østfold kommunerevisjon IKS

Cyberangrep og informasjonssikkerhet

Fredrikstad kommune

Forvaltningsrevisjonsrapport

Rolvsøy
24. januar 2020

INNHOLDSFORTEGNELSE

1. SAMMENDRAG

Denne forvaltningsrevisjonen handler om cyberangrep og informasjonssikkerhet. Revisjonen har undersøkt ulike deler ved kommunens arbeid med IKT-sikkerhetsmessige situasjoner og informasjonssikkerhet.

Rapporten besvarer følgende problemstillinger:

- Har kommunen tilfredsstillende planer og rutiner for håndtering av IKT-sikkerhetsmessige situasjoner?
- Har kommunen etablert tilfredsstillende sikkerhetstiltak av sine datasystemer mot cyberangrep?
- Har kommunen etablert et tilfredsstillende styringssystem (internkontroll) for informasjonssikkerhet?
- I hvilken grad har de ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

Gjennomføring

Forvaltningsrevisjonen ble opprinnelig startet i september 2018, men har av ulike årsaker blitt utsatt. Hoveddelen av prosjektet er gjennomført i 2019.

Revisjonen har gjennomført undersøkelsen ved hjelp av intervjuer, dokumentanalyse og spørreundersøkelse. I tillegg har revisjonen fått utført en rekognosering[1] av kommunens systemer, og en phishing-test[2] mot 100 av kommunens ansatte.

Revisjonens funn

Planer og rutiner

Faktagrunnlaget i vår rapport viser at kommunen i hovedsak har tilfredsstillende planer og rutiner for håndtering av IKT-sikkerhetsmessige situasjoner, herunder varsling fra ansatte. Kommunens beredskapsplan for alvorlige driftssituasjoner, vedlikehold av infrastruktur og prosedyrer for ulike driftsstans-kategorier vil kunne dekke de fleste forhold som kan føre til driftsavbrudd i kommunens IKT-systemer. Det er positivt at kommunen involverer sikkerhetsmyndigheter ved behov, men dette er ikke nedfelt skriftlig i kommunens planer og rutiner – noe vi mener ville vært en fordel. Det er også positivt at kommunen siden 90-tallet har gjennomført ROS-analyser for IT-sikkerhet. Vi anser det likevel som mangelfullt at det ikke er utarbeidet en overgripende beredskapsplan for håndtering av IKT-sikkerhetsmessige situasjoner basert på denne analysen.

Sikkerhetstiltak

Våre undersøkelser viser at kommunen har etablert en rekke sikkerhetstiltak av sine datasystemer mot cyberangrep, som i hovedsak tilfredsstiller kravene i våre revisjonskriterier. Revisjonen har likevel avdekket enkelte forbedringsområder. I hovedsak gjelder dette at dokumentasjon på området er delvis overlappende, samtidig som flere dokumenter er under revisjon, og at det kan se ut til å være en sammenblanding av personvern og IT-sikkerhet i kommunens prosedyrer. Vi har derfor vurdert at kommunen ikke i stor nok grad har kommunisert innholdet i sin sikkerhetsstyring på en tydelig nok måte slik at det er lett forståelig for de ansatte.

[1] Kartlegging av mulige angrepsflater for en eventuell angriper.
[2] Utsending av e-post for å kartlegge om en angriper kan komme inn i systemene via de ansatte.

Vi mener også at det innebærer risiko at sluttbrukere kan be om midlertidig tilgang til filnedlasting. Etter vår oppfatning åpner det opp for at det installeres mer funksjonalitet enn nødvendig på enheten, og risikoen for at skadelig programvare får tilgang til kommunens systemer øker.

I dag gjennomgås loggfiler kun ved mistanke om forhold som bør følges opp. Etter vår oppfatning vil en jevnlig gjennomgang av loggfiler kunne føre til oppdagelse av mistenkelig aktivitet på et tidligere tidspunkt.

Som rekognoseringen av kommunens hoved-domene, og samtaler med kommunen viste, bruker ikke kommunen på tidspunkt for revisjon de anbefalte prinsipper for beste praksis ved e-post-sikkerhet.

Det kan videre være en risiko for at data blir lagret lokalt på bærbare enheter.

Det øker risikoen for uautorisert tilgang til kommunens systemer når ikke 2-faktor autentisering er tatt i bruk på alle flater der de ansatte eksternt skal koble seg til kommunens systemer.

Vår spørreundersøkelse viser at det kan være tilfeller der det gis utvidede tilganger uten at e-kurset er bestått/gjennomført. Det kan være en risikofaktor at det ikke er implementert systemkontroll for å sikre at kurset er gjennomført før den ansatte får utvidede tilganger. Det kan også være hensiktsmessig å vurdere behov for en sentral oppfølging av at tilganger blir gjennomgått på jevnlig basis. Eventuelt kan kommunen vurdere å tydeliggjøre ansvaret i sine rutiner på området.

Når det gjelder fysisk tilgang til kommunens servere, er vår oppfatning at det kan ligge risiko i det at alle som har administratorrettigheter i adgangssystemet kan gi adgang til serverrom. Risikoen reduseres noe av at systemet loggfører aktivitet, men risikoen kan reduseres ytterligere ved jevnlig gjennomgang av logger, eller restriksjoner i tilgangssystemet som hindrer uautoriserte personer å gi tilgang til disse rommene.

Internkontroll

Vi har funnet at kommunen har etablert flere tiltak som har positiv effekt i kommunens internkontroll på området, herunder blant annet en rekke rutiner og retningslinjer. Vi kan likevel ikke si at kommunen på nåværende tidspunkt har et styringssystem for informasjonssikkerhet som er tilfredsstillende. Som våre vurderinger viser handler dette blant annet om at internkontrolldokumentasjonen fremstår som uoversiktlig, manglende risikovurderinger og manglende overvåkning av systemet, samt lite systematikk i dette arbeidet.

Ansattes kjennskap til rutiner og retningslinjer

Våre vurderinger viser at kommunen har etablert en rekke tiltak for å sikre at kommunens ansatte har kjennskap til kommunens rutiner og retningslinjer for informasjonssikkerhet. Funnene viser imidlertid et ganske stort behov for kompetanseheving på området. Slik revisjonen vurderer det har kommunens ansatte kun i noen grad kjennskap til retningslinjer og rutiner for informasjonssikkerhet.

Anbefalinger

Basert på våre vurderinger og konklusjoner anbefaler vi at kommunen bør:

- implementere varsling til sikkerhetsmyndigheter i sine skriftlige rutiner/prosedyrer.
- prioritere å få på plass en overordnet beredskapsplan for IKT-sikkerhetsmessige situasjoner, basert på deres ROS-analyse.
- gjennomgå sine rutiner og prosedyrer på området, med særlig hensyn til gyldighet, begrepsbruk, ansvarsfordeling og overlapping av innhold.
- vurdere å gjennomgå viktige loggfiler jevnlig.
- prioritere å få på plass ytterligere sikring av sin e-post-kommunikasjon.

- vurdere å kryptere bærbare enheter der det er risiko for at sensitiv data blir lagret lokalt, som anbefalt i NSMs grunnprinsipper.
- innføre 2-faktor autentisering på alle flater der ansatte eksternt skal koble seg til kommunens systemer, eventuelt sperre for flater der 2-faktor autentisering ikke er tilgjengelig.
- vurdere å innføre sentral kontroll av gjennomgang av tilganger – eventuelt gjennomgå sine dokumenter på området med hensyn til tydeliggjøring av ansvaret for å gjennomgå tilganger.
- vurdere å jevnlig gjennomgå aktivitetslogg for tilgang til serverrom, eventuelt vurdere å innføre sperrer i systemet slik at det ikke er mulig for alle med administratorrettigheter å gi tilgang til slike rom.
- sørge for at risikovurderinger av informasjonssikkerheten gjennomføres i tråd med egne rutiner og retningslinjer.
- etablere en systematisk overvåkning av informasjonssikkerheten i kommunen for å sikre at lovverket etterleves.
- kartlegge de ansattes kompetansebehov innen informasjonssikkerhet, og vurdere nødvendige tiltak. Det kan være hensiktsmessig om kommunen også benytter resultatene fra spørreundersøkelsen som en indikasjon på hvordan kompetansetiltakene bør innrettes.

Revisjonen takker Fredrikstad kommune for bistanden og samarbeidet i forbindelse med gjennomføring av revisjonen.

2. INNLEDNING

2.1. Bakgrunn

Bystyret i Fredrikstad kommune vedtok forvaltningsrevisjonsplan for 2018-2019 den 15. mars 2018. I denne planen står det følgende om behovet for forvaltningsrevisjon knyttet til cyberangrep og informasjonssikkerhet:

Faktaboks 1: Bakgrunn

Revisjonen har som en av sine oppgaver å utføre forvaltningsrevisjon, jfr. kommunelovens § 78 og forskrift om revisjon kapittel 3. Forvaltningsrevisjon innebærer blant annet å kontrollere at forvaltningens aktiviteter foregår i samsvar med gjeldende bestemmelser og kommunestyrets vedtak.

«De siste årene har antallet cyberangrep rettet mot norske interesser økt i omfang. [...]

Norsk sikkerhetsmyndighet (NSM) opplyser at de erfarer fortsatt at digitale angrep så godt som alltid innledes med bruk av ulike varianter av skadevare distribuert via e-post, og at denne typen angrep fremstår med økende grad av profesjonalitet. Det er derfor viktig for kommunen å sikre gode rutiner knyttet til håndtering av e-post.

Revisjonen har ikke konkrete holdepunkter for å si at risikoen er større i Fredrikstad enn andre steder, men i lys av risikobildet som tegnes av norske sikkerhetsmyndigheter mener revisjonen at sannsynligheten for at kommunen kan bli utsatt for cyber-angrep fremstår som meget høy. Konsekvensen av et slikt angrep kan i verste fall få store konsekvenser både for kommunens mulighet til å levere tjenester til innbyggerne, men også for kommunens økonomi.

Den pågående digitaliseringen av samfunnet blir drevet fremover og gjort mulig av teknologiutvikling. Digitaliseringen gjør at stadig flere arbeidsprosesser utføres eller støttes av digitale verktøy. Kunnskap om, eller muligheten for å gjennomføre, manuelle rutiner forsvinner. Med økt digitalisering følger også økte krav til tilgjengelighet av viktige IKT-systemer. Dette er helt sentrale faktorer når nye, sikre digitale løsninger skal planlegges og implementeres. Ny teknologi kan gjøre det mulig å lage sikrere løsninger, men kan også medføre økt kompleksitet, introduksjon av nye sårbarheter og økt behov for sikkerhetskompetanse.

NSM opplyser i sin årsrapport at de erfarer at økte muligheter innen teknisk sikring ikke alltid utnyttes og at mangelfullt teknisk vedlikehold av systemer, eksempelvis manglende sikkerhetsoppdateringer, skaper unødvendige sårbarheter.

[...]

I forbindelse med digitalisering av kommunens løsninger er det derfor avgjørende å sikre informasjonen slik at den ikke kommer på avveie. For eksempel ved hjelp av tilgangsstyring, kryptering, osv. Personopplysningsloven § 13 med den tilhørende forskriftens kapittel 2 oppstiller i dag krav til kommunenes sikring av informasjon (informasjonssikkerhet). Den nye personvernforordningen som trer i kraft 25. mai 2018 innebærer strengere regler knyttet til informasjonssikkerhet.

Vi har ikke opplysninger som indikerer at det er en spesiell risiko knyttet til informasjonssikkerheten i Fredrikstad kommune. Datatilsynets tilsyn med kommuner i 2016 viste imidlertid vesentlige avvik knyttet til informasjonssikkerhet, noe som indikerer at det kan være god grunn til å også se nærmere på dette i Fredrikstad. Eksempelvis ble det avdekket at virksomheter ikke har tilstrekkelig fokus på å ivareta personvernet og på å oppfylle pliktene i personopplysningsloven knyttet til internkontroll og informasjonssikkerhet. Dette omfattet virksomheter med ansvar for digitaliseringsprosesser, men også for virksomheter som i økende grad benytter nye digitale løsninger. Datatilsynet vurderer det

som viktig for virksomhetene å ha et akseptabelt nivå på internkontroll og informasjonssikkerhet før store digitaliseringsprosesser starter opp.»

Prosjektplan for denne forvaltningsrevisjonen ble vedtatt av kontrollutvalget i Fredrikstad 13.juni 2018.

2.2. Problemstillinger

Rapporten omhandler følgende problemstillinger:

1. Har kommunen tilfredsstillende planer og rutiner for håndtering av IKT-sikkerhetsmessige situasjoner?
2. Har kommunen etablert tilfredsstillende sikkerhetstiltak av sine datasystemer mot cyberangrep?
3. Har kommunen etablert et tilfredsstillende styringssystem (internkontroll) for informasjonssikkerhet?
4. I hvilken grad har de ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

Risikoen som er beskrevet i planen for forvaltningsrevisjon knytter seg både til IT-sikkerhet, men også informasjonssikkerhet og grensene opp mot personvernregelverket -GDPR. Personvern er neste prosjekt på forvaltningsrevisjonsplanen for 2018-2019, og vi har derfor valgt å se nærmere på de temaene som faller naturlig inn under personvernområdet i egen rapport på personvernområdet. Det vil imidlertid være noe overlappende informasjon. Men en grundig vurdering av kommunens arbeid med personvern vil først kommune i neste forvaltningsrevisjonsrapport.

2.3. Metode og gjennomføring

Revisjonen har gjennomført undersøkelsen ved hjelp av intervjuer, dokumentanalyse og spørreundersøkelse. I tillegg har revisjonen fått utført en rekognosering[1] av kommunens systemer, og en phishing-test[2] mot 100 av kommunens ansatte.

Faktaboks 2: Metode og gjennomføring

Østfold kommunerevisjon IKS gjennomfører all forvaltningsrevisjon i tråd med «Standard for forvaltningsrevisjon» (RSK 001). Dette innebærer blant annet at rapporten skal skille klart mellom fakta, og revisjonens vurderinger og konklusjoner.

Fakta plasseres under egen overskrift, og er en gjengivelse av informasjon som revisjonen har fått tilgang til gjennom datainnsamlingen. Informasjonen bygger på beskrivelser hentet fra skriftlige dokumenter, mappegjennomgang, spørreundersøkelse og/eller verifiserte intervjuer. Det gjøres oppmerksom på at fakta i noen tilfeller kan gjengi kommunens egen vurdering eller opplevelse av en gitt tilstand. Fakta kan også være enkeltpersoners meninger, erfaringer eller holdninger.

Intervjuer/møter

Intervjuer og møter ble avholdt høsten 2019. Revisjonen har gjennomført arbeidsmøte med konstituert kommunaldirektør, og fra virksomhet digitalisering: digitaliseringssjef, leder for utviklingsavdeling, leder for driftsavdeling og sikkerhetsrådgiver. Her ble aktuelle temaer diskutert, og spørsmål besvart. I etterkant av møtet ble det utarbeidet et referat, som så ble verifisert av deltagerne.

Revisjonen har også gjennomført separate intervjuer med personvernombud og sikkerhetsrådgiver. Det er også sendt ut oppfølgingsspørsmål til digitaliseringssjef og kommunens ledergruppe. Intervjuene er gjennomført både stedlig og pr. e-post. Ved bruk av stedlige intervjuer er det utarbeidet referat som er verifisert av informanten.

[1] Kartlegging av mulige angrepsflater for en eventuell angriper.
[2] Utsending av e-post for å kartlegge om en angriper kan komme inn i systemene via de ansatte.

Dokumentanalyse

Revisjonen etterspurte dokumenter 20. august 2019, med frist for levering 30. august 2019. Dokumentasjon ble først mottatt 6. september 2019. Det ble etter dette også mottatt dokumentasjon fortløpende. Siste oversendelse, med ny beredskapsplan, ble mottatt i slutten av oktober. Revisjonen har gjennomgått de oversendte dokumentene knyttet til kommunens arbeid med IT-sikkerhet og personvern/GDPR. Revisjonen har også hentet ut enkelte dokumenter fra kommunens kvalitetssystem. Fullstendig dokumentliste følger i vedlegg (kapittel 9.3).

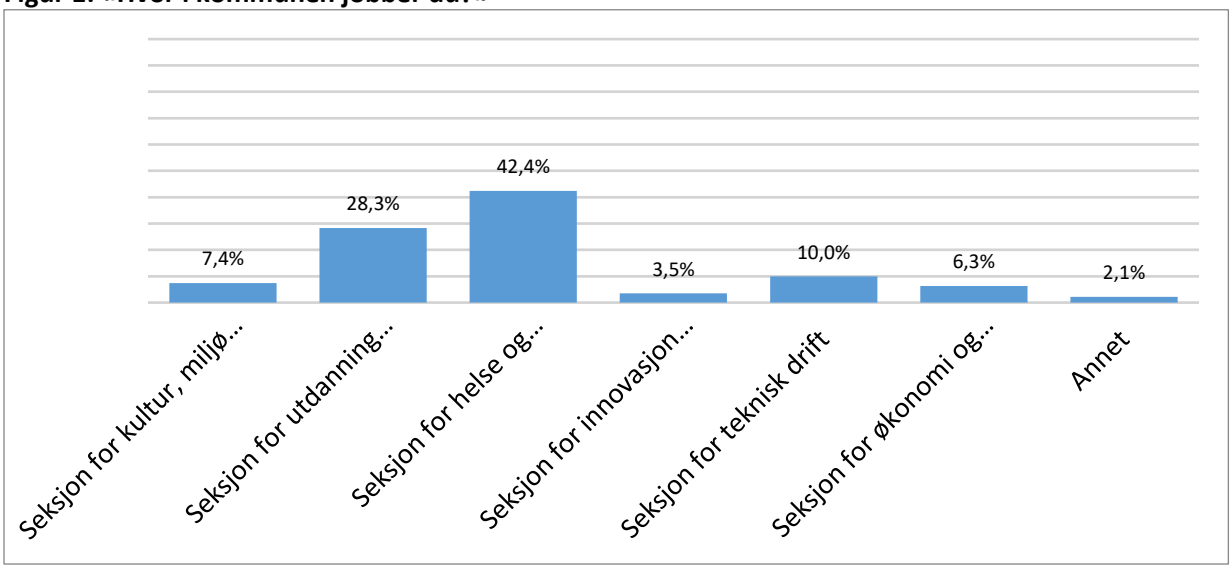
Spørreundersøkelse

Utkast til spørreundersøkelsen ble oversendt kommunen 11. september 2019 for gjennomgang og mulighet for å komme med innspill. Kommunens innspill er hensyntatt i spørreundersøkelsen.[3] Spørreundersøkelsen følger i vedlegg (kapittel 9.4).

Spørreundersøkelsen ble sendt ut til 8 169 respondenter, basert på en liste med alle ansatte mottatt fra kommunen. Vi mottok svar fra 1 303 ansatte, noe som utgjør en svarprosent på 15,95. Med over 1300 respondenter mener vi at svarene vil kunne gi et godt innblikk i ansattes oppfatninger.

Tilbakemeldinger revisjonen har fått på undersøkelsen, fra blant annet politikere, viser at respondentlisten også inneholdt e-post adresser til flere enn de ansatte i kommunen. Vi har ikke informasjon om hvor mange av mottakerne dette gjelder. Nedenfor presenteres noen opplysninger om respondentene.

Figur 1: «Hvor i kommunen jobber du?»

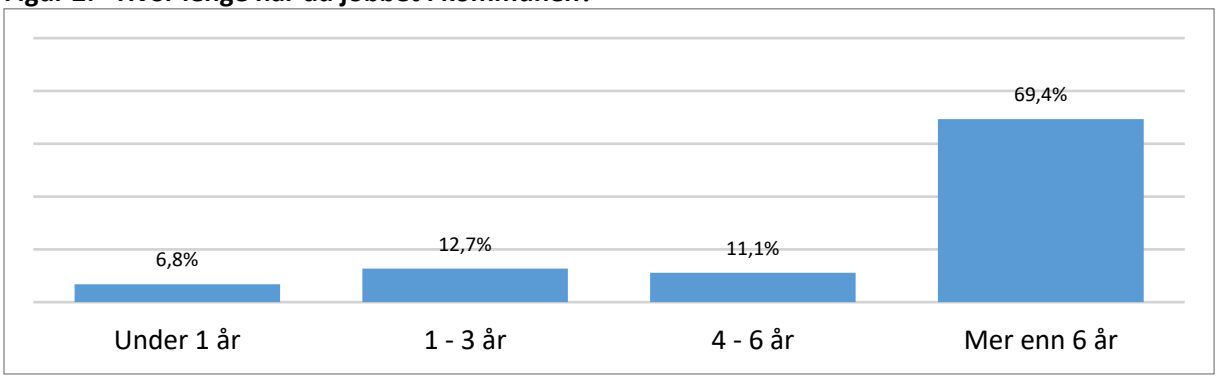


Antall respondenter: 1303

Figur 1 viser at de fleste respondentene arbeider i seksjon utdanning og oppvekst eller helse og velferd. Det er også i disse to seksjonene kommunen har flest av sine ansatte.

[3] I arbeidsmøte den 13.9.2019 ble det gitt tilbakemelding på at et av spørsmålene ikke lenger var relevant. Revisjonen fjernet dette spørsmålet fra undersøkelsen før den ble sendt ut.

Figur 2: «Hvor lenge har du jobbet i kommunen?»



Antall respondenter: 1303

I figur 2 ser vi at 69,4 prosent har jobbet i kommunen i mer enn seks år. På spørsmål om stillingstype oppgir 94 prosent av respondentene å ha fast stilling, mens 3,9 prosent oppgir engasjement/vikariat og 2,1 prosent oppga annet. Blant respondentene oppgir 77,3 prosent at de arbeider i en stilling på 80 prosent eller mer.

Rekognosering av kommunens hoved-domene

Et eksternt selskap har bistått revisjonen med rekognosering av kommunens systemer. En rekognosering har som mål å identifisere eventuelle datalekkasjer, sensitive systemer som ikke bør være på nett og andre forhold som kan utgjøre en risiko for at uvedkommende kan komme seg inn i kommunens systemer. En rekognoseringsrapport danner gjerne grunnlaget for penetrasjonstesting, der man simulerer hvordan en målrettet angriper vil angripe systemene.

Revisjonen har kun fått gjennomført en rekognosering, for å avdekke mulige svakheter i kommunens systemer. Det er ikke gjort tester utover dette. Fredrikstad kommune har en kompleks datastruktur med flere tilknyttede enheter, og en rekke underleverandører og tjenester. Av ressursmessige hensyn er undersøkelsen begrenset til en kortvarig undersøkelse av kommunens hoved-domene.

I undersøkelsen er det også kartlagt hvilken informasjon fra kommunen som er lett tilgjengelig, og om ansatte bruker kommunale e-post-adresser på internett. Videre er kommunens og ansattes bruk av sosiale medier, og om kommunen har applikasjoner til telefoner/nettbrett som kan være sårbare innganger til kommunens systemer kartlagt.

Resultatet av rekognoseringen gjengis på et overordnet nivå i denne rapporten. Av hensyn til sikkerheten kan vi ikke gjengi detaljer om de funnene som er gjort. Kommunen vil få fullt innsyn i rapport fra utøvende part.

Phishing-test

Det eksterne selskapet gjennomførte også en phishing-test, rettet mot 100 ansatte i Fredrikstad kommune. Revisjonen hadde på forhånd gjort et utplukk av ansatte som oppfylte minst ett av følgende kriterier:

- Den ansatte har omfattende tilganger i de kommunale systemene
- Den ansatte får mange henvendelser via e-post
- Den ansatte har tilgang til personsensitive opplysninger om innbyggere

Basert på disse kriteriene gjorde revisjonen et tilfeldig utplukk av 100 ansatte med over 50 % stilling. Fullstendig oversikt over hvilke ansvar og antall ansatte, følger i vedlegg (kapittel 9.2).

Virksomhet digitalisering kjente til phishing-testen på forhånd, og på oppfordring fra revisjonen lot være å følge egen rutine for slike situasjoner. Testen kan således kun ses på som en test av reaksjoner og handlinger hos ansatte, og ikke hvorvidt det er mulig å hacke kommunen på denne måten.

Validitet og reliabilitet

Vi har benyttet data fra ulike kilder, og brukt ulike innsamlingsmetoder for å sikre et faktagrunnlag med høyest mulig grad av gyldighet og pålitelighet. Utfordringer og begrensninger i rapportens faktagrunnlag er beskrevet ovenfor sammen med beskrivelsen av de ulike metodene som er benyttet. Vi tar også hensyn til metodens begrensninger i vurderingene. På denne bakgrunn mener vi at rapporten fremstiller kommunen på en mest mulig riktig måte, og at vi har et godt grunnlag for våre konklusjoner og anbefalinger.

Forvaltningsrevisjonen er gjennomført av forvaltningsrevisor Constance Hauser og revisor Anita Marie Torp i perioden august til oktober 2019. Som nevnt er det også benyttet ekstern bistand fra leverandør av IT-sikkerhetstjenester.

2.4. Revisjonskriterier

Revisjonskriterier fastsettes normalt med basis i en eller flere autoritative kilder og ut fra trinnhøydeprinsippet[4]. Med autoritative kilder menes normalt lovverk, politiske vedtak og føringer, men også kommunens egne retningslinjer, anerkjent teori på området og/eller andre sammenlignbare virksomheters løsninger og resultater, kan danne basis for revisjonskriterier.

I dette prosjektet er følgende kilder benyttet for å utlede revisjonskriteriene:

- Kommuneloven
- Personopplysningsloven
- Lov om kommunale helse- og omsorgstjenester m.m., 2011
- Ot. Prp. Nr. 58, 2002-2003
- Stortingsmelding nr. 38 2016-2017 – «IKT-sikkerhet – Et felles ansvar»
- Nasjonal strategi for digital sikkerhet
- EUs personvernforordning (GDPR)
- eForvaltningsforskriften
- Virksomhetssikkerhetsforskriften
- ISO/IEC 27001:2013
- Difis veiledning til ISO/IEC 27001:2013, versjon 1.4
- NSMs veileder «Grunnprinsipper for IKT-sikkerhet»
- NSMs sjekkliste S-01 «fire effektive tiltak mot dataangrep»
- NSMs sjekkliste S-02 «ti viktige tiltak mot dataangrep»
- Rammeverk for håndtering av IKT-sikkerhetshendelser, per 7.12.17. Fastsatt av Justis- og beredskapsdepartementet for sivil sektor og Forsvarsdepartementet for forsvarssektoren.
- Fredrikstad kommunes rutiner og retningslinjer på området

Utledning av revisjonskriteriene følger i vedlegg (kapittel 9.1), samt punktvis oppsummert under hver problemstilling (kapittel 3.1, 4.1, 5.1 og 6.1).

