ROMERIKE
REVISJON IKS

FORVALTNINGSREVISJONSRAPPORT NR. 1-2022

DIGITAL SIKKERHETSRISIKO

AURSKOG-HØLAND KOMMUNE

JANUAR 2022

INNHOLD

SAMMENDRAG

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

Hovedfunn

1. Aurskog-Høland kommunen har gode formelle systemer for datasikkerhet.
2. Kommunens interne nettverk har nå et egnet sikkerhetsnivå mot datainnbrudd via kommunens internetteksponerte tjenester.
3. Det ble avdekket internetteksponert tjeneste uten tofaktorautentisering, noe som nå er utbedret.

Undersøkelsen viser at internkontrollen er dokumentert og at det er utformet rutiner og prosedyrer for å ivareta god internkontroll på området. Den viser videre at kommunedirektøren har praksis for å avdekk og følge opp avvik og risiko for avvik. Skriftlige prosedyrer og andre tiltak for internkontroll evalueres og forbedres ved behov. Revisjonen merker seg at IKT-avdelingen mener internkontrollen rundt sikkerhetsarbeidet bør opp på et overordnet nivå og innlemmes i overordnet plan for organisasjonen.

Norsk Helsenett SF har som ledd i undersøkelsen gjort en inntrengingstest i kommunens systemer. Norsk Helsenett er helse- og omsorgssektorens nasjonale senter for cybersikkerhet. Testen avdekket ikke sårbarheter i internetteksponerte tjenester som ga videre tilgang til internt nett i kommunen. For én tjeneste ble det avdekket en svakhet i konfigurasjonen av tofaktorautentisering[1] Kommunens IKT-avdeling presiserer at tofaktor var satt opp, men at det under gitt omstendigheter (relatert til enhet) var mulig å logge inn med kun brukernavn og passord. Det opplyses om at denne svakheten nå er utbedret.

Revisjonen har fått rask og god bistand fra administrasjonen i kommunen i gjennomføringen av undersøkelsen. En fullstendig rapport med alle detaljene fra testen utført av Norsk Helsenett er oversendt avdeling IKT og dokumentasjonssenter for oppfølging. Revisjonen vurderer det som positivt av det er en pågående prosess for å heve den totale IT-sikkerheten i kommunen, som ikke kun er relatert til internetteksponerte tjenester.

Kommunedirektørens høringsuttalelse

Et utkast til rapport er forelagt kommunedirektøren til uttalelse. Høringssvar ble mottatt 7.1.2022 og er i sin helhet vedlagt rapporten.

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

Kommunedirektøren skriver at hovedfunnene i rapporten har vært nyttige, og samsvarer godt med de områdene kommunen har prioritert for å sikre infrastruktur, systemer og data. Det vises også til at IKT-avdelingens internkontrollarbeid vil bli løftet til et høyere nivå og innlemmes i en overordnet plan for kommunen. Dette støttes og følges opp av kommunedirektøren, og er planlagt gjennomført i 2022.

Jessheim, 10.1.2022

Øyvind Nordbrønd Grøndahl
avdelingsleder forvaltningsrevisjon

Dokumentet er elektronisk godkjent

1 INNLEDNING

1.1 Bakgrunn

Kontrollutvalget i Aurskog-Høland kommune vedtok 25.1.2021 (sak 4/21) å be Romerike Revisjon utarbeide en prosjektplan for «Digital sikkerhetsrisiko» på bakgrunn av dialogen med kontrollutvalget.

Innbrudd i en kommunes IT-systemer kan ha store konsekvenser. Januar i år ble Østre Toten lammet av et datainnbrudd med løsepengevirus. Løsepengevirus er programmer som krypterer alle tilgjengelige filer og der eieren får beskjed om å betale løsepenger for å få tilbake innholdet i filene sine. Som følge av angrepet ble store deler av de kommunale systemene 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. De siste årene har vi sett løsepengevirus ramme hardt både i kommuner i Norge, privat sektor og sykehus i Europa.

