ROMERIKE REVISJON IKS

FORVALTNINGSREVISJONSRAPPORT NR. 11-2022

IKT-SIKKERHET I KOMMUNEN

RÆLINGEN KOMMUNE

OKTOBER 2022

INNHOLD

SAMMENDRAG

Formålet med denne undersøkelsen har vært å avdekke eventuelle svakheter i IKT-sikkerheten i Rælingen kommune, slik at feil kan rettes og systemene gjøres sikrere.

Hovedfunn

1. Ansatte har for lite opplæring innen personvern og informasjonssikkerhet.
2. Det gjennomføres i for liten grad risikovurderinger knyttet til IKT-sikkerhet.
3. Praksis for å melde avvik knyttet til personvern og informasjonssikkerhet er ikke god nok.
4. Kommunen har ikke rutine for å gjennomføre inntrengningstester.

Internasjonale undersøkelser viser at de ansatte er den største sikkerhetsrisikoen på IKT-området. I denne undersøkelsen finner vi at det tilbys systematisk opplæring om IKT-sikkerhet, men at kompetansen til de ansatte i Rælingen kan bedres. Det varierer hvorvidt enhetene har gjennomført opplæringstiltak knyttet til IKT-sikkerhet. Revisjonen mener at dersom Rælingen kommune ønsker å styrke IKT-sikkerheten ytterligere, så er gjennomføring av mer systematisk opplæring av ledere og ansatte et viktig tiltak. I tillegg er det behov for å styrke kommunens spesialkompetanse innen IKT.

Kommunens egne kartlegginger viser at over halvparten av enhetene ikke har gjennomført risikovurderinger knyttet til etterlevelse av IKT-sikkerheten. Revisjonen mener det er viktig at slike risikovurderinger skjer på alle nivåer i organisasjonen, blant annet for å sikre nok oppmerksomhet rundt IKT-sikkerhet og identifisere opplæringsbehov hos de ansatte.

Det er et viktig internkontrollprinsipp å sikre at avvik meldes og følges opp, også på IKT-sikkerhetsområdet. Undersøkelsen viser at det meldes få avvik knyttet til informasjonssikkerhet og personvern. Det er etter revisjonens syn viktig å jobbe videre med å utvikle en kultur for å melde avvik, slik at feil og mangler innenfor IKT-sikkerheten kan utbedres. Mangelfull avviksmelding kan også føre til at avvik som skulle vært meldt til Datatilsynet ikke fanges opp.

Kommunen har ikke rutine for og har heller ikke gjennomført inntrengningstester tidligere. NSM anbefaler å ha rutiner for slike tester jevnlig. Inntrengningstesten som er gjennomført i denne undersøkelsen avdekket flere sårbarheter. Digitaliseringsavdelingen angir de konkrete tiltakene som er iverksatt og opplyser at alle de avdekkede svakhetene nå er lukket.

Anbefalinger

På bakgrunn av dette er revisjonens anbefalinger:

Kommunedirektøren bør sørge for

1. at alle ledere og ansatte gjennomfører systematisk opplæring for å sikre tilstrekkelig kompetanse og at ansvar for informasjonssikkerhet og personvern ivaretas på alle nivåer i organisasjonen.
2. at det gjennomføres risikovurderinger knyttet til IKT-sikkerhet på alle nivåer i organisasjonen.
3. at avvik knyttet til informasjonssikkerhet og personvern oppdages, meldes inn og følges opp.
4. at det kommer på plass en rutine for å gjennomføre inntrengningstester jevnlig.

Kommunedirektørens høringsuttalelse

Et utkast til rapport er forelagt kommunedirektøren til uttalelse. Høringssvar er mottatt 25.10.22, og er i sin helhet vedlagt rapporten. Det er gjort endringer i rapporten på bakgrunn av tilleggsopplysningene som er oppgitt i høringssvaret.

I svarbrevet peker kommunedirektøren blant annet på at systematisk og strukturert opplæring av ansatte vil være en stor fordel for IKT-sikkerheten, samt at det er behov for å bedre kulturen for å melde avvik. Kommunedirektøren opplyser også at kommunen har gått til anskaffelse av et overvåkningsverktøy som vil ha stor betydning for eksponering av tjenester ut mot offentligheten.

Jessheim, 31. oktober 2022

Øyvind Nordbrønd Grøndahl
avdelingsleder forvaltningsrevisjon

Miriam Sethne
oppdragsansvarlig forvaltningsrevisor

Dokumentet er elektronisk godkjent

1 INNLEDNING

1.1 Bakgrunn

Kontrollutvalget i Rælingen kommune vedtok 28.10.2021 (sak 39/21) å be Romerike revisjon IKS gjennomføre en forvaltningsrevisjon om digitalisering og IKT-sikkerhet.

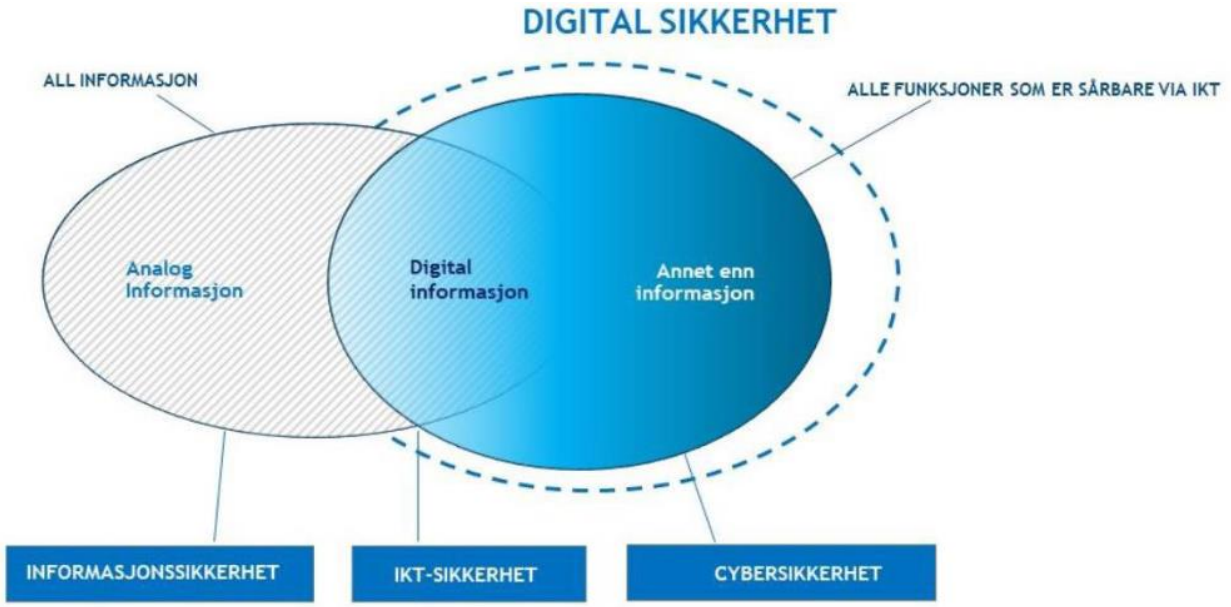
Innbrudd i en kommunes IKT-systemer kan ha store konsekvenser. I januar 2021 ble Østre Toten lammet av et datainnbrudd med løsepengevirus. Som følge av angrepet ble store deler av de kommunale systemene i Østre Toten satt ut av drift. På sykehjemmene forsvant både journaler og turnusplaner samt at signalsystemet ble satt ut av spill. I tillegg kan store mengder opplysninger være på avveie. Både KS og nasjonale myndigheter har i etterkant av dataangrepet mot Østre Toten pekt på at flere kommuner kan ha mangler i sine IKT-systemer slik at de kan rammes av lignende angrep i tiden som kommer.

Digitaliseringsdirektoratet oppsummerer i en rapport fra 2020 at fylkeskommuner og kommuner, og spesielt små og mellomstore kommuner, ikke har tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet (Digdir-rapport 2020:3).

Begrepet informasjonssikkerhet har med sikring av informasjon å gjøre uavhengig av om den er lagret digitalt eller ikke. IKT-sikkerhet har med sikring av informasjons- og kommunikasjonsteknologi å gjøre, altså maskinvare og programvare[1]. Årsaken til at IKT-sikkerhet og informasjonssikkerhet blir brukt om hverandre, er at mye informasjon er lagret og formidlet ved hjelp av IT. For å beskytte slik informasjon, må man beskytte teknologien den er lagret og formidlet på.

Figuren under illustrerer ulike begreper innenfor digital sikkerhet:

[1] IKT er en forkortelse for informasjons- og kommunikasjonsteknologi.



Kilde: Direktoratet for e-helse 2020

1.2 Formål og problemstillinger

Formålet med undersøkelsen er å avdekke eventuelle svakheter i IKT-sikkerheten i Rælingen kommune, slik at feil kan rettes og systemer kan gjøres sikrere.

Undersøkelsen vil besvare følgende hovedproblemstillinger:

1. Har kommunen etablert en tilfredsstillende overordnet styring og oppfølging av IKT-sikkerheten?
2. Er kommunen tilstrekkelig sikret mot innbrudd i kommunens interne nettverk via kommunens internetteksponerte tjenester?

1.3 Rapportens oppbygging

I sammendraget innledningsvis i rapporten framstilles rapportens hovedfunn og kommunedirektørens høringssvar til rapporten.

Kapittel 2 beskriver gjennomføring og bruk av metode. Kapittel 3 gir en samlet framstilling av revisjonskriteriene som ligger til grunn for undersøkelsen. I kapittel 4 og 5 gjennomgås funn fra undersøkelsen. Hvert av disse kapitlene avsluttes med revisjonens vurdering og konklusjon, samt anbefalinger.

2 GJENNOMFØRING OG METODE

Undersøkelsen er gjennomført i henhold til *RSK 001 - Standard for forvaltningsrevisjon*, som er fastsatt i styret i Norges Kommunerevisorforbund. Standarden (Standard for forvaltningsrevisjon RSK 001) definerer hva som er god revisjonsskikk innen kommunal forvaltningsrevisjon. [2]

2.1 Dokumentanalyse

Revisjonen har gjennomgått dokumentasjon som beskriver kommunens overordnede styring knyttet til IKT og informasjonssikkerhet, herunder mål og strategier, beskrivelser av roller, ansvar og oppgaver og risikoanalyser. Revisjonen har fått oversendt etterspurt dokumentasjon og svar på spørsmål underveis på e-post.

2.2 Intervju

Revisjonen har intervjuet leder av digitaliseringsavdelingen og fagansvarlig for informasjonssikkerhet i kommunen, samt daglig leder av Øyeren IKT (ØIKT), som har det tekniske sikkerhetsansvaret.

Intervjuet ble gjennomført som delvis strukturerte intervjuer. I forkant av intervjuet ble det utarbeidet en intervjuguide med forhåndsdefinerte spørsmål som ble gjennomgått i intervjuet. Det ble i etterkant skrevet referat fra intervjuet som er brukt som datagrunnlag i rapporten. Intervjureferatene er verifisert. Alle tre som ble intervjuet ga tilbakemelding på referatene.