[4] Trinnhøydeprinsippet, også kalt lex superior-prinsippet, er et rettslig prinsipp som innebærer at rettsregler av høyere rang går foran regler av lavere rang dersom det er motstrid mellom reglene.

3. PLANER OG RUTINER

Har kommunen tilfredsstillende planer og rutiner for håndtering av IKT-sikkerhetsmessige situasjoner?

3.1. Revisjonskriterier

Revisjonen har utledet følgende kriterier for å besvare denne problemstillingen[5]:

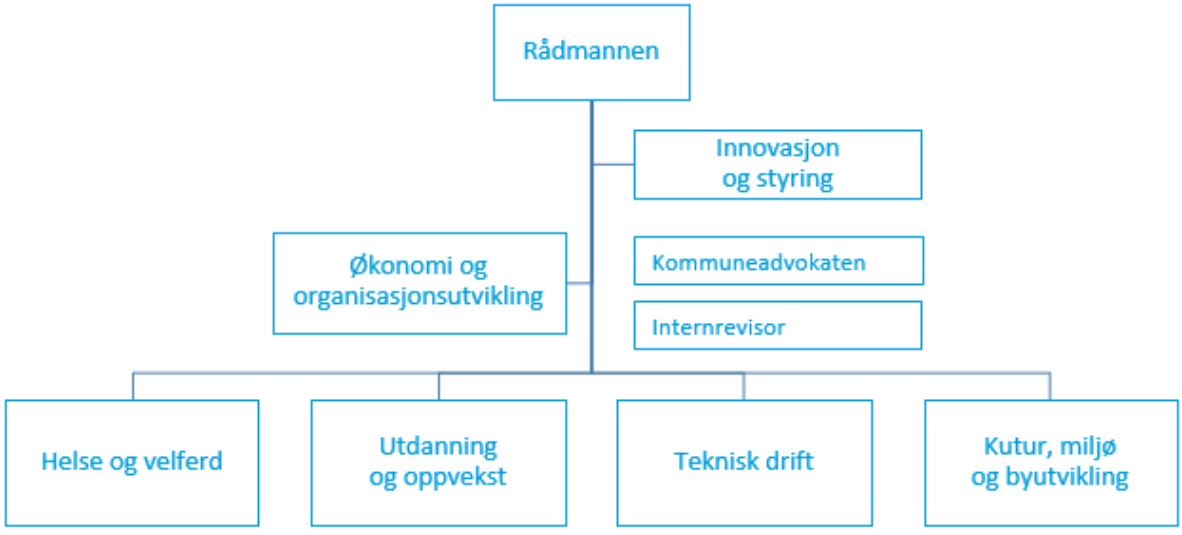
- Kommunen gjennomfører risikovurderinger knyttet til IT-sikkerhet.
- Kommunen har planer og rutiner (sikkerhetstiltak) for å sikre beredskap ved sikkerhetshendelser.
- Planene og rutinene er kjent for de ansatte.
- Det er utarbeidet rutiner for å varsle om IKT-sikkerhetshendelser. Herunder om det skal varsles til SRM[6] og eventuelt samarbeidende virksomheter, samt til NSM[7] om nødvendig.
- Kommunen vurderer behov for bistand ved IKT-sikkerhetshendelser.

3.2. Fakta

Organisering av IT-sikkerhetsarbeidet

Fredrikstad kommune har organisert sin virksomhet i seks seksjoner, i tillegg til funksjonene kommuneadvokat og internrevisor som er frittstående organisert i forhold til øvrige seksjoner. Kommunens prosedyre «Organisering av personvern- og informasjonssikkerhetsarbeidet» fastslår at det overordnede, generelle sikkerhetsansvaret ligger til rådmannen.

Figur 3: Fredrikstad kommunes organisasjonskart



Ansvaret for drift og vedlikehold av kommunens IT-systemer ligger til virksomhet digitalisering, som er organisert under seksjon for innovasjon og styring. Virksomhetens drift er delt inn i tre avdelinger; IT drift, IT service og IT utvikling, med digitaliseringssjef som virksomhetsleder.

[5] Se vedlegg 1 for utledning av kriterier
[6] Sektorvist responsmiljø. Se utledning av revisjonskriterier.
[7] Nasjonal sikkerhetsmyndighet. Se utledning av revisjonskriterier.

Det overordnede ansvar for drift av informasjonssystemet er delegert til digitaliseringssjef. Prosedyren «Digitaliseringssjefens ansvar og myndighetsområde» slår videre fast at digitaliseringsjefen har det faglige ansvaret for kommunens IT-system, herunder drift og vedlikehold, i tillegg til ansvar for blant annet:

- installasjon av programvare og programvare-oppdateringer
- tilgang/innmelding av brukere til nettverk og systemer, herunder sperre tilganger eller fjerne slike brukere
- å forvalte vedtatt sikkerhetspolicy
- utarbeidelse og løpende oppdatering av konfigurasjonsoversikt og beskrivelser av utstyr/programmer
- logg over endringer
- å kjøre oppgraderinger
- backup-rutiner
- installasjon av nye arbeidsmaskiner/klienter

Digitaliseringssjefen har videredelegert en del av arbeidet rundt IT-sikkerhet. I virksomhet digitalisering er det en ansatt som bruker ca. 50 % av sin stilling til IT-sikkerhetsarbeid, og en IT-driftssjef som blant annet har ansvar for å godkjenne endringer i kommunens systemer.

Hvert IT-system har en systemeier, som ofte også vil være daglig ansvarlig. I tillegg har kommunen egne systemansvarlige, med detaljkunnskap om IT-systemet. Daglig ansvarlig er, ifølge prosedyren:

- hovedansvarlig for IT-systemet i sin virksomhet
- juridisk part i relasjon til leverandør
- ansvarlig for at lover og forskrifter, respektive regler og retningslinjer følges ved utvikling, drift og vedlikehold av IT-systemet
- ansvarlig for kvaliteten (sikkerhet) på IT-systemet
- ansvarlig for at opplæringstilbud og dokumentasjon er tilfredsstillende og tilgjengelig
- ansvarlig for å følge opp kravet til avbruddsplan/katastrofeplan for IT-systemet

Risikovurdering

I kommunens kvalitetssystem ligger det en overordnet risiko- og sårbarhetsanalyse fra 2014. Dokumentet gjelder i hovedsak katastrofer som kan inntreffe i kommunen. Den har også et punkt om svikt i EKOM[8] systemer, hvor konsekvenser som fare for liv og helse og utfall av kommunal tjenesteproduksjon er vurdert.

Basert på denne har kommunen utarbeidet en beredskapsplan for kommunens virksomhet. Beredskapsplanen er på et overordnet nivå, og omhandler ikke direkte IKT-sikkerhetshendelser.

Virksomhet digitalisering har gjennomført ROS-analyse for IT-sikkerhet. Analysen omhandler sikkerhet for egne data og systemer hvor driftsansvar ligger hos virksomhet digitalisering. Analysen inkluderer ikke systemer som driftes av tredjepart. For disse systemene skal behandlingsansvarlige utarbeide egne ROS-analyser, samt databehandleravtale.

Arbeidet med siste versjon av analysen startet opp i april 2018 og ble avsluttet i juni 2019.[9] Analysen beskriver sikkerhetsbrudd som følge av kriminelle handlinger, menneskelige feil eller teknisk svikt. I henhold til rapporten er analysen begrenset til hendelser som vil kunne få alvorlige konsekvenser for Fredrikstad kommune eller innbyggerne. Konsekvenser kan være av økonomisk art, driftsmessig art

[8] Telekommunikasjon og IKT-systemer.
[9] Digitaliseringssjef informerer om at slike analyser er gjennomført siden 90-tallet.

eller at ansattes eller innbyggeres personopplysninger kommer på avveie. Å utelukke sikkerhetsbrudd av denne type 100 % vil være vanskelig å oppnå og særdeles kostbart. Det vil derfor være nødvendig å akseptere en viss risiko, samtidig som kommunen skal ivareta innbyggernes lovfestede rettigheter til vern av personopplysninger.

Følgende hendelser er risikovurdert:
- Datainnbrudd og skadeverk
- Menneskelig svikt
- Teknisk svikt
- Utroskap, misbruk av stilling

Vurderingen bygger på nå-situasjonen med de eksisterende tiltak, samt eventuelle nye tiltak som vil kunne føre til en forbedret sikkerhet. Analysen viser at kommunen har en rekke eksisterende tiltak som bidrar til å redusere risikoen for svikt. På enkelte områder er det avdekket en risiko som kan aksepteres dersom det finnes enkle tiltak. Men det er ikke avdekket risiko som ikke kan aksepteres. Nye tiltak skal saksbehandles i linjen og må vurderes opp mot effekt og kostnader, og beslutning må tas av digitaliseringssjef.

Kommunen har også til hensikt å utarbeide mer detaljerte tiltakskort[10] på dette området. Det vil være hensiktsmessig å bruke ROS-analysen som et verktøy for å følge opp, øke bevisstheten, og dokumentere at arbeid med IT-sikkerhet blir fulgt opp.

Planer

Kommunen opplyser om at de anser beredskapen ivaretatt gjennom vedlikehold av infrastruktur og nettverk, samt i «Beredskapsplan for alvorlige driftssituasjoner»[11]. Kommunens definisjon av en alvorlig driftsforstyrrelse er:

«En alvorlig driftsforstyrrelse innebærer at en vesentlig del av brukere ikke kommer inn på kommunens IT-systemer eller at en vesentlig del av tjenestene ikke fungerer og at dette ikke kan løses innen rimelig tid.»

Hensikten med beredskapsplanen er å få en optimal arbeidsflyt for å etablere normal driftsituasjon så raskt som mulig. Ved alvorlige driftssituasjoner skal det blant annet utnevnes en informasjonsansvarlig som har ansvar for å gi informasjon til alle ansatte ved virksomhet digitalisering og legge ut driftsmelding på Frekit. Informasjonsansvarlig skal også be kommunikasjon og service om å legge ut en driftsmelding på Frekit og kommunens hjemmesider dersom feilen antas å bli langvarig, og be de vurdere behov for å informere pressen.

Ifølge kommunen er de ansatte gjort kjent med beredskapsplanen gjennom virksomhet digitaliserings informasjonsaktiviteter. Kommunen jobber nå med en beredskapsplan for IKT-sikkerhetsmessige hendelser og situasjoner, som er basert på gjennomført ROS-analyse. På tidspunkt for revisjon er denne ikke ferdigstilt.

[10] Konkrete tiltak for å håndtere uønskede hendelser dokumenteres i tiltakskort. Tiltakskortene er scenariobaserte og bygger på ROS-analysen. Tiltakskortene er ikke utfyllende, men skal være representative for de mest relevante krisene som kan ramme kommunen. Tiltakskortene er forhåndsklarerte og kan iverksettes uten videre tillatelser på det nivået arbeidet ligger. Et tiltakskort er en oversikt over tiltak som på forhånd er identifisert og som må iverksettes når det inntreffer en hendelse. Tiltakskortene skal inneholde beskrivelser av hva som skal gjøres og hvem som skal varsles. (forvaltningsrevisjonsrapport Ekstremvær, 20. september 2019).
[11] Dokumentet er utarbeidet i februar 2007 og revidert i 2010, 2013, 2014, 2018, og sist 22. oktober 2019.

Når det gjelder gjenoppretting etter driftsstans informerer kommunen om at de har en rekke prosedyrer tilhørende ulike driftsstans-kategorier. Prosedyrene er tekniske og inneholder også informasjon om hvordan organisasjonen skal reagere og arbeide.

Kommunen informerer videre om at helse- og omsorgstjenester er prioritert ved eventuell driftsstans.

Varsling om sikkerhetshendelser

I henhold til kommunens retningslinjer for personvern og informasjonssikkerhet skal avviksbehandling iverksettes ved brudd på sikkerhetstiltak og/eller når oppgaver er utført i strid med de rutiner som er besluttet. Alle medarbeidere er ansvarlig for å melde avvik ved å bruke kommunens avviksmodul i kvalitetssystemet. Avvikene vil da behandles av nærmeste leder. Det fremgår av retningslinjene at det er utarbeidet egen prosedyre for avviksbehandling informasjonssikkerhet. Revisjonen har fått forelagt prosedyren *Avvik personvern.*

Her fremgår blant annet at ved brudd på informasjonssikkerheten som har medført uautorisert utlevering av sensitive personopplysninger, eller ved mistanke om slik utlevering, skal avviket straks meddeles personvernombudet som meddeler videre til Datatilsynet. Dette skal gjøres innen 72 timer. De berørte parter skal også varsles. (f.eks. innbygger/ansatt). Grove brudd som blir meldt til datatilsynet skal drøftes i sikkerhetsutvalget. Prosedyren nevner ikke varsling til SRM (sektorvise responsmiljøer)[12], samarbeidende virksomheter eller NSM (nasjonal sikkerhetsmyndighet).

Daglig ansvarlig og drift- og utviklingssjef skal fortløpende vurdere videre tiltak, eksempelvis kontakte leverandør ved behov. Eksternt vil det etter alvorlighetsgrad kunne være nødvendig å involvere særlig helsenettleverandør[13], informasjonsleverandører, osv.

Kommunen informerer om at de varsler Datatilsynet ved grove sikkerhetsbrudd, og at de har dialog med Politiet og NSM. De vurderer også om det er behov for bistand fra andre ved sikkerhetshendelser, og avtaler i slike tilfeller med NSM og helseCERT. Kommunen samarbeider med Politiets sikkerhetstjeneste ved behov.

3.3. Vurderinger

Ansvaret for drift og vedlikehold av kommunens IT-systemer ligger til virksomhet digitalisering, med digitaliseringssjef som virksomhetsleder.

Vi mener det er bra at kommunen har gjennomført ROS-analyse for IT-sikkerhet. Analysen omhandler sikkerhet for egne data og systemer hvor driftsansvar ligger hos virksomhet digitalisering. Analysen ble avsluttet i juni 2019, og er begrenset til hendelser som vil kunne få alvorlige konsekvenser for kommunen eller innbyggerne. Konsekvenser av økonomisk eller driftsmessig art, samt personopplysninger på avveie, er vurdert i analysen.

Revisjonen finner det positivt at analysen viser at kommunen har en rekke eksisterende tiltak som bidrar til å redusere risikoen for svikt, og at det ikke er avdekket risiko som ikke kan aksepteres. Vi er også positive til opplysningen om at kommunen har gjennomført slike analyser siden 90-tallet.

[12] For nærmere informasjon om SRM, se utledning av revisjonskriterier.
[13] Norsk helsenett. Leverandør som jobber for at all helseinformasjon alltid skal være trygg og tilgjengelig.

Kommunen opplyser om at de anser beredskapen ivaretatt gjennom vedlikehold av infrastruktur og nettverk, samt i «Beredskapsplan for alvorlige driftssituasjoner». Når det gjelder gjenoppretting etter driftsstans informerer kommunen om at de har en rekke prosedyrer tilhørende ulike driftsstans-kategorier, og at helse- og omsorgstjenester er prioritert ved eventuell driftsstans. Etter revisjonens oppfatning er det positivt at kommunen har beredskapsplan for driftssituasjoner, og at virksomhet digitalisering formidler informasjon om denne gjennom sine informasjonsaktiviteter. Vi finner det likevel mangelfullt at kommunen foreløpig ikke har en beredskapsplan basert på gjennomført ROS-analyse. Revisjonen finner det imidlertid positivt at kommunen har flere prosedyrer for å håndtere driftsstans, og at de prioriterer helse- og omsorgstjenester i slike tilfeller.

Etter revisjonens oppfatning har kommunen retningslinjer og prosedyre som omhandler varsling fra ansatte i kommunen – både for generell varsling, og for varsling innen informasjonssikkerhet. Det er mangelfullt at kommunens rutiner ikke inneholder punkter om varsling til SRM, andre virksomheter eller NSM, men ifølge kommunen er dette forhold de uansett vurderer. Revisjonen mener at dette med fordel kunne vært nedfelt i skriftlige rutiner.

4. SIKKERHETSTILTAK

Har kommunen etablert tilfredsstillende sikkerhetstiltak av sine datasystemer mot cyberangrep?

4.1. Revisjonskriterier

Revisjonen har utledet følgende kriterier for å besvare denne problemstillingen:

Kommunikasjon

- Kommunens prosess for risikostyring, ansvar for denne og rapporteringslinjer til øvre ledelse er kjent.
- Kommunens ledelse kommuniserer krav og forventninger til sikkerhet på en tilgjengelig og forståelig måte til sine ansatte.

Soner

- Kommunen har oversikt over hvor viktige data lagres og hvem som har tilgang til disse dataene.

Anskaffelse

- Kommunen stiller krav om sikkerhet ved anskaffelse av digitale produkter og tjenester.

Konfigurering og endringer

- Kommunen konfigurerer enheter som skal kobles til kommunens nett. Program- og maskinvare oppdateres kontinuerlig, og kjøring av ikke-autoriserte programmer er blokkert.
- Unødvendig kode og makroer deaktiveres i autoriserte programmer/applikasjoner.
- Kommunen bruker sikker oppstart.
- IKT- systemet overvåkes og analyseres, endringer er planlagt og dokumentert, og viktige logger gjennomgås jevnlig.

Brannmur og antivirus

- Kommunen loggfører nettverkstrafikk.
- Uønsket/ubedt trafikk blokkeres av brannmur/klientbrannmur og loggfiler gjennomgås jevnlig.
- Kommunen bruker antivirus/antiskadevare og har kodebeskyttelse mot ukjente sårbarheter.

E-post og kryptering

- Kommunen har beskyttet sin e-post kommunikasjon, og krypterer informasjon på bærbare medier og ved oversendelse på nett.

Passord og tilgang

- Kommunen setter krav til passordstyrke, og bruker 2-faktor autentisering.
- Sluttbrukere har ikke administratorrettigheter og kommunen gjennomgår jevnlig tilgangsrettigheter.

Fysisk tilgang

- Fysisk tilgang til nettverk- og informasjonssystemer er tilgangsstyrt.

4.2. Fakta

Kommunikasjon

Kommunen publiserer rutiner, prosedyrer, retningslinjer o.l. i sitt kvalitetssystem. Virksomhet digitalisering informerer om at de jobber med å få ut alle relevante dokumenter på IT-området, men at de ikke er helt i mål med hvilken struktur de ønsker. Det ble lansert et nytt kvalitetssystem tidligere i 2019, og det gjenstår en del arbeid med å flytte over og rydde i dokumenter.

Kommunen informerer om at de har rutiner og prosess for risikostyring i sitt kvalitetssystem.

Det fremkommer av retningslinjer for personvern og informasjonssikkerhet – ansatte, at alle kommunens medarbeidere som behandler personopplysninger skal kjenne til kommunens kvalitetssystem for informasjonssikkerhet og personvern. Herunder hvem som har ansvar for hva i sikkerhetsarbeidet. Retningslinjene sier også at alle medarbeidere har et viktig ansvar for å melde avvik i tråd med kommunens rutiner for avvikshåndtering.

Videre står det i retningslinjene at de dokumenterte og detaljerte sikkerhetsprosedyrene i kommunen kan finnes i kvalitetssystemet, fellesdokumenter, informasjonssikkerhet på kommunens intranett. Som medarbeider er de ansatte forpliktet til å sette seg inn i gjeldende prosedyrer, og holde seg oppdatert på nye retningslinjer/prosedyrer.

Kommunen har mange rutiner/retningslinjer som omhandler IT-sikkerhet og informasjonssikkerhet. Rutinene/retningslinjene er delvis overlappende og det kan være vanskelig å få oversikt. Flere av rutinene er også under revisjon.

Revisjonen har fått opplyst at informasjon fra virksomhet digitalisering til de ansatte i hovedsak går gjennom meldinger på kommunens intranett, og i rådmannens nyhetsbrev som går ut til alle ansatte i kommunen.

Nyansatte i kommunen må gjennomføre et elektronisk plattformkurs (e-kurs). Det fremkommer av «Rutine for elektroniske plattformkurs» at kurset er forankret i kommunens rutiner for informasjonssikkerhet og er utarbeidet av IT-service. Kurset består av viktig informasjon, og en quiz som må være besvart riktig for at kurset blir registrert som gjennomført.

På intranettet, under siden til IT-service, kan de ansatte finne informasjon om IT-service og hvordan de kan ta kontakt. Her finner man også en kunnskapsbase med informasjons- og læringssekvenser for IT-relaterte problemstillinger. Det er laget sekvenser om blant annet spam, phishing, hvordan konfigurere e-post, hvordan håndtere utrangert datautstyr mm.

Utover dette, legger kommunens ledelse til at oppfølging av krav og forventninger til sikkerhet fortrinnsvis skal følges opp i lederlinjene gjennom lederdialogen. I tillegg har kommunen nylig hatt fokus på krav og forventninger til sikkerhet ved at de har hatt en gjennomgang med oppfølging av ansatte som ikke har deltatt på obligatorisk plattform kurs.

Soner

Kommunens virksomhet er delt inn i flere soner. Det er blant annet en lukket internsone, et brukersegment, egne segmenter for spesialiserte tjenester, mm. Mellom segmentene er det brannmurer med antiskadevare- og trusselbeskyttelse. Alle virksomheter med egen lokasjon har egne brannmurer internt. Printerne er også segmenterte, og de ansatte legger selv til skrivere dersom de har behov for det. Revisjonen har fått forelagt en oversikt over brannmur-soner og tilganger fra brukere og internett.

Når det gjelder sensitive opplysninger er disse lagret på servere i lukket sone. Det er kun begrensede tilganger til lukket sone, og det er kun spesifikke systemer som har tilgang til data som lagres her. Datamaskinen den ansatte jobber på har ikke direkte tilgang til lukket sone, men har tilgang til f.eks. en terminalserver som igjen har tilgang til den lukkede sonen. Når man er logget på en terminalserver til lukket sone, er det heller ikke mulig å skrive til en printer som befinner seg utenfor lukket sone.

Anskaffelse

En leverandør som skal besvare et anbud etter en forespørsel fra kommunen, må innrette seg etter de krav og spesifikasjoner som fremkommer i «Kravspesifikasjon, standarder for IKT». Dokumentet stiller en rekke detaljerte krav til systemer som eventuelt skal implementeres i kommunen.

Det er flere krav i dokumentet, blant annet krav til type plattform, databasestandarder, kommunikasjonsprotokoller, dokumentasjon, fysisk installasjon, distribusjon og publisering av programvare, og sikkerhetsarkitektur. Kommunen stiller også krav til garantier fra leverandøren.

Konkret når det gjelder sikkerhet fremkommer det i kravspesifikasjonen at NSMs «Grunnprinsipper for IKT-sikkerhet» skal etterleves, i tillegg til Datatilsynets krav og retningslinjer.

Konfigurering og endring

Prosedyren «Oppgradering og vedlikehold av programvare» skal sikre at kommunen kun bruker godkjente programversjoner ved oppgraderinger, at oppsett og konfigurering av utstyr med oppgradert programvare skjer på riktig måte, og at oppgradert programvare ikke tas i bruk før driftstesting og godkjenning er gjennomført.

Videre sier prosedyren at IT-sjef[14] skal godkjenne programvare som brukes til oppgraderinger, at IT-driftsansvarlig skal vurdere behov for gjennomføring av risikoanalyse og at fremgangsmåten ved oppgraderinger skal dokumenteres.

For å sikre at konfigurasjonsendringer er i samsvar med besluttet sikkerhetsstrategi, og at informasjonssystemet fungerer som forutsatt etter at endringen er gjennomført, har kommunen dokumentet «Konfigurasjonskontroll». Kun utstyr eller program som er eiet eller disponert av kommunen skal inngå i konfigurasjonen. Det gjelder også utstyr eller program som brukes på hjemmekontor.

Ifølge dokumentet er konfigurasjonen dokumentert i en oversikt, i form av konfigurasjonskart, som angir:

- koblinger mellom utstyr og program
- inndeling av informasjonssystemet i soner
- kommunikasjonspunkt for tilkobling til ekstern dataoverføring
- sikkerhetsfunksjoner med opplysninger om oppsett/innstilling av utstyr/program
- opplysninger om vedlikehold, skade, funksjonsfeil, reparasjoner

Virksomhet digitalisering har oversikt over kommunens infrastruktur, med alle lokasjoner og komponenter. De har også en egen database hvor all programvare, alle servere i de ulike sonene, hvilke som har ansvar for de ulike systemene mv., er registrert. Ifølge kommunen har de også en mengde tekniske konfigurasjonstegninger, over både infrastruktur og programvareinstallasjoner.

[14] Tilsvarer digitaliseringssjef med dagens organisering.

Backup og restore sørger for at kommunen kan bygge opp systemene på nytt dersom noe skulle være galt med systemene. Kommunen har en egen rutine som beskriver hyppighet og type av backup som kommunen utfører. Ved inkrementell backup, som gjøres hver natt, sendes det rapport til ansvarlig medarbeider.

Konfigurasjonskontrolldokumentet sier videre at konfigurasjon av datasystemer ikke skal skje uten at IT-sjef har godkjent endringen – det gjelder både for maskinvare, programvare og systemer. Endringer skal utføres planmessig og systematisk, og bare etter godkjenning fra virksomhetens ledelse. Prosedyren fastslår videre at sikkerhetsmessige hensyn alltid skal tas, og beskrives, ved endringer. Det gjelder for eksempel backup, beredskapsplaner, autorisasjon og lignende. Også endringens konsekvenser skal beskrives, herunder hvem som blir berørt av endringen.

Ved endringer i programmer/systemer informerer sikkerhetsrådgiver om at praksis er at endringer godkjennes av driftssjef før de implementeres i kommunens systemer. Kommunen bruker et fagsystem for endringshåndtering for å dokumentere risikovurderinger og type endringer. I systemet ligger det en mal for endringer som krever informasjon om hvorfor endringen bør gjøres, hvem som ønsker endringen gjennomført, retrettmulighet (mulighet til å gå tilbake til tidligere versjon dersom oppdateringen/endringen ikke virker som forutsatt), dato for utføring og hvem som skal gjennomføre endringen. Endringshåndtering loggføres i fagsystemet.

Virksomhet digitalisering klargjør og registrerer alle nye maskiner som skal kobles på kommunens nett. De sjekker at alt fungerer som det skal, og at riktige versjoner av programvare er på plass. Siden sommeren 2016 har avdelingen satt opp alle nye maskiner, og eldre maskiner som settes opp på nytt, med sikker oppstart. Sikker oppstart kan hindre uønsket programvare fra å starte opp sammen med systemet. Uønsket programvare er programvare som har til hensikt å skade eller infiltrere maskinen, og som brukeren selv ikke er klar over/ønsker.

