi	5,0%
Virksomhet familie	3,0%
Oppvekstområdet Saltnes	16,8%
Oppvekstområdet Karlshus	22,8%
Råde ungdomsskole og kulturskole	15,8%
NAV	0,0%
Helse-, omsorg og rehabilitering	2,0%
Tildelingskontor	3,0%
Ankomstsenter	0,0%
Miljø, plan og teknikk	12,9%
Annet	0,0%
Antall respondenter	101

Tabell 1 Hvor i kommunen jobber du?

Spørreundersøkelsen besto av 27 spørsmål. Målsettingen med spørreundersøkelsen var å få et inntrykk av hvor god opplæring de ansatte selv opplever å ha fått innen informasjonssikkerhet, samt om de kjenner til kommunens sentrale dokumenter på området.

4 DIGITALISERINGSDIREKTORATETS KRAV OG ANBEFALINGER

Problemstilling 1:

Følger Råde kommune Digitaliseringsdirektoratet sine krav og anbefalinger gjeldende digitalisering i sitt informasjonssikkerhetsarbeid?

4.1 Revisjonskriterier

Revisjonskriteriene er punktvis oppsummert nedenfor.

Kommunen skal:

- ha en etablert internkontroll på informasjonssikkerhetsområdet, som er basert på en vurdering/identifisering av relevante lov- og regelverk, herunder bør kommunen bruke Digdirs «Internkontroll i praksis – informasjonssikkerhet» i arbeidet med internkontroll, konkretisert i følgende syv hovedpunkter:
    - Ledelsens styring og oppfølging
    - Vurdering av risiko
    - Håndtering av risiko
    - Overvåking og hendelseshåndtering
    - Måling, evaluering og revisjon
    - Kompetanse- og kulturutvikling
    - Kommunikasjon

- bruke IPv4 og IPv6 ved kommunikasjon på internett, og vurdere om nytt IT-utstyr støtter disse protokollene.
- bruke kravspesifikasjon for PKI ved anskaffelse av PKI-tjenester, når det er obligatorisk.
- bruke HTTPS på sine nettsteder, og ved eventuelle andre offentlige tjenester der http-protokoll brukes for overføring.

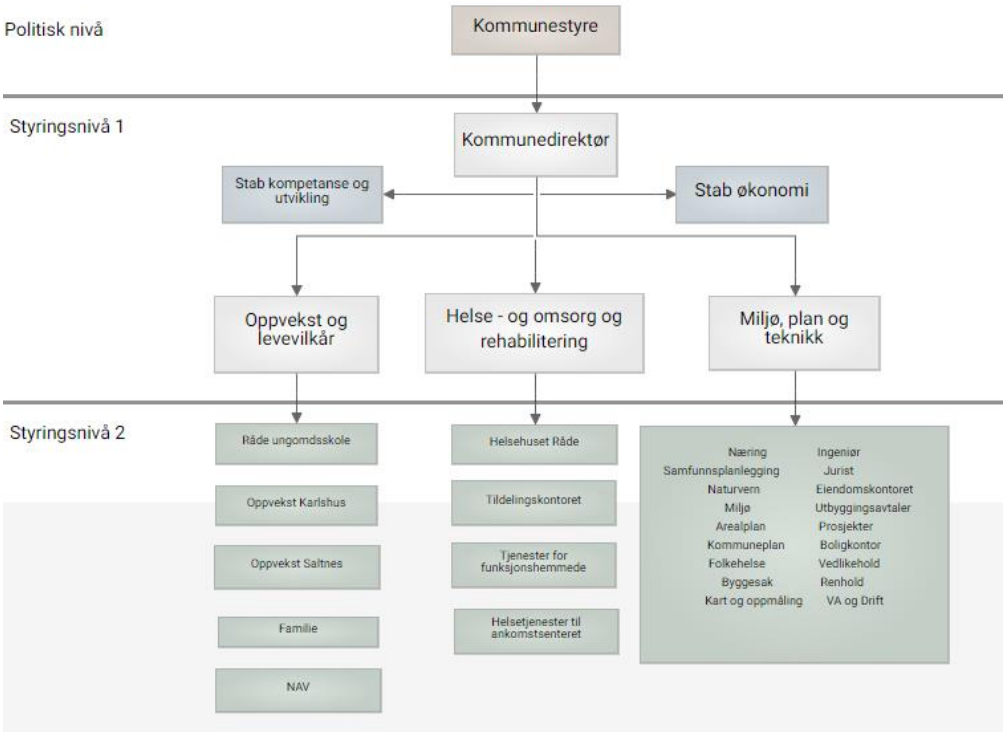
Kommunen bør:

- bruke NSM sine grunnprinsipper for IKT-sikkerhet i sitt arbeid med informasjonssikkerhet.
- støtte FTP som protokoll for filoverføring.
- bruke DNSSEC for å redusere risikoen for brudd på integritet ved oppslag i domenenavnsystemet.
- bruke standarder fra Digdirs veiledning for bruk av VPN, for å sikre sine kommunikasjonskanaler.
- bruke DMARC for å motvirke falske avsendere av e-post. DMARC brukes som anbefalt sammen med SPF og/eller DKIM.
- bruke STARTTLS og SPF for transportsikring av e-post.

4.2 Datagrunnlag

4.2.1 Organisering

Råde kommune har organisert sin virksomhet i tre seksjoner for tjenestelevering, og to staber som ivaretar kommunens fellesfunksjoner.



Figur 1 Råde kommunes organisasjonskart

Organisert under Stab Kompetanse og utvikling finner vi:

- HR
- Organisasjonsutvikling
- Kommunikasjon og servicetorg
- Dokumentforvaltning/arkiv
- IKT
- Politisk sekretariat
- Internkontroll og kvalitetsarbeid
- Personvern

I denne staben, plassert under kommunedirektøren, finner vi kommunens arbeid med internkontroll, herunder også internkontroll på informasjonssikkerhetsområdet. Funksjonene og deres plassering er hentet fra kommunens dokument «Funksjoner innen internkontroll, beredskap, digital personsikkerhet og HMS».

Funksjonen fagansvarlig beredskap er lagt til stabsleder ved Stab kompetanse og utvikling. Når det gjelder fagansvarlig internkontroll er denne rollen plassert hos rådgiver internkontroll og beredskap, som jobber under internkontroll i Stab Kompetanse og utvikling. Fagansvarlig digital sikkerhet er lagt til rådgiver i kommunens IKT-avdeling.

4.2.1 Internkontroll

Kommunedirektørens ansvar for internkontroll etter kommuneloven § 25, er forankret i dokumentet «Virksomhetsstyring og Internkontroll i Råde kommune», hvor det også fremkommer at Rådmannsteamet er kommunens øverste ledelse av internkontrollarbeidet. Det er dette teamet som godkjenner styrende dokumenter og initierer ledelsens årlige gjennomgang av internkontrollen. Deltakere i temaet er kommunedirektør, kommunalsjefer og stabsledere.

Kommunen har også et internkontrollteam som har det overordnede ansvar for kommunenes samlede internkontroll, og som rapporterer til rådmannsteamet. Det er rådgiver for internkontroll og beredskap som leder internkontrollteamet – som i tillegg til leder består av:

- En representant fra internkontrollgruppen i hver virksomhet
- Leder av hver virksomhets internkontrollgruppe
- Rådgiver HR
- Controller økonomi
- IT konsulent

Dokumentet sier videre at hver virksomhet skal ha en egen internkontrollgruppe utpekt av virksomhetsleder. Gruppen har som oppgaver å gjennomgå kvalitetssystemet for eget område og sørge for utarbeiding og revisjon av kvalitetsdokumenter, gjennomføre ROS-analyser for eget område, sette opp plan for internkontroll i tråd med kommunens overordnede prosedyre, bidra til implementering av rutiner og prosedyrer, og lage plan for kontinuerlig intern opplæring i internkontroll og internkontrollsystemet.

Revisjonen har fått oversendt dokumentet «Funksjoner innen internkontroll, beredskap, digital personsikkerhet og HMS», hvor det fremkommer at ansvar tillagt rollen som fagansvarlig innen digital informasjonssikkerhet er å:

- Støtte virksomhetsledelsen i internkontrollspørsmål innen digital informasjonssikkerhet
- Koordinere eget arbeid med fagansvarlig for internkontroll
- Koordinere eget arbeid med fagansvarlig for personvern
- Være en ressursperson, pådriver og tilrettelegger for en god etablering og risikobasert gjennomføring av virksomhetens samlede internkontrollarbeid innen informasjonssikkerhet
- Lede og koordinere arbeidet med å avgjøre omfanget av virksomhetens fellessikring
- Utarbeide saksnotat til virksomhetsledelsens gjennomgang innen informasjonssikkerhet
- Utarbeide minimum årlige statusrapporter som grunnlag for linjeledernes risikovurderinger innen informasjonssikkerhet

På spørsmål fra revisjonen har kommunen informert om at det ikke er utarbeidet saksnotater eller årlige statusrapporter.

Under avsnitt om faste fora med roller i internkontroll- og sikkerhetsarbeidet finner vi informasjon om Sikkerhetsutvalget (informasjonssikkerhet og beredskap). Utvalget skal være et rådgivende organ i informasjonssikkerhet og beredskap, koordinere forvaltningen av IKT-system og bidra til kompetanseheving og erfaringsdeling. Stabsleder er leder av utvalget, og har i tillegg med seg:

- Fagansvarlig digital informasjonssikkerhet
- Lederrepresentant (er) fra hver virksomhet
- Systemeiere IKT-system
- Fagansvarlig for informasjonssikkerhet
- Fagansvarlig beredskap
- Fagansvarlig internkontroll
- Fagansvarlig personvern og personvernombud
- Arkivleder

Kommunen har opplyst om at fagansvarlig digital informasjonssikkerhet og fagansvarlig for informasjonssikkerhet i listen ovenfor, er en og samme rolle.

Kommunen arbeider med «Håndbok for informasjonssikkerhet og personvern i Råde kommune». Versjonen revisjonen har fått oversendt er oppdatert i mars 2022. Ifølge dokumentet er håndboken et styrende dokument som skal inneholde mål og strategi for informasjonssikkerhet og personvern, intern sikkerhetsorganisering samt identifiserte krav og plikter ved internkontroll. I tillegg til styrende dokument er det utarbeidet gjennomførende og kontrollerende prosedyrer og instrukser, som beskriver formål/omfang, målgruppe og aktiviteter for ulike prosesser innen informasjonssikkerhet og personvern.

Håndboken starter med å definere ulike begrep – som adgangskontroll, arkivverdig informasjon, autorisasjon, informasjonssikkerhet mv. Det står videre under avsnitt om formål og omfang at dokumentet skal sikre at alle ansatte ivaretar tilfredsstillende informasjonssikkerhet og personvern i Råde kommune. Videre at håndboken gjelder all informasjonsbehandling som skjer internt i kommunen, og som kommunen har ansvaret for eksternt. Dette omfatter bruk av IKT-løsninger, all behandling, lagring og kommunikasjon av informasjon både muntlig, på papir og digitalt.

Som grunnlag for håndboken, har kommunen benyttet følgende lover/retningslinjer:
- Lov om behandlingsmåten i forvaltningssaker
- Forskrift om elektronisk kommunikasjon med og i forvaltningen
- Lov om behandling av personopplysninger
- Lov om kommunale helse- og omsorgstjenester mm.
- Lov om helsepersonell mv.
- Lov om helseregistre og behandling av helseopplysninger
- Lov om pasient- og brukerrettigheter
- Norm for informasjonssikkerhet i helse- og omsorgssektoren
- Personvernprinsippene
- Veileder: internkontroll og informasjonssikkerhet (Datatilsynet)
- Veileder: internkontroll i praksis – informasjonssikkerhet (Difi)

I håndboken har kommunen definert sikkerhetsmål som beskriver kommunens overordnede mål for vern av kommunens informasjonsbehandling mot interne og eksterne trusler av tilsiktet og utilsiktet art. Sikkerhetsmålene er utformet for å sikre konfidensialitet, integritet og tilgjengelighet – slik informasjonssikkerhet er definert av Digdir og Datatilsynet.

I sikkerhetsmålene har kommunen vurdert behandling av informasjon i tråd med lover og forskrifter, forankring av informasjonssikkerhet i ledelsen, beskyttelse av sensitive opplysninger, sikring av faglig drift, informasjonstilgjengelighet, kontinuerlig vurdering av egen internkontroll for informasjonssikkerhet, og kompetanse.

Kommunens sikkerhetsmål er:
- Kommunen skal sikre at informasjon blir behandlet i tråd med kravene i relevante lover og forskrifter
- Informasjonssikkerheten i kommunen skal ha forankring i ledelsen i kommunen
- Sensitive opplysninger skal beskyttes mot uønskede hendelser og ulovlige handlinger. Uvedkommende skal ikke ha tilgang på informasjon
- Faglig drift skal sikres. Opplysninger skal være pålitelige i den forstand at de er sikret mot utilsiktet og uautorisert endring eller sletting
- Virksomhetsinformasjon skal være tilgjengelig for saksbehandler på sin arbeidsplass når han trenger den. Helse- og annen sensitive opplysninger skal være tilgjengelig der det er behov for det behandlende personell

- Kommunen skal kontinuerlig forbedre egnethet, tjenlighet og virkninger av internkontrollen for informasjonssikkerhet
- Kommunen skal sikre at ansatte har nødvendig kompetanse for å ivareta informasjonssikkerhet

Sammen med sikkerhetsmålene er det for flere av punktene satt opp sikkerhetsstrategier som skal bidra til at kommunen når de definerte målene.

Videre er det i håndboken gjort vurderinger rundt konfigurasjonsstyring, oversikt over enheter, sikkerhetsarkitektur, autorisasjon, taushetserklæring, avvik, og ansvar.

Risikovurdering på informasjonssikkerhetsområdet er ikke lagt inn i håndboken på tidspunkt for revisjon, men revisjonen har fått oversendt overordnet risikoanalyse for informasjonssikkerhet, datert 5.9.2022. Risikoanalysen er gjort i et risikostyringsverktøy.

4.2.1.1 Ledelsens styring og oppfølging

Kommunen har en IKT beredskapsplan som er et styrings, opplærings- og oversiktsdokument.
I dokumentet «Virksomhetsstyring og internkontroll i Råde kommune» fremkommer det at internkontrollen i kommunen gjennomføres etter COSO-modellen. Her beskriver kommunen at dette innebærer at alle områder for internkontroll skal følges opp ved at følgende funksjoner blir ivaretatt:

- Kontrollmiljø
    - Omfatter alt fra forhold som holdninger, atferd, verdier og kompetanse til hvordan ledelsen fordeler ansvar og myndighet, organiserer arbeidet og utvikler kommunens menneskelige ressurser. Kontrollmiljøet består av både det formelle og det uformelle i organisasjonen. Det formelle kontrollmiljøet i Råde kommune er delt opp i to nivåer: kontrollutvalgets virksomhet og kommunedirektørens internkontroll. Kommunedirektørens internkontroll er den samlede kontrollen administrasjonen fører med egen virksomhet og består av fullmakter, prosessbeskrivelser med tilhørende prosedyrer, avvikssystemet, risikoanalyser og kontinuerlig forbedringsarbeid.
    - Kommunalsjefer og virksomhetsledere har gjennom delegert fullmakt fra kommunedirektøren ansvar for internkontroll i egen virksomhet, som innebærer:
        - Å utvikle og praktisere internkontroll som en del av den daglige driften
        - Utarbeide nødvendige prosedyrer og oversikter, sørge for at ansatte er kjent med internkontrollen
        - Følge opp at virksomhetens internkontroll er effektiv, hensiktsmessig og tilpasset risikobildet
        - Behandle og følge opp avvik i egen virksomhet
        - Rapportere vesentlige avvik knyttet både til sektorovergripende prosesser og tjenestespesifikke prosesser i internkontrollen til overordnet nivå
    - Det uformelle miljø i Råde kommune dreier seg om det psykososiale arbeidsmiljøet som preger arbeidet med internkontroll.
    - Leder er ansvarlig for at arbeidet med internkontroll gis preg av å være et verdiskapende arbeid, bygget på kommunens vedtatte verdier «raushet, glede og respekt». Kommunens ledelse går foran som rollemodeller og legger til rette for samhandling i oppgaveløsningen.
- Risikovurdering
- Kontrollaktiviteter
- Ledelsesoppfølging

Angående oppfølging står det at resultatoppfølging og rapportering er en viktig del av virksomhetsstyring i kommunen. Rapportering gir ledere på alle nivå et grunnlag for å vurdere kvaliteten på og effekten av

etablert internkontroll. Etter at ledere på ulike nivåer har rapportert resultatet fra oppfølgingen av internkontrollen innenfor eget ansvarsområde, skal informasjon om status og tilstand for internkontrollen i kommunen som helhet sammenstilles og kommuniseres. Informasjonen brukes i ledelsens styring og kontroll av virksomheten, og gir viktige innspill til læring og forbedring, og dessuten til planleggingen av internkontrollen for neste periode.
Månedlig skal det rapporteres fra virksomhetsleder til kommunalsjef som en del av statussamtale. Internkontrollen er en del av denne rapporteringen, og herunder skal det rapporteres på:

- status ROS
- status tiltak
- forslag til nye tiltak eller kontroller på bakgrunn av erfaringer eller analyser
- status avvik.

Hvert tertial skal det rapporteres fra kommunalsjef til kommunedirektør og fra administrasjon til folkevalgt nivå. For internkontroll rapporteres det fra hvert tjenesteområde om status innmeldte og lukkede avvik, gjennomførte ROS, iverksatte tiltak og resultater, evt. klargjøring av ansvar for oppfølging og iverksetting av tiltak.

Årlig rapportering, blant annet for internkontroll, foretas gjennom kommunens årsberetning. Årlig avlegges også kvalitetsmeldinger fra hvert tjenesteområde, med informasjon om:

- Statlig tilsyn og erfaring med tilsyn: hvilke tilsyn har vært gjennomført, avvik og pålegg, oppfølging og effekt av tilsyn
- Effekt og resultat: hendelser som er unngått, risikoer som er redusert, forbedringsprosesser
- Aktiviteter: tjenesteområder med særskilt oppmerksomhet, iverksatte tiltak.