2.3 Inntrengingstest

For å få svar på om kommunen er tilstrekkelig sikret mot innbrudd, er det gjennomført et «innbruddsforsøk» (inntrengingstest) i kommunens systemer. Inntrengingstesten er gjort av Norsk Helsenett SF. Dette er helse- og omsorgssektorens nasjonale senter for cybersikkerhet. Deres oppgave er å øke organisasjonens evne til å oppdage, forebygge og håndtere alvorlige cyberangrep. Norsk Helsenett har i testen forsøkt å angripe med kjente angrepsteknikker via internett. Både selve sårbarheten og beskyttelsesmekanismer som antivirus, brannmur og IDS/IPS er testet.[3] Dette har skjedd i samarbeid med IKT-avdelingen i Rælingen, bl.a. for å unngå nedetid under testingen.

Tjenester som er eksponert på internett er spesielt utsatt for datainnbrudd ettersom disse kan angripes direkte fra hvor som helst i verden. Slike angrepsforsøk foregår hele tiden og er gjerne helautomatisert av kriminelle aktører med økonomiske motiver.

---

[2] Standarden bygger på internasjonalt anerkjente standarder og prinsipper vedtatt av International Organization of Supreme Audit Institutions (INTOSAI) og The Institute of Internal Auditors (IIA).

[3] IDS (Intrusion Detection Systems) analyserer nettverkstrafikk for signaturer som matcher kjente cyberanngrep. IPS (Intrusion Prevention Systems) analyserer også signaturer/pakker, men kan også stoppe pakken fra å bli levert.

2.4 Dataenes pålitelighet og gyldighet

Pålitelige data sikres ved å være nøyaktig under innsamling og analyse av data. Kravet til gyldighet innebærer at dataene skal være relevante for å besvare problemstillingene i undersøkelsen. Revisjonen mener dataene denne rapporten bygger på samlet sett er pålitelige og gyldige og derfor gir et forsvarlig grunnlag for revisjonens vurderinger og konklusjoner.

Undersøkelsen er ikke en grundig testing av alle tjenester og nettverk. Arbeidsmetoden under en inntrengingstest er å bruke tid på systemer som virker mest lovende for å bryte sikkerhetsbarrierer. Rapporten gir derfor ikke en fullstendig oversikt over sårbarheter i tjenestene eller organisasjonen.

3 REVISJONSKRITERIER

Revisjonskriterier er normer og krav som kan stilles til kommunens virksomhet på det området som er gjenstand for en forvaltningsrevisjon. Revisjonskriteriene er dermed den målestokken som kommunens praksis holdes opp mot, og utgjør grunnlaget for revisjonens vurderinger. Revisjonskriteriene kan utledes fra lov, kommunens egne rutiner og hva som ansees som god forvaltningsskikk på området. I denne undersøkelsen er revisjonskriteriene utledet fra:

- Lov av 22. Juni 2018 nr. 83 om kommuner og fylkeskommuner (kommuneloven).
- Lov av 18. Juni 2021 nr. 38 om behandling av personopplysninger (personopplysningsloven)
- Lov av 6. Juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven)
- Forskrift av 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Forskrift om kommunal beredskapsplikt av 22. august 2011 nr. 894 (forskrift om kommunal beredskapsplikt)
- Norsk sikkerhetsmyndighet (NSM) (2020): NSMs grunnprinsipper for IKT-sikkerhet versjon 2.0
- Digdir (2022): Internkontroll i praksis – Informasjonssikkerhet Versjon 2.0
- Datatilsynet (2022): Veiledning på Datatilsynets nettsider: datatilsynet.no.
- KS og KPMG (2022): Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet - Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus

Lov om kommuner og fylkeskommuner (Kommuneloven) sier i § 25-1 at «Kommuner og fylkeskommuner skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Ved internkontroll etter denne paragrafen skal kommunedirektøren:

a) utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering
b) ha nødvendige rutiner og prosedyrer
c) avdekke og følge opp avvik og risiko for avvik
d) dokumentere internkontrollen i den formen og det omfanget som er nødvendig
e) evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Det er kommunedirektøren som har det øverste ansvaret for at kravene i informasjonssikkerheten etterleves i hele kommunen jf. kommuneloven § 13-1.

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) sier i § 15 at forvaltningsorganet (her kommunen) skal ha en internkontroll på informasjonssikkerhetsområdet. Kommunen skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for kommunens internkontroll (styring og kontroll) på sikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks. Omfang og innretning på internkontrollen skal være tilpasset risiko.

eForvaltningsforskriften gir en rekke krav om prosedyrer knyttet til informasjonssikkerheten jf. bokstav a til h i § 15 i forskriften. Ifølge forskriftens § 15 skal forvaltningsorganet 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. Det er Digdir som gir anbefalinger på området.

Lov om behandling av personopplysninger (Personopplysningsloven), hvor personvernforordningen (GDPR) er innlemmet, regulerer behandling av personopplysninger. Denne stiller også krav til internkontroll på informasjonssikkerhetsområdet. Personopplysningsloven sier i Artikkel 32 i personvernforordningen at kommunen skal «[…] gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen […]».

I artikkel 24 i personvernforordningen som er innlemmet i personopplysningsloven er det beskrevet at:

> Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

I henhold til Datatilsynets veiledning (2022) innebærer personvernforordningen at kommunen skal ha nødvendige rutiner og prosedyrer for å sikre tilstrekkelig internkontroll på informasjonssikkerhetsområdet. Dette innebærer blant annet sjekklister for krav på informasjonssikkerhetsområdet. Kommunen skal også gjennomføre risikovurderinger for å kartlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd, og informasjonssikkerhetsarbeidet skal baseres på klar fordeling av roller og ansvar som skal være dokumentert. Organisering av sikkerhetsarbeidet skal beskrives. Kommunen skal kartlegge sine informasjonsverdier, herunder utarbeide oversikter over personopplysninger som behandles i virksomhetens IKT-systemer.

I artikkel 28, i personvernforordningen, som er innlemmet i personopplysningsloven, finner man kravene til innholdet i en databehandleravtale. En databehandleravtale må beskrive selve behandlingen, den behandlingsansvarliges plikter og rettigheter, samt databehandlerens forpliktelser. Avtalen skal beskrive dette på en klar og tydelig måte slik at det er klare rammer for hva databehandleren kan gjøre med personopplysningene.

I artikkel 33, i personvernforordningen, som er innlemmet i personopplysningsloven, er det beskrevet regler om melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten dersom det er sannsynlig at bruddet vil ha negativ betydning for den registrerte. Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet som i Norge er Datatilsynet.

Lov om nasjonal sikkerhet (Sikkerhetsloven) med tilhørende forskrifter stiller krav til sikkerhetsstyring og forsvarlig sikkerhetsnivå for skjermingsverdige verdier, herunder blant annet krav i kapittel 4 om forebyggende sikkerhetsarbeid. Ifølge lovens § 4-1 har virksomhetens leder ansvaret for det forebyggende sikkerhetsarbeidet og arbeidet skal være en del av virksomhetens styringssystem. Sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres. Ifølge lovens § 4-2 skal virksomheten regelmessig gjennomføre vurdering av risiko. Vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak.

Digdir (2022) angir at sikkerhetsnivå kan være et definert sett av sikkerhetstiltak, som skal dokumenteres. Eksempler på forskjellige sikkerhetstiltak for å redusere risikoen for sikkerhetsbrudd er:

- organisatoriske tiltak (eksempelvis roller og ansvar, retningslinjer, prosedyrer og rutiner)
- menneskelige tiltak (kompetanse og kultur)
- tekniske tiltak (eksempelvis skap, dører, rom, bygninger, IKT-løsninger som tofaktorautentisering

Digdir (2022) anbefaler og oppfordrer virksomheter, herunder kommuner, til å jobbe kontinuerlig med sikkerhetsvurderinger, sikkerhetsopplæring og sikkerhetskultur, for å være best mulig forberedt hvis et angrep kommer:

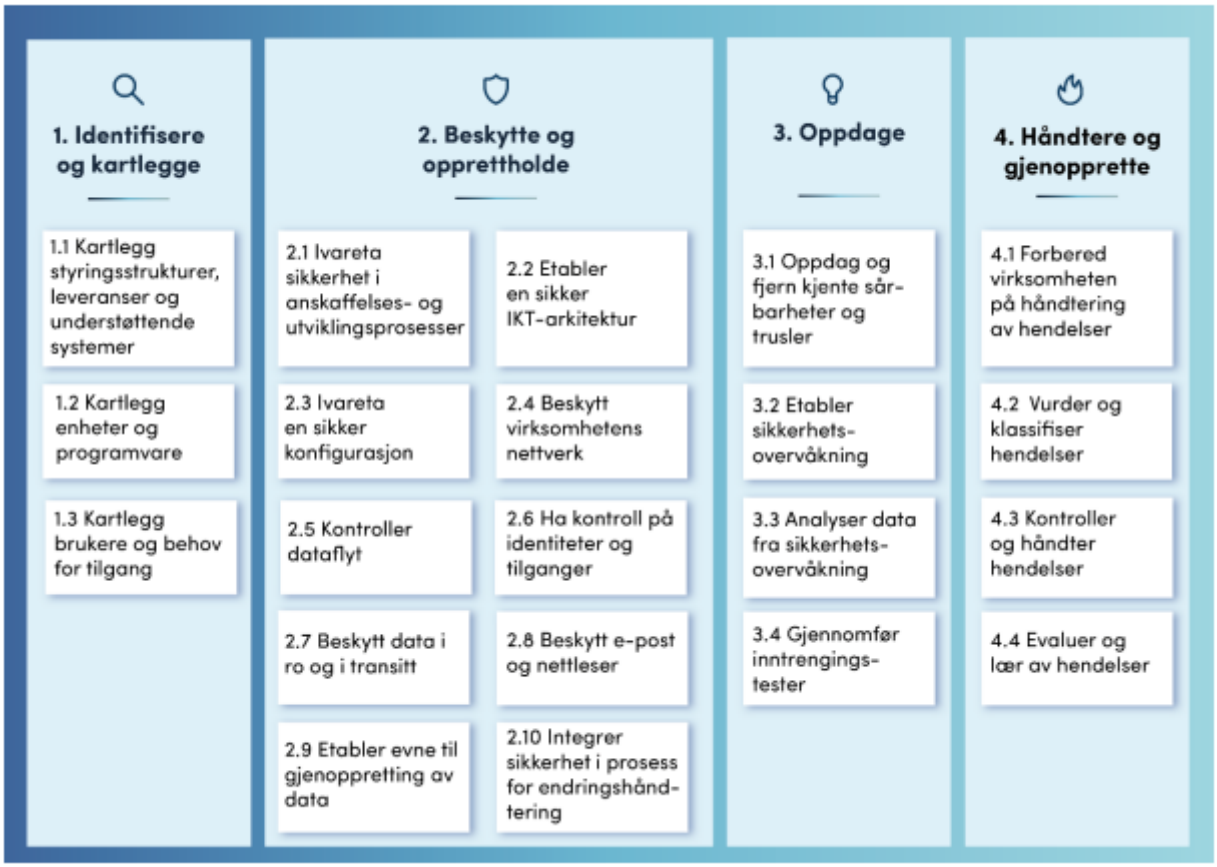
- Virksomhetene bør sette seg inn i Nasjonalt cybersikkerhetssenters råd mot skadevare
- Virksomheter som ikke har vurdert faren for denne type hendelser bør gjøre det, og etablere nødvendige tiltak
- Virksomheter som ikke har gjort slike vurderinger nylig bør sette seg inn i oppdatert informasjon, og se om de har behov for å oppdatere vurderingene og planene for håndtering av risiko
- Virksomheter bør vurdere om felles grunnleggende sikkerhetsnivå for alle virksomhetens oppgaver og tjenester bør oppdateres med tiltak mot slik skadevare.