Videre informerer kommunen om at de bruker Microsoft konfigurasjonsmanager for å sende ut sikkerhetsoppdateringer. Alle Microsoft oppdateringer blir tvunget igjennom når de kommer, og øvrig programvare kan oppdateres gjennom programvaresenteret. Ifølge kommunens kravspesifikasjon oppdateres operativsystem gjennom konfigurasjonsmanageren en gang pr. måned. Virksomhet digitalisering styrer alle Windows og programvareoppdateringer på kommunale maskiner.

Kommunen har blokkert alle eksekverbare[15] filer for nedlasting fra nett. Det er anledning for ansatte til å be om midlertidig tilgang til filnedlasting (nærmere omtalt i avsnittet «passord og tilgang»). I vedlegg som kommer fra usikre kilder har kommunen også sperret for makroer[16].

Virksomhet digitalisering har endringsrutiner, med blant annet en mal for hvordan de skal vurdere behov for endringer – herunder størrelse på endringer, og hvilke konsekvenser endringen vil ha. Samtlige endringer registreres i endringshåndteringssystemet, men det er ikke behov for behandling i driftsmøte dersom det er snakk om mindre endringer. Virksomheten har driftsmøter tre ganger i uken hvor de behandler forslag til endringer.

Noen av systemene har egne test-baser, men utover dette har ikke kommunen dedikerte testmiljøer. En del endringer/implementeringer blir testet ut litt og litt (eks. ved i første omgang å rulle det ut til en avgrenset del av brukerne), men ikke i et eget testmiljø. Testmiljøer krever duplisering av

[15] Utførbare filer. Filer som inneholder program/kode som kan kjøres på en datamaskin. Dette i motsetning til en ren datafil som inneholder informasjon.
[16] En serie kommandoer og instruksjoner (kode) som er gruppert sammen til en kommando for å utføre en oppgave automatisk.

systemer. Dette er dyrt, ressurskrevende og vanskelig gjennomførbart. Men alt som skal direkte til brukere må testes på forhånd. Kommunen tar jevnlig øyeblikksbilder av systemene sine, slik at de kan gå tilbake til en tidligere versjon dersom det viser seg at en oppdatering/endring ikke fungerte som forutsatt.

Overvåking av IKT-systemer foregår på flere måter. Brannmurer har automatiske varsler, og sender ut e-post når det dukker opp kritiske innslag. Kommunen får også rapporter fra både HelseCERT og Allvis NOR (avtalene er nærmere beskrevet i neste avsnitt, om brannmur og antivirus). Kommunen går gjennom logger i brannmur dersom det er mistanke om forhold som krever oppfølging. Loggene gjennomgås ikke systematisk, men kommunen får automatiske varsler fra filtre i brannmuren. Loggene analyseres automatisk og fortløpende av brannmurmekanismer. I tillegg til logger i brannmur er det en sikkerhetslogg i windowsmiljøet, og i windows antivirus/antiskadevare programvaren. Videre er det logg på e-post systemet, og i fysiske låsesystem.

Ifølge dokumentasjon for Tilgangsportalen blir alle endringer som gjøres i Tilgangsportalen logget. For hver aksjon som blir foretatt går det en e-post til en egen postboks, og alle endringer kan spores her. Dokumentasjonen viser også at systemet sender e-post til løsningsansvarlig ved fjerning av tilganger. Backupsystemet sender ut meldinger om status etter gjennomført backup, og kommunen følger opp ved feilmeldinger.

Brannmur og antivirus

Prosedyren «Antivirusprogram» har som formål å sikre persondataenes integritet og tilgjengelighet, ved hjelp av beskyttelse mot ødeleggende program (eksempelvis virus) i informasjonssystemet. Antivirusverktøy skal brukes for kontroll av arbeidsstasjoner og servere (filserver, e-postserver etc.) og i tilknytning til eventuell brannmursfunksjonalitet.

Ifølge prosedyren er det IT-sjef som skal tilrettelegge tekniske tiltak og sørge for installasjon av programvare som kan avvise, oppdage og fjerne ødeleggende program, samt fastlegge rutiner som hindrer tilstedeværelse av ødeleggende program i informasjonssystemet.

Aktiviteter som skal gjennomføres i henhold til prosedyren:

- Installere tekniske sikkerhetsbarrierer som skal gjøre det mulig å hindre utførelse av program som automatisk overføres fra eksternt datanett
- Gjøre oppdateringer av de siste sikkerhetspatcher for brannmur og operativsystem og sikkerhetsbarrieren skal være motstandsdyktig mot tjenestenektangrep (Denial of Service)[17]
- Installere antivirusprogram på alle servere, klienter og frittstående PC-er. Virusprogram skal oppdateres regelmessig i samsvar med retningslinjer fastlagt av IT-driftsansvarlig.

Kommunens brannmur er levert av tredjeparts leverandør, med god kompetanse på området. Brannmurene har flere funksjoner. De varsler for eksempel om mulige trusler basert på kjente IP-adresser[18], «virus-signaturer» mv. I brannmuren er det satt opp regler for håndtering av trafikk, som for eksempel at kommunen kun tillater inngående trafikk med https. Https betyr at trafikken er kryptert mellom avsender og mottaker. Brannmuren tillater deling av skjerm, men blokkerer fjernstyring av pc. Det er også en egen funksjon i muren som håndterer tjenestenektangrep. Eksempelvis om det kommer mye trafikk fra en og samme IP-adresse, eller det ser ut til at noen prøver å overbelaste serveren, vil denne trafikken droppes for å unngå overbelastning av systemet.

[17] Et angrep hvor angriperen forsøker å hindre at legitime brukere får tilgang til en tjeneste eller informasjon.
[18] En unik adresse som tildeles en enhet, for eksempel en PC eller en skriver i et datanettverk.

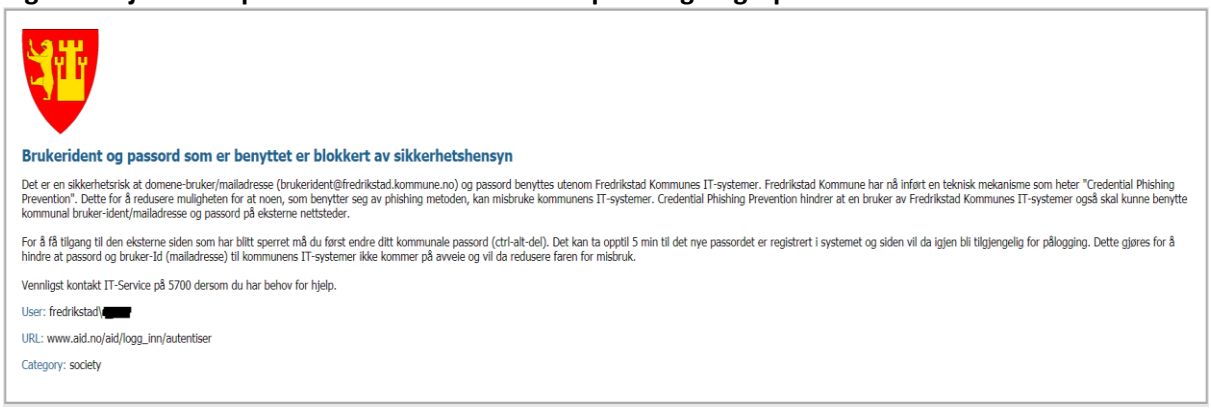
Kommunen dekrypterer i hovedsak all internettrafikk, og skanner den for skadevare[19]. Dersom det oppdages mistenkelig trafikk sendes trafikken gjennom WildFire[20], i tillegg til at trafikken går til mottaker. Dersom det viser seg at mistanken om skadevare er riktig, får kommunen beskjed om at en maskin kan være infisert.

Brannmuren oppdateres hvert femte minutt, med oppdaterte lister over uønskede IP-adresser, «virus-signaturer» mv.

Revisjonen har fått forelagt en oversikt over kommunens brannmur og «demilitariserte soner»[21], samt oversikt over kommunens sikkerhetssoner.

Tidligere i 2019 innførte kommunen også tiltak mot phishing. Tjenesten leveres av samme leverandør som leverer brannmurer til kommunen. Tiltaket har til hensikt å stoppe ansatte fra å logge på andre nettsider med samme brukeridentitet og passord som de bruker i kommunen. I de tilfeller en ansatt prøver seg på dette vil innloggingen bli blokkert, og brukeren vil få opp en advarsel med informasjon om hvorfor siden er blokkert, og at passordet til kommunens systemer må endres. Figuren nedenfor viser en skjermdump av hvordan denne advarselen ser ut.

Figur 4: Skjermdump sikkerhetsmekanisme mot phishing-angrep.



Kommunen benytter seg av tjenesten Allvis NOR. Dette er en tjeneste NSM tilbyr for å bedre sikkerheten i offentlige virksomheter og eiere av kritisk infrastruktur. I hovedsak består tjenesten av regelmessig kartlegging og sårbarhetsundersøkelse av utvalgte IP-adresser som er tilgjengelige på internett. Gjennom avtalen får Allvis NOR all metadata[22] om internettrafikk som går ut og inn i kommunen. Til gjengjeld får kommunen informasjon om hva tjenesten eventuelt oppdager.

Kommunen har også en avtale med HelseCERT[23]. HelseCERT har en oversikt/liste over domenenavn og IP-adresser som anses som ondsinnede/forsøk på svindel. Listen går direkte til kommunens brannmur som oppdateres automatisk. Listene oppdateres hvert femte minutt.

Avtalen gir videre HelseCERT utvidede rettigheter i kommunens systemer – de skanner alle systemer og servere og sjekker om systemene svarer på protokoller de ikke skal svare på, om det brukes utdaterte versjoner mv. Kommunen får månedsrapport med sårbarhetsoversikt for tjenester

[19] Samlebetegnelse for ondsinnet programvare. Eks. datavirus, ormer, trojanere, spyware, adware osv.
[20] En skybasert tjeneste som tester ut den mulige ondsinnede programvaren i et lukket, virtuelt miljø.
[21] Også kalt DMZ. Et fysisk eller logisk subnett som offentliggjør en organisasjons offentlige tjenester mot internett. Har til hensikt å sørge for at hackere ikke skal få tilgang til hele kommunens nettverk, dersom de klarer å komme seg inn til en maskin som er tilgjengelig fra internett.
[22] Data som definerer/beskriver annen data.
[23] Se nærmere omtale i utledning til revisjonskriterier.

eksponert på internett. Dersom det er gjort kritiske funn får kommunen beskjed med en gang. Revisjonen har fått kopi av en slik rapport fra HelseCERT. Rapporten gir informasjon om hvilke tjenester det er funnet sårbarhet ved, og hva slags sårbarheter det er snakk om.

Lokalt på stasjonære og bærbare maskiner bruker kommunen Windows defender som antiskadevare-beskyttelse. Programvaren oppdateres kontinuerlig.

E-post og kryptering

Kommunen har flere ledd med kontroll knyttet til e-post. All post som kommer utenfra kommunens nettverk blir skannet av et antivirusprogram som ser etter kjente uønskede avsendere, signaturer eller linker, og som stopper mistenkelig trafikk. I neste trinn blir e-posten skannet av kommunens brannmur, på samme måte som omtalt i avsnitt om brannmur og antivirus, før den til slutt er gjenstand for kommunens egen antivirus og skadevare-skanning i Exchange[24]. Kommunen fjerner alle vedlegg som inneholder eksekverbare[25] filer.

På tidspunkt for revisjon har ikke kommunen implementert DMARC[26] for sikring av sin e-post-kommunikasjon. Kommunen har planer om å implementere ytterligere sikkerhetsmekanismer for sikring av e-post kommunikasjon. Det finnes alternativer til DMARC, og det er ikke avklart om kommunen vil ta i bruk DMARC eller tilsvarende sikkerhetsmekanismer.

Når en ansatt kobler seg opp med mobilt kontor (bærbar maskin) kobler maskinen til kommunens nettverk gjennom en VPN-løsning[27] fra samme leverandør som leverer kommunens brannmurer. Mobilt kontor gir samme sikkerhet som om man fysisk sitter på en maskin på innsiden av kommunens nettverk. Bærbare medier er satt opp til først og fremst koble seg på kommunens eget trådløse nett for ansatte.

Som det fremkommer i forrige avsnitt er all trafikk fra bærbare medier kryptert gjennom bruk av VPN. Kommunen krypterer ikke harddisker, verken på bærbare medier eller øvrige maskiner.

I prosedyren «Passord» står det at når det gjelder løsninger med nettverksforbindelse er det blant annet krav til at dersom det skal lagres sensitive personopplysninger på bærbar arbeidsstasjon, skal harddisken på disse maskinene automatisk krypteres.

I «retningslinjer for personvern og informasjonssikkerhet – ansatte» fremkommer det, under avsnitt om taushetsplikt, at sensitive data ikke skal lagres elektronisk andre steder enn på sentral server. Kommunen anser det som generelt større risiko for at noen bryter seg inn i kommunens systemer fra internett, enn at noen bryter seg inn i et serverrom for å stjele informasjon.

Det fremkommer videre fra dokumentet «Klienter» at lagring kun foregår mot kommunens servere, og at lagring av data lokalt på PC klienter ikke er støttet og gjøres eventuelt på eget ansvar.

Kommunens brannmur tillater kun inngående kommunikasjon med https over internett, som nevnt under avsnitt om brannmur og antivirus. Denne kommunikasjonen er kryptert.

[24] Microsofts e-post og kalenderløsning.
[25] Se tidligere beskrivelse, fotnote 8.
[26] Se nærmere beskrivelse i utledning av revisjonskriterier, DMARC.
[27] Virtual Private Network. Skaper en kryptert «tunnel» mellom maskinen og kommunens nettverk.

Passord og tilgang

Kommunens krav til passord omtales både i retningslinjer for personvern og informasjonssikkerhet – ansatte, og i egen prosedyre for passord.

Det fremkommer av retningslinjene at når en ansatt blir etablert som IT-bruker får vedkommende tildelt en brukeridentitet og et passord. Det tildelte passordet byttes til et selvvalgt passord ved førstegangs pålogging til kommunens systemer. Etter dette er det krav til bytte av passord etter maks 90 dager. Passordbytte er ivaretatt gjennom systemet, som minner de ansatte på å bytte passord når fristen nærmer seg. Brukere som ikke bytter sitt passord i tide, mister tilgang til IT-systemet. Når relasjonen til kommunen opphører, blir identitet og passord slettet.

I møte med kommunen er revisjonen gjort kjent med at når brukeridentitet og passord blir tildelt, får den ansatte standardtilgang til systemene. Deretter mottar brukeren et e-kurs pr. e-post, som alle nyansatte skal gjennomføre. Etter at e-kurset er gjennomført kan virksomhetsleder gi utvidede tilganger i systemene via kommunens tilgangsportal[28]. Det er mulig å gi utvidede tilganger i systemene uten at den ansatte har ferdigstilt e-kurset.

Det ligger til virksomhetsleder å følge opp at den ansatte gjennomfører e-kurset. I vår spørreundersøkelse spurte vi ansatte med myndighet til å gi tilganger til andre, hvor viktig de mener det er at de ansatte faktisk har gjennomført e-kurset før de gis utvidede tilganger. Figuren nedenfor viser resultatet.

Figur 5: Hvor viktig mener du det er at den ansatte har gjennomført e-kurs før du tildeler tilgang?

Antall respondenter: 136

Figur 5 viser at 77,2 % av respondentene mener at det er viktig eller svært viktig at ansatte gjennomfører e-kurs før tilgang tildeles. Tilgangsbegrensninger og passord er nærmere regulert i prosedyren «Passord», som blant annet stiller minimumskrav til antall og typer av tegn i passord. Tilgangsbegrensninger ved hjelp av passord innen sone hvor sensitive data behandles har som formål å sikre at kun autoriserte medarbeidere får tilgang til data og programmer som er nødvendig ut fra sin stilling. Dette gjelder også for informasjon om sikring av slike opplysninger.

[28] Kommunens egenutviklede digitale plattform for å gi tilganger til ansatte.

Kommunen har 2-faktor autentisering på innlogging i ansattportalen – en nettbasert pålogging via VPN, til kommunens systemer. Det er også mulig for ansatte å bruke en nettbasert versjon av Outlook [29], hvor det ikke er tatt i bruk 2-faktor autentisering for pålogging. Kommunen har planer om å sperre for denne løsningen, og all tilgang som ikke skjer fra en fredrikstad-maskin må da gjøres gjennom ansattportalen.

Systemadministrator har administratorrettigheter i Microsoft-nettverket. Det er atskilt fra øvrige systemer, og dersom man har administratorrettigheter i ett system, eksempelvis Gerica[30] , gjelder ikke samme administratorrettigheter i et annet system.

Sluttbrukere har normalt sett ikke administratortilgang på egen maskin, og dermed ikke mulighet til å laste ned filer eller installere programvare/applikasjoner utover det som er tilgjengelig i programvaresenteret i Windows. Ved behov er det mulig å be om midlertidig administratortilgang og filnedlastingsrettigheter, men brukeren blir da informert om at det er på eget ansvar. Slik utvidet tilgang nullstilles etter kort tid.

I «retningslinjer for personvern og informasjonssikkerhet – ansatte», under avsnitt om utvidede rettigheter, fremkommer det at enkelte brukere, f.eks. løsningsansvarlig, har utvidede rettigheter på dataanlegget for å administrere anlegget eller tilhørende programvare. Slike rettigheter er knyttet til en egen brukerkonto med spesielle egenskaper. Slike kontoer skal kun benyttes til å administrere den delen av anlegget som er tiltenkt, og ikke til vanlig bruk eller andre oppgaver.

De som har behov for det i kraft av sin stilling, får flere brukeridenter, med ulike nivå av tilgangsrettigheter – eksempel administratorrettigheter på server mv. Det er kun ordinær brukerident som brukes på egen maskin til ordinær bruk.

Kommunen bruker Microsoft Identity Management for håndtering av tilganger i sin tilgangsportal. Ved sluttmelding i Visma, vil blant annet den ansatte automatisk bli deaktivert i tilgangssenteret – og det vil ikke lenger være mulig å gi denne personen tilganger i tilgangsportalen.

Passord-prosedyren sier at det skal gjøres en periodisk revurdering av de enkelte medarbeideres behov for tilganger. I retningslinjer for personvern og informasjonssikkerhet fremkommer det at hvert større fagsystem har en løsningsansvarlig, og at ansvar for vedlikehold og ajourhold av tilganger ligger til denne rollen.

Kommunen informerer om at virksomhet digitalisering ikke gjør særskilte gjennomganger av de enkelte medarbeideres behov for tilganger. Det ligger til virksomhetsleder, og den som gir tilganger i tilgangsportalen å oppdatere tilganger for sitt ansvarsområde.

Leverandører kan også få tilgang til kommunens systemer. I så tilfelle må de inngå en avtale med kommunen. De får kun tilgang til de systemer de har behov for, og logger på via en VPN-løsning. Leverandørene må registrere når de logger ut, og informere kommunen om hva som er gjort i systemene. Leverandørtilganger er kun midlertidige.

[29] Kommunens e-postklient.
[30] Kommunens journalsystem for pleie- og omsorg.

Fysisk tilgang

Formålet til rutinen «Låserutiner og adgangskontroll» er å sikre konfidensialitet og integritet i kommunens data. Virksomhetens øverste leder skal vurdere behov for å innføre fysisk områdeinndeling av lokaler, og det kan være aktuelt å opprette områder med forskjellig grad av adgangskontroll innenfor samme enhet. Der publikum har adgang skal kommunen definere hvor man må ha adgangskontroll, og hvor man må bruke sikring på bruk av utstyr som pc, skriver o.l.

Rutinen fastslår at områder der kommunen behandler personopplysninger skal sikres, og at det kun er autorisert personell som har adgang til disse. Det betyr blant annet at områdene skal være kontrollert av adgangskontrollsystem, at det skal være skriftlig signering før ansatte får tildelt adgangskort og koder for adgang, og at datateknisk utstyr (pc, skriver o.l.) oppbevares i låste kontorer.

Ifølge rutinen er alle servere i kommunen som inneholder sensitive opplysninger fysisk plassert i godkjente datarom, beskyttet med kodelås. Koden blir skiftet etter faste rutiner. Lokalet er alltid avlåst når personell ikke er til stede, og rommet er fysisk sikret for adgang med blant annet gitter for vinduene. Det er automatisk brannslukningsanlegg på serverrom, og uautorisert personell skal alltid følges av autorisert personell. Ved forsøk på uautorisert adgang skal det meldes avvik.

Kommunen har flere serverrom, på ulike lokasjoner. Adgang til rommene styres gjennom kommunens generelle adgangssystem, det er ikke virksomhet digitalisering som styrer dette. Det er mulig å se hvem som kan gi tilgang til hva i systemet, og hvem som har brukt tilgangen sin i døren.

De som har administratorrettigheter i adgangssystemet har mulighet til å gi tilganger til alle områder/dører. Dette gjelder også for dører som ligger utenfor ansvarsområdet til den som tildeler rettigheter.

Videre fremkommer det at det pr. i dag er flere som har tilgang til datarom, hvor det ikke er virksomhet digitalisering som har gitt tilgang. Det ligger oversikt over de som har tilganger i adgangssystemet.

Rekognosering av kommunens hoved-domene

Kommunen har flere titalls tusen IP-adresser i store nettverksblokker, som gir mange inngangsmuligheter for potensielle dataangrep. Undersøkelsen viser at kommunen bruker en VPN-tjeneste som har hatt en del kjente kritiske sårbarheter. VPN-tjenester er tjenester som gjerne brukes for å beskytte datakilder som bør ha høy grad av beskyttelse, eksempelvis persondata.

Digitaliseringssjef har i møte informert revisjonen om at de kontinuerlig oppdaterer VPN-tjenesten, og at funnet ikke er en reell sikkerhetstrussel for kommunen.

Undersøkelsen viser også at kommunen ikke bruker de anbefalte prinsippene for beste praksis når det gjelder e-post-sikkerhet. Flere sikkerhets-protokoller/-teknologier mangler. Hvilke det er snakk om er spesifisert i rapporten.

Videre viser undersøkelsen at kommunen gir eksterne tilgang til oversikt over alle kommunens ansatte. Informasjon om personale kan potensielt brukes som mål for phishing-angrep, og forsøk på å få tak i brukeridentiteter og passord.

Kommunen er kjent med at det kan være en sikkerhetstrussel å offentliggjøre oversikt over sine ansatte, men av hensyn til åpenhet i offentlig sektor er dette et bevisst valg fra kommunens side.

Når det gjelder hvilke e-post-adresser kommunen og de ansatte bruker på internett, er det funnet 149 kommunale e-post/passord-kombinasjoner tilgjengelig på nett. Slike adresser og passord er enkelt å få tak i for uvedkomne. Et utvalg av de adressene dette gjelder er spesifisert i den detaljerte rapporten fra undersøkelsen.

Kommunen informerer i møte om at det er svært lite sannsynlig at det er brukerens kommunale passord som er brukt i disse kombinasjonene – og om det er det vil ikke passordet være gyldig til kommunens systemer i mer enn maks 3 måneder, som er intervallet for skifte av passord til kommunale systemer. Med kommunens nye tiltak mot phishing er det ikke lenger anledning til å bruke samme e-post/passord-kombinasjon som brukes til kommunens systemer.

Også kommunens og de ansattes bruk av sosiale medier har vært gjenstand for undersøkelsen. Det viser seg at Facebook er den mest brukte sosiale plattformen, og den som vil være den største sikkerhets-sårbarheten for kommunen.

Undersøkelsen viser at kommunen har applikasjoner for håndholdte enheter (Android og iOS)[31], som kan være sårbare innganger til kommunens systemer.

Kommunen informerer i møte om at de ikke har apper som går mot kommunens domene. De har en omfattende app knyttet til helsetjenester, men dette programmet kjører i lukket system og ikke på internett.

4.3. Vurderinger

Kommunikasjon

Revisjonens oppfatning er at kommunen gjennom kvalitetssystemer og retningslinjer for informasjonssikkerhet, kommuniserer til sine ansatte hvor de kan finne informasjon om kommunens prosess for risikostyring, herunder ansvar og avvikshåndtering/rapportering, og rutiner og retningslinjer. Det fremgår tydelig av retningslinjene at de ansatte selv har ansvar for å holde seg oppdatert på kommunens retningslinjer/prosedyrer.

Vår oppfatning er at kommunen kommuniserer krav og forventninger til sikkerhet på en tilgjengelig måte gjennom kvalitetssystemet, retningslinjer, intranettet og pr. e-post gjennom nyhetsbrev og e-kurs.

Oppfølging av krav og forventninger til sikkerhet skal fortrinnsvis følges opp i lederlinjene gjennom lederdialogen. Vår vurdering er at det er positivt at sikkerhet er forankret i kommunens ledelse.

Vi ser imidlertid at kommunens dokumentasjon på området er delvis overlappende, og flere dokumenter er under revisjon. Etter vår oppfatning kan det være vanskelig for ansatte å orientere seg i kommunens planer, rutiner og retningslinjer på området. Det er også uklart for revisjonen om alle de rutinene som er tilgjengelig faktisk er gjeldende, og det er etter vår vurdering en risiko for at rutinene har et ulikt eller utdatert innhold. Vår gjennomgang viser også at kommunen bør vurdere

[31] Operativsystemer som er mye brukt på mobiler/nettbrett.

sin begrepsbruk i rutinene. Etter vår oppfatning kan det eksempelvis se ut til at det er en sammenblanding av personvern og IT-sikkerhet i kommunens prosedyrer.

På denne bakgrunn kan revisjonen ikke si at kommunen i stor nok grad har kommunisert innholdet i kommunens sikkerhetsstyring på en tydelig nok måte slik at det er lett forståelig for de ansatte.

Soner

Kommunens virksomhet er delt inn i flere soner, atskilt med brannmurer. Kommunen lagrer sensitive opplysninger på servere i lukket sone, hvor kun spesifikke systemer har tilgang til dataene. Etter revisjonens oppfatning har kommunen god oversikt over hvor sensitive og viktige data lagres.

Anskaffelse

En leverandør som skal besvare et anbud etter en forespørsel fra kommunen, må innrette seg etter de krav og spesifikasjoner fremkommer i «Kravspesifikasjon, standarder for IKT». Dokumentet stiller en rekke detaljerte krav til leverandørens systemer, herunder at de etterlever NSMs «Grunnprinsipper for IKT-sikkerhet», og Datatilsynets krav og retningslinjer. På bakgrunn av dette mener revisjonen at kommunen er tydelige på at de stiller krav om sikkerhet til sine leverandører ved anskaffelse av digitale produkter og tjenester.