4.2.1.2 Vurdering av risiko

Under avsnitt om risikovurdering i «Virksomhetsstyring og internkontroll i Råde kommune» står det at kommunens internkontroll er risikobasert, og at metoden for risikoanalyse som brukes innen ulike tjenesteområder i kommunen skal være tilpasset virksomhetens størrelse og egenart.

Videre at alle virksomheter i Råde kommune gjennomfører årlige ROS-analyser. Dette er en prosess i fem deler; identifisere hva som kan gå galt, vurdere hvor galt det kan gå, dokumentere hvilke kontrolltiltak som er iverksatt, vurdere hvorvidt kontrolltiltakene i tilstrekkelig grad reduserer risiko til et akseptabelt nivå og oppfølging ved å endre eller etablere kontrolltiltak. Som tidligere nevnt har revisjonen fått oversendt kommunens risikoanalyse for informasjonssikkerhet, datert 5.9.2022. Analysen er en overordnet risikoanalyse for informasjonssikkerhet, og er utarbeidet av fagansvarlig beredskap, fagansvarlig internkontroll, fagansvarlig digital sikkerhet og arkivleder/personvernombud.

4.2.1.3 Håndtering av risiko

I dokumentet «Virksomhetsstyring og internkontroll i Råde kommune» beskriver kommunen kontrollaktiviteter som nøye sammenhengende med risikovurderingen. De skal sikre at det settes i verk tiltak for å håndtere risikoene som kan hindre oppnåelse av virksomhetens målsettinger. Slike aktiviteter skal bidra til at prosesser og systemer fungerer som forutsatt.

Leders kontrolltiltak innebærer å kontrollere om det forekommer avvik fra den standarden som er fastsatt for kapasitet og kvalitet i kommunens virksomhet, samt å danne grunnlag for risikovurdering.
Kontrollaktivitetene skal forhindre, oppdage og korrigere avvik. De består i å:

- gjennomføre forebyggende tiltak i forkant av mulige hendelser på grunnlag av ROS-analysen
- registrere avvik ved manglende oppfyllelse av krav

- sette inn korrigerende tiltak
- gjennomføre årsaksanalyse
- sette inn forebyggende tiltak, hvis hensiktsmessig

Avvik av alvorlig karakter skal virksomhetsleder videresende til kommunalsjef. Kommunalsjef skal melde til kommunedirektøren. Med avvik av alvorlig karakter menes avvik som:

- avdekker at arbeidsgiver eller en arbeidstaker har begått et alvorlig brudd på inngått arbeidsavtale
- avvik som innebærer at kommunen kan bli anmeldt til politiet eller kommunen selv bør anmelde forholdet til politiet
- avvik som tilsier at varsling av tilsynsmyndighet, kommunerevisjon eller kontrollutvalget bør vurderes.

Kommunens risikoanalyse for informasjonssikkerhet beskriver de tiltak som er satt i verk for å redusere identifiserte risikoer. Tiltakene omhandler brukere og tilgang, IKT-teknisk, menneskelige faktorer, lovkrav og avtaler og personvern. Der risikoen er satt som kritisk høy er det lagt inn nye tiltak, med ansvarlig for utførelse og frist for gjennomføring.

4.2.1.4 Overvåking og hendelseshåndtering

«Rutine for kartlegging av trusler» beskriver at kommunen bruker program i brannmuren for å få et oversiktlig bilde av trusler og hendelser- det viser hvilke trusler som har blitt detektert og stoppet av brannmurens Intrusion Prevention System (IPS), Anti-Bot, Anti-Virus.

Programmet fra brannmuren vises på storskjerm på IKT-avdelingen, og avdelingen får også daglig e-post med rapport over hendelser fra brannmuren. Ved ny oppdatert IPS beskyttelse får kommunen e-post om hvilke nye beskyttelser som har blitt oppdatert.

Som det står i IKT beredskapsplan, og revisjonen har blitt kjent med gjennom intervjuer, abonnerer kommunen på tjenester fra HelseCERT, Kommune-CSIRT, Haveibeenpwned, og varsler fra leverandører av de ulike systemene. Alle varsler som kommunen får gjennom disse tjenestene følges opp straks informasjonen foreligger.

HelseCERT og Kommune-CSIRT skanner kommunens systemer for sårbarheter, og forsøker å angripe kommunens løsninger som er tilgjengelig fra internett. På spørsmål om kommunen foretar spesifikke inntrengningstester svarer fagansvarlig digital informasjonssikkerhet at dette ivaretas ved medlemskapet i HelseCERT og Kommune-CSIRT, og at disse antageligvis utfører slike tester jevnlig – kommunen får oversikt over resultat fra HelseCERT hver 3. måned.

I møte med fagansvarlig digital informasjonssikkerhet har vi fått informasjon om at HaveIbeenpwned overvåker alle råde kommune-adresser. Om de finner en lekkasje med kommunens e-post/brukere blir kommunen varslet per e-post. I slike tilfeller blir berørt bruker bedt om å endre passord.
Fagansvarlig digital informasjonssikkerhet opplyser om at HelseCERT også har utarbeidet en hurtigtest for å teste sikkerheten i sine systemer. Denne har kommunen benyttet seg av, og oversendt resultatet av siste test utført i august. Revisjonen har også fått informasjon om rapporter fra HelseCERT og Kommune-CSIRT i intervjuer, samt mottatt eksempler på rapporter som er sendt kommunen. En slik rapport i 2021 viste en sårbarhet som muligens kunne føre til innbrudd i kommunens systemer.

Revisjonen har fått oversendt sammenstilling av kommunens håndtering etter dette varselet. «Statusrapporter for mulige innbrudd i perioden 2019-22» viser kommunens arbeid med et varsel fra Helse-

CERT. Dokumentet viser at etter at kommunen først fikk videresendt varselet fra Nasjonalt Cybersikkerhetssenter, fikk de e-post fra HelseCERT med instruksjoner for hvordan søke etter sårbarheten, e-post fra brannmur med informasjon om at denne var oppdatert mot sårbarheten, og flere e-poster om oppdateringer og informasjon fra både brannmur og HelseCERT. Tre dager etter at kommunen fikk varselet holdt HelseCERT webinar om sårbarheten. HelseCERT og Kommune-CSIRT bidro med instruksjoner for søk. Sistnevnte tilbød også støtte til arbeid med sårbarheten ved å skanne kommunens nettverk for sårbarheten. I dette tilfellet kunne kommunen konkludere med at det ikke var gjort innbrudd i deres systemer.

Videre får kommunen også e-postvarsler gjennom Microsoft 365 Defender ved sikkerhetsbrudd på endebrukere. Ved mottak av slike varsler opprettes det Helpdesk-sak til en ansatt ved IKT-avdelingen.

Revisjonen har fått oversendt IKT-avdelingens driftsrutine som er inndelt i daglige, månedlige og halvårlige kontroller. Daglig skal IKT-avdelingen sjekke informasjon på storskjerm (brannmurens program SmartView som viser hvilke trusler som har blitt detektert og stoppet, jf. «rutine for kartlegging av trusler»), og kontrollere om det er kommet varsler/informasjon til avdelingens e-post som må følges opp. Månedlige kontroller består blant annet av gjennomgang og kontroll av at servere/systemer/programvare bruker siste versjon/sikkerhetsoppdatering. I dokumentet vi har fått oversendt er samtlige kontroller gjennomført innen siste mnd.

I møte med fagansvarlig digital informasjonssikkerhet får revisjonen informasjon om at IKT-avdelingen kontinuerlig får varsler om trusler mot kommunens systemer. Varslene filtreres etter hva som er reelle trusler mot kommunens sikkerhet, og diskuteres i møter på avdelingen. Det opplyses om at det ca. ukentlig kommer inn varsler som kommunen anser som interessante. Typiske varsler er at noen har fått tak i e-postadressen til en ansatt, og det forsøkes ulike passord for å komme seg inn i systemene. Slike varsler er det ifølge kommunen ikke nødvendig å følge opp. Fagansvarlig digital informasjonssikkerhet begrunner dette med at bruk av tofaktor-autentisering[3] for pålogging til systemer reduserer risikoen for faktisk inntrengning til et nivå hvor det ikke er nødvendig å følge opp slike varsler.

I «IKT beredskapsplan» finner vi, under forebyggende tiltak, at alle alvorlige hendelser skal følges opp, og at alle hendelser skal registreres og behandles i kommunens avvikssystem. Kommunen har egen prosedyre for avvikshåndtering, som er revidert 14. september 2022.

Formålet med kommunens avvikssystem er å bidra til kontinuerlig læring og forbedring. Ved at avvik blir fulgt opp på en systematisk og helhetlig måte bidrar dette til nyttig styringsinformasjon, slik at avdekkede avvik effektivt blir lukket, og nye lignende avvik ikke inntreffer. Avvikssystemet skal også bidra til at virksomhetens ansatte overholder interne føringer fastsatt av ledelsen og eksterne lovkrav.

Prosedyren gjelder for alle ansatte i kommunen, og det er rådgiver internkontroll og beredskap som er ansvarlig for utforming, implementering og oppdatering. Det står videre at den enkelte ansatte har ansvar for å melde avvik, og nærmeste leder har ansvar for at avviksprosedyren blir fulgt. Det er leder, prosesseier eller andre som mottar avvik gjennom avvikssystemet som har ansvar for at tiltak blir iverksatt og avviket lukket. Det fremkommer i prosedyren at dersom avvik som er meldt i avvikssystemet ikke blir lukket innen fristene går de automatisk videre til virksomhetsledere etter 14 dager og til kommunalsjef etter 21 dager. På regelmessig basis skal rådgiver internkontroll og beredskap følge opp at alle tiltak

[3] En metode for tilgangskontroll hvor en bruker kun gis adgang etter å ha presentert to forskjellige bevis for sin identitet (https://no.wikipedia.org/wiki/Flerfaktor-autentisering). Eks. Noe du vet (passord) og noe du har/er (mobil/fingeravtrykk).

blir lukket, samt sammenstille og analysere samlede avvik. Det skal rapporteres til ledergruppen ved behov, og minst en gang i året.

Revisjonen er informert om at kommunen har en egen kategori for avvik innen IT- og informasjonssikkerhet i sitt avvikssystem, kategorien inneholder syv mulige valg innen slike avvik:

- Brukerkontoen din har blitt brukt på et tidspunkt da du ikke var pålogget
- Du har mistet eller ble frastjålet en datamaskin eller en minnepinne med sensitiv informasjon
- Brudd på personvern/GDPR
- Uvedkommende har fått tilgang til sensitive opplysninger/fagsystem
- Data på avveie
- Anskaffelse av IKT-utstyr eller programvare hvor IKT ikke har vært involvert
- Annet

Revisjonen har fått opplyst i intervju at denne kategorien ble opprettet i 2021, og at det er vanskelig å gi et utviklingsbilde på avvik innen denne kategorien – da den ikke er direkte sammenlignbar mot tidligere registrerte avvik. Det er mottatt oversikt over syv registrerte avvik i perioden 2021/2022 som omhandler IT- og informasjonssikkerhet, og samtlige har status som lukket.

I forbindelse med kommunens overordnede beredskapsplan er det også utarbeidet et tiltakskort for «Dataangrep med bortfall digitale systemer». Tiltakskortet beskriver den uønskede hendelsen, mulige konsekvenser, eksisterende tiltak/forberedelser, og hva kommunen skal gjøre i de ulike fasene (alarm/mobilisering/håndtering, normalisering og evaluering) i hendelseshåndteringen.

4.2.1.5 Kompetanse- og kulturutvikling

Fagansvarlig beredskap har blant annet som oppgave å gjennomføre opplæring, trening og øvelser i krisehåndtering. Fagansvarlig digital informasjonssikkerhet har blant sine oppgaver å være aktiv og rådgivende i organisasjonen og i lederlinjen, og en ambassadør for arbeidet med sikkerhetskultur og opplæring.

I «Virksomhetsstyring og internkontroll i Råde kommune», under avsnitt om organisering av internkontrollarbeidet, står det at internkontrollteamet, som har overordnet ansvar for kommunenes samlede internkontroll, er ansvarlig for å organisere opplæring i internkontroll og internkontrollsystemet.

Internkontrollteamet har ansvar for å lage plan for kontinuerlig intern opplæring i internkontroll og internkontrollsystemet, og det ligger til virksomhetsleders ansvar å:

- etablere kultur for kontinuerlig forbedring i virksomheten
- sørge for at alle ansatte har nødvendig kompetanse i internkontroll og internkontrollsystemet, samt tilgang til internkontrollsystemet
- etterspørre og bruke avvik systematisk som grunnlag for forbedringsarbeid
- bidra aktivt til utvikling av kommunens internkontroll, både i virksomheten og på tvers av organisasjonen
- rapportere til kommunalsjef om etterlevelse av internkontrollen

Spesifikt for internkontroll på informasjonssikkerhetsområdet fremkommer det i IKT beredskapsplan at de ansatte på IKT selv sørger for at egen kompetanse er oppdatert. Dette gjør de ved å delta i diverse aktuelle foredrag og seminarer, kurs og andre opplæringsmøter. Ifølge planen skal IKT gjennomføre halvårlige dialogmøter med alle kommunens virksomheter. I intervju med fagansvarlig digital informasjonssikkerhet har revisjonen fått nærmere informasjon om at ivaretakelse av kompetansenivå og behov for kompetansepåfyll for IKT-avdelingen vurderes både av den enkelte ansatte, og samlet for avde-

lingen. Videre at kommunen deltar på webinarer med faglig påfyll fra HelseCERT[4], og gjennom Kommune-CSIRT[5] får de deltatt på webinarer og statusmøter i forhold til informasjonssikkerhet og det trusselbildet som foreligger. Foreningen for kommunal informasjonssikkerhet (KINS) er en kilde til informasjonsdeling for kommunen, og IKT-avdelingen har deltatt på flere kurs i regi av foreningen. I tillegg ser kommunen stor nytte av informasjonsdeling med andre kommuner og deres IT-avdelinger. Kommunen deltar også i Digidirs nettverk for informasjonssikkerhet (NIFS) hvor de får tilgang til webinarer, møter og faglig påfyll.

Kommunens oppfatning er at innholdet i digital sikkerhetsopplæring kontinuerlig må tilpasses utviklingen i trusler, kunnskap og systemer innen området. Opplæring bør kjøres når det skjer endringer, og ha større dynamikk, enn en statisk opplæringsplan.

I kommunens IKT beredskapsplan står det om forebyggende tiltak at opplæringer av sluttbrukere i sikkerhetsarbeid gjøres via nanolæring, og ved at IKT avdelingen informerer på allmøter på virksomhetene. I møte med fagansvarlig beredskap fremkommer det at kommunen for ca. 3 år siden gikk bort fra allmøter, og startet med nyansattopplæring. Kommunen forteller at opplæringen samler opp alle nyansatte, uavhengig av stilling, og foregår over en hel dag. Det avholdes ca. 3 ganger i året, og har samme program hver gang, og fagansvarlig digital informasjonssikkerhet og fagansvarlig internkontroll har innlegg om sine fagområder.

Nanolæring, som nevnt i IKT beredskapsplan, er opplæring i små porsjoner. Kommunen sender ut e-post til alle ansatte med nyttige tips og spørsmål knyttet til relevante temaer innen digital sikkerhet. Tidligere har de fullført en læringsmodul innen personvern, og per dato er det en læringsmodul innen informasjonssikkerhet som pågår ut året. Hver 14. dag får alle ansatte en e-post med lenke til en leksjon. En påminnelse sendes ut til brukere som ikke har fullført alle tidligere sendte aktiviteter 5 arbeidsdager etter at aktiviteten er sendt. Påminnelser gjentas 2 ganger med mindre en ny aktivitet sendes ut, eller brukeren har fullført alle aktiviteter.

Øvrig opplæring innen informasjonssikkerhet håndteres på virksomhetsnivå, og foregår typisk gjennom diskusjoner på personalmøter o.l.

4.2.1.6 Kommunikasjon

I dokumentet «Virksomhetsstyring og internkontroll i Råde kommune», under avsnitt om kommunikasjon og dokumentasjon, fremkommer det at kommunen bruker et elektronisk system bestående av elektronisk dokumentbibliotek og avviksmodul for å ivareta følgende krav til strukturert lagring av dokumentasjon:

- Felles mal for instrukser, prosedyrer og andre dokumenter
- Mal for risikokartlegging og vurdering
- Frekvens og form av rapportering
- Statistikk

[4] Helse- og omsorgssektorens nasjonale senter for cybersikkerhet. Skal øke sektorens evne til å oppdage, forebygge og håndtere alvorlige cyberangrep (https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert).

[5] Et ressurssenter for praktisk rådgivning og støtte ved cyberhendelser og andre digitale utfordringer i kommunesektoren. Støtter kommuner og fylkeskommuner med relevant informasjon om trusler, hendelser og sårbarheter i det digitale domenet (https://www.kommunecsirt.no/).

Videre kan vi lese at kommunedirektøren formulerer og formidler sine forventninger til virksomheter og tjenester, synliggjort blant annet gjennom strategier og andre styringsdokumenter som setter rammer for hvordan kommunens oppgaver og tjenester skal organiseres og løses. For å sikre ansattes forståelse for kommunens prosesser er det utarbeidet et sektorovergripende reglement som inneholder felles dokumenter og sektorovergripende prosedyrer.

Ifølge dokumentet er det leder som er ansvarlig for at kommunikasjon og informasjon om internkontroll er effektiv, og virker i alle retninger av kommunen. Tilstrekkelig og relevant informasjon til rett tid skal gjøre det mulig for hver enkelt å ivareta det ansvar som vedkommende er tildelt.

Informasjon om internkontroll, også på informasjonssikkerhetsområdet, gis som tidligere nevnt til ansatte gjennom nyansattopplæring – og i IKT-dialogmøter mellom IKT-avdelingen og virksomhetene. Informasjon om sikkerhetspolicy formidles gjennom kommunens nanolæring.