Den amerikanske bransjeorganisasjonen Comptia har sett på årsaken til svikt i IT-sikkerheten. Som oftest var det menneskelige feil som lå bak. I en undersøkelse mente 84 prosent av deltagerne at menneskelige feil helt eller delvis var skyld i at sikkerhetshullene oppstod. Av organisasjonene i undersøkelsen hadde 58 prosent opplevd et sikkerhetshull som resulterte i tap av data eller avbrudd i driften i løpet av de siste seks månedene. Opplæring og bevisstgjøring blant alle ansatte er det viktigste tiltaket mot datainnbrudd og det er viktig med regelmessig repetisjon. (https://www.nettavisen.no/du-er-den-storste-sikkerhetsrisikoen/s/12-95-208398).

En rapport fra NorSIS sier at selv om det finnes teknologi som kan gjøre oss bedre beskyttet, kan denne bare beskytte til en viss grad. Til syvende og sist er det den enkelte ansattes kunnskap, som avgjør om en unngår lammende dataangrep (NorSIS-rapport Trusler og Trender (https://www.nsr-org.no/uploads/images/Digital_Trusler_Trender_2021.pdf).

NSMs grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. NSM har etablert fire grunnprinsipper for IKT-sikkerhet.

Figur 1 NSMs grunnprinsipper for IKT-sikkerhet



Punkt 1 dreier seg om å opparbeide og forvalte forståelse om virksomheten herunder styringsstrukturer, ledelsesprioriteringer, leveranser, IKT-systemer og brukere. Punkt 2 handler om å ivareta en forsvarlig sikring av IKT-systemet og opprettholde den sikre tilstanden over tid og ved endringer. Punkt 3 dreier seg om å oppdage og fjerne kjente sårbarheter og trusler og etablere sikkerhetsovervåking. Virksomheten bør teste elementer i egne forsvarsmekanismer (teknologi, prosesser og personell) ved å simulere målene og handlingene til en angriper. IKT-systemer er under konstant endring og utvikling og utfordres jevnlig av angrepsaktører. Virksomheter bør derfor jevnlig teste egen forsvarsevne for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Punkt fire omhandler prinsipper for å håndtere sikkerhetshendelser effektivt.

Forskrift om kommunal beredskapsplikt § 4 angir krav om utarbeidelse av overordnet beredskapsplan for kommunen som skal samordne og integrere øvrige beredskapsplaner i kommunen. Beredskapsplanen bør være utformet slik at de bidrar til å ivareta kravene til personvern og informasjonssikkerhet (KS og KPMG 2022, 9).

Vi utleder følgende kriterier til problemstilling 1:

Problemstilling 1	
Har kommunen etablert en tilfredsstillende overordnet styring og oppfølging av IKT-sikkerheten?	Kommunen skal ha: ➔ en beskrivelse av internkontrollsystemet på informasjonssikkerhetsområdet, herunder mål og strategi for IKT-sikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi) ➔ klare ansvars- og myndighetsforhold for kommunens IKT-sikkerhetsarbeid ➔ tilstrekkelige kompetansetiltak for å ivareta kommunens sikkerhetsbehov ➔ risikovurderinger av IKT-sikkerheten med tiltak ➔ oversikt over personopplysninger i sine IKT-systemer og kartlegge informasjonsverdier ➔ avdekking og oppfølging av hendelser med tiltaksplan knyttet til IKT-sikkerhet ➔ evaluering og evt. forbedring av skriftlige prosedyrer og andre tiltak for internkontroll. ➔ beredskapsplan ved sikkerhetsbrudd ➔ rutiner for meldinger til Datatilsynet ved avvik på informasjonssikkerhetsområdet ➔ databehandleravtaler med eksterne leverandører som behandler personopplysninger

Vi utleder følgende kriterium til problemstilling 2:

Problemstilling 2	
Er kommunen tilstrekkelig sikret mot innbrudd i kommunens interne nettverk via kommunens internetteksponerte tjenester?	➔ Kommunen bør ha rutine for å gjennomføre inntrengningstester jevnlig. ➔ Kommunen skal være sikret fra eventuelle innbrudd i kommunens interne nettverk via kommunens internetteksponerte tjenester.

4 STYRING OG OPPFØLGING AV IKT-SIKKERHETEN

I kapittelet legges følgende revisjonskriterier til grunn:

Problemstilling 1	
Har kommunen etablert en tilfredsstillende overordnet styring og oppfølging av IKT-sikkerheten?	Kommunen skal ha: ➔ en beskrivelse av internkontrollsystemet på informasjonssikkerhetsområdet, herunder mål og strategi for IKT-sikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi) ➔ klare ansvars- og myndighetsforhold for kommunens IKT-sikkerhetsarbeid ➔ tilstrekkelige kompetansetiltak for å ivareta kommunens sikkerhetsbehov ➔ risikovurderinger av IKT-sikkerheten med tiltak ➔ oversikt over personopplysninger i sine IKT-systemer og kartlegge informasjonsverdier ➔ avdekking og oppfølging av hendelser med tiltaksplan knyttet til IKT-sikkerhet ➔ evaluering og evt. forbedring av skriftlige prosedyrer og andre tiltak for internkontroll. ➔ beredskapsplan ved sikkerhetsbrudd ➔ rutiner for meldinger til Datatilsynet ved avvik på informasjonssikkerhetsområdet ➔ databehandleravtaler med eksterne leverandører som behandler personopplysninger

4.1 Dokumentasjon av internkontrollen

4.1.1 System for informasjonssikkerhet

Kommuneloven §25-1 a) sier at «kommuner og fylkeskommuner skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges». I denne rapporten fokuserer vi på internkontroll knyttet til informasjonssikkerhet.

Rælingen kommune har utarbeidet et internkontrollsystem for informasjonssikkerhet. Dette er beskrevet i dokumentet «System for informasjonssikkerhet» – datert 16.10.2019 og er signert av sikkerhetsansvarlig. Dokumentet er utarbeidet som et oppslagsverk der ulike grupper av brukere finner beskrivelser av hvordan de skal sikre kommunens informasjonsressurser best mulig.

Styrende del av «systemet» i dokumentet er godkjent av kommunedirektøren og inneholder den øverste ledelsens overordnede retningslinjer for arbeidet med informasjonssikkerhet. Rutinen knyttet

til ledelsens gjennomgang av informasjonssikkerhet sier at dokumentet skal gjennomgås og revideres årlig.

Ledelsen har hatt årlige gjennomganger av dokumentet og revisjonen får opplyst at deler av dokumentet er oppdatert etter 16.10.2019. Endringene/revidert utgave er imidlertid ikke loggført (intervju 8.8.2022). Revisjonen har i etterkant fått oversendt dokumentasjon som viser at siste revisjon av dokumentet er 3.9.2021 (Rælingen kommune 2022c).

Revisjonen har videre fått oversendt dokumentasjon av ledelsens årlige gjennomgang av systemet for informasjonssikkerhet. En Power-Pointpresentasjon med tittel «Årsrapportering informasjonssikkerhet» viser at ledelsen har gjennomgått:

- lover og regler om internkontroll på informasjonssikkerhetsområdet,
- formål med ledelsens årlige gjennomgang av informasjonssikkerheten,
- organisering av informasjonssikkerheten,
- kort om overordnede dokumenter om informasjonssikkerhet og om gjennomførte aktiviteter siste år i stikkords form. Eksempelvis presenteres punkter som:
    - avklare status på internkontrollarbeidet innen informasjonssikkerhet
    - avklare status på områder og tjenester der ledelsen er spesielt opptatt av informasjonssikkerhet

Rapporteringen eller presentasjonen gir imidlertid lite informasjon om resultatene eller innholdet i hva som er gjort i løpet av siste året og ingenting om hva som er besluttet. Formålet med gjennomgangen er bl.a. å “Reagere og følge opp der det er nødvendig” (Rælingen kommune 2020a).

«System for informasjonssikkerhet» beskriver også at det gjennomføres ROS-analyser, årlig kartlegging av enheter i kommunen samt stedlige og tekniske kontroller i gjennomgangen av internkontrollen (Rælingen kommune 2019a)

Digitaliseringsavdeling har et fagsystem som heter Digiorden. Det brukes primært til å ha oversikt over virksomhetsarkitektur, herunder fagsystemer, systemansvarlige, tilknyttede felleskomponenter og integrasjoner. Databehandleravtaler dokumenteres i sak-/ arkivsystemet (Elements). Behandlingsprotokoller og vurdering av personvernkonsekvenser, også kalt data protection impact assessment (DPIA), dokumenteres i Draftit[4]. ØIKT bruker Compilo til å dokumentere rutiner, instrukser og retningslinjer, samt gjennomføre risiko- og sårbarhetsanalyser (intervju 8.8.2022).

4.1.2 Årlig internkontrollkartlegging av enhetene i kommunen

Revisjonen har mottatt dokumentasjon som viser at det gjennomføres årlige kartlegging av de ulike enhetene i kommunen (Rælingen kommune 2020a og 2021g).

[4] System som forenkler og digitaliserer etterlevelse av GDPR i offentlig og privat sektor.

I kartleggingen etterspørres det informasjon om ulike forhold knyttet til internkontroll med informasjonssikkerhet og personvern (Rælingen kommune 2019a). Kartleggingen viser andel som vurderes å være på plass/ikke være på plass på informasjonssikkerhet og personvern i de ulike enhetene i kommunen, blant annet:

- om enheten har gjennomført og dokumentert risiko og sårbarhetsanalyser i løpet av 2020 og 2021 der informasjonssikkerhet og personvern blir vurdert
- om enheten etter leders vurdering har nødvendig kunnskap om informasjonssikkerhet og personvern
- liste over hva som er gjennomført av opplæringstiltak overfor ansatte
- leders vurdering av om de opplever at medarbeidere sier ifra til leder dersom de selv eller andre medarbeiderne ikke følger nedskrevne rutiner, utdaterte rutiner eller annet som kan utgjøre en risiko for virksomheten
- om lederes vurdering av ivaretakelsen av informasjonssikkerhet og personvern i egen enhet

Det er utarbeidet oppsummering av kartleggingene og en tiltaksliste på de punktene som har størst mangler i forhold til kravene på området. Revisjonen har fått oversendt oppsummeringene på kartleggingen i 2020 og i 2021 med tiltaksliste (Rælingen kommune 2020a og 2021g).