Konfigurering og endringer

Program- og maskinvare skal være oppdatert. Nyere produktversjoner har tettet flere sikkerhetshull enn eldre versjoner, og har ofte flere og bedre sikkerhetsfunksjoner. Vår vurdering er at når virksomhet digitalisering setter opp alle enheter som skal kobles på kommunens nett, sørger kommunen med dette for at alle enheter er konfigurert og oppdatert på tidspunkt for tilkobling. Vi finner det videre positivt at kommunen har rutiner for oppgradering og vedlikehold og konfigurasjonskontroll. Kommunen se setter nå opp alle maskiner med sikker oppstart. Dette er et viktig tiltak for å oppdage manipulering av oppstartsprosessen.

Kommunen bruker Microsoft konfigurasjonsmanager for å sende ut oppgraderinger, kjøring av ikke-autoriserte programmer er i hovedsak blokkert og oppdateringer skjer kontinuerlig. Gjennom dette er kommunens håndtering av sikkerhetsoppdateringer tilfredsstillende.

Gjennom bruk av programvaresenteret og blokkering av nedlastning/filvedlegg er det revisjonens oppfatning at kommunen deaktiverer unødvendig kode og makroer i autoriserte programmer/applikasjoner.

Rekognoseringen av kommunens hoved-domene viste at kommunen bruker en VPN-tjeneste som har hatt en del kjente kritiske sårbarheter, men digitaliseringssjef har informert revisjonen om at de kontinuerlig oppdaterer tjenesten, og at funnet ikke er en reell sikkerhetstrussel for kommunen. Revisjonens vurdering er at det viktigste for å unngå (vellykkede) angrep er hyppig oppdatering og tetting av sikkerhetshull – det vil alltid ligge en risiko for sårbarhet i de programvarer kommunen velger å bruke. Det er imidlertid anledning til å be om midlertidig tilgang til filnedlasting, noe som etter revisjonens oppfatning kan være motstridende med anbefalinger om å ikke installere mer funksjonalitet enn nødvendig.

Det er i tråd med grunnprinsipper for IKT-sikkerhet at virksomhet digitalisering planlegger og dokumenterer endringer gjennom sine rutiner for endringer, og loggføring av gjennomførte endringer i et eget fagsystem. Det er positivt at kommunen tar øyeblikksbilder av systemene, slik at de ved behov kan gå tilbake til en tidligere versjon.

Kommunens brannmurer har filtre som automatisk varsler om trusler. Kommunen får også rapporter fra HelseCERT og Allvis NOR. Allvis NOR overvåker all metadata om kommunens internettrafikk. Kommunen gjennomgår ikke logger i brannmurer systematisk, men de analyseres automatisk og fortløpende av brannmurmekanismer. I tillegg til logger i brannmur er det en sikkerhetslogg i windowsmiljøet, og i windows antivirus/antiskadevare programvaren. Videre er det logg på e-post systemet, og i fysiske låsesystem. Alle endringer i Tilgangsportalen blir logget, og kan spores i en egen postboks. Backupsystemet sender ut meldinger om status etter gjennomført backup. Basert på dette er det vår vurdering at kommunen har flere funksjoner som overvåker IKT-systemet, og som varsler kommunen ved mulige og oppdagede trusler. Kommunen loggfører aktivitet på flere områder, som e-post, nettrafikk, tilgangsportalen og backupsystemet. Det kan være en svakhet at loggene ikke gjennomgås jevnlig, men kun ved mistanke om forhold som bør følges opp.

Brannmur og antivirus

Som det fremkommer i forrige avsnitt, om konfigurering og endringer, loggfører kommunen nettverkstrafikk gjennom sin brannmur. Videre er det satt opp regler for håndtering av trafikk i brannmuren, hvor blant annet fjernstyring av pc blir blokkert. Muren har også en funksjon som spesielt er rettet mot håndtering av tjenestenektangrep. Revisjonens vurdering er at kommunens brannmur i stor grad blokkerer uønsket/ubedt trafikk. Men som nevnt ovenfor kan det være en svakhet at loggfiler ikke er gjenstand for jevnlig gjennomgang.

Brannmuren har installert antivirus, og lokalt på stasjonære og bærbare maskiner bruker kommunen Windows defender som antiskadevare-beskyttelse. Antivirus oppdateres jevnlig og kontinuerlig. Vi finner det positivt at kommunen har antivirus i brannmurer og lokalt på enheter.

Revisjonen har fått forelagt en oversikt over kommunens brannmur og «demilitariserte soner», samt oversikt over kommunens sikkerhetssoner. Oversikten viser at trafikk inn til kommunen i noen tilfeller passerer flere brannmurer for å komme igjennom. Etter vår oppfatning bidrar dette til økt sikkerhet, og øker sannsynligheten for at kommunen oppdager skadevare.

Kommunen har innført tiltak mot phishing, og de har avtaler med HelseCERT hvor de blant annet får informasjon om domenenavn og IP-adresser som anses som ondsinnede/forsøk på svindel og sårbarhetsoversikt over kommunens tjenester som er eksponert på internett, i tillegg til tidligere nevnte avtale med Allvis NOR. Dataangrep de senere årene har dreiet mer mot sosial manipulasjon av ansatte/brukere av systemer, mer enn direkte angrep på systemene. Etter revisjonens oppfatning er det positivt at kommunen har innført egne tiltak mot phishing, for å forsøke å beskytte seg mot slike trusler.

På bakgrunn av fremlagt fakta er det revisjonens oppfatning at kommunen i stor grad sikrer seg mot skadevare og ukjente sårbarheter gjennom bruk av antivirus i sin brannmurfunksjonalitet, og lokalt på enheter knyttet til kommunens nett, samt gjennom phishing-tiltak og avtaler med eksterne parter.

E-post og kryptering

Kommunen har flere ledd med kontroll knyttet til e-post. All post som kommer utenfra kommunens nettverk blir skannet av et antivirusprogram, av kommunens brannmur, og i Exchange. Alle vedlegg med eksekverbare filer fjernes. Kommunen har også planer om å implementere ytterligere sikkerhetsmekanismer for sikring av e-postkommunikasjon.

Etter revisjonens oppfatning har kommunen beskyttet sin e-post kommunikasjon i flere trinn. Vi registrerer at kommunen på revisjonens tidspunkt ikke har beskyttet e-post med DMARC. Rekognosering av kommunens hoved-domene viste også at kommunen ikke bruker de anbefalte prinsippene for beste praksis når det gjelder e-post-sikkerhet. Flere sikkerhets-protokoller/-teknologier mangler. Kommunen har også planer om å implementere ytterligere sikkerhetsmekanismer i nær fremtid – noe revisjonen vurderer som et godt tiltak for økt sikring av e-post kommunikasjon.

Kommunens retningslinjer og dokumentasjon sier at lagring kun skal foregå på kommunens servere, ikke lokalt på enheten, men revisjonens vurdering er at det kan være en risiko for at bærbare maskiner inneholder sensitiv informasjon som er lagret lokalt. Sett i lys av dette er det vår oppfatning at kommunen bør vurdere om det kan være behov for å kryptere noen bærbare maskiner – slik det fremkommer av prosedyren «Passord». Kommunen krypterer for øvrig sin kommunikasjon over nett, ved bruk av VPN-løsninger for nettbasert tilkobling, og ved at brannmuren kun tillater kommunikasjon med https over internett.

Passord og tilgang

Fakta viser at kommunen stiller krav til passordstyrke og varighet av passord, og at identitet og passord blir slettet når ansattes relasjon til kommunen opphører. Det er positivt at 2-faktor autentisering er tatt i bruk i ansattportalen, men det er mulig å bruke en webversjon av Outlook hvor dette ikke er tatt i bruk. Revisjonen oppfatter det som positivt at kommunen har planer om å sperre for denne løsningen, eventuelt bør kommunen vurdere å ta i bruk 2-faktor autentisering også her.

Alle nyansatte må gjennomføre et e-kurs, før de gis utvidede tilganger i kommunens systemer. Det er mulig å gi utvidede tilganger i systemene uten at e-kurset er ferdigstilt. I vår spørreundersøkelse kommer det frem at over 90 % av respondenter med myndighet til å gi tilganger mener det er litt viktig, viktig eller svært viktig at e-kurset er gjennomført før det gis utvidede tilganger. Kun 2,9 % mener at det ikke er viktig. Det ligger til virksomhetsleder å følge opp at e-kurset er gjennomført. Etter revisjonens oppfatning bidrar det til økt sikkerhet at ansatte må gjennomføre et e-kurs før de får utvidede tilganger i kommunens systemer, men det kan være en svakhet at det er mulig å gi slike tilganger uten at kurset faktisk er gjennomført. På den positive siden mener over 90 % i vår spørreundersøkelse at det er viktig at kurset er gjennomført før de gir tilganger, og vår vurdering er at dette reduserer risikoen for at det faktisk gis utvidede tilganger før e-kurset er gjennomført. Revisjonen mener imidlertid at det kan være en svakhet at det kun er virksomhetsleder som følger opp at e-kurset er gjennomført, og at kommunen bør vurdere implementering av systemkontroll for å sikre at kurset er gjennomført før det gis utvidede tilganger. Vi finner det positivt at det er automatikk i systemet, som fører til at ansatte deaktiveres i tilgangssenteret/tilgangsportalen ved sluttmelding i Visma.

Det er vår vurdering at det er risikoreduserende at kommunens systemer opererer atskilt ved at administratorrettigheter i ett system ikke automatisk gjelder i et annet. Videre er det revisjonens oppfatning at det kan være en sikkerhetsrisiko at samtlige brukere har mulighet til å få administratorrettigheter og filnedlastingsrettigheter på egen maskin. Det samme gjelder for tilganger

til eksterne leverandører. Vi anser risikoene som redusert ved at slik tilgang nullstilles etter kort tid. Vår vurdering er at det også er et godt sikkerhetstiltak at kommunen ved behov bruker flere brukeridenter til samme ansatt. Ved at den ordinære/daglige brukeridenten ikke har administratorrettigheter kan man unngå at det skjer utilsiktede feil.

Kommunen har retningslinjer for informasjonssikkerhet hvor det fremkommer at hvert større fagsystem har en løsningsansvarlig, og at ansvar for vedlikehold og ajourhold av tilganger ligger til denne rollen. Revisjonen har imidlertid fått opplyst fra kommunen at dette ansvaret ligger til virksomhetsleder, og den som gir tilgang i tilgangsportalen. Vår vurdering er at det kan være noe vanskelig å forstå hvem som faktisk har dette ansvaret, og som skal gjøre den jevnlige vurderingen av behov for tilganger. Vi mener at det kan være hensiktsmessig å vurdere behovet for en sentral oppfølging av at tilganger blir gjennomgått jevnlig.

Ved rekognosering av kommunens hoved-domene var flere kommunale e-post/passord-kombinasjoner tilgjengelige på nett. Kommunen har informert revisjonen om at det er lite sannsynlig at passordet i kombinasjonen tilsvarer brukerens kommunale passord – og om det er det vil ikke passordet være gyldig til kommunens systemer i mer enn maks tre måneder jf. passordprosedyre. Kommunens tiltak mot phishing forhindrer at den e-post/passord-kombinasjon som brukes til kommunens systemer, blir brukt andre steder på nett. Revisjonens vurdering er at risikoen for at riktig og gyldig e-post/passord-kombinasjon kommer på avveie, reduseres av phishing-tiltak og kommunens krav til hyppig endring av passord.

Fysisk tilgang

Fakta viser at kommunen har rutiner som sikrer at alle servere i kommunen, som inneholder sensitive opplysninger, er plassert i godkjente datarom. Datarommet er beskyttet med kodelås, fysisk sikring og alltid avlåst når personell ikke er til stede. Adgang til serverrommene er styrt gjennom kommunens generelle adgangssystem, slik at de som har administratorrettigheter i adgangssystemet også har mulighet til å gi tilganger til alle områder/dører.

Revisjonen anser det som en mulig svakhet at det ikke er virksomhet digitalisering som styrer systemet som fysisk sikrer kommunens servere. Vi er også av den oppfatning at det kan ligge risiko i at alle som har administratorrettigheter i adgangssystemet kan gi adgang til serverrom. Risikoen reduseres noe av at systemet loggfører aktivitet, men det kan være grunn til å vurdere om det er mulig å redusere risikoen ytterligere.

Annet

Rekognosering av kommunens hoved-domene viste at informasjon om alle kommunens ansatte ligger tilgjengelig på nett. Kommunen har opplyst revisjonen at dette er gjort av hensyn til åpenhet i offentlig sektor. Revisjonens vurdering er at selv om publisering av e-post adresser og navn er en mulig sikkerhetstrussel mot kommunens IKT-systemer, ser vi at dette også må vurderes opp mot grad av offentlighet/åpenhet.

Kommunen har Facebook som den mest brukte sosiale plattformen, og den som kan være den største sikkerhets-sårbarheten for kommunen. Kommunen har også applikasjoner for håndholdte enheter, som kommunen har opplyst revisjonen om at ikke går mot kommunens domene. Revisjonens oppfatning er at tilstedeværelse på sosiale medier alltid vil medføre en viss økt risiko for angrep, men risikoen må veies opp mot hvor kommunen ønsker å møte sine innbyggere, og hvor

innbyggerne befinner seg. Når det gjelder applikasjoner er vår vurdering at kommunen virker å ha kontroll på at det ikke er mulig å komme seg inn til kommunens systemer gjennom disse plattformene.

5. INTERNKONTROLL

Har kommunen etablert et tilfredsstillende styringssystem (internkontroll) for informasjonssikkerhet?

5.1. Revisjonskriterier

Basert på gjeldende regelverk, har revisjonen utledet følende kriterier for denne problemstillingen[32]:

- Det er fastsatt overordnede målsettinger for informasjonssikkerhet i kommunen.
- Det er utarbeidet en overordnet strategi for å nå målene på området.
- Strategien gjennomgås jevnlig, og oppdateres ved behov, for å sikre at den til enhver tid er i samsvar med kommunens behov.
- Det er etablert og beskrevet klare ansvars- og myndighetsforhold for kommunens informasjonssikkerhetsarbeid.
- Kommunen har rutiner og retningslinjer for risikovurdering og risikohåndtering knyttet til informasjonssikkerhet.
- Kommunen dokumenterer prosessene rundt risikohåndtering og resultatene fra håndtering av informasjonssikkerhetsrisikoene og resultat av korrigerende tiltak.
- Informasjonssikkerheten i kommunen overvåkes etter definerte mål og metoder, og resultatene analyseres og evalueres.
- På et overordnet nivå, følger kommunen opp at informasjonssikkerheten blir ivaretatt i tråd med lov og forskrift, og øvrig internt og eksternt regelverk på området.

5.2. Fakta

Sikkerhetsmål og strategi for informasjonssikkerhet

I IT-sikkerhetsreglement for Fredrikstad kommunes digitaliseringsavdeling fremkommer det at kommunens overordnede sikkerhetsmål er å ivareta konfidensialitet, integritet og tilgjengelighet for alle fysiske og elektroniske informasjonsverdier i institusjonen, for å sikre at regulative, virksomhetsmessige og kontraktsmessige krav blir oppfylt.

Kommunen har et dokument med mål for området[33]. Videre har kommunen et dokument hvor roller, myndighet og ansvar for personvern- og informasjonssikkerhetsarbeidet blir beskrevet, samt retningslinjer for personvern og informasjonssikkerhet (versjon 3 er sist godkjent i desember 2019).[34]

Ansvar og myndighet

I prosedyren «Organisering av personvern- og informasjonssikkerhetsarbeidet» fremkommer det at personvernombudet har ansvar for koordinering av sikkerhetsoppgavene i kommunen. Det betyr blant annet ansvar for kvalitetssikring av rutiner, ansvar for at avvikshåndtering iverksettes i de ulike enhetene, tilrettelegging av ledelsens gjennomgang, initiativtaker til egenkontroll og revisjon mm.

[32] Se vedlegg for utledning.
[33] «Sikkerhetsmål».
[34] «Organisering av personvern- og informasjonssikkerhetsarbeidet».

Rådmannen har det overordnede sikkerhetsansvaret, og skal utpeke medlemmer til sikkerhetsutvalget og personvernombud. Prosedyren legger også føringer for digitaliseringssjefens ansvarsområder, systemeiere, virksomhetsledere, sikkerhetsutvalg og den enkelte medarbeider i kommunen. Både personvernombuds og digitaliseringssjefens ansvar og myndighetsområde blir i tillegg presisert i en egen prosedyre.[35] I de overfor nevnte retningslinjene for personvern og informasjonssikkerhet er det også beskrevet ansvarsfordeling.

Det er ikke gjennomført årlige ledergjennomganger av sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene, men dette skulle ha vært gjort.

Risikovurdering og risikohåndtering

Kommunen har utarbeidet prosedyre for risikovurdering av informasjonssikkerhet og personvern. Her fremgår det at kommunen skal risikovurdere sin behandling av personopplysninger. Formålet er å sikre at den risikoen som avdekkes ved behandling av personopplysninger, er innenfor de akseptkriterier kommunen har fastlagt.

Risikovurderingen danner grunnlag for iverksetting av nødvendige sikkerhetstiltak, og inngår i underlaget for ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten.

Den som er daglig ansvarlig har på vegne av rådmann ansvar for å iverksette risikovurdering. Sikkerhetsleder/personvernombud, IT-driftsansvarlig, løsningsansvarlige og linjeledere plikter å melde fra om behov for å gjennomføre risikovurdering.

Risikovurderinger skal gjennomføres av virksomhetsledere/daglig ansvarlige i Fredrikstad kommune med mulig bistand fra IT-driftsansvarlig og sikkerhetsleder/personvernombud. Risikoen vurderes og dokumenteres i kvalitetssystemet i egen modul for dette. Resultat fra vurderingen rapporteres til sikkerhetsleder og i årlige ledelsesgjennomganger.

Risikovurderinger skal gjennomføres før behandling av helse- og personopplysninger igangsettes, og ved endringer som kan berøre informasjonssikkerheten (eksempelvis endringer i informasjonssystemet eller i det generelle risikobildet).

Risikovurderingen skal gi følgende resultat:
- oversikt over identifiserte trusler
- angivelse av sannsynlighet for at en uønsket hendelse kan inntreffe
- angivelse av konsekvenser av en uønsket hendelse
- resultat fra analyse av sikkerhetstiltakenes effekt i forhold til risiko

Ved innføringen av GDPR[36] i mai 2018 sendte kommunen ut et rundskriv med informasjon om risikovurdering i kommunen. Det finnes dokumentasjon på gjennomførte risikovurderinger. Det gjennomføres ikke kontroller av hvorvidt virksomhetene har gjennomført slike vurderinger, men det er flere virksomheter som ikke har foretatt risikovurderinger.

Kommunen har en egen prosedyre for registrering av avvik som gjelder personvern.[37] Avviksbehandling skal i henhold til prosedyren, iverksettes ved sikkerhetsbrudd og/eller når

[35] «Digitaliseringssjefens ansvar og myndighetsområde» av 20.5.19 og «Sikkerhetsleder – Personvernombud» av 17.12.2018

[36] General Data Protection Regulation. På norsk: personvernforordningen. En forordning som skal styrke og harmonisere personvernet ved behandling av personopplysninger i EU.

[37]

oppgaver er utført i strid med de prosedyrer som er besluttet. Alle avvik meldes automatisk til nærmeste leder, og grove avvik drøftes i sikkerhetsutvalget og meldes til Datatilsynet.

Personvernombud opplyser om at ansvaret for gjennomføring av risikovurderinger knyttet til informasjonssikkerhet er delegert til den enkelte virksomhet/etat i kommunen. Personvernombud kan dermed ikke svare på hvor ofte og i hvilke tilfeller det gjennomføres slike risikovurderinger. Kommunen har ifølge personvernombud et eget system for risikovurdering. I kvalitetssystemet ligger også brukerveiledning til systemet. Personvernombud deltar i risikovurderingen dersom virksomhetene ønsker det. Resultater av håndtering av informasjonssikkerhetsrisiko, og resultater av korrigerende tiltak legges i kvalitetssystemet, og er ifølge personvernombud tilgjengelig i linja.

Måling, evaluering, revisjon og overvåking

På spørsmål om hvordan effekten av styringssystemet for informasjonssikkerhet måles vises det til at alle ansatte og spesielt de med roller innen IT-sikkerhet benytter kvalitetssystemet for å melde avvik. Avvik håndteres for å kunne få spesielt fokus på sikkerhet. Både Kommunedirektørens sikkerhetsråd og digitaliseringsavdelingens sikkerhetsråd har avvikene oppe til vurdering. Samtidig tas alle avvik opp i organisasjonens samarbeidsutvalg i hver seksjon. På bakgrunn av dette iverksettes tiltak for å forbedre området.

I tillegg har Digitaliseringsavdelingen utstrakt kontakt med brukerorganisasjonen. Meldinger som tilflyter IT-service, registreres i avdelingens fagsystem og tas opp i Sikkerhetsrådet. Digitaliseringsavdelingen gjennomgår kontinuerlig rutiner/prosedyrer/dokumenter.

5.3. Vurderinger

Kommunens overordnede sikkerhetsmål fremkommer av IT-sikkerhetsreglementet til kommunens digitaliseringsavdeling. Kommunen har ingen overordnet strategi for å sikre at målene nås, men har retningslinjer som skal bidra til effektiv og sikker bruk av datasystemene, og sikker håndtering av all behandling av personopplysninger, som sist er godkjent i desember 2019.

Fakta viser at kommunen har flere dokumenter som, i ulikt omfang, omtaler ansvar og myndighet knyttet til informasjonssikkerhetsarbeid. Med flere dokumenter som omhandler det samme, er det etter vår vurdering en risiko for at rutinene har et ulikt eller utdatert innhold, og vi er derfor usikre på om rutinene i stor nok grad oppfattes som klare.

Kommunen har prosedyre for gjennomføring av risikovurdering knyttet til informasjonssikkerhet. Prosedyren redegjør for hvem som har ansvar for å melde ifra om behov for risikovurdering, i hvilke tilfeller det skal gjennomføres og hvordan og hvem som skal utføre vurderingen. Kommunen har et eget system for risikovurdering, og brukerveiledning til systemet ligger tilgjengelig i kvalitetssystemet. Dette finner revisjonen positivt.

Selv om kommunen har prosedyrer for risikovurdering er det imidlertid revisjonens oppfatning at kommunen ikke i tilstrekkelig grad har sikret seg at risikovurderinger gjennomføres. Vi legger til grunn at kommunen ikke har hatt årlige ledelsesgjennomganger, som er en arena for å fange opp eventuelt manglende vurderinger, og kommunen har heller ikke etablert andre kontroller av hvorvidt risikovurderinger faktisk er gjennomført. Med kunnskap om at risikovurderinger ikke er gjennomført fullt ut, kan vi heller ikke si at kommunen i tilstrekkelig grad har sørget for at prosessene rundt risikovurderinger er dokumentert. Ved å gjennomføre systematiske risikovurderinger vil kommunen i større grad få oversikt over svakheter i den eksisterende internkontrollen og kunne innrette sine

kontrolltiltak, herunder rutiner og retningslinjer, på en måte som i størst mulig grad vil kunne hindre svikt.

Kommunen benytter blant annet avviksrapportering til å følge med på informasjonssikkerheten i kommunen. Etter revisjonens oppfatning finnes det imidlertid ikke informasjon som tilsier at kommunen har en systematisk tilnærming til arbeidet med å overvåke informasjonssikkerheten i kommunen og sørge for etterlevelse av lovverk på området. Kommunen bør kontrollere at rutinene for håndtering av personopplysninger brukes og fungerer etter hensikten, herunder jevnlig teste, vurdere og evaluere hvor effektive sikkerhetstiltakene er.

6. ANSATTES KJENNSKAP TIL RUTINER OG RETNINGSLINJER

I hvilken grad har de ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

6.1. Revisjonskriterier

Revisjonen har utledet følgende kriterier for denne problemstillingen[38]:

- Det gjennomføres kompetansetiltak som bidrar til at medarbeidere som bruker kommunens informasjonssystemer, har tilstrekkelig kompetanse til å ivareta kommunens sikkerhetsbehov, og til å ivareta gjeldende krav og føringer for informasjonssikkerhet.
- De ansatte kjenner til kommunens informasjonssikkerhetspolicy/overordnet strategi for informasjonssikkerhet.
- De ansatte har fått opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer.
- De ansatte kjenner til kommunens egne rutiner og prosedyrer for informasjonssikkerhet.
- De ansatte har undertegnet en taushetserklæring ved inngåelse av arbeidsforholdet.

6.2. Fakta

Kompetansetiltak

Kommunens retningslinjer for personvern og informasjonssikkerhet har til hensikt å bidra til effektiv og sikker bruk av datasystemene, og sikker håndtering for all behandling av personopplysninger. Retningslinjene gjelder for alle medarbeidere som behandler personopplysninger, og påpeker *«Som medarbeider i Fredrikstad kommune er det viktig at du har kjennskap til kommunens kvalitetssystem for informasjonssikkerhet og personvern. Du skal være kjent med hvem som har ansvar for hva i sikkerhetsarbeidet, du skal ha kjennskap til hvilke mål og strategier vi sammen skal jobbe etter, du skal være kjent med og forstå de prosedyrer og retningslinjer som er besluttet, og kommunen er avhengig av at alle medarbeidere bidrar til å melde fra om avvik ved brudd på gjeldende sikkerhetstiltak.»*

Ifølge retningslinjene er innføring i sikkerhet og sikkerhetsrutiner en del av introduksjonsprogrammet for nye medarbeidere. E-læringskurs er tidligere omtalt-

Kommunen har ikke på et overordnet nivå kartlagt kompetansebehov blant ansatte som utfører arbeid som kan påvirke informasjonssikkerheten eller dokumentert gjennomførte kompetansetiltak.

Nyansatte får opplæring om internkontroll og informasjonssikkerhet via E-læring. Systemet fungerer slik at virksomheten kan sjekke om det er gjennomgått av den ansatte før utvidede tilganger gis.

I ettertid av opplæringen er det, ifølge retningslinjene, den enkelte ansattes ansvar å holde seg oppdatert, og følge opp og praktisere vedtatte rutiner og sikkerhetstiltak. Dette innebærer også en årvåkenhet i det daglige, og til å varsle gjennom avviksmelding dersom uregelmessigheter oppdages.