I intervju med fagansvarlig beredskap fremkommer det at kommunen informerer ansatte om viktige endringer/nye dokumenter gjennom kvalitetssystemet. Der det er viktig at de ansatte leser og signerer for dette, blir det lagt på de ansattes leseliste. Der det ikke er nødvendig med signatur kan det legges inn som en nyhetsoppdatering, som fremkommer som et varsel/notifikasjon når den ansatte logger på kvalitetssystemet.

Når dokumenter ligger i de ansattes leseliste, får de påminnelse om at de har dokumenter til lesing/signering. Det kan også legges inn frist for signering i systemet.

4.2.2 Internettprotokoller og PKI

I intervju med fagansvarlig digital informasjonssikkerhet er revisjonen gjort kjent med at kommunen bruker IPv6 for kommunikasjon på internett, og at de ivaretar at nytt nettverksutstyr og IP-avhengig programvare støtter IPv4 og/eller IPv6 gjennom sin anskaffelsesprosess. Fagansvarlig digital informasjonssikkerhet bemerker videre at alt av nettverksutstyr som produseres i dag støtter IPv4 og/eller IPv6. Videre informerer kommunen om at alle kommunens nettsider har sertifikater fra Buypass[6], og bruker HTTPS ved overføring av nett-trafikk. Sertifikatene som benyttes støtter TLS 1.0, 1.1 og 1.2.

Revisjonen har fått oversendt dokumentet «IKT kravspesifikasjoner/Kravspekk/Anskaffelsesprosess» som presiserer krav til leverandører som skal levere programvare eller IKT infrastruktur til Råde kommune. Dokumentet gjelder ved anskaffelser, vesentlige endringer av eksisterende IKT-systemer og nybygg, bygningsmessige utvidelser eller større restaureringsarbeider som berører kommunikasjonsområder. Når det gjelder krav til kommunikasjonsprotokoller (punkt 2.3 i dokumentet), er det angitt at kun TCP/IP er tillatt – systemer må ikke kreve eller generere andre protokoller. TCP/IP er en forkortelse for Transmission Control Protocol/Internet Protocol, og er en gruppe kommunikasjonsprotokoller som brukes for å koble datamaskiner sammen i nettverk, blant annet på internett.

[6] Selskapet Buypass ble etablert i 2001, og tilbyr tjenester for identifisering og kryptering av informasjon gjennom hele den elektroniske verdikjeden. Ifølge selskapets hjemmeside er de Norges eneste utsteder av internasjonalt godkjente SSL-sertifikater (https://www.buypass.no/selskapet).

I intervjuet fremkommer det også at det er kommunens oppfatning at ved å benytte ID-porten som PKI[7]-tjeneste, har kommunen hensyntatt kravspesifikasjon for PKI. ID-porten er en tjeneste levert av Digitaliseringsdirektoratet, og er en felles innloggingsløsning til offentlige tjenester på internett.

4.2.3 NSM grunnprinsipper for IKT-sikkerhet

Et av Digdirs bør-tiltak for informasjonssikkerhet er å følge NSMs grunnprinsipper for IKT-sikkerhet. Grunnprinsippene er et sett med underliggende tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. NSM tilbyr også kurs i grunnprinsipper for IKT-sikkerhet, og i intervju med fagansvarlig digital informasjonssikkerhet har vi fått informasjon om at samtlige i kommunens IKT-avdeling har deltatt på slike kurs.

I kommunens IKT beredskapsplan fastslår kommunen at hensikten med beredskapsplanlegging er å planlegge hvordan virksomheten skal håndtere uventede IKT-avbrudd, samt å beskytte kritiske tjenester og systemer mot negative konsekvenser ved feil eller uhell.

I beredskapsplanen har kommunen vurdert sine fagsystemer, og satt opp en liste over hvilken rekkefølge de skal prioriteres dersom en alvorlig hendelse rammer flere systemer samtidig. Videre har kommunens sentrale datarom et aggregat som kobler inn automatisk ved bortfall av strøm, og UPS[8] som sikrer god kvalitet på strømmen som leveres.

I intervju med fagansvarlig digital informasjonssikkerhet fremkommer det også at kommunens sentrale datarom er sikret med låst dør. Låsen er fysisk, og nøkkel oppbevares på sted som er kjent for IKT-avdelingen. Det er ingen loggføring med hvem som går inn og ut av datarommet. Fagansvarlig opplyser om at det ikke har vært anledning til å bygge ut kommunens eksisterende adgangssystem, for å sikre rommet med elektronisk adgangskontroll, men at det er håp om å få dette på plass i 2023.

Revisjonen har fått oversendt dokumentet «Kartlegging av fagsystemer i Råde kommune - GDPR», hvor kommunens fagsystemer er kartlagt i forhold til GDPR. Forsiden i dokumentet viser hvilke program kommunen har, en kort beskrivelse, hvem som er system- og databehandlingsansvarlig, kommunalsjef knyttet til systemet, hvilken enhet som eier systemet – og om databehandleravtale er på plass der det er nødvendig.

I intervju med fagansvarlig digital informasjonssikkerhet fremkommer det at kommunen har kartlagt alle enheter som er koblet mot kommunens domener. Revisjonen har fått oversendt oversikten, som viser enheter fordelt på domenet kommunen er på vei bort fra, og kommunens nye domene.

Når det gjelder brukere står det i kommunens håndbok for informasjonssikkerhet og personvern i Råde kommune, at autorisasjon er personlig og skal registreres i et autorisasjonsregister. Videre at alle typer autorisasjon som gis skal være i henhold til kommunens gjeldende sikkerhetsstrategi.
Virksomhetsleder er autorisasjonsansvarlig for manuelle og elektroniske behandlinger av personopplysninger i sin enhet, og skal:

- Sørge for at alle nye ansatte, vikarer og periodisk personell får tilgang til aktuelle informasjonssystemer ved tilsetting i henhold til tjenstlige behov

[7] Public Key Infrastructure. Angir en sikker metode som knytter personlige identiteter til offentlige krypteringsnøkler ved lagring hos en tiltrodd tredjepart. PKI bygger på krypteringsnøkler som opptrer i par, der den ene er offentlig tilgjengelig og den andre er privat (https://snl.no/PKI).

[8] UPS står for Uninterruptible Power Supply, og er et apparat som opprettholder kontinuerlig leveranse av elektrisk kraft. Hensikten er å sikre at viktig utstyr ikke mister strømmen hvis strømnettet faller ut, samt filtrere urenheter i nettet – så sensitivt utstyr ikke tar skade. https://no.wikipedia.org/wiki/Avbruddsfri_str%C3%B8mforsyning

- Skriftlig informere aktuelle instanser om endringer i behov for tilgang til informasjonssystemene.
- Trekke tilbake autorisasjoner når ansatte slutter eller ikke lenger har tjenstlig behov for autorisasjonen. Ved endringer i arbeidsforhold eller ansvar skal den ansattes tilganger i kommunens informasjonssystemer vurderes.
- Føre autorisasjonsregister med oversikt over hvilke IKT-løsninger/manuelle behandlinger hver enkelt ansatt er autorisert for. Autorisasjonsregisteret skal oppdateres hver gang det skjer endringer og skal oppbevares i minst 5 år.
- Årlig gjennomgå brukertilganger i egen enhet og gi melding til IKT og andre dersom tilganger skal slettes eller endres.

Det står videre at IKT-enheten/systemansvarlige/superbrukere har ansvar for tildeling, endring og tilbaketrekking av autorisasjon til kommunens IKT-løsninger i henhold til melding fra autorisasjonsansvarlig.

Kommunen har også en «Prosedyre for å opprette eller fjerne bruker for tilgang til IKT systemer», som har som formål å beskrive hvordan man oppretter, sletter eller endrer tilgang til IKT-systemene. Det fremkommer her at det skal sendes personalmelding, og tilgangsskjema, når en ansatt skal ha bruker i kommunenes IKT systemer. Når personalmelding er sendt vil stab økonomi legge ansatt i Visma HRM. En synkroniseringstjeneste vil da innhente informasjon fra Visma HRM, og automatisk opprette en bruker i kommunens system.

I intervju med fagansvarlig beredskap har revisjonen fått opplyst at det i hovedsak er virksomhetsledere som har myndighet til å gi tilganger, men at denne myndigheten kan delegeres. Tilganger til kommunens fagsystemer er det systemansvarlig som beslutter.

I prosedyren for å opprette eller fjerne brukere står det at det skal gjøres en gjennomgang av sluttede brukere. I intervju med fagansvarlig digital informasjonssikkerhet er det gitt informasjon om at dette nå er integrert i HRM-systemet, og at gjennomgangsprosessen er faset ut. Det som skjer nå er at brukerne mister sine tilganger automatisk ved sluttmelding i HRM, og blir stående som deaktivert i systemet for eventuell etterkontroll eller gjenbruk.

Kommunens sikkerhetsarkitektur er beskrevet i «IKT Kravspesifikasjoner/Kravspekk/Anskaffelsesprosess», og er basert på følgende prinsipper:

- Nettverk er delt i tre soner (DMZ[9], Åpent og Lukket)
- Klart skille mellom tjenester og klienttyper inndelt i relevant sikkerhetspolicy
- Tilgang til tjenester reguleres gjennom bruk av sikkerhetsbarrierer (brannmurer, VLAN, pakkefilter, applikasjonsfilter, innholdsfilter, autentiseringsløsninger, VPN/SSL-GW, krav til klienter og tjenere, mm.
- En sone har ikke tilgang til en sone med høyere sikkerhetsnivå med mindre det er eksplisitt tillatt, og regulert i en brannmur
- En sone med høyere sikkerhetsnivå har ikke nødvendigvis tilgang til en sone med lavere sikkerhetsnivå
- Hver sone inneholder ett eller flere nettverkssegmenter

Om de ulike sonene står det at:

[9] DMZ står for demilitarized zone, og er et fysisk eller logisk subnet som offentliggjør en organisasjonsoffentlige tjenere mot internett. Hensikten er å sørge for at hackere ikke skal få tilgang til hele bedriftens nettverk ved innbrudd på maskinen som er tilgjengelig fra internett. https://no.wikipedia.org/wiki/DMZ_(datanettverk)

- DMZ brukes for internettrelaterte systemer. Det er flere soner i DMZ, og systemer som kommuniserer fra internett til kommunens nettverk eller omvendt tillates ikke å passere to soner uten å kommunisere gjennom en sikkerhets-gateway. Det følger også med en liste over hvilke tjenester kommunen har organisert i DMZ.
- Åpen/intern sone er for administrative og fagorienterte nett:
    - Systemadministrative og fagorienterte nett
    - Tekniske tjenester
    - Administrative systemer og driftsnett
    - Administrasjon av fjerntilgang samt klienter med mulighet for aksess til tjenester i lukket sone
- Sikker sone for behandling av sensitive personopplysninger og virksomhetskritiske løsninger. Alle tjenester og systemer som inneholder sensitive personopplysninger ligger her. I intervju med fagansvarlig fremkommer det også at systemer i sikker sone ikke har tilgang til internett eller e-post.

Kravspesifikasjonen beskriver også krav til installasjon, hvor det fremkommer at dette skal kunne settes opp «unattended». Det betyr at installasjon gjøres sentralt fra kommunens IKT-avdeling, og uten brukermedvirkning. Når det gjelder oppdateringer stiller kommunen krav til at alle nye versjoner av et program skal leveres ITK-avdelingen for kvalitetssikring før den settes i produksjon. Om Fjerndrift/-leveranse står det at alle løsninger og systemer som hovedregel skal kjøres i kommunens datasentral, eller i egen skyløsning. Alle programmer skal installeres av personell fra kommunens IKT-avdeling, eller i samarbeid med IKT-avdelingen, og databehandleravtaler skal utarbeides ved behov. Fagansvarlig digital informasjonssikkerhet bekrefter i intervju at kommunen har nødvendige databehandleravtaler på plass.

I intervju med fagansvarlig digital informasjonssikkerhet har revisjonen fått informasjon om at brukere ikke har rettigheter til å laste ned programvare e.l. lokalt til sin PC, da dette krever administrasjonsrettigheter.

Fagansvarlig kan videre fortelle at kommunen har tatt i bruk ny ordning ved oppsett av PCer. De blir nå levert direkte til bruker, og konfigurasjon/oppsett skjer automatisk når den ansatte logger på med sin bruker. Dette er nærmere beskrevet i «rutine for oppsett av PCer og klienter», hvor det også fremkommer at det er IKT-avdelingen som konfigurerer nettverk, sikkerhet og programdistribusjon gjennom Microsoft Endpoint Manager – basert på hvilke brukere det er snakk om.

IKT beredskapsplan, punkt 12, endringskontroll og konfigurasjonsstyring. Alle endringer logges, og oppsett av systemer og servere utføres etter beskrevne rutiner som er lagret på IKTs dokumentområde.

Kommunen har egen rutine for oppsett av ny, eller fjerning av server. Denne beskriver trinn for trinn hvordan en ny server skal settes opp. Herunder også overvåkning.

Håndbok for informasjonssikkerhet og personvern i Råde kommune har et eget avsnitt om konfigurasjonsstyring hvor det blant annet fremkommer at kommunens informasjonssystem skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås i henhold til kommunens sikkerhetsstrategi, risikovurderinger og beslutninger om sikkerhetstiltak. Konfigurasjonskontroll omfatter all programvare, servere, nettverksutstyr, interne og eksterne kommunikasjonsforbindelser mm. Som eies/disponeres av kommunen. Videre er det beskrevet at følgende gjelder:

- Kommunens informasjonssystem er inndelt i soner som gjenspeiler skillet mellom behandling av sensitive og ikke sensitive personopplysninger
- Soneinndelingen sikrer også at ansatte skilles med tanke på nettverkstilgang for kun å nå opplysninger som de er autorisert for

- De deler av informasjonssystemet hvor sensitive personopplysninger behandles, er videre inndelt i samsvar med formålet med behandlingen av personopplysninger/tjenester kommunen leverer
- Sikker sone er adskilt fra eksterne nett med to sikkerhetsbarrierer. All aktivitet skal initieres fra sikker sone til intern sone og til eksterne nett.
- På hjemmekontor brukes kun kommunens hjemmekontorløsning. Hjemmekontorløsningen skal sikre at uautoriserte personer ikke får tilgang til kommunens informasjonssystem
- Kun utstyr eller program eiet/disponert av kommunen skal inngå i informasjonssystemet
- Endringer i informasjonssystemets konfigurasjon skal utføres planmessig og systematisk og sikre at
    - Alle konfigurasjonsendringer er i samsvar med besluttet sikkerhetsstrategi
    - Informasjonssystemet fungerer som forutsatt også etter at endringen er gjennomført

Når det gjelder oppgraderinger står det i kravspesifikasjonen at når en programvare oppgraderes til kommende versjoner skal den nye oppgraderingen bestå av en fullverdig installasjon – noe som innebærer at den nye oppgraderingen skal kunne installeres uten å ha den gamle tilgjengelig.

I kommunens IKT reglement, under avsnitt om bruk av internett, står det at internettilgangen primært skal brukes til kommunerelaterte formål, og at det ikke er lovlig å hente ned programvare uten samtykke fra IKT-avdelingen. Åpen tilgang til internett fra kommunens nettverk er en tillitssak mellom den ansatte og kommunen som arbeidsgiver. Det er videre ikke lov å laste ned usømmelig materiale, eller å bruke delingstjenester og proxytjenester. Strømming av tv, film, radio, musikk mv. skal unngås.

I IKT beredskapsplan er det et avsnitt om forebyggende tekniske tiltak. Kommunens tiltak er:
- Forebyggende tiltak og sikkerhet alltid er vurdert ved endringer i systemer (plan for tilbakerulling)
- Kompetanse og kunnskap innenfor sikkerhet og kontroll
- Opplæring i beredskapsarbeid
- Driftsrutiner IKT
- Tilgangskontroll
- Oppfølging av varsler fra eksterne og interne
    - Eksterne varsler – eks. fra HelseCERT og Kommune-CSIRT per e-post.
    - Interne varsler blir håndter og jobbet med via kommunens Helpdesk system
- Oppdatering av systemer og programvare gjøres i henhold til avdelingens driftsrutine
- Oppfølging av varsler fra antivirusløsning blir registrert i kommunens Helpdesk system hvor saken jobbes med til den er løst
- Oppfølging av varsler fra brannmur kommer til IKT-avdelingens e-postkonto. Rapportene som kommer dit vurderes av de ansatte på IKT (som en del av den daglige rutinen – se foregående avsnitt om konfigurering)
- Sikre at backup blir tatt og gjennomføre testing av restore
- Sikre at systemer logger korrekt og logg. Alle systemer skaper egne logger som kan brukes ved behov
- Fysisk sikring (brann, vann, temperatur og innbrudd)
    - Brann – sentralt datarom har brannvarsling som aktiverer byggets brannalarm, og eget slukkeanlegg som fjerner oksygen i rommet
    - Vann – sentralt datarom har detektor for vann, som utløser byggets brannalarm ved aktivering
    - Bygget har innbruddsalarm tilknyttet vekter
- Gjennomføring av øvelser og test av egne rutiner
- Strøm
    - Sentralt datarom har automatisk aggregat ved bortfall av strøm.

- Sentralt datarom har UPS som sikrer god kvalitet på strømmen, og fjerner unormale svingninger

Kommunen har en egen «Rutine for backup/Sikkerhetskopi av servere», hvor det står at alle virtuelle servere sikkerhetskopieres hver natt. Disse dataene tas vare på i 100 dager. Filserver sikkerhetskopieres en gang i måneden, og disse dataene tas vare på i 1 år. Innmeldte Teams[10] sikkerhetskopieres tilsvarende. I tillegg kopieres all sikkerhetskopiering til en sikker «offsite» som ikke kan slettes.

I møte med fagansvarlig digital informasjonssikkerhet har vi fått informasjon om at kommunens offline sikkerhetskopi lagres i en skyløsning, levert av ekstern leverandør med oppbevaring i Norge. Videre informerer fagansvarlig om at kommunen krypterer sine sikkerhetskopier med høyeste krypteringsnivå, og at det i tillegg ikke er mulig å slette sikkerhetskopiene hos ekstern leverandør. Krypteringsprosessen kjøres like ofte som sikkerhetskopieringen, dvs. hver natt. Kommunen har ingen data som lagres utover 1 år.