Oppsummeringene viser at det varierer i hvilken grad enhetslederne mener informasjonssikkerhet og personvern blir godt nok ivaretatt i enheten. Noen av enhetslederne mener det er vanskelig å få ansatte til å etterleve dette i praksis (Rælingen kommune 2020a og 2021g). Nyansatte skriver under på en avtale knyttet til informasjonssikkerhet og personvern (intervju 8.8.2022).

4.1.3 Øyern IKT og internkontroll

«System for informasjonssikkerhet» viser at Øyern IKT (ØIKT) har ansvar for alle tjenestemaskiner og alt infrastruktur-/nettverksutstyr i kommunen og det oppgis i «System for informasjonssikkerhet» at ØIKT utformer krav, retningslinjer og rutiner for driften av disse. ØIKT skal ha retningslinjer og rutiner som en del av sin dokumentasjon. Dette betyr bl.a. at ØIKT må konsulteres i enhver anskaffelse som involverer IT tekniske løsninger (Rælingen kommune 2019a).

ØIKT oppgir at det kommer an på området om det utarbeides skriftlige rutiner. ØIKT oppgir at for mye av den tekniske driften er det ikke mulig å ha detaljerte skriftlige rutiner for arbeidet. ØIKT har imidlertid intranett hvor all deres virksomhet er dokumentert. Internkontrollsystemet til ØIKT er beskrevet i fagsystemet Compilo. ØIKT kan imidlertid ikke dokumentere at det gjennomføres interne gjennomganger av internkontrollsystemet i virksomheten (intervju 8.8.2022).

Som del av kommunens dokumentasjon på internkontrollsystemet på informasjonssikkerhet har revisjonen fått oversendt et dokument som beskriver organisasjonen og hvem som jobber med hva i ØIKT *(*Rælingen kommune 2021i*)* Dette er ikke en beskrivelse av internkontrollsystemet for ØIKT, men en organisasjonsbeskrivelse som «skal gi en samlet oversikt over hvordan enheten er organisert og hvordan den skal fungere».

4.1.4 Stedlige og tekniske kontroller

I internkontrolldokumentet til Rælingen kommune stilles også krav om gjennomføring av stedlige og tekniske kontroller. Utøver av behandleransvaret, personvernombudet og sikkerhetsansvarlig skal samarbeide om disse. De skal kontrollere etterlevelse av rutiner for personvern og informasjonssikkerhet. Dette inkluderer gjennomgang av IT-systemer, arbeidsmåter og tiltak fra tidligere ROS-analyser, samt oppfølging av eventuelle utfordringer avdekket i den årlige gjennomgangen av internkontrollen. ØIKT gjør i tillegg flere ulike typer tekniske grep og kontroller, for å supplere de ovenstående punktene (Rælingen kommune 2019a). Sikkerhetsansvarlig i kommunen oppgir at så vidt denne kjenner til er det ikke gjennomført stedlige eller tekniske kontroller som en del av gjennomgang av internkontrollen i 2022. Leder for ØIKT oppgir at de ikke har noe «regime» for å utføre spesifikke tekniske kontroller utover egen løpende involvering i tekniske løsninger (e-post fra Rælingen kommune 22.08.22).

4.1.5 Mål og strategi for IKT-sikkerhet i virksomheten

Forskrift om elektronisk kommunikasjon med og i forvaltningen sier i § 15 at kommunen skal ha beskrevet mål og strategi for informasjonssikkerheten i virksomheten. Dette skal danne grunnlaget for kommunens internkontroll på sikkerhetsområdet.

Mål og strategi for sikkerhetsarbeidet i kommunen er beskrevet i «System for informasjonssikkerhet» (Rælingen kommune 2019a).

Sikkerhetsmålet er:

> å sikre rett nivå på sikkerhet, stabilitet, tilgjengelighet og kvalitet av IT-tjenester og IT-ressurser slik at primærvirksomheten og støttetjenestene kan utføres mest mulig problem- og avbruddsfritt. Samtidig skal personopplysninger være tilstrekkelig godt ivaretatt, slik at dataene har god tilgjengelighet, konfidensialitet og integritet. I tillegg skal dette arbeidet balanseres mot hensynet til innbyggere og ansattes personvern.

Overordnet sikkerhetsstrategi omfatter strategi knyttet til organisering rundt informasjonssikkerhets-arbeidet, krav til internkontroll og sikkerhetsarbeid og krav til ansatte (Rælingen kommune 2019a).

ØIKT har flere dokumenter knyttet til sikkerhetsmål- og strategi. Dokumentene fra ØIKT signaliserer at det er behov for endringer i kommunens overordnede strategi på informasjons- og personvernområdet. ØIKT peker blant annet på at det er for lite fokus på beredskap og et økt behov for ressurser og kompetanse (Dokumenter fra ØIKT som omhandler sikkerhetsstrategi). Digitaliseringsavdelingen oppgir at de ikke har fått innspill til overordnet sikkerhetsmål og sikkerhetsstrategi fra ØIKT i forhold til overordnet strategidokument. I det praktiske sikkerhetsarbeidet samt i budsjett- og ressursdiskusjoner med ledelsen i kommunen er imidlertid er innspillene tatt opp (Intervju 8.8.22).

4.2 Ansvars- og myndighetsforhold

I henhold til Datatilsynets veiledning om personvernforordningen, skal informasjonssikkerhetsarbeidet baseres på klar fordeling av roller og ansvar som skal være dokumentert. Organisering av sikkerhetsarbeidet skal beskrives.

«System for informasjonssikkerhet» beskriver at kommunedirektøren er den formelt ansvarlige for sikkerhetsarbeidet, men at mye av ansvaret er delegert til digitaliseringsavdelingen og sikkerhetsansvarlig i denne avdelingen. Dette dreier seg om den daglige oppfølgingen av informasjonssikkerhet, herunder opplæring, databehandleravtaler, ROS og avvikshåndtering (intervju 8.8.22). En del er også delegert til ØIKT v/daglig leder, personvernombud, sikkerhetsrådet, enhetsledere/avdelingsleder og systemeier (Rælingen kommune 2019a). Deres roller beskrives nærmere nedenfor:

- **ØIKT** er et vertskommunesamarbeid mellom Enebakk og Rælingen kommune med ansvaret for IKT drift og har de ansatte i kommunen som sine kunder. Medarbeiderne er ansatt i Rælingen kommune. De sørger for at kommunenes ansatte alltid har tilgjengelige IKT-verktøy for oppgavene som skal løses. ØIKT ved daglig leder rapporterer til kommunedirektøren. ØIKT har det tekniske ansvaret for informasjonssikkerhet (intervju 8.8.2022). ØIKT skal blant annet godkjenne tilkopling av utstyr knyttet til aktuelt område i hvert enkelt tilfelle.
- **Personvernombudet** har ansvar for å informere og gi råd om de krav kommunen har etter personvernlovgivningen til behandlingsansvarlig eller databehandleren, og til ansatte som utfører behandling av personopplysninger.
- **Sikkerhetsrådets** formål er å sikre at sikkerhetsarbeidet og personvernet blir en samordnet prosess som ivaretas på en systematisk og dokumentert måte. Sikkerhetsrådet er opprettet for å sikre samarbeid mellom enhetene. Rådet er ikke et besluttende organ, men et diskusjonsfora for deling og læring (intervju 08.08.22) Det er åtte medlemmer i rådet:leder av sikkerhetsrådet, leder digitaliseringsavdelingen, leder ØIKT, beredskapskoordinator, organisasjonssjef, eiendomssjef, arkivleder og personvernombud (Rælingen kommune 2021c).
- **Enhets- eller avdelingslederne** har blant annet ansvar for å sikre internkontroll på informasjonssikkerhetsområdet og å sørge for at egne medarbeidere har kunnskap og er bevist på informasjonssikkerheten.
- **Systemeier** er ansvarlig for den daglige informasjonssikkerheten knyttet til medarbeideres bruk av aktuelt system. Systemeier skal også håndtere systemet og systemets sikkerhet under hele dets livsløp, samt gjennomføre ROS-analyser og utarbeide og påse gjennomføring av tiltaksplan.
- **Medarbeidere i kommunen** har ansvar for å etterleve «Retningslinjer for bruk av IKT i Rælingen kommune», og gjeldende prosedyrer i «system for informasjonssikkerhet». Medarbeidere har ansvar for å melde avvik som angår informasjonssikkerhet i kommunens kvalitetssystem Compilo til nærmeste leder (Rælingen kommune 2019a).

Revisjonen har fått oversendt dokumenter med funksjonsbeskrivelse av sikkerhetsrådet (Funksjonsbeskrivelse sikkerhetsrådet, sist revidert april 2021) og en organisasjons- og rolle/ansvarsbeskrivelse av ØIKT (Rælingen kommune 2021j).

4.3 Kompetansetiltak

Digdir peker på at det bør iverksettes sikkerhetstiltak, bl.a. knyttet til å sikre nødvendig kompetanse, for å redusere risikoen for sikkerhetsbrudd (Digidir 2022).

«System for informasjonssikkerhet» beskriver at medlemmene i sikkerhetsrådet har som oppgave å utvikle kompetanse hos ledere, som igjen viderefører kompetansen til medarbeidere (Rælingen kommune 2019a).

Revisjonen har fått oversendt dokumentasjon på opplæringsmateriell knyttet til informasjonssikkerhet og personvern. Dokumentasjonen inneholder:

- Opplæring av enhets- og avdelingsledere om GDPR (General Data Protection Regulation) og informasjonssikkerhet (Rælingen kommune 2021e)
- Opplæring av nyansatte om informasjonssikkerhet og GDPR (Rælingen kommune 2021f)
- Prosedyre for opplæring av ledere og medarbeidere i informasjonssikkerhet (Rælingen kommune udatert g)

Digitaliseringsavdelingen oppgir at de to ganger i året har gjennomgang med nyansatte om informasjonssikkerhet og GDPR, sammen med personvernombudet, og hva dette har å si for det arbeidet de skal gjøre i kommunen (intervju 8.8.2022). På introdagen for nyansatte fokuseres det blant annet på hva den enkelte ansatte har ansvar for når det gjelder etterlevelsen av retningslinjene i «System for informasjonssikkerhet». Ledere får opplæring tilpasset hva de har av ansvar (Rælingen kommune 2019a).

I sikkerhetsmåneden (oktober) får de ansatte dessuten årlig gjennomgå et e-læringsopplegg (intervju 8.8.2022).

Sikkerhetsansvarlig, leder av digitaliseringsavdelingen, teknisk ansvarlig og leder ved ØIKT med flere, har en del opplæring og kompetansehevende tiltak i forbindelse med sin rolle som spisskompetansepersonale. De oppgir imidlertid ønske om mer kompetanseheving (intervju 8.8.2022).

En gang i året sender sikkerhetsansvarlig en spørreundersøkelse til enhetslederne. Resultatet gir oversikt over behov for opplæring på enhetene. Kartleggingen gir sikkerhetsansvarlig og personvernombudet bedre utgangspunkt for å bistå enhetene med opplæring og informasjon. Resultatene følges opp med tiltaksliste og tas med som innspill til ledelsens gjennomgang (Rælingen kommune 2019a). Både i 2020 og i 2021 har kartleggingen ført til tiltak (Rælingen kommune 2020a og 2021g).