Kommunen sørger for at alle ansatte har lest retningslinjene for informasjonssikkerhet og personvern ved at hver enkelt ansatt signerer et skjema hvor de bekrefter å ha lest og forstått retningslinjene. Dette skjemaet legges i personalmapper etter signering.

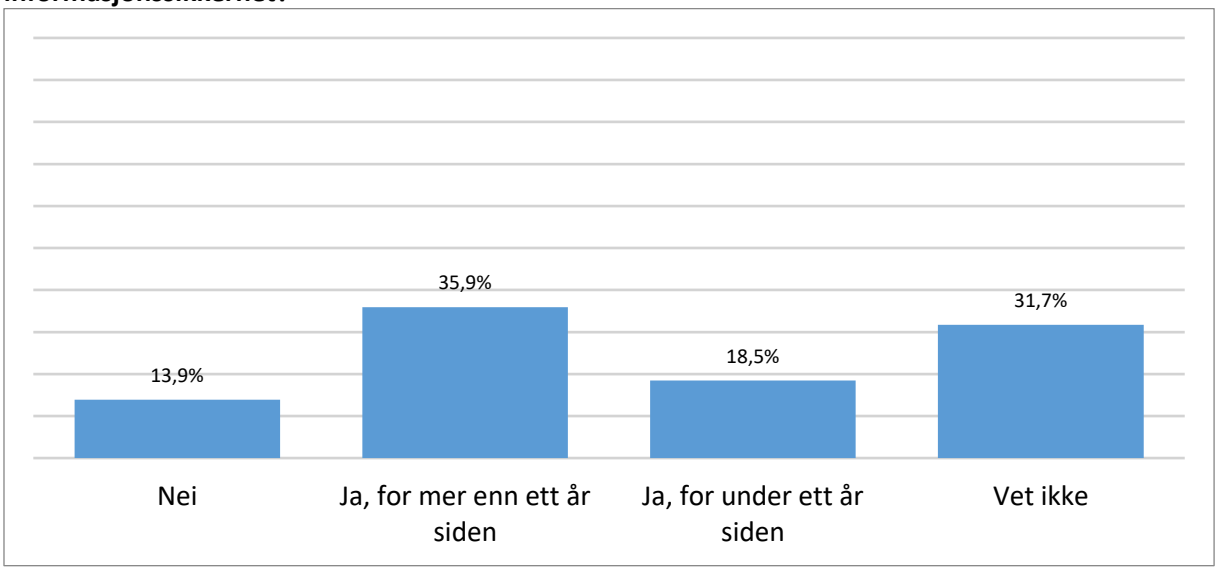
[38] Se vedlegg for utledning

Når det gjelder kommunikasjon, har kommunen rutiner og retningslinjer for både intern og ekstern kommunikasjon. Disse ligger på intranettet, samt noe i kvalitetssystemet. Rutinene og retningslinjene tar for eksempel for seg lagring i skyløsning og bruk av e-post. Ekstern og intern kommunikasjon er også omtalt i retningslinjer for informasjonssikkerhet og personvern som alle nyansatte skal lese og signere på at de har lest. Revisjonen har undersøkt hvor godt de ansatte kjenner til de mest aktuelle rutinene og retningslinjene. Denne undersøkelsen blir presentert i neste kapittel.

Kjennskap til kommunens informasjonssikkerhetspolicy

Figuren nedenfor viser hvorvidt respondentene mener de har fått informasjon om kommunens krav og forventninger til informasjonssikkerhet.

Figur 6: «Har du fått informasjon om kommunens krav og forventninger til informasjonssikkerhet?»



Antall respondenter: 1303

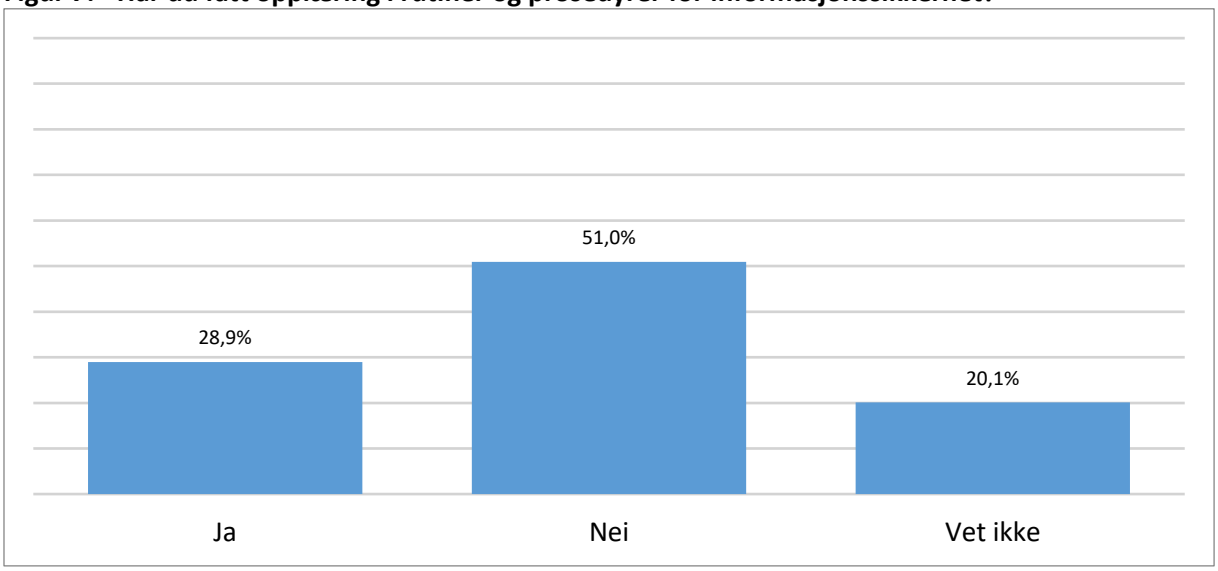
Som figur 6 viser, oppgir over halvparten at de har fått informasjon om kommunens krav og forventninger til informasjonssikkerhet. 35,9 prosent har fått informasjonen for mer enn ett år siden, og 18,5 prosent for under ett år siden.

Opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer

Som vist til innledningsvis, får nyansatte i kommunen, opplæring om internkontroll og informasjonssikkerhet via E-læring. Systemet fungerer slik at virksomheten skal/kan sjekke om det er gjennomgått av den ansatte før utvidede tilganger gis. I ettertid av opplæringen er det ifølge retningslinjene, den enkelte ansattes ansvar å holde seg oppdatert, og følge opp og praktisere vedtatte rutiner og sikkerhetstiltak.

Figurene nedenfor viser svar på spørsmål knyttet til opplæringen.

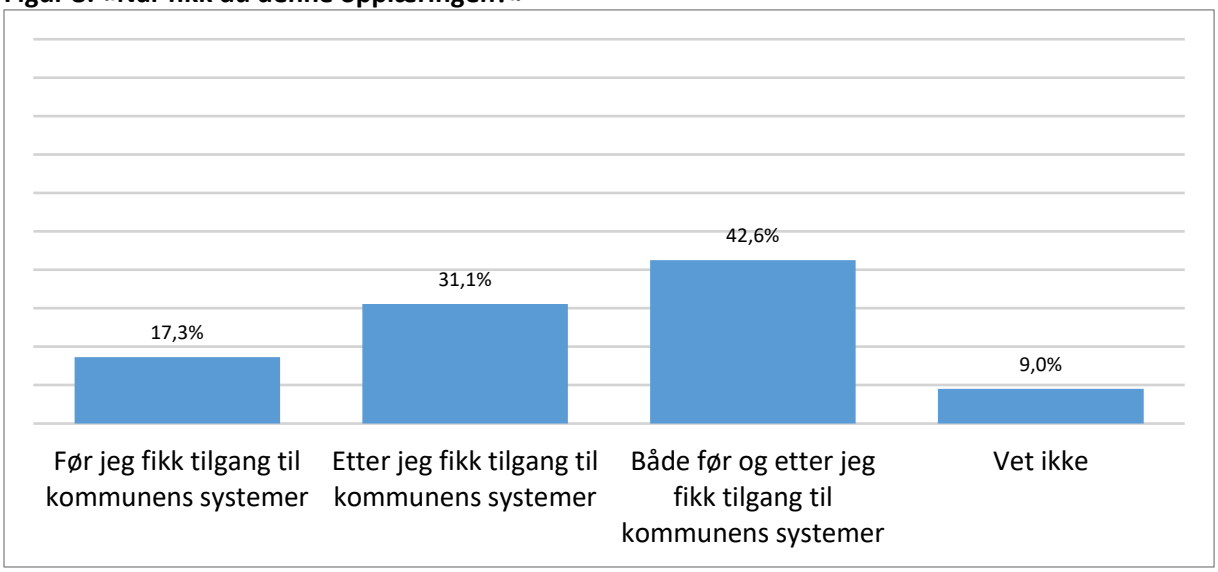
Figur 7: «Har du fått opplæring i rutiner og prosedyrer for informasjonssikkerhet?»



Antall respondenter: 1303

Figur 7 viser at over halvparten av respondentene i spørreundersøkelsen mener de ikke har fått opplæring i rutiner og prosedyrer knyttet til informasjonssikkerhet. Ansatte som svarte at de hadde fått denne opplæringen, ble spurt om *når* denne opplæringen ble gitt.

Figur 8: «Når fikk du denne opplæringen?»

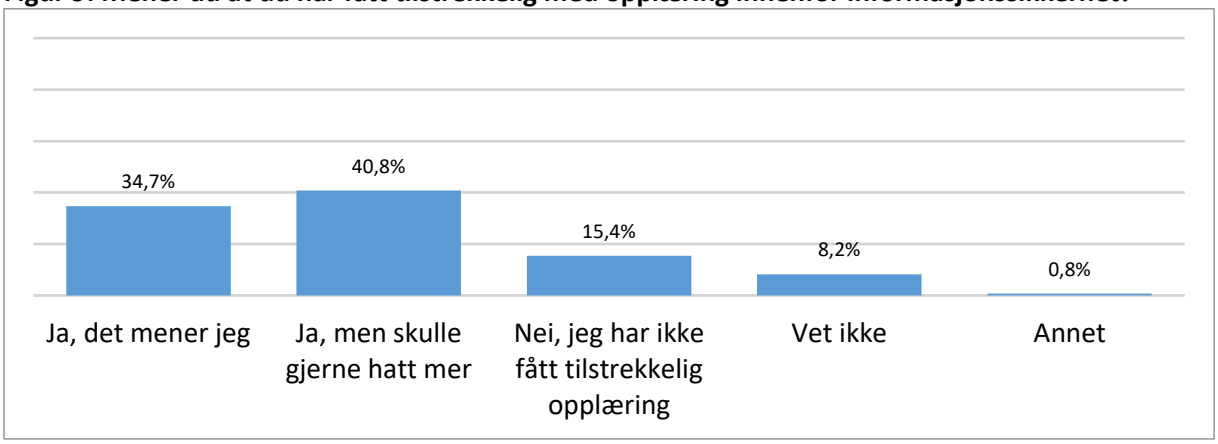


Antall respondenter: 376

Figur 8 viser at opplæring blir gitt både før og etter at tilganger er utdelt. I spørreundersøkelsen ble respondentene gitt muligheten til å kommentere kommunens arbeid med informasjonssikkerhet og personvern. Flere bekreftet i kommentarene at der er behov for mer opplæring.

Figuren nedenfor viser hvorvidt de ansatte, som har fått opplæring innen informasjonssikkerhet, selv mener at de har fått tilstrekkelig med opplæring.

Figur 9: Mener du at du har fått tilstrekkelig med opplæring innenfor informasjonssikkerhet?



Antall respondenter: 377

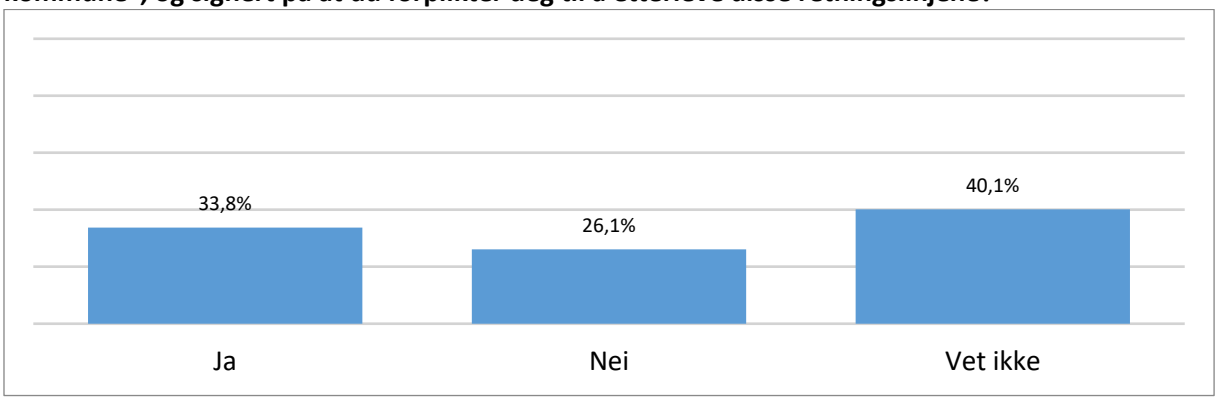
Figur 9 viser at om lag en tredjedel mener de har fått tilstrekkelig opplæring, mens over halvparten ønsker mer opplæring eller mener at opplæringen ikke har vært tilstrekkelig.

Kjennskap til kommunens egne rutiner og prosedyrer for informasjonssikkerhet

Vi har spurt de ansatte om kjennskap til kommunens prosedyrer for informasjonssikkerhet. Nedenfor følger flere figurer som sier noe om de ansattes kjennskap til de aktuelle rutinene og prosedyrene.

Som vist til innledningsvis skal kommunen sørge for at alle ansatte har lest retningslinjene for informasjonssikkerhet og personvern, ved at hver enkelt ansatt signerer et skjema hvor de bekrefter å ha lest og forstått retningslinjene.

Figur 10: «Har du lest "Retningslinjer for informasjonssikkerhet og personvern i Fredrikstad kommune", og signert på at du forplikter deg til å etterleve disse retningslinjene?»



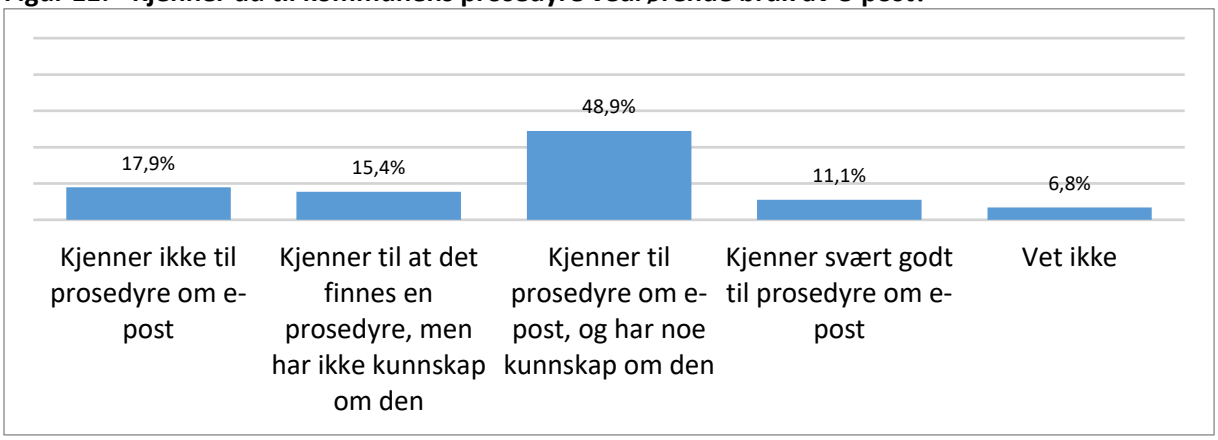
Antall respondenter: 1303

Figur 10 viser at en tredjedel av respondentene har lest og signert retningslinjene. De resterende respondentene svarer Nei eller vet ikke på spørsmålet.

Kommunen har en prosedyre for bruk av e-post, som finnes i kvalitetssystemet. IT-ansvarlig opplyser om at deler av prosedyren er utdatert.[39] Figuren nedenfor sier noe om hvor godt respondentene kjenner til prosedyren.

[39] Gjelder rutinens oppfordring om å ikke sende e-post umiddelbart.

Figur 11: «Kjenner du til kommunens prosedyre vedrørende bruk av e-post?»



Antall respondenter: 1299

Figur 11 viser at over halvparten av respondentene har kunnskap om denne prosedyren. I kommunens prosedyre for bruk av e-post står det følgende om bruk av e-post til private gjøremål:

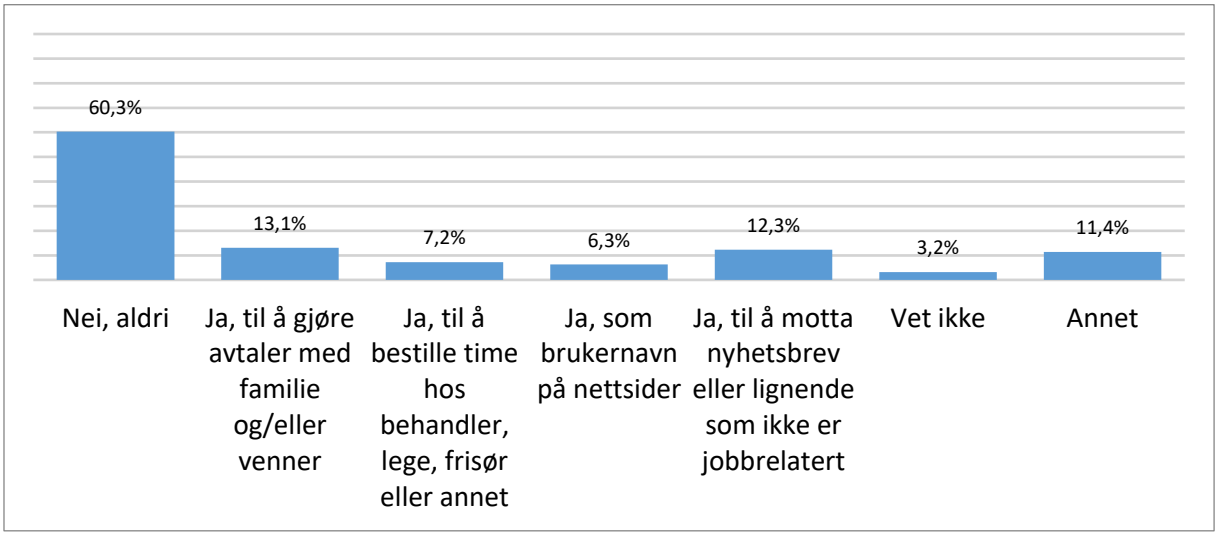
«I Fredrikstad kommune tillates at våre medarbeidere kan benytte e-posten sin til små og tidsbegrensede private gjøremål.»

Prosedyren beskriver også hva som ikke er tillatt når det gjelder bruk av e-post til private gjøremål:

«Det er ikke tillatt å delta i nyhetsgrupper/e-mail lister eller på andre måter offentliggjøre din e-mail adresse på Internett (f.eks. Facebook). Dersom dette tillates anbefales det å opprette en egen e-mail adresse som lett kan stenges.»

Revisjonen har spurt de ansatte om de benytter e-posten til private gjøremål. Figuren nedenfor viser hva respondentene svarte.

Figur 12: «Hender det at du benytter e-posten til private gjøremål? Du kan velge flere svaralternativer.»

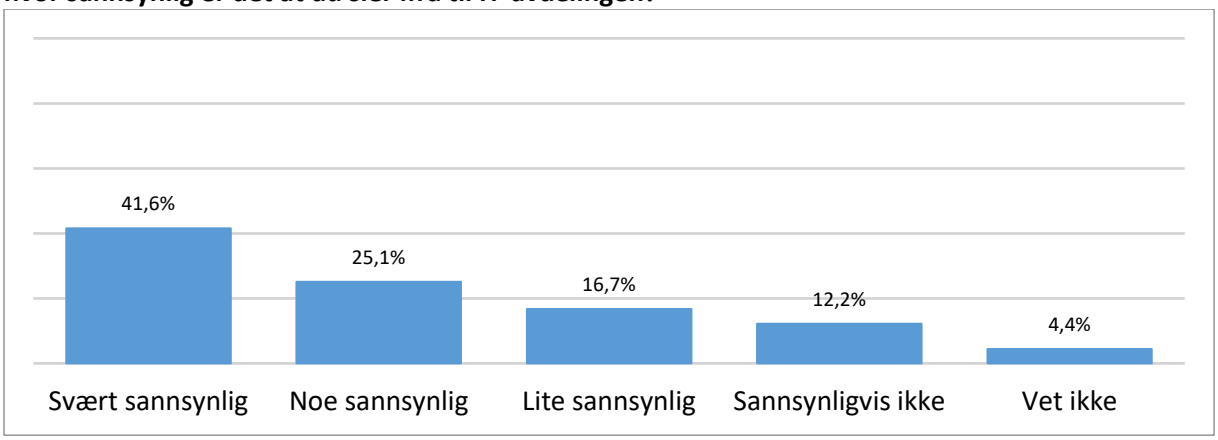


Antall respondenter: 1300

Figur 12 viser at 60,3 % aldri benytter e-posten til private gjøremål. Av de respondentene som benytter e-posten til private gjøremål svarer de fleste at de benytter den til å gjøre avtaler med familie/venner eller til å motta nyhetsbrev eller lignende som ikke er jobbrelatert.

Revisjonen har spurt de ansatte om de melder fra til IT-service dersom de mottar en e-post som kan se ut til å være spam (søppelpost), eller et svindelforsøk.

Figur 13: «Hvis du mottar e-post du mistenker for å være spam (søppelpost), eller et svindelforsøk - hvor sannsynlig er det at du sier ifra til IT-avdelingen?»



Antall respondenter: 1299

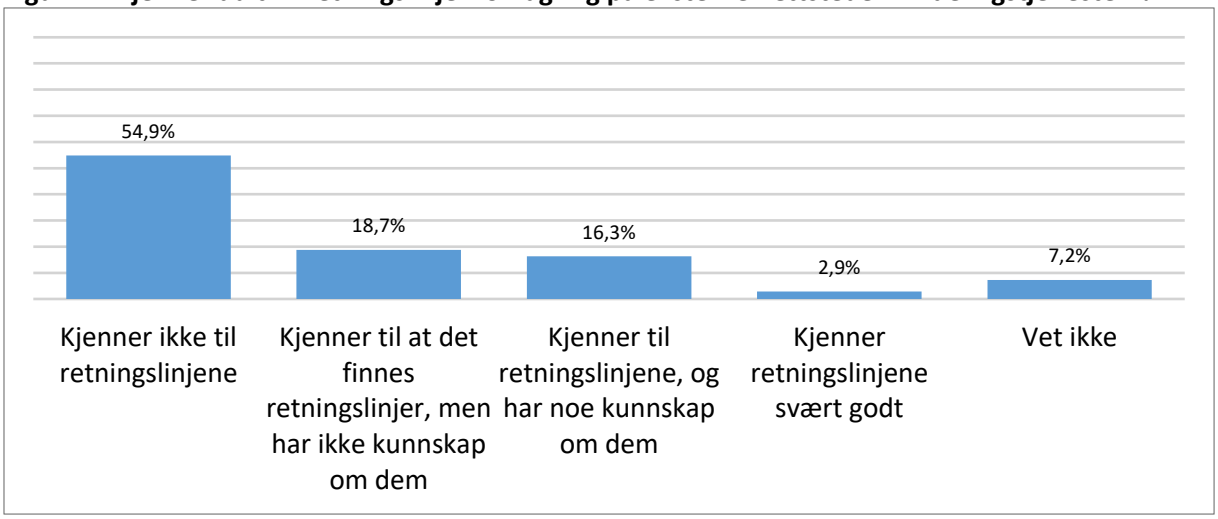
Figur 13 viser at 41,6 % av respondentene mener det er svært sannsynlig at de ikke vil melde fra til IT-avdelingen (virksomhet digitalisering) ved spam eller svindelforsøk.

Revisjonen har som nevnt tidligere i rapporten, utført et phishingforsøk for å undersøke om ansatte la inn brukernavn og passord i oversendt påloggingsvindu. E-posten ble sendt til 100 ansatte og ga ingen negative resultater.

Kommunen har en rutine for hvordan de skal håndtere spam/phishing. Dersom IT-service får varsel fra brukere om mistenkelig e-post skal de varsle IT-drift som iverksetter tiltak for å få bukt med problemet. Kommunen har informert revisjonen om at denne rutinen ikke ble iverksatt under phishing-testen, og at de fikk rundt 15 tilbakemeldinger på at e-posten virket mistenkelig.

Kommunen har i senere tid åpnet for deling og lagring av dokumenter i skyløsinger, og fikk i oktober 2018 egne retningslinjer for dette. I figuren nedenfor vises hvorvidt respondentene i spørreundersøkelsen er kjent med disse retningslinjene.

Figur 14: Kjenner du til "Retningslinjer for lagring på eksterne nettsteder - fildelingstjenester"?

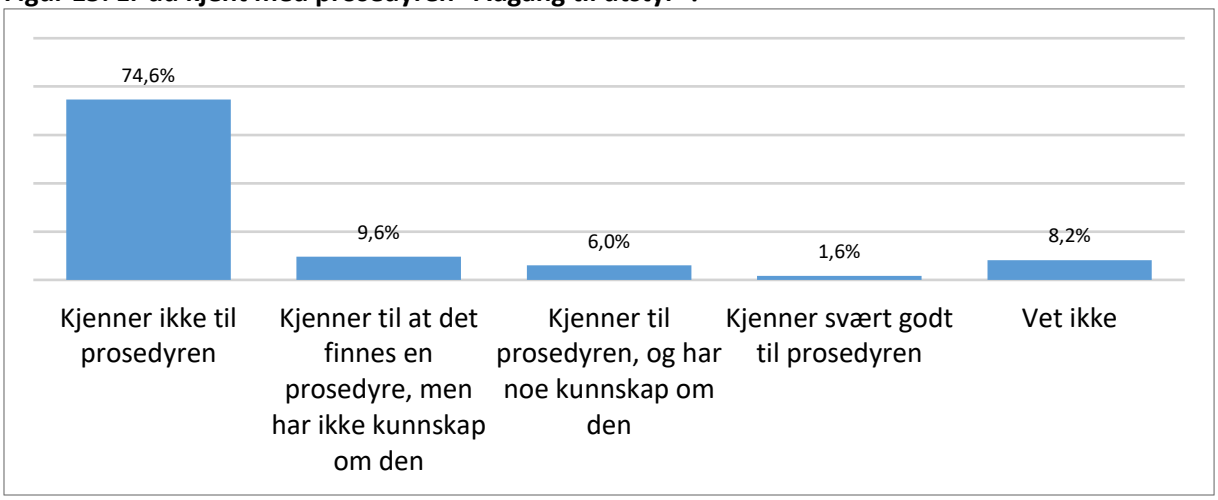


Antall respondenter: 1303

Figur 14 viser at over halvparten av respondentene ikke kjenner til disse retningslinjene.