Både KS og nasjonale myndigheter har i etterkant av dataangrepet mot Østre Toten pekt på at flere kommuner er utsatt for å kunne rammes av lignende angrep (brev fra KS til kommunene). Digitaliseringsdirektoratet oppsummerer i en rapport fra 2020 at fylkeskommuner og kommuner, ikke har tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet (Digdir rapport 2020:3). Ifølge analyseselskapet Canalys var 2020 det verste året med tanke på datainnbrudd generelt. Antallet datainnbrudd var omtrent dobbelt så høyt i 2020 som i 2019 (Digi.no, 2020). Årsaken antas bl.a. å være omstillingen til obligatorisk hjemmekontor.

1.2 Formål og problemstillinger

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

Undersøkelsen besvarer følgende hovedproblemstillinger:

1. Har kommunen gode formelle systemer for datasikkerhet?
2. Er det mulig å bryte seg inn i kommunens interne nettverk via kommunens internetteksponerte tjenester?

1.3 Rapportens oppbygging

Kapittel 2 beskriver gjennomføring og bruk av metode. Kapittel 3 gir en samlet fremstilling 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.

I sammendraget innledningsvis i rapporten fremstilles rapportens hovedfunn og rådmannens høringssvar til rapporten.

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]

Undersøkelsen bygger på dokumentanalyse og resultatene av inntrengingsforsøk i kommunens systemer, samt svar fra kommunen på skriftlige spørsmål fra revisjonen. Undersøkelsen er avgrenset til overordnede krav til formell sikkerhet ut fra internkontrollbestemmelser i kommuneloven, Forskrift om elektronisk kommunikasjon med og i forvaltningen samt Lov om behandling av personopplysninger.

2.1 Dokumentanalyse

Den første problemstillingen omhandler om kommunen har retningslinjer og rutiner knyttet til datasikkerhet. Dette undersøkes ved innsamling og gjennomgang av aktuelle dokumenter.

Revisjonen har fått oversendt etterspurt dokumentasjon og svar på spørsmål underveis på e-post. Det er i teksten referert til hvem vi har fått denne informasjonen av.

2.2 Inntrengingstest

For å få svar på den andre problemstillingen testes mulighetene for å bryte seg inn i kommunens interne nettverk via kommunens internetteksponerte tjenester. Inntrengingstesten er gjort av Norsk Helsenett SF. Dette er helse- og omsorgssektorens nasjonale senter for cybersikkerhet. Deres oppgave er å øke sektorens evne til å oppdage, forebygge og håndtere alvorlige cyberangrep. Norsk Helsenett har i testen forsøkt å angripe med kjente angrepsteknikker, via internett. Dette har skjedd i samarbeid med IKT-avdelingen i Aurskog-Høland, bl.a. for å unngå nedetid under testingen.

2.3 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 tjenesten eller organisasjonen.

[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 REVISJONSKRITERIER

Revisjonskriterier er de 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 utledes fra lov, kommunens egne rutiner og hva som ansees som god forvaltningsskikk på området. I denne undersøkelsen er revisjonskriteriene utledet fra to kilder.

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.

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) sier i § 15 at forvaltningsorganet skal ha en internkontroll på informasjonssikkerhetsområdet som bør være en integrert del av virksomhetens styringssystem. Vi setter følgende kriterier til problemstilling 1:

Problemstilling 1	
Har kommunen gode formelle systemer for datasikkerhet?	Kommunen skal: ➔ dokumentere internkontrollen i den formen og det omfanget som er nødvendig ➔ ha nødvendige rutiner og prosedyrer ➔ avdekke og følge opp avvik og risiko for avvik ➔ evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Lov om behandling av personopplysninger (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…».
Vi setter følgende kriterium til problemstilling 2:

Problemstilling 2	
Er det mulig å bryte seg inn i kommunens interne nettverk via kommunens internetteksponerte tjenester?	➔ Kommunen skal ha et sikkerhetsnivå som er egnet med hensyn til risikoen.