I kartleggingen til enhetslederne rapporterer flere av enhetene at de ikke har nødvendig kunnskap om informasjonssikkerhet og personvern. I 2020 oppgir 28 prosent av lederne at deres enhet ikke har nødvendig kunnskap om informasjonssikkerhet og personvern. I 2021 er det 36 prosent av enhetslederne som oppgir dette (Rælingen kommune 2020a og 2021g).

I kartleggingen har lederne også fylt ut lister over gjennomførte opplæringstiltak. Det er stor variasjon i hva lederne oppgir av opplæringstiltak i sin enhet; fra ingen opplæring til at alle ansatte har gjennomført kurs i informasjonssikkerhet (Rælingen kommune 2020a og 2021g). Hver enkelt enhetsleder er delegert ansvar for opplæring på informasjonssikkerhetsområdet (intervju 8.8.2022). Digitaliseringsavdelingen oppgir at mange av lederne i enhetene ikke er så bevisst på dette ansvaret. Det er stort sprik i kompetanse og engasjement knyttet til informasjonssikkerhet hos ledere og

ansatte. Enhetene fokuserer på fag mens informasjonssikkerhet ses på som en «biting». Enhetene stiller som regel på opplæring når de blir innkalt, men det er ikke alltid prioritert lokalt (intervju 8.8.2022).

Digitaliseringsavdelingen oppgir at det tidligere fantes flere obligatoriske kurspakker eller «Datakort». En slik type opplæringspakke kunne være aktuelt for kommunen for å forbedre opplæringen på informasjonssikkerhetsområdet. Rælingen har ikke hatt slike kurspakker tidligere, verken generelt på IKT eller informasjonssikkerhet. Å få ansatte med på opplæring knyttet til informasjonssikkerhet en utfordring. De ansatte er den største sikkerhetsrisikoen, slik leder for digitaliseringsavdelingen ser det (intervju 8.8.2022).

Digitaliseringsavdeling har bedt enhetslederne ta kontakt om hva de ønsker av bistand. Avdelingen har besøkt flere enheter som har meldt om behov (intervju 8.8.2022).

ØIKT sender alle ansatte e-post om aktuelle sikkerhetstrusler når de dukker opp (intervju 8.8.2022).

ØIKT har signalisert i flere dokumenter som omhandler sikkerhetsstrategi at de også selv har behov for økt spesialkompetanse for å ivareta sikkerheten. (Rælingen kommune 2019b og 2022 a). Dette handler om mer teknisk personale, behov for økt fokus på beredskap og mer ressurser til IKT støtte.

4.4 Risikovurderinger av IKT-sikkerheten med tiltak

Ifølge kommuneloven paragraf 25-1 skal kommunedirektøren avdekke risiko for avvik, gjennom å påse at det gjennomføres risikovurderinger for å kartlegge sannsynligheten for og konsekvensene av sikkerhetsbrudd.

4.4.1 Overordnet risikoanalyse og ROS-analyse av systemene

Det er utarbeidet overordnet risikoanalyse med tiltaksplan av informasjonssikkerheten i Rælingen kommune i 2020 og 2021 (Rælingen kommune 2020b og 2021h).

I risikoanalysen er det identifisert en rekke risikoer, gjort vurdering av sannsynlighet og konsekvens og laget tiltaksplan (Overordnet risikoanalyse pr. 31.12.2020). I tiltaksplan for 2020 står en rekke tiltak. De fleste av disse er borte i tiltaksplan for 2021. Tre tiltak er overført til tiltaksplanen for 2021. Disse er ikke gjennomført i 2020 og er derfor overført. (Rælingen kommune 2020b og 2021h).

Punktene i risikoanalysen er basert på innmeldte avvik gjennom det siste året, identifiserte trusler, sårbarheter og risikoanalyser fra enhetsledere, samt erfaring og potensielle trusler og sårbarheter definert av sikkerhetsansvarlig og personvernombudet (Rælingen kommune 2020b og 2021h).

I e-post den 22.8.22 opplyser sikkerhetsansvarlig i Rælingen kommune at kommunen har etablert en systemorganisasjon rundt drift og forvaltning av IKT-systemer. For hvert IKT-system er det en systemeier og en systemansvarlig. Dette er viktige roller for drift og forvaltning av kommunens IKT-systemene. Alle systemansvarlige gjennomførte i 2021 ROS-analyse for det systemet de har ansvar for.

4.4.2 Risikoanalyse hos enhetene i kommunen

I internkontrollkartleggingen til enhetene i kommunen spørres det om enheten har gjennomført ROS-analyse der informasjonssikkerhet og personvern er blitt vurdert. Det kommer fram i kartleggingen både i 2020 og 2021 at en relativt stor andel av enhetene ikke har gjennomført slike ROS-analyser. Kartleggingen viser at 48 prosent av enhetene i 2020 og 58 prosent i 2021 oppgir at de ikke har gjennomført og dokumentert risiko- og sårbarhetsanalyser der informasjonssikkerhet og personvern har blitt vurdert (Rælingen kommune 2020a og 2021g).

I administrasjonens tilbakemelding til faktagrunnlaget i denne rapporten, sendt revisjonen 25.10.22, presiseres det at risikoanalysene hos enhetene er knyttet til ansattes etterlevelse av IKT-sikkerhet, og ikke IKT-sikkerhet i hvert enkelt IKT-system.

4.4.3 Risikoanalyse hos ØIKT

Revisjonen har fått oversendt Risiko og sårbarhetsanalyse (ROS) på sikkerhetsområdet ved ØIKT med påfølgende tiltaksplan for 2021 (Rælingen kommune 2021k)

Det er utarbeidet flere dokument fra ØIKT der risiko vurderes. Disse viser blant annet:

- Utfordringer på IKT-området (Rælingen kommune 2021i)
- At ØIKTs virksomhet i forhold til NSMs grunnprinsipper bare delvis er oppfylt (Rælingen kommune 2021d).
- Innspill til overordnet ROS datert 19.2.21 hvor det angis flere risikoer (Rælingen kommune 2021i).

I Dokument «Overordnet ROS – IKT sikkerhets trussel v2» sendt fra ØIKT er gis det innspill til overordnet ROS. Leder ved ØIKT oppgir at risikoene fremst handler om ressurser og innspill til budsjett for teknisk i ØIKT. Dette spilles inn til kommunen på budsjettområdet og i hovedsak ikke til overordnet ROS til Digitaliseringsavdeling. ØIKT utarbeidet også lister over hva de mener burde forbedres og gjøres noe med, som også er innspill til budsjett (intervju 8.8.2022).

Digitaliseringsavdelingen oppgir at det kan være momenter knyttet til brukerstyring og tilgang til PC som bør tas inn i årlig overordnet ROS-analyse (intervju 8.8.2022).

4.5 Oversikt over personopplysninger og informasjonsverdier

I henhold til Datatilsynets veiledning (2022) skal kommunen kartlegge sine informasjonsverdier, herunder utarbeide oversikter over personopplysninger i virksomhetens IKT-systemer.

Informasjonssikkerhet dreier seg om å håndtere risiko for kommunens informasjonsverdier og personopplysninger – om å sikre konfidensialitet, integritet og tilgjengelighet på informasjon som trenger slik sikring.

Digitaliseringsavdelingen oppgir i intervju at deres fagsystem (Digiorden), samt ØIKT sitt intranett, per dags dato er de viktigste løsninger for sikre oversikt over informasjonsverdier i kommunen. I sin tilbakemelding til faktagrunnlaget, sendt revisjonen 25.10.22, presiserer administrasjonen at kommunen har oversikt over alle IKT-systemene i verktøyet Digiorden. Digiorden viser oversikt over

sammenheng og dataflyt mellom de ulike systemene. Digitaliseringsavdelingen oppgir at de har 87 systemer i sitt fagsystem (intervju 8.8.2022). Revisjonen har fått oversendt en oversikt over disse. Oversikten angir beskrivelse av system, om versjon er i skyløsning eller lokalt, samt produsent og systemansvarlig, men oversikten viser ikke noe nærmere om personopplysninger behandles i systemene (Rælingen kommune 2022c). I tilbakemeldingen til faktagrunnlaget peker administrasjonen på at kommunen i tillegg til Digiorden har verktøyet Draftit. I dette systemet har kommunen oversikt over alle personopplysninger. Digiorden og Draftit sørger ifølge administrasjonen for at kommunen har god oversikt over personopplysninger og hvordan disse personopplysningene håndteres i kommunens tjenesteutøvelse.

Digitaliseringsavdelingen oppgir at hvert nytt system blir vurdert i forhold til kritikalitet i verktøyet Digiorden (kritiske verdier/ behov for å sikre konfidensialitet, integritet og tilgjengelighet). Ved nyanskaffelser stilles det krav til tilstrekkelig informasjonssikkerhet, samt at det gjennomføres bruker- og funksjonalitetstesting, før løsningene settes i drift. Det gjennomføres også test i samarbeid med leverandører før overlevering fra prosjekt til drift hos leverandør. Enhetene har ikke lov til å installere systemer selv. Installering må avklares med digitaliseringsavdeling eller ØIKT (intervju 8.8.2022).

Digitaliseringsavdelingen oppgir at de mangler en virksomhetsarkitekt som kan jobbe overordnet med å sikre oversikt over informasjonsverdier som kan skape helhetlig systematikk på dette området (intervju 8.8.2022).

4.6 Avdekking og oppfølging av hendelser med tiltaksplan

Ifølge paragraf 25-1 i kommuneloven skal kommunedirektøren avdekke og følge opp avvik knyttet til informasjonssikkerheten.

«System for informasjonssikkerhet» omhandler også håndtering av hendelser og avvik, og beskriver definisjon, eksempler, rutiner og ansvar for håndtering av avvik (Rælingen kommune 2019a). I tillegg har kommunen rutine for avvikshåndtering og GDPR[5], som skal sikre at avvik knyttet til personvern og informasjonssikkerhet blir fulgt opp (Rælingen kommune udatert).

Kommunen sikrer dokumentasjon på avvik/hendelser og oppfølging av disse gjennom overordnet ROS-analyse med tiltaksliste, oppfølging av avvikshåndtering og gjennom internkontrollkartleggingen til enhetene (intervju 8.8.2022).

Revisjonen har mottatt dokumentasjon som viser kommunens praksis knyttet til avviksmeldinger og hendelser i kommunen og oppfølging av disse (Rælingen kommune 2021b).

I internkontrollkartleggingen som gjennomføres overfor enhetene i kommunen er det kartlagt om:

- enhetene har mottatt avvik knyttet til tema informasjonssikkerhet og personvern og
- om medarbeidere i egen enhet har rapportert sikkerhetshendelser eller brudd på personvernet i henholdsvis 2020 og 2021.

[5] General Data Protection Regulation

Internkontrollkartleggingen viser at det er få enheter som melder avvik. I 2020 er det 8 av 29 enheter som har meldt avvik knyttet til tema informasjonssikkerhet og personvern, mens for 2021 gjelder dette 4 av 25 enheter (Rælingen kommune 2020a og 2021g).