Kommunen har en egen prosedyre som gjelder sikring av utstyr som benyttes ved behandling av sensitive personopplysninger (arbeidsstasjoner og skrivere, samt kopimaskiner og telefaksmaskiner).[40] Figuren nedenfor viser hvorvidt spørreundersøkelsens respondenter kjenner til denne prosedyren.

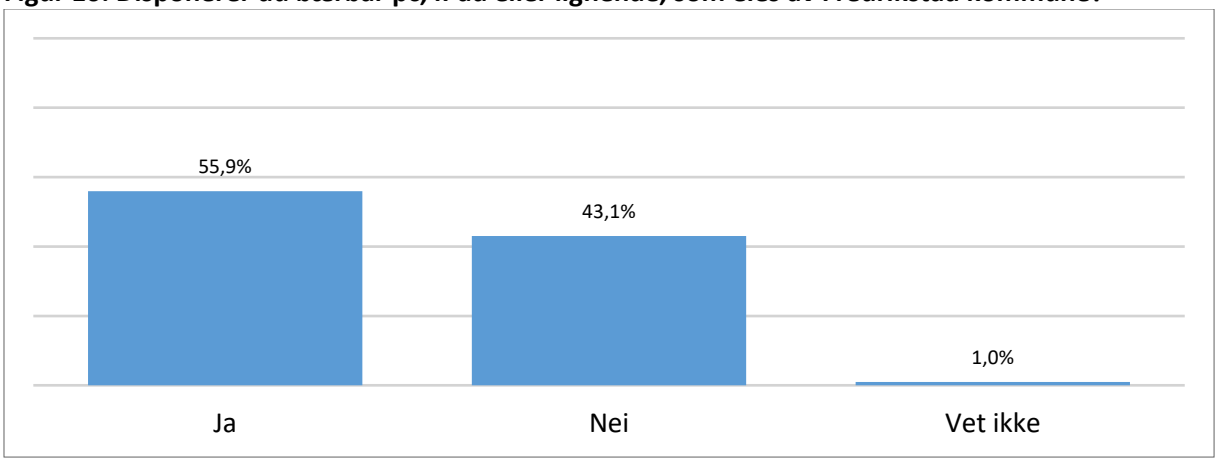
Figur 15: Er du kjent med prosedyren "Adgang til utstyr"?



Antall respondenter: 1303

Figur 15 viser at 74,6 % av respondentene ikke kjenner til prosedyren. Revisjonen ønsket også å vite hvor stor andel av respondentene som disponerer en bærbar PC, iPad eller lignende, som eies av kommunen.

Figur 16: Disponerer du bærbar pc, iPad eller lignende, som eies av Fredrikstad kommune?



Antall respondenter: 1303

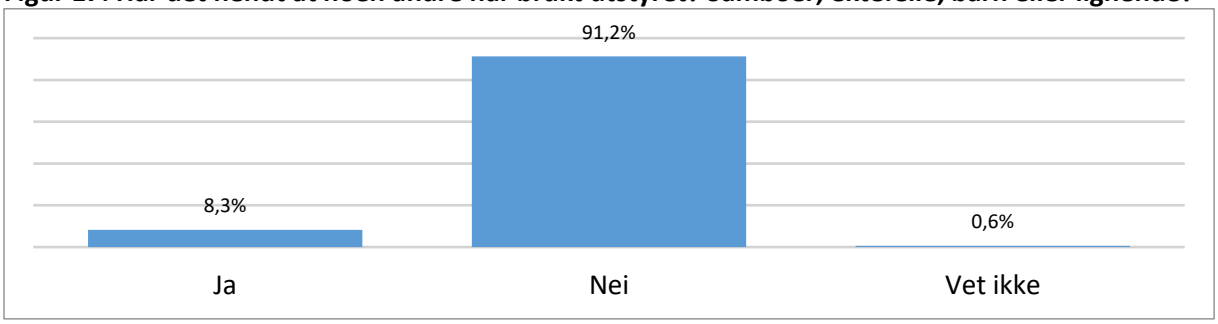
Figur 16 viser at over halvparten av respondentene disponerer jobb-PC, jobb-iPad eller lignende. I kommunens prosedyre «Adgang til utstyr» står det følgende om sikring av bærbart utstyr:

«Bærbare PC-er skal ikke lånes ut til uvedkommende. Dette forbudet gjelder også utlån til familiemedlemmer.»

I figuren nedenfor vises respondentenes svar vedrørende utlån av bærbart utstyr.

[40] «Adgang til utstyr» godkjent 17.12.18

Figur 17: Har det hendt at noen andre har brukt utstyret? Samboer, ektefelle, barn eller lignende?

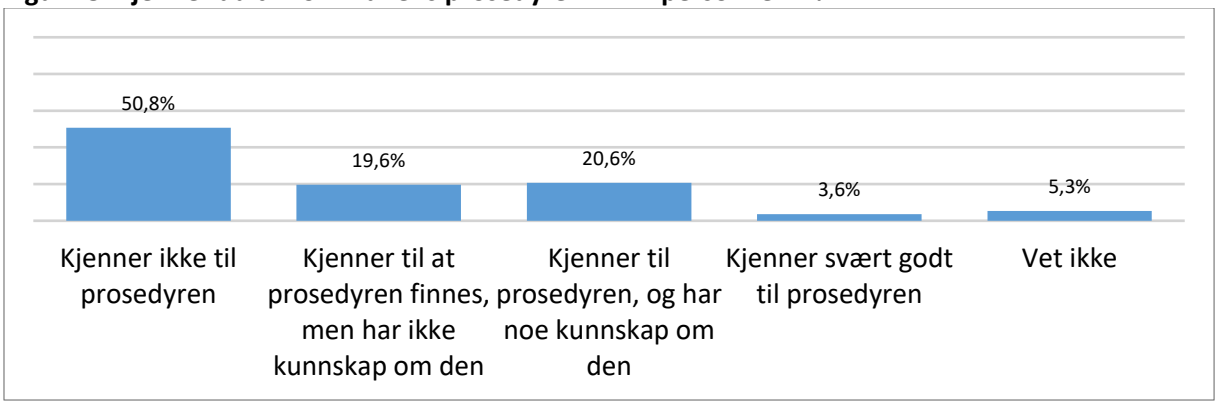


Antall respondenter: 727

Som figur 17 viser, har det hendt at 8,3 prosent av respondentene har lånt bort utstyret sitt til andre, for eksempel i familien. 8,3 prosent utgjør her 60 ansatte.

Kommunen fikk i juni 2019 en egen prosedyre for melding av avvik som gjelder personvern. Ifølge prosedyren skal avviksbehandling iverksettes ved sikkerhetsbrudd og/eller når oppgaver er utført i strid med de prosedyrer som er besluttet. Ifølge prosedyren, har alle brukere ansvar for å registrere avvik i avviksmodulen i kvalitetssystemet. Figuren nedenfor viser respondentenes svar på hvorvidt de kjenner til avviksprosedyren

Figur 18: Kjenner du til kommunens prosedyre "Avvik personvern"?

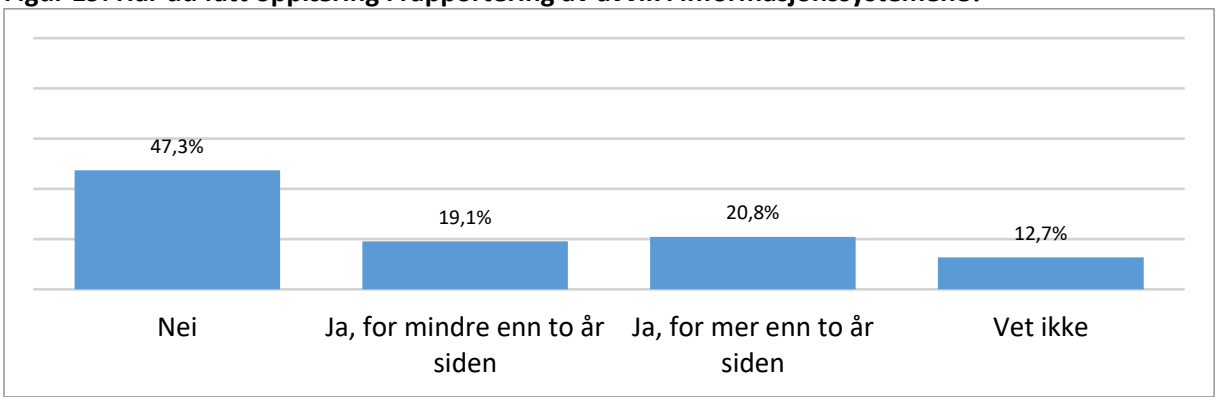


Antall respondenter: 1294

Figur 18 viser at halvparten av respondentene ikke kjenner til prosedyren.

Revisjonen har også spurt respondentene om de har fått opplæring i rapportering av avvik i informasjonssystemene. Figurene nedenfor viser svarene.

Figur 19: Har du fått opplæring i rapportering av avvik i informasjonssystemene?



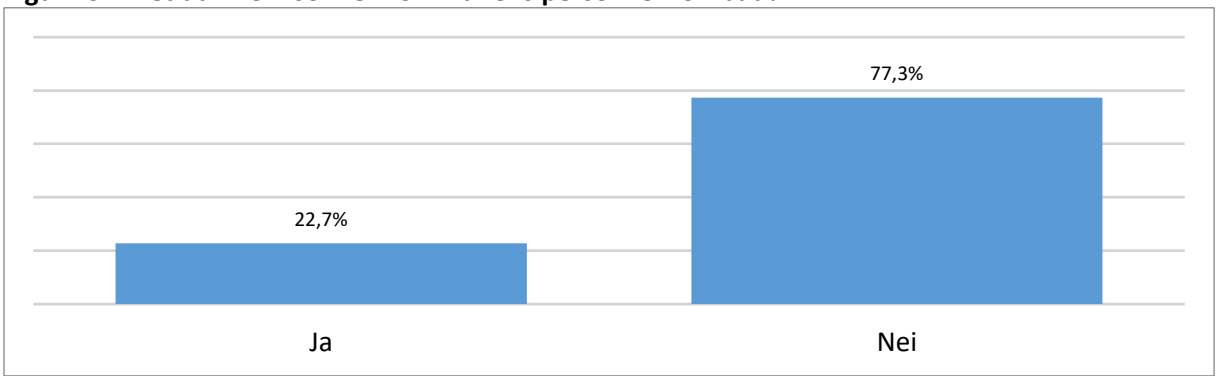
Antall respondenter: 1295

Figur 19 viser at i underkant av halvparten av respondentene mener at de heller ikke har fått opplæring i rapportering av avvik i informasjonssystemene.

Kommunen hadde i 2019 et personvernombud i 50 prosent stilling, organisert under seksjon for økonomi og organisasjonsutvikling. Ifølge kommunens handlingsplan for 2019-2022 er det ikke satt av midler til en større stilling i perioden, men seksjonen vil følge med på utviklingen og vurdere om denne stillingen må økes til 100 prosent.

Figuren nedenfor viser hvor stor andel av spørreundersøkelsens respondenter som vet hvem som er personvernombud.

Figur 20: «Vet du hvem som er kommunens personvernombud?»



Antall respondenter: 1303

Figur 20 viser at 77,3 % av respondentene ikke vet hvem som er personvernombud i kommunen.

Taushetserklæring for ansatte

Digitaliseringssjef informerer om at kommunen har gått bort fra bruk av taushetserklæring som eget dokument. Taushetserklæringen ligger implisitt i arbeidskontrakten.

Regler for taushetsplikt er også beskrevet i kommunen retningslinjer for personvern og informasjonssikkerhet for ansatte.

6.3. Vurderinger

Fakta viser at det blir gjennomført kompetansetiltak. Kommunen har imidlertid ikke foretatt en overordnet kartlegging av kompetansebehovet blant ansatte som utfører arbeid som kan påvirke informasjonssikkerheten. Gjennomførte kompetansetiltak dokumenteres heller ikke noe spesielt sted. Etter revisjonens oppfatning vil man gjennom å kartlegge kompetansebehov, i større grad kunne tilpasse opplæringen og sørge for at ansatte får den opplæringen de har behov for. Samtidig vil dette legge til rette for at kommunen også kan dokumentere sitt arbeid med kompetanseheving.

Kommunens retningslinjer for informasjonssikkerhet stiller krav til at medarbeidere skal være kjent med kommunens kvalitetssystem for informasjonssikkerhet. Videre stilles det krav til at medarbeidere vet hvem som har ansvar for hva i sikkerhetsarbeidet, hvilke mål og strategier det skal jobbes etter, hvilke retningslinjer og prosedyrer som er besluttet og at medarbeidere melder avvik ved brudd på gjeldende sikkerhetstiltak. Innføring i sikkerhet og sikkerhetsrutiner er ifølge retningslinjene en del av introduksjonsprogrammet for nye medarbeidere. Nyansatte får også opplæring om internkontroll og informasjonssikkerhet via E-læring. Systemet fungerer slik at aktuell leder kan sjekke om E-læringen er gjennomgått, før tilganger gis. Kommunen sørger for at alle ansatte har lest retningslinjene for informasjonssikkerhet, ved at de ansatte signerer et skjema hvor

de bekrefter å ha lest disse. Etter revisjonens oppfatning har kommunen etablert en rekke tiltak som vil kunne sikre medarbeiderne kunnskap om kommunens rutiner og retningslinjer for informasjonssikkerhet.

I ettertid av opplæringen er det ifølge retningslinjene, medarbeideren selv som skal sørge for å holde seg oppdatert. I dette perspektivet, er det, etter revisjonens oppfatning spesielt viktig å sørge for at planer, rutiner og retningslinjer på området er lett tilgjengelig, klare og tydelige. Som nevnt i de foregående vurderingene fremstår kommunens dokumentasjon på området som noe uoversiktlig. Slik revisjonen ser det har ikke kommunen i stor nok grad lagt til rette for at medarbeiderne selv skal kunne holde seg oppdatert på hva som er gjeldende.

Ved bruk av spørreundersøkelse har vi sett nærmere på de ansattes opplevelse av egen kjennskap og kunnskap om aktuelle rutiner og retningslinjer, og behovet for opplæring. Revisjonen har stilt en rekke spørsmål til respondentene. Undersøkelsen har en svarprosent på 15,95. Antall respondenter er høyt – 1303 ansatte har besvart, og vi mener at resultatene gir et godt innblikk i mange ansattes oppfatninger. Etter vår vurdering viser resultatene at flere ansatte opplever at de har fått opplæring og at de har en viss kompetanse knyttet til informasjonssikkerhet. Samtidig kan spørreundersøkelsen også indikere at kommunen har et ganske stort behov for kompetanseheving på feltet. Vi legger blant annet til grunn at 51 % av respondentene svarer at de ikke har fått opplæring i rutiner og retningslinjer vedrørende informasjonssikkerhet og en tredjedel vet ikke om de har fått informasjon om kommunens krav og forventninger til informasjonssikkerhet. Revisjonen har også stilt spørsmål om praksis opp mot innhold i kommunens rutiner, og også her viser resultatene at flere ansatte har en praksis i strid med kommunens rutiner og retningslinjer. Etter revisjonens oppfatning kan det være hensiktsmessig om kommunen foretar en gjennomgang av resultatene fra undersøkelsen i sin helhet, og vurderer om kompetansehevingstiltak kan settes inn på områdene hvor resultatene indikerer høyest risiko for svikt opp mot egne rutiner, eventuelt vurdere innholdet i rutinene som ikke etterleves.

7. KONKLUSJONER OG ANBEFALINGER

Planer og rutiner

Faktagrunnlaget i vår rapport viser at kommunen i hovedsak har tilfredsstillende planer og rutiner for håndtering av IKT-sikkerhetsmessige situasjoner, herunder varsling fra ansatte. Kommunens beredskapsplan for alvorlige driftssituasjoner, vedlikehold av infrastruktur og prosedyrer for ulike driftsstans-kategorier vil kunne dekke de fleste forhold som kan føre til driftsavbrudd i kommunens IKT-systemer. Det er positivt at kommunen involverer sikkerhetsmyndigheter ved behov, men dette er ikke nedfelt skriftlig i kommunens planer og rutiner – noe vi mener ville vært en fordel. Det er også positivt at kommunen siden 90-tallet har gjennomført ROS-analyser for IT-sikkerhet. Vi anser det likevel som mangelfullt at det ikke er utarbeidet en overgripende beredskapsplan for håndtering av IKT-sikkerhetsmessige situasjoner basert på denne analysen.

Sikkerhetstiltak

Våre undersøkelser viser at kommunen har etablert en rekke sikkerhetstiltak av sine datasystemer mot cyberangrep, som i hovedsak tilfredsstiller kravene i våre revisjonskriterier. Revisjonen har likevel avdekket enkelte forbedringsområder. I hovedsak gjelder dette at dokumentasjon på området er delvis overlappende, samtidig som flere dokumenter er under revisjon, og at det kan se ut til å være en sammenblanding av personvern og IT-sikkerhet i kommunens prosedyrer. Vi har derfor vurdert at kommunen ikke i stor nok grad har kommunisert innholdet i sin sikkerhetsstyring på en tydelig nok måte slik at det er lett forståelig for de ansatte.

Vi mener også at det innebærer risiko at sluttbrukere kan be om midlertidig tilgang til filnedlasting. Etter vår oppfatning åpner det opp for at det installeres mer funksjonalitet enn nødvendig på enheten, og risikoen for at skadelig programvare får tilgang til kommunens systemer øker.

I dag gjennomgås loggfiler kun ved mistanke om forhold som bør følges opp. Etter vår oppfatning vil en jevnlig gjennomgang av loggfiler kunne føre til oppdagelse av mistenkelig aktivitet på et tidligere tidspunkt.

Som rekognoseringen av kommunens hoved-domene, og samtaler med kommunen viste, bruker ikke kommunen på tidspunkt for revisjon de anbefalte prinsipper for beste praksis ved e-post-sikkerhet.

Det kan videre være en risiko for at data blir lagret lokalt på bærbare enheter.

Det øker risikoen for uautorisert tilgang til kommunens systemer når ikke 2-faktor autentisering er tatt i bruk på alle flater der de ansatte eksternt skal koble seg til kommunens systemer.

Vår spørreundersøkelse viser at det kan være tilfeller der det gis utvidede tilganger uten at e-kurset er bestått/gjennomført. Det kan være en risikofaktor at det ikke er implementert systemkontroll for å sikre at kurset er gjennomført før den ansatte får utvidede tilganger. Det kan også være hensiktsmessig å vurdere behov for en sentral oppfølging av at tilganger blir gjennomgått på jevnlig basis. Eventuelt kan kommunen vurdere å tydeliggjøre ansvaret i sine rutiner på området.

Når det gjelder fysisk tilgang til kommunens servere, er vår oppfatning at det kan ligge risiko i det at alle som har administratorrettigheter i adgangssystemet kan gi adgang til serverrom. Risikoen reduseres noe av at systemet loggfører aktivitet, men risikoen kan reduseres ytterligere ved jevnlig gjennomgang av logger, eller restriksjoner i tilgangssystemet som hindrer uautoriserte personer å gi tilgang til disse rommene.

Internkontroll

Vi har funnet at kommunen har etablert flere tiltak som har positiv effekt i kommunens internkontroll på området, herunder blant annet en rekke rutiner og retningslinjer. Vi kan likevel ikke si at kommunen på nåværende tidspunkt har et styringssystem for informasjonssikkerhet som er tilfredsstillende. Som våre vurderinger viser handler dette blant annet om at internkontrolldokumentasjonen fremstår som uoversiktlig, manglende risikovurderinger og manglende overvåkning av systemet, samt lite systematikk i dette arbeidet.

Ansattes kjennskap til rutiner og retningslinjer

Våre vurderinger viser at kommunen har etablert en rekke tiltak for å sikre at kommunens ansatte har kjennskap til kommunens rutiner og retningslinjer for informasjonssikkerhet. Funnene viser imidlertid et ganske stort behov for kompetanseheving på området. Slik revisjonen vurderer det har kommunens ansatte kun i noen grad kjennskap til retningslinjer og rutiner for informasjonssikkerhet.

Anbefalinger

Basert på våre vurderinger og konklusjoner anbefaler vi at kommunen bør:

- implementere varsling til sikkerhetsmyndigheter i sine skriftlige rutiner/prosedyrer.
- prioritere å få på plass en overordnet beredskapsplan for IKT-sikkerhetsmessige situasjoner, basert på deres ROS-analyse.
- gjennomgå sine rutiner og prosedyrer på området, med særlig hensyn til gyldighet, begrepsbruk, ansvarsfordeling og overlapping av innhold.
- vurdere å gjennomgå viktige loggfiler jevnlig.
- prioritere å få på plass ytterligere sikring av sin e-post-kommunikasjon.
- vurdere å kryptere bærbare enheter der det er risiko for at sensitiv data blir lagret lokalt, som anbefalt i NSMs grunnprinsipper.
- innføre 2-faktor autentisering på alle flater der ansatte eksternt skal koble seg til kommunens systemer, eventuelt sperre for flater der 2-faktor autentisering ikke er tilgjengelig.
- vurdere å innføre sentral kontroll av gjennomgang av tilganger – eventuelt gjennomgå sine dokumenter på området med hensyn til tydeliggjøring av ansvaret for å gjennomgå tilganger.
- vurdere å jevnlig gjennomgå aktivitetslogg for tilgang til serverrom, eventuelt vurdere å innføre sperrer i systemet slik at det ikke er mulig for alle med administratorrettigheter å gi tilgang til slike rom.
- sørge for at risikovurderinger av informasjonssikkerheten gjennomføres i tråd med egne rutiner og retningslinjer.
- etablere en systematisk overvåkning av informasjonssikkerheten i kommunen for å sikre at lovverket etterleves.
- kartlegge de ansattes kompetansebehov innen informasjonssikkerhet, og vurdere nødvendige tiltak. Det kan være hensiktsmessig om kommunen også benytter resultatene fra spørreundersøkelsen som en indikasjon på hvordan kompetansetiltakene bør innrettes.

Rolvsøy, 24. januar 2020

Anita M. Torp (sign.)
revisor

Lene Brudal (sign.)
oppdragsansvarlig revisor

8. KOMMUNEDIREKTØRENS UTTALELSE

FREDRIKSTAD KOMMUNE

Østfold kommunerevisjon

Postboks 24
1662 Rolvsøy

Deres referanse	Vår referanse	Klassering	Dato
Lene Brudal	2018/12150-6-15396/2020-MARMAN	060	23.01.2020

Kommunedirektørens høringsuttalelse – forvaltningsrevisjonsrapport cyberangrep og informasjonssikkerhet

Vi viser til høringsutkast forvaltningsrevisjon – cyberangrep og informasjonssikkerhet Fredrikstad kommune, mottatt 17.1.2020.

Kommunedirektøren ser det som svært nyttig at det nå er gjennomført en forvaltningsrevisjon på området. Kommunedirektøren anser rapporten å være gjennomarbeidet, omfangsrik og god.

Samlet sett oppfatter kommunedirektøren at rapporten viser at kommunen har et forsvarlig system og en tilfredsstillende teknologisk plattform. Samtidig er det avdekket enkelte forbedringsområder, som kommunedirektøren vil legge til grunn for videre forbedringsarbeid.

Dette gjelder følgende områder:

Styringssystem, rutiner, instrukser og dokumentasjon
Revisjonen avdekker at kommunen har etablert mange rutiner og prosedyrer, og har en omfattende dokumentasjon på plass i kvalitetssystemet. Det er avdekket noe overlappende informasjon, og at innholdet i sikkerhetsstyringen ikke i stor nok grad har blitt kommunisert tydelig for de ansatte.

Forslag til tiltak:
Det bør iverksettes gjennomgang av rutiner og prosedyrer på området, med særlig hensyn til gyldighet, begrepsbruk, ansvarsfordeling, struktur og overlapping av innhold. Det bør etableres et klarere grensesnitt mellom Digitalisering (teknologi) og Personvern. Det bør etableres prosedyre for varsling til sikkerhetsmyndigheter.

Opplæring
Revisjonens undersøkelser avdekker at brukere av IT-systemet mener det er behov for mer opplæring innen IT-sikkerhet.

Styring og eierskap
Besøksadresse: Nygaardsgt. 16, 1606 Fredrikstad
E-postadresse: postmottak@fredrikstad.kommune.no
Telefon: 69 30 60 00 Org.nr: 940039541
Postadresse: Postboks 1405, 1602 FREDRIKSTAD
Webadresse: www.fredrikstad.kommune.no
Tlf. saksbeh.: 69 36 13 62 Bankkonto:

Forslag til tiltak:
Kompetansen på området *cyberangrep* bør økes. Dette kan gjøres gjennom å utvide aktiviteten av e-læringskurs. Informasjon om kommunens sikkerhetsstyring bør også inngå i brukeropplæringen.

Det er behov for å øke lederkompetansen på området *personvern*. Opplæring bør inngå i kommunens lederopplæring.

Beredskap
Revisjonen påpeker at det mangler en overordnet beredskapsplan for IKT-sikkerhetsmessige situasjoner. Risikovurderinger av informasjonssikkerheten må sikres gjennomført i tråd med egne rutiner og retningslinjer og det må etableres en systematisk overvåking av styringssystemet.

Forslag til tiltak:
Det pågår gjennomgang av overordnet beredskapsplanverk, inkludert risikovurderinger. Følges opp i den forbindelse.

Tilgangsstyring
Rapporten avdekker at tilgangsstyringen til IT-systemer kan optimaliseres.

Forslag til tiltak:
Kommunen har god tilgangsstyring, ved hjelp av en tilgangsportal som innebærer at ansvaret til enhver tid ligger på rett ledernivå. Problemstillingen er, som det påpekes i revisjonsrapporten, at enkelte ansatte kan gis tilgang til lukkede fagsystemer uten gjennomført IT-sikkerhetsopplæring. Det bør iverksettes barrierer for at en slik praksis ikke kan gjennomføres.