Under forebyggende tiltak i kommunens IKT beredskapsplan står det om endringskontroll og konfigurasjonsstyring at alle endringer logges, og at endringslogg lagres i Teams. I tillegg er det som nevnt egne rutiner for oppsett av systemer og servere.

Fagansvarlig digital informasjonssikkerhet har i møte med revisjonen forklart at endringer diskuteres internt i IKT-avdelingen. Fagmiljøet sitter samlet, og har mulighet til å diskutere problemstillinger ved behov. Det er også et møte hver morgen, hvor aktuelle problemstillinger diskuteres. Det gjennomføres endringer nærmest daglig – vurderinger av disse blir ikke dokumentert, men selve endringene loggføres. Det er alltid mulig å rulle tilbake til tidligere versjoner ved behov.

Nye klientPCer har eksempelvis blitt testet internt i avdelingen, for så å bli rullet ut til et utvalg for ny test. Fagsystemer settes gjerne opp i en testløsning først, hvor IKT-avdelingen ber om tilbakemelding fra virksomhetene før det tas i bruk. Avhengig av type system/programvare kan kommunen noen ganger velge å rulle ut løsningen, for så eventuelt å ta den tilbake hvis det skulle medføre større problemer.

4.2.4 Filoverføring

Digdir anbefaler at offentlige kommunikasjonstjenester støtter FTP (File Transfer Protocol), som protokoll for filoverføring. Digdir sier også at protokollen har begrenset sikkerhet, og bør brukes over en sikker kommunikasjonskanal.

Fagansvarlig digital informasjonssikkerhet sier at kommunen ikke støtter FTP, da denne protokollen er usikker og ukryptert. Kommunen anser protokollen som utdatert og bruker e-dialog, som de informerer om at er både kryptert og sikkert, både i overføring og ved sending/mottak.

4.2.5 Standarder - oppslag og VPN[11]

Kommunen informerer om at de bruker DNSSEC (DNS[12] Security Extensions) for å kontrollere at svar på oppslag i domenenavnsystemet kommer fra riktig kilde og ikke er endret underveis.

[10] Sikkerhetskopi av office 365 – det som ligger i Teams (notater og dokumenter)

[11] Virtuelt privat nettverk. Et datanettverk som oppretter en trygg «tunnel» mellom din enhet og ekstern server på nettet (VPN-tjeneren). All utveksling av data er kryptert.

[12] Domain Name Server – Server som oversetter nettadressen du skriver inn i adressefeltet til en IP-adresse.

Kommunens VPN[13]-løsning for hjemmekontor er integrert med brannmuren. Revisjonen har fått informasjon om at kommunen har 1 stk. SSL/TLS[14] VPN som er gammel, og ikke følger anbefalingene til NIST Special Publication (SP)[15] 800-113 – Guide to SSL VPNs. Videre har kommunen 6 stk. IPsec[16] VPN forbindelser, hvorav den nyeste av disse følger anbefalingene til NIST Special Publication (SP) 800-77 – Guide to IPsec VPNs. De resterende 5 er eldre, og følger ikke anbefalingene. Kommunen informerer om at de jobber med å få alle VPN forbindelser til å møte anbefalingene, og planlegger å ferdigstille arbeidet innen 1.4.2023.

4.2.6 E-post

IKT reglementets del 5 omhandler bruk av elektronisk post. Her står det at det interne e-postsystemet brukes til å gi meldinger og informasjon internt i kommunen, og at det finnes eget sakarkivsystem til formell saksbehandling. Det står videre at privat e-postkontakt via arbeidsstasjonen skal reduseres mest mulig, og at den ansatte skal unngå å få sin jobb e-postadresse registrert i private adressekataloger.

Siste punkt om e-post bruk sier at kommunens ansatte er kjent med at bruk av ekstern e-post må sees på som en åpen kommunikasjonsform der informasjon kan leses av uvedkommende, og at personsensitiv eller fortrolig informasjon ikke skal sendes per e-post.

Fagansvarlig digital informasjonssikkerhet informerer om at kommunen sikrer kommunens e-post mot falske avsendere med DMARC[17], sammen med SPF (Sender Policy Framework) og DKI (Domain Keys Identified Mail). Ved overføring bruker de STARTTLS[18] for å informere e-postserveren om at e-postklienten ønsker å oppgradere til sikker kobling ved bruk av TLS (Transport Layer Security) eller SSL (Secure Sockets Layer), og SPF (Sender Policy Framework) for å spesifisere hvilke e-posttjenere som er autorisert til å sende e-post på vegne av et gitt domene.

[13] https://www.digdir.no/standarder/sikre-kommunikasjonskanalar/1495

[14] Secure Sockets Layer/Transport Layer Securit, kryptografiske protokoller som autentiserer dataoverføring mellom servere, systemer, applikasjoner og brukere.

[15] National Institute of Standards and Technology.

[16] Internet Protocol Security, navn på en rekke protokoller som sørger for sikker kommunikasjon med IP.

[17] Domain-based Message Authentication, Reporting, and Conformance.

[18] Protokoll-kommando som informerer e-postserveren om at e-postklienten ønsker å oppgradere fra en usikker til sikker kobling ved bruk av TLS eller SSL.

4.3 Vurderinger

I dokumentet «Internkontroll i Råde kommune» har kommunen beskrevet kommunedirektørens ansvar for internkontroll etter kommuneloven § 25, og i «Håndbok for informasjonssikkerhet og personvern i Råde kommune» har kommunen vurdert relevante lover og retningslinjer som grunnlag for håndboken.

Kommunen har flere dokumenter som omhandler internkontroll i sitt kvalitetssystem, og har definert flere funksjoner og roller knyttet til arbeidet med dette. Det fremkommer blant annet at kommunens internkontrollgrupper har ansvar for å gjennomføre ROS-analyser for sine områder. Hva gjelder informasjonssikkerhetsområdet, finner revisjonen at kommunen har vurdert risikoer for området i en ROS-analyse, oppdatert i september 2022. Kommunen har etablert en beredskapsplan på området som bidrar til oversikt og styring, identifisering av tiltak og hendelseshåndtering, og i forbindelse med overordnet beredskapsplan er det utarbeidet et tiltakskort som omhandler håndtering ved bortfall av IKT-systemer.

Videre finner revisjonen at kommunen har definert sikkerhetsmål og sikkerhetsstrategier i sin «håndbok for informasjonssikkerhet og personvern i Råde kommune», hvor også kontinuerlig vurdering av egen internkontroll for informasjonssikkerhet er vurdert. Håndboken er ikke fullstendig, det er punkter som ikke er ferdigstilt, men det er positivt at kommunen jobber med en slik håndbok innen informasjonssikkerhet. Etter revisjonens oppfatning vil håndboken kunne bli et viktig verktøy når den er oppdatert og fullstendig, og både kunne bidra til å redusere risikofaktorer, men også være grunnlag for styring og oppfølging, samt måling og evaluering av kommunens arbeid.

At det skal rapporteres på virksomheters arbeid med internkontroll, også på informasjonssikkerhetsområdet, er nedfelt i dokumentet «virksomhetsstyring og internkontroll i Råde kommune». Revisjonens oppfatning er at det er fint at rapportering på området er klart definert og angitt i dokumentene.

Det fremkommer av dokumentet virksomhetsstyring og internkontroll at internkontrollteamet har ansvar for å lage plan for kontinuerlig intern opplæring i internkontroll og internkontrollsystemet. Etter hva revisjonen har fått av informasjon er det ikke utarbeidet slik plan. Revisjonen kan til dels si seg enig i kommunens vurdering om at utviklingen innen digital sikkerhet skjer kontinuerlig og raskt, og at opplæring bør kjøres når det er endringer. Men etter vårt syn kan en strukturert opplæringsplan bidra til å løfte kunnskapsnivået der den i utgangspunktet er lavest, for å få hele organisasjonen så gode på informasjonssikkerhet som mulig. Videre er det ikke utarbeidet saksnotat til virksomhetsledelsens gjennomgang eller årlige statusrapporter som angitt i dokumentet funksjoner innen internkontroll, beredskap, digital personsikkerhet og HMS. Det oppleves som uheldig at kommunens praksis ikke er i overensstemmelse med egne retningslinjer.

Det kan være sårbart at ansatte på IKT-avdelingen har ansvar for egen kompetanseutvikling, men revisjonens inntrykk er at avdelingen er liten, samlet på ett sted, og har høy grad av dynamikk når det kommer til utvikling. Det er også positivt at kommunen er tilknyttet eksterne kompetansesenter, og drar nytte av informasjonssdeling med omkringliggende kommuner.

Digdirs veileder viser til at god kommunikasjon, både skriftlig og muntlig, er en forutsetning for god styring og kontroll – og at dokumentasjon er en viktig del av dette. Revisjonen synes kommunens nyansattoppæring, og bruk av nanolæring (både som opplæring og informasjon) virker positiv, og vil favne svært mange av kommunens ansatte. Det er imidlertid en viss fare for at nanolæringen ikke gjennomføres, og dermed ikke fungerer slik som tenkt. Revisjonens inntrykk er at det er lite oppfølging utover påminnelsespost. Videre mener revisjonen at det er fint med leselister og påminnelser i kvalitetssystemet, som sikrer at de som er innom systemet får den informasjonen de har behov for. IKT-dialogmøter

mellom IKT-avdelingen og virksomhetene virker som et godt tiltak, som også vil være tilpasset brukergruppen i større grad. Nyansattopplæring har erstattet allmøter som nevnt i kommunens IKT beredskapsplan, og beredskapsplanen avviker fra praksis.

Det er positivt at kommunen har en prosedyre for avvikshåndtering, og et avvikssystem med egne avvikskategorier for avvik innen informasjonssikkerhet. Revisjonen har sett at det er registrert syv avvik i perioden 2021-2022, noe som etter revisjonens skjønn kan være litt lite på et utsatt område som informasjonssikkerhet. Det kan derfor være risiko for at det har forekommet avvik som ikke er registrert. Når det er sagt kan det være flere forhold som fører til få registrerte avvik, som at de ansatte ikke vet at det er egne kategorier for dette, og har registrert avvik på øvrige områder – eller at prosedyren ikke er fulgt, og avvik enten ikke er rapportert, eller er rapportert på annen måte enn via avvikssystemet.
Revisjonen har inntrykk av at kommunen kontinuerlig overvåker trusler mot sine informasjonssikkerhetssystemer, ved å vise brannmurens program på storskjerm i IKT-avdelingen, samt informasjon, tester og rapporter fra eksterne leverandører. Revisjonen har videre sett eksempel på hvordan kommunen jobber med sårbarheter, og er av den oppfatning at kommunens hendelseshåndtering er kontinuerlig og målrettet. Også tofaktorautentisering, og sentral styring av passordbytte, bidrar til videre reduksjon av risiko for innbrudd i kommunens systemer.
Kommunen bruker HTTPS overføring av nett-trafikk, og TLS sertifikatene som benyttes støtter versjoner anbefalt av Digdir. Videre bruker kommunen IPv6 for kommunikasjon på internett. Vedrørende om nytt utstyr og programvare støtter IPv4/IPv6 anser revisjonen at dette, i tråd med kommunens oppfatning, ivaretas gjennom kommunens anskaffelsesprosess.

For PKI-tjenester bruker kommunen ID-porten. Løsningen er en nasjonal løsning for innlogging til offentlige systemer, og revisjonens oppfatning er at det er sannsynlig at dette ivaretar kravspesifikasjonen for PKI.

Kommunen følger i stor grad NSMs grunnprinsipper for IKT-sikkerhet, og det anses som positivt at hele IKT-avdelingen har vært på kurs i disse.

Det er uheldig at kommunens sentrale datarom ikke er sikret med elektronisk dørlås, som sørger for loggføring av bruk. Det er risiko for at uvedkommende kan få tak i nøkkelen, og låse seg inn i rommet. Revisjonen er gjort kjent med at kommunen har planer om å anskaffe elektronisk lås til datarommet, noe som er positivt med hensyn til sikkerhet.

Kommunen har, i tråd, med grunnprinsippene, kartlagt sine enheter og systemer, og satt opp en prioriteringsliste for systemer dersom uønskede hendelser inntreffer.

Videre finner revisjonen at oppretting og fjerning av brukere i IKT-systemene i stor grad er ivaretatt gjennom integrasjon med HRM-systemet, som sørger for at brukere deaktiveres dersom de ikke lenger jobber i kommunen. I prosedyre for oppretting eller fjerning av brukere, er det angitt at det gjennomføres en gjennomgang av sluttede brukere, men revisjonen er gjort kjent med at dette er faset ut, og praksis avviker fra prosedyren.

Kommunen har inndelt sine systemer i soner, hvor blant annet fagsystemer som inneholder personopplysninger er lagt inn i sikker sone – dette er i tråd med NSMs grunnprinsipper.

Det er positivt at konfigurering av systemer og enheter styres sentralt, at nye løsninger testet ut før utrulling der det er mulig, samt at det er muligheter for tilbakerulling til tidligere versjoner ved behov.

Kommunen har også driftsrutiner på IKT-avdelingen, som sikrer at programvare og systemer er tilstrekkelig herdet, ved at nyeste versjon er installert - herunder også seneste sikkerhetsoppdatering. Kommunen bruker logger der det er mulig, i tråd med grunnprinsippene.

Kommunen har rutine for sikkerhetskopiering, og revisjonen anser det som positivt at dette gjennomføres ofte, dvs. hver natt. Det er svært positivt at kommunen også har krypterte, offline, sikkerhetskopier av sine systemer. Dette bidrar til å redusere risikoen for at systemene vil bli utilgjengelige for kommunen som følge av angrep.

Digidirs anbefaling om å støtte FTP er ikke fulgt. Men det er positivt at kommunen har gjort egne vurderinger rundt at dette ikke oppleves som trygt nok, og har valgt en sikrere løsning for filoverføring.
Revisjonen er gjort kjent med at kommunen bruker standarder for oppslag i domenenavnsystemet som er i tråd med Digidirs anbefalinger. Når det gjelder VPN løsninger er kun en av syv VPN forbindelser i tråd med Digdirs anbefalinger. Det er positivt at kommunen jobber med å få dette på plass innen 1.4.2023.

For å sikre sin e-post bruker kommunen DMARC, DKI, STARTTLS og SPF. Alle løsningene er i tråd med Digdirs anbefalinger.

4.4 Konklusjon og anbefalinger

Kommunen har flere dokumenter og prosedyrer som omhandler internkontroll og informasjonssikkerhet, og revisjonens inntrykk er at kommunen jobber aktivt med informasjonssikkerhet. Etter revisjonens vurdering følger Råde kommune i stor grad Digitaliseringsdirektoratet sine krav og anbefalinger gjeldende digitalisering i sitt informasjonssikkerhetsarbeid. Vi har funnet enkelte forbedringsområder. Undersøkelsen viser i noen tilfeller at det er manglende samsvar mellom hva som er beskrevet i kommunens dokumenter, og hva som er kommunens praksis. I tillegg er det en svakhet at sentralt datarom ikke er sikret med elektronisk dørlås for sporbarhet og sikring mot tilgang fra uvedkommende. Vi ser også at standarder for bruk av VPN i liten grad er fulgt opp, ved at kun seks av syv løsninger er i henhold til veiledning for bruk av VPN.

Kommunen bør:

- sørge for at det er samsvar mellom prosedyrer og praksis, og oppdatere dokumentene der det er nødvendig, herunder:
    - Virksomhetsstyring og internkontroll i Råde kommune
    - Funksjoner innen internkontroll, beredskap, digital personsikkerhet og HMS
    - Prosedyre for oppretting eller fjerning av brukere
    - IKT beredskapsplan
- vurdere å utarbeide opplæringsplan innen digital sikkerhet
- anskaffe elektronisk dørlås til sitt sentrale datarom
- sørge for at alle VPN-løsninger er oppdatert i henhold til Digdirs anbefalinger

5 RETNINGSLINJER OG RUTINER

Problemstilling 2:

Har kommunens ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

5.1 Revisjonskriterier

- De ansatte skal få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer.
- De ansatte skal kjenne til kommunens egne rutiner og prosedyrer for informasjonssikkerhet.

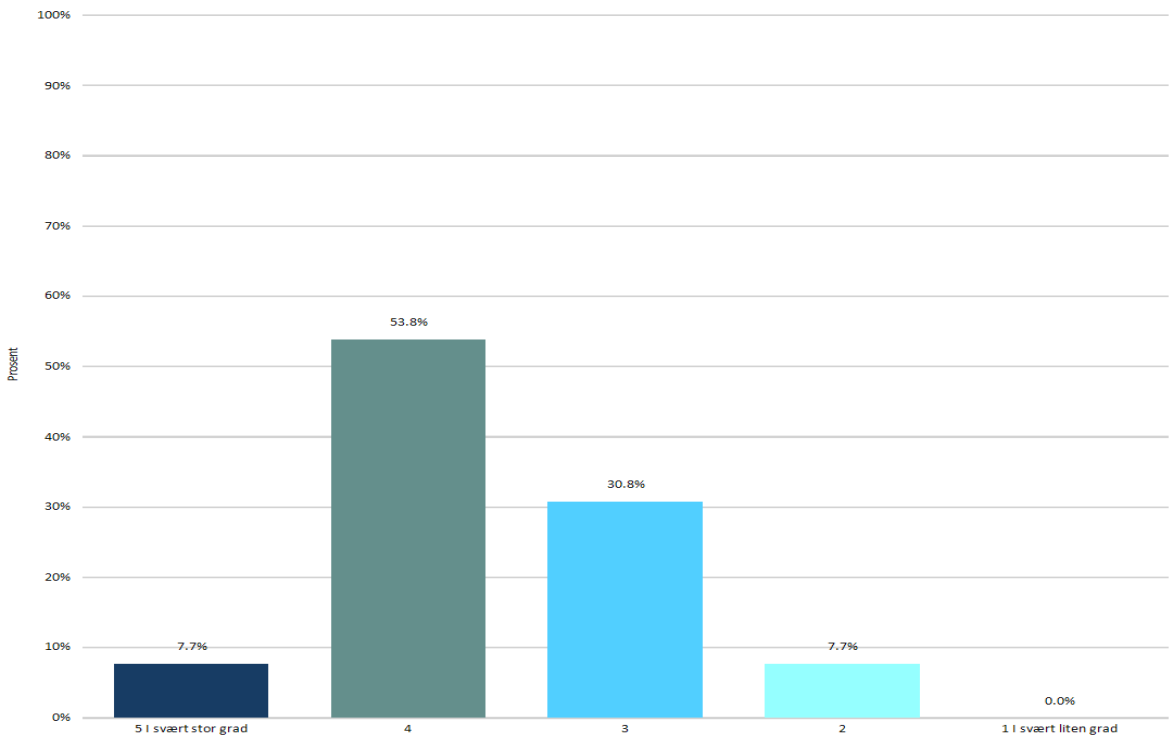
5.2 Datagrunnlag

5.2.1 Opplæring

I møter med kommunen har revisjonen fått informasjon om at gjeldende praksis for opplæring innen informasjonssikkerhet er nyansattmøter, dialogmøter med IKT-avdelingen, notifikasjoner i kvalitetssystemet og nanolæring. Kommunen har flere rutiner og prosedyrer på informasjonssikkerhetsområdet.