Digitaliseringsavdelingen mener det er underrapportering av avvik på informasjonssikkerhet. Det er ikke kultur for å tenke avvik på informasjonssikkerhet. Det ligger generelt ikke i «ryggmargen» å melde inn avvik og det er derfor få som melder avvik. På pleie- og omsorgsområdet er det derimot kultur for å melde avvik og gi innspill til forbedringer. Der meldes det markant flere avvik også på informasjonssikkerhet. Digitaliseringsavdelingen oppgir at de i opplæring av ansatte og i e-læring, oppfordrer til å melde avvik (intervju 8.8.2022).

4.7 Evaluering av skriftlige prosedyrer og andre tiltak for internkontroll

Kommunedirektøren skal etter paragraf 25-1 i kommuneloven evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Digitaliseringsavdelingen oppgir at det ikke er gjennomført noen egen systematisk evaluering av arbeidet med informasjonssikkerhet. Kommunen oppgir at rutiner og retningslinjer for arbeidet med informasjonssikkerhet i Rælingen blir gjennomgått gjennom ledelsens overordnede gjennomgang av internkontrollsystemet, samt fortløpende ved behov. I tillegg har kommunen den årlige internkontrollkartleggingen som gjennomføres overfor enhetene i kommunen (intervju 8.8.2022).

4.8 Beredskapsplan ved sikkerhetsbrudd

Forskrift om kommunal beredskapsplikt § 4 angir krav om utarbeidelse av overordnet beredskapsplan for kommunen. Beredskapsplanen bør være utformet slik at den bidrar til å ivareta kravene til personvern og informasjonssikkerhet (KS og KPMG 2022, 9)

Kommunen har utarbeidet overordnet beredskapsplan for IKT samt at det er utarbeidet beredskapssystem ved ØIKT (Rælingen kommune udatert c og udatert d). ØIKT beredskapssystem beskriver overordnede prinsipper for håndtering av beredskap i ØIKT. IKT beredskapsplan omhandler organisering av IKT beredskap i Enebakk og Rælingen kommune. Ansvarlig for IKT beredskap er leder ved ØIKT. Beredskapsplanen angir ansvar og organisering, forebyggende tiltak og organisasjon for beredskap hvor blant annet prosess for kriseledelse angis. Det angis videre plan for trusselvurdering, beredskapsøvelser og forebyggende tiltak for å forhindre eller begrense effekter av en evt. katastrofe/hendelse. Planen angir også revisjon av beredskapsplan, rutiner og tiltak (Rælingen kommune udatert c).

4.9 Rutiner for melding til Datatilsynet

Ifølge artikkel 33, i personvernforordningen, skal den behandlingsansvarlige ved brudd på personopplysningssikkerheten, uten ugrunnet opphold og senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet som i Norge er Datatilsynet.

Kommunen har en skriftlig rutine for melding til Datatilsynet ved avvik på informasjonssikkerhet (Rutiner for varsling til Datatilsynet, udatert). Ifølge rutinen skal de ansatte melde om avvik i fagsystemet (Compilo). Personvernombud og sikkerhetsansvarlig har lesertilgang til alle avvik som gjelder GDPR. Personvernombud og sikkerhetsansvarlig blir varslet og har tilgang til avvik som er tagget med personvern/informasjonssikkerhet. Personvernombud, i samarbeid med innmelder, evt. leder av tjenesten, melder eventuelt avvik til Datatilsynet dersom konsekvensene av avviket har medført brudd på personvernet. Det er angitt krav til hva evt. varsling skal inneholde (Rælingen kommune udatert a).

Revisjonen har mottatt dokumentasjon på melding av avvik fra 2021 til datatilsynet med tiltak for å lukke avviket samt dokumentasjon på avslutning av sak fra Datatilsynets side (Rælingen kommune udatert b). I 2021 ble det rapportert 24 avvik og tre av disse[6] ble meldt til Datatilsynet. De tre avvikene er nå lukket av Datatilsynet (Rælingen kommune 2021a).

Internkontrollkartleggingen gjennomført overfor enhetene i kommunen, viser at ca. en fjerdedel av medarbeiderne har rapportert sikkerhetshendelser eller brudd på personvernet (Rælingen kommune 2020a).

4.10 Rutine for databehandleravtale med eksterne leverandører

Kommunen har dokumentasjon på prosedyre for databehandleravtale med eksterne leverandører som behandler personopplysninger (Rælingen kommune udatert i). Det skal opprettes avtale ved engasjement av databehandler som skal behandle personopplysninger. I prosedyrene er det nedfelt krav til databehandler og innhold i databehandleravtalen. Det foreligger mal for utarbeidelse av avtale (Mal for databehandleravtale – benytter mal fra www.anskaffelser.no, udatert).

Revisjonen har fått oversendt dokumentasjon på inngåtte databehandleravtaler med eksterne leverandører (Rælingen kommune udatert j).

4.11 Revisjonens konklusjon, vurdering og anbefalinger

God overordnet styring og oppfølging av IKT-sikkerheten er en forutsetning for å kunne oppdage svakheter i systemer, rette feil og gjøre systemene sikrere. Revisjonens konklusjon er at kommunen har fått på plass et godt grunnlag for å sikre styring og oppfølging av IKT-sikkerheten, men at det er arbeid som står igjen når det gjelder å følge opp og etterleve dette i praksis.

Revisjonen har i undersøkelsen lagt til grunn at det skal være en beskrivelse av internkontrollsystemet på informasjonssikkerhetsområdet, med mål og strategi for IKT-sikkerhet. Undersøkelsen viser at kommunen har beskrevet et system for internkontroll på informasjonssikkerhetsområdet i et eget dokument. Dette dokumentet inneholder retningslinjer og rutiner for overordnet ledelses oppfølging på området, blant annet skal systemet gjennomgås årlig. Dokumentet beskriver videre at det skal

[6] For disse tre avvikene var det sannsynlig at bruddet vil ha negativ betydning for den registrerte.

gjennomføres årlige internkontrollkartlegginger av enhetene i kommunen, i tillegg skal det gjennomføres stedlige og tekniske kontroller som skal sikre etterlevelse av rutiner for personvern og informasjonssikkerhet. Også mål og strategier for IKT-sikkerhet i kommunen er beskrevet her.

Det er derfor revisjonens vurdering at kommunen har en god beskrivelse av internkontrollsystemet på informasjonssikkerhetsområdet, som legger grunnlag for god styring og oppfølging av IKT-sikkerheten i kommunen. I tillegg mener vi at den årlige gjennomgangen av systemet, med tilhørende internkontrollkartlegginger, ivaretar kravet om å evaluere og forbedre rutiner og andre tiltak for internkontroll på området. Revisjonen mener imidlertid at de konkrete forbedringene i systemet i større grad burde vært skriftliggjort og at nye versjoner av dokumentet burde være datert. Rapporteringen på ledelsens overordnede gjennomgang av informasjonssikkerheten gir lite informasjon om resultat og innhold i hva som er gjennomgått og ingenting om hva som er besluttet å følge opp.

Revisjonen mener videre at krav knyttet til å ha på plass en beredskapsplan ved sikkerhetsbrudd, rutiner for å melde fra om avvik til Datatilsynet og databehandleravtaler med eksterne leverandører er på plass i Rælingen kommune. Kommunen vurderes å ha en god og tilstrekkelig beskrivelse av mål og strategier for kommunens IKT-sikkerhetsarbeid.

Revisjonen har lagt til grunn at det skal være klare ansvars- og myndighetsforhold for kommunens IKT-sikkerhetsarbeid. Vi har mottatt flere dokumenter som beskriver ulike roller knyttet til dette arbeidet, og hvordan ansvar og myndighet er fordelt. Det oppgis imidlertid at mange av enhetslederne ikke er bevisste nok på ansvaret de er delegert knyttet til opplæring på informasjonssikkerhetsområdet.

I undersøkelsen er det videre lagt til grunn at det skal være tilstrekkelige kompetansetiltak for å ivareta kommunens sikkerhetsbehov. Undersøkelsen viser at det tilbys systematisk opplæring om IKT-sikkerhet i Rælingen kommune. Likevel oppgir rundt en tredjedel av enhetslederne i kommunen at det ikke er tilstrekkelig kunnskap om informasjonssikkerhet og personvern hos de ansatte, og flere oppgir at det ikke er gitt noen opplæring av de ansatte knyttet til dette. Revisjonen mener det er avgjørende å sikre god nok opplæring av alle ansatte for å ivareta IKT-sikkerheten i kommunen. Revisjonen vil også påpeke at det er viktig at kommunen har god spesialkompetanse på IKT. ØIKT har signalisert i flere dokumenter at det er behov for økt kompetanse i ØIKT.

Når det gjelder risikovurderinger av IKT-sikkerheten med tiltak, finner vi at slike risikovurderinger skjer på overordnet nivå i kommunen og i ØIKT, men at det er mangler på enhetsnivå. Kommunens egne kartlegginger viser at over halvparten av enhetene ikke har gjennomført risikovurderinger av ansattes etterlevelse av IKT-sikkerheten. Revisjonen mener det er viktig at risikovurderinger knyttet til IKT-sikkerhet skjer på alle nivåer i organisasjonen, blant annet for å sikre nok oppmerksomhet rundt IKT-sikkerhet og identifisere opplæringsbehov hos de ansatte. Revisjonen mener manglende gjennomføring av ROS-analyser medfører fare for sikkerhetsbrudd.

Videre er det lagt til grunn at kommunen skal ha oversikt over personopplysninger i sine IKT-systemer og kartlegge informasjonsverdier. Det er revisjonens vurdering at verktøyene DigiOrden og DaftIt som er tatt i bruk i kommunen bidrar til å sikre dette.

Det er et viktig internkontrollprinsipp å sikre at avvik meldes og følges opp, også på IKT-sikkerhetsområdet. Undersøkelsen viser at det meldes få avvik knyttet til informasjonssikkerhet og personvern. Det er etter revisjonens syn viktig å jobbe videre med å utvikle en kultur for å melde avvik, slik at feil og mangler innenfor IKT-sikkerheten kan utbedres. Som nevnt over har kommunen rutiner for å melde avvik knyttet til brudd på personopplysningssikkerheten til Datatilsynet. Mangelfull avviksmelding generelt knyttet til informasjonssikkerhet og personvern kan imidlertid føre til at avvik som skulle vært meldt til Datatilsynet ikke fanges opp, meldes inn og følges opp.

På bakgrunn av dette er revisjonens anbefalinger:

Kommunedirektøren bør sørge for

1. at alle ledere og ansatte gjennomfører systematisk opplæring for å sikre tilstrekkelig kompetanse og at ansvar for informasjonssikkerhet og personvern ivaretas på alle nivåer i organisasjonen.

2. at det gjennomføres risikovurderinger knyttet til IKT-sikkerhet på alle nivåer i organisasjonen.

3. at avvik knyttet til informasjonssikkerhet og personvern oppdages, meldes inn og følges opp.

5 INNBRUDD I INTERNE NETTVERK

I dette kapittelet legges følgende problemstilling med tilhørende revisjonskriterium til grunn:

Problemstilling 2	
Er det mulig å bryte seg inn i kommunens interne nettverk via kommunens internetteksponerte tjenester?	➔ Kommunen bør ha rutine for å gjennomføre inntrengningstester jevnlig. ➔ Kommunen skal være sikret fra eventuelle innbrudd i kommunens interne nettverk via kommunens internetteksponerte tjenester.