Teknologi
Revisjonen konkluderer med enkelte teknologiske forbedringspunkter. Her oppsummeres funn som kommunedirektøren anser som mest aktuelle:

Funn 1 – Gjennomgang av loggfiler
Det er avdekket manglende rutiner for gjennomgang av tekniske logger. Deler av dette kan synes unødvendig, men enkelte rutiner forbedres og det innføres rutinemessig gjennomgang.

Funn 2 – E-post
Det er allerede i gang arbeider med å etablere DMARC-løsninger i epostsystemet. Likeledes også 2-faktor for tilgang. Begge forholdene er påpekt i rapporten.

Funn 3 – Kryptering av bærbare enheter
Revisjonen påpeker manglede sikkerhet på bærbare enheter. Det er to nivåer for å hindre lagring lokalt på bærbare enheter. I dag reguleres dette med å redirigere alle lagringsbaner til sentrale filservere. Dette er nær 100 prosent tilfredsstillende, da det nærmest ikke forekommer lokalt lagrede filer. Det er dog teknisk mulig, men praktisk komplisert for brukeren. På grunn av den teoretiske muligheten, vurderes det etablering av teknologien Bitlocker, som krypterer enheten.

Funn 4 – 2-faktor beskyttelse
Det er allerede iverksatt arbeider med etablering av 2-faktor tilgangskontroll på de systemflatene der dette lar seg gjøre.

Funn 5 – Fysisk tilgangssikring serverrom
Det påpekes i rapporten at den fysiske tilgangen (nøkkelkort) kontrolleres av ansatte på TD-Bygg. Tilgangskontrollen på kommunens tre datarom fjernes fra denne driftsmodellen.

Funn 6 – Åpne e-postadresser på kommunens nettsted
Det rettes kritikk mot at alle ansattes e-postadresser publiseres på kommunens nettsted, slik at disse kan høstes med tanke på angrep og phishing. Dette er et form for dilemma, da hensikten med publiseringen er åpenhet og offentlighetsprinsippet. Det må vurderes om offentlighetsprinsippet står i hensiktsmessige forhold til en eventuell risiko.

Funn 7 – Lokal administratortilgang
Det kommenteres i rapporten at det gis administratorrettigheter til brukere med spesielle behov for installasjon på PCer. Tilgangen er riktignok tidsbegrenset til to timer. Det må vurderes om denne prosedyren skal fjernes. I så fall må det etableres en ny rutine der den ansatte får besøk av en teknikker fra Virksomhet digitalisering. Vurderingen av eventuell ny løsning bør sees opp mot mulig risiko.

Med hilsen

Dette dokumentet er elektronisk godkjent og sendes uten signatur

Martine Bjar Manskow
kst. virksomhetsleder

Kopi til interne mottakere:

Nina Tangnæs Grønvold	Kommunedirektør
Atle Holten	Seksjon for innovasjon og styring
Ketil Johansen	Digitalisering
Bjørn Klubbenes	Styring og eierskap

9. VEDLEGG

9.1. Utledning av revisjonskriterier

Planer, rutiner og tiltak (problemstilling 1 og 2)

Personvernforordningens regler om informasjonssikkerhet følger av artikkel 32. Bestemmelsen fastslår at både den behandlingsansvarlige og databehandleren plikter å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen», eForvaltningsforskriften skal legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger.
Digitaliseringsdirektoratet sier i sin veileder til informasjonssikkerhet at offentlige virksomheter skal i henhold til eForvaltningsforskriften §15 etablere mål og strategi for informasjonssikkerhet og et tilfredsstillende system for internkontroll.

Sikkerhetsmålene bør beskrive både formål med informasjonsbehandlingen i forvaltningsorganet og overordnede føringer for informasjonsbehandling og bruk av IKT. Disse føringene vil naturlig uttrykkes som mål med vekt på konfidensialitet, integritet og tilgjengelighet i virksomhetens informasjonsbehandling og bruk av IKT. Sikkerhetsstrategien omfatter sentrale valg og prioriteringer i sikkerhetsarbeidet. Sikkerhetsstrategien består naturlig av to hoveddeler:

1. Retningslinjer for hvordan sikkerhetsarbeidet skal organiseres og gjennomføres
2. Retningslinjer for relevante tiltaksområder.

De siste bør etableres etter risikovurderinger i internkontrollarbeidet.

Alle offentlige virksomheter må imidlertid ha tilstrekkelig oversikt for å være i stand til gjøre gode vurderinger, og kunne identifisere skjermingsverdig informasjon og skjermingsverdige informasjonssystemer. Alle virksomheter bør også vurdere om de i gitte situasjoner må være i stand til å motta og håndtere sikkerhetsgradert informasjon, eksempelvis i en krisesituasjon. Disse virksomhetene må legge til rette for at klarert personell kan motta og håndtere gradert informasjon.

Stortingsmeldingen om IKT-sikkerhet (Meld. St. nr. 38 (2016-2017) IKT-sikkerhet – Et felles ansvar), ble lagt frem våren 2017 og behandlet i Stortinget i vårsesjonen 2018. Styrking av den nasjonale evnen til å avdekke og håndtere digitale angrep er et av hovedområdene som omtales i stortingsmeldingen. Et sentralt tiltak for å bidra til en slik styrking er etableringen av et rammeverk for håndtering av IKT-sikkerhetshendelser.

Hensikten med rammeverk for håndtering av IKT-sikkerhetshendelser er å avklare og tydeliggjøre innsatsen mellom relevante aktører, for å være i bedre i stand til å håndtere alvorlige IKT-sikkerhetshendelser som rammer på tvers av sektorer. De etablerte beredskapsprinsippene[41] ligger til grunn for rammeverket.

[41] Arbeidet med samfunnssikkerhet og beredskap tar utgangspunkt i etablerte prinsipper for krisehåndtering; ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet. Se Meld. St. nr. 10 (2016-2017) Risiko i et trygt samfunn – Samfunnssikkerhet

Det følger av Rammeverk for håndtering av IKT-sikkerhetshendelser kapittel 3 at IKT-sikkerhetshendelser som faller inn under rammeverkets virkeområde skal håndteres gjennom en systematisk prosess bestående av 1) planlegging og forberedelse; 2) deteksjon og vurdering av omfang og alvorlighetsgrad; 3) varsling av relevante parter; 4) iverksetting av prosesser og tiltak for å håndtere hendelsen; 5) situasjonsrapportering og 6) tilbakeføring og læring av hendelsen. En slik prosess er i overensstemmelse med ISO/IEC 27001.[42]

Planlegging og forberedelse
Planlegging og forberedelse handler om å etablere prosedyrer for håndtering av hendelser, inkludert rapportering, ansvarslinjer og eskaleringsrutiner og etablering av et IKT-risikobilde.
Det forutsettes at virksomheter som omfattes av rammeverket har implementert en grunnsikring basert på egne risiko- og sårbarhetsvurderinger. En risiko- og sårbarhetsanalyse er en strukturert vurdering av sannsynlighet og konsekvenser av uønskede hendelser, som bidrar til å avdekke fokusområder for sikring av systemene.
Virksomheter forutsettes å:

- motta, vurdere og formidle informasjon fra og til eget sektorvise responsmiljø (SRM)
- ha systemer for loggføring av nettverkstrafikk
- delta i samhandlingsøvelser
- ha beredskapsplaner for håndtering av større hendelser og sikkerhetspolitiske kriser i det digitale rom
- oppdatere seg gjennom relevante utredninger og årlige og løpende trusselvurderinger rettet mot det digitale rom
- gjennomføre jevnlige risikovurderinger for egen virksomhet rettet mot det digitale rom
- oppdatere kontaktinformasjon og melde inn endringer til eget SRM

NorSIS[43] ferdigstilte i desember 2017 en utredning om behovet for et kommune CSIRT[44]. Utredningen har kartlagt og beskrevet de felles behovene for støtte til håndtering av IKT-sikkerhetshendelser i kommunal sektor. Rapporten legger til grunn at det ikke er formalisert et kontaktpunkt for kommunal sektor i den nasjonale CERT[45]-strukturen, men at deler av kommunal sektor dekkes gjennom kontaktpunkter i øvrige responsmiljøer som HelseCERT, KraftCERT og NorCERT[46].
Vi tolker dette slik at sektorvist responsmiljø som er relevant for kommunen i denne sammenhengen, i hovedsak vil være NorCERT – den operative delen av NSM, og Norges nasjonale CERT og cybersenter. NorCERT håndterer alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon. Avhengig av type hendelse vil også HelseCERT være et relevant SRM.

Deteksjon og vurdering av omfang og alvorlighetsgrad
Brukere, enheter, leverandører, politiet, NSM eller andre kan oppdage sikkerhetskritiske hendelser. Dersom en IKT-sikkerhetshendelse identifiseres skal alltid de som oppdager at andre er rammet, gjøre den rammede virksomheten oppmerksom på dette.
Her forutsettes virksomheter å:

- ha beredskap for rettidig å avdekke hendelser

[42] Standard for informasjonssikkerhet, publisert av International Organization for Standardization (ISO) og International Electrotechnical Commision (IEC).
[43] Norsk senter for informasjonssikring
[44] Computer Security Incident Response Team
[45] Computer Emergency Response Team – en koordinerende enhet for informasjonssikkerhet.
[46] Den operative delen av Nasjonal sikkerhetsmyndighet (NSM) og Norges nasjonale CERT og cybersenter som håndterer alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.

- ha kompetanse om relevante systemer i virksomhet og kunne vurdere alvorlighetsgrad, omfang og konsekvenser på overordnet nivå
- kunne vurdere om kritisk infrastruktur og/eller kritiske samfunnsfunksjoner er eller står i fare for å bli berørt av hendelsen
- bruke NSMs system for klassifisering av hendelser, eller et system som er kompatibelt med dette
- vurdere behov for bistand

Varsling av relevante parter
Når en hendelse er avdekket igangsettes varsling parallelt med kartlegging av inntruffet hendelse. Varsling kan gjøres til nære samarbeidspartnere som er mistenkt utsatt for samme hendelse, før det vurderes om virksomhetens SRM varsles.
Virksomheter forutsettes å:

- ha rutiner for å varsle om IKT-sikkerhetshendelser til SRM og eventuelt samarbeidende virksomheter, samt til NSM under forutsetninger[47] angitt i kapittel 3.3 i rammeverket.

Iverksetting av prosesser og tiltak for å håndtere hendelsen
Rammeverket omfatter kun håndtering knyttet til å stanse hendelsen, skadevurdere, begrense skadeomfang og gjenopprette sikker tilstand. Tiltak for å gjenopprette sikker tilstand utføres i all hovedsak av virksomheten selv gjennom sin IT-avdeling / -partner.
Virksomheter forutsettes å:

- etablere, eller ha tilgang til, tilstrekkelig evne og kapasitet til å håndtere IKT-sikkerhetshendelser.

Situasjonsrapportering
Situasjonsrapportering skal gå både fra virksomhets- og sektornivå til nasjonalt nivå, og fra nasjonalt nivå til sektor- og virksomhetsnivå.
Virksomheter forutsettes å:

- benytte NSMs system for rapportering av IKT-sikkerhetshendelser, herunder klassifisering og kategorisering, eller et system som er kompatibelt med dette.
- Rapportere alle IKT-sikkerhetshendelser til SRM, også de hendelser som blir håndtert internt i virksomhet. Sistnevnte rapportering kan skje i etterkant av hendelseshåndteringen.

Tilbakeføring og læring av hendelsen
Etter at hendelseshåndteringen knyttet til gjenoppretting av sikker tilstand er avsluttet, starter arbeidet i virksomheten med å lukke sårbarheter og øke grunnsikringen dersom det er nødvendig. Tiltak som iverksettes må baseres på en grundig analyse av hva som gikk galt og om det etablerte sikkerhetsnivået gir god nok sikkerhet.
Virksomheter forutsettes å:

- Dersom hendelsen ikke allerede er varslet og/eller anmeldt til politiet, bør dette gjøres av virksomheten
- Delta i evalueringsarbeid i egen sektor, avhengig av omfang og involvering
- Evaluere og forbedre egen evne til håndtering av IKT-sikkerhetshendelser

[47] Dersom virksomheten er knyttet til VDI-samarbeidet (Varslingssystem for Digital Infrastruktur, et nasjonalt sensornettverk på internett), har en bilateral avtale med NSM, eller ikke er tilknyttet et SRM og hendelsen oppfyller kriteriene for å varsle SRM.

- Implementere tiltak for å styrke evne til å motstå lignende hendelser senere (grunnsikring)
- Dele læringspunkter etter en hendelse med SRM.

Som en del av **Nasjonal strategi for digital sikkerhet**, lagt frem på lanseringskonferanse i januar 2019, er det utarbeidet anbefalte tiltak for bedret digital sikkerhet. Tiltakene er todelt. Den første delen er rettet mot sentrale tiltak, og den andre delen har 10 anbefalte tiltak rettet mot virksomheter i offentlig og privat sektor. Det fremkommer av dokumentet at virksomheter må gjennomføre nødvendige tiltak for å sikre IKT-systemene, og at NSMs grunnprinsipper for IKT-sikkerhet beskriver tiltak som alle virksomheter bør implementere for god grunnsikring. Anbefalte tiltak for virksomheter er:

- **Ledelse**. Det bør etableres aktiviteter for sikkerhetsstyring, hvor det er tydelige krav og forventninger til sikkerhet.
- **Risikostyring**. Etabler prosess for risikostyring som er en del av en helhetlig styringsstruktur, prosessen må være kjent i virksomheten. Etabler tydelig ansvar og effektive rapporteringslinjer til toppledelse og styre.
- **Kartlegg verdikjeder, informasjonsverdier, utstyr og brukertilganger**. Lag en oversikt over virksomhetens sentrale mål, hvilke verdier og verdikjeder som inngår, hvor viktige data lagres og hvem som har tilgang til disse dataene.
- **Inkluder digital sikkerhet i virksomhetskulturen**. Virksomheter må sørge for at ansatte har nødvendig informasjon, kunnskap og ferdigheter til å opprettholde ønsket sikkerhetsnivå. Kartlegg virksomhetens sikkerhetskultur og identifiser hva som kan forbedres. Fastsett ønsket kultur og gjennomfør tilpasset, årlige treningsprogram for å fremme god sikkerhetskultur.
- **Leverandørkontroll**. Det må stilles krav til produkter og leverandører slik at sikkerheten er ivaretatt i hele produktets eller tjenestens levetid. Sats på god bestillerkompetanse og gjør en risikovurdering som forankres hos ledelsen.
- **Sikker konfigurasjon**. Konfigureringen må oppdateres kontinuerlig, i takt med endringer i teknologi, bruksmønster og trusselbilde. Oppgrader program- og maskinvare. Fjern unødvendig kompleksitet og ubrukt funksjonalitet. Blokker kjøring av ikke-autoriserte programmer.
- **Kontroll på nettverk og systemkomponenter**. Virksomheten må innføre tiltak for beskyttelse mot skadevare, overvåkning og analyse av IKT-systemet og håndtering av endringer. Installer sikkerhetsoppdateringer så raskt som mulig. Beskytt trådløse nettverk med sterke sikkerhetsmekanismer. Planlegg og dokumenter endringer. Slå på logging og gjennomgå viktige logger jevnlig.
- **E-post og websikkerhet**. Virksomheten bør ha kontroll på informasjonsflyten som går til og fra eget nettverk, samt innad i eget nettverk. Bruk kun siste versjon av nettlesere. Beskytt e-post med DMARC[48]. Krypter viktig informasjon når det lagres på bærbare medier og når det sendes over nettet.

- **Tilgangskontroll**. Virksomheten må ha kontroll på kontoer, kontrollere bruk av administrative privilegier, sørge for sikker pålogging og jevnlig gjennomgå tilgangsrettigheter. Fysisk tilgang til nettverk og informasjonssystemer, inkludert datarom, bør tilgangsstyres på lik linje med logiske tilganger. Endre standard passord og ikke tildel sluttbrukere administratorrettigheter. Bruk 2-faktor autentisering, eller som et minimum, sterke passord.

[48] Domani based Message Authentication, Reporting and Conformance. Mekanisme som sjekker om innkommende e-post faktisk kommer fra domenet det påstår at det kommer fra (autentisering av avsender).

- **Hendelsesberedskap**. Etabler en beredskapsplan for ulike typer hendelser og gjennomfør øvelser som tester planverket.

Nasjonal strategi for digital sikkerhet og rammeverk for håndtering av IKT-sikkerhetshendelser viser begge til NSMs veileder **«Grunnprinsipper for IKT-sikkerhet»** som beskriver hva en virksomhet bør gjøre for å sikre et IKT-system, og hvorfor. Grunnprinsippene er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet, og uthever de viktigste sikringstiltakene i ISO/IEC 27002:2017.
Ifølge veilederen vil en angriper som regel bruke enkleste veien inn i systemene. Om det finnes sikringstiltak som er enkle å omgå vil angriperen lete etter, og utnytte, dette. Sårbarheter kan oppstå dersom kvaliteten på anskaffelsesprosessen ikke er god nok slik at komponenter eller tjenester med manglende sikkerhetsfunksjonalitet, manglende sikkerhetsrettinger eller feil konfigurasjon innføres. Sårbarheter kan også skyldes feil på produktet, plantede sårbarheter, oppdateringer eller vedlikehold. For i størst mulig grad å hindre sårbarheter fra å oppstå bør sikkerhet være en del av virksomhetens tankegang fra beslutning og anskaffelse til drift, vedlikehold og avskaffelse.
Veilederen er delt i fire kategorier som hver beskriver tiltak som virksomheten bør implementere for å sikre sine systemer:

- **Identifisere og kartlegge –** opparbeide og forvalte forståelse om virksomheten, herunder leveranser, tjenester, systemer og brukere.
- **Beskytte –** prinsipper som må til for å ivareta en sikker tilstand for IKT-miljøet, for å motstå eller begrense skaden fra dataangrep.
- **Opprettholde og oppdage –** prinsipper som ivaretar behovet for å håndtere endringer, både planlagte endringer, feilretting og sikkerhetsoppdateringer for å opprettholde den sikre tilstanden over tid.
- **Håndtere og gjenopprette –** prinsipper for å få på plass aktiviteter for å håndtere oppdagede sikkerhetstruende hendelser.

For nærmere beskrivelse av kategoriene og tilhørende tiltak viser vi til veilederen i sin helhet.
NSM har videre publisert sjekklistene S-01, «fire effektive tiltak mot dataangrep» og S-02, «ti viktige tiltak mot dataangrep», som supplerer dokumentet «Grunnleggende tiltak for sikring av Windows 7, U-01». Veilederen og sjekklistene er tilgjengelige på NSMs hjemmesider. Sjekklistene er av generell karakter og anses for å være relevante til tross for at nyere versjoner av Windows operativsystem er tilgjengelig.

Fokuset til sjekklistene er grunnleggende Windows 7 sikkerhetstiltak. Målgruppen er store og middels store virksomheter, primært i offentlig forvaltning. Tiltakene gir ikke 100 % sikkerhet mot alle typer angrep, som for eksempel tapping av kommunikasjon over internett, tjenestenektangrep, eller angrep fra avanserte statlige aktører og angrep der angriperen har fysisk tilgang til utstyret. Tiltakene forhindrer heller ikke at godtroende brukere oppgir sensitive opplysninger på nett.
De fire første tiltakene i S-02 er sammenfallende med tiltakene i S-01. Tiltakene i S-02 er:

- oppgrader program- og maskinvare
- installer sikkerhetsoppdateringer så fort som mulig
- ikke tildel administrator-rettigheter til sluttbrukere
- blokker kjøring av ikke-autoriserte programmer
- aktiver kodebeskyttelse mot ukjente sårbarheter
- herde applikasjoner
- bruk klientbrannmur
- bruk sikker oppstart og diskkryptering
- bruk antivirus/antiskadevare

- ikke installer mer funksjonalitet enn nødvendig

Basert på ovennevnte føringer, har revisjonen utledet følgende revisjonskriterier for problemstilling 1 og 2:

Problemstilling 1
Har kommunen tilfredsstillende planer og rutiner for håndtering IKT-sikkerhetsmessige situasjoner?

- Kommunen gjennomfører risikovurderinger knyttet til IT-sikkerhet.
- Kommunen har planer og rutiner (sikkerhetstiltak) for å sikre beredskap ved sikkerhetshendelser.
- Planene og rutinene er kjent for de ansatte.
- Det er utarbeidet rutiner for å varsle om IKT-sikkerhetshendelser. Herunder om det skal varsles til SRM og eventuelt samarbeidende virksomheter, samt til NSM om nødvendig.
- Kommunen vurderer behov for bistand ved IKT-sikkerhetshendelser.

Problemstilling 2
Har kommunen etablert, evt. innført/gjennomført? tilfredsstillende sikkerhetstiltak av sine datasystemer mot dataangrep?

- Kommunen loggfører nettverkstrafikk.
- Kommunens ledelse kommuniserer krav og forventninger til sikkerhet på en tilgjengelig og forståelig måte til sine ansatte.
- Kommunens prosess for risikostyring, ansvar for denne og rapporteringslinjer til øvre ledelse er kjent.
- Kommunen har oversikt over hvor viktige data lagres og hvem som har tilgang til disse dataene.
- Kommunen stiller krav om sikkerhet ved anskaffelse av digitale produkter og tjenester.
- Kommunen konfigurerer enheter som skal kobles til kommunens nett. Program- og maskinvare oppdateres kontinuerlig, og kjøring av ikke-autoriserte programmer er blokkert.
- Unødvendig kode og makroer deaktiveres i autoriserte programmer/applikasjoner.
- IKT- systemet overvåkes og analyseres, endringer er planlagt og dokumentert, og viktige logger gjennomgås jevnlig.
- Kommunen har beskyttet sin e-post kommunikasjon, og krypterer informasjon på bærbare medier og ved oversendelse på nett.
- Kommunen bruker antivirus/antiskadevare og har kodebeskyttelse mot ukjente sårbarheter.
- Fysisk tilgang til nettverk- og informasjonssystemer er tilgangsstyrt.
- Sluttbrukere har ikke administratorrettigheter og kommunen gjennomgår jevnlig tilgangsrettigheter.
- Kommunen setter krav til passordstyrke, og bruker 2-faktor autentisering.
- Uønsket/ubedt trafikk blokkeres av brannmur/klientbrannmur og loggfiler gjennomgås jevnlig.
- Kommunen bruker sikker oppstart og diskkryptering.

Styringssystem for informasjonssikkerhet (problemstilling 3)

Informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger.

Informasjonssikkerhet omfatter beskyttelse av[49]:

- Konfidensialitet – at informasjonen ikke blir kjent for uvedkommende
- Integritet – at informasjonen ikke blir endret utilsiktet eller av uvedkommende
- Tilgjengelighet – at informasjonen er tilgjengelig for autoriserte ved behov
- Robusthet – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser

Med andre ord krever personvernregelverket at personopplysninger skal beskyttes mot uberettiget innsyn og endringer. Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene, når de har behov for dem.

Personvernforordningen stiller krav til den behandlingsansvarliges ansvar. Det innebærer å sette i verk egnede tiltak, både tekniske og organisatoriske, for å sikre og påvise at personopplysninger behandles i samsvar med regelverket.

Kommunen er gjennom eforvaltningsforskriften § 15 pålagt å ha internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Kravet gjelder all informasjonsbehandling i kommunen, og eforvaltningsforskriften vil derfor være et naturlig utgangspunkt for alt informasjonssikkerhetsarbeid i offentlige virksomheter. Relevante krav i annet regelverk, som for eksempel personopplysningsregelverket, skal da inkluderes. Behandling av informasjon som kommer inn under sikkerhetsloven, skal også bli henledet til de bestemmelsene som gjelder for de. eForvaltningsforskriften § 15 stiller krav om at internkontrollen på informasjonssikkerhetsområdet skal basere seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Difi er i henhold til forskriften utpekt til å gi anbefalinger på området. Difi anbefaler at internkontrollen skal baseres på den internasjonale standarden ISO/IEC 27001:2013.[50] Difi har utarbeidet veiledningsmateriell basert på denne standarden. Standarden videreutvikles løpende. Revisjonen har i denne utledningen benyttet versjon 1.4, sist oppdatert 7.2.19.

Sikkerhetsmål
Sikkerhetsmålene omfatter ledelsens beslutninger om hva IKT skal brukes til i virksomheten, og hvordan den skal benyttes for å oppnå virksomhetens øvrige mål. I henhold til Difis veileder for internkontroll informasjonssikkerhet bør sikkerhetsmålene beskrive både formål og føringer for informasjonsbehandling og bruk av IKT, med vekt på konfidensialitet, integritet og tilgjengelighet.

Strategi for informasjonssikkerhet
I henhold til Difis veileder omfatter strategien sentrale valg og prioriteringer i sikkerhetsarbeidet, og består naturlig av to hoveddeler:

1. Retningslinjer for hvordan sikkerhetsarbeidet skal organiseres og gjennomføres. Retningslinjene må klargjøre roller, myndighet og ansvar, og omfatte føringer for en systematisk organisering og gjennomføring av aktivitetene i internkontrollarbeidet.
2. Retningslinjer for relevante tiltaksområder, som bør etableres basert på risikovurderinger i internkontrollarbeidet.

[49] Jf. Personvernforordningen artikkel 32 bokstav b
[50] Jf. Referansekatalogen, bruksområde «Internkontroll/styringssystem/ledelses system for informasjonssikkerhet».