20 % av respondentene har jobbet mindre enn 3 år i kommunen. 70 % av disse oppgir at de har deltatt, eller skal delta, på kommunens nyansattopplæring. 20 % oppgir at de ikke har deltatt på slik opplæring, mens 10 % ikke vet om de har deltatt, eller skal delta på nyansattopplæring.

Figur 2 viser at 61,5 % av respondentene opplevde å ha stort eller svært stort utbytte av opplæringen. 7,7 % opplevde liten grad av utbytte.

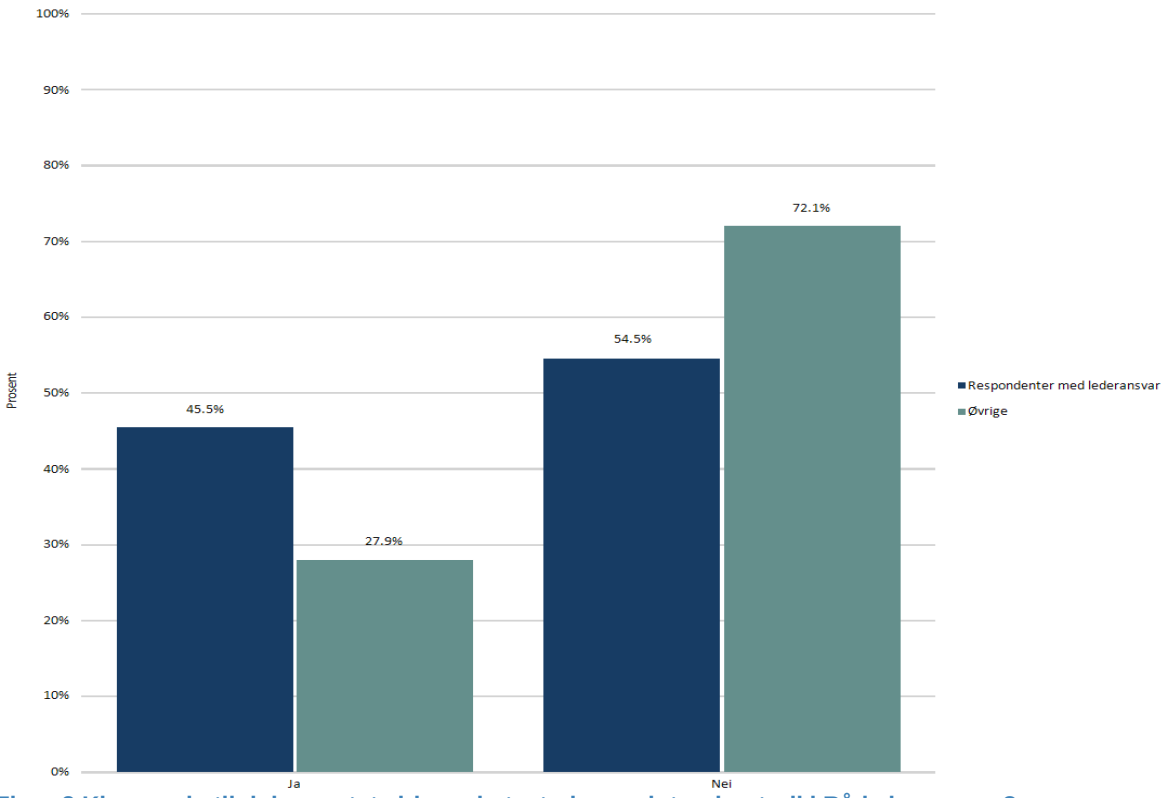


Figur 2 I hvilken grad hadde du utbytte av kommunens nyansattopplæring knyttet til informasjonssikkerhet?

I spørreundersøkelsen oppgir 32,7 % at de har lederansvar for fag, personal eller budsjett.

31,3 % av respondentene med lederansvar svarer bekreftende på at de har deltatt på dialogmøte med IKT-avdelingen, og 90 % fant møtene med IKT-avdelingen nyttig i stor, eller svært stor, grad. 10 % mener at møtene i liten grad var nyttig.

Dokumentet «Virksomhetsstyring og internkontroll i Råde kommune» beskriver at kommunalsjefer og virksomhetsledere, gjennom delegert fullmakt fra kommunedirektøren, har ansvar for internkontroll i egen virksomhet. På spørsmål om de kjenner til dokumentet, svarer 66,3 % av respondentene at de ikke kjenner til dette. I figuren nedenfor er spørsmålet filtrert til å vise hvordan kjennskapen til dokumentet fordeler seg blant de som har lederansvar (enten innen budsjett, fag eller personal), og øvrige respondenter, og vi kan se at 45,5 % av respondenter med lederansvar kjenner til dokumentet.



Figur 3 Kjenner du til dokumentet virksomhetsstyring og internkontroll i Råde kommune?

I tabell 2 kan vi se hvor ofte respondentene med lederansvar har informasjonssikkerhet som tema i samhandling med sine ansatte.

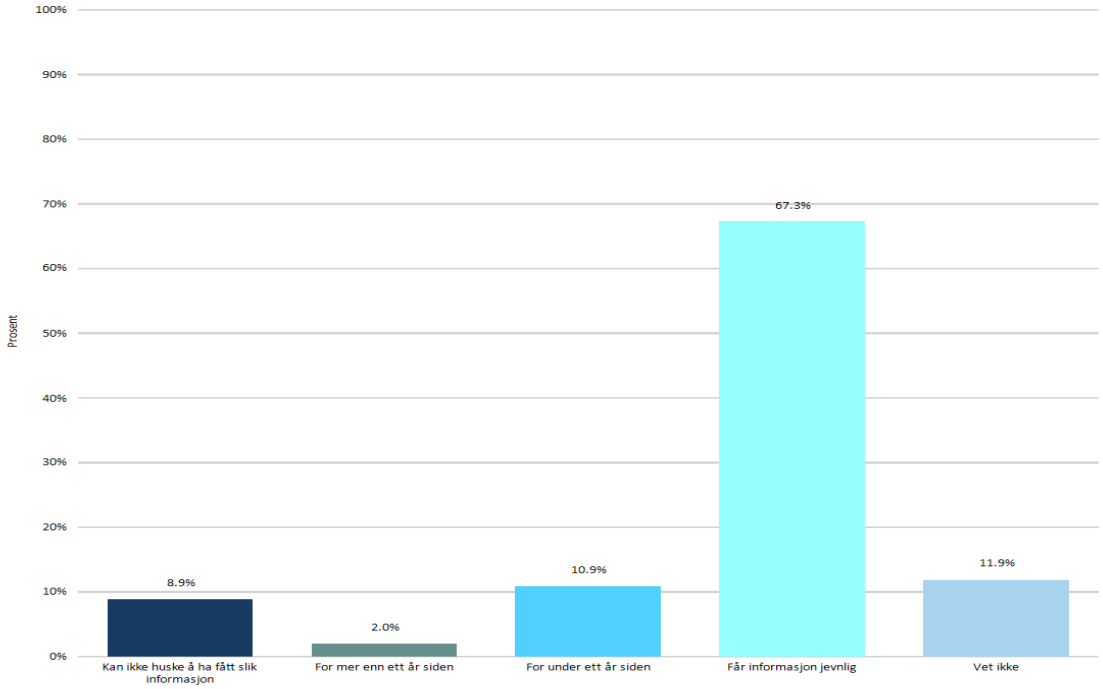
Har du informasjonssikkerhet/digital sikkerhet som tema i samhandling med dine ansatte?	Prosent
Ja, ofte	21,2%
Ja, noen ganger	30,3%
Sjelden	15,2%
Nei, det har ikke blitt prioritert	9,1%
Nei, informasjonssikkerhet er ikke mitt ansvarsområde	21,2%
Annet	3,0%

Tabell 2 Har du informasjonssikkerhet/digital sikkerhet som tema i samhandling med dine ansatte? Eks. i møter, rutiner, e-post mv.

Tabellen viser at 21,2 % mener at informasjonssikkerhet ikke er deres ansvar, mens 51,5 % ofte, eller noen ganger, har informasjonssikkerhet som tema i samhandling med sine ansatte.

Når det gjelder egen leder, svarer 65 % at deres leder i stor, eller svært stor grad, er opptatt av informasjonssikkerhet. 11 % svarer at de opplever sin leder å være lite, eller svært lite, opptatt av informasjonssikkerhet.

I figur 4 kan vi se når de ansatte selv mener å ha mottatt informasjon om kommunens krav og forventninger til informasjonssikkerhet.
To tredjedeler (67,3 %) av respondentene mener at de får informasjon om kommunens krav og forvent-



Figur 4 Når fikk du sist informasjon om kommunens krav og forventninger til informasjonssikkerhet?

ninger til informasjonssikkerhet jevnlig, og 10,9 % oppgir å ha fått informasjon for under ett år siden. På dette spørsmålet var det mulig å velge flere svaralternativer. 8,9 % kan ikke huske å ha fått slik informasjon, mens 11,9 % ikke vet om de har fått informasjon om kommunens krav og forventninger.

Som det fremkommer i kapittel 4.2.1.5 om Kompetanse- og kulturutvikling foregår opplæring av sluttbrukere i sikkerhetsarbeid gjennom nanolæring. Opplæringsseksjoner sendes jevnlig til alle kommunale e-postadresser. I vår spørreundersøkelse oppgir 71,3 % at de har gjennomført de nanolæringsleksjonene de har fått tilsendt, og 21,8 % har delvis gjennomført. 5 % kjenner ikke til nanolæring, og 2 % har ikke gjennomført tilsendte leksjoner. Av de 93,1 % av respondentene som helt eller delvis har gjennomført nanolæring, mener 70,2 % at slik læring i stor, eller svært stor, grad er nyttig for å få mer kunnskap om digital sikkerhet.

Tabellen nedenfor viser de ansattes opplevelse av informasjon og opplæring innen informasjonssikkerhet.

I hvor stor grad opplever du å ha fått tilstrekkelig informasjon og opplæring?	Prosent
5 I svært stor grad	19,2%
4	44,4%
3	27,3%
2	4,0%
1 I svært liten grad	5,1%

Tabell 3 I hvor stor grad opplever du at du har fått tilstrekkelig informasjon og opplæring innen informasjonssikkerhet/digital sikkerhet?

På generell basis opplever 9,1 % av de spurte at de i liten, eller svært liten grad, har fått tilstrekkelig informasjon og opplæring innen informasjonssikkerhet, mens 63,6 % mener de i stor, eller svært stor, grad har fått tilstrekkelig informasjon og opplæring.

5.2.2 IKT reglement og lagring

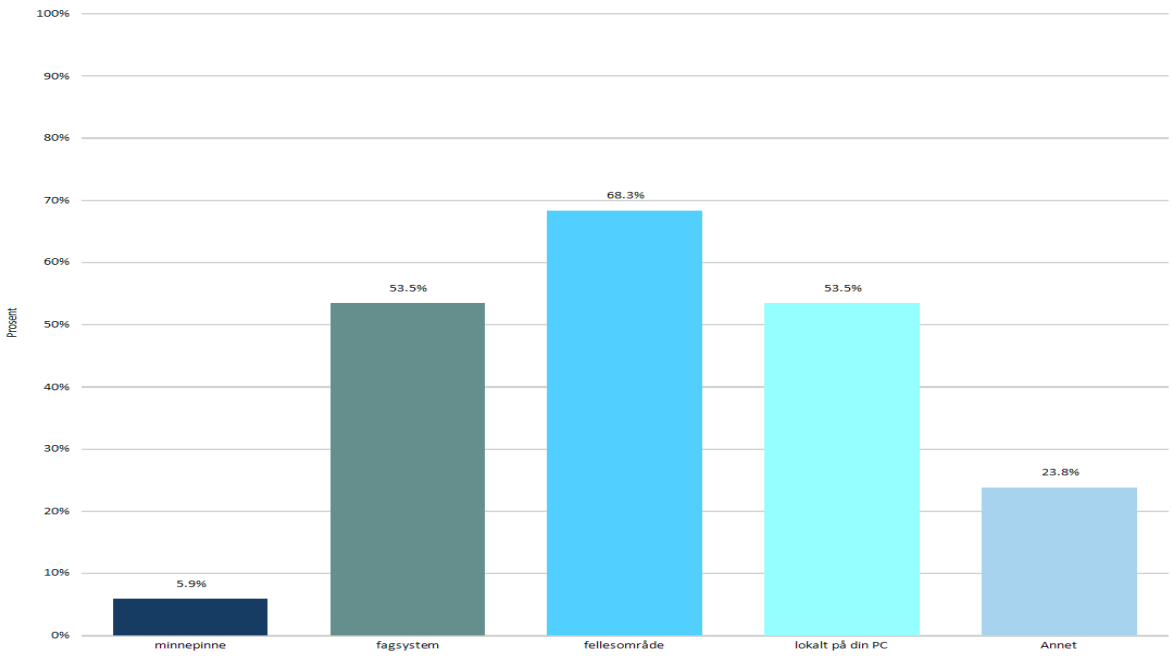
Kommunens IKT reglement gjelder for all bruk av Råde kommunes IKT-tjenester. Reglementet fastslår at med IKT-tjenester menes datamaskiner og IKT-systemer, sluttbrukerutstyr, nettverk, programmer, data mv. som kommunen stiller til disposisjon, eller andres maskiner og systemer som man får tilgang til gjennom slike ressurser. Reglementet gjelder også for privat utstyr så lenge det er koblet til Råde kommunes nettverk.

I reglementets punkt 1.3 fremkommer det at alle brukere plikter å holde seg informert om det til enhver tid gjeldende reglement. Punkt 1.2 slår fast at «Alle nyansatte må lese dette dokumentet og signere på at teksten er lest og forstått».

På spørsmål om de ansatte kjenner til kommunens IKT reglement svarer 73,5 % bekreftende på dette. Av disse svarer 55,6 % at de har signert IKT reglementet, mens 36,1 % ikke vet om de har signert. Etter gjennomføring av spørreundersøkelsen er revisjonen gjort kjent med at kommunen sikrer at alle ansatte leser og signerer IKT reglementet, ved at dette gjennomføres i samme prosess som de ansatte signerer arbeidsavtale ved oppstart av arbeidsforholdet med kommunen.

IKT reglementet har også en egen del (del 2) knyttet til bruk av PC. Her står det at all kommunal informasjon skal lagres på kommunens servere, og det er forbudt å lagre personsensitiv informasjon på egen PC. Det er også et eget avsnitt helt til slutt i dokumentet, som omhandler lagring av filer. Der fremkommer det at ansatte skal bruke fagsystemer der dette er på plass, og ellers på angitt stasjoner i intern sone. Avsnittet beskriver også hvem som har tilgang til informasjonen på de ulike stasjonene.

Som det fremkommer av figuren nedenfor, spurte vi kommunens ansatte om hvilke lagringsløsninger de bruker i sitt arbeid. Det var mulig å velge flere svaralternativer på dette spørsmålet.

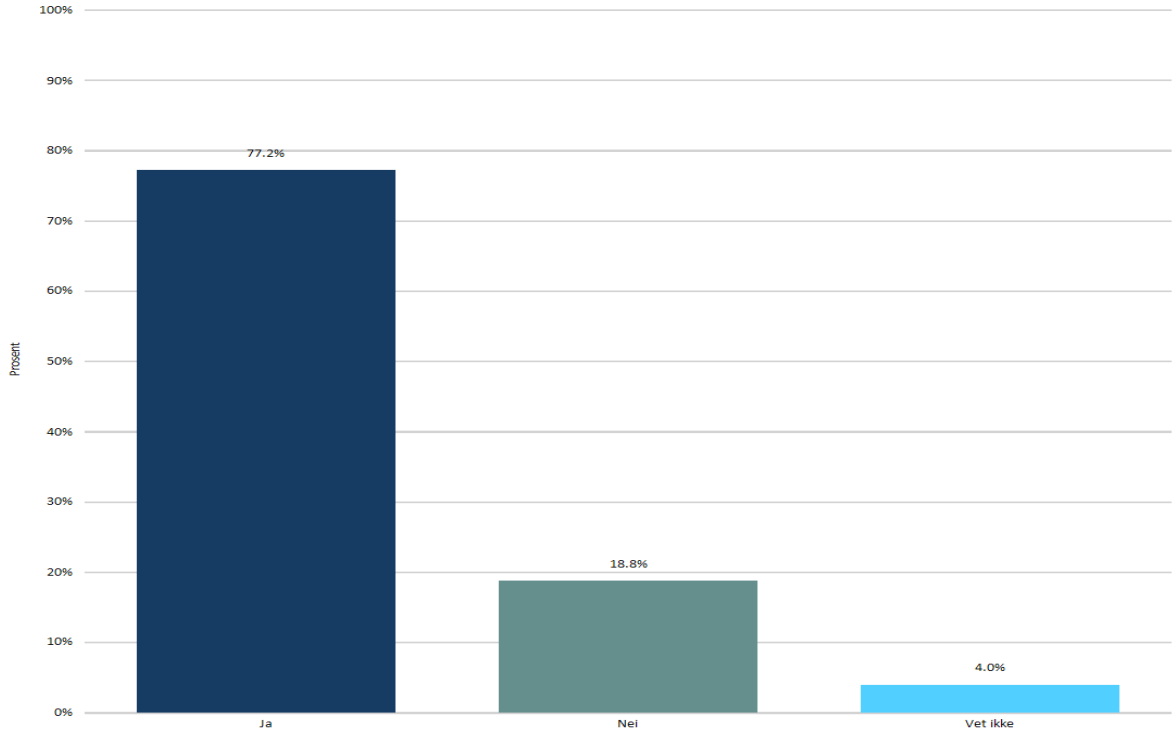


Figur 5 Hvilke av disse lagringsmulighetene bruker du i ditt arbeid?