5.1 Rutine for å gjennomføre inntrengningstester jevnlig

Personopplysningsloven sier i Artikkel 32 i personvernforordningen at kommunen skal «[…] gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen […]». NSMs grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. NSM har etablert fire grunnprinsipper for IKT-sikkerhet. Et av punktene under tiltak for å oppdage risiko i informasjonssystemene er å gjennomføre jevnlig inntrengningstester.

Kommunen opplyser at det ikke er gjennomført noen eksterne inntrengningstester i Rælingen kommune (møte 25.04.2022, e-post 19.9.2022). Revisjonen kan heller ikke finne dette i kommunens rutiner. Leder for ØIKT oppgir at det er gjort en gjennomgang av virksomheten på digitaliseringsområdet knyttet til status i forhold til NSMs grunnprinsipper. Kommunen og digitaliseringsavdelingen bruker NSMs grunnprinsipper som rettesnorer på det organisatoriske. En intern gjennomgang av NSM sine sikkerhetsanbefalinger viser at kommunene har flere mangler når det gjelder bl.a. feilretting og rutiner knyttet til teknisk krisehåndtering (intervju 08.08.22).

5.2 Er kommunens internetteksponerte tjenester innbruddssikre?

Romerike revisjon bestilte en inntrengningstest for å sjekke eksternes muligheter for å trenge inn i Rælingen kommunens nettverk via internetteksponerte tjenester. Testen er gjort av helse- og omsorgssektorens nasjonale senter for cybersikkerhet Helsenett. Revisjonen har oversendt en fullstendig rapport med alle detaljer fra testen til Digitaliseringsavdeling og ØIKT (Norsk helsenett 2022).

Testen avdekket at Rælingen kommune krever tofaktorautentisering[7] ved innlogging fra internett på sentrale tjenester. I tillegg har kommunen få tjenester eksponert mot internett og dermed få mulige angrepsflater fra internett (Norsk helsenett 2022).

Helsenett rangerer sårbarheter i internetteksponerte tjenester som KRITISK, HØY, MEDIUM eller LAV. Rangeringen er basert på følgende faktorer:

- Hvor lett sårbarheten kan utnyttes.
- Antatt konsekvens dersom sårbarheten blir utnyttet.
- Om sårbarheten blir aktivt utnyttet av kjente trusselaktører, og i hvor stor utstrekning.

Helsenett fant ingen svakheter som gjør at de rangerer noen av kommunens internetteksponerte tjenester som KRITISK.

De fant to forhold med HØY sårbarhet:

- Svakt passord på et system (Visma Ressursstyring).
- Flere sårbarheter i et gammelt kamerasystem.

Rapporten fra Helsenett viser at det var mulig å logge inn med brukernavn “ralingen” og passord “ralingen” på et system tilhørende Rælingen kommune, Visma Ressursstyring som er et system som brukes for å legge ut vakter for folk som jobber turnus i helsesektoren. Det er begrenset hva man har tilgang til i systemet, men det var mulig å hente ut fullt navn på alle brukere av systemet. Helsenett anbefaler å bytte passord på eller fjerne den gjeldende brukeren Norsk helsenett 2022).

Rælingen kommune ved Digitaliseringsavdelingen oppgir i sin tilbakemelding at når det gjelder svakhet til passord på Visma Ressursstyring, handlet dette kun om en tjeneste som gir en oversikt over ledige vakter. Kommunens ressursstyringssystem ligger ikke eksponert på internett. På siden det henvises til har ansatte mulighet til å velge vakter. Disse kommer ut på egen liste, og saksbehandles manuelt (E-post fra Rælingen kommune 01.09.22). Digitaliseringsavdelingen er inne i en anskaffelsesprosess på en skybasert løsning for ressursstyring. Da vil løsningen flyttes til ekstern leverandør. Planen er at dette vil skje tidlig i 2023. Digitaliseringsavdelingen oppgir at brukeren det er henvist til i rapporten fra Helsenett, er slettet (E-post fra Rælingen kommune 01.09.22).

Når det gjelder kamerasystemet opplyser Helsenett at dette er fra 2013. Det er kjente sårbarheter i versjonen, men ingen kritiske sårbarheter, og ingen sårbarheter Helsenett greide å utnytte under testen. Helsenett kunne hente ut informasjon om serveren, filbaner, hvilke moduler som er i bruk osv. I tillegg gjøres all innlogging over ukryptert forbindelse. Helsenett anbefaler bl.a. å undersøke hvorvidt systemet er i bruk og om det må være eksponert på internett. Helsenett anbefaler kommunen å

[7] Tofaktorautentisering er en metode for styre tilgangskontrollen og legge på ekstra lag med sikkerhet i tillegg til passord.

vurdere å bytte til nyere versjoner, samt å sjekke om det går an å oppgradere server (Inntrengingstest – Rælingen kommune, 24.08.2022, Norsk helsenett).

Digitaliseringsavdelingen oppgir at tjenesten det henvises til ikke er en del av kommunens nettverk, men tilhører fotballklubben i kommunen. Fotballklubben får internett fra kommunen (E-post fra Rælingen kommune 01.09.22) Digitaliseringsavdelingen oppgir at de nå har gitt fotballklubben informasjon og anbefaling om å oppgradere programvaren (E-post fra Rælingen kommune 01.09.22post 01.09.22).

Helsenett fant to forhold med MEDIUM sårbarhet:

- Mulighet for å finne gyldige brukernavn og gjette passord
- Enkelte svake brukerpassord

Rapporten viste også at det i et bestemt system var mulig for eksterne å sjekke hvorvidt de ansattes brukernavn eksisterte og å gjette passord uten at dette sendte av gårde sms med krav om tofaktorautentisering til brukeren. Helsenett fant ca. 300 gyldige brukernavn. Ett passord ble også funnet ved gjetting på dette systemet. Muligheten for å sjekke om et brukernavn er gyldig, og spesielt bruk av enkle brukernavn (olanor) for Ola Nordmann, gjør at passordgjetting blir mer effektivt for angripere. Helsenett anbefaler å skru av systemet *Enhanced Security Feedback på NetScaler* som gjør at en får forskjellige feilmeldinger avhengig av hvorvidt brukeren finnes, (Norsk helsenett 2022). Digitaliseringsavdelingen i Rælingen kommune opplyser etter at de fikk Helsenetts rapport, om at de gjør tiltak som angitt og oppgir også at tjenesten bak adressene på lenger sikt vil fjernes (E-post fra Rælingen kommune 01.09.22).

Helsenett fant at enkelte ansatte hadde svake passord. Helsenett hadde ikke mulighet til å skifte passord på deres utdelte bruker, og kunne derfor ikke se den gjeldende passordpolicyen. De fikk derimot verifisert at en bruker hadde passordet Sommer2022. Helsenett anbefaler å tvinge brukerne av systemet til å velge bedre og sikrere passord. Dette vil i stor grad eliminere faren for at uvedkommende kan gjette seg til passord. Bruk av enkle passord utgjør en risiko både knyttet til internett og i internt nettverk. Dette kan forbedres ved å opprette en strengere passordpolicy, samt å forby de vanligste passordene. De anbefaler å innføre krav om minimum 15 tegn på passord og avvikle krav om jevnlig bytte av passord (Inntrengingstest – Rælingen kommune, 24.08.2022, Norsk helsenett).

Digitaliseringsavdelingen oppgir at de per i dag har krav om minimum tolv karakterer i passordet, at passordet ikke skal være et eget navn og ikke skal være brukt tidligere. Sommer2022 skulle derfor ikke ha kunnet fungere som passord. Årsaken til at passordet er funnet må være at det ligger igjen fra gammelt av og til en bruker som har vært inaktiv siden før siste endring av systemet. Digitaliseringsavdelingen viser til nettsted fra Microsoft med «anbefalinger for passordpolicy for Microsoft 365-passord» der antall anbefalte karakterer i passord ikke samsvarer med anbefalinger fra Helsenett. Digitaliseringsavdelingen i Rælingen kommune har ikke krav til jevnlig passordbytte. Rælingen kommune og ØIKT oppgir at de vil vurdere gjeldende passordpolicy og evt. endre slik at

passord skal ha 15 karakterer samt eventuelt andre nye krav (E-post fra Rælingen kommune 01.09.22).

Helsenett fant dessuten et forhold med LAV sårbarhet:

- Mulig unødvendig eksponerte tjenester

I rapporten til Helsenett vises det til at Rælingen kommune har internetteksponerte tjenester som ikke synes å fungere eller ikke er i bruk. Helsenett anbefaler å vurdere i hvilken grad flere av kommunens systemer som er i bruk skal være eksponert på internett. Det blir stadig funnet sårbarheter i alle slags programvareløsninger, og en reduksjon av mengden eksponerte tjenester reduserer sannsynligheten for at man får kjente og risikoutsatte sårbarheter (Inntrengingstest – Rælingen kommune, 24.08.2022, Norsk helsenett)

Digitaliseringsavdelingen oppgir at tjenestene som rapporten viser til ikke er i bruk. De vil som tiltak fjerne tjenestene slik at de ikke lenger er eksponert på internett (E-post fra Rælingen kommune 01.09.22).

5.3 Revisjonens konklusjon, vurdering og anbefaling

Revisjonens konklusjon er at kommunen er rimelig godt sikret mot innbrudd i kommunens interne nettverk via kommunens internetteksponerte tjenester. I tillegg har kommunen fått lukket ytterligere sikkerhetshull i etterkant av inntrengningstesten Helsenett utførte tilknyttet denne undersøkelsen.

Testen viste bl.a. at i Rælingen kreves tofaktorautentisering ved all innlogging fra internett og at kommunen har få mulige angrepsflater fra internett. Begge deler er positivt for sikkerheten. Helsenett fant ingen svakheter de rangerer som KRITISK. De fant likevel fire sårbarheter som Helsenett rangerer som MEDIUM eller HØY. Digitaliseringsavdelingen i Rælingen kommune og ØIKT, har gitt tilbakemelding på funnene fra inntrengingstesten fra Helsenett. Digitaliseringsavdelingen angir de konkrete tiltakene som er iverksatt og opplyser at alle de avdekkede svakhetene nå er lukket.

Revisjonen vil likevel påpeke at kommunen ikke har rutine for og heller ikke har gjennomført inntrengningstester tidligere. NSM anbefaler å ha rutiner for slike tester jevnlig.

På bakgrunn av dette er revisjonens anbefaling:

> Kommunedirektøren bør sørge for at det kommer på plass en rutine for å gjennomføre inntrengningstester jevnlig.