4 HAR KOMMUNEN GODE FORMELLE SYSTEMER FOR DATASIKKERHET?

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. Kommunedirektøren skal dokumentere internkontrollen i den formen og det omfanget som er nødvendig. eForvaltningsforskriften sier i § 15 at internkontroll på informasjonssikkerhetsområdet bør være en integrert del av virksomhetens styringssystem.

I kapittelet legges følgende problemstilling med tilhørende revisjonskriterier til grunn:

Problemstilling 1	
Har kommunen gode formelle systemer for datasikkerhet?	Kommunedirektøren skal ➔ dokumentere internkontrollen i den formen og det omfanget som er nødvendig ➔ ha nødvendige rutiner og prosedyrer ➔ avdekke og følge opp avvik og risiko for avvik ➔ evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

4.1 Er internkontrollen dokumentert?

Kommuneloven § 25-1 a) sier at internkontrollen skal beskrivelse virksomhetens hovedoppgaver, mål og organisering.

Kommunen har utarbeidet «Internkontroll i Aurskog-Høland Styringsdokument for arbeid med helse, miljø og sikkerhet HMS» og «Overordnet IKT-beredskapsplan» (e-post 15.9.21 fra IKT-avdelingen). Disse dokumenterer kommunens internkontroll.

I Økonomiplanene er kommunens hovedoppgaver, mål og organisering beskrevet. Økonomiplan 2021 – 2024 opplyser at «IKT og dokumentsenter» er en avdeling i «Økonomi og organisasjon», som er en støttestab for de andre sektorene i kommunen (Kommunestyret 14.12.2020). Avdelingen skal drifte og utvikle, veilede, håndtere og sikre IKT-infrastruktur, IKT-løsninger, dokumentflyt og arkiv.

4.2 Finnes nødvendige rutiner og prosedyrer?

Kommuneloven sier i § 25-1 b) at ved internkontroll skal kommunedirektøren bl.a.: ha nødvendige rutiner og prosedyrer.

Kommunen har rutiner og prosedyrer. I «Styringsdokument for internkontroll» står det at kommunen bruker et elektronisk baserte systeme som hovedverktøy i gjennomføring av internkontroll (Internkontroll i Aurskog-Høland kommune Styringsdokument for arbeidet med HMS, fra 1.1.2020). Her finnes lenker til lover og forskrifter, lokale reglementer, samt skjemaer/rutiner for å melde avvik,

gå vernerunder, gjennomføre risikoanalyser m.m. Det digitale internkontrollsystemet ble innført ved årsskiftet 2009/2010 (e-post 12.10.2021 fra IKT og dokumentasjonssenter). Dokumentet «Overordnet IKT-beredskapsplan» plasserer ansvar og definerer roller samt beskriver hvordan uønskede hendelser skal håndteres.

4.3 Avdekkes avvik og risiko for avvik, og følges de opp?

Kommuneloven sier i § 25-1 c) at ved internkontroll skal kommunedirektøren bl.a.: avdekke og følge opp avvik og risiko for avvik.

IKT og dokumentasjonssenter har oversendt dokumentasjon på kommunens system for avvikshåndtering. I internkontrollsystemet finnes skjemaer/rutiner både for å melde avvik og for å gjennomføre risikoanalyser.

Kommunen avdekker avvik. IKT og dokumentasjonssenter oppgir at det er meldt 409 avviksmeldinger hittil i 2021[3]. Vi har ikke gjennomgått alle avviksmeldingene, men har fått eksempler på slike avviksmeldinger (e-post 12.10.2021 fra IKT og dokumentsenter). Alle ansatte har tilgang til internkontrollsystemet og kan melde avvik når de oppstår. Systemet gir de ansatte et "lavterskelverktøy" for rapportering av alle typer avvik. I internkontrollsystemet følges de standardiserte prosedyrene for avvik. Avhengig av område leder systemet de som er involvert gjennom oppfølgingspunktene for avviket.