Tabellen viser at 53,5 % benytter seg av muligheten for å lagre i fagsystemet, og 68,3 % bruker kommunens fellesområde til lagring av informasjon.

53,5 % oppgir at de lagrer informasjon lokalt på sin PC, 5,9 % bruker minnepinne og 23,8 % bruker andre lagringsløsninger enn de vi har skissert i svaralternativene. Revisjonen har ikke bedt om informasjon om hvilke andre lagringsløsninger dette dreier seg om.

I figuren nedenfor kan vi se at svært mange, 77,2 %, behandler personopplysninger i sitt arbeid. 18,8 % behandler ikke personopplysninger, mens 4 % ikke vet om de behandler personopplysninger eller ikke.



Figur 6 Behandler du personopplysninger i ditt arbeid?

Av de 77,8 % som behandler personopplysninger, svarer 93,6 % at de er kjent med de regler som gjelder for lagring og bruk av personopplysninger (personopplysningsloven og personopplysningsforskriften). 6,4 % er ikke kjent med regelverket.

5.2.3 Beredskapsplan og avvik

Kommunens prosedyre for avvikshåndtering gjelder for alle ansatte i kommunen, og det er den enkelte ansatte som har ansvar for å melde avvik. I prosedyren er et avvik definert som en «uønsket hendelse», som oppstår når det ikke er samsvar mellom praksisen som blir utøvd og det som følger av eksterne lover, forskrifter, regelverk eller av Råde kommunes interne policyer og prosedyrer. Avvik omfatter også feil og mangler som omfatter teknologi, systemer og verktøy dersom disse ikke fungerer som forutsatt.

I prosessbeskrivelsen kan vi lese at den som opptager avvik skal melde dette i kvalitetssystemet/avvikssystemet.

86,1 % av de spurte oppgir at de kjenner til kommunens prosedyre for avvikshåndtering, og på spørsmål om de har opplevd situasjoner som omhandler avvik på informasjonssikkerhetsområdet oppgir 87,9 % at de ikke har opplevd slike situasjoner.

Tabellen nedenfor viser hva slags avvik, om noen, de ansatte har opplevd innenfor informasjonssikkerhet.

Forhold som innebærer avvik på informasjonssikkerhetsområdet	Prosent
Din brukerkonto har blitt brukt på et tidspunkt da du ikke var pålogget	0,0%
Du har mistet eller blitt frastjålet en datamaskin eller minnepinne med sensitiv informasjon	0,0%
Brudd på personvern/GDPR	8,1%
Uvedkommende har fått tilgang til sensitive opplysninger/fagsystem	3,0%
Data på avveie	1,0%
Andre brudd på informasjonssikkerhet	3,0%
Nei, har ikke opplevd noe slikt	87,9%

Tabell 4 Har du opplevd noe av følgende?

Av de 17,1 % som har opplevd avvik innen informasjonssikkerhet, oppgir 66,7 % at de meldte fra til sin nærmeste leder, 25 % meldte fra i avvikssystemet og 25 % meldte ikke fra om hendelsen. 8,3 % meldte fra til kommunens IKT-avdeling.

Kommunens IKT beredskapsplan er et styrings, opplærings- og oversiktsdokument i Råde kommune, og er nærmere beskrevet i kapittel 4.2.1.1 Ledelsens styring og oppfølging, og kapittel 4.2.1.4 Overvåking og hendelseshåndtering. 45,5 % av de spurte oppgir at de er kjent med kommunens IKT beredskapsplan, og 54,5 % oppgir at de ikke er kjent med denne. Tabellen nedenfor er fordelt på svaralternativene i forhold til respondenter med, og uten, lederansvar. Det er færre av respondentene med lederansvar som kjenner til beredskapsplanen (60,6 %), enn de som ikke har lederansvar (51,5 %).

Er du kjent med kommunens IKT beredskapsplan?	Ja	Nei	N
Respondenter med lederansvar	39,4%	60,6%	33
Øvrige	48,5%	51,5%	68

Tabell 5 Er du kjent med kommunens IKT beredskapsplan?

5.2.4 Kommentarer fra ansatte

På spørsmål om de har kommentarer/forbedringsforslag til kommunens arbeid med informasjonssikkerhet er det nevnt at kontorer og møterom ikke er lydtette, slik at det er fare for at uvedkommende overhører informasjon de ikke skal ha tilgang til.

Av andre forhold er det gitt tilbakemelding på at egen enhet kunne vært bedre på kommunikasjon og informasjon, samt et innspill om at virksomhetsleder setter av tid til informasjon/drøfting i virksomhetsmøter.

5.3 Vurderinger

For at kommunens arbeid med informasjonssikkerhet skal bli en suksess, er det avgjørende at de ansatte får opplæring, og at de kjenner til de dokumenter og retningslinjer som kommunen har på området.

Det er svært positivt at de aller fleste i undersøkelsen mener de har fått tilstrekkelig informasjon og opplæring innen informasjonssikkerhet, og revisjonens oppfatning er at kommunens arbeid med informasjonssikkerhet er gjenspeilet i store deler av organisasjonen.

Som nevnt i besvarelsen av første problemstilling har kommunen et opplæringssystem på området som består av nyansattopplæring, nanolæring, samt oppfølging i dialogmøter og informasjon via dokumenter og rutiner i kvalitetssystemet.
Vår undersøkelse viser at flesteparten av de som har deltatt i kommunens nyansattopplæring innen informasjonssikkerhet opplevde dette som nyttig i større grad, noe revisjonen ser på som positivt ettersom en slik opplæring vil favne de fleste av kommunens ansatte.

Det er kun ca. en tredjedel av respondentene med lederansvar som har deltatt på dialogmøte med IKT-avdelingen. Men de som har deltatt opplever dette møtepunktet som svært nyttig. Revisjonen kjenner ikke til årsaken til at dialogmøter ikke benyttes i større grad, men med hensyn til nytteverdien disse møtene synes å ha, mener vi at kommunen i større grad bør sørge for at slike møter gjennomføres.

Kommunalsjefers og virksomhetslederes ansvar for internkontroll er forankret i dokumentet virksomhetsstyring og internkontroll i Råde kommune, og det er lite tilfredsstillende at under halvparten av respondentene med lederansvar kjenner til dokumentet.

Det er likevel positivt at de aller fleste respondentene med lederansvar har informasjonssikkerhet som tema i samhandling med ansatte, men når det gjelder spørsmål om ansvar for informasjonssikkerhet merker vi oss at en av fem med lederansvar mener at informasjonssikkerhet ikke er deres ansvarsområde.

De aller fleste respondentene i undersøkelsen opplever likevel at deres leder er opptatt av informasjonssikkerhet, noe som taler for at kommunen langt på vei har etablert en kultur og et miljø som omfavner internkontroll, og herunder også informasjonssikkerhet.

Videre viser undersøkelsen at de aller fleste opplever å få informasjon om kommunens krav og forventninger til informasjonssikkerhet jevnlig. Revisjonen er positiv til at kun en av ti ikke vet om de får slik informasjon, og at enda færre ikke kan huske om de har fått informasjon om kommunens krav og forventninger.

Revisjonen ser det som positivt at de aller fleste i undersøkelsen synes at nanolæringen er nyttig for å få mer kunnskap om digital sikkerhet, men at det, selv om det er svært få, er uheldig at noen av respondentene ikke kjenner til nanolæring. Det kan tyde på at, selv om kommunen selv mener dette er riktige veien å gå med opplæring, bør bruken av nanolæring i enda større grad følges opp.

Det er en del (mer enn en fjerdedel) av respondentene som ikke kjenner til kommunens IKT reglement, og flere som kjenner til det, men som ikke vet om de har signert. Revisjonen er gjort kjent med at reglementet signerer i forbindelse med ansettelse, i samme prosess som arbeidsavtalen. Revisjonen forstår at det kan være vanskelig å huske konkret signering av reglementet i en slik prosess, men at alle uansett bør ha kjennskap til dokumentet.

Undersøkelsen viser også at det er flere som bruker andre lagringsløsninger enn det som er beskrevet i kommunens IKT reglement, eksempelvis lokalt på egen PC eller på minnepinne. Etter revisjonens oppfatning kan dette føre til at sensitive opplysninger kan komme på avveie, ettersom kommunen ikke har kontroll på hvilke medier, eller hvor denne informasjonen befinner seg. Revisjonen er i forbindelse med problemstilling 1 gjort kjent med at det ikke er mulig å sperre for lokal lagring på klientPCer, noe som peker i retning av at god kommunikasjon og opplæring på dette området er kritisk for i størst mulig grad kunne forhindre at sensitiv og/eller kritisk informasjon blir lagret lokalt på de ansattes PCer.

Det er positivt at de fleste som behandler personopplysninger i sitt arbeid, kjenner til de lover og regler som gjelder for området. Det bidrar til å redusere risiko for feil behandling av slike.

Langt på vei de fleste i undersøkelsen oppgir at de kjenner til prosedyre for avvikshåndtering, men de aller fleste mener de ikke har opplevd avvikssituasjoner innen informasjonssikkerhet.
Det kan tenkes at dette skyldes at det kan være vanskelig å forstå hva som er en avvikssituasjon på informasjonssikkerhetsområdet. Skal det for eksempel meldes i fra om man mottar en e-post man selv forstår er til feil mottaker, eller som den ansatte forkaster grunnet at det tydelig er et svindelforsøk?

Riktig bruk av avvikssystemet er viktig for å sikre at alle avvik blir synliggjort og fulgt opp. Det er også viktig i forhold til å kunne fange opp om det er gjentagende avvik, som eventuelt kan tyde på at det foreligger systemfeil. Det er positivt at de fleste som har opplevde informasjonssikkerhetsavvik meldte ifra til sin nærmeste leder, og at en av fire brukte avvikssystemet. Det kan imidlertid se på som litt uheldig at ikke samtlige avvik er meldt inn via avvikssystemet, slik prosedyre for avvik tilsier. Videre er det uheldig at så mange som en av fire ikke meldte ifra om hendelsen i det hele tatt.

Over halvparten av de spurte kjenner ikke til kommunens IKT beredskapsplan, men revisjonen mener at dette har sammenheng med at dokumentet er på overordnet nivå, og kommunen selv mener også at det ikke er meningen at alle ansatte skal ha kjennskap til denne. Vi stiller dog spørsmål ved at det er flere uten lederansvar, enn med, som oppgir å kjenne til planen.

Hva gjelder ansattes egne kommentarer til forbedringspunkter innen informasjonssikkerhet, ser revisjonen at det er noen punkter, eksempelvis mulig behov for støyisolerende tiltak, som kommunen kan vurdere å se nærmere på.

5.4 Konklusjon og anbefalinger

Etter revisjonens vurdering har kommunen etablert flere tiltak som er egnet til å sikre ansattes kjennskap til retningslinjer og rutiner for informasjonssikkerhet. Fakta viser at Råde kommune på flere måter har arbeidet for å skape en kultur med fokus på informasjonssikkerhet og etter revisjonens vurdering har de i stor grad lyktes med det, selv om det viser seg at det er noe manglende kjennskap til konkrete dokumenter/rutiner/retningslinjer. Basert på funnene våre anbefaler vi at kommunen bør:

- følge opp at de ansatte gjennomfører nanolæring
- sørge for at virksomhetene i større grad gjennomfører dialogmøter med IKT-avdelingen
- sørge for at de ansatte i større grad har kjennskap til IKT reglementet
- sørge for at relevante ledere har større grad av kjennskap til dokumentet virksomhetsstyring og internkontroll i Råde kommune, herunder også deres ansvar for internkontroll (også innen informasjonssikkerhet)
- sørge for at ansatte lagrer opplysninger i tråd med kommunens reglement
- sørge for at det i større grad meldes fra om avvik på informasjonssikkerhetsområdet, og at avvikssystemet benyttes til dette

6 KILDER

- Sikkerhetsloven, https://lovdata.no/dokument/NL/lov/2018-06-01-24
- eForvaltningsforskriften, https://lovdata.no/dokument/SF/forskrift/2004-06-25-988
- Digitaliseringsrundskrivet H2021-5, rundskriv fra Kommunal- og distriktsdepartementet
- Digitaliseringsdirektoratet (2022). Digdir. https://www.digdir.no/
    - Referansekatalogen for IT-standarder. https://www.digdir.no/standarder/referansekatalogen-it-standardar/1480
    - Internkontroll i praksis – informasjonssikkerhet. https://www.digdir.no/informasjonssikkerhet/internkontroll-i-praksis-informasjonssikkerhet/2601
- Nasjonal sikkerhetsmyndighet (2022). NSM. https://nsm.no/
    - Grunnprinsipper for IKT-sikkerhet 2.0. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

Dokumenter fra Råde kommune:

- Rutine for backup/sikkerhetskopi av servere
- IKT Beredskapsplan
- Virksomhetsstyring og internkontroll i Råde kommune
- Resultat av hurtigtest fra HelseCERT
- Rapport fra HelseCERT
- Rutine for kartlegging av trusler
- Statistikk over gjennomført nanolæring
- IKT Kravspesifikasjoner/Kravspekk/Anskaffelsesprosess
- Statusrapporter for mulige innbrudd i perioden 2019-22
- Rutine for oppsett av ny, eller fjerning av server
- Rutine for oppsett av PCer og klienter
- Driftsrutiner, IKT
- Oversikt over PCer i Vansjoreg domenet
- Oversikt over PCer i Azure
- Oversikt over iOS enheter i Azure
- Oversikt over avvikskategorier
- Avviksrapport for kategori informasjonssikkerhet 2020 22
- Funksjoner innen internkontroll, beredskap, digital personsikkerhet og HMS
- Håndbok for informasjonssikkerhet og personvern i Råde kommune
- IKT reglement
- Kartlegging IT systemer GDPR
- Organisasjonskart
- Overordnet risikovurdering IKT, oppdatert 2022
- Prosedyre for avvikshåndtering
- Prosedyre for å opprette eller fjerne bruker for tilgang til IKT systemer
- Tiltakskort T=) – Dataangrep med bortfall digitale systemer

7 VEDLEGG

7.1 Kommunedirektørens uttalelse

Revisjonen mottok følgende uttalelse fra kommunedirektøren 13.1.2023:

Råde kommune

Østre Viken kommunerevisjon IKS
Østre Viken kommunerevisjon IKS

Dato: 12.01.2023
Vår ref.: 22/2181 - 11// MAGLA
Deres ref.: / Anita Marie Torp
Sentralb.: 69 29 50 00
Saksbh.: Marina Glazkova
marina.glazkova@rade.kommune.no

Oversendelse av kommunedirektørens kommentarer til høringsutkast av forvaltningsrevisjonsrapport Informasjonssikkerhet - Råde kommune

En forvaltningsrevisjon innen informasjonssikkerhet er en viktig del av forbedringsarbeid i Råde kommune.

Kommunedirektøren tar forvaltningsrapporten til etterretning og vil følge opp revisjonens anbefalinger. Samtidig er kommunedirektøren tilfreds med funnene forvaltningsrevisjonen presenterer. De forbedringspunktene som rapporten viser til, er områder som organisasjonen jobber aktivt med og har stort fokus på.

Resultatene som har kommet frem i kommunerevisjonens rapport må sees også i sammenheng med pandemiperioden mars 2020-februar 2022, som har vært krevende og gitt store utfordringer i organisasjonen. Med dette bakteppe er kommunedirektøren i hovedsak fornøyd med resultatene av forvaltningstilsynet, og er av den oppfatningen at Råde kommune jobber i den rette retningen innen informasjonssikkerhet.

De funnene som revisjonen har gjort og som er lagt frem i denne rapporten, harmonerer i stor grad med de områder kommunen allerede er i gang med forbedringsarbeid eller har planlagt dette i 2023.
Revisjonsrapporten er en god bekreftelse på at det er de riktige områdene innenfor informasjonssikkerhet som får særlig fokus inneværende år.

Råde kommune jobber kontinuerlig med å sikre samsvar mellom prosedyrene og praksisen på arbeidsplassene. Det dreier seg dels om opplæring i de prosedyrer som er bestemt, og dels om revisjon av prosedyrene i tråd utvikling av tjenestene og endringer i krav og forventninger fra omgivelsene. Alle kvalitetsdokumenter blir revidert årlig for å sikre at mest mulig samsvar mellom krav til tjenestene, effektiv praksis og gjeldende prosedyre.

Kommunedirektøren er enig i revisjonens konklusjon om at det ikke er tilfredsstillende at under halvparten av respondentene med lederansvar har kjennskap til dokumentet «Virksomhetsstyring og internkontroll», til tross for at dette dokumentet har vært en del av internkontrollsamling i januar 2022.

Postadresse: Skråtorpveien 2A 1640 Råde
Besøksadresse:
Hjemmeside: www.rade.kommune.no
Org.nr 940802652
Kontonr: 10140720661

I løpet av samlingen ble dokumentet «Virksomhetsstyring og internkontroll» presentert, og deltakerne fikk mulighet til å diskutere ulike problemstillinger knyttet til internkontroll. Deltakere hadde også mulighet til å gi tilbakemelding om de trengte hjelp med internkontrollarbeidet. De fleste svarte at det er behov for opplæring og veiledning. I løpet av 2022 har 6 virksomheter fått bistand med internkontrollarbeid og det ble gjennomført 9 opplæringsøkter for ulike virksomheter.
Flere av virksomhetene har fått ny virksomhetsleder det siste året og dette påvirker nok antallet som ikke kjenner til dette dokumentet. Dokumentet skal revideres i 2023 og alle ledere med personalansvar skal få ny gjennomgang.