LITTERATUR- OG KILDELISTE

Lov og forskrift (lov, forskrift, tekst fra proposisjoner)

Lov av 22. Juni 2018 nr. 83 om kommuner og fylkeskommuner (kommuneloven) https://lovdata.no/dokument/NL/lov/2018-06-22-83. [27.9.22]

Lov av 18. Juni nr. 38 om behandling av personopplysninger (personopplysningsloven)

https://lovdata.no/dokument/NL/lov/2018-06-15 38?q=lov%20om%20behandling%20av%

20personopplysninger [27.9.22]

Lov av 6. Juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven) https://lovdata.no/dokument/NL/lov/2018-06-01-24?q=sikkerhetsloven [27.9.22]

Forskrift av 25. Juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) https://lovdata.no/dokument/SF/forskrift/2004-06-25-988?q=eForvaltningsforskriften[27.9.22]

Forskrift om kommunal beredskapsplikt av 22. August 2011 nr. 894 (forskrift om kommunal beredskapsplikt) https://lovdata.no/dokument/SF/forskrift/2011-08-22-894?q=forskrift%20om%20kommunal%20beredskap [27.9.22]

Nasjonale veiledere, retningslinjer og annen litteratur

Digdir (2020:3) Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-fylkeskommuner-og-kommuner/2102 [27.9.22]

Digidir (2022): Internkontroll i praksis – Informasjonssikkerhet Versjon 2.0 https://www.digdir.no/search?search=internkontroll%20i%20praksis&f%5B0%5D=global_taxonomy%3A296 [27.9.22]

Direktoratet for e-helse (2020). Strategi for digital sikkerhet i helse- og omsorgssektoren. https://www.ehelse.no/publikasjoner/strategi-for-digital-sikkerhet-i-helse-og-omsorgssektoren-vurdering-av-behov-og-innretning [27.9.22]

Datatilsynet (2022): Veiledning på Datatilsynets nettsider: datatilsynet.no. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/ [27.9.22]

KS og KPMG (2022): Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet – Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus https://www.ks.no/contentassets/c019638eeb1e4972bac838e34c75dc47/-19-03185-6-Kommunedirektorens-verktoykasse-for-personvern-og-informasjonssikkerhet-1418678-2-1.pdf [27.9.22]

KPMG – IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021. https://www.ototen.no/_f/p1/i40fd2566-64fa-437b-b0e1-73cb446d3775/sikkerhetsrapport-usladdet-versjon.pdf [27.9.22]]

Nasjonal sikkerhetsmyndighet (NSM) (2020): NSMs grunnprinsipper for IKT-sikkerheten versjon 2.0 https://nsm.no/regelverk-og-hjelp/grunnprinsipper/ [27.9.22]

Standard for forvaltningsrevisjon (RSK 001), Fastsatt av styret i Norges Kommunerevisorforbund 1.2.2011. https://www.nkrf.no/filarkiv/File/Publikasjoner/RSK_RevisjonsStandard_Kommune/RSK_001_Standard_for_forvaltningsrevisjon_200812.pdf [27.9.22]

Kilder fra Rælingen kommune

Rælingen kommune 2019a, Internkontrollsystem for informasjonssikkerhet, «System for informasjonssikkerhet»

Rælingen kommune 2019b, 20210419 Strategi ifht. sikkerhet ØIKT

Rælingen kommune 2020a, Oppsummering – årlig kontroll 2020 med tiltaksliste

Rælingen kommune 2020b, Overordnet risikoanalyse pr. 31.12.2020

Rælingen kommune 2020c, 20210530 Strategidokument v2.1 ØIKT

Rælingen kommune 2021a, Informasjonssikkerhet/avvik 2021 sendt Datatilsynet

Rælingen kommune 2021b, Håndtering av avvik 2021

Rælingen kommune 2021c, Funksjonsbeskrivelse sikkerhetsrådet, revidert april 2021

Rælingen kommune 2021d, NSM punkter 2021.05.07

Rælingen kommune 2021e, Opplæring av enhets- og avdelingsledere om GDPR og informasjonssikkerhet

Rælingen kommune 2021f, Opplæring av nyansatte informasjonssikkerhet

Rælingen kommune 2021g, Oppsummering – årlig kontroll 2021 med tiltaksliste - 31.12.21

Rælingen kommune 2021h, Overordnet risikoanalyse pr. 31.12.2021

Rælingen kommune 2021i, Overordnet ROS-IKT sikkerhet - 19.02.21

Rælingen kommune 2021j, 20211014 Organisasjonsbeskrivelse ØIKT v3

Rælingen kommune 2021k, ROS sikkerhet -utgangspunkt for - 7.02.21

Rælingen kommune 2021l, Årsrapportering informasjonssikkerhet 2021

Rælingen kommune 2022a, 20220510 Sikkerhetsstrategi og beskrivelse ØIKT v1

Rælingen kommune 2022b, Tiltakskort Rælingen kommune - 28.04.2022

Rælingen kommune 2022c, utskrift av skjermdump som viser siste dato for revisjon av dokument «System for informasjonssikkerhet» overlevert 19.08.22

Rælingen kommune udatert a, Rutiner for varsling til Datatilsynet

Rælingen kommune udatert b, Rutiner og status vedrørende personvernombudet/-fagansvarliges arbeide med avvik og melding til Datatilsynet

Rælingen kommune udatert c, IKT beredskapsplan

Rælingen kommune udatert d, ØIKT Beredskapssystem

Rælingen kommune udatert e, Ledelsens gjennomgang av arbeidet med informasjons-sikkerhet

Rælingen kommune udatert f, Mål og strategi for informasjonssikkerhet

Rælingen kommune udatert g, Prosedyre for opplæring av ledere og medarbeidere i informasjonssikkerhet

Rælingen kommune udatert h, Rutine for avvikshåndtering informasjonssikkerhet og GDPR

Rælingen kommune udatert i, Prosedyre for databehandleravtale

Rælingen kommune udatert j, Databehandleravtaler

Rælingen kommune udatert k, Mal bilag databehandleravtale fra www.anskaffelser.no,

Rælingen kommune udatert l, Mal for databehandleravtale

E-post fra sikkerhetsansvarlig Rælingen kommune 22.08.22

E-post fra leder for digitaliseringsavdelingen Rælingen kommune 01.09.22

E-post fra sikkerhetsansvarlig Rælingen kommune 19.09.22

Møte med leder av avdeling digitalisering og enhetsleder i Øyern IKT i Rælingen kommune 25.04.2022

Intervju med leder av avdeling digitalisering, sikkerhetsansvarlig og enhetsleder Øyern IKT i Rælingen kommune 08.08.2022

Kilder fra andre

Norsk helsenett 2022. Rapport fra inntrengingstest - Rælingen kommune, 24.08.2022..

https://www.nettavisen.no/du-er-den-storste-sikkerhetsrisikoen/s/12-95-208398

https://www.nsr-org.no/uploads/images/Digital_Trusler_Trender_2021.pdf

VEDLEGG 1: KOMMUNEDIREKTØRENES HØRINGSSVAR

RÆLINGEN KOMMUNE

Digitaliseringsavdelingen

Romerike revisjon IKS

Ringveien 4
2050 Jessheim

Offl. § 5 1. ledd

Deres ref:	Vår ref:	Dato:
	2022/1718-BENLUN	25.10.2022

FORELEGGELSE - FORVALTNINGSREVISJONSRAPPORT IKT-SIKKERHET
Viser til forvaltningsrevisjon om digitalisering og IKT-sikkerhet i Rælingen kommune, og kommer med tilbakemelding på hovedfunnene i rapporten.

Hovedfunn

1. **Ansatte i kommunen har for lite opplæring innen personvern og informasjonssikkerhet.**

   Rælingen kommune har systematisk opplæring av ledere, enhetsledere og avdelingsledere, innen personvern og informasjonssikkerhet. I rapporten kan det virke som om det ikke eksiterer opplæring på området. Opplæring av ansatte varierer i større grad mellom de ulike enhetene.

   Systematisk og strukturert opplæring av ansatte vil være en stor fordel på IKT-sikkerhet, slik rapporten beskriver.

2. **Det gjennomføres i for liten grad risikovurderinger knyttet til IKT-sikkerhet**

   Rælingen kommune har etablert en systemorganisasjon rundt drift og forvaltning av IKT-systemer. For hvert IKT-system er det en systemeier og en systemansvarlig. Dette er viktige roller for drift og forvaltning av kommunens IKT-systemene. Alle systemansvarlige gjennomførte i 2021 ROS-analyse for det systemet de har ansvar for.
   Ref. e-post fra Hege Holmgren mandag 22. august 2022 11:23.

   Rapporten viser til at det er liten grad av risikovurdering knyttet til IKT-sikkerhet hos hver enkelt enhet. Dette kommer frem i internkontrollen; ledelsens gjennomgang av informasjonssikkerhet. I denne gjennomgangen har kun 50 % av lederne svart at de har gjennomført risikovurdering knyttet til IKT-sikkerhet. Denne risikovurderingen er knyttet til ansattes etterlevelse av IKT-sikkerhet, og ikke IKT-sikkerhet i hvert enkelt IKT-system.

3. **Det mangler oversikt over personopplysninger og informasjonsverdier i kommunen**

   Rælingen kommune har oversikt over alle IKT-systemene i verktøyet DigiOrden. DigiOrden viser oversikt over sammenheng og dataflyt mellom de ulike systemene. Systemenes kritikalitet er også vurdert i dette systemet.

Postadresse: Postboks 100, 2025 FJERDINGBY
Besøksadresse: Bjørnholthagan 6, 2008 Fjerdingby
Organisasjonsnummer:
Hjemmeside: www.ralingen.kommune.no
E-post: postmottak@ralingen.kommune.no
Telefon: 63835000
Bankgiro: 1503 05 43707

I tillegg til DigiOrden har kommunen verktøyet DraftIt. I dette systemet har kommunen oversikt over alle personopplysninger. DraftIt inneholder også oversikt over alle gjennomførte DPIA og ROS analyser, samt hvilke roller som har ansvaret for hvilket system. Rollene er i tillegg knyttet til navngitte personer, som igjen har ansvar for kontinuerlig oppfølging av sitt system.

DigiOrden og DraftIt sørger for at kommunen har god oversikt over personopplysninger og hvordan disse personopplysningene håndteres i kommunens tjenesteutøvelse. Dette ble kommunisert på møte 8.8.21.

Vi oppfatter at punkt 3 i rapporten ikke medfører riktighet.

4. Praksis for å melde avvik knyttet til personvern og informasjonssikkerhet er ikke god nok

Rælingen kommune er enig i at kulturen for å melde avvik burde vært bedre. Det arbeides kontinuerlig med å utvikle en kultur for å melde avvik. Det er etablert gode rutiner til hvordan avvikene skal behandles, når de først er meldt inn. Rælingen kommune har relativt mange innmeldte avvik til Datatilsynet sammenlignet med andre tilsvarende kommuner.

5. Kommunen har ikke rutine for å gjennomføre inntrengningstester

Det er riktig at kommunen mangler rutiner for å gjennomføre slike tester. Tidligere i år gjennomførte kommunen en grundig gjennomgang av NSM sine grunnprinsipper. Et resultat av denne gjennomgangen ble en anskaffelse av et overvåkningsverktøy, med tilhørende leverandørbistand. Dette tiltaket vil ha stor betydning for vår eksponering av tjenester ut mot offentligheten, og ikke minst redusere behovet for hyppige inntrengningstester.

Med hilsen

Eivind Glemmestad
kommunedirektør

Eivind Glemmestad
Kommunedirektør

Dokumentet er elektronisk godkjent og har ingen underskrifter