Avdeling IKT og dokumentasjonssenter har oversendt to avviksmeldinger sendt gjennom internkontrollsystemet fra 2021 knyttet til IKT[4]. Begge disse avviksmeldingene har rutinesvikt, manglende opplæring og uklare ansvarsforhold, som årsak til avviket. For den ene saken oppgis at rutine foreligger, men at den må følges som tiltak fremover. For den andre saken foreslås tiltak som metodeforbedring og opplæring. IKT-avdelingen har sendt over to eksempler på avviksmeldinger meldt gjennom andre kanaler enn internkontrollsystemet. Dette er interne avvik som løses i IKT avdelingen. Meldingene dreier seg dels om problemer knyttet til mulige avvik i bruk av bedriftstelefonnett knyttet til taushetsbelagte opplysninger og dels avvik meldt om misbruk av en av kommunens telefonnummer (e-post 12.10.2021).

Kommunen avdekker også risiko for avvik. Vi har fått eksempler på gjennomføring av ROS-analyser (e-post 15.9.2021 fra IKT og dokumentsenter). Revisjonen har blant annet fått oversendt dokumentasjon på ROS-analyse i 2020 angående Cyberangrep[5] (e-post 1.10.2021 fra IKT og dokumentsenter). Her vurderes sannsynligheten for et angrep som høy og konsekvensene vurderes som store for forstyrrelser i dagliglivet, omdømme og tillit.

[3] Per. oktober 2021.
[4] Fra henholdsvis 27.1.2021 og 6.6.2021.
[5] Cyberangrep er en ekstern trussel som har til hensikt å skade, forstyrre eller overbelaste datasystemet.

Avdeling IKT og dokumentasjonssenter opplyser at de har gjennomført stikkprøver og gjennomtreningstester knyttet til daglig drift. I tillegg har de gjennomført automatiserte sårbarhetstester av nettverk og applikasjoner. Avdelingen har også gjennomført tester med såkalte digitale honningkrukker[6].

Kommunen følger opp avvik og avdekte risikoer. Avvik som rapporteres går automatisk til nærmeste leder, med en tidsfrist for oppfølging. Utfra risikoanalysene lages aktivitetsplaner med tiltak for å forebygge avvik. I disse aktivitetsplanene nedfelles sjekklister for de ansatte og deres oppfølging av tiltakene, samt ledelsens kontroll av sjekklistene. For trusselen om Cyberangrep er flere tiltak oppgitt som iverksatte: Adgangskontroll, logiske sikringstiltak, holdningsskapende arbeid, backup, manuell drift og nødnett. Det er også anbefalt flere nye tiltak.

4.4 Evalueres og forbedres tiltakene for internkontroll?

I følge § 25-1 e) skal kommunedirektøren evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

I internkontrollsystemet står det at kommunen har en årlig intern revisjon for å sjekke om internkontrollsystemet virker. (Internkontroll i Aurskog-Høland kommune - Styringsdokument for arbeidet med helse, miljø og sikkerhet). Tidligere versjoner av internkontrollsystemet foreligger ikke digitalt. Det foreligger heller ikke dokumentasjon på oppgradering og justering av det digitale systemet for avvikshåndtering (e-post 12.10. 2021 fra IKT og dokumentasjonssenter).

Kommunen har laget en mal for «Gjennomføring av hendelseslæring» for å lære av de avvikene som skjer. Dette er et verktøy for forbedring som følge av avvik. Hendelseslæringen inneholder 14 faste punkter knyttet til bl.a. beskrivelse av feilen, analyse av årsaken til feilen og hva som er gjort for å løse feilen. Denne prosedyren benyttes hovedsakelig for avvikshendelser utenom det digitale internkontrollsystemet med felles møter mellom de involverte parter hvor man finner ut av avviket. Det digitale internkontrollsystemet følger de samme prosedyrene som i hendelseslæringsmalen, men noe forenklet.