Kommunedirektøren er fornøyd med at de aller fleste respondenter svarer at de er kjent med kommunens prosedyrer for avvikshåndtering, men at de ikke har opplevd avvikssituasjoner innenfor informasjonssikkerhet. Dette tyder på at kommunen har god internkontroll, sikkerhet og bevissthet hos de ansatte innenfor dette området.

Fra november 2021 har informasjonssikkerhet fått en egen kategori i avviksrapporteringen, for å gjøre det lettere og tydeligere å melde avvik på dette området.
Det er utarbeidet egen prosedyre for digitale svindelforsøk via e-post, da dette er noe som er blitt svært vanlig både til private og jobbrelaterte e-postadresser.
Håndtering av mistenkelige e-poster har også hatt stort fokus gjennom nanolæringen, hvor ansatte får kunnskap om horden de skal håndtere slike hendelser. Det er viktig å bemerke i forhold til informasjonssikkerhet at i henhold til kommunens prosedyrer er e-post ikke godkjent for sending av sensitiv informasjon.

Revisjonens undersøkelse avdekker at de gangene ansatte avdekker avvik innenfor informasjonssikkerhet, blir 75% av avvikene meldt til nærmeste leder, men at halvparten av disse blir meldt utenom avvikssystemet.

Kommunedirektøren vurderer det som positivt at det i aller fleste tilfeller sies i fra når det oppdages avvik, og vil arbeide videre for at avvik meldes via kommunens avvikssystem, som det er beskrevet i interne prosedyrer. Kommunedirektøren ønsker å presisere at alle avvik blir fulgt opp uansett meldemåte og overordnet ledelse i kommunen får månedlige rapporter med status på alle avvik i virksomhetene.

Dialogmøtene med fokus på informasjonssikkerhet ble startet opp i 2022 med målsetting om ett dialogmøte med hver virksomhet pr år. I løpet av 2022 ble det avholdt ett møte med hver virksomhet. I de fleste møtene er det virksomhetsleder selv som har deltatt i møtet. Virksomhetene bestemmer selv hvem som skal delta. Det er dermed mange respondenter med lederansvar som ikke har vært invitert til disse møtene. Dette gjelder både avdelingsledere og kommunalsjefer.
I tillegg har det tiltrådt flere nye virksomhetsledere etter møterunden i 2022. Dette er grunnen til at så mange ledere med personalansvar har svart at de ikke har deltatt i dialogmøtet. Dialogmøtene for 2023 har nå startet opp og alle virksomheter vil ha slikt møte i løpet av året.

Nanolæring innenfor IKT området har vært tilbudt alle ansatte med kommunal e-postadresse siden høsten 2021. Kommunedirektøren setter pris på at de aller fleste som har deltatt i opplæring har opplevd denne som positiv og relevant. Temaene har for det aller meste dreid seg om hvordan man som ansatt bidrar til datasikkerhet og har gitt kunnskap de ansatte kan benytte både i jobb og privat. Opplæring har bidratt til økt bevissthet om datasikkerhet og hvordan man avslører forsøk om svindel og datainnbrudd. Kommunedirektøren vil i 2023 vurdere om denne opplæringen skal gjøres obligatorisk for alle som får tildelt kommunal e-postadresse.

Kommunedirektøren betrakter denne rapporten som et konstruktivt innspill i det videre arbeidet med informasjonssikkerhet.

Takk til revisjonen for godt samarbeid.

For kommunedirektør

Med hilsen

Marina Glazkova
Rådgiver internkontroll og beredskap
Mobil: 98 85 08 34

Dokumentet er elektronisk godkjent og har derfor ingen signatur

7.2 Utledning av revisjonskriterier

7.2.1 Problemstilling 1

– Følger Råde kommune Digitaliseringsdirektoratet sine krav og anbefalinger gjeldende digitalisering i sitt informasjonssikkerhetsarbeid?

I 2019 vedtok regjeringen en digitaliseringsstrategi for offentlig sektor for perioden 2019-2025. Retningen for arbeidet med digitalisering av offentlige tjenester er i tråd med føringene i Meld. St. 27 (2015-2016). Det fremkommer av strategien at ivaretakelse av personvern og informasjonssikkerhet er avgjørende for at offentlig sektor skal lykkes med digitaliseringsarbeidet. Videre at digitaliseringen krever gjennomgripende endringer i måten offentlig sektor utfører sine oppgaver på, og dermed også hvordan man sikrer og forvalter dokumentasjon. Ambisjonen om økt digitalisering betyr at styrking av personvern og informasjonssikkerhet blir stadig viktigere.

Regjeringen er øverste organ i sentralforvaltningen og ansvarlig overfor Stortinget, både når det gjelder saksforberedelser og gjennomføring av Stortingets vedtak. Departementene skal sørge for å gjennomføre vedtatt politikk, ofte gjennom ytre etater som direktoratene. Ifølge sikkerhetsloven er departementene ansvarlig for forebyggende sikkerhetsarbeid innenfor sine ansvarsområder.[19]

Det følger av eForvaltningsforskriftens § 15 om internkontroll på informasjonssikkerhetsområdet at forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Videre står det at forvaltningsorganet skal ha en interkontroll (styring og kontroll) på informasjonssikkehetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem, og det organet departementet peker ut skal gi anbefalinger på området.

I digitaliseringsrundskrivet H2021-5[20], fra Kommunal- og distriktsdepartementet (KDD), punkt 1.4 om oppfølging av informasjonssikkerheten, fremkommer det at KDD har pekt ut Digitaliseringsdirektoratet (Digdir) til det organ som skal gi anbefalinger om internkontroll (styring og kontroll) på informasjonssikkerhetsområdet, jf. eForvaltningsforskriften § 15. Digdir har utviklet en veileder som understøtter virksomhetsledelsens arbeid med helhetlig internkontroll, blant annet ved å hjelpe virksomheten til å identifisere plikter etter annet regelverk, som personvernforordningen.

Digdir ble formelt opprettet 1. januar 2020. Direktoratet har følgende hovedfunksjoner:

- Bidra til utvikling og gjennomføring av regjeringa sin ikt-politikk.
- Premissgiver for digitalisering og helskapt informasjonsforvaltning.
- Premissgiver for innovasjon i offentlig sektor, og et særlig ansvar som tilrettelegger for godt samspill mellom aktører på feltet.
- Koordinering av tverrgående digitaliseringstiltak.

[19] https://lovdata.no/lov/2018-06-01-24/§2-1

[20] Digitaliseringsrundskrivet er en sammenstilling av pålegg og anbefalinger om digitalisering i offentlig sektor. Rundskrivet gjelder for departementene, statens ordinære forvaltningsorganer, forvaltningsorganer med særskilte fullmakter og forvaltningsbedrifter.

- Strategisk planlegging og videreutvikling av en helskapt digital infrastruktur for offentlig sektor.
- Samordner og pådriver i offentlig sektors arbeide med forebyggende informasjonssikkerhet.
- Forvalte og utvikle klart språk.
- Utvikling av digitale tjenester for innbyggere, kommuner og næringsliv.
- Drift og forvaltning av felleskomponenter og fellesløsninger.
- Tilsyn for universell utforming av IKT.

Digdir beskriver arbeidet med informasjonssikkerhet som at det handler om å sikre informasjonsbehandling som inngår i oppgaver og tjenester[21]. Videre at det handler om å:

- Sikre informasjonssystemene som benyttes – inkludert digitale tjenester, IKT-systemer og komponenter som inngår i IKT-systemer.
- Tilrettelegge arbeidsoppgaver (prosesser) slik at det er enkelt for mennesker å utføre oppgavene sine med god sikkerhet.
- Sikre tilstrekkelig kompetanse hos de som utfører oppgaver for virksomheten og å jobbe for en kultur som understøtter arbeidet med informasjonssikkerhet.

Som det fremkommer på Digdirs hjemmeside er det vanlig å si at informasjonssikkerhet handler om å sikre at informasjon i alle former:

- Ikke blir kjent for uvedkommende (konfidensialitet)
- Ikke blir endret utilsiktet eller av uvedkommende (integritet)
- Er tilgjengelig ved behov (tilgjengelighet)

Digdir har sammenstilt en oversikt over krav og anbefalinger som gjelder ved digitaliseringsarbeid i offentlig forvaltning. Knyttet til informasjonssikkerhet finner vi fire krav, som alle er forankret i forskrift om IT-standarder i offentlig forvaltning. De fire kravene er som følger:

1. **Bruk grunnleggende protokoller for kommunikasjon på internett.**
   IPv4 og IPv6 er grunnleggende protokoller for kommunikasjon på internett. Alt IT-utstyr som det offentlige anskaffer bør ha støtte for IPv4 og IPv6.

Forskrift om IT-standarder i offentlig forvaltning § 12, siste ledd, presiserer dette ytterligere, og sier at nye interne nett og løsninger i offentlige virksomheter skal ha støtte for IPv6, men at det er tillatt å støtte IPv4 i tillegg.

2. **Bruk internkontroll på informasjonssikkerhetsområdet.**

Referansekatalogen for IT-standarder inneholder obligatoriske og anbefalte standarder som gjelder for internkontroll/styringssystem/ledelsessystem på informasjonssikkerhetsområdet.

Det er obligatorisk for forvaltningsorgan som benytter elektronisk kommunikasjon å ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. eForvaltningsforskriften § 15 «Internkontroll på informasjonssikkerhetsområdet» sier følgende i 1.-3. ledd:

«Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget

[21] https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-en-forutsetning-na-virksomhetens-mal/1123

for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området. Omfang og innretning på internkontrollen skal være tilpasset risiko.»

Det er anbefalt å basere seg på gjeldende versjon av ISO/IEC 27001[22]. Digdirs veiledning «Internkontroll i praksis – informasjonssikkerhet» er basert på denne standarden, og konkretiserer de mest sentrale delene av standarden til syv hovedaktiviteter. Det er anbefalt å bruke veiledningsmateriellet som referanse og støtte ved analyse av status, og ved etablering og forbedring av internkontroll på informasjonssikkerhetsområdet. De syv hovedaktivitetene er:

- **Ledelsens styring og oppfølging.** Ledelsen er ansvarlig for å etablere tilstrekkelig styring og kontroll i virksomheten. For å lede virksomheten på en god måte, er ledelsen avhengig av tilstrekkelig styring på informasjonssikkerhetsområdet. Det oppnås gjennom etablering og oppfølging av et systematisk arbeid med styring av informasjonssikkerhet i hele virksomheten.
- **Vurdering av risiko** – vurderingene kan gjelde hele virksomheten på strategisk nivå, enkelte oppgaver eller tjenester, eller spesifikke informasjonssystemer eller deler av disse.
- **Håndtering av risiko.** Grovt sett finnes fire hovedalternativer for håndtering av risiko; unngå, dele, redusere, akseptere. Sikkerhetstiltak etableres og forvaltes for å redusere risiko, gjennom å redusere konsekvenser av uønskede hendelser eller sannsynligheten for at de inntreffer. Risikoen kan også deles eller aksepteres.
- **Overvåking og hendelseshåndtering.** Virksomheten må forberede seg på at uønskede hendelser, avvik og informasjonssikkerhetsbrudd kan forekomme. Som en del av risikohåndteringen blir det derfor etablert tiltak som har som formål å oppdage informasonssikkerhetshendinger, håndtere dem og redusere konsekvensene ved slike hendinger.
- **Måling, evaluering og revisjon.** Formålet er at ledere på alle nivåer skal få bedre kunnskap om tilstanden på sitt ansvarsområde. Det må systematisk gjøres vurderinger om sikkerhetstiltakene fungerer, om regelverk blir etterlevd, og om internkontrollarbeidet i virksomheten blir gjennomført som planlagt. Dette gjøres gjennom ulike kombinasjoner av målinger, undersøkinger, evalueringer og revisjoner.
- **Kompetanse- og kulturutvikling.** Både kompetanse og kultur er en avgjørende del av arbeidet med styring av informasjonssikkerhet. Ansatte med ulike roller må ha nødvendig kunnskap, vite hvorfor informasjonssikkerhet er viktig, og ha grunnleggende forståelse for hva det handler om.
- **Kommunikasjon.** God kommunikasjon, både skriftlig og muntlig, er en forutsetning for god styring og kontroll. Dokumentasjon er en viktig del av dette, og virksomheten må ha tydelige føringer for hvordan kommunikasjon og dokumentasjon skal foregå.

Digdir presiserer at lov- og regelverkskrav kan være mer omfattende enn krav og anbefalinger i nevnte standard. Virksomhetene må derfor, som en del av arbeidet, identifisere og etterleve de lov- og regelverkskrav som gjelder for dem.

3. **Bruk kravspesifikasjon for PKI ved anskaffelse av PKI-tjenester.**

[22] ISO/IEC 27001 – Sertifisering av ledelsessystem for informasjonssikkerhet – anerkjent standard for datasikkerhet.

Public Key Infrastructure (PKI) er en overordnet, funksjonell kravspesifikasjon for anskaffelse av PKI, og blir brukt i forbindelse med elektronisk kommunikasjon med og i offentlig sektor. Offentlig nøkkelkryptering (PKI) handler om elektronisk identifisering og signatur, samt kryptering for hemmelighold. Dette er en nyttig, og ofte nødvendig, funksjonalitet når offentlig sektor tilbyr digitale tjenester til sine innbyggere. Det er viktig at brukeren er identifisert, slik at det er sikkert at vedkommende er den den utgir seg for å være – slik at sensitiv informasjon ikke gis ut til feil person, eller kommer på avveie. For kommunen er det obligatorisk å bruke «Kravspesifikasjon for PKI i offentlig sektor versjon 2.0» ved:

- Anskaffelse av PKI-tjenester i markedet til bruk i elektronisk kommunikasjon mellom offentlige virksomheter og med innbyggere eller næringsliv.
- Elektronisk signering i forbindelse med tinglysning, jf. Forskrift om prøveprosjekt for elektronisk kommunikasjon ved tinglysing av 3.5.2007 nr. 0476.
- Elektronisk signering av tilbud i forbindelse med offentlige anskaffelser. Dette gjelder når det i eller i medhold av tinglysingsloven er krav om underskrifter på dokument, og det brukes elektronisk kommunikasjon.

4. Bruke standard for sikker datakommunikasjon fra offentlige nettsteder (HTTPS)

HTTPS er overføring av nett-trafikk over en sikker forbindelse. Ved å bruke krypteringsprotokollen Transport Layer Security (TLS) kan klienten verifisere identiteten til tjenesteleverandøren, og nett-trafikken kan overføres kryptert – som gjør det uleselig for uvedkommende under transporten.

Krav om sikker datakommunikasjon fra offentlige nettsteder kom i oktober 2021. I forskrift om IT-standarder i offentlig sektor, § 11. Obligatoriske standarder for kryptert datakommunikasjon med offentlige nettsteder og –tjenester, står det:

«Nettsteder og andre offentlige tjenester, herunder applikasjonsgrensesnitt (API-er), som benytter hypertekstoverføringsprotokollen (http) skal kryptere kommunikasjonen med transportlagssikkerhet i henhold til standarden HTTP over TLS [RFC 2818] ved bruk av protokollene HTTP/1.1 [RFC 7230 til RFC 7235] og TLS 1.2 [RFC 5246] eller TLS 1.3 [RFC 8446]. Fram til 1.1.2024 skal TLS 1.2 brukes, hvis en av kommunikasjonspartene ber om det. Kravet gjelder ikke lukkede tjenester hvor forvaltningsorganet ivaretar sikkerheten på annen måte. Dersom en tjeneste får en forespørsel om kommunikasjon over HTTP uten bruk av TLS skal tjenesten svare ved omdirigering til samme URL med bruk av HTTP over TLS».

Utover de fire skal-kravene, har Digdir også definert **syv anbefalte** løsninger for kommunens informasjonssikkerhet. Kommunen bør bruke:

1. grunnprinsippene for IKT-sikkerhet
2. rettleder om internkontroll i praksis (utredet sammen med skal-kravet til internkontroll)
3. standard for filoverføring
4. standard for sikker bruk av domenenavn
5. standarder for sikring av kommunikasjonskanaler
6. standarder for å motvirke falske avsendere av e-post
7. standarder for sikring av e-post.

Nasjonal sikkerhetsmyndighet (NSM) sin veileder **«Grunnprinsipper for IKT-sikkerhet»** beskriver hva en virksomhet bør gjøre for å sikre et IKT-system, og hvorfor. Grunnprinsippene er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet, og uthever de viktigste sikringstiltakene i SIO/IEC 27002:2017. NSM påpeker at hvilke anbefalinger som er

relevante vil variere med type virksomhet, og for store virksomheter vil de fleste tiltakene være relevante. Veilederen oppdateres jevnlig basert på innspill fra brukere og fagmiljøer fra offentlig og privat sektor.

Ifølge veilederen vil en angriper som regel bruke enkleste veien inn i systemene. Om det finnes sikringstiltak som er enkle å omgå vil angriperen lete etter, og utnytte, dette. Sårbarheter kan oppstå dersom kvaliteten på anskaffelsesprosessen ikke er god nok slik at komponenter eller tjenester med manglende sikkerhetsfunksjonalitet, manglende sikkerhetsrettinger eller feil konfigurasjon innføres. Sårbarheter kan også skyldes feil på produktet, plantede sårbarheter, oppdateringer eller vedlikehold. For i størst mulig grad å hindre sårbarheter fra å oppstå bør sikkerhet være en del av virksomhetens tankegang fra beslutning og anskaffelse til drift, vedlikehold og avskaffelse.

Veilederen er delt i **fire** kategorier, med til sammen 21 prinsipper, som hver beskriver tiltak som virksomheten bør implementere for å sikre sine systemer:

1. **Identifisere og kartlegge –** opparbeide og forvalte forståelse om virksomheten herunder leveranser, tjenester, systemer og brukere.