Ledelsens styring og oppfølging
I henhold til ISO/IEC 27001, skal virksomheten kontinuerlig forbedre egnetheten, tilstrekkeligheten og effektiviteten til styringssystemet for informasjonssikkerhet.[51] Toppledelsen skal gjennomgå styringssystemet ved planlagte intervaller for å forsikre seg om at dette skjer.[52]
Virksomheten skal, i henhold til ISO/IEC 27001, definere og dokumentere styringssystemets omfang, basert på kartlagte eksterne og interne forhold, interessenters krav og forventninger, grensesnitt og avhengigheter mellom aktiviteter utført av virksomheten selv, og de som utføres av andre. [53]
Virksomheten skal videre ha kontroll med prosesser som er satt ut til tredjepart.[54]
I henhold til standardens punkt 5.2, skal toppledelsen etablere en informasjonssikkerhetspolicy, og sørge for at den er dokumentert og kommunisert. Policyen skal

- være hensiktsmessig sett opp mot virksomhetens formål
- inneholde mål for informasjonssikkerheten, eller et rammeverk for å sette slike mål
- forplikte virksomheten til å oppfylle definerte krav til informasjonssikkerhet og sørge for kontinuerlig forbedring

Videre skal toppledelsen sørge for at ansvar og myndighet, som er relevant for informasjonssikkerheten, er delegert og kommunisert. Dette gjelder også ansvar og myndighet for å sikre at styringssystemet er i samsvar med standarden, og for å rapportere til toppledelsen om hvordan styringssystemet fungerer.[55]
Datatilsynet gir i sin veileder for internkontroll og informasjonssikkerhet[56] nærmere beskrivelse av hvordan ansvar og myndighet bør fordeles:
«Det må klargjøres roller og ansvar knyttet til personvern og sikkerhet internt i virksomheten. Det inkluderer for eksempel hva som ligger i linjeansvar og hva som ligger i nøkkelroller som personvernombud, personvernrådgiver, sikkerhetsleder, IKT-ansvarlig, HR-ansvarlig, prosjektledere, produkteiere, systemeiere, systemforvaltere mv. Klare ansvars- og myndighetsforhold etableres med utgangspunkt i beslutninger tatt av virksomhetens ledelse. Rolle- og ansvarsfordeling skal være dokumentert.»
Datatilsynets veileder foreslår også at ledelsen årlig skal gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. I ledelsens gjennomgang av informasjonssystemet kan blant annet følgende vurderes:

- Resultater fra sikkerhetsrevisjoner og kontroller utført av offentlig myndighet
- Endringer med betydning for drift av informasjonssystemet eller for informasjonssikkerheten, herunder endringer i offentlige sikkerhetskrav, endringer i personopplysninger som virksomheten skal behandle, endringer i trusselbildet som blant annet beskrevet i rapport fra utførte risikovurderinger
- Om informasjonssystemet bør endres, eksempelvis som følge av ønske om ny funksjonalitet
- Overordnet behandling av alvorlige avvik og hendelser

Risikovurdering
I henhold til ISO/IEC 27001 punkt 8.2 skal risikovurderinger gjennomføres i planlagte intervaller, og når vesentlige endringer planlegges eller oppstår. Videre skal en plan for håndtering av risikoer implementeres.[57] Virksomheten skal oppbevare dokumentert informasjon om prosessene for

[51] Jf. 10.2
[52] Jf. 9.3
[53] Jf. 4.3
[54] Jf. 8.1
[55] Jf. 5.3
[56] Publisert 23.6.2018
[57] Jf. 8.3

risikovurdering og risikohåndtering[58], og også oppbevare dokumentert informasjon om resultatene av risikovurderingene og risikohåndteringsprosessen med påfølgende tiltaksetablering.[59]
Datatilsynet skriver følgende om dette i sin veileder for internkontroll og informasjonssikkerhet:
«En risikovurdering begynner med en kartlegging av verdier som bør sikres. Personvernregelverket definerer personopplysninger som en verdi. Det bør gjøres en trusselvurdering av hvilke aktører som kan være interessert i verdiene og hvilke angrepsvektorer de ulike trusselaktørene benytter. Deretter gjøres en vurdering av om verdiene er sårbare for de gitte truslene.»

Risikohåndtering
Ifølge standarden[60] skal virksomheten velge hensiktsmessig håndtering av de risikoene som krever håndtering ut fra risikokriterier, og bestemme hvilke tiltak som er nødvendige å innføre. Tiltak kan designes etter behov eller velges fra hvilken som helst kilde. De valgte tiltakene skal vurderes opp mot tiltakene som er beskrevet i standardens vedlegg A, for å sikre at ingen relevante tiltak er utelatt i vurderingen. Virksomheten skal så lage en erklæring om relevans (Statement of Applicability – SoA), som viser valgte tiltak med begrunnelse for hvorfor de er valgt, og om de er implementert eller ikke. Erklæringen skal også inneholde begrunnelser for de tiltakene i vedlegg A som er utelatt. Det skal videre utarbeides en plan for håndtering av risikoen. Risikoeier skal godkjenne planen og den gjenværende risikoen.[61]
Virksomheten skal oppbevare dokumentert informasjon om prosessene for risikohåndtering, om resultatene fra håndteringen av informasjonssikkerhetsrisikoene, og resultatene av korrigerende tiltak.[62]

Overvåking og hendelseshåndtering
Virksomheten skal overvåke informasjonssikkerheten. I henhold til standardens punkt 9.1, skal det defineres hva som skal overvåkes, og når, hvilke metoder som skal benyttes, hvem som skal overvåke, når resultatene skal analyseres og evalueres, og hvem som skal gjennomføre analysen og evalueringen.

Måling, evaluering og revisjon
Virksomheten skal gjennomføre måling av effektiviteten på styringssystemet for informasjonssikkerhet, herunder de iverksatte sikkerhetstiltakene. Det skal defineres hva som skal måles, når det skal måles, hvilke metoder som skal benyttes, hvem som skal gjennomføre målingen, når resultatene skal analyseres og evalueres, og hvem som skal gjennomføre analysen og evalueringen.[63] Trender observert gjennom resultatene av målingene skal identifiseres og benyttes under ledelsens gjennomgang.[64]

Datatilsynet beskriver i sin veileder hvordan virksomheten kan kontrollere sitt eget styringssystem for informasjonssikkerhet. Ifølge veilederen skal virksomheten kontrollere at rutinene for håndtering av personopplysninger brukes og fungerer etter hensikten. Videre må virksomheten i henhold til veilederen, jevnlig teste, vurdere og evaluere hvor effektive sikkerhetstiltakene er. En sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak, og bruk av sikkerhetsparter og databehandlere. Ifølge veilederen består sikkerhetsrevisjon vanligvis av egenkontroller, internrevisjon og revisjon av eksterne parter. Dersom sikkerhetsrevisjonen avdekker

[58] Jf. 6.1.2 og 6.1.3
[59] Jf. 6.1.3 og 8.3
[60] ISO/IEC 27001 punkt 8.1
[61] Jf. 6.1.3 a-f
[62] Jf. 6.1.3, 8.3 og 10.1 g
[63] Jf. ISO/IEC 27001 9.1
[64] Jf. 9.3

bruk av informasjonssystem som ikke er forutsatt, skal dette behandles som et avvik. Resultatet fra sikkerhetsrevisjonen skal dokumenteres og være en del av ledelsens gjennomgang.
Ifølge ISO/IEC 27001, skal virksomheten oppbevare dokumentert bevis på gjennomføring av måling.[65] Trender som er observert gjennom målingen, skal dokumenteres, og er del av grunnlaget for ledelsens gjennomgang.[66] Revisjonsplanene med tilhørende beskrivelse av kriterier og omfang, og resultatene av revisjonen, skal dokumenteres og rapporteres til relevant ledelse. Disse er også en del av grunnlaget for ledelsens gjennomgang.[67]

Utledede revisjonskriterier
Oppsummert, vil revisjonen benytte følgende revisjonskriterier for å svare på om kommunen har etablert et tilfredsstillende styringssystem for informasjonssikkerhet:

- Det er fastsatt overordnede målsettinger for informasjonssikkerhet i kommunen.
- Det er utarbeidet en overordnet strategi for å nå målene på området, som er basert på risikovurderinger.
- Strategien gjennomgås jevnlig, og oppdateres ved behov, for å sikre at den til enhver tid er i samsvar med kommunens behov.
- Det er etablert og beskrevet klare ansvars- og myndighetsforhold for kommunens informasjonssikkerhetsarbeid.
- Kommunen har rutiner og retningslinjer for risikovurdering og risikohåndtering knyttet til informasjonssikkerhet.
- Kommunen dokumenterer prosessene rundt risikohåndtering og resultatene fra håndtering av informasjonssikkerhetsrisikoene og resultat av korrigerende tiltak.
- Informasjonssikkerheten i kommunen overvåkes etter definerte mål og metoder, og resultatene analyseres og evalueres.
- På et overordnet nivå, følger kommunen opp at informasjonssikkerheten blir ivaretatt i tråd med lov og forskrift, og øvrig internt og eksternt regelverk på området.

De ansattes kjennskap til retningslinjer og rutiner for informasjonssikkerhet (problemstilling 4)

Kompetanse- og kulturutvikling
I henhold til standardens punkt 7.3, skal ansatte kjenne til informasjonssikkerhetspolicyen, deres bidrag til effektiviteten av styringssystemet for informasjonssikkerhet, og fordelene med forbedret håndtering av informasjonssikkerheten. De skal også kjenne til hva det kan medføre dersom kravene til informasjonssikkerhet ikke etterleves.

Standardens punkt 7.2 sier at virksomheten skal kartlegge hvilken kompetanse som er nødvendig for ansatte som utfører arbeid som kan påvirke informasjonssikkerheten. Basert på kartleggingen skal virksomheten påse av disse ansatte får nødvendig erfaring og kompetanse gjennom utdanning og trening. Effekten av slike kompetansehevingstiltak skal evalueres. Standarden stiller dessuten krav til at virksomheten oppbevarer hensiktsmessig dokumentert informasjon som bevis på kompetansen.

[65] Jf. 9.1
[66] Jf. 9.3
[67] Jf. 9.2 og 9.3

Datatilsynet råder i sin veileder virksomheten til å sørge for hensiktsmessig opplæring, før ansatte og eventuelle tredjepartsbrukere får tilgang til informasjon eller tjenester. Dette omfatter krav til internkontroll og informasjonssikkerhet, juridisk ansvar og interne sikringstiltak, så vel som opplæring i riktig bruk av informasjonssystemer. Dette inkluderer for eksempel innloggingsprosedyrer, bruk av programvare, sikkerhetsinstruks, og rapportering av avvik. I tillegg bør de få regelmessig oppdatering i organisasjonens policy og rutiner.

Kommunikasjon
I henhold til standardens punkt 7.4, skal virksomheten fastsette behovet for intern og ekstern kommunikasjon, herunder hvem som er ansvarlige for å kommunisere, hva som skal kommuniseres, når det skal kommuniseres, i hvilken form det skal kommuniseres, og til hvem.
Dokumentert informasjon skal ha hensiktsmessig identifikasjon, være hensiktsmessig beskrevet og være i et hensiktsmessig format. Den skal være gjennomgått og godkjent ut fra formålene egnethet og tilstrekkelighet.[68]

Dokumentert informasjon skal være tilgjengelig og egnet for bruk når det er behov for den. Den skal være tilstrekkelig sikret. Avhengig av relevans, skal virksomheten vurdere blant annet distribusjon, tilgang, lagring, bevaring og endringskontroll.[69]

Skal en kommune lykkes med å få tilstrekkelig styring og kontroll med informasjonssikkerheten, er det ikke nok med systematiske planer, policyer, retningslinjer, styringsparametere og oppfølging. Kulturen i organisasjonen er avgjørende.

Som vist i utleding av kriterier til problemstilling 3, er kompetanse- og kulturutvikling en viktig del av et tilfredsstillende styringssystem for informasjonssikkerhet, og de ansatte skal kjenne til virksomhetens informasjonssikkerhetspolicy, og deres bidrag til effektiviteten av styringssystemet for informasjonssikkerhet. De skal også kjenne til hva det kan medføre dersom kravene til informasjonssikkerhet ikke etterleves.

Datatilsynet skriver følgende om brukeropplæring i sin veileder om internkontroll og informasjonssikkerhet:
«Målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt, og at de er gitt mulighet til å etterleve dette i sitt daglige arbeid. Opplæring bør være tilpasset ulike målgruppers behov for opplæring og fordeles over tid. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.»
I henhold til veilederen, bør de ansatte ha fått hensiktsmessig opplæring før de får tilgang til informasjon eller tjenester. Dette inkluderer for eksempel at de kjenner til innloggingsprosedyrer, bruk av programvare, sikkerhetsinstruks og rapportering av avvik. I tillegg bør de ansatte, ifølge veilederen, få regelmessig oppdatering i organisasjonens policy og rutiner.
Datatilsynets veiledere påpeker også at taushetserklæringer kan brukes for å gjøre oppmerksom på at det forekommer konfidensiell informasjon i virksomheten. De ansatte skal ifølge veilederen, undertegne en slik erklæring samtidig med ansettelseskontrakten. Dette gjelder også midlertidig ansatte.

[68] Jf. 7.5.2
[69] Jf. 7.5.3

Utledede revisjonskriterier

Basert på dette legger revisjonen følgende kriterier til grunn for denne problemstillingen:

- Det gjennomføres kompetansetiltak som bidrar til at medarbeidere som bruker kommunens informasjonssystemer, har tilstrekkelig kompetanse til å ivareta kommunens sikkerhetsbehov, og til å ivareta gjeldende krav og føringer for informasjonssikkerhet.
- De ansatte kjenner til kommunens informasjonssikkerhetspolicy/overordnet strategi for informasjonssikkerhet.
- De ansatte har fått opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer.
- De ansatte kjenner til kommunens egne rutiner og prosedyrer for informasjonssikkerhet.
- De ansatte har undertegnet en taushetserklæring ved inngåelse av arbeidsforholdet.

9.2. Utplukk til phishing-test

Ansvarsnummer	Ansvarsnavn	Antall
155040	KOMMUNIKASJON	6
171001	INNOVASJON OG STYRING STAB OG LEDELSE (NY 2019)	3
175001	PU STAB (NY 2019)	2
322001	FAGSTAB MILJØ OG BYUTVIKLINGSETATEN	3
322201	FAGGRUPPE OPPMÅLING	2
322202	FAGGRUPPE KART/GIS	2
322601	REGULERING OG BYGGESAK	6
412001	TD STAB FOR PLAN OG UTVIKLING	7
413101	BE STAB OG LEDELSE	3
413201	BE EIENDOMSDRIFT	4
413301	BE EIENDOMSFORVALTNING	1
413701	BE BOLIGBYGG (NY 2019)	4
414101	VAR STAB OG LEDELSE	2
415101	BYDRIFT STAB OG LEDELSE (NY 2019)	1
570201	SKOLE	15
571001	FREDRIKSTAD INTERNASJONALE SKOLE (FRIS)	
572001	BORGE UNGDOMSSKOLE	
572101	VESTBYGDA UNGDOMSSKOLE	
572201	GRESSVIK UNGDOMSSKOLE	
572301	HAUGEÅSEN UNGDOMSSKOLE	
572401	KRÅKERØY UNGDOMSSKOLE	
572501	KVERNHUSET UNGDOMSSKOLE	
573001	BEGBY BARNE- OG UNGDOMSSKOLE	
573101	CICIGNON BARNE- OG UNGDOMSSKOLE	
573201	GUDEBERG BARNE- OG UNGDOMSSKOLE	
574001	AMBJØRNRØD SKOLE	
574101	BORGE SKOLE	
574201	HAUGE SKOLE	
574301	HURRØD SKOLE	
574401	KJØLBERG SKOLE	
574501	LUNDE SKOLE	
574601	MANSTAD SKOLE	
574701	SAGABAKKEN SKOLE	
574801	NYLENDE SKOLE	
574901	NØKLEBY SKOLE	
575001	REKUSTAD SKOLE	
575101	K - RØD SKOLE	
575201	O - RØD SKOLE	
575301	RØDSMYRA SKOLE	
575401	SLEVIK SKOLE	
575501	TORP SKOLE	
575601	TORSNES SKOLE	
575603	VIKARRESSURS SFO	
575701	TRARA SKOLE	
575801	TROSVIK SKOLE	

575901	ÅRUM SKOLE	
576501	RÅKOLLEN SKOLE	
576502	RÅKOLLEN SKOLE, AVD FREDENLUND	
581101	BARNEVERN ADMINISTRASJON	6
582101	HELSEVERN BARN OG UNGE	2
583101	PP - TJENESTEN	1
584101	FOREBYGGENDE TJENESTER TIL BARN, UNGE OG FAMILIER (NY 2019)	1
752001	STAB TILDELINGSKONTORET	2
753101	STAB TJENESTER TIL FUNKSJONSHEMMEDE	3
753201	BOVEILEDNING NORD - ADM/FELLES	1
753301	BOVEILEDNING SYD/VEST - ADM/FELLES	1
753401	BOVEILEDNING ØST - ADM/FELLES	1
753701	DAGTILBUD ADM/FELLES	1
753801	TJ. TIL FUNKSJ.HEMMEDE - ADMINISTRASJON	2
754001	STAB OMSORGSSENTRE	1
754101	OMSORGSSENTRE NORD - ADM.	1
754201	OMSORGSSENTRE SYD - ADM.	1
754401	OMSORGSSENTRE VEST - ADM.	1
754601	OMSORGSSENTRE - ADMINISTRASJON	2
754701	ØSTSIDEN SYKEHJEM - ADMINISTRASJON	1
754801	FRSTAD KORTTIDSSENTER - AVDELING 1, ADM/FELLES 1 ETG (NY 2018)	1
755201	HJ.SYKEPLEIE NORD - NORD ADM/FELLES	1
755301	HJ.SYKEPLEIE SYD - ADM/FELLES	1
755401	HJ.SYKEPLEIE ØST - ADM/FELLES	1
755501	HJ.SYKEPLEIE VEST - ADM/FELLES	1
755601	HJ.SYKEPLEIE RESSURSENHET - ADM	2
755701	STAB MEDISINSKE TJENESTER (NY 2018)	1
755715	OVERGREPSMOTTAKET I ØSTFOLD (NY 2018)	1
757001	STAB FRISKLIV OG MESTRING	2
Sum utplukk		**100**

9.3. Litteratur- og dokumentliste

Følgende dokumenter ligger til grunn for faktafremstillingen:

- Prosedyre for organisering av personvern- og informasjonssikkerhetsarbeidet av 20.5.2019
- Prosedyre for digitaliseringssjefens ansvar og myndighetsområde av 20.5.2019
- Prosedyre for sikkerhetsleder – personvernombud av 17.12.2018
- Prosedyre for avvik personvern av 2.6.2019
- Prosedyre for risikovurdering informasjonssikkerhet og personvern av 2.6.2019
- Prosedyre for oppgradering og vedlikehold av programvare av 17.12.2018.
- Prosedyre for passord av 13.4.2012
- Prosedyre for konfigurasjonskontroll av 13.4.2012
- E-post av 17.12.2018
- Låserutiner og adgangskontroll av 17.12.2018
- Adgang til utstyr av 17.12.2018
- Antivirusprogram av 17.12.2018
- Avvik personvern av 2.6.2019
- Rutine for elektroniske plattformkurs av 24.9.2019
- Spam Phishing rutine
- Retningslinjer for lagring på eksterne nettsteder – Fildelingstjenester av 4.1.2016
- Retningslinjer for personvern og informasjonssikkerhet – ansatte av 4.4.2019
- Personvernerklæring av 1.10.2015
- IT-sikkerhetsreglement for FK-digitaliseringsavdelingen
- Sikkerhetsmål av 18.4.2012
- Kravspesifikasjon, standarder for IKT av 23.1.2019
- Dokumentasjon for Tilgangsportalen
- Oversikt over IT-sikkerhetsdokumenter, Datasikkerhet av 17.5.2017
- Oversikt over Firewall soner og tilganger fra Brukere og Internett
- Oversikt over brannmur DMZ soner i Fredrikstad kommune
- Klienter
- Dokumentasjon for Fredrikstad kommune NetBackup versjon 7.7.2
- Overordnet risiko- og sårbarhetsanalyse (ROS-analyse) 2014 av 20.6.2014

9.4. Spørreundersøkelsen

Cyberangrep og informasjonssikkerhet

Spørreundersøkelsen handler om Fredrikstad kommunes rutiner og arbeid med informasjonssikkerhet.

Den består av totalt 26 spørsmål/påstander/kommentarfelt og er sendt ut til samtlige ansatte i Fredrikstad kommune. For å få et mest mulig riktig bilde av kommunens praksis på feltet er din deltagelse veldig viktig. Undersøkelsen vil ta deg ca. 5-10 minutter å besvare.

Til orientering vil resultatet av undersøkelsen bli presentert slik at enkeltpersoner ikke kan gjenkjennes.

1) * Hvor i kommunen jobber du?

- Seksjon for kultur, miljø og byutvikling
- Seksjon for utdanning og oppvekst
- Seksjon for helse og velferd
- Seksjon for innovasjon og styring
- Seksjon for teknisk drift
- Seksjon for økonomi og organisasjonsutvikling
- Annet

2) * Hvilken stillingsprosent har du?

- 1 - 20 %
- 21 - 40 %
- 41 - 60 %
- 61 - 80%
- 80 % eller mer

3) * Hva slags type stilling har du?

- Fast ansatt
- Engasjement/vikariat
- Annet

4) * Hvor lenge har du jobbet i kommunen?

- ○ Under 1 år
- ○ 1 - 3 år
- ○ 4 - 6 år
- ○ Mer enn 6 år

5) * Har du lederansvar?

- ○ Ja
- ○ Nei

Denne informasjonen vises kun i forhåndsvisningen

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

Dersom spørsmålet Har du lederansvar? inneholder noen av disse alternativene

- Ja

6) På hvilket nivå er du leder?

- ○ Seksjon
- ○ Etat
- ○ Virksomhet
- ○ Avdeling
- ○ Faggruppe/Team
- ◉ Annet

Denne informasjonen vises kun i forhåndsvisningen

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

Dersom spørsmålet Har du lederansvar? inneholder noen av disse alternativene

- Ja

7) Har du myndighet til å gi tilganger til kommunens systemer?

- Ja
- Nei
- Vet ikke

Denne informasjonen vises kun i forhåndsvisningen

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

Dersom spørsmålet Har du myndighet til å gi tilganger til kommunens systemer? inneholder noen av disse alternativene

- Ja

8) Hvor viktig mener du det er at den ansatte har gjennomført e-kurs før du tildeler tilgang?

- Svært viktig
- Viktig
- Litt viktig
- Ikke viktig
- Vet ikke

9) * Har du fått informasjon om kommunens krav og forventninger til informasjonssikkerhet?

- Nei
- Ja, for mer enn ett år siden
- Ja, for under ett år siden
- Vet ikke

10) * Kjenner du til overordnet strategi for informasjonssikkerhet i kommunen?

- Kjenner ikke til den
- Kjenner til at den finnes, men har ikke kunnskap om den
- Kjenner til den, og har noe kunnskap om den
- Kjenner svært godt til den
- Vet ikke

11) * Har du fått opplæring i rutiner og prosedyrer for informasjonssikkerhet?

- Ja
- Nei
- Vet ikke

Denne informasjonen vises kun i forhåndsvisningen

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

Dersom spørsmålet Har du fått opplæring i rutiner og prosedyrer for informasjonssikkerhet? inneholder noen av disse alternativene

- Ja

12) Når fikk du denne opplæringen?

- Før jeg fikk tilgang til kommunens systemer
- Etter jeg fikk tilgang til kommunens systemer
- Både før og etter jeg fikk tilgang til kommunens systemer
- Vet ikke

Denne informasjonen vises kun i forhåndsvisningen

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

Dersom spørsmålet Har du fått opplæring i rutiner og prosedyrer for informasjonssikkerhet? inneholder noen av disse alternativene

- Ja'''

13) Mener du at du har fått tilstrekkelig med opplæring innenfor informasjonssikkerhet?

- Ja, det mener jeg
- Ja, men skulle gjerne hatt mer
- Nei, jeg har ikke fått tilstrekkelig opplæring
- Annet
- Vet ikke

14) * Har du lest "Retningslinjer for informasjonssikkerhet og personvern i Fredrikstad kommune", og signert på at du forplikter deg til å etterleve disse retningslinjene?

- Ja
- Nei
- Vet ikke

15) * Vet du hvem som er kommunens personvernombud?

- Ja
- Nei

16) Kjenner du til kommunens prosedyre vedrørende bruk av e-post?

- Kjenner ikke til prosedyre om e-post
- Kjenner til at det finnes en prosedyre, men har ikke kunnskap om den
- Kjenner til prosedyre om e-post, og har noe kunnskap om den
- Kjenner svært godt til prosedyre om e-post
- Vet ikke

17) Hender det at du benytter e-posten til private gjøremål? Du kan velge flere svaralternativer.

- [ ] Nei, aldri
- [ ] Ja, til å gjøre avtaler med familie og/eller venner
- [ ] Ja, til å bestille time hos behandler, lege, frisør eller annet
- [ ] Ja, som brukernavn på nettsider
- [ ] Ja, til å motta nyhetsbrev eller lignende som ikke er jobbrelatert
- [ ] Annet
- [ ] Vet ikke

18) Hvis du mottar e-post du mistenker for å være spam (søppelpost), eller et svindelforsøk - hvor sannsynlig er det at du sier ifra til IT-avdelingen?

- Svært sannsynlig
- Noe sannsynlig
- Lite sannsynlig
- Sannsynligvis ikke
- Vet ikke

19) * Kjenner du til "Retningslinjer for lagring på eksterne nettsteder - fildelingstjenester"?

- Kjenner ikke til retningslinjene
- Kjenner til at det finnes retningslinjer, men har ikke kunnskap om de
- Kjenner til retningslinjene, og har noe kunnskap om de
- Kjenner retningslinjene svært godt
- Vet ikke

20) * Er du kjent med prosedyren "Adgang til utstyr"?

- Kjenner ikke til prosedyren
- Kjenner til at det finnes en prosedyre, men har ikke kunnskap om den
- Kjenner til prosedyren, og har noe kunnskap om den
- Kjenner svært godt til prosedyren
- Vet ikke

21) * Disponerer du bærbar pc, iPad eller lignende, som eies av Fredrikstad kommune?

- Ja
- Nei
- Vet ikke

Denne informasjonen vises kun i forhåndsvisningen

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

Dersom spørsmålet Disponerer du bærbar pc, iPad eller lignende, som eies av Fredrikstad kommune? inneholder noen av disse alternativene

- Ja

22) Har det hendt at noen andre har brukt utstyret? Samboer, ektefelle, barn eller lignende?

- Ja
- Nei
- Vet ikke

23) Kjenner du til kommunens prosedyre "Avvik personvern"?

- Kjenner ikke til prosedyren
- Kjenner til at prosedyren finnes, men har ikke kunnskap om den
- Kjenner til prosedyren, og har noe kunnskap om den
- Kjenner svært godt til prosedyren
- Vet ikke

24) Har du fått opplæring i rapportering av avvik i informasjonssystemene?

- Nei
- Ja, for mindre enn to år siden
- Ja, for mer enn to år siden
- Vet ikke

25) Kjenner du til kommunens prosedyre "Innsyn i e-post og annet elektronisk materiale"?

- Kjenner ikke til prosedyren
- Kjenner til at prosedyren finnes, men har ikke kunnskap om den
- Kjenner til prosedyren, og har noe kunnskap om den
- Kjenner svært godt til prosedyren
- Vet ikke

26) Har du andre kommentarer vedrørende kommunens arbeid med cyberangrep/informasjonssikkerhet?