Avdeling IKT og dokumentasjonssenter oppgir at den strukturerte hendelsesprosedyren/malen og internkontrollsystemet har ført til at mangler i de skriftlige prosedyrene i internkontrollsystemet avdekkes. Det foreligger dokumentasjon på dette i form av at det er utarbeidet nye og endrede prosedyrer (e-post 12.10.2021 fra IKT og dokumentasjonssenter).

IKT-avdelingen mener det er behov for et overordnet nivå i forhold til internkontroll rundt sikkerhetsarbeidet (e-post 7.12.2021). Denne oppfattes for segmentert/oppdelt slik den fremstår i dag,

[6] En honningkrukke er et luresystem en kan bruke for å oppholde angripere, lure dem bort fra de virkelig kritiske systemene, og samle informasjon om deres aktiviteter.

og vanskeliggjør visualisering av «det store bildet». Dette er noe de ønsker å løfte oppover i organisasjonen, slik at sikkerhetsarbeidet blir innlemmet i overordnet plan for organisasjonen.

4.5 Revisjonens vurdering og konklusjon

Det er revisjonens vurdering av kommunen har gode formelle systemer for datasikkerhet. Undersøkelsen viser at kommunen har dokumentert internkontrollen når det gjelder IT-sikkerhet og at det er utformet skriftlige rutiner og prosedyrer for denne. Undersøkelsen viser videre at kommunen har en praksis for å avdekke og følge opp avvik og risiko for avvik. Den viser også at skriftlige prosedyrer og andre tiltak for internkontroll evalueres og forbedres ved behov. Revisjonen merker seg at IKT-avdelingen mener det er behov for et overordnet nivå i forhold til internkontroll rundt sikkerhetsarbeidet og ønsker at sikkerhetsarbeidet blir innlemmet i overordnet plan for organisasjonen.

Ifølge Kommuneloven skal kommunedirektøren dokumentere internkontrollen i den formen og det omfanget som er nødvendig (§ 25-1 d). Om kommunens rutiner og prosedyrene for datasikkerhet er tilstrekkelige, belyses delvis i neste kapittel som bygger på tester av om det er mulig å bryte seg inn i kommunens interne nettverk via internett.

5 ER DET VIA INTERNETT MULIG Å BRYTE SEG INN I KOMMUNENS INTERNE NETTVERK?

Dette kapittelet er det undersøkt om det er mulig å bryte seg inn i kommunens interne nettverk via kommunens internetteksponerte tjenester.

Personopplysningsloven sier i Artikkel 32 at kommunen skal «… gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen …».

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 skal ha et sikkerhetsnivå som er egnet med hensyn til risikoen.

Testen gjort av Norsk Helsenett viste at kommunen hadde forholdsvis få tilgjengelige tjenester via internett.[7] Webtjenester for internt bruk av kommuneansatte krever innlogging før en når tjenesten innenfor. Flere tjenester krevde tofaktorautentisering[8], blant annet for tilgang til eksternt skrivebord på terminalservere.

Én tjeneste eksponert på internett kunne logges inn på med kun brukernavn og passord. I dette tilfellet kunne komplett liste over navn og brukernavn hentes ut gjennom tjenesten, men ingen sensitive data var tilgjengelig. Svakheten her er at en angriper kan gjette brukernavn og passord, og deretter hente ut informasjon. I en organisasjon med mange ansatte vil det ofte være en del brukere med svært svake passord. Norsk Helsenett vurderer denne sårbarheten som høy utfra hvor lett sårbarheten kan utnyttes, konsekvensene og hvor ofte den utnyttes av kjente trusselaktører.