Manglende styringsstrukturer og prosesser for risikovurdering kan føre til at ledelsen ikke får tilstrekkelig informasjon til å prioritere og styre virksomhetens sikkerhetsarbeid. Prinsippet **kartlegg styringsstrukturer, leveranser og understøttende systemer**, handler om at virksomheten må identifisere, prioritere og beskytte sine viktigste leveranser. Mangelfull oversikt kan føre til at enkelte, mindre viktige deler av IKT-systemet kan være godt sikret, mens andre mer vesentlige deler er eksponert og sårbart for angrep.

Kartlegging av enheter og programvare er viktig for å få oversikt over hva som befinner seg i virksomheten. En slik kartlegging bør avdekke både virksomhetsstyrte enheter, legitime enheter med begrensede rettigheter (for eksempel IoT[23]-enheter) og ukjente enheter (eks. ansattes private utstyr eller ondsinnede enheter). Kartleggingen bør dekke all programvare som brukes i virksomheten, både installert av IT-avdelingen og uautorisert programvare. Virksomheten bør få oversikt over enheter, programvarer og sårbarheter før eventuelle angripere gjør det.

En angriper har ofte som mål å øke sin tilgang, ofte gjennom å ta over ulike kontoer og søke seg til større rettigheter. Ved å **kartlegge brukere og behov for tilgang** minimeres risikoen for at brukere har tilgang til systemer og tjenester de ikke har behov for, og med mer rettigheter enn nødvendig for å gjøre jobben sin. NSM anbefaler at tilgangene til de ulike delene av et informasjonssystem deles opp, for å redusere skaden ved kompromittering eller utro ansatte.

2. **Beskytte og opprettholde –** prinsipper som må til for å ivareta en sikker tilstand for IKT-miljøet for å motstå eller begrense skaden fra dataangrep.

Ved å **ivareta sikkerhet i anskaffelses- og utviklingsprosesser** vil virksomheten minimere risikoen for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter. Sikkerhet er ikke kun viktig ved anskaffelse av rene sikkerhetsprodukter som eks. en brannmur. Om virksomheten anskaffer IKT-produkter og –tjenester med svak sikkerhet eller dårlig integrasjon med øvrig sikkerhetsarkitektur og produkter, kan det øke sårbarheten og redusere sikkerhetsnivået i IKT-systemet. Hvis virksomheten mangler gode prosesser for utvikling, test, verifisering og implementering vil sannsynligheten være stor for at sårbarhetene ikke blir oppdaget.

[23] Internet of Things – samlebegrep for enheter som kan kobles til internett, eks. klokker, avtrekksvifter, kjøleskap, biler mv.

Etabler en sikker IKT-arkitektur. Angripere går minste motstands vei, slik at dårlig planlegging, mangelfull kontroll ved byggeprosess og/eller manglende vedlikehold kan det føre til mange hull og inngangsdører som en angriper kan benytte seg av. For god sikring beskrives viktige momenter som å sikre at alle virksomhetens IKT-produkter fungerer godt og sikkert sammen, drift og sikkerhetskonfigurasjon bør skje sentralt og likt per type enhet, samt at IKT-systemet bør deles opp i forskjellige deler etter tillitsnivå – for å begrense konsekvenser ved eventuelt angrep eller menneskelig feil.

De fleste IKT-produkter leveres med en standardkonfigurasjon fra produsent eller forhandler, som vanligvis er utviklet for å forenkle installasjon eller bruk. Åpne tjenester og porter, standardkontoer og passord, eldre protokoller og forhåndsinstallert programvare kan gi angripere en rekke muligheter til å få uautorisert tilgang. Virksomheten bør **ivareta en sikker konfigurasjon** av sine maskin- og programvarer, og herde sine produkter, slik at det tilfredsstiller sikkerhetsbehovet. Det bør være etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester.

Virksomhetens eget nettverk kan være spredt over flere geografiske lokasjoner, og tjenester kan også være satt ut til leverandører. Tilkobling av virksomhetens nettverk til internett eller andre nettverk utenfor virksomhetens kontroll eksponerer systemene for nye angrepsflater. I tillegg kan enheter og datatrafikk angripes fra innsiden; kompromittert server eller klient, utro tjener, kompromitterte leverandører med tilgang til nettverket, svakt sikret trådløse nett eller manglende fysisk sikring av porter/kabler. Det er derfor viktig å **beskytte virksomhetens nettverk** godt mot interne og eksterne trusler, og tilgangen til nettverket bør sikres og dataflyt på nettverket bør beskyttes med kryptering.

Det bør være **kontroll på dataflyt**, både mellom de ulike delene av egne systemer, og inn og ut av virksomheten. Det er viktig for, blant annet, å hindre at kompromittering av en enhet eller sone sprer seg videre i nettverket, for å tvinge datatrafikk gjennom virksomhetens sikkerhetstiltak, og for å isolere enheter som er spesielt kritiske sårbare eller eksponerte.

Prinsippet om å **ha kontroll på identiteter og tilganger** er nært knyttet mot kartlegging av brukere og tilganger, under kategorien identifisere og kartlegge. Ansatte med flere rettigheter enn de trenger ser et problem for mange, blant annet er det vanlig at alle ansatte kan skrive til og slette alt av filer og filmapper, og kan kjøre alt som finnes av programvare. Dette er kanskje ikke nødvendig for gjennomføring av jobben, men kan være til stor hjelp for en som ønsker å angripe virksomheten. Hvis alle har rettigheter til alt, vil kompromittering av én bruker kunne kompromittere hele IKT-systemet. For å redusere skaden bør rettigheter til ulike deler av informasjonssystemet deles opp, og en virksomhet må ha kontroll på brukerne – altså kontoer, rettigheter og tilganger de disponerer.

Kryptering er en forutsetning for beskyttelse av IKT-systemet. I en virksomhet er det ulike typer informasjon med ulikt behov for beskyttelse, og virksomheten må **beskytte data i ro og i transitt.** Dersom virksomhetsdata ikke krypteres kan uvedkommende lese eller manipulere den, og føre til at informasjonens konfidensialitet og integritet brytes. Samme risiko er til stede om programvaren eller maskinvaren som brukes er implementert med utilsiktede sårbarheter, eller om krypteringsnøkler er svakt beskyttet.

For å minimere angriperes mulighet til å manipulere menneskelig oppførsel i forbindelse med bruk av epostklienter og nettlesere bør virksomheten **beskytte e-post og nettleser.** Funksjoner og applikasjoner som skal motta og behandle data fra ukjente eksterne filer er ekstra utsatt for angrep. E-post og nettsider med skadevare (virus, trojanere, osv.) er vanlige inngangsportaler for angrep. Vedlegg og lenker i e-post er en av de vanligste inngangsveiene for distribuering av datavirus, ormer og annen type skadevare. Slike vedlegg og lenker utnytter ofte sårbarheter i andre applikasjoner, eller filtypen som vises i epostklienten (.JPG, .exe, .ZIP, osv.) kan være feil i forhold til faktisk filtype.

Virksomheten bør **etablere evne til gjenoppretting av data**. Enkelte dataangrep kan føre til at kritiske konfigurasjoner, programvare eller informasjon endres eller gjøres utilgjengelig, noe som kan påvirke virksomhetskritiske prosesser. Eksempelvis ble Østre Toten kommune utsatt for kryptovirus/løsepengevirus i 2021, noe som blant annet førte til lekking av personsensitiv data og utestengelse fra egen systemer i flere uker. I dette tilfellet førte også den manglende informasjonssikkerheten til at Datatilsynet valgte å bøtelegge kommunen.

For å opprettholde virksomhetens etablerte sikkerhetstilstand ved planlagte endringer er det viktig at virksomheten **integrerer sikkerhet i prosess for endringshåndtering.** Det vil alltid være behov for endringer i en virksomhet, blant annet som følge av oppgradering og utskifting av IKT-utstyr, og organisatorisk vekst eller tilpasninger, sammenslåing av virksomheter eller tjenesteutsetting. Alle endringer som gjøres kan påvirke virksomhetens etablerte sikkerhetstilstand, og det er viktig at virksomheten forstår konsekvensen av endringene, og justerer og konfigurerer IKT-systemene for å tilpasse seg disse. Her bør det også gjennomføres tilstrekkelig med testing for å verifisere at ønsket sikkerhetstilstand opprettholdes.

3. **Oppdage –** prinsipper som ivaretar behovet for å håndtere endringer, både planlagte endringer, feilretting og sikkerhetsoppdateringer for å opprettholde den sikre tilstanden over tid.

Selv de beste produkter har feil og sårbarheter i seg, som kan utnyttes av angripere. Ondsinnet programvare kommer seg inn gjennom blant annet sluttbrukerutstyr, e-postvedlegg, nettsider, skytjenester og flyttbare medier. Virksomheten bør ha rutiner for å **oppdage og fjerne kjente sårbarheter og trusler.**

Ved å **etablere sikkerhetsovervåkning** av sine IKT-systemer og samle inn relevante data for å oppdage sikkerhetshendelser, kan virksomheten legge et grunnlag for analyse av data. Dette kan bidra til å oppdage sikkerhetshendelser tidlig, vurdere skadeomfang og hendelsens karakter, og forstå hendelsesforløpet. Mangelfull sikkerhetsovervåkning og deteksjon i informasjonssystemer, og mangelfull sammenstilling og analyse av sikkerhetsrelevante data hjelper angripere med å skjule tilstedeværelse, handlinger og aktiviteter i virksomhetens systemer.

Analyser data fra sikkerhetsovervåkning. Det kan være utfordrende å oppdage uautoriserte handlinger og sikkerhetstruende hendelser. Sammenstilling og analyse av innhentet data bidrar til å øke sjansen for å avdekke hendelser. Virksomheten bør være i stand til å finne kjente trusler i egen infrastruktur, ha kompetanse til å benytte automatiserte verktøy, og forstå hvordan disse kan utnyttes best mulig.

Virksomheten bør teste elementer i egen forsvarsmekanismer ved å **gjennomføre inntrengningstester**. Slike tester bør gjøres jevnlig for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Eksempler på svakheter kan være for langt tidsvindu fra annonsering av sårbarhet og sikkerhetsretting fra leverandør til installasjon i virksomheten, vide brukertilganger i kombinasjon med svake autentiseringsløsninger, mangelfull etablering av sikker konfigurasjon av enheter, manglende evne til å forstå egne verdikjeder og avhengigheter mellom systemer.

4. **Håndtere og gjenopprette –** prinsipper for å få på plass aktiviteter for å håndtere oppdagede sikkerhetstruende hendelser.

Forbered virksomheten på håndtering av hendelser slik at hendelser oppdages hurtig, kontrolleres, skaden minimeres og hendelsesårsaken fjernes effektivt. Dette inkluderer gjenopprettelse av integrite-

ten til systemer og nettverk. Når hendelsen inntreffer er det for sent å utarbeide gode prosedyrer, rapporteringsrutiner, datainnsamling, ledelsesansvar og kommunikasjonsstrategier. Slike ting må være på plass og øves jevnlig for å gjøre virksomheten i stand til å forstå, håndtere og gjenopprette normaltilstand.

Vurdering og klassifisering av hendelser er viktig for at virksomheten kan disponere ressurser fornuftig og løse hendelsen så raskt som nødvendig. Feilaktig klassifisering kan føre til at en virksomhet bruker mye tid og krefter på uvesentlige hendelser mens viktigere hendelser går under radaren.

Det er viktig å **kontrollere og håndtere hendelser** slik at de håndteres riktig og med riktige ressurser, for å minimere spredning og konsekvenser, og normaltilstand opprettholdes/gjenopprettes effektivt. I etterkant er det viktig å **evaluere og lære av hendelser.** Dette gjør virksomheten i stand til å forbedre sikkerhetstiltak, hendelsesprosesser, opplæring av personell og oppdatering av gjeldende prosedyrer.

Etter Digdirs anbefaling bør offentlige kommunikasjonstjenester støtte FTP (File Transfer Protocol) som protokoll for **filoverføring**. Protokollen har begrenset sikkerhet, og bør brukes over en sikker kommunikasjonskanal.

Kommunen bør også **bruke standard for sikker bruk av domenenavn**, som har som formål å redusere risikoen for brudd på integritet ved oppslag i domenenavnsystemet. Mer konkret er DNSSEC (DNS[24] Security Extensions) en sikkerhetsmekanisme som legges inn i domenenavnsystemet. Da vil svarene på et domeneoppslag signeres på en måte som gjør at det er mulig å kontrollere at de kommer fra riktig kilde og ikke er endret underveis. DNSSEC sikrer at du kommer til den adressen du vil nå, men ikke at innholdet på siden er trygt.

Det bør **brukes standarder for sikring av kommunikasjonskanaler.** VPN protokoller (Virtual Private Network) brukes for å sette opp sikre kommunikasjonskanaler mellom to eller flere endepunkt som kommuniserer over åpne nett. Det brukes kryptering og andre sikkerhetsmekanismer for å sikre at det kun er de autoriserte endepunktene som får tilgang til data som oversendes i kanalen.

Digdirs veiledning for bruk av VPN[25] viser til Referansekatalogen for IT-standarder for anbefalinger innen implementering av VPN løsninger. Det er ulike standarder som anbefales, ut fra hvilken VPN-løsning som benyttes:

a) Ved SSL/TLS[26] VPN – anbefales å bruke NIST Special Publication (SP)[27] 800-113 – Guide to SSL VPNs.
b) Ved SSH[28] VPN for sikker fjernadministrasjon av server – anbefales RFC 4251 – The Secure Shell Protocol Architecture.
c) Ved IPsec[29] VPN – anbefales NIST Special Publication (SP) 800-77 – Guide to IPsec VPNs.
d) Ved L2VPN[30]– anbefales RFC 4664 – Framework for Layer 2 Virtual Private Networks og RFC 4665 – Service Requirements for Layer 2 provider-provisioned Virtual Private Networks

[24] Domain Name Server – Server som oversetter nettadressen du skriver inn i adressefeltet til en IP-adresse.
[25] https://www.digdir.no/standarder/sikre-kommunikasjonskanalar/1495
[26] Secure Sockets Layer/Transport Layer Security, kryptografiske protokoller som autentiserer dataoverføring mellom servere, systemer, applikasjoner og brukere.
[27] National Institute of Standards and Technology.
[28] Secure shell, protokoll for kryptert forbindelse.
[29] Internet Protocol Security, navn på en rekke protokoller som sørger for sikker kommunikasjon med IP.
[30] Layer 2 VPN, ulike protokoller for kryptert utveksling av dataoverføring.

DMARC[31] er anbefalt **standard for å motvirke falske avsendere av e-post.** Det fremkommer av Digdirs veiledning på området at DMARC anbefales brukt sammen med minst en av de underliggende standardene Sender Policy Framework (SPF) og Domain Keys Identified Mail (DKIM).

Standarder for sikring av e-post. Transportsikringen bruker kryptert kommunikasjon for å overføre meldinger mellom epostservere. Digdir viser her til NSMs veileder for grunnleggende tiltak for sikring av e-post. For overføring av e-post anbefales STARTTLS[32], som er en beskyttelsesmekanisme som sørger for autentisering av eposttjenere og konfidensialitetssikring, og SPF som brukes for å spesifisere hvilke eposttjenere som er autorisert til å sende e-post på vegne av et gitt domene. For ytterligere sikring av e-post anbefaler NSMs veileder også DKIM og DMARC, som omtalt i forrige avsnitt.

Punktvis oppsummering av kriteriene:

- Kommunen skal bruke IPv4 og IPv6 ved kommunikasjon på internett, og vurdere om nytt IT-utstyr støtter disse protokollene.
- Kommunen skal ha en etablert internkontroll på informasjonssikkerhetsområdet, som er basert på en vurdering/identifisering av relevante lov- og regelverk.
- Kommunen bør bruke Digdirs «Interkontroll i praksis – informasjonssikkerhet» i arbeidet med internkontroll.
- Kommunen skal bruke kravspesifikasjon for PKI ved anskaffelse av PKI-tjenester, når det er obligatorisk.
- Kommunen skal bruke HTTPS på sine nettsteder, og ved eventuelle andre offentlige tjenester der http-protokoll brukes for overføring.
- Kommunen bør bruke NSM sine grunnprinsipper for IKT-sikkerhet i sitt arbeid med informasjonssikkerhet.
- Kommunen bør støtte FTP som protokoll for filoverføring.
- Kommunen bør bruke DNSSEC for å redusere risikoen for brudd på integritet ved oppslag i domenenavnsystemet.
- Kommunen bør bruke standarder fra Digdirs veiledning for bruk av VPN, for å sikre sine kommunikasjonskanaler.
- Kommunen bør bruke DMARC for å motvirke falske avsendere av e-post. DMARC brukes som anbefalt sammen med SPF og/eller DKIM.
- Kommunen bør bruke STARTTLS og SPF for transportsikring av e-post.

7.2.2 Problemstilling 2

Har kommunens ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

Datatilsynet skriver følgende om brukeropplæring i sin veileder om internkontroll og informasjonssikkerhet: *«Målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt, og at de er gitt mulighet til å etterleve dette i sitt daglige arbeid. Opplæring bør være tilpasset ulike målgruppers behov for opplæring og fordeles over tid. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.»* I henhold til veilederen, bør de ansatte ha fått hensiktsmessig opplæring før de får tilgang til informasjon eller tjenester. Dette inkluderer for eksempel at de kjenner til innloggingsprosedyrer, bruk av programvare, sikkerhetsinstruks og rapportering av avvik. I tillegg bør de ansatte, ifølge veilederen, få regelmessig oppdatering i organisasjonens policy og rutiner.

[31] Domain-based Message Authentication, Reporting, and Conformance.

[32] Protokoll-kommando som informerer epostserveren om at epostklienten ønsker å oppgradere fra en usikker til sikker kobling ved bruk av TLS eller SSL.

Punktvis oppsummering av kriteriene

- De ansatte skal få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer.
- De ansatte skal kjenne til kommunens egne rutiner og prosedyrer for informasjonssikkerhet.