IKT-avdelingen mener denne avdekkede sårbarhet er alvorlig og opplyser at den nå er utbedret (e-post 7.12.2021). Det blir opplyst at tofaktorautentisering var satt opp, men at det under gitte omstendigheter (relatert til enhet) var mulig å logge inn med kun brukernavn og passord (e-post 20.12.2021). Dette skyldtes en svakhet i konfigurasjonen.

Kommunen har få tjenester eksponert på internett og dermed få mulige angrepsflater fra internett. Det ble ikke funnet noen sårbarheter i internetteksponerte tjenester som ga videre tilgang til internt nett hos Aurskog-Høland kommune.

[7] En fullstendig rapport med alle detaljer fra testen er oversendt IKT og dokumentsenter.
[8] Tofaktorautentisering er en metode for styre tilgangskontrollen og legge på ekstra lag med sikkerhet i tillegg til passord.

Norsk Helsenett mener at alle internetteksponerte tjenester i kommunen bør beskyttes med tofaktorautentisering. IKT-avdelingen opplyser at det nå gjenstår kun én tjeneste uten tofaktorautentisering (e-post 7.12.2021). Det arbeides med å få denne på plass i forbindelse med det pågående arbeidet med utskifting av sikkerhetsløsninger. Arbeidet med to-faktorautentisering har gått parallelt med tjenestene kommunen fortløpende har gjort tilgjengelig fra internett.

5.1 Revisjonens vurdering og konklusjon

I dette kapittelet er det undersøkt om det er mulig å bryte seg inn i kommunens interne nettverk via kommunens internetteksponerte tjenester. Undersøkelsen viser at det fantes få eksponerte tjenester på internett. Det ble funnet én tjeneste som manglet tofaktorautentisering, noe som ifølge kommunen skyldtes en svakhet i konfigurasjonen. Denne svakheten er nå utbedret.

Revisjonen vurderer at kommunens interne nettverk nå har et egnet sikkerhetsnivå mot datainnbrudd via kommunens internetteksponerte tjenester.

LITTERATUR- OG KILDELISTE

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

LOV-2018-06-22-83 Lov om kommuner og fylkeskommuner (kommuneloven).
https://lovdata.no/dokument/NL/lov/2018-06-22-83.

LOV-2018-06-15-38 Lov om behandling av personopplysninger (personopplysningsloven)
https://lovdata.no/dokument/NL/lov/2018-06-15
38?q=lov%20om%20behandling%20av%20personopplysninger

LOV-2006-05-19-16 Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
https://lovdata.no/dokument/NL/lov/2006-05-19-16

FOR-2004-06-25-988 Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) https://lovdata.no/dokument/SF/forskrift/2004-06-25-988

Nasjonale veiledere, retningslinjer og annen litteratur

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

Oslo Economics, Kantar TNS og Prof. Tina Søreide (2018) «Status og råd for etikkarbeid i Digdir-rapport 2020:3 Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner, https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-fylkeskommuner-og-kommuner/2102

Brev fra KS til kommunenes IT ansvarlig/IT sikkerhetsansvarlig (udatert).

WEB-sider

Digi.no, 2020 var et ekstremår for datainnbrudd, https://www.digi.no/artikler/rapport-2020-var-et-ekstremar-for-datainnbrudd/508638

Kilder fra Auskog-Høland kommune

«Overordnet IKT-beredskapsplan». Oversendt i e-post 15.9.2021 fra IKT og dokumentsenter.

«Internkontroll i Aurskog-Høland kommune Styringsdokument for arbeidet med helse, miljø og sikkerhet (HMS) Gjeldende fra 1.1.20», Aurskog-Høland kommune

Kommunestyret 14.12.2020 sak 128/20 Budsjett 2021 m/økonomiplan 2022 – 2024. https://pub.framsikt.net/2021/nyeaurskog-holand/bm-2021-op_2021-2024_kommunestyrets_vedtak/#/home

E-post 15.9.2021 fra IKT og dokumentsenter.

E-post 1.10.2021 fra IKT og dokumentsenter.

E-post 12.10.2021 fra IKT og dokumentsenter.

E-post 7.12.2021 fra IKT og dokumentsenter.

E-post 20.12.2021 fra IKT og dokumentsenter.

Kilder fra andre

Inntrengingstest - Aurskog-Høland kommune, 24.11.2021 Norsk helsenett.

Cyberangrep har kostet Hydro opptil 450 millioner https://e24.no/boers-og-finans/i/7078VV/cyberangrep-har-kostet-hydro-opptil-450-millioner

Synsam bekrefter datainnbrudd https://nrkbeta.no/2020/10/09/synsam-bekrefter-datainnbrudd/

Hospital ransomware attack leads to fatality after causing delay in care. https://www.healthcareitnews.com/news/hospital-ransomware-attack-leads-fatality-after-causing-delay-care

VEDLEGG 1: KOMMUNEDIREKTØRENES HØRINGSSVAR

IKT og dokumentsenter

Høringsuttalelse - forvaltningsrevisjonsrapport digital sikkerhetsrisiko

Det vises til forvaltningsrevisjonsrapport digital sikkerhetsrisiko, datert 14.12.2021.

Økningen i antall dataangrep, og spesielt hendelsen i Østre Toten kommune, var bakgrunnen for at kontrollutvalget i Aurskog-Høland kommune bestilte et arbeid for gjennomgang av digital sikkerhet i kommunen.

Vår erfaring er at det er en økning i antall angrep, noe logger fra våre systemer bekrefter. I tillegg er vi av samme oppfatning, slik rapporten beskriver, at praktisering av hjemmekontor for flere ansatte øker sårbarheten og bidrar til en høyere risiko for dataangrep.

Kommunedirektøren stiller seg derfor positivt til en gjennomgang av digital sikkerhetsrisiko, og til informasjon har IKT- avdelingen dette som et prioritert område i daglig arbeid med den tekniske infrastrukturen.

Rapporten som er gjennomført er en standard, overordnet og generell forvaltningsrapport. Detaljert arbeid med digital sikkerhet er innarbeidet i IKT- avdelingens rutinemessige arbeid, men ikke en del av undersøkelsens omfang.

Formelle systemer for datasikkerhet
Jmf Kommuneloven § 25-1 og eForvaltningsforskriften § 15 skal kommunen gjøre internkontroll av digital sikkerhet og innlemme dette i sin virksomhetsstyring.

Resultatet av undersøkelsen viser at kommunen har nødvendig dokumentasjon for at internkontroll praktiseres og etterleves, og at overordnet og mer spesifikk dokumentasjon som beskriver på det aktuelle ansvarsområdet i organisasjonen er ivaretatt.

IKT-avdelingens internkontrollarbeid vil bli løftet til et høyere nivå og innlemmes i en overordnet plan for kommunen. Dette støttes og følges opp av kommunedirektøren, og er planlagt gjennomført i 2022.

Risiko for å bryte seg inn via internett
Resultatet av undersøkelsen har avdekket en mulig risiko for tjenestene som er publisert på internett. Det ble avdekket sårbarhet ved innlogging til en av tjenestene, noe som gjaldt svakhet i konfigurasjonen av to faktor-kravet. Dette er nå utbedret, og arbeidet med å sikre to faktor-autentiseringer på internetteksponerte tjenester er et kontinuerlig arbeid for å opprettholde sikkerhetsnivået.

Hovedfunnene i forvaltingsrapporten har vært nyttige, og samsvarer godt med de områdene kommunen har prioritert for å sikre infrastruktur, systemer og data.

Med vennlig hilsen

Inger Hegna
kommunedirektør

Kjellaug Johansen
leder IKT og dokumentsenter

Dokumentet er godkjent elektronisk uten underskrift.